3rd International Conference on
Cryptography, Cyber Security
and Information Warfare
(3rd CryCybIW)
Hellenic Military Academy
26th -27th May 2016

Abstracts

Editor: Nicholas J. Daras
Contents

Invited Speakers (Amphitheatre KSIROS)

- Michael Th. Rassias: On Certain Cotangent Sums Related to the Riemann Hypothesis
- Ross W. Tsagalidis: Strategic Leadership in Cyberspace & Collaboration Gov – Academia

Thursday 26 May 2016

Electronic Crime, Ethics and IT Risk Management in Cyberspace (Amphitheatre PENTEAS)

- S. Sofiou: Ethics in Cyberspace - Cyber Security
- M. Dimarogkona and P. Stefaneas: Computer Ethics and Institutions

Cryptology Methods and Network Applications (Amphitheatre CHRISOFAKIS)

- A. V. Doumas: An Occupancy Type Problem and its Generalization
- P. Fika: Stochastic Estimates for the Trace of Functions of Matrices with Applications to Networks
- C. L. Asimomytis, P. N. Koumantos and P. K. Pavlakos: The Second Law of Thermodynamics and Stochastic Quantum-Thermodynamical Integrals
- V. C. Moussas: Adaptive Traffic Modeling for Network Anomaly Detection

New Technologies in Security Systems (Amphitheatre PENTEAS)

- M. Koutsoupidou and I. Karanasiou: THz Technology for Homeland Security
- F. Pelesís: Printed Flexible Electronics in Military Applications
- K. Kitsakis, N. Petrou, I. Tanos and J. Kechagias: Design and 3d Printing of a Robotic Arm

Economic Information Warfare (Amphitheatre CHRISOFAKIS)

- I. D. Salavrakos: Economic, Financial Warfare and Economic Espionage: From Total War to Modernity
- K. Athanasouli: Economic Implications of the Rise of Information Warfare, Cyber-War and Cyber-Security
M. Chalikias, P. Lalou and M. Skordilis: Mathematical Modeling of a Bank Data Set: The Case of Greek Oligopoly

**Cyber Warfare** *(Amphitheatre PENTEAS)*

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>E. Mitakidis and D. Taketzis</td>
<td>MalOrbot: An Android Malware to Bridge the Mixes in Tor</td>
</tr>
<tr>
<td>S. Gasteratos, V. Vlachos, M. Dimou and K. Papapanagiotou</td>
<td>The Hackademic Challenges Project: Teaching future cyber warriors</td>
</tr>
<tr>
<td>G. Karapilafis</td>
<td>Artificial Intelligence in Cyber-Defense</td>
</tr>
</tbody>
</table>

**Military Information Support Operations in the International Contemporary Geostrategic Environment** *(Amphitheatre CHRISOFAKIS)*

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>K. Grivas</td>
<td>Omnipotent, Omniscient and Omnipresent Commanders. The Impact of a Cultural Paradigm Derived from a Secularized Christianity on the Philosophy of Network Centric Warfare</td>
</tr>
<tr>
<td>A. Paris and V. Vrisagotis</td>
<td>Modeling Supply Disruptions for Logistics Network of R Defense Suppliers to a Battlefield</td>
</tr>
<tr>
<td>P. P. Laimos,, M. Chronopoulos, C. Laimou and N. Atanasova</td>
<td>Case Studies Analysis from Attacks in the Supply Chain and Losses with the Use of GPS or GSM Jammers by the Attackers</td>
</tr>
<tr>
<td>Th. Zikos, D. Zaires and N. V. Karadimas</td>
<td>Automated Procedure for Utilization - Operation of Hellenic Army Empty Warehouses</td>
</tr>
</tbody>
</table>

**Cyber Security** *(Amphitheatre PENTEAS)*

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>K. Demertzis and L. Iliadis</td>
<td>A Computational Intelligence System for Identification Cyber-Attacks on the Smart Energy Grids</td>
</tr>
<tr>
<td>D. P. Iracleous and A. Papadimitraki</td>
<td>Nature Inspired Algorithms for Intrusion Detection Systems</td>
</tr>
<tr>
<td>K. Demertzis and L. Iliadis</td>
<td>Real-time Computational Intelligence Protection Framework Against Advanced Persistent Threats</td>
</tr>
<tr>
<td>A. Manaras, V. Vlachos A. Papanikolaou and C. Ilioudis</td>
<td>Analyzing Epidemiological Characteristics of Biological Viruses and Correlation with Computer Viruses</td>
</tr>
</tbody>
</table>

**Information Based Psychology in Social Structures** *(Amphitheatre CHRISOFAKIS)*

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>M. Sakalaki</td>
<td>The Uncertainty Surrounding Information’s Economic Value</td>
</tr>
</tbody>
</table>

Hellenic Military Academy
<table>
<thead>
<tr>
<th>Authors/Dates/Institutions</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>V. Ignatiou Karamanoli</td>
<td>Information and Emotions: Imposed Hope, Fear, Desire and their Impacts to Human Behavior</td>
<td>93</td>
</tr>
<tr>
<td>K. Papachristopoulos</td>
<td>Organizational Social Structure and Motivation as Predictors of Employees’ Information Sharing Attitudes</td>
<td>94</td>
</tr>
<tr>
<td>V. Ignatiou-Karamanoli and N. Bardis</td>
<td>Information Value and Influence During Period of Uncertainty Using Leaflets and Social Network: the Example of Refugees in Greece</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>Friday 27 May 2016</td>
<td>97</td>
</tr>
<tr>
<td><strong>Mathematical Foundations of Cyber-Defense Methods</strong> (&lt;Amphitheatre PENTEAS&gt;)</td>
<td></td>
<td>99</td>
</tr>
<tr>
<td>N. J. Daras</td>
<td>On the Mathematical Definition of Cyberspace</td>
<td>101</td>
</tr>
<tr>
<td>A. Alexopoulos</td>
<td>Mathematical Modeling of Cyber-Defense Methods</td>
<td>107</td>
</tr>
<tr>
<td>N. J. Daras</td>
<td>Mathematical Description of Cyber-Attacks and Proactive Defense</td>
<td>108</td>
</tr>
<tr>
<td><strong>Communication Systems and Networks</strong> (&lt;Amphitheatre CHRISOFAKIS&gt;)</td>
<td></td>
<td>111</td>
</tr>
<tr>
<td>D. Syvridis and A. Argyris</td>
<td>Coupled Semiconductor Lasers Operating in a Chaotic Regime: Experiments on Synchrony, Clustering and Encryption Techniques</td>
<td>113</td>
</tr>
<tr>
<td>I. Triantafyllou</td>
<td>Bivariate Copulas-Based Models for Communications Networks</td>
<td>116</td>
</tr>
<tr>
<td>N. Doukas</td>
<td>Security in a Remote Controlled UAV</td>
<td>117</td>
</tr>
<tr>
<td><strong>Encryption Methods</strong> (&lt;Amphitheatre PENTEAS&gt;)</td>
<td></td>
<td>119</td>
</tr>
<tr>
<td>D. P. Kalogeras</td>
<td>RNA/DNA Encryption Method- Another Encryption Algorithm</td>
<td>121</td>
</tr>
<tr>
<td>K. Draziotis and A. Papadopoulou</td>
<td>Improved Algorithms for Hard Knapsack Problems and its Variants</td>
<td>122</td>
</tr>
<tr>
<td>D. Poulakis</td>
<td>A Voting Scheme Based on Elliptic Curves</td>
<td>124</td>
</tr>
<tr>
<td><strong>Communications Security</strong> (&lt;Amphitheatre CHRISOFAKIS&gt;)</td>
<td></td>
<td>125</td>
</tr>
<tr>
<td>G. Theodorou, N. Kranitis, A. Tsigkanos, and A. Paschalidis</td>
<td>Implementation of the AES-GCM</td>
<td>127</td>
</tr>
<tr>
<td>C. Mesaritakis, A. Kapsalis, M. Akriotou and D. Syvridis</td>
<td>Authenticated Encryption Algorithm Targeting Xilinx’s Defense-Grade Virtex-5Q FPGAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Photonic Physical Unclonable Functions as a Secure Key Generator for Cryptographic Applications</td>
<td>131</td>
</tr>
<tr>
<td>Y. Kiouvakis and P. Stefaneas</td>
<td>Towards Abstract Logics for Secure Communication</td>
<td>135</td>
</tr>
</tbody>
</table>
# Cryptosystems and Computations

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>K. Limniotis and N. Kolokotronis</td>
<td>Cryptographic Boolean functions with Maximum Algebraic Immunity</td>
<td>141</td>
</tr>
<tr>
<td>I.-P. Krommyda, G.C. Meletiou, D.S. Triantafyllou, and M.N. Vrahatis</td>
<td>Cryptographic Techniques for Secure Linear Computations in the Supply Chain Management</td>
<td>144</td>
</tr>
</tbody>
</table>

# Military Communications

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>M.Gargalakos, I.Karanasiou, R. Makri and N.K. Uzunoglu</td>
<td>The use of Millimeter Wave Frequencies in Future Military Communications</td>
<td>149</td>
</tr>
<tr>
<td>D. P. Kalogeras</td>
<td>Simplified Jamming Methods for Direct Sequence Spread Spectrum (DS/SS) Systems</td>
<td>150</td>
</tr>
<tr>
<td>K. A. Psilopanagiotis</td>
<td>Computational Simulation of Passive Synchronization Method for Frequency Hopping Systems</td>
<td>151</td>
</tr>
</tbody>
</table>

# Engineering Applications to Security Aspects

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>D. Mouzakis</td>
<td>Time Temperature Superposition Principle: application to process dynamic mechanical analysis data of environmentally aged Carbon Fiber Reinforced Composites</td>
<td>157</td>
</tr>
<tr>
<td>A. K. Lazopoulous</td>
<td>Analyzing Epidemiological Characteristics of Biological Viruses and Correlation with Computer Viruses</td>
<td>159</td>
</tr>
<tr>
<td>S.K. Georgantzinos</td>
<td>Dynamic Response of Protein Microtubules</td>
<td>162</td>
</tr>
<tr>
<td>T. G. Kostis</td>
<td>The Stealth Concept as Explained by Low Probability of Intercept &amp; Low Observability</td>
<td>163</td>
</tr>
</tbody>
</table>

# City Risks and Privacy

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>N. Papadakis and C. Raftopoulos</td>
<td>RST-Invariant Block-based Watermarking for Image Regions</td>
<td>167</td>
</tr>
<tr>
<td>N. Bakalos</td>
<td>Tackling Privacy and QoS issues in the Cloud</td>
<td>168</td>
</tr>
<tr>
<td>A. Madia, S.E. Nikoletseas, Y.C. Stamatiou, D. Tsolovos and V. Vlachos</td>
<td>Crowd Sourcing Based Privacy Threat Analysis and Alerting</td>
<td>169</td>
</tr>
<tr>
<td>N. Papadakis and A. Litke</td>
<td>City.Risks: Avoiding and Mitigating Safety Risks in Urban Environments</td>
<td>174</td>
</tr>
</tbody>
</table>
### Chaos and Randomness in Cryptography  
**Amphitheatre PENTEAS**

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. S. Andreatos</td>
<td>A Smart Port Knocking Mechanism for Hiding the SSH Port from Attackers</td>
<td>177</td>
</tr>
<tr>
<td>G. Marinakis</td>
<td>Optimum Sampling of Cipher Keys and Output Streams for Cryptographic Tests</td>
<td>180</td>
</tr>
<tr>
<td>A. S. Andreatos and A. P. Leros</td>
<td>Optimization of Hénon Chaotic Coefficients Based on Lyapunov Exponents</td>
<td>181</td>
</tr>
</tbody>
</table>

### Cloud Security and Big Data Analytics  
**Amphitheatre CHRISOFAKIS**

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>N. Bardis</td>
<td>Secure Data Restoration in Cloud Systems</td>
<td>187</td>
</tr>
<tr>
<td>N. Doukas</td>
<td>Big Data Analytics for Crisis Detection and Management</td>
<td>188</td>
</tr>
<tr>
<td>F. Toufeksis, E. Dontas, N. Doukas and N. Bardis</td>
<td>Secure System for Refugee Flow Management</td>
<td>189</td>
</tr>
</tbody>
</table>
Invited Speakers
On Certain Cotangent Sums
Related to the Riemann Hypothesis

Michael Th. Rassias

Institute for Advanced Study, Einstein Drive, Princeton,
New Jersey 08540, U. S. A.

and

Institute of Mathematics, University of Zürich, Winterthurerstrasse 190,
CH-8057 Zürich, Switzerland

E-mails: michailrassias@math.princeton.edu and michail.rassias@math.uzh.ch

Abstract Certain cotangent sums are associated to the zeros of the Estermann zeta function and they have also proven to be of importance in the Nyman-Beurling criterion for the Riemann Hypothesis.

The main result presented in this talk is the existence of a unique positive measure $\mu$ on $\mathbb{R}$ with respect to which certain normalized cotangent sums are equidistributed, hence providing crucial information for the behavior of the cotangent sums in question. $\square$
Strategic Leadership in Cyberspace & Collaboration Gov – Academia +

“Hope for the best, but prepare for the worst. And proceed on what we actually know.”

Wladimiros Ross Tsagalidis

Department of Computer and Systems Sciences,
Center for Strategic Leadership and Cyber Security,
Stockholm University, 164 07 Kista Sweden

E-mail: ross@dsv.su.se

Abstract The Internet of Things, the revival of Internet, even if it’s not something just pop-upped from nowhere though more complex than ever, has the potential to transform the way we live, work and communicate. By all concurrences the growth in IoT connected devices will provide significant benefits, yet as they proliferate, the security and privacy risks are augmented. Left unchecked society could be faced with scenarios where hundreds of thousands of devices are compromised simultaneously, creating uncertainty, chaotic conditions and disrupting planned actions.

Security of Things in the Internet-of-Everything is the challenge much to the technology but much more to humans.

The questions that evolve are:
1. Who's responsible, who feels responsible and who's going to take actions for the security and safety of cyber-physical systems?
2. How cohesive are certain roles, i.e. CEO, CFO, CIO, CTO, CSO, and CDO with each other?
3. Are you prepared to act in the event of a crisis or incident? Do you know how you should communicate and who should do it?
4. Can you provide assurance to stakeholders on your cyber security policy?
5. Does your board communicates something about the importance of cyber security?
Electronic Crime, Ethics and IT Risk Management in Cyberspace
Ethics in Cyberspace - Cyber Security

Stamatia Sofiou
Department of Theoretical Sciences, Hellenic Military Academy,
Vari, GR-16673, Greece
E-mail: dr.sofioustamatia@gmail.com

Key words: cyber ethics • cyber attack • cyber war • cyber security • jus ad bellum • jus in bello • self-regulation

Abstract  The present announcement attempts to link ethics to cyberspace, common ground of action and reaction of man and technology, with regard to the issue of security when taking into consideration “quiet, asymmetrical threats,” namely electronic crime, cyber attacks and cyber war - all principles of jus ad bellum and jus in bello.

The ethical approach to cyber space examines ethical dilemmas, the result of divergent conduct that disturbs the system of a responsible administration, while restoring fundamental democratic principles that govern a well-governed state, i.e. freedom, prosperity and happiness.

Internationally, cyber war has taken huge dimensions as cyber attacks increase every day with regard to complexity. It constitutes a great challenge regarding stability, prosperity and security in a region. Today, no one is wondering whether there is going to be an attack but when there is going to be an attack. To face “asymmetrical threats,” we need the active, ethical cooperation of all factors whose common interest is the regular function of cyberspace. Powerful governments need to assume responsibility with regard to their actions as they are responsible for the protection of their citizens: “Prosperity in a country depends on the security of its cyberspace” (Barack H. Obama, 29 May 2009).

Cyberspace is the new expanded environment of the collective Nous. It is created by the Internet and telecommunication networks. The new digital environment or the new “Far West” of the post-industrial era of the 21st century demands the abolition of physical boundaries and “gives prominence to information as the driving
force of the new era” ([2]). It constitutes a field of technological achievements, aiming to influence human thought and redefine human relations, while defining “the site of human engagement with each other and self-creation” ([3]).

Technology itself is neutral: it is neither good nor bad. The benign or malignant circulation of information lends it a positive or negative character in the interactive function of cyberspace and its progressive evolution. According to Aristotle, in Nicomachean Ethics, “in republics governed by law and social values there is no demagogue” ([1]).

Ethics in cyberspace balances between uneducated progress and threat. The safe use of cyberspace demands a qualitative, not a quantitative regulation. As Socrates said 2500 years ago, “self-control” is the constant component of ethical conduct. What is more, according to Professor A. Merezhko, self-regulation preserves the anthropocentric character of the technological “common inheritance of the human species” ([4]).

Contemporary forms of attacks are reconsidering defence and security issues on a national and international level while they are setting masterminds thinking about the best ways to face their catastrophic consequences. Cyber war, in this dynamically evolving environment, comprises one of the most serious threats because it aims to destabilize society by striking the crucial sectors of a country’s infrastructure. □

References

[1]. Aristotle: Nicomachean Ethics
[2]. Διακλαδική Επιθεώρηση, Ιούλιος-Οκτώβριος 2007:48-51
Attacks against Information Systems in the E.U. Environment: Legal Texts & the Joint Cybercrime Action Taskforce (J-CAT) Model

Papathanasiou Anastasios¹, Germanos Georgios²
Cyber Crime Division – Hellenic Police
E-mails: a.papathanasiou@cybercrimeunit.gr¹, g.germanos@cybercrimeunit.gr²

Abstract Rarely, nowadays, are cybercrime and cyber incidents limited to the boundaries of a single state. Their investigation requires the representatives of law enforcement authorities, the representatives of the Computer Emergency Response Teams (CERTs) and the competent prosecutors and magistrates to seek the assistance and cooperation of companies, bodies and organizations established in other Member States, either within or outside the European Union.

Especially for the European Union, cyber security issues and effective response to cyber incidents have led to the co-decision and drafting of legal texts, with compulsory or voluntary compliance for the Member States. Characteristic and representative texts are the Convention on Cybercrime (better known as the Budapest Convention - 2001), the Directive 2013/40 / EU of the European Parliament and of the Council (2013) on attacks against information systems and the European Union Strategy for cyber security "to an open, safe and secure cyberspace" (2013), where Member States have clearly declared their will to formulate ideal conditions in cyberspace to ensure the smooth and healthy development of social and economic activities.

Decisive role, however, in the actions of the competent bodies of the Member States plays the contribution of the European agencies, in particular Europol, Eurojust and ENISA. Particular mention should be made in the Joint Cybercrime Action Taskforce (J-CAT) model. J-CAT is a group that operates under the umbrella of the European Cybercrime Centre (EC3) of Europol. Its members are law enforcers - experts in the investigation of cybercrime from several States. The list of crimes, in the
investigation of which J-CAT is participating, includes attacks against information systems with the use of malicious software (such as botnets).

The J-CAT has the ability to coordinate large-scale operations to arrest criminals, seize illegally used equipment and collect digital evidence, not limited to the territorial boundaries of a single state. Through its activities, it was demonstrated that close cooperation between states is not only theoretical discussion, but a reality with tangible and enviable results.

Of course, effective collaboration requires the harmonization of national laws concerning cyber crime; however, this model can be emulated by other organizations with transnational action, not only in the field of law enforcement. ❑
Computer Ethics and Institutions

Maria Dimarogkona¹ and Petros Stefaneas²

¹,² School of Applied Mathematics and Physical Sciences, National Technical University of Athens, Department of Mathematics, Herron Polytechniou 9, 15780 Zografou, Greece

E-mails:¹ mdimarog@central.ntua.gr and ² petros@math.ntua.gr

Abstract Computer ethics as a distinct field of study is concerned with issues like privacy, accessibility, work ethics, and computer crime. What we suggest is a hybrid semantics of computer science ethics, based on the theory of institutions. In particular, we suggest that a logical framework appropriate for computer science ethics would be a combination of Grothendieck and Kripke institutions.

One of the main benefits of having such a semantics, apart from the possible applications in language design, system specification and new algorithms, is the possibility of performing computer supported (or semi-automated) computer ethics. But in order to provide such a semantics various different logics need to be employed, if we are to include all the different concepts involved. More specifically, we need deontic logic, which is concerned with obligation, permission, duties, rights and related concepts; action logic, which in computer science provides a means to reason about programs, that is, the execution of programs and their effects, as well as the actions of getting and giving information, preventing people from believing falsehoods and related concepts; and epistemic logic, which is a subfield of modal logic concerned with reasoning about knowledge.

Abstract model theory in the form of institutions theory gives us a flexible conceptual/logical framework that can encompass all these different logics, allowing us – at the same time - to abstract away from the details of each logic while studying computer ethics issues, and concentrate on the bigger picture.

The theory of institutions was developed in the 90s by Goguen and Burstall to tackle the explosion of logical systems used in computer science. An institution
constitutes, in essence, a formal definition of the notion of a logic or logical system including a translation mechanism between different such systems. The approach is based on a Tarskian definition of truth, which is treated as invariant under change of notation. Although institutions were initially introduced to fulfill the practical need for a logic-independent computer science, their field of application has been growing ever since. In fact their logic-independent approach seems to offer a much needed change of perspective in fields as diverse as philosophy of science and aesthetics. In the case of computer ethics, they constitute a promising approach not only because of the variety of logics involved, but also because they allow for the performance of computer supported computer ethics.  

Integrated Risk Management: A Tool for Efficiency & Compliance

Ioannis A. Issaris

Omikron Systems, 1, Artis str, GR-18345 Athens, Greece
E-mail: info@osys.gr

Abstract IT risk assessments (and other relevant mechanisms), especially those required or implied by international standards like ISO 27001 or ISO 20000, has been seen as the responsibility of the IT staff, as those individuals have the best understanding of the components of the control infrastructure.

Moreover, IT risk assessments have typically been performed within the IT department with little or no input from others.

This approach has limitations. As systems have become more complex, integrated and connected to third parties, the security and controls budget quickly reaches its limitations.

Therefore, to ensure best use of the available resources, IT should become more efficient and understand the relative significance of different sets of systems, applications, data, storage and communication mechanisms.

To meet such requirements, organizations should perform IT risk assessments that employ the whole enterprise and include all stakeholders to ensure that all aspects of the IT organization are addressed, including hardware and software, employee awareness training, and business processes.

This paper describes a risk management & compliance tool that allow organizations to assess, identify and modify their overall security posture and to enable security, operations, organizational management and other personnel to collaborate during this sensitive process. The tool that is presented is also used to obtain organizational management’s commitment to allocate resources and implement the appropriate security solutions. □
Cryptology Methods and
Network Modeling
An Occupancy Type Problem and its Generalization

Aristides V. Doumas
MSc, PhD

Department of Mathematics, National Technical University of Athens
Zografou Campus, GR-157 80 Athens, Greece
E-mail: aris.doumas@hotmail.com

Abstract We deal with the following occupancy type problem rising from the area of the basic probability theory. Persons $p_1, p_2, \ldots, p_{100}$ have been assigned seats $s_1, s_2, \ldots, s_{100}$ in an airplane. The passengers board in numerical order. Unable to follow directions, $p_1$ chooses a seat uniformly at random. Subsequent boarders take their assigned seat if available, and choose a vacant seat at random if not. Find the probability that $p_{100}$ sits in $s_{100}$. We briefly present a well-known solution, since the problem has been discussed in several websites. Then we present a new solution for the general problem which asks on the probability that $p_k$ sits in $s_k$, where $k \geq 2$.

Occupancy problems play an important role in probability theory and its applications, among others in Cryptography (see, e.g., [1], [2]). In this talk we will present a well-known problem which falls in this category. Moreover, we will obtain a proof on its generalization, which is of particular interest. The approach selected for the general problem is different than the one of the initial problem.

References


Stochastic Estimates for the Trace of Functions of Matrices with Applications to Networks

Paraskevi Fika
PhD(c) Department of Mathematics, National and Kapodistrian University of Athens, Panepistimiopolis, GR-157 84 Ilissia, Athens
Email: pfika@math.uoa.gr

Abstract The necessity of evaluating the trace of functions of matrices arises in many applications such as in network analysis and graph theory. The computation of the trace of a function of a matrix can have a high computational cost, especially for large matrices that arise in real world networks like Facebook, Wikipedia, Airlines, Military networks and other complex networks that provide models for physical, biological, engineered or social systems (e.g., molecular structure, gene and protein interaction, food webs, telecommunication and transportation networks, power grids, energy, economic and social networks). Therefore, it is necessary to study and develop estimates for the trace of functions of matrices, aiming to the avoidance of the explicit computation of the matrix function.

In this work, stochastic estimates for the trace of functions of matrices \( f(A) \), denoted as \( Tr(f(A)) \), are developed, where \( A \) is a symmetric matrix of dimension \( p \) and \( f \) a suitable smooth function defined on the spectrum of the matrix \( A \). The derived estimates require only some inner products and few matrix-vector products and thus they provide a computationally efficient tool for approximating the \( Tr(f(A)) \).

It can be proved that the expected value of the quantity \( x^T f(A)x \), for suitable vector \( x \), equals to the \( Tr(f(A)) \). Thus, the stochastic estimates are based on the computation of the quantity \( \sum_i^N x_i^T f(A)x_i / N \) for different sample vectors \( x_i \), where \( N \) is the sample size (the number of the sample vectors).

The bilinear form \( x_i^T f(A)x_i \) can be approximated, without computing the matrix \( f(A) \) explicitly, by using an extrapolation method for the moments of the matrix \( A \) or Gauss quadrature rules.
Moreover, since the proposed estimates are of a statistical nature, it is natural to expect that the application of some statistical designs may improve their quality and their effectiveness in estimating the trace $Tr(f(A))$.

Various statistical designs will be studied and compared, arising from Hadamard-like sampling or the CCD (Central Composite design). Numerical examples stemming from real world networks will be discussed.

References

The Second Law of Thermodynamics and Stochastic Quantum-Thermodynamical Integrals

Christos L. Asimomytis ¹, Panagiotis N. Koumantos ² and Panayiotis K. Pavlakos ³

¹³ Department of Mathematics, University of Athens, Panepistimiopolis GR-15784 Athens, Greece
² Department of Physics, University of Athens, Panepistimiopolis GR-15784 Athens, Greece

E-mails: xlasimom@otenet.gr ¹, pnkoumantos@gmail.com ², ppavlakos@math.uoa.gr ³

Abstract In this work we are interesting to develop a connection between the Second Law of Thermodynamics and stochastic quantum-thermodynamical integrals taking values in a quantum-thermodynamical system endowed with an ordered Hilbert structure. We use and apply previous results and ideas of M. Feinberg and R. Lavine, R. Giles, R. S. Ingarden and A. Kossakowski, K. Kraus, E. Lieb and J. Yngvason, under the Carathéodory Second Law of Thermodynamics, the mean of adiabatic accessibility (transition) and the Kelvin-Planck Second Law of Thermodynamics.

References

Adaptive Traffic Modeling for Network Anomaly Detection

Vassilios C. Moussas

School of Technological Applications,
Technological Educational Institution (T.E.I.) of Athens,
GR-12210 Egaleo, Greece,

E-mail: vmouss@teiath.gr

Keywords:  traffic modelling • fault detection • anomaly detection • network simulation • network modelling • adaptive estimation • forecasting

Abstract  With the rapid expansion of computer networks, security has become a crucial issue, either for small home networks or large corporate intranets. A good way to detect illegitimate use of a network is through traffic monitoring and classification. Consistent modelling of typical network activity can help separate the normal use of a network from an intruder activity or an unusual user activity.

In addition to security, traffic monitoring and modelling are essential in order to determine the network’s current state (normal or faulty) and predict its future trends. In this work an adaptive traffic modelling & estimation method for network unusual activity and intrusion detection is presented, using simple and widely found sets of traffic data, such as bandwidth utilization. Bandwidth use is the most common set of network traffic data as almost all network administrators monitor periodically the bandwidth utilization for their servers, routers, LAN users, and network connections.

The proposed method uses past traffic data to learn and model (ARMA, State-space, etc.) the normal/typical periodic behaviour (hourly, daily, yearly) of a network connection. In addition, any known faulty/abuse/anomaly states can be modelled and stored in a continuously updated base. An adaptive detection mechanism applies the on-line data, collected by the monitoring program, to all available traffic models. If the traffic pattern does not match the expected behaviour of the network connection an anomaly is detected, and furthermore, if the pattern matches a known case, the type of anomaly can be identified.
The advantage of the method is the use of already available measurements at the network nodes, usually collected through the MIB of the network components. The method can perform equally well off-line or in real-time depending on the sampling interval required by the network monitoring programs. Real traffic data were used and real world cases were tested from a university campus network. The applied adaptive multi-model estimation algorithm identified successfully the unusual activities.

References


New Technologies in Security Systems
THz Technology for Homeland Security

Maria Koutsoupidou ¹ and Irene Karanasiou ¹,²

¹Advanced Electronics and Telecommunication Systems Laboratory, Department of Mathematics & Engineering Sciences, Hellenic Military Academy, GR-16673 Vari, Greece
E-mail: ikaran@esd.ece.ntua.gr

²Informatics Laboratory, Department of Mathematics & Engineering Sciences, Hellenic Military Academy, Vari, GR-16673, Greece
E-mail: mkouts@mail.ntua.gr

Abstract The THz spectrum lies between the infrared and microwave electromagnetic regimes and it is typically ranging from 0.1 to 10 THz. THz radiation, though it has recently attracted an increased interest because of its characteristic interaction with mater, like metal, plastic and water, it had been neglected for a long time due to the difficulties developing effective systems for generation, detection and processing of THz waves ([1]). Additionally, as a ‘non-ionizing’ radiation, it is harmless to biological tissues. These unique properties have rendered THz frequencies useful in a large variety of applications (homeland security, military, medical, chemical, etc).

Specifically, THz technology is a promising candidate for detecting chemical substances, as explosives or drugs, disclosed in paper, plastic or other type of non-metallic package. The large molecules of those materials provide a unique THz spectroscopic response (THz “fingerprint”) aiding to their positive identification and characterization.

Herein, the results of the spectroscopic analysis of various mixtures chemical substances are presented. Different materials have been tested using a novel THz Time Domain Spectrometer (THz-TDS) in transmission geometry. The broadband THz pulse generation and detection are performed by two dipole shaped photoconductive antennas. The emitter antenna is biased by a femtosecond laser pulse. The detection of the THz pulse is performed by sampling the THz path in the time domain using an optical delay unit ([2]). Additionally, a setup of lenses is used to effectively focus the THz beam between the antennas and the sample.
The advantage of using the THz-TDS technique lies on the fact that both the amplitude and the phase of the received signal are measured, acquiring information regarding the spectral properties and thickness of the samples. The results show that it is feasible to classify various chemical by their THz “fingerprint”.

References


Printed Flexible Electronics in Military Applications

Fotios Pelesis
Mechanical Engineer (B. Eng, Ph.D.)
16, Marathonos Street, Vrilissia, Athens, Greece

E-mail: pelesis7@hotmail.com

Abstract Printed electronics is an emerging technology with good prospects for success which has the potential to substitute the manufacture of conventional electronics and introduce innovative products to the market in the near future. This revolutionary concept changes the end-product applicability by introducing physical flexibility to the integrated system. From a commercial perspective, flexible electronics aim to dominate the short- and mid-life electronics global market by combining cost effectiveness, unique mechanical properties and the ability to create large-scale unit. They cover a wide range of applications such as sensors, energy harvesting, energy supplying, communications and displays.

The specific presentation is divided into two parts: the first part performs an introduction to printing technology, the state-of-the-art inks and substrates needed for the fabrication of printed flexible electronics and the research areas which have attracted the global scientific community’s attention. The second part discusses how this innovative technology can be used in the military by presenting realistic applications and products. It is strongly believed that, the adoption of this technology by the Greek military could substantially improve its capabilities in the battlefield. In addition, emphasis is given on the opportunities that the Greek Universities and the domestic industry should take advantage of regarding research and manufacture of printed flexible military products.
Design and 3d Printing of a Robot Arm

Konstantinos Kitsakis 1, Nikos Petrou 2,
Ilias Tanos 3, and John Kechagias 4

1, 4 Department of Mechanical Engineering, TEI of Thessaly, Larissa, GR-41110, Greece
E-mails: 1 kitsakis@teithessaly.gr and 4 jkechag@teithessaly.gr

2, 3 Digital Idea, Lithaiou 19, Larissa, GR-41335, Greece
E-mails: 2 petrou@digitalidea.gr and 3 tanos@digitalidea.gr

Abstract 3D printing, a section of Additive Manufacturing, is the manufacturing process of three-dimensional objects by printing or adding very thin layers of material. It is already widely used in Rapid Prototyping, Rapid Manufacturing, Health, Dental, Orthopedics, Jewelry and Architecture while its usage in other areas is constantly expanding.

3D objects are created in a digital form, either by designing, using a Computer Aided Design application on a computer, or by scanning, using 3d digitizing devices or photographs taken around the perimeter of the object. The digital form items having the appropriate data format are guided in the three-dimensional printer, where they are converted into very thin horizontal slices and sequentially printed one above the other, to produce the completed object.

This presentation will introduce the main design concepts and the 3D printing procedure of a robotic arm. The robotic arm has one degree of freedom, namely one rotation axis and consists of two parts, a motor support base and the controlled arm.

The design of the two objects is done using the free 3D design application 123D Design from AUTODESK. The first session presents the interface of the application and the navigation tools. Following that is the design of the base object using the box, primitive tool. Modification, molding, alignment, and combination techniques are applied, to obtain the desired form and the suitable slot for placement of the servomotor. For the construction of the arm another method is been followed.
An outline is firstly designed with 2D drawing tools, such as rectangle, circle and polyline and when the 2D sketch is completed the extrusion tool is applied perpendicular to the surface, for the creation of the 3D object arm. Finally, the two objects are stored in an appropriate 3D file format (STL) that can be identified by 3D-printing applications.

Using the free application MakerBot, the file from the previous step is imported and positioning, rotation and scaling on the virtual printing surface can be applied on the objects. The material to be used, quality, speed and temperature of the head, usage of draft and support materials are the main printing options. The Print Preview command shows all the individual levels from bottom to top which will be printed out and create the integrated 3D object. At the final session the parts are printed out, checked and assembled to complete the construction.

The main purpose of this paper is to provide the procedures and settings needed to construct 3D objects from scratch with easy to use but free software and cost effective printing devices. □
Economic Information Warfare

AMPHITHEATRE CHRISOFAKIS
Chair: Kyriaki Athanasouli
Economic, Financial Warfare and Economic Espionage: From Total War to Modernity

Dr. Ioannis-Dionysios Salavrakos
Visiting Professor, Hellenic Air-Force Academy,
Visiting Professor, Hellenic Navy, Command and Control Naval School,
Greece

E-mail: isalavra@uwg.gr

Abstract The Intellectual aspiration of the paper is to cast light to a rather neglected aspect of war that of Economic and Financial warfare and economic espionage. The paper argues that during various conflicts the belligerent countries used various economic and financial techniques as weapons against their opponents. These include:

1) Causing inflation,
2) Depreciation of enemy’s currency in the international financial markets,
3) Causing “financial drowning” by terminating bank loans to the economy of the enemy,
4) Imposition of capital controls and asset freezing,
5) Creating trade barriers which destroy enemy’s trade with the rest of the world especially on critical goods such as raw materials, as well as food supplies,
6) Follow a policy of scorched earth,
7) Creating negative expectations related to the future of the enemy’s economy by spreading unsubstantiated rumors to international press,
8) Follow a slave labor policy with the enemy war prisoners,
9) Targeting enemy’s industrial base and infrastructure,
10) Targeting enemy’s entrepreneurial class by pointing out that they should continue the “business as usual” policy before the war thus undermine the war effort of the opponent.

The aim of these techniques is to destroy the moral of the enemy thus the home front assuming that if this occurs then the will of the enemy to fight will be perished and the enemy will seek a peaceful resolution.
The paper examines the application of these techniques from the era of the Napoleonic wars until nowadays using various case studies and demonstrates how modern cyber warfare can be used as a tool for the above policies in the current era of information capitalism.
Economic Implications of the Rise of Information Warfare, Cyber-War and Cyber-Security

Kyriaki Athanassouli
Department of Theoretical Sciences, Hellenic Military Academy,
GR-166 73 Vari, Greece
E-mail: k.athanassouli@gmail.com

Abstract Post-industrial societies are characterized by rapid technological changes, which have influenced the sector of Armed Forces. In the early 90’s, after the end of the Cold War, the Revolution in Military Affairs reinforces the technological applications in the Army by the introduction of “intelligent arms”, giving new dimensions in the art of war. Internet, being the main tool of the information society, has resulted from a series of military investigations. The appearance of internet is due to the USA’s authorities (Advanced Research Project Agency (ARPA)) willing to possess a communication system able to resist a nuclear war from the Soviet Union. This initiative played a vital role in creation of the Arpanet, the basis for the present form of internet.

The information society is characterized by the wide use of Internet by an increasing part of the population. Economic and military activities became increasingly reliant on Internet and networked technologies. Indicatively, in 2015 the number of internet users was around 3.07 million worldwide and they are expected to reach the number of 3.6 million in 2018, representing 48.2% of Earth’s population. Internet access is becoming a basic priority. Nevertheless, access in technology upsets the geopolitical balance. The introduction of technology in industry and the interdependence between networks of critical infrastructures has led to new cyber-dangers and cyber-threats. The information revolution implies the rise of cyber-attacks or cyber-war. For instance, in 2007, the Estonian Government was victim of large-scale cyber-attacks, resulting in the interruption of the state services functioning. A year later, the Georgian Government became the next victim of such cyber-attacks. Hackers blocked the take off of a military aircraft and caused problems in the accessibility of official media sites, ministries and public entities.
These facts highlighted the intention of disruption or destruction of enemy’s information and communication systems and the vulnerabilities arising from the interconnectivity of computer systems. The appearance of cyber-war is a culmination of the extended use of technology. Cyber-war consists a new type of war as is defined as actions directed towards targeting any aspect of an opponent’s cyber systems such as communications, logistics or intelligence. Cyber-attacks target on public or private sectors entities, while perpetrator remains legally unknown. The military dimension has expanded into non-military areas. Cyber-war can also include either the destabilization of the government’s financial systems and critical infrastructures, infiltrating a computer system for the purposes of espionage, or false information by using cyber-weapons and making offensive interventions across cyberspace. It can appear during both periods of peace and war. Questions arise whether cyber-war is analogous to traditional warfare and in which circumstances. Technologically advanced countries tend to dominate in the cyberspace. Furthermore, cyber-war is an asymmetrical warfare, not realized in a precise geographical area, and geopolitical instabilities can occur.

Nowadays, many states are developing defensive and offensive abilities aiming at the reinforcement and acceleration of securitization process. This has led to the cyber-security market. Cyber-security is defined as “an emerging field of protecting computer systems and data from interference through the Internet”. Cyber-security concerns are reflected at the efforts made by several countries in order to identify the level of securitization in the cyberspace. The Global Cyber-security Index (GCI) is an initiative to measure the commitment of countries to cyber-security. The GCI provides an overview of the countries’ level of cyber-security developments, including five areas: legal measures, technical measures, organizational measures, capacity building and international cooperation. This index gives a global cyber-security ranking of each country. Many countries share the same ranking which indicates that they have the same level of readiness. Moreover, the increase in demand for goods and services in the field of cyber-security has impact on arms-producing and military services companies. Taking into account the growing importance of cyber-security, arms industry and services operate in cyber-security market aiming at the coverage of such needs.
Typical are the cases of Airbus Defense & Space, BEA Systems, Lockheed Martin, Saab and Thales etc, which diversified into cyber-security in order to widen their production range and their customer base into the civilian sector and to develop technical competences for the military market. Finally, Cyber-security from an economic perspective, using tools of cost-benefit analysis can contribute to decision making in the context of risk management. It aims to determine the amount of investment in cyber-security depending on the expected cost. Furthermore, cyber-security as an economic problem uses tools of microeconomics, modeling the attack and defense behavior in order to analyze whether decisions made at individual levels are likely to result in the socially optimal amount of cyber-security. Modern approach of public economics highlights some situations in which private benefits and costs fail to account for all of the social benefits and costs. The market economy is characterized by individual behaviors which are not always socially optimal for ensuring social welfare and the required degree of cyber-security. Specifically, cases in which these situations can arise are network externalities, prisoner’s dilemma, information asymmetries and public goods aspects (non-rivalry and non-excludability) of private security investment. The potential market failure in information sharing is a result of the incentive to ‘free ride’. Thus, economic barriers to improving the securitization of cyberspace call out for government involvement and regulation. The government needs to better consider the economics of cyber-security in order to achieve the optimal level. For these reasons, it is necessary for cyber-security to become a strategic national asset. Current cyber-security measures have to be based on private and international measures (North Atlantic Treaty Organization-NATO, European Commission, European Defense Agency), taking into account international cooperation and regulation. □
Mathematical Modeling of a Bank Data Set: The Case of Greek Oligopoly

Miltiadis Chalikias¹, Panagiota Lalou² and Michalis Skordoulis³

¹, ², ³ Department of Business Administration, School of Business and Economics, Piraeus University of Applied Sciences (T.E.I. of Piraeus), 250 Thivon & Petrou Ralli, GR- 12244, Egaleo, Greece

E-mails: mchalikias@hotmail.com¹, glalou@hotmail.com², mskordoulis@gmail.com³

Keywords: operations research • Lanchester's combat model • system of differential equations • oligopoly

Abstract The purpose of this research is to investigate the possibility of applying an extension mathematical theory of war models based on Lanchester Theory in a set of banking data.

The mathematical models which will be applied in this research will be based on 4x4 differential equations systems.

Previous research has already proved that mathematical theories of war models can be successfully applied to business data as there are many similarities between the battle fields and the business competition.

The examined models applications results will lead to the analysis of the competition between the four banks with the biggest market share in Greece.
Cyber Warfare
MalOrbot: An Android Malware to Bridge the Mixes in Tor

Evangelos Mitakidis¹ and Dimitrios Taketzis²
Hellenic Army General Staff

¹ Andreopoulou 33, Thessaloniki, Greece
² Lechovou 37, Thessaloniki, Greece

E-mails: ¹ Mitakidis@gmail.com and ² d.g.taketzis@army.gr

Abstract

Internet was not created and designed with anonymity in mind. For this reason, there has been significant development for methods destined to provide anonymity to its users. The aim of this presentation is to provide a moderately simple to implement but very effective deanonymization scheme for Tor traffic. This is done by controlling both the traffic leaving the Onion Proxy (OP) and the traffic entering the Exit Node. Specifically, from a user’s point of view, this has been implemented in the popular Android platform as a malware, having the dual aim to manipulate user traffic before it enters the Tor overlay and instruct OP to choose an Exit Node that is controlled by the attacker. When the user’s traffic is received by the rogue Exit Node it is filtered, and the sender’s IP details become visible. Finally, apart from deobfuscating normal HTTP traffic send via the Tor browser, the proposed scheme is able to manipulate HTTPS requests as well.

In our presentation we will initially state the motivation of our work which was to investigate Tor attack vectors including attacks on user-side software (onion proxy) and to estimate the anonymity level of Tor users.

The idea was to develop a malware destined to popular Android platform with stealthiness in its operation. With proper configuration of the (controlled by the attacker) Exit Node, so that it logs both the ID and the traffic of the victim we are able to instantly deanonymize Tor users. Our method also protects the Exit Node because it takes measures to protect itself from being blocked (flagged).

Firstly we will briefly present how Tor network operates focusing on its scheme and deanonymizing techniques.
On the next few slides we will briefly explain the security features of Android operating system and the corresponding apps for using the Tor network, namely Orweb and Orbot.

The next section of our presentation is dedicated to our implementation. We will explain the techniques we used and the possible attacks referred to Open Systems Interconnection (OSI) model. In the figure below is depicted the architecture of our scheme.

It consists of the user side malware (Malorbot) which is installed on the smart device and a specially configured Exit Node. We will technically explain the features of the components and present screenshots of both smart device during installation of the malware and Exit Node server during deanonymization.

Finally we will refer to the assumptions that must exist for our scheme to fulfil its deanonymization purpose. □
Military Operations Continuity Using Information Technology Virtualization

Theodoros G. Kostis¹, Nikitas V. Nikitakos² and Panos Mavropoulos³ (LtGen, ret)

¹Department of Mathematics and Engineering Sciences, Hellenic Military Academy, GR-16673, Vari Attikis, Greece
²School of Business Administration Department of Shipping, Trade and Transport, University of the Aegean, 2a Korai Street, GR-82100 Chios, Greece
³Department of Theoretical Sciences, Hellenic Military Academy, GR-16673, Vari Attikis, Greece

E-mails: ¹ tkostis@iee.org , ² nnik@aegean.gr , ³ pmavropoulos@yahoo.gr

Keywords: cyber-warfare • virtualization • cyber-attack • system restore

Abstract The use of information technology is an integral part in military operations. Specifically the domain of information technology is used from planning a military operation to the operating system of a weapon system that will be used in this operation. As a consequence the security of the involved information is of paramount importance: without proper cyber-security countermeasures to cyber-threats, the battle worthiness of any military asset could be greatly compromised.

Nevertheless cyber-threats are sometimes successful in the deliverance of their destructive payload. Battleship engines may stop, electronic operations maps may be stolen or deleted, database systems may be altered.

In this paper we explain the use of virtualization in order to provide seamless operation continuity after such a successful cyber-attack.
The Hackademic Challenges Project: Teaching Future Cyber Warriors

Spyros Gasteratos¹, * Vasileios Vlachos², Marianna Dimou³ and Konstantinos Papapanagiotou⁴

¹, ², ⁴Open Web Application Security Project
², ³Technological Educational Institute of Thessaly, Computer Science and Engineering Department, GR-411 10, Larissa, Greece

*E-mail: ² vsvlachos@gmail.com

Abstract The rapid rise of cyber-attacks ([1]) combined with the introduction of network-enabled equipment to manage critical infrastructure increases the need of security aware personnel. In order to provide insights in the mentality and the techniques used by malicious agents, we developed Hackademic, a tool for teaching application security in practice. It is based on well established frameworks and development techniques and includes features that provide insight on the training process and student performance. Moreover, it offers both theoretical and realistic challenges. Theoretical challenges, developed by academics around the globe include courses and tutorials on basic cryptography, buffer overflows and old hashing algorithms. Realistic challenges involve tests ranging from structured query language injections and cross site scripting to return oriented programming chaining, binary reversing and other attacks used by security professionals on their day to day assignments. The Hackademic Challenges Project, enables students carry out these attacks in an isolated, secure environment backed up by either Docker containers or Vagrant boxes. It is already utilized by many educational institutions in Greece, Europe, North and Latin America and Asia Pacific.

According to[8], “the wide use of computers in military and defense installations has long necessitated the application of security rules and regulations. A basic principle underlying the security of computer systems has traditionally been that of isolation—simply removing the entire system to a physical environment in which penetrability is acceptably minimized. First, the security problem is not unique to any one type of computer system or configuration; it applies across the spectrum of computational
technology. Secondly, resource-sharing systems, where the problems of security are admittedly most acute at present, must be designed to protect each user from interference by another user or by the system itself, and must provide some sort of ‘privacy’ protection to users who wish to preserve the integrity of their data and their programs“. However, raising awareness and efficiently training personnel to be security conscious is a challenging task. Additionally, attackers continuously develop different tools and sophisticated techniques. Therefore it is of crucial importance to provide cyber-security training to all personnel.

In this paper we present the Hackademic Challenges Project an educational software security platform which can be used as a framework for software security training. The project consists of three loosely connected systems, the content management system, the challenges and the Hackademic sandbox. The content management system is an easily extendable PHP application tasked to handle the presentation of the teaching material and user management. The sandbox takes care of isolating the vulnerable applications from the rest of the server and monitors student performance, gathering data which can be used for evaluation purposes and analytics. The challenges are the vulnerable applications, hosts or networks the students are tasked on compromising.

Many institutions have developed educational systems in order to train their students for different types of attacks. For example, the Department of Computer Science at Texas A&M University offers a graduate course in Advanced Networks and Security. During this course, students are divided into either offensive or defensive teams aiming to either compromise machines or defend them by patching vulnerabilities and detecting any unauthorised access ([2]). In another example, the Department of Computer Science in the University of California, created a network of hosts configured with a number of different operating systems. The network was remotely accessed by the students who were able to utilise security tools to perform attacks in a safe environment ([3]).

The use of different types of security games is regarded as an effective educational approach. In [4], several university teams took part in a game that required setting up and protecting a network that was at the same time attacked by an opposing
team. A different approach, based on role playing was adopted in [5], the simulation of cyber-attacks was chosen. The participating teams had to assure the security of the network through cooperation and critical decision taking.

The use of various defensive tools and defensive techniques was employed in [6] were students had to come up with various hands on exercises that gave them useful experience and knowledge on password cracking, network reconnaissance techniques and security auditing. In addition to supervised security labs, there is a number of unsupervised applications. According to OWASP ([7]), most of these labs can be broadly characterized by three attributes. Whether they can be safely hosted on a server and accessed via the Internet (Online) or not (Offline) and whether the vulnerable applications are somehow separated from the rest of the server and thus pose little to no threat to the hosting system and do not interact with each-other (Sandboxed). Finally they can be characterized according to if they are Teaching Oriented thus providing reading material or not. Online labs usually don’t require the end user to download the application. Instead they are hosted on a server where end users can access it and try to exploit the application. Offline labs require the user to download either the application executable or a virtual machine image which contains the application. A comprehensive list of notable unsupervised labs can be found in [7].

The Hackademic Project is an open source application offering attack scenarios based on a number of scenarios. The project was introduced in 2011 as a Joomla plugin containing example vulnerabilities. It’s introduction was followed by widespread adoption in the academic sector. Since 2011 a rapid rise in new technologies and related attacks has been observed.

Drawing 1: The new interface of the Hackademic project
To reflect this, Hackademic has evolved to address better these developments. In the latest versions Hackademic includes more than 100 challenges ranging from introductory javascript cross site scripting attacks to advanced cryptanalysis. The interface is in English and the platform supports internationalization using the i18n. The project consists of three code bases. Challenges, Content Management System (CMS) and Sandbox engine all discussed bellow. A challenge is a vulnerable application, a vulnerable host or a network. Each challenge is accompanied by a scenario presenting students with the topic in an appealing way. It should target a limited amount of realistic topics that depict specific security threats. Furthermore each challenge has only one possible solution that follows the designated methodology. Time is also critical for the students as they should not overcome specific time limits. Each one presents a different level of difficulty and aims to test not only the acquired knowledge but also the ability to combine it with a short response time. Every exercise presents a clear and focused target, but also displays a congratulatory message when being solved. In this way, the trainee will know whether there are more steps to be made. Finally, the platform offers the option of fuzzy scoring allowing the trainer to define a number of penalties or bonuses based on various conditions including time limits, spamming, experimentations or bonus answers etc.

The CMS handles the management of users, classes and teaching material. It consists of a simple PHP application backed by MySQL storage accessed by any browser. It is the main contact point for students allowing them to find all the relevant information on a challenge including theory and study material needed to solve it as well as scenario and objectives. A trainer using the platform can split the students into classes, assign challenges and articles as well as manage bonuses or penalties for a number of occasions. The whole platform is widely extensible allowing the users to write and install plugins and custom themes.

The Sandbox engine uses virtualization and container solutions to host vulnerable applications or whole networked setups. After researching efficient implementations the Vagrant and Docker projects were chosen as a virtualization and container solution respectively. They are both very active open source tools and
industry leaders in the field. Moreover their support is exceptional and there are well maintained programming libraries around them.

The implementation consists of monitor and orchestration scripts as well as wrappers around Python’s vagrant and docker libraries. When a user clicks on ‘Try Challenge’ the CMS sends a 'launch challenge X' command to the orchestration script which accesses a dictionary mapping challenge_ids to container configurations. Then it launches the container and depending on the configuration, it provisions it using either Puppet or Ansible, depending on what is available on the hosting environment and what the challenge supports. From there, the container is responsible for monitoring the user’s activity and reporting successful or failed solving attempts. Every box or container exists on a configurable time limit and resource limit after which it is killed. For the future versions of Hackademic the CMS is being rewritten in Python using Django for faster development and better security. Also, the sandbox engine is getting a REST API which allows the two systems to run on different networks. Finally the frontend is also getting reworked using the latest in javascript technology. Finally many more challenges are under development and a complete course feature is being finalized.

References

[2]. P. Mateti: A Laboratory Course Based on Internet Security, Department of Computer Science and Engineering, Wright State University, Dayton, Ohio, 252-256
[3]. G. Vigna: Teaching Hands on Network Security, Department of Computer Science, University of California, Santa Barbara, 8-24
[5]. L. Catuogno and A. De Santis: An Internet Role-Game for the Laboratory of Network Security Course, in TiCSE ’08 – 13th Annual Conference on Innovation and
Technology in Computer Science Education. ACM, 2008, pp. 240-244.

[6]. M. O Leary: A Laboratory Based Capstone Course in Computer Security for Undergraduates, in SIGCSE ’06 – 37th SIGCSE Technical Symposium on Computer Science Education. 2006, pp. 2-6

[7]. OWASP: Vulnerable Web Applications Directory

Artificial Intelligence in Cyber-Defense

Cpt (HE-A) Georgios Karapilafis
Department of Mathematics and Engineering Sciences, Hellenic Military Academy,
Vari, GR- 16673, Greece
E-mails: g.c.karapilafis@army.gr and evelpil@gmail.com

Abstract In a rapid changing and demanding environment, decision makers need to have at their disposal the most valuable information at the right time, in order to follow the best course of action. Cyber operations, defensive or not need just that. Accurate and time-sensitive information that give competitively advantages against the virtual adversaries and threats. Each problem that a company or an organization face, either it is military or civilian, is a matter of information. The amount, the complexity and the variety of information make the decision process a demanding task. The wish for effective decision making process is the factor that makes the need of information such important. In cyber era, all this information cannot be processed by human brain without considerable automation and this automation, cannot be offered from conventional algorithms anymore. A good decision may be either the best decision that could be taken or just a satisfactory one. But in our case, what matters is precision. For example we want to recognize immediately when a network is under attack, and the way this happens. Thus, it is not a matter of satisfaction, but precision and timely available and accurate information of the underlying situation when it comes to confidentiality, integrity and availability of data.

The role of intelligent software in cyber operations increased rapidly over the years, because handling large amount of information very fast in order to describe and analyze events in cyber space and make the required decisions remains a difficult task, and without automation, which is offered from such intelligent applications, fighting against persistent adversaries would be a lost battle. Events of the past years have shown a rapidly increasing intelligence of malware and cyber-weapons. Adversaries use new techniques that constantly try to obfuscate the origin of data by using for example advanced cryptography and tunneling methods that are hard to analyze. The new
defense methods like dynamic setup of secured perimeters, comprehensive situation awareness, and highly automated reaction on attacks in networks will require wide usage of artificial intelligence methods and knowledge-based tools. “American cyber defense has fallen far behind the technological capabilities of our adversaries [such]...that the number of cyber attacks is now so large and their sophistication so great that many organizations are having trouble determining which new threats and vulnerabilities pose the greatest risk”([1]). The above, is a clear indication for the need of new approaches in cyber defense.

In this direction, this presentation gives a brief survey of potential artificial intelligence applications in the cyber defense era. The reason for the selective emphasis on artificial intelligence is that it has the potential to enable cyber security systems to detect, evaluate and counter threats by assessing anomalies within packets, byte-patterns, data traffic and user behaviors across the entire network ([2-9]). So, as sophistications of cyber attacks and malware grow rapidly, the need for development of intelligent cyber defense methods becomes unavoidable. Areas such as decision support, situation awareness and knowledge management are some that could benefit the most from the development of expert systems and artificial intelligence in general. New developments in knowledge understanding, representation and handling as well in machine learning will greatly enhance the cyber defense capability of systems that will use them. Such intelligent approaches, in combination with conventional security practices —encrypted data, multi-level authentication requirements and general best practices, could provide the necessary tools needed to keep up in a challenging cyber environment.

References


Military Information Support
Operations in the
International Contemporary
Geostrategic Environment
Omnipotent, Omniscient and Omnipresent Commanders: The Impact of a Cultural Paradigm Derived from a Secularized Christianity on the Philosophy of Network Centric Warfare

Konstantinos Grivas
Department of Mathematics and Engineering Sciences, Hellenic Military Academy,
GR- 16673 Vari, Greece
E-mail: gki821@otenet.gr

Abstract This article examines how a religious cultural paradigm deriving from the Humanism of the West affects the modern art and science of War. In the framework of a religified Humanism, in which Man ‘stole’ God’s competences and properties, the worldview of man-god was created. This worldview penetrated the development of military strategy being transformed in the worldview of commander-god, which threatens today to reach extreme ends, assisted by technological evolution allowing the development of robust C4ISR networks interconnected with PGMs of various configurations.

The article then examines the influence of western intellectualism, which is a basic element of Western Christianity, over the development of modern warfare theories and the risks that can arise for the western armies of the future from this impact. As an antidote to this influence, the article suggests a new perception on military strategy which emphasizes adaptability and flexibility and is based on a cultural paradigm from the Orthodox Christian Faith.
Modeling Supply Disruptions for Logistics Network of R Defense Suppliers to a Battlefield

Anastasia Paris  and Vasilios Vrisagotis

1Department of Theoretical Sciences, Hellenic Military Academy, Vari, GR-16673, Greece
E-mail: Kinshasa@otenet.gr

2Department of Business Administration, University of Aegean, Chios Island, Greece
E-mail: brisxri@otenet.gr

Key words: two-echelon defence supply network • performance measures • Markov analysis • merge system

Abstract Supplying military units is a crucial task for any military administration: the quantity of supplies and their replenishment rate directly affects how effective a team is during a military operation. Replenishing the supplies efficiently is thus a very important factor of success in the field. The unpredictable circumstances, such as weather changes, attacks or breakdowns in transport encountered by the suppliers may affect the performance of the troop. Therefore, planning the replenishment service must take into account the variability of delivery time, both in expected and unexpected situations.

In this paper, we aim to evaluate how time variability in replenishing the supplies can affect military units during an operation and to discover how to best organize the replenishment service of operating units. We suppose R unreliable suppliers and one military unit. The unreliable suppliers have sufficient supplies to cover any demand of the supported unit, which communicate with it when the fire power is critically limited. The duration of replenishment cycles varies, following an exponential distribution with a mean value $\mu_1$. Unpredictable events result in a delay of replenishment, which then follows an exponential distribution with a mean value $\mu_2$. Thus, the variability of replenishment time can be expressed as a Coxian distribution with two phases ($1^{st}$ phase: normal replenishment, $2^{st}$ phase: replenishment facing difficulties).
We based our modeling on Markov stochastic processes, which allowed us to evaluate different scenarios, each with certain parameters in place, such as:

1) Number of unreliable suppliers \( s_i \), where \( i = 1, 2, 3, ..., R \)
2) quantity of supplies \( q_i \) each unit demands
3) mean time value of normal replenishment \( \mu_{i,1} \)
4) mean time value of delayed replenishment \( \mu_{i,2} \)
5) probability of unpredictable events occurring \( d_i \)
6) rate of consumption \( \lambda_i \) for the team.
Case Studies Analysis from Attacks in the Supply Chain and Losses with the Use of GPS or GSM Jammers by the Attackers

Panayiotis P. Laimos¹, Michalis Chronopoulos², Chrysanthi Laimou³ and Nikoleta Atanasova⁴

¹ European Projects Director, G4S Telematix S.A. & Electronic Security Systems Director, G4S Secure Solutions Bulgaria

² Head of Technology, G4S Telematix S.A.

³ Project Manager, G4S Telematix S.A.

⁴ Security Manager, G4S Secure Solutions Bulgaria

E-mails: ¹ panagiotis.laimos@gr.g4s.com, ² michalis.chronopoulos@gr.g4s.com, ³ chrysanthi.laimou@gr.g4s.com and ⁴ nikoleta.atanasaova@bg.g4s.com

Abstract As the value of the transported goods continuously increases, the Organized Crime has developed modern methods to take advantage of any security whole in our supply chain – especially in long distance international transportation. Thieves also seem to make an increasing use of jamming devices, trying to disturb or block GSM signals emitted or GPS signals received by the trucks. Suspected jamming was indeed mentioned in many more incident reports recorded lately than it had been the case in the previous years. In this paper selected attacks that jamming was involved and an analysis of the modus operandi of the attackers are presented.

In many incidents, attackers are making use of GPS jamming technology to help them steal trucks and containers. Although it is illegal to use in many countries, GPS jammers are widely available to buy on the internet, and are finding a ready market among criminals keen to disable GPS tracking devices. Depending on the jamming target (GSM jamming – GPS jamming or GPS spoofing), there are serious uncertainties surrounding jamming, both as regards the efficiency of the devices available on the market and its real impact on cargo crime.
The analysis of the incidents shows that the modus operandi of the attackers varies from simple GSM jamming to disrupt the communications of the truck driver and telematics system with their base to a combination of violent armed attack to use of very sophisticated GPS jamming and spoofing activities. Furthermore, some intelligence is currently added on some High Value Theft Targeted transporting goods trucks, so they can react in case GSM communication is detected.

Finally this paper investigates the encryption methods applied to the Supply Chain tracking related communications and presents the current status as well as some technology trends.
Automated Procedure for Utilization – Operation of Hellenic Army Empty Warehouses

Theodore Zikos (Colonel)¹, Demetrios Zaires (Lieutenant)² and Nikolaos V. Karadimas ³

Department of Mathematics and Engineering Sciences, Hellenic Military Academy, GR- 16673 Vari, Greece

E-mails: ¹ hellas.ted@gmail.com , ² d.k.zaires@army.gr and ³ nkaradimas@gmail.com

Abstract  The aim of this study is to analyze all factors concerning the utilization and exploitation of empty warehouses belonging to the Hellenic Army pointing out that in periods of economic crisis the Hellenic Army has the capability of self-sustainability at every level of administration. This approach begins with the citation of the factors that lead to the necessity of the study, such as the adequacy of the warehouses, the reduction of human resources, the difficulty of maintaining the facilities by allocated credits and the capability of their evacuation. Formal methods like SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis and decision making procedures are used for the accurate determination of all alternative options which will lead to the best possible solution for the development and utilization of the aforementioned facilities. This proposal invests in the extroversion of the Hellenic Army by creating an automated process for the exploitation of the warehouses by the Hellenic army units and also by suggesting the best possible provision of information for their operational use. □
Cyber Security
A Computational Intelligence System for Identification
Cyber-Attacks on the Smart Energy Grids

Konstantinos Demertzis (2Lt)¹ and Lazaros Iliadis²

¹, ² Democritus University of Thrace
Department of Forestry & Management of the Environment & Natural Resources
193 Pandazidou st., GR-68200 N Orestiada, Greece

E-mails: kdemertz@fmenr.duth.gr¹ and liliadis@fmenr.duth.gr ²

Keywords: smart energy grids • cyber-attacks • advanced persistent threats • supervisory control and data acquisition – SCADA • big data • network forensics tool

Abstract  According to the latest projections of the International Energy Agency, smart grid technologies have become essential to handling the radical changes expected in international energy portfolios through 2030. A smart grid is an energy transmission and distribution network enhanced through digital control, monitoring and telecommunications capabilities. It provides a real-time, two-way flow of energy and information to all stakeholders in the electricity chain, from the generation plant to the commercial, industrial and residential end user.

New digital equipment and devices can be strategically deployed to complement existing equipment. Using a combination of centralized IT and distributed intelligence within critical system control nodes ranging from thermal and renewable plant controls to grid and distribution utility servers to cities, commercial and industrial infrastructures, and homes a smart grid can bring unprecedented efficiency and stability to the energy system.

Information and communication infrastructures will play an important role in connecting and optimizing the available grid layers. Grid operation depends on control systems called Supervisory Control and Data Acquisition (SCADA) that monitor and control the physical infrastructure. At the heart of these SCADA systems are specialized computers known as Programmable Logic Controllers (PLCs).
There are destructive cyber-attacks against SCADA systems as Advanced Persistent Threats (APT), were able to take over the PLCs controlling the centrifuges, reprogramming them in order to speed up the centrifuges, leading to the destruction of many and yet displaying a normal operating speed in order to trick the centrifuge operators and finally can not only shut things down but can alter their function and permanently damage industrial equipment.

This paper proposes a computational intelligence System for Identification Cyber-Attacks on the Smart Energy Grids (SICASEG). It is a big data network forensics tool which can capture, record and analyze the smart energy grid network events to find the source of an attack to both prevent future attacks and perhaps for prosecution.
Nature Inspired Algorithms for Intrusion Detection Systems

Demetrius P. Iracleous 1,2 and Aikaterini Papadimitraki 2

1 Department of Mathematics and Engineering Sciences, Hellenic Military Academy, Vari, GR-16673, Greece
   e-mail: iracleous@gmail.com

2 IST College in collaboration with London South Bank University, Pireos 72, 18346 Moschato, Greece
   e-mail: aikaterini.papadimitraki@msc15.ist.edu.gr

Abstract  Intrusion Detection Systems (IDS) is a crucial component of most network security infrastructure. They have been extensible studied and modeled with exact mathematical approaches, rule-based systems and artificial intelligence arrangements.

The problem consists of the real time interpretation of network calls to identify if the request is a normal call from a legitimate user or from a suspicious packet to a malicious appeal. There is a wide range of classifications with vague discrimination criteria. The system uses explicit rules, configuration directions from the administrators, previous knowledge and naïve to smart algorithms based on current research.

Biologically Inspired Algorithms (BIAs) have been used in the context of these systems. They include Artificial Neural Networks (ANNs), Fuzzy Logic Algorithms (FLAs) and Genetic Algorithms (Gas) are the usual triad in the design of a BIA enabled feedback system. The collection of BIAs has been enriched with Swarm Intelligence, Artificial Immune Systems, Ant Colony Optimization, etc. Nature inspired algorithms extend the range of algorithms to physical and chemical systems.

In this work, the IDS are presented, along with their most important categories; the most important cases are reviewed and summarized. Most recent studies are studied and evaluated. A combined approach is proposed and discussed.

Implementation issues are studied and are specialized to sensor network systems with multimedia content like open systems monitoring highways and remote installations.
References


[10]. C. M. Ou: *Host-based intrusion detection systems adapted from agent-based artificial immune systems*, Neurocomputing, 88(2012), 78-86


Real-time Computational Intelligence Protection Framework against Advanced Persistent Threats

Konstantinos Demertzis (2Lt)\textsuperscript{1} and Lazaros Iliadis\textsuperscript{2}

\textsuperscript{1, 2} Democritus University of Thrace' 
Department of Forestry & Management of the Environment & Natural Resources 
193 Pandazidou st., GR-68200 N Orestiada, Greece 
E-mails: kdemertz@fmenr.duth.gr \textsuperscript{1} and liliadis@fmenr.duth.gr \textsuperscript{2}

**Keywords:** advanced persistent threats • tor anonymity network • tor traffic analysis • semi-supervised learning • online sequential learning • extreme learning machine

**Abstract** An Advanced Persistent Threat (APT) is a set of stealthy and continuous computer hacking processes in which an unauthorized person gains access to a network and stays there undetected for a long period of time.

The "advanced" process signifies sophisticated techniques using zero-days malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack. APT attacks target organizations in sectors with high-value information, such as military networks, national defense, manufacturing and the financial industry.

Traditional digital security mechanisms face such vulnerabilities in a conventional manner, they create often false alarms and they fail to forecast them. As APT activities are stealthy because they use Tor anonymity network, the command and control network traffic associated with APT can be undetected at the network layer level. Deep log analyses and log correlation from various sources cannot be useful in detecting APT activities and network agents can be useless to collect logs (TCP and UDP) directly from assets into a syslog server.

This paper proposes an innovative fast and accurate Real-time Computational Intelligence Protection Framework against Advanced Persistent Threats (CIPFaAPT). It is about an automate forensic analysis system that use Semi-Supervised Online Sequential Extreme Learning Machines. It can process millions of data points in real-
time, establishing, or learning a “normal” baseline, comparing data points to past behavior and identifying anomalous differences in values over time, differences in rates over time, and population outliers. Using computational intelligence and machine learning algorithms, user transactions, server processes, internet traffic, IPS alerts and traffic flow can all be analyzed for unusual activities.

The CIPFaAPT is a next generation security platform that uses sophisticated analytics to monitor, track and classify risk across critical network infrastructures in order to identify APT.
Analyzing Epidemiological Characteristics of Biological Viruses and Correlation with Computer Viruses

Antonios Manaras¹, Vasileios Vlachos², Alexandros Papanikolaou³ and Christos Ilioudis ⁴

¹,²Technological Educational Institute of Thessaly, Computer Science and Engineering Department, GR-411 10, Larissa, Greece

³,⁴Department of Information Technology, Alexander Technological Educational Institute of Thessaloniki, GR-57 400 Sindos, Thessaloniki, Greece

E-mails: ¹antonis@antonismanaras.me, ²vsvlachos@teilar.gr, ³alxpapanikolaou@gmail.com and ⁴iliou@it.teithe.gr

Abstract The scientific field of epidemiology is sufficiently defined and studies the distribution and evolution of various diseases or characteristics and factors that shape or influence human population. In contrast with clinical medicine, which focuses on the patient’s treatment, epidemiology deals with the assessment of various disease types that occur within groups with similar characteristics. In [1] epidemiology is defined as “the study of the occurrence and distribution of health-related events, states, and processes in specified populations, including the study of the determinants influencing such processes, and the application of this knowledge to control relevant health problems”. Epidemiologists study and analyze patterns and deviations in health and disease conditions of specified populations. They follow statistical analysis methods and develop epidemiological models in order to measure indicators, such as morbidity and mortality of a specified population, to discover causative factors that lead to a disease and study the conditions and causes of epidemics and pandemics. The goal is to be able to control and predict disease outbreaks.

This study attempts to address the similarities in the epidemiology, between the biological viruses and computer viruses. It presents the characteristics of both biological and computer viruses, as well as the similar procedures that these viruses follow, in terms of propagation and behavioral models. What is more, it also exhibits the key factors that contribute to their propagation.
This study proposes the potential of using the expertise, procedures and methodologies of the study of the biological viruses’ epidemiology, in the study and analysis of computer viruses, taking advantage of the similar characteristics.

The connection of the virulence and epidemiological characteristics in biological and computer viruses has concerned the researchers since the early occurrences of malicious programs and their first description as “computer viruses” in [2-3]. A study suggests the concept of “computer immunology”, by examining the analogies between biological viruses and computer viruses with respect to the human immunology system [4-5]. Previous studies have shown the ways in which computer viruses choose their targets and what preconditions must be met in order to infect them successfully ([6]), while the authors in [7] consider the three essential ingredients of worms’ effectiveness to be vulnerability prevalence, age of the vulnerability at the time of the exploitation and exploitation difficulty, followed by their attempt to interpret biological epidemiology in a computer network context.

By studying and analyzing computer and biological viruses, it becomes evident that there are similarities in both cases regarding the virus dissemination and spread, thus leading to epidemiological and sometimes epidemic or pandemic phenomena, if the appropriate conditions are satisfied.

The spread and behavior of biological viruses can be observed and studied with the use of appropriate mathematical epidemiological models, which define all those factors and qualities that characterize the population and the conditions under which the virus propagates. It is those characteristics that will define the easiness or difficulty which the virus will spread with and whether it will eventually succeed in massively spreading itself within the population, thus causing an epidemic or even a pandemic outbreak. An equally important factor is whether a virus is harmful, especially if it is fatal or curable. Therefore, the aforementioned features depend on biological and natural phenomena, which are the areas of interest to biologists and medical scientists.

In the case of computer viruses, the human factor intervenes, which determines the behavior of the virus. The author of the malicious software is the one who will determine the way in which the virus operates at large.
However, this is not always the case, as there have been documented cases in which the malware's behavior has gone out of control and has led to a massive spread. Nevertheless, the computer virus spreading mechanism follows a similar pattern with that of biological virus, showing similarities in the features which define the scale of ease or difficulty in their spreading, accordingly.

In order to observe the similarities between biological viruses and computer viruses, matching certain key characteristics is necessary, as shown in Table 1, for example spatial determination where the spreading occurs or the spread agent.

<table>
<thead>
<tr>
<th>Biological Viruses</th>
<th>Computer viruses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infected patient</td>
<td>Infected computer</td>
</tr>
<tr>
<td>Geographical area</td>
<td>Computer network</td>
</tr>
<tr>
<td>Direct contact with infected person</td>
<td>External storage drive inserts the system</td>
</tr>
<tr>
<td>Death</td>
<td>Computer system destruction</td>
</tr>
<tr>
<td>Cure</td>
<td>Disinfection – System clean up</td>
</tr>
<tr>
<td>Vaccine</td>
<td>Patch</td>
</tr>
<tr>
<td>Viral mutation</td>
<td>Viral polymorphism</td>
</tr>
</tbody>
</table>

Table 1 Analogy between biological viruses and computer viruses

Comparing a human cell with a computer system we can map the cell’s genetic material, DNA and RNA, with the program’s codes (source code and executable code). In the same principal that DNA is a blueprint for RNA, source code is the blueprint for the executable code.

Computer systems play a major role in our everyday lives and their impact is expected to increase in the future. At the same time, malicious programs are becoming more sophisticated and more harmful, thus causing a need for taking appropriate measures to protect computer systems against modern threats.

By inspecting the characteristics of epidemiology models of computer viruses carefully, we identified the similarities among the biological viruses and computer viruses. We presented the characteristics of biological and computer viruses, as well as the similar procedures that these viruses follow, in terms of propagation and behavioral models. What is more, we have also emphasized on the key factors that contribute to their propagation.
Some of the relationships between the computer and biological viruses’ main characteristics (dissemination and spread), were identified, thus leading to epidemiological sometimes epidemic or pandemic phenomena. Our research proposes the potential of exploiting the knowledge, expertise, procedures and methodologies used in biological viruses’ epidemiology for the study and analysis of computer viruses, in an attempt to treat common characteristics in a similar manner.

There is room for improvement and work to be done in order to keep the computer viruses’ spreading below epidemic thresholds and this can be achieved by applying well-documented epidemiological models. Future work could focus on investigating ways for applying immunity to computer systems by simulating biological immunity systems, in which an individual becomes permanently immune after recovery. Furthermore, it should also be examined whether such mechanisms can mimic the nervous system, thus reinforcing threat detection and communication of threat-related information in computer systems with centralized reporting and response mechanisms.

References

[1]. M. Porta, editor: A Dictionary of Epidemiology, Oxford University Press, USA, 2014
Information Based Psychology
in Social Structures
The Uncertainty Surrounding Information’s Economic Value

Maria Sakalaki

Department of Psychology, Panteion University of Social and Political Sciences, 136, Syngrou Avenue, 176 71 GR-176 71 Athens, Greece

Email: sakalaki@panteion.gr

Keywords: information • material goods • immaterial goods • valuation • paradoxes of information • heuristics • uncertainty • lay economic thinking

Abstract This experimental study focuses on the uncertainty surrounding information's value. It compares the valuation of economic information to the valuation of material goods when subjects possess perfect information so that uncertainty about the outcome of the transaction is eliminated. It also aims to study the participants’ justifications of their valuations, in order to examine the underlying cognitive processes.

Given that economists consider information a paradoxical good of uncertain value, the main hypotheses of this paper were that: (a) even if subjects deal with perfect information they will underestimate its value compared to the value of material goods; (b) underestimation of the value of information will be greater in conditions of high involvement, that is when expected payoff and therefore investment and risk are high; and (c) expert information will be valued more highly than non-expert information, since it should be regarded as more reliable. In the main study, two groups of students in the same university were asked to value and justify their valuation of material goods, under conditions of certain low (€1000) and high (€100,000) payoffs, respectively. Two other groups were asked to value and to justify their valuation of non-expert information under the same conditions of profit. Finally, two more groups of students were asked to value and justify their valuation of expert information, again under conditions of low or high expected profit. The findings of the study show that under all conditions the value of information is underestimated both absolutely and relatively in comparison to material goods, especially under conditions of high involvement. The participants’ justifications of their own valuations are heuristics which take into
consideration the uncertain character of informational goods of high involvement. The participants’ justifications of their own valuations are heuristics which take into consideration the uncertain character of informational goods.

**Bibliography**


Information and Emotions: Imposed Hope, Fear, Desire and their Impacts to Human Behavior

Vassia Ignatiou Karamanoli

Laboratory of Psychology, Department of Theoretical Sciences,
Hellenic Military Academy, GR-166 73 Vari, Greece
Email: vaskar3@yahoo.com

Key Words: information • hope • fear • desire • influence • behavior

Abstract Information is composed of complex structures and human react to information in complex ways indicating that information is valuable because it can affect decision making and behavior in several fields such as economy, workplace, politics, warfare. Information, from its creation and production to its dissemination and interpretation, and in all of its many formats, is an essential and ubiquitous element of everyday life; it can provoke high expectations and motivation to behavior. Individuals are not always rational; emotions often mediate thoughts and behavior.

The aim of the present study is to investigate how information with imposed emotions can influence human behavior. Two experimental studies were designed for that purpose. Study one was addressed to groups while study two was addressed to individuals, and one to individuals, in order to investigate whether information with socially imposed emotions has different power rather than information with individually imposed emotions. Participants of the two experiments were divided into ten groups, five for each condition: social or individual, they had five scenarios one for each sub condition:

a) hope,
b) fear,
c) desire,
d) hope, fear, desire altogether

and finally there was a control group, for each experiment. Results illustrated the field and gave us some indications of how information with imposed emotions can influence human behavior and provided Hope Fear and Desire Model (HoFeDeModel). Implications for further research are made.

Hellenic Military Academy
Organizational Social Structure and Motivation as Predictors of Employees’ Information Sharing Attitudes

Konstantinos Papachristopoulos

Laboratory of Psychology, Department of Theoretical Sciences, Hellenic Military Academy, GR-166 73 Vari, Greece
Email: papachristopouloskostas@gmail.com

Keywords: information sharing • employee motivation • self determination • organizational social structure

Abstract Information sharing is critical to an organization’s competitiveness and requires a free flow of information among members that is undistorted and up-to-date. Knowledge management and information sharing facilitates the creation and use of knowledge for increased innovation and could have a profound influence on the doctrinal shift anticipated by the recent revolutions in Military Affairs.

However, extensive information sharing within organizations still appears to be the exception rather than the rule since it is a personal choice that cannot be forced and is associated with employees’ motivation as well as formal and informal social network structures. Information-sharing research has mostly concentrated on controlled motivation—namely, reciprocity, improving one’s reputation, doing the right thing, and positive feelings. Nevertheless, autonomous motivation has proven superior to controlled motivation with regard to the employee’s tendency to take advantage of the knowledge-sharing opportunities inherent in their networks and this result would be beneficial to be utilized in a military context where extrinsic and introjected motivational techniques dominated are prevalent.

This study uses Self-Determination Theory, SDT and Social Network Approach, (SNA) in order to describe principles and change interventions to increase connectivity and manage information sharing.
The aim of this survey is to present a model of knowledge-sharing motivation based on a combination of self-determination theory and Social Network Approach, along with a review of research supporting the model and suggestions for future research and methodologies to study knowledge sharing behavior.

The study examines a model that depicts the impudence of personal (i.e. motivation) and environmental (i.e. formal and informal social network structures) factors on employees’ information sharing attitudes and provides a proposed model for knowledge sharing supporting environment adapted to military contexts.
Information’s Value and Influence during Period of Uncertainty Using Leaflets and Social Network: The Example of Refugees in Greece

Vassia Ignatiou Karamanoli ¹ and Nikos Bardis ²

¹Laboratory of Psychology, Department of Theoretical Sciences, Hellenic Military Academy, GR-166 73 Vari, Greece

²Informatics Laboratory, Department of Mathematics and Engineering Sciences, Hellenic Military Academy, GR-166 73 Vari, Greece

Emails: vaskar3@yahoo.com ¹ and bardis@ieee.org ², bardis@itr.gr ²

Key Words: information • refugees leaflet • intelligence application

Abstract Information resolves uncertainty. The uncertainty of an event or situation is measured by its probability of occurrence and is inversely proportional to that. The more uncertain an event or situation, the more information is required to resolve uncertainty of that event or situation. Information’s way of presentation increases or diminishes the possibilities to be believed. Study one of this research aims to investigate how information works in period of uncertainty when is communicated socially with leaflets.

The example of refugees in Greece is examined, focusing on its structure, its context and its impact to refugees’ thought, emotion and behavior. Social network can facilitate communication more individually and can influence human thought, emotion and behavior also. Study two makes data mining from and big data bases are performed. Analysing information with intelligence applications and tools are presented. Implications for future research are made. □
Mathematical Foundations of Cyber–Defense Methods
On the Mathematical Definition of Cyberspace

Nicholas J. Daras

Department of Mathematics and Engineering Sciences, Hellenic Military Academy,
GR- 16673 Vari, Greece

E-mails: ndaras@sse.gr and njdaras@gmail.com

Abstract According to a commonly accepted formality given by the Oxford English Dictionary, 2009 Edition, "cyberspace is the notional environment in which communication over computer networks occurs (www.oxforddictionaries.com/us/definition/american_english/cyberspace ; see also http://en.wikipedia.org/wiki/Cyberspace )." During this period, the uses of the internet, networking, and digital communication were all growing dramatically and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging.

However these two concepts clearly suffer in terms of their rigorous definitions. Actually, there are many other formalities of the term in question. The most recent draft formality is the following: "cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources (www.academia.edu/7096442/How_would_you_define_Cyberspace )." The problem occurs particularly complex or even entangled, since “today, the word "cyberspace” is used in many contexts, but it is not always clear what exactly that term describes and what it means. Thus, different organizations have adopted different definitions of what cyberspace means. Some of them -- like the EU -- do not have an official definition at all, but that does not prevent it from discussing the term (http://blogs.cisco.com/security/cyberspace-what-is-it )”.

Without questioning the validity of all the well known formalities for the concept of cyberspace, we can make the following observations based on the information presented in the table above:
• Virtually all formalities agree that cyberspace includes tangible elements. This would imply that cyberspace cannot exist without tangible elements.
• Virtually all formalities agree that cyberspace must include information. Information can either be stored data, signaling between processes and/or devices or as a content that is being transmitted.
• Cyberspace includes tangibles but, at the same time, it is also virtual.
• Only a few definitions consider activities and interactions (within cyberspace) part of cyberspace.
• Probably contrary to popular beliefs, networks and Internet are not necessarily part nor are required for cyberspace but they are still ‘desired.’ Nevertheless, even implicitly, it is intuitively clear that the cyberspace has a network structure.
• Interconnectedness seems to have an equal weight as the Internet itself.

All these formalities are abstract and introduce the interested reader to the spirit of the text, but, on the other hand, they may not give a univocal, literal and rigorous description of the concept. On the contrary, the availability of more than 27 various such formalities can be confusing. Furthermore, there is no relevant mathematical background guarantying coherent development and systemic safety, unlike other scientific fields which have been built on solid mathematical foundations. Moreover, in all these formulations, there is nowhere any provision for the description of the perpetual change of cyberspace. Indeed, it is clear that, each time moment, appear new nodes that connect to the cyberspace in different points of the Earth (even of the Space), while at the same time moment, other nodes cease to be connected, so the points displaying their presence in cyberspace disappear completely. On the other hand, there are nodes that are connected but do not have an active connection with the cyberspace.

Inevitably, the lack of a rigorous definition has the consequence that they have developed and are continually being developed varying techniques, without any mathematical foundation which can support the best and efficient solutions on the issues of a beneficial settlement and utilization of these techniques. So, it is not longer possible to organize a solid defense (or planned attack) in the cyberspace, if previously there has not been a closed and rigorous mathematical definition of cyberspace. Nor is
it possible to guarantee effective protection into the cyberspace, if previously there has not been a strict definition of the concept of cyber-attack, as well as the different types of these attacks.

The aim of this paper is to give a rigorous mathematical definition of cyberspace, which will include all the basic specifications of the above mentioned different formalities of the cyberspace. In short, we will define and discuss categories of embeddings of multi-layered graphs (on the three-dimensional space or the Riemann sphere) and we will give a definition for the cyber-map that sends any closed interval within such a category. A cyberspace is defined to be the image of a cyber-map.

More specifically, in Section 1, we shall determine strong incentives of formulation such definitions by introducing and investigating the mathematical model that corresponds completely to the given above abstract definition of what is understood by saying “cyberspace”. As to the substance in this section, we consider the (infinite) set $\mathcal{M}nf_e$ of all pairs $(V, E)$ of $e$-node manifestations $V$ and interconnected $e$-arrow manifestations $E$ of instantaneous virtual e-archetype germs (with N-layers) over a given geographical region $U_1 \times \ldots \times U_N$. A good thinking for introducing utilitarian algebraic structure in the set $\mathcal{M}nf_e$ is to see this set as the class of objects of a large category. In Section 2, we will introduce the $e$-graph category $\mathcal{E}_C$, whose objects $X \in \text{ob}(\mathcal{E}_C)$ are simply the pairs $X = (V, E) \in \mathcal{M}nf_e$. Further, for later use, in the same Section, we will also introduce four other $e$-categories: The $e$-set category $e_{Set}$ whose objects are the subsets of $\mathcal{E}_C$, the $e$-homomorphism category whose objects are sets of homomorphisms between subsets of $e_{Set}$, the $e$-group category whose objects are the groups of $\mathcal{E}_C$ and the $e$-topological category $e_{Top}$ whose objects are topological subcategories of $\mathcal{E}_C$. The Section will conclude with a study of the functors between these e-categories. In the next Section 1.3 we shall give some examples of $e$-universality in a categorical construction. Specifically, we will define the e-product and the e-coproduct between any two objects lying in an e-category of the above type. Section 1.4 will be devoted to the study of attachment of suitable vector weights to all the objects and morphisms of an e-category $\mathcal{W}_e = \{\mathcal{E}_C, e_{Set}, e_{Gpr}, e_{Top}\}$. Towards this end, we will consider two types of vector weights that can be attached to any object and/or morphism of such a e-category: the maximum weight and the square weight.

Hellenic Military Academy
Any such weight will be a point in the positive quadrant of the plane. In Section I.5, any 
\( e \)-category \( W_e \in \mathcal{W}_e = \{ \mathcal{E}_c, e_{\text{Set}}, e_{\text{Hom}}, e_{\text{Gpr}}, e_{\text{Top}} \} \) will be viewed as an \( e \)-graph \((\mathcal{V}, \mathcal{E})\) with vector weights: the \( e \)-nodes in \( \mathcal{V} \) are the \( e \)-objects \( X \in ob(W_e) \), while the \( e \)-arrows or \( e \)-arcs in \( \mathcal{E} \) are the \( e \)-morphisms \( h \in hom(W_e) \). For such an \( e \)-graph \( \mathcal{G}_{\mathcal{E}_c} \) corresponding to the \( e \)-graph category \( \mathcal{E}_c \), the vector weight of the \( e \)-node associated to the \( e \)-manifestation \( X = (V_X, E_X) \in \mathcal{V} \equiv ob(\mathcal{E}_c) \) is equal to a weight of \( X \). Similarly, for the \( e \)-graph \( \mathcal{G}_{W_e} \) corresponding to an \( e \)-category \( W_e = \{ e_{\text{Set}}, e_{\text{Hom}}, e_{\text{Gpr}}, e_{\text{Top}} \} \), the vector weight of the \( e \)-node associated to the \( e \)-manifestation \( X = \mathcal{M} \in W_e \) is equal to a weight of \( \mathcal{M} \). The fact that each \( e \)-category \( W_e \) would be a metric space provides topological structure on every \( W_e \) permitting profound and rigorous analytic investigation of local cyber-mappings. Bearing all this in mind, in Section I.6, we will introduce a suitable metrizable topology on \( e \)-graphs and \( e \)-categories. The introduction of this appropriate metric \( d_{W_e} \) in the set \( ob(W_e) \) of objects of a \( e \)-category \( W_e \in \mathcal{W}_e \) will allow the consideration of open, closed, compact, dense and connected areas in \( ob(W_e) \). And, as it is expected, the most significant benefits coming from the consideration of this appropriate topology in \( ob(W_e) \) can be derived from the definitions of cyber-evolution and cyber-domain given in Section I.7. However, before formulating the definition of these concepts in Section I.7, we will have given some supportive and informative notions. Specifically, in the beginning of Section I.7, we will see that a mapping \( cy: [0,1] \rightarrow (ob(W_e), d_{W_e}) \) is a local \( e \)-dynamics and the overall image \( cy(\mathbb{I}) \) is a \( e \)-arrangement. Obviously, each image \( cy(t) \) has the form of an instantaneous local \( e \)-node manifestation with the interrelated \( e \)-arc manifestation. An \( e \)-arrangement together with all of its instant \( e \)-morphisms is an \( e \)-regularization. If the given geographical region \( U_1 \times \ldots \times U_N \) is selected so as to cover the whole domain of interest, then the above mapping is called a global \( e \)-dynamics. In such a case, the image \( cy(\mathbb{I}) \) is a global \( e \)-arrangement; the associated \( e \)-regularization is a \( e \)-settlement. The elements of the completion \( |ob(W_e)| \) \( ob(W_e) \) in \( \overline{U_1 \times \ldots \times U_N} \subseteq \mathbb{CP}^N \) are the cyber-elements while the topological space \( (|ob(W_e)|, d_{W_e}) \) is a cyber-domain. With this notation, a continuous local \( e \)-dynamics \( cy: [0,1] \rightarrow (|ob(W_e)|, d_{W_e}) \) is said to be a cyber-evolutionary path or simply cyber-evolution of the cyber-domain \( (|ob(W_e)|, d_{W_e}) \). Sometimes, we may use
the compellation cyber-track of \((\text{lob}(W_e), d_{W_e})\). In such a case, the \(e\)—arrangement \(cy(\mathbb{I})\) is a cyber-arrangement. A cyber-arrangement together with all of its instant homomorphisms is called a cyberspace. If, in particular the given geographical region \(U_1 \times \ldots \times U_N\) is selected so as to cover the whole domain of interest, then the corresponding cyber-arrangement \(cy(\mathbb{I})\) is said to be a cyber-configuration; the associated cyberspace is also called cyberspace. In view of the above concepts, Section I.8 will seek to limit any further study to a brief study of local \(e\) —dynamics. To do so, we will investigate if an \(e\) —regularization which is projection \(e\) —system may be susceptible of a projective \(e\) —limit. According to the main result of this Section, it is important to know if a sub-\(e\) — regularization is projective \(e\) —system. Subsequently, in Section I.9 we will define and discuss the concept of the length in a cyber-domain. The intrinsic length metric is a metric possible to define on every cyber-domain \((\text{lob}(W_e), d_{W_e})\). For this metric the distance between two cyber-elements is the length of the ‘shortest cyber-track’ between these cyber-elements. The term shortest cyber-track will be defined later and is in fact crucial for the understanding of cyber-geodesics. Although every shortest cyber track on a cyber-length space \((\text{lob}(W_e), q_e)\) is a cyber-geodesic, the reverse argument is not valid. In fact, some cyber-geodesics may fail to be shortest cyber-tracks on large scales. All the same, since each cyber-domain \((\text{lob}(W_e), d_{W_e})\) is a compact, complete metric space, and since for any pair of cyber-elements in \(|\text{lob}(W_e)|\) there is a cyber-evolutionary path of finite length joining them, one obtains the following converse result: any pair of two cyber-elements in each cyber-domain \((\text{lob}(W_e), d_{W_e})\) has a shortest cyber track joining them. Section I.9 will conclude with a discussion about the speed (cyber-speed) of a cyber-evolution. Finally, in the last Section, we will examine pointwise and uniform convergence of cyber-evolutions. □

References


[10]. A. Georgakopoulos: Graph topologies induced by edge lengths, Technische Universität Graz, June 16, 2010
Mathematical Modeling of Cyber-Defense Methods

Argyrios Alexopoulos

MSc Electrical Engineering, MSc Applied Math, CCNA, ITIL, PRINCE 2
Darwin 4, SHAPE,
MONS 7010, Belgium

E-mails: a.d.alexopoulos@army.gr and argyrios.alexopoulos@yahoo.com

Abstract This scientific communication includes two parts. In the first part, we will summarize the mathematical definition of cyberspace ([3]) and apply this definition to different and specific types of germs of cyber attacks, such as the germs of reconnaissance attacks, the germs of access attacks, the germs of denial of service intrusion, the germs of cyber crimes, the germs of cyber espionages, the germs of cyber terrorism, the germs of cyber war, the germs of active attacks, the germs of malicious attacks, the germs of non malicious attacks, the germs of attacks in MANET and the germs of attack on WSN ([1]).

In the second part, we will review a mathematical description of cyber-attacks and proactive defense ([2]) and investigate the 3 main types of proactive defense against the above mentioned germs of cyber attacks ([2]).

References

[1]. A. Alexopoulos: Mathematical study of different special types of germs of cyber attacks, in preparation
[2]. A. Alexopoulos: Proactive defense against different special types of germs of cyber attacks. A mathematical study, in preparation
[4]. N. J. Daras: Subjectivity in the evaluation of the estimates and the vulnerabilities of a cyber-node and its implication on the interactions between different cyber-nodes, submitted
Abstract Our aim is to document a holistic modeling background and set up a corresponding mathematical theory in order to provide a rigorous description of cyber-attacks and cyber-security. The presentation comes as a follow-up of a forthcoming article [6] in which it has been given a mathematical definition of cyberspace.

We will first introduce general assumptions and some basic notations that we will use later in the article. The starting point is to determine the concepts of valuations and vulnerabilities of the parts of a node constituent. Based on these two concepts, one may be led to consider the fundamental concept of node supervision and subsequently to give the definition of cyber-effects and from this the definition of cyber-interaction. As we shall see a germ of cyber-attack can be viewed as a family of cyber-interactions having coherence properties and depending strongly on subjective aims, information and/or estimates on the valuations and the vulnerabilities of parts of the involved nodes. In general the germs of cyber-attacks can be distinguished in three types: the germs of correlated cyber-attacks, the germs of absolute cyber-attacks and the germs of partial cyber-attacks. The above described approach provides the immediate possibility of a rigorous determination of the concepts of proactive cyber defense and proactive cyber protection. A systematic effort to introduce and give a practical definition, description and technical organization of the concept of preventive cyber-defense has become by Richard Colbaugh and Kristin Glass in [1-5]. Here, we discuss the theoretical foundation of this concept.

Having established rigorous determination of cyber-attacks and proactive cyber-defense, we are able to proceed to two main applications. The first application has to do with a description of cyber navigations and protection from unplanned attacks. In this context, we will give a mathematical definition of cyber navigation and, after giving
the meaning of infected nodes, will determine what is meant by dangerous cyber navigation and protection of cyber nodes from unplanned attacks. Our second application relates to a rigorous description of the main types of cyber attacks and corresponding protections. So, after a brief classification of cyber attacks, we will separately consider the cases of the definitions of passive and active cyber attacks, as well as the relevant protections of nodes from such attacks.

The presentation will conclude with a brief report which will provide some basic and reasonable questions which, in our opinion, should be explored and studied.

References


Communications Systems and Networks
Coupled Semiconductor Lasers Operating in a Chaotic Regime: Experiments on Synchrony, Clustering and Encryption Techniques

Demetrios Syvridis and Apostolos Argyris
Optical Communication and Photonic Technology Laboratory, Department Informatics & Telecommunications, National & Kapodistrian University of Athens, Panepistimiopolis GR-15784, Ilisia, Athens-Greece

E-mails: dsvrdivdi@di.uoa.gr and argiris@di.uoa.gr

Abstract In this paper a fiber – optic network of 16 mutually coupled semiconductor lasers is studied experimentally. High level of consistent global or cluster synchrony via chaotic signals is demonstrated among all devices of the same origin and under appropriate operation. Devices that are not identical fail to synchronize at any condition, when coupled to the network. Under multiplexed operation, groups of lasers that emit at spectral distances as low as 50pm are shown to preserve intra-cluster synchronization when transmitted in the same fiber-optic channel, despite their large bandwidth of emitted signals. A one-time pad cryptographic scheme has been successfully implemented and demonstrated using a pair of highly synchronized lasers.

Deterministic chaos characterizes the behavior of a broad range of non-linear dynamical systems in physical, biological, socio- economic, etc. sciences. Mutual coupling of these systems leads to synchronization, a general concept which includes a broad range of dynamics and instabilities such as low frequency oscillations, ultra-broadband chaotic signals, bubbling effects, etc. Semiconductor lasers have been extensively studied as nonlinear photonic devices in mutually coupled systems. Synchronised semiconductor lasers have been used in the first demonstration of a secure optical communication link operating under real conditions in installed fiber-optic network ([1]). Further development of the basic concept included the implementation of an optoelectronic integrated circuit to be used as chaotic transceiver ([2]).
In this paper we present the synchronization properties of a network of 16 semiconductor lasers coupled through long fiber-optic paths. We show that each unit's properties and operating parameters establish it as a member of the overall synchronized network, a member of intra-network synchronized clusters or just an outlier unit. Strict frequency matching (<200MHz) of the optical emitted signals allow synchrony at configurations with even a few identical SLs. In contrast, when non-identical SLs couple with the network they fail to synchronize at any operational condition. Moreover, when shifting identical SLs from a common emission wavelength (global operation) to multiplexed wavelengths (cluster operation), it is shown that the network can maintain intra-cluster synchrony. The latter property is validated for ultra-dense wavelength multiplexing of the coupled units, with chaotic carrier spectral distance of only 50pm. All the above properties of the coupled-SL networks could be exploited towards multi-channel hardware authentication protocols.

The experimental setup is shown in fig. 1a where 16 Distributed Feedback (DFB) semiconductor lasers are coupled through a variable reflecting node. Amplification stages based on Erbium Doped Fiber Amplifiers have been used to control the injection signal strength. A set of diagnostic instruments have been used such as optical spectrum analysis with resolution up to 10 pm and RF spectral analysis using Photodiode arrays - 40 GSample real time oscilloscopes and RF spectrum analysers. In fig. 1.b typical time traces of a pair of synchronized lasers / members of the network is presented with a cross correlation of 0.916.

![Fig.1](Image)

**Fig. 1** (a) The experimental setup consisting of 16 identical semiconductor DFB lasers mutually couple through a tunable central reflector. (b) Typical time traces of two (members of the network) synchronized lasers (depicted in red and black).
The high synchronization quality achievable through the mutually coupled lasers has been used for the implementation of the “one-time pad” cryptographic scheme.

In fig. 2a the One-Time Pad concept is schematically presented. Synchronized broadband chaotic analog signals are the seed for ultrafast TRBS generation (True Random Bit Sequence). Each user's transceiver locally generates a TRBS synchronized with the TRBSs of other users. User #1 encodes data with the appropriate FEC convolutional code and applies a XOR operation with the locally generated TRBS. User's #2 locally generated TRBS through an XOR operation provide the initially encoded data.

![Fig2 (a) The concept of the realized One-Time Pad cryptographic scheme. (b) The experimental realization using mutually coupled lasers controlled by a central laser hub.](image)

The obtained experimental results showed that under very strict conditions, a cross correlation of 0.995 can be achieved, which leads, with the proper Forward Error Correction Codes, to the generation of identical synchronized true random number streams for both users, needed for the encryption of the data. Error free operation has been achieved using FEC (3/8) codes.

References


Bivariate Copulas-Based Models for Communications Networks

Ioannis S. Triantafyllou,

Department of Computer Science & Medical Bioinformatics,
University of Thessaly,
2-4 Papasiopoulou str., GR-35131 Lamia, Greece

E-mail: itriantafyllou@uth.gr

Keywords: Farlie-Gumbel-Morgenstern distribution; Bivariate copulas; Ali-Mikhail-Haq distribution; communications networks

Abstract  The construction and properties of copulas have been studied rather extensively during the last two decades. Briefly speaking, copulas are functions that join or “couple” multivariate distributions to their one-dimensional marginal distribution functions. Equivalently, copulas are multivariate distributions whose marginals are uniform on the interval (0,1). In the present article, we restrict our attention to bivariate copulas. More precisely, we discuss the Farlie-Gumbel-Morgenstern (F-G-M) copula (and its generalization) and the Ali-Mikhail-Haq bivariate distribution. For each model, several properties are established, while several numerical results and remarks are also concluded. For illustration purposes, applications in the field of communications networks are presented in detail.
Security in a Remote Controlled UAV

Nikolaos Doukas
Department of Mathematics and Engineering Sciences, Hellenic Military Academy,
GR- 16673 Vari, Greece
E-mails: ndoukas@sse.gr and nikolaos@doukas.net.gr

Abstract   An unmanned autonomous vehicle has been developed that is based on an Arduino platform and is controlled remotely via a wireless connection. The UAV transmits surveillance images to a remote command station, also via wireless connection. This presentation focuses on the security problems that arise during this operation and the solutions that have been developed. These are concerned principally with the secrecy and integrity of the command session, the privacy and authenticity of the surveillance imaging and the possible repercussions of the capture of the UAV.
Encryption Methods
RNA/DNA Encryption Method-
Another Encryption Algorithm

Dionysios P. Kalogeras, Hellenic Army.
(Phd (cand) in Telecommunications, MSc In Networking and Data
Communications, Dipl in Radioelectrology, BSc in Physics
Kanigos st 14 Pireas, GR-18534, Greece
E-mail: dionkaloger@yahoo.gr

Keywords: DNA encryption • encryption algorithm

Abstract  The DNA cryptography is a new and very promising direction in
cryptography research. DNA can be used in cryptography for storing and transmitting
the information, as well as for computation. Although in its primitive stage, DNA
cryptography is shown to be very effective. Currently, several DNA computing
algorithms are proposed for quite some cryptography, cryptanalysis and steganography
problems, and they are very powerful in these areas. However, the use of the DNA as a
means of cryptography has high tech lab requirements and computational limitations,
as well as the labor intensive extrapolation means so far. These make the efficient use
of DNA cryptography difficult in the security world now. Therefore, more theoretical
analysis should be performed before its real applications.

The fundamental idea behind this encryption method is the exploitation of DNA
cryptographic strength and easy application. In this project, real DNA is used to
perform the cryptography process; the theoretical analysis and experiments show this
method to be efficient in computation, storage and transmission; and it is very
powerful against certain attacks. Thus, this method can be of many uses in
cryptography such as an enhancement insecurity and speed to the other cryptography
methods. There are also extensions and variations to this method, which have
enhanced security, effectiveness and applicability.

A Matlab program is used on order to decide for the algorithm strength and web
services are proposed for application into this method. □
Improved Algorithms for Hard Knapsack Problems and its Variants

Konstantinos Draziotis ¹ and Anastassia Papadopoulou ²

¹Department of Informatics, Aristotle University of Thessaloniki, P.O. Box 114, GR- 54124, Thessaloniki, Greece
E-mail: drazioti@csd.auth.gr

²Department of Mathematics, Aristotle University of Thessaloniki, GR- 54124, Thessaloniki, Greece and Kapetan Varda 7, GR-58100, Giannitsa, Greece
E-mail: anastapc@math.auth.gr

Abstract  In the present study we applied improved algorithms in order to solve hard knapsack problems that are used in cryptography. The study goals are:

1) Presenting two variants of Shnorr-Shevchenko method and collect some experimental results
2) Adopt the same method to find small solutions in linear Diophantine equations
3) Provide a branch and bound algorithm for the compact knapsack problem
4) Provide an Id-scheme based on compact knapsack problem.

There are cryptosystems that are based in knapsacks and they have some significant advantages. That is one of the reasons which motivated us to undertake this study.

At first, we describe the knapsack problem which is fairly simple: Given $n$ positive integers $(a_i)_{i=1}^n$ and an integer $s$, find a binary vector $X = (x_i)_{i=1}^n$ such that

$$\sum_{i=1}^n x_i a_i = s.$$ 

Subsequently, we cite the work that has been done until now. The algorithm of Shroeppe-Shamir (SS), the improvement of Becker, Coron and Joux and finally Howgrave-Graham Joux algorithm are provided and compared. Then, we particularly describe Schnorr-Shevchenko method, which is the algorithm we use to apply our variants.
For these variants, we use BKZ-reduction, as SS method. Our experiments denote that the dimension and the density of a knapsack are dependent parameters of the requiring time. For this reason, in the first variant we manage to decrease these parameters with brute force on the initial bits of the solution and it can be easily parallelized in order to become faster. The second variant includes a simple way to reduce efficiently the density. From the results we can claim that these variants in average are better than the original method.

Compact knapsack is the next subject of this study. The only difference from the original problem is that the vector $X$ is not binary here, since it belongs in $\{0,1,\ldots,2^{\delta n}\}$, for some $\delta > 0$. It is solved in polynomial time (for instance using Euclidean algorithm), therefore we are interested in solutions that satisfy some constraints, which is a NP-complete problem. This problem has some important applications in discrete optimization, in designing integrated circuits and is also applied in knapsack cryptography systems. In order to find a solution in a specific range, we used a branch and bound algorithm. For dimension $n = 10$ and constraints $2^{R-1} \leq X \leq 2^{R} - 1$ with $R = 8$, this method is efficient enough with success over 80%. Although, if we choose the parameters $a_i$ such that half of them have $R$ bits and the other half $R/2$ bits, with $n, R \geq 0$, then we can be certain that our system which uses compact knapsack is safe.

Finally, the last section of this study provides a three-move Id-scheme based on compact knapsacks. We manage to prove its security under passive attacks and the reasons we use it are the following: this scheme is lightweight in the sense that does not use exponentiation and it also potentially quantum resistant. Lastly, the parameters of the scheme are checked. We do not fully address the choice of the parameters in the paper. But, we provide some minimal conditions for them, in order our system to be secure. □
A Voting Scheme Based on Elliptic Curves

Dimitrios Poulakis
Department of Mathematics, Aristotle University of Thessaloniki,
GR- 54124 Thessaloniki, Greece
E-mail: poulakis@math.auth.gr

Abstract In this paper we propose a new efficient voting scheme that is suitable for large scale elections over Internet which is based on Elliptic Curve Cryptography. For the accuracy of the voting outcome we have considered a voting center which has to collaborate with an authentication center.

The voters submit their votes to the authentication center which signs them using the BLS signature scheme and next the voters send their ballots encrypted with the Menezes-Vastone encryption scheme via a public proxy server to the voting center. It is shown that the proposed algorithm satisfies the more important requirements of any e-voting scheme. □
Communications Security
Implementation of the AES-GCM
Authenticated Encryption Algorithm
Targeting Xilinx’s Defense-Grade Virtex-5Q FPGAs

Georgios Theodorou¹, Nektarios Kranitis², Antonius Tsigkanos³ and Antonius Paschalis⁴

Digital Systems & Computer Architecture Laboratory (DSCAL),
Department of Informatics & Telecommunications,
National and Kapodistrian University of Athens,
Panepistimiopolis, Ilissia, GR- 15784 Athens, Greece

E-mails: ¹ gthe@di.uoa.gr , ² nkran@di.uoa.gr , ³ antts@di.uoa.gr and ⁴ paschalis@di.uoa.gr

Keywords: Galois/counter mode (GCM) • advanced encryption standard (AES) • very large scale integration (VLSI) • high throughput • field programmable gate array (FPGA)

Abstract  Confidentiality is defined as the assurance that information is not disclosed to unauthorized entities or processes. In other words, those who are not authorized are prevented from obtaining information from the protected data. For communications systems, there are essentially two mechanisms to accomplish confidentiality:
   1) transmission through a physically protected medium (e.g., wire encased in alarmed conduit) and
   2) cryptography.

However, it has been shown in the security community that the use of encryption by itself without authentication is dangerous. Authentication algorithms can be applied to the transmitted data on communications systems to uniquely identify the person or an entity that is authorized to access the transmitted information. Therefore, the use of encryption is highly encouraged in communication systems to provide the simultaneous security services of confidentiality, integrity, and authenticity.

Authenticated encryption, also known as Authenticated Encryption with Associated Data (AEAD), can be performed by combining an encryption algorithm with
an authentication algorithm (e.g., MAC) as long as both are known to be secure against attack. It has been shown that encrypting data and then applying a MAC to the ciphertext implies security against an adaptive chosen ciphertext attack.

The AES algorithm was published by NIST as FIPS-197 standard in 2001 ([1]). For this algorithm, several modes of operation were proposed such as ECB, CBC, CFB, OFB and CTR ([2]). These modes provide data encryption but no data authentication. Therefore, NIST proposed among others GCM as a mode of operation supporting authenticated encryption ([3]). AES-GCM can provide very high-speed authenticated encryption in hardware, as well as, in software. It can also be parallelized and pipelined and does not require padding with extraneous, throwaway bits. These featured of AES-GCM are very advantageous in the communications systems.

Defense-grade SRAM Virtex-5Q FPGAs ([4]), delivers state-of-the-art cryptographic technology to address the next-generation secure systems and constitutes an ideal solution for developing of modern defense electronics systems, particularly for secure communications, electronic warfare, aircraft and transport vehicles. Moreover, the Virtex-5Q defense-grade FPGA provides ruggedized packaging protection against ‘tin-whiskering’ and caustic solvent cleaning systems to ensure high-reliability. Finally, Virtex-5Q devices are pin-to-pin compatible with the Xilinx commercial parts, enabling seamless migration from prototyping to production. Therefore, a Virtex-5 commercial FPGA chip is an excellent platform for prototyping an FPGA implementation of authenticated encryption algorithms, since the prototyped design can be directly migrated to a defense-grade FPGA production platform.

In this work, we present a high data-rate performance AES-GCM FPGA implementation that can be incorporated in next-generation secure communication systems to perform authenticated encryption. The target platform FPGA is a Xilinx’s Virtex-5 XC5VFX130T FPGA that is pin-to-pin compatible with the Defense-grade Xilinx’s Virtex-5Q XQ5VFX130T FPGA. In this AES-GCM FPGA implementation, we have chosen to restrict the AES cipher key to 256 bits and the authentication initialization vector (IV) length to its default value that is exactly 96 bits for efficiency following the suggestion in [5].
The top level architecture of the AES-GCM implementation consists of four main units:

1) The Advanced Encryption Standard encoder core (AES) that performs that implements the AES-256 algorithm. The length of the input block is 128 bits and the length of the cipher key is 256 bits. The AES encoder core consists of four functional units. Each unit implements one of the four transformation phases (SubBytes, ShiftRows, MixColumns, AddRoundKey) that should be performed in each AES round. Additionally, a functional unit, termed as key scheduler, calculates and generates a new AES internal key every round that is needed for the final transformation (AddRoundKey) in the AES encoder. In AES-256 algorithm the number of rounds is 14. We have chosen to implement an iterative non-pipelined AES architecture to minimize the hardware utilization. In each clock cycle, one round of the AES algorithm valuated, the result is fed back to the circuit through a multiplexer, and stored in a register. Therefore, four AES transformations (SubBytes, ShiftRows, MixColumns and AddRoundKey) are applied on a single clock cycle and 14 clock cycles are needed to encrypt a data block of 128 bits.

2) The GHASH unit that implements a 128-bit parallel GF ($2^{128}$) multiplier and a XOR operation. The temporal result is fed back and exclusive-ored with the next input to generate the next operand for the GF multiplier. A GF multiplier can be implemented in either parallel, digit-serial or bit-serial architecture. This implementation we use a pure combinational parallel GF multiplier. Although the parallel GF multiplier can be pipelined to achieve a higher clock rate, the achieved clock frequency of the parallel multiplier in the Virtex-5Q FPGA eliminates the need for a pipelined GF multiplier implementation.

3) The incremener unit that generates successive counter values that are needed by the GCM algorithm to feed the data input of the AES encryption core. This unit treats the rightmost 32 bits of its 128 bit input as nonnegative integer with the least significant bit on the right, and increments this 32 bit value modulo $2^{32}$.

4) The master controller that orchestrates the three AES GCM units (AES, GHASH and Incremener). The controller is responsible to control the multiplexers that select the inputs for the AES unit and the GHASH unit based on data flow and the units status signals.
The AES-GCM FPGA implementation is verified through extensive RTL simulation using Questa Advanced Simulator and code coverage measurements with all the test cases for a key size of 256 bit that are provided in [6]. The AES-GCM FPGA implementation (AES Key = 256 bits, IV vector = 96 bits, full parallel GHASH multiplier) requires 16% of slices and 2% of BRAMs targeting the Xilinx Virtex-5 XC5VFX130T SRAM FPGA allowing its flexible integration on any FPGA-based communication system along with any other IP core. The maximum achievable clock frequency is 143MHz. The measured total (static and dynamic) power consumption at 143MHz is 4.54 W. The critical performance-per-watt metric is 3.72 mW/Mbps. The AES-GCM FPGA implementation needs 15 cycles to process 128-bits of plaintext. Therefore, the achieved data-rate (throughput) performance is constant for larger inputs and is equal to 1.22 Gbps. Further, frequency optimization can be achieved by pipelining the Galois field multiplier in the GHASH function if needed.

References

Photonic Physical Unclonable Functions as a Secure Key Generator for Cryptographic Applications

Charis Mesaritakis 1*, Alexandros Kapsalis 2, Marialena Akriotou 3 and Demetrius Syvridis 4

1,2,3,4 National & Kapodistrian University of Athens,
Department Informatics & Telecommunications,
Optical Communication and Photonic Technology Laboratory,
Panepistimiopolis, Ilisia GR-15784, Athens-Greece

*Email: 1 cmesar@di.uoa.gr

Abstract In this paper a photonic physical unclonable function scheme, based on the complex coherent interference of optical beams subject to multipath propagation is demonstrated. The proposed scheme allows the generation of fully unclonable true random bit strings that are suitable for a variety of cryptographic applications ranging from symmetric cryptography to authentication applications for counterfeiting. The experimental data are evaluated in terms of robustness, unclonability and unpredictability employing typical information theory benchmark tests and the NIST statistical suit.

Physical unclonable functions (PUFs) are defined as one-way mathematical transformations that are based on highly complex and non-reproducible physical mechanisms instead of traditional hashing transformations ([1]). The directionality of the transformation is preserved through the complexity of the physical system that renders brute force attacks computationally infeasible, whereas the physical random process that is involved in the PUF realization, alleviates the possibility of cloning. Electronic based PUFs based on low manufacturing yield of various components have exhibited enhanced security features but they have been proven vulnerable to machine learning attacks, due to low physical complexity ([2]).

On the other hand, photonic implementations offer an alternative route by utilizing the coherent interaction of a laser beam with highly random disordered media. In these optically-based PUFs, radiation from a laser illuminates a transparent material (challenge) that has a set of unique random scatterers aiming to create unique image features (responses). These images are post-processed through hashing
functions [3], in order to produce unique binary code words. The physical complexity is induced mainly through Mie scattering that renders the system immune to statistical attacks.

In our case we utilize a transparent optical medium that allows multi-path propagation of the incoming radiation as an optical scrambler. The medium is illuminated through a tunable single mode laser, whereas the coherent interaction at the output of the system allow the generation of a unique speckle patterns, which depends on both the laser parameters (wavelength etc) and the micro structure of the optical medium (fig.1a).

Fig.1 (a) The experimental setup, WF corresponds to a wideband optical filter. (b) Intra hamming distance (blue) and inter hamming distance (red) for two hashing methods: binary (left) and Gabor (right)

The speckle patterns are recorded through a vidicon camera and are post-processed utilizing the methodology described in [3]. System characterization consists of two approaches. The first consists of acquiring images while keeping the medium and laser parameters constant so as to evaluate the robustness of the system in terms of inherent noise (Fig.1b-blue). The second consists in sweeping the laser’s wavelength from 1540 to 1550nm with a resolution of 100pm (fig.1c-red). In this case for each wavelength a discrete code word is generated, that can be employed as a true random cryptographic key. By comparing the bit flip probability (Hamming distance) in both cases (fig.1b, c) it can be concluded that different challenges (wavelength) induce significant higher number of bit-flips in the generated code word compared to the variations induced only through noise, thus the probability that a specific code word will not be recognized due to noise can be diminished through an error correction algorithm.
Furthermore, 1000 different PUFs have been manufactured and the speckle patterns for a specific input wavelength have been evaluated in terms of unclonability, meaning the probability that the generated code words exhibit bit variations that can be corrected through the error correction scheme. Through this approach our scheme provided a probability of cloning in the order of $10^{-6}$, whereas at the same time the probability for misclassifying a correct code word was zero. As shown in Fig.2 the proposed scheme offers radical performance enhancement compared to state of the art approaches ([4]).

![Fig.2](image)

(a) Probability of cloning vs robustness for the proposed scheme (black) and for state of the art PUF ([4]) (red). (b) Representation of the experimental bit-strings, black corresponds to 0 whereas white to logical 1. No pattern can be visually identified.

Finally, the generated code-words from multiple PUFs and for multiple wavelengths have been concatenated so as to feed typical NIST statistical suit (fig.2b). Through this approach the generated outputs were evaluated in terms of unpredictability. Results confirm that in this case the proposed system outperforms conventional PUF due to the fact that by employing a confidence level of 1% the utilized bit strings succeeded in all the NIST tests, while typical PUFs succeed only to a limited subset of the NIST test.

As a conclusion the demonstrated results confirm that the proposed scheme can offer robust and reproducible true random cryptographic keys, whereas the hardware generator cannot be cloned even by the device’s manufacturer. This generator alleviates the constraints of pseudo-random key generators and offer a fully secure hardware based solution compatible with various cryptographic protocols. □
References


Towards Abstract Logics for Secure Communication

Yiannis Kiouvrekis¹ and Petros Stefaneas²

¹,² National Technical University of Athens, Department of Mathematics, Herron Polytechniou 9, 15780 Zografou, Greece

Emails: ¹ yiannisq@central.ntua.gr and ² petros@math.ntua.gr

Abstract The formal verification of protocol correctness is a promising area of research with many real applications in security. Model checking is one the most popular such formal techniques with temporal semantics. In our paper we try to provide a classification of temporal logical systems using tools from abstract model theory and in particular from the theory of Institutions of Goguen and Burstall. We also prove a fundamental preservation result for abstract temporal satisfaction. The definition of Institutions provides a meta-mathematical framework for the development of an abstract model theory - free of any commitment to a specific logical system. Our work has three parts: In the first, we provide a survey of Institutions and other preliminaries. The second consists of an abstract definition of internal temporal logics and in the third we prove a fundamental theorem for temporal satisfaction.

References


[10]. Y. Kiouvrekis PhD Thesis (in progress), NTUA, Department of Mathematics, supervisor Pr. Petros Stefaneas


Cryptosystems and Computations
Secret Sharing Schemes through Structured Matrices

Stamatios-Aggelos N. Alexandropoulos, Gerasimos C. Meletiou, Demetris S. Triantafyllou and Michael N. Vrahatis

1st Computational Intelligence Laboratory, Department of Mathematics, University of Patras, GR-26110 Patras, Greece, E-mails: alekst@master.math.upatras.gr and vrahatis@math.upatras.gr

2nd A.T.E.I. of Epirus, P.O.110, GR-47100 Arta, Greece, E-mail: gmelet@teiep.gr

3rd Department of Mathematics and Engineering Sciences, Hellenic Military Academy, Vari, GR-16673, Greece, E-mail: dtriant@math.uoa.gr

Key words: Secret sharing schemes • structured matrix triangularization • LU factorization • matrix convolution

Abstract Secret sharing schemes through matrices of special structure are presented. The secret $S$, formulated by a matrix, is shared among $n$ participants in such a way that the $i^{th}$ participant receives from the dealer a part of the secret $S$ encrypted as a convolution of several matrices:

$$M_i = S \times \prod_j P_j, \forall j \in \{1,2,\ldots,i-1,i+1,\ldots,n\}, i = 1,2,\ldots,n$$

where $\prod$ indicates matrix convolution and $P_i$ represents the secret matrix of the $i^{th}$ participant which is also known to the dealer. The secret $S$ can be derived through numerical linear algebra techniques and more precisely through matrix factorization. The usage of well known and widely used methods such as the LU factorization with partial pivoting can guarantee the stability of the procedure. We show that a specific group of participants are in a position to construct a block banded matrix, by properly shearing their own information and by applying the LU factorization with partial pivoting, they can retrieve and extract the secret $S$. ☐
References

Cryptographic Boolean Functions with Maximum Algebraic Immunity

Konstantinos Limniotis ¹,² and Nicholas Kolokotronis ³

¹Hellenic Data Protection Authority, Kifissia 1-3, 11523, Athens, Greece
E-mail: klimniotis@dpa.gr

²Department of Informatics and Telecommunications,
National and Kapodistrian University of Athens, 15784, Athens, Greece
E-mail: klimn@di.uoa.gr

³Department of Computer Science and Technology, University of Peloponnese,
End of Karaiskaki Street, 22100 Tripolis, Greece
E-mail: nkolok@uop.gr

Abstract Algebraic attacks constitute a powerful cryptanalytic technique for symmetric ciphers receiving great attention over the last decade; their underlying idea rests with the construction of an appropriate overdefined system of nonlinear multivariate equations that allows one to determine the secret key [2]. Towards designing secure cryptosystems, the use of Boolean functions having properties like high algebraic degree, balancedness, and high nonlinearity, does not suffice to resist algebraic attacks. As a result, the cryptographic criterion of algebraic immunity (AI) was introduced to assess the strength of a Boolean function against such cryptanalytic attacks ([8]). Therefore, constructing Boolean functions with the maximum possible AI is of great importance.

In stream ciphers, algebraic attacks were further improved to the so–called fast algebraic attacks by exploiting linear relations amongst the keystream bits ([3]). Although they require knowledge of consecutive keystream bits (a constraint not previously imposed), they may be efficiently applied to cryptosystems that are resistant against conventional algebraic attacks. It is known that a maximum value of AI is a necessary but not sufficient condition for withstanding such attacks. Thus, the behavior of cryptographic Boolean function constructions against fast algebraic attacks need also be considered.

Amongst several constructions of functions with guaranteed maximum algebraic immunity, probably the most important one achieving also maximum degree and very
high nonlinearity is proposed by Carlet and Feng ([1]). More precisely, the so-called Carlet–Feng function with \( n \) number of variables described by 
\[
supp(f) = 1, \alpha, \ldots, \alpha^{2^n-1} \text{ for a primitive } \alpha \in \mathbb{F}_2^n,\]
where \( supp(f) \) denotes the set of elements of \( \mathbb{F}_2^n \) on which \( f \) evaluates to 1 (note that there is a vector space isomorphism between \( \mathbb{F}_2^n \) and the finite field \( \mathbb{F}_{2^n} \)). The most important feature of this class of functions is its optimum behavior in terms of fast algebraic attacks; this was first shown in [1] via experimental results for a small number of variables, and was subsequently rigorously proved in [6]. Suitable modifications of the Carlet–Feng construction have been presented in [4, 9, 10] utilizing the univariate representation of Boolean functions.

In general though, constructing functions with maximum AI without sacrificing other cryptographic criteria still remains an active research area.

In this talk, we focus on recent modifications of the Carlet–Feng function \( f \) so as to provide other functions with also maximum algebraic immunity. First we revisit a simple modification given in [4], which performs a simple swap between an element of \( supp(f) \) and one of \( supp(f + 1) \), such that the new function still achieves maximum algebraic immunity; this procedure – which holds for the case of odd number of variables - computest, for any given element of \( supp(f + 1) \), all the possible elements of \( supp(f) \) with the aforementioned property. Subsequently, based on this result, we prove general conditions that ensure maximum algebraic immunity when many entries of a function’s truth table are modified simultaneously, which in turn leads to an efficient approach to appropriately modify \( f \) in arbitrarily many positions (and not only two positions), so as to ensure that the algebraic immunity does not decrease ([5]).

This approach is based on the univariate representation of Boolean functions, which is used as more convenient for our analysis; by this way, we properly associate annihilators of Boolean functions with specific codewords of punctured Reed–Muller codes. It is shown that high nonlinearities, as well as good behavior against fast algebraic attacks, are also attainable. Finally, the problem of further generalization of these results so as to compute a larger number of functions with maximum algebraic immunity is also discussed. □
References

Cryptographic Techniques for Secure Linear Computations in the Supply Chain Management

Iris-Pandora Krommyda¹, Gerasimos C. Meletiou², Demetrius S. Triantafyllou³ and Michael N. Vrahatis⁴

¹Department of Business Administration of Food and Agricultural Enterprises, University of Western Greece, GR-30100 Agrinio, Greece, E-mail: ikrommyd@cc.uoi.gr

²A.T.E.I. of Epirus, P.O.110, GR-47100 Arta, Greece, E-mail: gmelet@teiep.gr

³Department of Mathematics and Engineering Sciences, Hellenic Military Academy, Vari, GR-16673, Greece E-mail: dtriant@math.uoa.gr

⁴Computational Intelligence Laboratory, Department of Mathematics, University of Patras, GR-26110 Patras, Greece, E-mail: vrahatismath.upatras.gr

Key words: supply chain management • optimization • linear programming • secure linear computations

Abstract Optimization problems encountered in a supply chain can often be modeled as linear programming problems, whose objective function and constraints combine data from several parties. However, this approach requires private data and sensitive information that the involved parties are often unwilling and hesitant to exchange and reveal to each other. In order to tackle these two conflicting goals, namely, the information sharing and protecting confidentiality, various cryptographic techniques for secure linear computations have been developed. These techniques ensure that the several parties can compute any function without any party to disclose its input to another. An overview of various efficient techniques for securely solving linear programming problems is presented.
References


Military Communications
The Use of Millimeter Wave Frequencies in Future Military Communications

Michael Gargalakos¹, Irene Karanasiou², Rodoula Makri³ and Nikolaos K. Uzunoglu⁴

¹,²,³ Department of Mathematics and Engineering Sciences, Hellenic Military Academy, GR-16673 Vari, Greece

³ Institute of Communications and Computer Systems (ICCS) 9, Iroon Polytechniou Str., GR-157 73 Zografou, Greece

and

⁴ School of Electrical and Computer Engineering, National Technical University of Athens, GR-15780 Athens, Greece

E-mails: ¹ michael@esd.ece.ntua.gr , ² ikaran@esd.ece.ntua.gr , ³ rodia@esd.ece.ntua.gr and ⁴ nuzu@cc.ece.ntua.gr

Abstract During the last decade frequencies exceeding 100 GHz is possible because of the sufficient development of relevant technologies for military communications. The available wide bands and also the relatively low (1-2 db/km) attenuation is making attractive to move 5th generation mobile communications into bands in the space 100-200 GHz. Although rain attenuation is a serious obstacle the use of multiple input multiple output (MIMO) signal processing technologies could be used to alleviate the rain attenuation problem. Available technologies of passive and active elements will be reviewed and will be presented for wide band communication networks. The atmospheric rain and other relevant conditions will also be presented. □
Simplified Jamming Methods for Direct Sequence Spread Spectrum (DS/SS) Systems

Dionysios P. Kalogerias, Hellenic Army.
Phd (cand) in Telecommunications, MSc In Networking and Data Communications, Dipl in Radioelectrology, BSc in Physics

Kanigos st 14 Pireas, GR-18534, Greece

E-mail: dionkaloger@yahoo.gr

Keywords: frequency hopping • direct sequence • jammers

Abstract Spread spectrum techniques were originated in answer to the needs of military communications. They are based on signaling schemes, which greatly expand the transmitted spectrum relative to the data rate. Spread spectrum communication systems have many applications, including interference rejection, multiple accessing, multi-path suppression, low probability of intercept transmission, and accurate ranging. Of all the potential applications, the ability of a spread spectrum system to withstand interference, both intentional and unintentional, is probably its greatest asset.

This paper discusses simplified Jamming Methods for DS/SS systems. Their performance is simulated into Matlab environment. □
Computational Simulation of Passive Synchronization Method for Frequency Hopping Systems

Konstantinos A. Psilopanagiotis

School of Telecommunications and Electronics for Signals’ Officers, Athens, GR-12461, Greece

E-mail: kopsili3@hotmail.com

Abstract In the 2012 conference a passive synchronization method for frequency hopping (FHOP) systems was presented. That method, which was invented by Dr. Prodromos E. Atlamazoglou in cooperation with Prof. N.K. Uzunoglou, was based on a mathematical process of linear algebra, and a respective pseudo-code, describing an eventual algorithm, for the implementation of the method.

The rationale for the development and the importance of that method is founded on the following aspects:

a. **Frequency Hopping**, as a modulation technique, is the only effective counter measure, which protects radio communication, from both interception and jamming.

b. The circuit of a **Linear Feedback Shift Register (LFSR)** is the basis for the generation of a pseudorandom frequency sequence that is comprised by the switching frequencies, which are used in a succession, during the communication between the transmitter and the receiver. That is the main reason, why the method is based on these circuits, which present large periodicities.

c. The achievement of **synchronization** between spatially separated communication nodes is a major challenge encountered in the design of FHOP systems, as this is perhaps the only drawback, of a frequency hopping system for two reasons:

1) The synch information is communicated in the clear, unprotected, disclosing information that can be intercepted or jammed by an eventual enemy.
2) The process of synchronization inserts some delay and is not easily established in a noisy environment.

d. Therefore, in order to address this vulnerability, the passive synchronization method that was presented does not require the broadcasting of any information about the current state of the frequency hopping system. The proposed method is based on monitoring one of the system frequencies by the stations that wish to synchronize. Using the detection of bursts of energy on this frequency, the time intervals between them are measured. Capitalizing on the information gathered this way, a Boolean linear system of equations is formulated, having as unknowns, the contents of the LFSR that directly correspond to a specific position in the period of the hopping pattern. This system is then solved, using a Boolean version of the Gaussian Elimination numerical solution technique.

Following that method’s presentation, an algorithm implementing it will be presented as well as:

a. The **challenges** and **complexities** that were encountered in the development of the algorithm in Matlab code language.

b. The **conclusions** from the computational simulation of the method.

c. The possible **future implementations** of the method and its algorithm.

More specifically:

a. This **algorithm** receives as **inputs**:

   1) The parameters of the Linear Feedback Shift Register (LFSR) circuit that generates pseudo-randomly the sequence of the switching frequencies, meaning the feed-backing and the frequency selection registers.

   2) The monitored frequency’s binary equivalent.

   3) The time interval between two successive observations of the monitored frequency.

b. The **output-response** of the algorithm, after successive processes of linear algebra and matrix management, is the state of the LFSR at the first
(among two) or generally at the penultimate observation of the surveyed frequency.

c. Once the receiver node knows or computes the above parameters, mentioned as inputs, then "runs" the algorithm and computes the previously mentioned state of the LFSR. This now known, state of the LFSR reveals the whole pattern of the LFSR from the initial to the current state. That information is enough for the synchronization between transmitter and receiver stations, without even the need for beacon frame being sent by the transmitter for the clock synchronization, among the communicating stations.

d. The main scope of this presentation will be the analysis of the conclusions from the computational simulation of the algorithm, proving that the passive synchronization method is fully functional and could be easily implemented in software defined radios that will be competent to communicate using FHOP modulation, without the need for active synchronization methods.

e. In the military framework, the passive synchronization method renders the frequency hopping radios even more tolerant against interception, jamming and generally the electronic counter measures of the enemy's electronic war systems and methods. Moreover, this method can be implemented in our respective efforts in intercepting the enemy's frequency hopping radios, especially if the circuit - generator of the switching frequencies (hops) is known.

f. Moreover, as an extension, our method could be implemented in civilian applications, as in communication systems-protocols where the frequency hopping is engaged (e.g. 802.11x - Wi-Fi, or mobile telephony). And if the sustainability against the enemy's electronic war is the big deal in the military sector, in such civilian implementations the big challenge is the trade-off between the bandwidth and the useful data transmission rate, as it is widely known that the less bits needed to be sent the better for the optimization of the speed, transmission rates and generally of the Quality of Services (QoS). □
Engineering Applications to Security Systems
Time Temperature Superposition Principle:
Application to Process Dynamic Mechanical Analysis Data
of Environmentally Aged
Carbon Fiber Reinforced Composites

Dionysius Mouzakis ¹* and Stefanos P. Zaoutsos ²

¹ Mechanics Laboratory, Department of Mathematics & Engineering Sciences,
Hellenic Military Academy, GR- 16673 Vari, Greece

² Technological Education Institute of Larisa, School of Mechanical Engineering,
GR-41110-Larisa, Greece

*E-mail: demouzakis@sse.gr

Abstract Composite materials in aviation-related structures are subjected to a continuous environmental aging procedure. Our findings on glass fiber polyester composites used in the manufacturing of wind turbine blades have already shown the dramatic alteration of the mechanical properties in aged structures [1].

The benefits in commercial flights in adopting all-composite passenger aircrafts are weight and fuel reduction and therefore an all composite aircraft is much greener than the conventional types. Composite aircraft are supposed to provide at least 20% economy on fuel consumption. Therefore, study of the exposure of high performance materials to environmental aging such as varying temperature, humidity, ultraviolet radiation, etc. is of paramount importance, in order to study the impact of these important aging factors on their mechanical behavior.

Viscoelastic data of polymer matrix carbon fiber composites upon exposure to climatic aging has been assessed in the present study. In order to investigate the combined action of temperature and humidity on composites subjected to changes of temperature from -35 to +40 °C and humidity variations from <10% to 95% RH (non-condensing) specimens were stored in a climatic chamber for 30 days. Some of the pristine specimens were subjected to thermal shock at the same temperature extremes for 12 days every 12 hours. Dynamic mechanical analysis was carried out in a DMA
Q800 (TA Instruments) machine. DMA tests were run in three point bending mode. Frequency (10⁻² - 200Hz) and thermal scans (20-180 °C) were performed, in order to assess the viscoelastic response, as well as the time-dependent behavior of the aged materials.

The Time-Temperature superposition principle was employed to obtain long term data for the viscoelastic response of the aged and pristine specimens. Both Arrhenius and Williams-Landel-Ferry models were applied to model the long term behavior of these specimens at varying characteristic temperature levels below and above the material glass transition regime.

Experimental data, for the range of temperatures and frequencies ranges in focus, showed that the aged materials gained in dynamic stiffness but the gain in the storage moduli, was accompanied by a decrease in the material damping ability, as expressed by the tanδ parameter. These results extend our findings [1] and of Hodzic et al [2] on accelerated aging of glass fiber reinforced composite materials for carbon fiber reinforced ones.

Finally, the applicability of the Time-Temperature superposition analysis was examined for these composites with interesting findings, with respect to the reference temperatures chosen.

References


Dynamic Response of Protein Microtubules

Anastassios K. Lazopoulos

Mechanics Laboratory, Department of Mathematics & Engineering Sciences,
Hellenic Military Academy, GR- 16673 Vari, Greece

E-mails: orfeakos74@gmail.com

Key words: Protein microtubules • gradient elastic flexural beams • free vibrations • micromechanics • new term.

2010 Mathematics Subject Classification 74B99, 74E99, 74M25

Abstract  Protein microtubules (MTs) are basic elements of the cytoskeleton. They are hollow cylinders with axial length that ranges from 10 nm to 100 micrometer, and inner diameter from 15 to 25 nm. MTs are the basic elements of the cytoskeleton that are able to undertake bending contrary to actin and intermediate filaments that are relatively very thin. Hence they are considered as the rod elements of the cytoskeleton whereas the actin filaments are considered as the string elements undertaking tension. Their mechanical behaviour was studied using classical theory of elasticity. Unfortunately, these studies ignored size effects. Classical theory does not analyze the effects of length scale parameters. In contrast, in micro and nano scales, those effects have important contribution. Thus, in order to analyze these structures we must use higher-order continuum theories which include parameters, revealing size effects. Such theories are: Cosserat theory ([2]), Couple stress theory ([3]) and strain gradient theory ([4] and [5]). In the present article we are going to study MTs with the help of thin beam theory which is described in [1]. Thin beam theories based on strain gradient elasticity theories were also introduced by Papargyri et al ([6]), Park & Gao ([7]), Yang et al ([8]). In Lazopoulos [1] bending Bernoulli-Euler beam theory is discussed, into the context of a simplified strain gradient elasticity theory. A new term is introduced, that depends on the area of the cross section of MT. That term strongly increase the stiffness of the beam, especially for thin beams. In fact the theory in [1] bridges the theories presented by Papargyri et al [6] and Yang et al. ([8]) in a consistent way, adding inertia terms as in Xu [9]. The equations derived from [1] are going to be
compared with equations of motion written in [10] and many interesting conclusions are going to be extracted.

In this paper, dynamic response of protein microtubules (MTs) is discussed. Microtubules are modeled as thin flexural beams on elastic foundation, studied in the context of strain gradient elasticity. The present study is performed into the context of linear strain gradient theory of elasticity, described in [1]. The equations of motion are derived through a variational method. A new term is introduced, indicating the importance of the cross-section area in bending of thin beams. That term is connected to the couple stresses, and is missing from existing strain gradient beam theories. Indeed, due to that term, the stiffness of the beam is highly increased, when it is thin. The frequencies of the vibration of the microtubules, derived from the proposed theory, are compared to the existing theories, pointing out the sources of the differences. □

References


On the Mechanics of Nanocomposite Structures using Multiscale Computational Techniques

Stylianos K. Georgantzinos

Mechanics Laboratory, Department of Mathematics & Engineering Sciences,
Hellenic Military Academy, GR- 16673 Vari, Greece
and
Machine Design Laboratory, Department of Mechanical Engineering and Aeronautics,
University of Patras, Rio, GR-26500 Patras, Greece

E-mails: sgeor@mech.upatras.gr and sgeorgantzinos@gmail.com

Keywords: nanomaterials • nanocomposites • finite element method • mechanical properties

Abstract The excellent properties of nanomaterials have generated technological interests in the development of nanocomposites. This work presents finite element techniques that are appropriate for the numerical prediction of the mechanical behavior of materials which are reinforced by carbon nanomaterials. Based on the micromechanical theory, the mechanical behavior of the composite may be predicted by utilizing a representative volume element. Here, within the representative volume element, the reinforcement is modeled according to its atomistic microstructure in nanoscale. Linear spring-based line elements are employed to simulate the discrete geometrical structure and behavior of nanomaterials. On the other hand, the matrix is modeled as a continuum medium in macroscale by utilizing solid elements and in order to describe its behavior an appropriate constitutive material model is adopted. The load transfer conditions between the nanomaterial and the matrix are simulated via the use of special joint elements of variable stiffness interconnecting the two phases in a discrete manner. Using the proposed multi-scale model, the mechanical behavior for various values of reinforcement volume fraction is extracted. Comparisons with available published works found in the literature demonstrate the accuracy of the proposed method.

Hellenic Military Academy
The Stealth Concept as Explained by
Low Probability of Intercept & Low Observability

Theodoros G. Kostis

Department of Mathematics and Engineering Sciences, Hellenic Military Academy,
Vari, GR-16673, Greece
and
Hellenic Quality Assurance & Accreditation Agency for Higher Education,
Athens, Greece

E-mail: tkostis@iee.org

Keywords: probability of intercept • observability • radar • stealth aircraft • AESA/PESA • anti-ship missile defence

Abstract The concept of stealth is an integral part in military operations in all parts of the electromagnetic spectrum (millimeter wave, infrared and optical). In this paper we explain the stealth concept using its major two components which are low probability of intercept and low observability.

All modern tactics that enhance these two components will be analysed and a relevant simulation will be presented.

For example for the low probability of intercept the phased array low power transmitter will be analyzed. This system has the ability to direct its energy into desired locations while minimizing its transmitted presence to other unwanted sectors. Moreover this system is using specially crafted waveforms that provide the stealth advantage.

And as an example of low observability we analyze the use of metamaterials which is a promising tool for reducing the radar cross section of a target. This is especially useful when the target is stealth by design and tries to hide as much data about its presence as possible. The radar detection problem with a stealth aircraft is that the frontal area of the platform is treated to have as low as a radar cross section as possible. Analytically the enhancement from ordinary radar cross section is the channelling of the electromagnetic energy around the target. This action diminishes
the reflection of radar waves to the front and to the sides of the aircraft making even a multistatic radar defence seem inadequate.

We simulate a stealth parameter as a target is crossing the field of view of a hostile sensor. The computational parameters are probability of intercept and observability and the independent variable is time. The radar sensors that are included in the simulation are a superheterodyne receiver with high sensitivity and selectivity connected first to a parabolic antenna and then to a phased array antenna. The environment of the target is taken under consideration in the simulation specifications. For example an anti-ship missile is flying close to the sea surface in order to mask its presence using the surrounding sea clutter.

In conclusion this study shows the balance between active and non-active qualities of a target and the use of its environment in order to successfully minimize its presence in the field of view of a hostile sensor. ☐
City.Risks and Privacy
RST-Invariant Block-based Watermarking for Image Regions

Nikolaos Papadakis¹ and Constantinos Raftopoulos²

¹ Department of Mathematics and Engineering Sciences, Hellenic Military Academy, GR- 166 73 Vari, Greece
E-mail: npapadakis@sse.gr

² Computer Science Division, National Technical University of Athens, Iroon Polytechniou 9, GR 157 80 Athens, Greece,
E-mail: raftop@image.ntua.gr

Abstract Plain rotation, scaling, and/or translation (RST) of an image can lead to loss of watermark synchronization and thus authentication failure. The block based approaches in particular, albeit strong against frequency and cropping attacks, are sensitive to geometric distortions due to the need for repositioning the block’s rectangular grid. In this paper, we propose a block based approach for watermarking image objects in a way that is invariant to RST distortions. With the term image object we refer to semantically contiguous parts of images that have a specific contour boundary.

The proposed approach is based on shape information since the watermark is embedded in image blocks, the location and orientation of which are defined by Eulerian tours that are appropriately arranged in layers, around the object’s robust skeleton. The object’s robust skeleton is derived by its boundary after applying an extraction technique and not only is invariant to RST transformations but also to cropping, clipping and other common deformation attacks.

Experiments using the KIMIA dataset of shapes and the Caltech image database, report results showing the advantages of the proposed scheme in comparison to alternative state of the art methods. □
Tackling Privacy and QoS issues in the Cloud

Dr Nikolaos Bakalos ¹ and Emmanouil N. Protonotarios ²

Internet Science Group, Institute of Communications and Computer Systems (ICCS),
National Technical University of Athens,
9, Iroon Polytechniou Str., GR-157 73 Zografou, Greece

E-mails: ¹ bakalosnik@gmail.com and ² protonot@cs.ntua.gr

Abstract  The current document is a brief presentation of the SLALOM project’s reference model that aims at proposing a specification for cloud Service Level Agreements (SLAs). The proposed SLA specification refers to the core SLA document that incorporates metrics (as specific objectives or quality attributes), parameters, rules as well as potential dependencies between rules.

The SLALOM project aims at tackling problems concerning both the Quality of Service, User Privacy and Data Security issues through a Service Level Agreement (SLA) reference model consisting of model contractual terms and model technical specifications. □
Crowd Sourcing Based Privacy Threat Analysis and Alerting

A. Madia1, S.E. Nikoletseas2, Y.C. Stamatiou3, D. Tsolovos4, and V. Vlachos*5

1,2,3,4 University of Patras, Computer Engineering and Informatics Department, GR- 26504, Rio, Patras, Greece

2,3,5 Computer Technology Institute & Press – “DIOPHANTUS”, N. Kazantzaki, GR- 26504, Rio, Patras, Greece

5 Technological Educational Institute of Thessaly, Computer Science and Engineering Department, GR-411 10, Larissa, Greece.

*E-mail: vsvlachos@gmail.com

Abstract The term crowd sourcing characterizes large scale experimental set-ups which engage large numbers of individuals. The individuals interact, using their portable devices (e.g. mobile phones and tablets), with specialized information systems that collect and process information sent by the individuals.

The main advantage of crowd sourcing is that it mobilizes large crowds of people who volunteer to contribute, using the sensors of their mobile devices, towards the collection of environmental data and information (e.g. weather conditions, city traffic status, pollution indicators, seismic wave propagation etc.) or their behavior itself (e.g. movement). Based on this local data and other information sent by the crowd, the experimenters can derive useful global information about the evolution of a physical phenomenon or explain an observed macroscopic behavior of the crowd population itself. Thus, typically, crowd sourcing mostly benefits the experimenter while it either benefits minimally the participating crowd or benefits it in a long term way.

Moreover, for people to be willing to engage in the crowdsourcing scheme they need to trust the crowdsourcing authority. Also, they can be offered diverse incentives (monetary or other) to compensate for their participation and the use of their mobile phones and other devices [1]. As an example, in a smart building application for energy saving, the personalized preferences (regarding the desired temperature, light level etc.) of people participating in the smart automation scenario by sharing their ambient
data (such as the local conditions at the exact place they are) can be prioritized, so as to achieve a satisfactory trade-off between energy saving and comfort level and in this way to motivate them ([2]). In a similar context, machine learning techniques can be used to extract the user status (whether they are moving, sleeping etc.) in order for the smart automation system to better adapt to their current condition and personalized preferences ([3]).

The work performed within the scope of the European project Privacy Flag is based on the crowd sourcing concept in the privacy domain but from a novel, different point of view: that of benefiting, directly and in real time, the participating individuals with respect to protecting their privacy when installing applications on their devices or visit web sites. The project’s focus is on the exploitation of crowd sourcing techniques, combined with ICT technologies and appropriate legal advice, in order to protect people’s on-line privacy when the visit various web sites using their portable devices roaming within the confines of a (smart) city.

As seen in the figure below, Privacy Flag will empower people to monitor and control their privacy, themselves, with a user-centered solution equipped with friendly interfaces. The solution consists of a smart phone application, a web browser add-on, and a publicly accessible web site. All these components communicate with a database containing information about privacy breach incidents, privacy violating app, web sites and services as well as possible threat combinations which, when they coexist, pose severe privacy risk for the user. This distributed platform aims at designing and implementing a new privacy protection paradigm which combines expert knowledge as provided by privacy threat analysis professionals with locally operating (by the users themselves) privacy enablers. These enablers continuously monitor the installed applications as well as users’ connections to web site in order to detect, using also the experts’ advice coded in the database, unwanted external access to users’ data. Upon detection of such privacy breach attempts, the central database is notified so as to update itself with a, possibly, new identified privacy threat as well as send back to the enabler advice directed to the user of how the privacy breach can be avoided. Further to this automatic, real time, interaction between the enablers on the users’ phones and the platform, users have the opportunity to complete questionnaires downloaded on
their devices and give feedback suggesting improvements and corrections to the platform’s functionality.

The project consortium has identified, as a starting point, the commonly arising privacy threats in users’ daily interactions with device applications, services and websites in the following taxonomy:

Confidentiality Threats:

- Does the website provide data encryption (SSL/TLS)?
- Does the website provide HSTS?
- Is the encryption method (cipher suite) negotiated between client and server considered as secure?
- What information does the website/server directly learn about a user (using forms)?
- Does the website use a trustworthy certification chain?
- Does the website use certificate pinning?
- Which communication parties is data transferred to?

Privacy Threats:

- Does the website use HTTP cookies?
- Does the website use third party cookies?
- Does the site exploits users Web history?
- Does the website use HTML5 Web SQL database?
- Does the website use LSOs?
Does the website use Supercookies?
Does the website comply with any known privacy policy eTrust, P3P, published privacy policy?
Does the website use known fingerprinting techniques?

Emerging Security Threats:

Does the website contain links to malicious sites (Google’s Safebrowsing API)?
Does the website use potentially dangerous advanced HTML5 APIs: Web Audio API?
Does the website use potentially dangerous advanced HTML5 APIs: WebRTC?
Does the website use potentially dangerous advanced HTML5 APIs: Geolocation (GPS)?
Does the website use HTML5 Local Storage?

High Risk Threats:

Does the website use technologies with known security issues - ActiveX?
Does the website use technologies with known security issues - Java?
Does the website use technologies with known security issues – Silverlight?
Does the website use technologies with known security issues - Flash?
Does the website use technologies with known security issues - PDF?

Our consortium has, already, designed a suitable database schema and the corresponding stored procedures which are responsible for codifying and processing these threats in collaboration with the enablers operating locally on users’ devices. The database will be, initially, populated with threats and processing algorithms based on experts’ advice and, later, will be continuously updated and enriched as the enablers will start operating on users’ devices, sending back to them notifications and alarms about potential privacy risks during their daily interaction with internet services and applications.

In summary, Privacy Flag presents a novel view on privacy protection of users in their daily interactions with the Internet based on the crowd sourcing paradigm. The project’s output will be a distributed and crowd-sourced monitoring framework able to provide a collective protection framework combined with increased user privacy
awareness which, as an important consequence, is expected to exert pressure on ICT companies to improve their privacy compliance and privacy protection mechanisms. □

Acknowledgment

This work was supported by the HORIZON 2020 project: “Privacy Flag: Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments”, Grant Agreement No. 653426. Project site: http://www.privacyflag.eu/Consortium.

References

City.Risks: Avoiding and Mitigating Safety Risks In Urban Environments

Nikolaos Papadakis ¹ and Antonius Litke ²

¹ Department of Mathematics and Engineering Sciences, Hellenic Military Academy, GR-166 73 Vari, Greece
E-mail: npapadakis@sse.gr

² Institute of Communications and Computer Systems (ICCS), National Technical University of Athens, 9, Iroon Polytechniou Str., GR-157 73 Zografou, Greece
E-mail: ali@telecom.ntua.gr

Abstract The main objective of the City.Risks project is to increase the perception of security of citizens in cities by activating in a more transparent and sustainable way their participation in communities, through which information and interventions can be provided both to proactively protect citizens from falling victims to criminal activities as well as to reactively provide more timely and effective response and assistance. In order to do so, the City.Risks project will leverage a set of innovative technologies, city infrastructures, and available data sources, but more importantly will aim at making the citizens’ smart phones the modern tool for increasing their personal and collective sense of security. The project will design and develop an innovative ecosystem of mobile services that will transform the smart phone or the tablet of the citizen into a tool that will collect, visualize and share safety-critical information with the appropriate authorities and communities. The project will rely on a wide spectrum of available technologies to design and implement an interactive framework among authorities and citizens through mobile applications that will allow in a collaboratively way to prevent or mitigate the impact of crime incidents or other security threats. Thus, it will contribute to an increase of the citizens’ perception of security, which will be measured and validated in real-life scenarios and conditions through the deployment and operation of pilot trials at several selected cities by the project partners. Moreover, to further found its sustainability, the project will devise business models and replication plans of its results that will contribute in the next generation innovative security solutions for the future smart cities. □
Chaos and Randomness in Cryptography
A Smart Port Knocking Mechanism
for Hiding the SSH Port from Attackers

Antonios S. Andreatos
Div. of Computer Engineering & Information Science
Hellenic Air Force Academy, Dekeleia Air Force Base
Dekeleia, Attica, TGA-1010, Greece

E-mails: informatics.hafa@haf.gr, aandreatos@gmail.com

Keywords: cyber-security • knockd • port-knocking • ssh port • knock sequences • pseudo-random number generator • Hénon map

Abstract A popular protocol for connecting to servers remotely is Secure Shell, or SSH. SSH is a cryptographic network protocol operating at the application layer to allow remote login and other network services to operate securely over an unsecured channel such as the one provided by the public Internet ([1]).

A good security practice is to deactivate services when not needed in order to reduce the so-called attack surface. For this purpose, port-knock software has been developed; port-knock software hides a specific port (here, the SSH port) until a specific port sequence happens. Port-knock software for Linux servers is knockd ([2]). A knockd server listens to all traffic on an Ethernet interface, looking for special "knock" sequences of port-hits. A client makes these port-hits by sending TCP or UDP packets to specific ports on the server. These ports need not be open; since knockd listens at the link-layer level, it sees all traffic even that destined for a closed port. When the server detects a specific sequence of port-hits, it runs a command defined in its configuration file, in order to open up port the SSH port (no. 22) in a firewall for quick access ([3, 4]). Figure 1 demonstrates an example of a port-knocking sequence using TCP and UDP.

13821:tcp, 7803:udp, 19552:tcp, 35813:udp, 54926:udp

Fig. 1 - Example port-knocking sequence using TCP and UDP packets
If the knock sequence is invariant, sniffing may uncover the secret sequence ([5]); hence, the security of this scheme is low. A better way is to use a pseudo-random number generator (PRNG) to produce a varying port sequence ([6]). However, the produced sequence will be the same each time the system re-starts; another weakness is that if the generator has a small period, the system is not safe enough. In order to solve this problem a powerful PRNG such as Mersenne twister ([7]) could be used.

This paper proposes an advanced port-knocking mechanism based on a PRNG which produces different sequences each time. The proposed mechanism meets the following requirements:

a/ It generates a number of pseudo-random port numbers and/or protocols (TCP or UDP) and writes them in a special file; the produced pseudo-random is different each time the algorithm is run because it uses a function of the system time as a seed;

b/ The produced port numbers fall in the upper port range (e.g., 10000-65000), and the range limits may be configured by the user;

c/ The same algorithm runs at both the client and the server;

d/ It modifies the server’s knockd configuration file to get the secret port-knocking sequence from the above special file;

e/ It generates a new port-knocking sequence after each ssh connection at the client and the server.

We demonstrate the mechanism using a server installed on a virtual machine and a Hénon chaotic number generator ([8, 9 and 10]).

A Hénon chaotic series (map) may be produced by the set of difference equations shown in Figure 2 ([8, 10]).

\[
\begin{align*}
    x(i+1) &= y(i) + 1 - ax(i)^2 \\
    y(i+1) &= bx(i)
\end{align*}
\]

Fig. 2 - - Hénon's difference equations
Matlab code simulating the Hénon map [10] produces two vectors (x and y). In this demonstration we use the x vector to produce the port numbers and the y vector to get the protocol.

References

Optimum Sampling of Cipher Keys and Output Streams for Cryptographic Tests

George Marinakis

Telecommunications and Electronics School of Military Signal Officers
“Karaiskakis A” Camp
Nikolaou Sourtzi,
GR-124 61, Haidari, Greece

and

National Intelligence Service
4, Panagioti Kanellopoulou Str.
GR-101 77, Athens, Greece

E-mail: gmari@tee.gr

Abstract The basic aim of cryptographic tests is to examine the randomness of the cipher output and the independency of its keys. Therefore, the tests are conducted in two steps: a) Randomness check: For each key, we produce an output bit stream of the cipher and we examine its randomness. b) Independency check: We compare each output stream with the output streams which we have produced with the other keys.

Since modern cryptographic ciphers have an enormous key diversity, if in the above tests we want to check all the keys, this will take practically an infinite time. Therefore, in practice we must check a much smaller number of keys, using a sampling method. And in order to have the minimum sampling error, we must solve three basic problems:

a) How many keys and corresponding output samples we must examine?

b) How large must be the size of each output sample?

c) The key selection will be completely random or it must follow some rules?

The general rule is that, the sampling error is reduced as we increase the number of the checked keys and output samples. But since the tests must be executed in an acceptable time, we must compromise the above rule with some additional factors, such as the type of the cryptographic cipher, the maximum size of the plain text and of course the available computer power.

In this study we examine the interrelations of the above factors, and we propose applicable solutions and procedures. And also we propose a method for the optimum selection of the keys, which combines a random and a concrete choice.
Optimization of Hénon Chaotic Coefficients Based on Lyapunov Exponents

Antonios S. Andreatos¹ and Apostolos P. Leros¹,²

¹ Div. of Computer Engineering & Information Science
Hellenic Air Force Academy, Dekeleia Air Force Base
Dekeleia, Attica, TGA-1010, Greece
E-mails: informatics.hafa@haf.gr, aandreatos@gmail.com

² Department of Automation, School of Technological Applications
Technological Educational Institute of Sterea Hellas,
GR-34400 Psachna, Evia, Greece
E-mail: lerosapostolos@gmail.com

Keywords: Hénon map • chaotic map • Lyapunov exponent • optimization • simulation • Matlab

Abstract The Hénon chaotic signals are produced by the solution of the Henon map which is a set of two coupled first-order difference equations:

\[ x(i + 1) = y(i) + 1 - ax(i)^2 \]
\[ y(i + 1) = bx(i) \]

with initial conditions \([x(0), y(0)] = [0, 0]\) and constant coefficients \(a\) and \(b\). Although the equations are simple, under specific initial values and coefficient values they produce chaotic attractors. Figure 1 shows the characteristic Hénon attractor obtained by 20000 iterations for \(a = 1.4\) and \(b = 0.3\), starting from the initial point \(x_0 = 0, y_0 = 0\).

Figure 1 – Hénon’s characteristic chaotic attractor
In this study, given an initial point \( a_{\text{opt}} \) and initial values for the parameters \( b \), we demonstrate a simple method for finding optimal Hénon’s parameters \( a_{\text{opt}} \) and \( b \), in order to get good quality chaotic behavior. Lyapunov exponent is used as the criterion for assessing chaotic behavior.

The proposed method during the first round optimizes the \( a \) parameter (finds \( a_{\text{opt}} \)) while keeping \( b \) constant; the \( a_{\text{opt}} \) value is that which gives the maximum Lyapunov exponent (Figure 2).

![Figure 2 - Optimization of Hénon’s \( a \) parameter](image)

In the second round we keep \( a_{\text{opt}} \) constant (the optimal value found in the first round) and optimize \( b \) (to find \( b_{\text{opt}} \)) using the same (Lyapunov exponent) criterion (Figure 3).

![Figure 3 - Optimization of Hénon’s \( b \) parameter](image)

The whole research is simulated in Matlab. From the simulations it was clear that there are countless parameter combinations which produce good chaotic behavior,
as well as, other sets which produce no chaos at all (indicated by zero Lyapunov exponent). Using this two-phase method we achieve an increase of the Lyapunov exponent from about 2.5 to up to 2.6 or even 2.7. The higher the Lyapunov exponent the more chaotic the signal; Lyapunov exponent values around 3 are considered good.

References

Cloud Security and Big Data Analytics
Secure Data Restoration in Cloud Systems

Nikolaos Bardis

Informatics Laboratory, Department of Mathematics & Engineering Sciences,
Hellenic Military Academy, GR- 16673 Vari, Greece

E-mail: bardis@ieee.org

Abstract In this work, a method for backup and restoring data is proposed for the reliable restoration of data in Cloud Systems. The data is stored on different storage nodes and temporary or permanent loss of access to any q of them appears. The high efficiency of the proposed method is achieved by using a theoretically proved minimum number of backup storage nodes based on users. The theoretical justification with a methodology of backup codes and their use for data recovery, which is illustrated by examples, is presented. The theoretical and experimental effectiveness evaluation of the proposed method is demonstrated as well. The proposed method is aimed to ensure a high level of survivability of cloud systems for military applications.
Big Data Analytics for Crisis Detection and Management

Nikolaos Doukas
Department of Mathematics and Engineering Sciences, Hellenic Military Academy,
GR- 16673 Vari, Greece

E-mails: ndoukas@sse.gr and nikolaos@doukas.net.gr

Abstract The scientific area of crisis management has been in the center of attention for multiple disciplines especially computer science for military applications. In the information centered and computer driven world, a major aim of computer scientists is to manage and analyze Big Data, extract information from heterogeneous sources and store it in unified structure formats that allow further processing. In this paper, Big Data analytics techniques and tools that are useful in all phases of crisis management are presented. Furthermore, a system-engineering approach of a big data management system will be analyzed that comprises of four phases; data generation, data acquisition, data storage, and data analytics. Benefits of the usage of Big Data for crisis management are analyzed. An innovative view of open problems concerning Big Data in crisis management is introduced.
Secure System for Refugee Flow Management

Faidon Toufeksis, Emmanouil Dontas, Nikolaos Doukas and Nikolaos Bardis*

Informatics Laboratory, Department of Mathematics & Engineering Sciences, Hellenic Military Academy, GR-16673 Vari, Greece

*E-mail: bardis@ieee.org

Abstract This paper aims to propose a plan of action at local level for the management of refugee and immigration flows and to coordinate the actions of Non-Government Organizations (NGOs). Military actions in various countries result in large immigration flows, the routes of which pass through neighboring countries.

In this paper, the establishment of a coordinating agency for the control and the authorization of voluntary organizations is proposed, including responsibilities and the structure of the reception centers.

An automated system for the authorization of voluntary organizations is presented that defines prerequisites and procedures for the activations for NGOs. Its architecture is structured in the Business Process Modeling Notation language.

An application of the model is explained for the case of the war in Syria and the flux of refugees to Greece. Big Data analysis is employed on data from the social media, for the purpose of the detection and early warning about crises.

Finally the ZEUS application is presented that handles communication and incident handling between users is presented, with emphasis on its cryptographic and security components.