November / December 2007, Volume 3, Number 3

ECN

European CIIP Newsletter

EU WS on ICT Financial Infrastructure

IRRIIS- Project WS

Government Security Vision 2020

Global View of Internet Security Situation

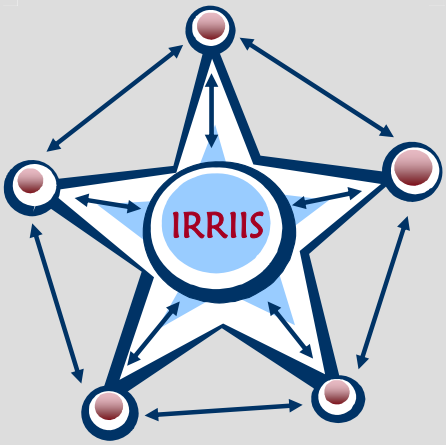
SCADA and C(I)IP

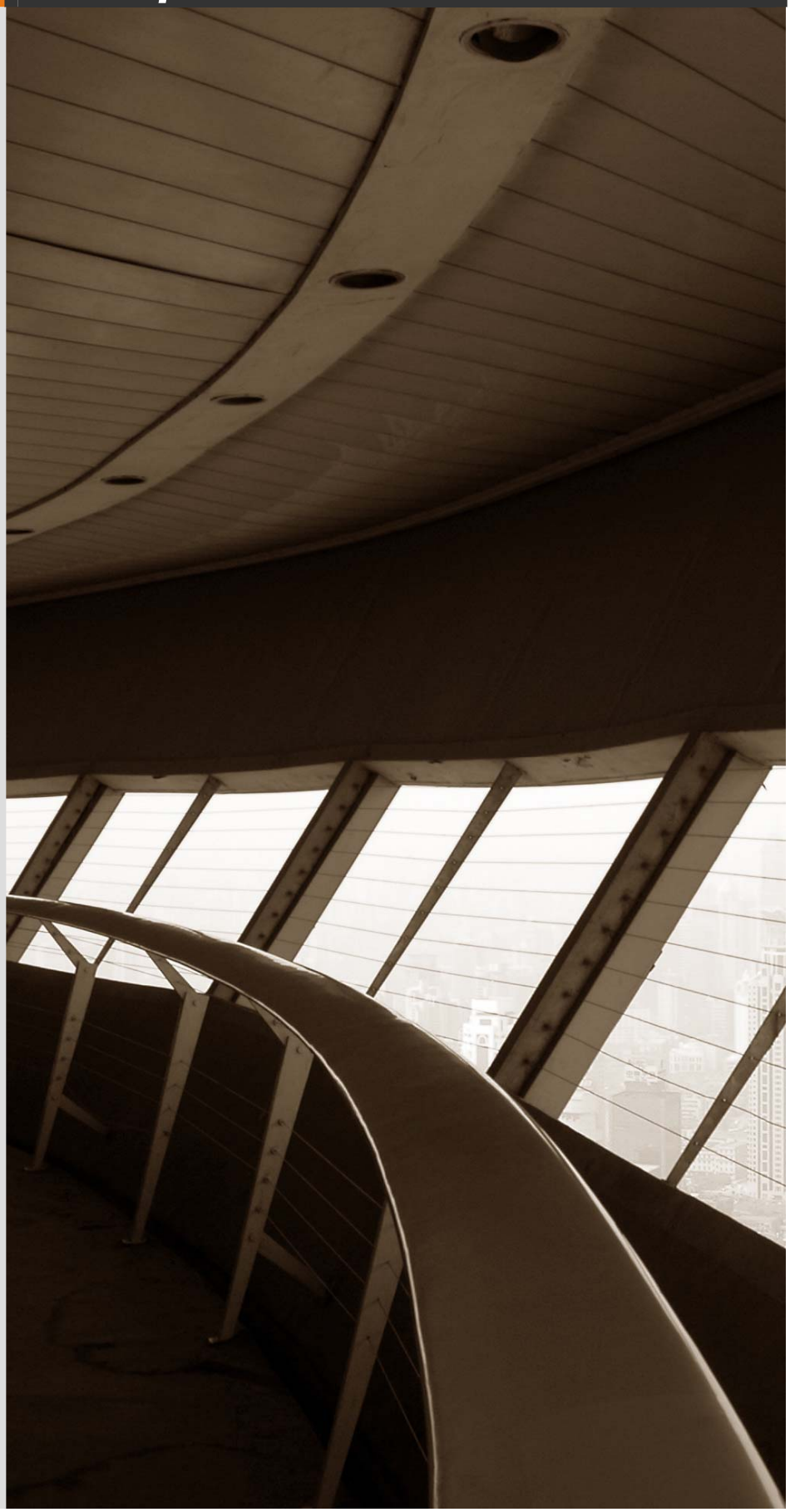
Security Infor-mation Reduction

Entropy-Based Alert Correlator

About CRITIS Conference Series

IMF und DIMVA 08





> About ECN
ECN is co-ordinated with
The European Commission, was initiated by Dr. Andrea Servida,
and is now coached and supervised by Angelo Marino
For 2007-2009, ECN is financed by the IRRIIS project
The IRRIIS project is an IST FP6 IP,
funded by the European Commission
under the contract no 027568

>For ECN registration send any email to:
subscribe@ciip-newsletter.org

>Article can be submitted to be published to:
submit@ciip-newsletter.org

>Questions about articles to the editors can be sent to:
editor@ciip-newsletter.org

>General comments are directed to:
info@ciip-newsletter.org

>Download site for specific issues:
http://irriis.org
http://www.ci2rco.org

>Founder and Editors
Eyal Adar CEO iTcon, ***eyal@itcon-ltd.com***
Bernhard M. Hämmerli, HTA, Initiator and Main Editor ***bmhaemmerli@acris.ch***
Eric Luiijf, TNO, ***eric.luiijf@tno.nl***

>Country specific Editors
For Germany: Heinz Thielmann, Prof. emeritus, ***heinz.thielmann@t-online.de***
For Italy: Louisa Franchina, ISCOM, ***luisa.franchina@comunicazioni.it***
For France: Michel Riguidel, ENST, ***riguidel@enst.fr***
For Spain: Javier Lopez, UMA, ***jlm@lcc.uma.es***
For Finland: Hannu Kari, HUT, ***kari@tcs.hut.fi***

> Spelling:
British English is used except for US contributions

Table of Content

Introduction

INTRO	**Focusing EU C(I)IP Conferences by Using Opportunities of Joint Activities** **by Bernhard M. Hämmerli**	**5**

European Activities

EU WS on ICT Financial Infrastructure	**Protection of Critical ICT-Based Financial Infrastructures** **by Henning H. Arendt**	**6**
IRRIIS-Project	**IRRIIS Workshop „Control Centres"** **by Ralf Linnemann & Césaire Beyel**	**9**

Country Specific Issues

Switzerland	**Medium and Long Term Security Visions for National Governments** **by Peter Trachsel**	**11**
Germany	**The global View of Security Situation in the Internet** **by Norbert Pohlmann**	**14**

Methods and Models

SCADA and CIP	SCADA Cyber Security, Critical Infrastructures' Achilles Heel? By Elyoenai Egozcue, Daniel Chavarri, David Barroso	18
Security Information Reduction	SERKET: CEP Adapters for securing public events and spaces by Antonio Skarmeta, Mercedes Valdés, Aljosa Pasic, Rafael Llarena	21
Entropy-Based Alert Correlator	Strategic Management of Security Information through an Entropy-Based Alert Correlator By G. C. Garriga, J. L. Balcázar, J. Ballesteros, J. Megias and A. Palomares	24

News and Miscellaneous

Critis 2007	2nd International Workshop on Critical Information Infrastructures Security by Javier Lopez and Bernhard Hämmerli	31

Slected Links and Events

	Upcoming CIIP Conferences	33
	Selected Links • Actual Upcoming CIIP Conferences in Europe • European Projects or Projects with Articles in this Issue • E-Reports	33
	Critis 08 by Roberto Setola	34
	IMF 2008 by Dirk Schadt	35
	Dimva 2008 by Hervé Debar	36

Focus in EU C(I)IP Conferences Using Opportunities of Joint Activities.

International collaboration of four associations in the critis'07 conference in Malaga gives focus to the C(I)IP conference world.

Dr. Bernhard M. Hämmerli

Professor in Information Security
Founder of the Executive Master Program IT Security, FHZ
Vice-President ISSS Information Security Society Switzerland and Chair of Scientific and International Affairs

bmhaemmerli@acris.ch
bmhaemmerli@hslu.ch

About this Issue

The conference CRITIS'07 was mainly organised by our Spanish editor Javier Lopez. To focus CIIP conference activities in Europe we brought people from the ITCIP conference of the EU project IRRIIS, of the Information Assurance Taskforce IEEE, the German Informatics Expert Groups KRITIS and of the IFIP together in one single conference in Malaga, October 3-5, 2007: critis07.lcc.uma.es. We wanted to leverage from the momentum gained with the conferences by producing a set of articles with focus on Spanish C(I)IP. Both, Javier Lopez (board of CRITIS steering committee) and Sofia Moreno which is responsible of the secretariat of eSEC (Spanish Technological Platform for Security and Dependability) were positive about the idea and supported ECN in this activity.

The post proceedings critis'07will be available later in 2008 in Springer Lecture Notes Series**.**

The set of Spanish articles will be distributed over two issues. This issue (ECN no 8) has three contributions of Spanish authors.

Highlights of this number:

- Workshop on "Protection of Critical ICT-Based Financial Infrastructures" was held, on 24-25th September in Frankfurt. Major results are given here in ECN.
- An unusual honest "Medium and Long Term Security Visions for National Governments" is given by a top executive of Swiss government.
- "A Global View of Security Situation in the Internet" presents an actual German project which may be enlarged to international level in the near future.
- Three Spanish industry contributions:
  - On SCADA Security
  - On public events monitoring
  - Correlation of monitoring

Sofia Moreno and Javier Lopez making fun of airport rules with a Swiss chocolate army knife

Authors willing to contribute to future ECN issues are very welcome. Please contact me. Further information about the ECN and its publication policies can be found in the introduction of the first ECN, see www.irriis.eu.

Enjoy reading the ECN!

Protection of Critical ICT-Based Financial Infrastructures.

A workshop entitled "Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years" was held in Frankfurt/Germany on 24-25th September 2007.

Henning H. Arendt

Chairman of the European Finance Forum and President of @bc® - Arendt Business Consulting
henning.arendt@europeanfinanceforum.org
henning.arendt@atbc.de

The rapid growth and deployment of Information and Communication Technologies (ICTs) that we are experiencing today is having profound impact on the financial service industry. On the one hand, the ICT infrastructures over which critical financial services are being delivered are becoming ever more interconnected, open and ubiquitous, but at the same time, ever more fragile and vulnerable to failure and cyber-attacks. On the other hand, over the coming years, it is expected that in the financial sector, the level of self-service will become significantly higher than today, with ubiquitous and mobile banking becoming strong market drivers.

Financial service value chain will change

Industrialisation, business process outsourcing and number of intervening actors in the service value creation chain will further increase, changing the way financial services will be composed and delivered, while continuing to guarantee their very high-level of trustworthiness. This, in turn, would require: defining trustworthiness and new levels of trust in the ever increasing supply chain, and reliability of highly distributed infrastructures while dealing at the same time with severe constraints over business continuity management. And, security and privacy in both the clients and the client advisors behaviour will be a key success factor for banking and, more broadly, for the financial industry.

Current rapid growth and deployment of ICTs is having profound impact on the financial service industry.

Two day workshop involves stakeholders and researchers

A workshop entitled Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years was held on 24-25th September 2007. The workshop was well attended by the European Commission and stakeholders from the financial industry and researchers from the ICT Security and Critical Information Infrastructure Protection domains. The participants over the two day workshop held intensive working group sessions based upon inspiration keynotes from industry and researchers in order to discuss and elaborate the research challenges associated with "massively distributed critical financial infrastructure protection (FIP)" and "trust in new value added business chains".

Purpose and goals of work sessions

The purpose and goals of the session were twofold: Part 1. Elaborate a number of scenarios or requirements for a Trust Framework in new value-added business chains for the next five years;
Part 2. Based upon the scenarios and requirements in Part 1, discuss and elaborate the current and future research and technological (RTD) challenges to achieve the Trust framework in new value added business chains.

Recent coordinated activities

A number of coordinated activities sponsored by ICT Unit F.5 "Security" have taken place over the last years and resulted in setting the scene for this dedicated workshop on financial infrastructure protection. In May 2006, the IST FP6 SecurIST project organised the Joint SecurIST, Mobile & Wireless Workshop. Its main purpose was to bring together the ICT Trust, Security and Dependability research community with the Mobile and Wireless research community to discuss and propose future research areas of common and mutual benefit to their constituencies. An incisive keynote address "Banking in 2015 and its Impact on Technology, namely on Mobile Technology " formed a basis for an important scenario used within a number of intensive working sessions. In September 2006, a Workshop was organized by the IST FP6 ESFORS project entitled Joint Workshop on Software and Services Development, Security & Dependability . Within working sessions, major research topics were discussed that would contribute to the provision of CIIP in the finance industry.

Focus of workshop sessions on tust and protection

During the Workshop held in September 2007, three dedicated working sessions entitled

- Trust in new value-added Business chains,
- Protection of Massively Distributed critical Financial Services and
- Protection of the Critical Base Infrastructure defined a number of research topics considered beneficial and necessary for continued mutual collaboration between all the stakeholders from the financial industry and researchers from ICT Security and Trust communities with a focus on:
  - How the situation in the European financial sector will evolve over the next 5 years in the two main themes of the workshop: protection of massively distributed critical financial infrastructures; and, trust in new added value business chains;
  - Developing joint scenarios and consequent strategic plans and research directions on how future trustworthy financial services could be constructed and delivered over critical ICT-based service infrastructures and how these latter could be protected from any kind of cyber-threat.

The workshop addressed issues that span beyond a single financial institution or national market. It specifically addressed global, cross border and multi-member state issues and correlations, which may impact or destabilize critical ICT-based financial infrastructures of the European economy.

Workshop outcomes provide input to future research

The workshop outcomes were twofold:

1. Bringing together all of the relevant stakeholders types (Financial industry, ICT TSD and CIIP researchers) to engage in dialogue and stimulate collaborative research actions in view of the EU's FP7 call for R&D proposals in the area of critical infrastructure protection, including the protection of ICT-based critical financial infrastructures;
2. Provides input to future strategic research directions that the European Commission will support in its next work programme for ICT Research, for the period 2009-2010.

Trust in new value-added Business chains

The participants of the session first discussed the focus criteria and centre of gravity of the session theme called “Trust in new value-added Business chains”. They agreed that this was centred on:

- Dealing with communities both within and outside EU;
- Dealing with huge volumes;
- Solution that is multiple and not monopolistic;
- Access to markets and provision of choices. Universal access e.g. equity markets;
- Modelling the risks assessment and execution chain;
- Collaboration to aggressively prevent and if necessary remedy attacks on the integrity and reliability of electronic communication;
- End user capabilities making them as a strong link in the chain as others;
- End user control and awareness of operational trust model;
- Using technology capabilities and techniques between banks and chains of service providers.

Protection of Massively Distributed critical Financial Services

The purpose and goals of the session were to examine the research challenges involved in “Trusted sharing of confidential information in massively distributed financial infrastructures”. Other goals pursued by the participants included the following:

- Identity federation in the supply chain based on trust levels that each participant needs to reach through certification
- Disaster, Outsourcing, Moving: transient organisational phases increase risks but for the speed and simplicity during these phases often the additional risks are neither controlled nor internally communicated. Also, the lower level of trust during these phases is not communicated partners and tracked.
- Society need to profit from convergence, for example tracking and localisation of goods
- Self healing systems, systems designed for flexibility. Individual nodes should have more intelligence. Self-conscious nodes.
- Accepted Polymorphic identities, for each identity representation some

attributes are mandatory others are discretionary.

The observations were confirmed, which were mentioned in several presentations, namely

- Socio economic trends drive towards
  - Online accessible real-time services
  - Further industrialization and commoditization of financial service supply chain
  - Privacy protection for customers
- Exposure to online organized crime requires new approach to security modelling into business logic (misuse cases)
- Catastrophic events transiently change risk appetite, meaning that trust (to devices and individuals) increases during recovery phase without trustworthiness having changed.

Protection of the Critical Base Infrastructure

The purpose and goals of the session were to discuss the challenges associated with the following topics:

- End-user protection in a highly distributed environment (mobility);
- Secure communication channels (current and future Internet);
- In a catastrophic disaster, recovery critical infrastructure methods;
- Regulatory issues, collaboration environment.

During the session, multiple issues arose related with the security of critical Infrastructure. In the first part of the session, the group identified the following scenarios summarized below:

- End-user protection in a highly distributed environment (mobility): Mobility is becoming one of the main differentiators within the financial services, providing the end user to access to the financial services

anytime, anywhere. This situation creates also some security deficiencies, related mainly with user terminals, privacy, malware detection and reaction, etc.

- Secure communication channels (Internet), this was one of the most controversial scenarios, taking into account that the secure communication channel is in principle part of the supposed Internet security infrastructure and protocols topic. It was noted by some group members that it could not be part of this R&D initiative.
- In a catastrophic disaster, critical infrastructure recovery methods: One of the main concerns is related with the critical single points of failure, what could happen in case one of the main European infrastructure nodes would be down, how could the rest of the infrastructure recover from such a situation.
- Regulatory issues, collaboration environments. Define a collaborative framework, managed and controlled by automatic processes that keep up-to-date every individual European entity (banks, government, police, etc.) with the possible threats environment.

Main challenges and goals

One of the main goals are the personal data protection (privacy), the way to define an identity and authentication management that guaranties the security within the user access taking into account the mobile environment. In addition to the protection of personal data and to having strong authentication methods, the quality of service and service availability are also important challenges to be discussed and analyzed within the scenarios defined above.

One of the main concerns of financial entities is related with the real time proactive and trusted data sharing environment, the possibility to define a federation system where the financial entities could share threats, risks and some other important information in order to apply the pertinent protection measurements. In order to go ahead with the previous topic, one important goal is the standardization, within the different interfaces, but also the interface standardization between communication entities. Risk assessment and risk modelling were also some important topics discussed during the session, identifying possible risk and quantifying the impact based on those risks. For this topic, one important research area is the attack simulation and the possibility to identify cascading effects. Other important topics discussed during the session included the following:

- European regulatory and laws enforcements
- Resiliency, redundancy, reliability of highly distributed financial environments
- Advanced behaviour detection, prevention and reaction mechanisms (i.e. heuristic analysis)
- Robust segmentation (of services and applications)
- Managing the organization of business aspects following merging of companies

Workshop outcome summary

The outcomes of this workshop included the following:

- In each of the scenarios, new technologies and associated risks were identified;
- Exposure to online organized crime requires new approaches to be addressed;
- Secure communication channels are required (current and future Internet);
- Regulatory issues in collaboration environments need to be addressed;
- Significant joint efforts of academia, stake holders and regulators are needed.

IRRIIS Workshop „Control Centres".

Insights in the daily business of energy management, one of the main research areas of critical infrastructures within the IRRIIS project at Siemens premises in Nürnberg and Erlangen.

Ralf Linnemann

Fraunhofer IAIS
IRRIIS Projekt Management
ralf.linnemann@iais.fraunhofer.de

Césaire Beyel

Fraunhofer Institut IAIS - Abteilung ART
Schloss Birlinghoven, IRRIIS Staff
cesaire.beyel@iais.fraunhofer.de

Members of the IRRIIS project had the opportunity to visit several technical facilities of Siemens at 5th and 6th of July in Nürnberg and Erlangen. Siemens hosted a workshop which offered valuable insights in the daily business of energy management, one of the main research areas of critical infrastructures within the IRRIIS project. More than 20 people seized the opportunity to get first hand knowledge from a leading technology provider. They came not empty handed, because Siemens offered the participants preliminary information in a document about the basics of power systems management, which allowed a thorough preparation.

The workshop started with an introduction into Siemens energy management systems. Since one of the goals of the IRRIIS project is the understanding of critical infrastructures (CIs) and their mutual interdependencies, the topic was of utmost interest. Of particular interest were structure and functionality of network control systems as well as the network control centre data model and its maintenance for the modelling activities within IRRIIS, which shall allow the simulation of scenarios with a network of CIs and their services.

Next was an overview about the basics of control centre activities, their communication network and the modular system architecture for energy automation. This topic was of major relevance for the IRRIIS activities aiming at the development of a middleware improved technology, which will comprise add-on components to facilitate the information exchange between operators of different CIs. The theoretical part was backed up by a demonstration in one of the Siemens operator training systems (OTS). Afterwards the chief operator readily answered the considerable number of questions from the participants.

IRRIIS topics from a network operator point of view were dealt with by an operator of e.on, one of the major power suppliers in Germany. A lot of questions prepared by IRRIIS members were thoroughly discussed. A special focus was on blackouts in general and particularly in the Emsland blackout. It is essential for projects like IRRIIS to understand the mechanisms and principles which lead to a blackout in order to take measures for prevention, mitigation and recovery, and this session led to a deeper understanding.

The first day was closed by a dinner in a restaurant lying in the picturesque Old Town of Nürnberg, which offered the opportunity to discuss interesting issues of the day in a relaxed mood.

Traditional German Dinner in Nürnberg

The second day was focussed on visiting facilities in operation. First was the control centre n-ergie, which presented its communication network. Data collection, data control and data exchange is of special interest for the IRRIIS activities to model CI components and their dependencies, and the lively discussion reflected this. Afterwards the participants were transferred by bus to Siemens facilities in Erlangen. A visit of an 110kV/ 20kV substation gave a realistic impression of real technical equipment. The workshop was closed by a control centre for Siemens facilities Emergency units in full operation.

Excursion leader Christine Schwaegerl and group

Control Centre in n-ergie

All participants felt that this workshop was a sound combination of insights into practical work of energy management and of theoretical background

.

Medium and long term Security Visions for National Governments.

With e-government the dependency on secure public IT will extend. Some aspects are discussed.

Peter Trachsel

Deputy Head Federal Strategic Information Unit, Switzerland.
Peter.Trachsel@ISB.admin.ch

In collaboration with Bernhard Hämmerli

Introduction

This article considers the medium- and long-term challenges that will confront e-government as a part of a secure information society.

Sensitization and regulation

In the next couple of years, society will be considerably more dependent on governmental information technology (IT) and IT security (ITSEC) than it already is today. Critical public infrastructures will depend entirely on secure IT – and vice-versa. The State will transact most of its information-channels and processes with citizens and the private sector digitally. Accordingly, ITSEC will for example become a critical success factor for equal opportunity in the context of efficient fulfilment of democratic rights and duties.

Critical infrastructures will depend entirely on secure IT – and vice-versa.

For nations enjoying stable economic and political circumstances, ITSEC will also become a business case. Modular and reusable ITSEC-services, built on an open SOA-architecture will get an economic and political asset, also for the public sector. More and more, politics and media will understand that and exert correspondingly more pressure on public administrations, demanding secure public IT. The currently still hypocritical approach to the topic will have made way to more serious consideration.

This consideration may also become contra-productive: e-government will progress now very quickly, ITSEC will lag behind, at least in the next years. Therefore the number of security-incidents with public visibility will grow. It should be avoided that politics and administration reflexively react to such consequences with over-regulation without concrete technical and methodical ITSEC-guidelines how that happened in the last years in many countries in the area of data protection.

Politics and administration will also have intensified their national and international cooperation in the security field and deal with security in a more integral way. Boundaries between civilian and military security, but also between ITSEC and more conventional security technologies and methods will become increasingly blurred. Even the private sector will join cooperation models that permit mutual information and assistance in the case of imminent or occurred security problems. The public sector will take on important coordinating and confidence-building tasks. This development is already apparent today: It is remarkable in that the culture of secrecy surrounding security problems is disappearing, and apparently even companies competing with each other economically classify the utility of cooperation on security issues as very high.

Threats, challenges, and risk management

Extrapolating from current developments, a diffuse and fast changing threat landscape will emerge in the next couple of years, which will make the protection of security both complex and labour-intensive. The security policy context will be characterized by the threats of international terrorism and regional, cross-border conflicts. These threats will also impact the security of critical information infrastructures. In particular, the rising level of professionalized crime will increasingly and systematically target IT, but also use IT as a tool.

Modular and reusable ITSEC-Services, built on an open SOA-architecture will get a strategic asset, also for the public sector.

Administrations will continue to be a particular focus of attacks, since they are of special interest in terms of intelligence and politics.

The globalization of society also entails a globalization of IT. This will affect e-government architectures in particular, which cover an especially broad group of users whose risk levels can only be differentiated with difficulty. The many administrative (and private) networks that are today still largely sealed off by firewalls should have to be "opened up" for fast and flexible communication. But the requisite end-to-end technologies with ergonomic security services on application level will be even by the next ten years, however, hardly available in all areas and regions.

For many e-government users, contacts with the administration are involuntary and often associated with costs and administrative work that add "no value". This increases the risk of careless, intentional, or irrational misconduct. This has to be considered in this kind of government-specific risk-management.

The demands on integral ITSEC risk management in the context of e-government will increase largely. With a high probability, most administrations will therefore have a very high base-level of IT-protection, satisfying the security demands of most e-government transactions and rendering explicit application-individual quantitative risk analyses more or less unnecessary. This entails, however, that communication partners outside the administration must meet this high level of basic protection and that someone must bear the associated costs.

A reassuring alternative could be a greater degree of technology-aided and therefore automated risk management procedures. To what extent however they will be available in time for the complex and extensive e-government-demands is still an open question?

SOA: Foundation of future ITSEC architectures

Most national e-government strategies aim to offer services that reflect the circumstances of life or business of the client in question. Contacts with the administration should be achievable via uniform interfaces and, where useful, administrative processes should be performable by way of non-stop transactions.

The demands on integral ITSEC risk management in the context of e-government will therefore certainly increase largely

However, federal structures in particular have difficulties in managing the requisite inter-structural harmonization of business- and IT-processes. Accordingly, the underlying integrated ITSEC policies, architectures, and services are also lacking.

One of the basic questions is whether, in the next years, the strategic administrative processes will drive IT and IT security or vice-versa. With a high degree of probability, the path will lead via technology, especially ITSEC; i.e. a bottom-up development will take place. The public sector plays a very important role in this regard. First of all, it must make generic, standardized, and reusable IT(SEC) services available relatively quickly. These services must be made available on the basis of service-oriented architectures (SOA) with respect to the development of downstream applications. In this way only an incentive can be created for a secure, integrated, interoperable and efficient basic e-government architecture, which might then lead to the harmonization of business processes. For instance, PKI services will likely be the basis for digital signature services, which in turn will lead to secure DMS and workflow components and business administration systems. Naturally, this vision does not correspond to the usual textbook "best practices", and many questions arise here as well:

Should public administrations bear the risks of the "early ITSEC-technology adaptor"? Should these services be offered in federal administrations in a concerted or in a competitive manner? How is the subsidiarity of the administration affected when such services also become a business case for the private sector? Do service-oriented architectures (SOA) really have a future? How must ITSEC services be modelled technically? Does e-government have a greater need for generic services (PKI, biometrics, etc.), or should ITSEC already be coupled with applicable modules such as form and directory services, micro billing, or mail systems? How great is the danger that national or international regulation will threaten the investments in the long term?

Whatever the case may be: ITSEC will be a critical success factor and important trigger for e-government. Administrations will have to bear preliminary investments in certain areas if there is no market for the private sector. How the ITSEC service market will develop in general is difficult to assess and also depends on the penetration of the services in other applications for citizens and the private sector. Certainly, ITSEC components will in the future reach citizens in a very natural way via the administration, such as by way of official digital forms of identification.

Should public administrations bear the risks of the "early ITSEC-technology adaptor"? How is the subsidiarity of the administration affected ITSEC become a business case for the private sector?

In other respects, the private sector and public administrations will deal with roughly the same security technolo-gies in the next years. The present article will not emphasize this topic any further. According to GartnerGroup©, it is worth noting that the hype cycles are shorter in the ITSEC field than with respect to other information technologies. This is due to the fact that ITSEC product developments generally arise as a consequence of an urgently needed solution to a specific security problem. For this reason, it is also relatively difficult to make serious forecasts.

ITSEC and New Public Management (NPM)

The goal of NPM is to achieve a more efficient administration by introducing some kind of new governmental-culture. Important part of this culture is intensified process-and service-orientation, controlling, quality management, project- and portfolio management, asset management, standardization etc. ITSEC will profit there from when it becomes an integral part of all these disciplines and service procurers are responsible for the management of their ITSEC requirements.

NPM becomes dangerous if ITSEC is seen just as an isolated cost-driver and not as an added value and remains therefore forgotten at the interface between service-procurer and - provider. Because many public administrations are still strongly input-driven, this risk remains rather big.

Use of IT for purposes of public security

Increasingly, not only the topic of "security for IT" will be a concern, but also "IT for national security". In the administrative field, three information technologies in particular are emerging as especially significant for the coming years:

- Identity management technologies, because government organizations worldwide share a common need to identify and register their citizens in a reliable manner;
- Geographic information systems, to visualize and analyze geographic fact patterns relevant to security;
- Specialized data management and integration tools for governments charged with criminal justice responsibilities.

Summary

More efficiency through IT as well in public administration processes and national security tasks such as defining crime and terrorist are most likely. In both fields the dependency on IT within the public administration and in the contact with citizen will increase enormously. As a consequence security measures oft the IT processes and systems will evolve to strategic assets of nations: However there will be some domains of mutual collaboration to improve security as well as some domains where strategic advantages through good security will be protected.

The global View of Security Situation in the Internet

The constantly growing importance of the Internet for our information society makes it necessary to analyze and be acquainted with its Security Situation beyond the limits of the individual network operators.

Norbert Pohlmann

Professor in the Computer Science Department for distributed systems and information security and director of the Institute for Internet Security at the University of Applied Sciences Gelsenkirchen, Germany.
Chairman of the board of the TeleTrusT association.
Member of the Permanent Stakeholders' Group of ENISA.
Chairman of the ISSE program committee.

www.internet-sicherheit.de
www.if-is.net

We have all experienced the situation: you are sitting in a traffic jam and all you can see is a long line of cars in front of and behind you. In this situation, without any assistance, you do not have an overview of the problem. There is no direct information concerning why the traffic jam has come about, how long it is, at what point of the traffic jam you are located or - the most important information - when the traffic jam will dissolve. As this is a problem faced on a day-to-day basis by thousands of motorists, solutions have been developed to overcome the lack of information. There is a close network of traffic counter loops which record the traffic volume and situation on the motor-ways/freeways. Important information about traffic jams is provided by means of radio announcements, SMS, telephone and the Internet, while modern navigation systems process the information directly when planning the route to be taken. Through the use of these resources, motorists are "liberated" from their constricted local view of the situation and can take decisions in good time on the basis of the global information available, e.g. leaving by the next exit and using an alternative route.

This situation can also be applied to the perspective that the network operators have of the Internet today. As a rule they have only a local perspective, i.e. an overview of their own network segments and the communication data that is transferred. If problems occur here and are detected, they can be rectified quickly and systematically. However, if it becomes apparent that a problem has occurred that is not within its own domain of action, or if the required perspective is lacking, the situation is more difficult. In most cases we do not know the origin of the problem and we are reliant on third parties to solve the problem.

The global view of security situation in the Internet required in order to detect the problem and to select the appropriate solutions is missing. Such a global view on the Internet is difficult to achieve as people like to play their cards close to their chest. The precise internal network structure, communication connections and topologies are often treated confidentially by the network operators [1].

Furthermore, in order to obtain a global perspective, there are a few challenges that have to be coped: communication data is relevant in principle to data protection, the quantities of data are enormous, the data rates are sometimes so large that they cannot always be analyzed in real time, while long-term storage of the communication data in order to observe long-term developments appears to be impossible. Moreover, the question also arises of who feels responsible for creating a global perspective?

The global view for the right decision.

Nevertheless, the Internet has developed into an omnipresent medium over the past few years, without which very large areas of the economy, research and private life

would be unimaginable today. For this reason the analysis and knowledge of the medium known as the Internet in its totality is of particular significance in order to be able to assess its development and guarantee the future functioning of all the services it provides.

The constantly growing importance of the Internet for our knowledge and information society makes it necessary to analyze and be acquainted with its status beyond the limits of the individual network operators. Only precise knowledge of the normal status makes it possible to detect anomalies which influence the functionality of the Internet.

With the help of the probe-based Internet Analysis System, which is currently being implemented as a research and development project of the Institute for Internet Security at the University of Applied Sciences in Gelsenkirchen in collaboration with the German Federal Office for Information Security (BSI), it is intended to create and analyze local and above all global perspectives in order to make the generation of the global view of the security situation in the Internet possible.

Aims and Task of the Internet Analysis System

The task of the Internet Analysis System on the one hand is to analyze local communication data in defined subnetworks of the Internet, and on the other to create a global perspective of the Internet by bringing together the large number of local perspectives.

The functions of the Internet Analysis System can be divided up into the four subsegments of pattern formation, description of the actual status, alarm signalling and forecasting.

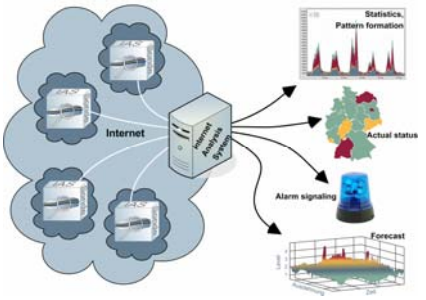


Fig. 1: Tasks of the Internet Analysis System

The main task of pattern formation is a comprehensive analysis and interpretation of the communication parameters of Internet traffic, with the aim of detecting technology trends, interrelationships and patterns which represent the various statuses and perspectives of the Internet. On the basis of this knowledge a search is carried out for anomalies among the current measured values and the causes of status changes analyzed and interpreted. Here it is important to find out whether the status anomalies have a natural origin, for example as a result of a technological change, or whether they are attributable to a wanton attack.

With knowledge of the current status of a communication line and the use of historical - i.e. previously collected - information (knowledge base) it is possible in the case of significant changes to traffic volumes or communication data to generate a warning message, on the basis of which measures can be initiated to protect and maintain the correct functioning of the Internet.

If you can‘t measure it, you can‘t manage it!

A further important function is the visual depiction of the Internet status similar to a weather or traffic jam map. Here intuitive depictions are being developed with which the most important parameters are discernible at first glance.

Fig. 2: Security Situation in the Internet

Through the examination and analysis of the extrapolated profiles, technology trends, interrelationships and patterns it will be possible by means of an evolutionary process of the acquired results to make forecasts of Internet status changes. In this manner it is possible to detect indications of attacks and important changes at an early stage and forecast the effects of the damage.

Principle of Raw Data Collection

Figure 3 shows the principle of raw data collection by the probes. This is divided up into three sections. The Internet is represented on the left. Packets of three different application sessions are shown: related HTTP packets, an FTP session and an SMTP session. The probe is located in the middle of illustration 3. The packets of the three applications are accessed passively by the probe one after the other in their random order and evaluated. The packet that is accessed is channelled through several analysis categories, each of which is responsible for a certain protocol. These evaluate strictly defined communication parameters in the protocol header at the various communication levels which are not relevant to data protection law. The counters allocated in the counting system are incremented according to how the header information of the packet is filled out. The frequency of certain header information is recorded in the same way as on a tally sheet. For simple example, in illustration 3 the

accessing of the FTP packet is recorded by incrementing the FTP-counter by 1. The raw data are therefore aggregates of counters, i.e. counters of communication parameters that have appeared at the various communication levels over a defined period. The packet - in illustration 3 an FTP packet - is immediately deleted physically, i.e. irreversibly and without trace, by the probe [2].

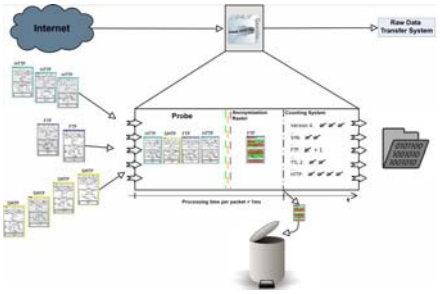


Fig. 3: Principle of raw data collection

Reconstitution of the context of a packet or only a communication parameter is not possible or necessary. At definable intervals the counter readings (raw data) of the probes can be transmitted to the raw data transfer system. All of this information is completely anonymous, as shown in Figure 4.

ID	Description	Count
131134	IP (Protocol Number 6)	: 18.854.151
131145	IP (Protocol Number 17)	: 1.123.149
327708	TCP (Flags: SYN)	: 334.435
327723	TCP (Flags: FIN/ACK)	: 480.697
327724	TCP (Flags: SYN/ACK)	: 275.779
545857	HTTP (Request Method POST)	: 2.026
545861	HTTP (Request Method GET)	: 293.616
545863	HTTP (Request Method HEAD)	: 18.992

Fig. 4: Counting system in the probe

On the right after the colon are the counter readings for the header information specified on the left. Each line stands for a counter. On the left-hand side of the colon is the count-if function (appearance of the corresponding communication parameters) and on the right the number of packets which contained the communication parameter during the defined measurement period. For example, line 2 of the raw data shown indicates that 1,123,149 packets with the IP protocol number 17 (UDP) appeared in the prescribed time.

Some results of the Internet Analysis Systems

For the purposes of illustration some results are presented in this section in order to provide an idea of the possibilities of the current status of the Internet Analysis System. At present there are approximately 800,000 different counters of communication parameters incorporated for the various communication levels. This large number clearly shows how complex the results can be.

Types of E-mail Messages

Illustration 5 shows the ability of the system to record the statistics of the headers of the e-mails sent by SMTP. The distribution can provide information on general communication behaviour, as well as deviations from it.

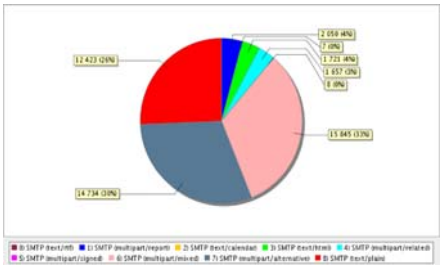


Fig. 5: Distribution of e-mail Content Types

Figure 5 shows an example of normal behaviour in which the total number of messages without attachments represents 60% of all messages. These e-mails include messages with the text/plain, text/html and multipart/alternative content types. As a rule, e-mails with attachments are provided with the multipart/mixed content type. E-mails with the multipart/related content type are considered mixed form. Here, for example, images are integrated directly into the text. If these e-mails are included in the e-mails with an attachment, approximately 36% of all e-mails are sent with an attachment. The remaining 4% essentially consist of confirmations of reading with the multi-part/report content type. An abrupt change to these values in particular may indicate a wave of spam affecting a company from the outside, or indicate that a computer is sending spam from within the company.

All of this statistical information is anonymous.

Transport Protocol Distribution

Figure 6 shows the distribution of the protocols of the transport layer used over a period of several days for a specific communication line.

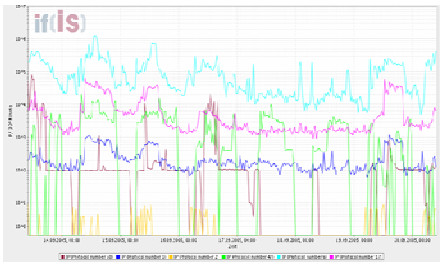


Fig. 6: Protocols of the transport layer

From the past the Internet Analysis System knows the profile, the standard deviation and from this can display an indication of untypical behaviour. Additionally, the use of certain protocols can be determined, enabling capacity planning for the use of Virtual Private Networks (ESP protocol), for example. Protocol dependencies can also be detected: UDP appears to be proportional to TCP, which can be attributed to the dependencies of HTTP and DNS.

More aspects

In the area of research various universities are working on other important issues, like the recognition and analysis of Trojan horses, pattern recognition, detection of anomalies, neural network models for communication parameters, Data-Mining algorithms, and anonymisation.

It has to be analyzed on which spots of the internet the probes need to be placed to make a representative statement [3].

On the sensors level there are more systems, like log-data based systems that have access to router log data, switches, Intrusion-Detection-Systems, firewalls,

web servers and therefore are able to analyze it.

Examples for such systems are the "Symantec DeepSight Threat Management System" and "DShield.org - Distributed Intrusion Detection System".

The driving force behind DShield is the Internet Storm Centre of the SANS Institute in the USA. Anybody who operates a firewall and is willing to contribute his logfiles to the project can participate. The possibility to contribute logfiles completely anonymous, without checking the country of origin and time zone is quite questionable. This raises a considerable doubt on the trustworthiness of data.

Most of the input data comes from the USA. Together with designated experts important alerts can be spoken out by the system.

Other Early-Warning-Systems have an active access to internet services and record the availability data. This enables a quick overview of the availability of important services like DNS, E-Mail, and web servers.

Besides the sensors and interpretation level there are a valuation and categorization level, which can refer recognized irregularities to normal network behaviour or a cyber attack.

The valuation and categorization can hardly be automated.

This is the point where humans have to take decisions, based on their technical knowledge, their expertise and by accessing additional information.

Another very important aspect is the distribution level. Here the addressees of alerts have to be selected carefully. If responsibilities and competence fields aren't defined exactly, the alert may be sent to an addressee, who is not allowed to react, or doesn't have the suitable knowledge to perform the necessary measures.

Perspective

Even if we do not know today if we could recognize the most important attacks, we need to be able to have a global view of the internet.

Similar to the situation of road traffic the results will be implemented to infrastructural security measures (Black List, Router Policies, Identity Management, and so on) and to a higher level of operating system security (Trusted Computing, and so on.), as well as applications (e.g. digital signature).

We have to make ourselves aware that there are new laws to come, which will help to create a more trustworthy internet.

We face a challenging way to establish a working Internet-Early-Warning system.

The cooperation of companies, organizations and governments is important to create a global view of the internet.

We face a challenging way to establish a working Internet Early Warning System.

By that we will be able to detect attacks in time.

Further information

Institute for Internet Security, www.internet-sicherheit.de or www.if-is.net

Federal Office for Information Security (BSI), www.bsi.de/english/index.htm

References

[1] N. Pohlmann, M. Proest: „Internet Early Warning System: The Global View", in "Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2006 Conference", Publisher: S. Paulus, N. Pohlmann, H. Reimer, Vieweg-Verlag, Wiesbaden 2006

[2] N. Pohlmann: "Probe-based Internet Early Warning System", ENISA Quarterly Vol. 3, No. 1, Jan-Mar 2007

[3] S. Dierichs, N. Pohlmann: "Netz-Deutschland", iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 12/2005

[4] N. Pohlmann: "Internetstatistik", Proceedings of CIP Europe 2005, Publisher: B. M. Hämmerli,

.

SCADA Cyber Security, Critical Infrastructures' Achilles Heel?

Critical Infrastructures' control networks are facing security problems that IT networks suffered a decade ago. Their singularity makes impossible to directly deploy traditional IT solutions so an adaptation process has to be undertaken.

Elyoenai Egozcue (left)

Security researcher in S21sec R&D department.
e-mail: eegozcue@s21sec.com

Daniel Chavarri (right

R&D project Manager in S21sec labs
e-mail: dchavarri@s21sec.com

David Barroso

CTO S21sec labs
e-mail: dbarroso@s21sec.com

S21sec labs
http://www.s21sec.com
http://blog.s21sec.com
Address: Parque Empresarial La Muga 7, oficina 1. CP 31160 (Orcoyen) – Navarra, Spain

It is well known that Critical Infrastructures rely heavily on SCADA systems. SCADA networks support real time decisions that prevent, detect and of course, react against any anomalous situation that could damage the integrity of the Critical Asset that they protect. Back in the 90's, these networks were isolated and implemented with ancient protocols without any security features. Nowadays, these systems are connected to the Internet, implements newer technologies (WIFI, WIMAX, Zigbee, ...) and run modern operating systems. But, are we aware of the vulnerabilities and threats that we are facing?

SCADA adoption of new technologies will inevitably lead the market to face up the emerging threats, working at different levels in order to assure the security (confidentiality, integrity, availability) of these critical infrastructures. There will be no big changes in the way we see security nowadays, but an adaptation and, sometimes, the inability to reuse current security practices due to some legacy systems will slow down the process.

Cyber Attacks, a real threat against Critical Infrastructures

During the last years multiple incidents have been identified as related to cyber attacks or to security flaws of one or another type.

Its singularity makes it impossible to directly deploy traditional ITSEC solutions

Just remember the case of the blaster worm which caused the blackout in 2003 in the east coast of the United States of America. This worm exploited a Remote Procedure Call (RPC) flaw to infect unpatched Windows 2000 and Windows XP systems.

At the beginning of this year, it was announced that systems which control dams, oil refineries, railroads and nuclear power plants have a vulnerability that could be used to cause a denial of service or a system takeover

It is clear that security incidents are already happening in SCADA systems and therefore security needs to be seriously implemented in SCADA Systems.

The EC has already pointed out the fact that a cyber attack against Critical Infrastructures is a possibility that has to be managed. The Communication entitled "Critical Infrastructure Protection in the Fight against Terrorism," and the Green Paper on a European Programme for Critical Infrastructure Protection provides an indicative list of critical infrastructure sectors and services which includes SCADA systems.

Outside Europe, in early 2006, the US Department of Homeland Security (DHS) performed a "Cyber Storm" exercise which involved the simulation of a cyber attack that included elements of a SCADA protocol attack that spread throughout the critical infrastructure. The results found that we are not yet-prepared to take on a serious cyber attack. From obscured isolated

pure control to opened hybrid IT-SCADA systems.

SCADA systems and more generally Control networks, share a common architecture. Main parts of these systems are Programmable Power Controllers (PLCs) and Remote Terminal Units (RTUs) which are responsible of directly controlling process based on set points established by a higher level controller system (e.g. HMI). To directly control a process means reading values from sensors and applying working points for the actuators related to the controlled process. A Human-Machine Interface (HMI) allows human operators to monitor the state of a process under control and modify control settings by sending set points to the PCLs and RTUs. Moreover, Remote Diagnostics and Maintenance utilities are used to prevent, identify and recover from abnormal operation and failures. Finally, a set of proprietary protocols (Modbus,

Profibus, DNP3 on the field level and an ICCP or OPC on a higher level – e.g. management) provide the architecture for the aforementioned devices to intercommunicate.

Nowadays, vendors are migrating legacy technology to standard software and hardware components in order to reduce costs. This migration means that it is very common to find a Windows based system running not only on a central server but also on a RTU. Meanwhile, these isolated control networks have increasingly been connected to corporate networks without proper isolation in order to provide ubiquitous network supervision capability. Moreover, it is quite often that, for support purposes, those systems have remote access through a reduced secured VPN connection. Also, technicians might use their laptops to connect to SCADA element just after having browsed the Internet using the corporate network or any insecure network (home, airport, …) and spread some worms in the control network.

This tendency to openness and standardisation has helped attackers to break into these systems through the Internet taking advantage of a mis-configuration in an authentication server, wardriving when locating an insecure Wi-FI connection, or any other method.

Facing technical Problems when applying Traditional Security Measures

Simultaneously to this technological evolution, security measures have been undertaken. These measures are mainly related to perimeter security: firewalls, intrusion detection systems, authentication servers, network segmentation, etc. Actually, a security company specialized in SCADA, already provides SCADA signatures which have been included into famous IDS as Snort or the Cisco family ones.

Since initially SCADAs were isolated systems, security was not considered vital or even was not addressed at all.

Initially SCADAs were isolated systems, and security was not considered vital or even not addressed at all. Again, it is very common to find traffic in clear text, no data encryption, no authentication or no accounting information.

It is naive to think that nowadays these issues should have been solved. There are technical issues that have to be addressed first. One of the key differences between SCADA and traditional IT systems is the real-time character of the first ones. Installing an Anti Virus (AV) program or implementing cryptographic capabilities in PLCs or RTUs require from these devices high computational power. This might lead to a degradation of system performance resulting in an out of time reaction to a certain event. This can be tolerated on a personal computer (PC) but not on a control network responsible for the power supply of a whole country.

Since availability is of major importance for critical infrastructures, patching can not be deployed as fast as in the IT world. Testing cycles of patches oriented to control software last longer.

On the other hand, pen-testing is of major importance in regular security auditing processes. It provides answers to “what would happen if ...” but can not be accomplished in SCADA networks since it may lead to a denial of service (DoS) when applied to legacy devices. Software running on these devices sometimes has been developed under the assumption that traffic coming from the network adjusts to the standard. This makes them prone to buffer overflows and other similar flaws.

The above mentioned facts illustrate the reasons why security in the SCADA world has only been tackled from a perimeter prism, and generate a wide range of research topic on this matter.

Deploying Security, an easy Task?

Currently available security measures for SCADA systems are limited to secure the network perimeter and to define security policies and test emergency plans, but implementing security measures into the SCADA world is challenging since there are issues in different topics like security policies or the scarcity of test beds etc.

Regarding security policies, it is a common practice the inexistence of backups or not having tested the recovery plans.

Test beds emulating real systems are very rare due to the high cost of SCADA systems. This fact complicates

testing solutions before deploying them into the real world.

Sometimes, documentation regarding physical and logical topology of the control network does not exactly match. Often Documentation is insufficient. This fact does not help when designing network segmentation or a firewall deployment plan.

SCADA vendors usually provide information about software and hardware configuration that have implemented their main customers in order to promote their solutions. An attacker may use this information to obtain valuable information to perpetrate an attack to one of these customers.

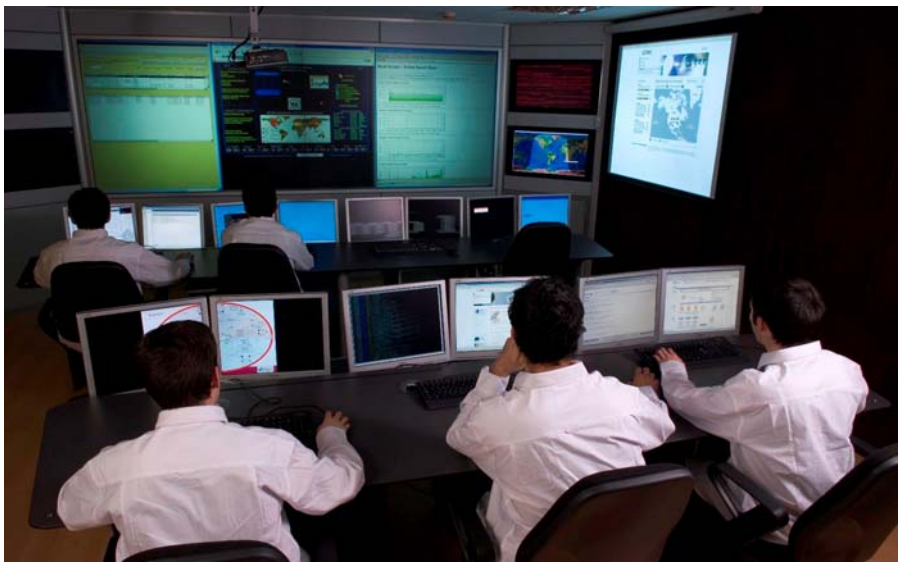
The above issues in combination with technical security limitations derived from the SCADA systems inherent nature shows a threatening scenario.

Beyond Perimeter Security: New Security Trends for Control Systems.

In order to improve cyber security on the current hybrid IT-SCADA systems, new research lines have to be investigated. The singularities of real-time control networks will be of major importance on this process.

One of the main research lines will be to improve risk assessment methodologies: there are threats related to legacy systems, and others that involve opening systems to the new technologies that we need to take into account. In 2007, it is hard to spot a critical communication sent in clear text, or without any authentication. Those are examples of the risks we thought would never appear again.

On this direction, new cryptographic techniques will have to be investigated. For instance, the use of elliptic curve cryptography requires less computational resources. This makes it a perfect candidate to implement authentication, traffic encryption and to guarantee data integrity.



S21sec's Security Operations Centre

On the other hand, vulnerability scanners will have to be adapted to the SCADA world in order to guarantee vulnerability identification avoiding accidental DoS of the assets being scanned. To this aim, specific control network test beds will have to be available at a low cost – virtualisation can be a good choice. Vendors will have to accomplish an in-depth update of current security software to be able to detect and patch security flaws. Moreover, in future SCADA protocols should be standardized to facilitate interoperability and minimize security bugs (avoiding the security by obscurity method).

Log analysis and event correlation tools are currently heavily used in the IT world and can be an interesting research topic. They may help to provide an alternative way for improving security and to control de entire systems and networks health.

Since security is not only about prevention but also about mitigating incidents impact, response procedures need to be improved. Interdependency analysis (cascading effect) based on ontology tools can be a good choice on this field.

Forensic tools adaptment and/or development will also be a hot research topic due to the increasing number of security incidents.

Finally, SCADA security user awareness will have to be addressed: there is a misleading opinion that SCADA systems cannot be compromised or attacked (as for instance, an AS/400). There should be specific education sessions to raise user awareness.

SERKET: CEP Adapters for securing public events and spaces.

SERKET is tackling the issue of security for public areas and events by developing an innovative software approach whereby dispersed data coming from discrete devices are automatically correlated and analyzed to provide security personnel with the right information at the right time.

Antonio Skarmeta

Associate Professor at University of Murcia
skarmeta@dif.um.es

Mercedes Valdés

Assistant Professor at University of Murcia
mvaldes@dif.um.es

Aljosa Pasic

Head of Area at Atos Origin Research and Innovation.
Aljosa.Pasic@atosorigin.com

Rafael Llarena

Software Engineer at Atos Origin Research & Innovation
rafael.llarena@atosorigin.com

Security in public areas (such as airports or train stations) and events (bug sport events, concerts) has stepped into the spotlight due to recent tragically events (September 11th or March 11th).

Despite the vast amount of technology employed, the security of public places and events remains inadequate. The evaluation of available technologies shows that the bottleneck of security does not centre upon the surveillance hardware, but rather on the real-time analysis and correlation of data provided by the various sensors. The project SERKET is tackling the issue of security for public areas and events by developing an innovative software approach whereby dispersed data coming from discrete devices are automatically correlated and analyzed to provide security personnel with the right information at the right time.

Bottleneck of security is not on the surveillance hardware, but rather on the real-time analysis and correlation of data.

This article describes the software component CEP (Complex event processing) adapter developed by Atos Origin and University of Murcia which is responsible of making a preliminary filter to keep just relevant subset of events. The main objective of CEP is delivering less traffic of information to the surveillance middleware and to increase the overall speed of processing.

SERKET's main objective is the development of a software system to provided support to the security personnel, avoiding the problem of the *cognitive overload*. Cognitive overload happens when the working memory can no longer process information in the quantities or at the speed of which it is being presented. In the scope of the SERKET project, we aim to help prevent a typical problem in security systems, in which security personnel has to deal with huge amounts of information coming from different sources (e.g. control room with lots of screens). In traditional security systems, the human being is a crucial factor for the overall performance.

The developed system tries to help humans, by means of the on-line analysis and fusion of complementary as well as redundant information coming from different sources -from sensors to human beings- creating a *global snapshot of the current situation,* raising alarms whenever an undesired situation is recognized. To make it possible, a Complex Event Processing approach is adopted. CEP is an emerging technology comprising the tools and techniques for analysing and controlling the complex series of interrelated events that drive modern distributed information systems. Moreover, the system intends to be open, flexible and scalable at low cost.

CEP Adapter

The developed software module that will deal with the CEP process is the CEP Adapter. It is not a simple CEP Adapter performing just the translation from an event's codification to another. Instead it extends a classical adapter's functionality.

Events in SERKET are supplied by different types of sensors distributed along the target public place. Sensors, in the broadest sense, mean cameras, microphones or even human beings. The CEP adapter provides three functionalities:

- Unified management of heterogeneous sensors whose design favours the incorporation of new types of sensors into the system.
- A *Local Decission Module* (LDM) in charge of an area of interest instead of an only sensor. All the sensors in that area are attached to the same adapter. Instead of supplying basic events to the SERKET system, the LDM performs a local CEP processing of the events occurring in its attached area of interest. In this way, the problem of cognitive overload is faced in the lowest level of the system, what prevents the massive and unnecessary flow of basic events to higher levels of the system.
- Mechanisms to request information from the sensors and to reconfigure their settings in order to tune the definition of interesting events.

This module's design is also related with other interesting technologies such as Service Oriented Architecture, the use of a common OWL ontology and the definition of the XML schemes and protocols needed to register new incoming sensors, communicate the detected events and provide the translation between the required information from sensors and their proprietary management language.

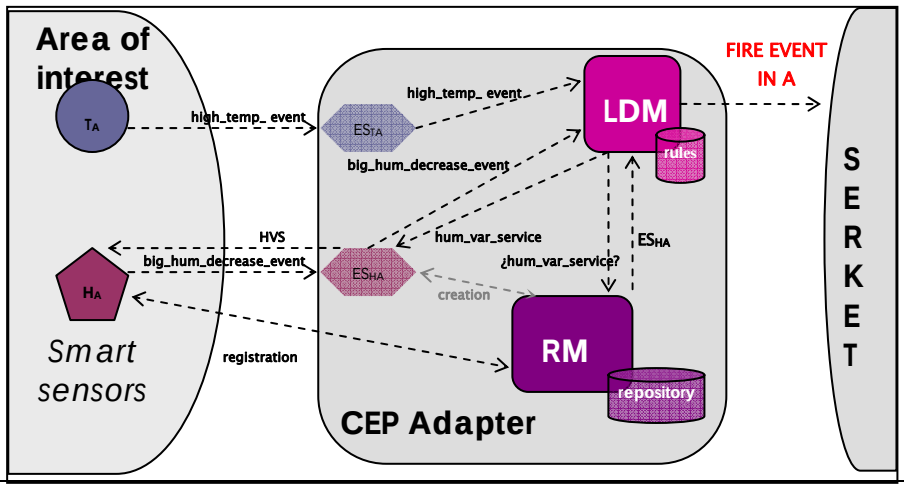
Architecture of the Adapter

The overall architecture of the CEP Adapter is shown in Figure 1, along with a very simple example of how it works. The first step to overcome the problem of cognitive overload is to divide the space under surveillance in several *areas of interests*, each of those areas comprising several smart sensors. The adapter in charge of an area of interests makes all the sensors inside its area invisible to the rest of the system. In the figure you can see the three main entities composing the CEP Adapter modules: a *Registration Module* (RM), a set of *Event Sources* (ES) and the LDM. For this example, we consider a basic ontology containing concepts about humidity and temperature changes as possible signals of a fire.

When a humidity smart sensor H_A located in certain area A is incorporated into the system, it sends a registration request to the CEP Adapter in charge. The request contains information about the *capacities* of the sensor. They are expressed in base of the ontology. The RM performs the registration. As a consequence this information is saved in its local *repository*.

When RM receives a registration request an event source ES_{HA} is created and connected to that sensor. From that moment the sensor will be able to send events to the system through its ES_{HA}. The event sources will be in charge of forwarding the events to the LDM in order to perform its local pre-processing.

Sometimes, the adapter needs to discover what sensors in its area of interest detect certain type of events, according to the rules it was configured with. In the figure, the adapter needs information about the suppliers of humidity change events. The RM answers that ES_{HA} has that capability. Then the adapter requests for the humidity variation to ES_{HA}. Then ES_{HA} translates this petition into a sensor H_A *propietary command*. The response is sent to the adapter. Finally, in this dummy example the adapter rules engine infers that a high temperature and an important decrease of the relative humidity are signals of a fire situation and sends the event just created to the system.



Processing events

The LDM is the entity in charge of asking for the needed information, reacting to the incoming events, sending CEP events to higher level of the systems, and so on. It is loaded at execution time with a set of rules. The rules define the LDM behaviour and they are dependent on the concrete

scenario and the concrete ontology of events. Changing the rules of the LDM changes its reaction to the incoming events. The rules are loaded in execution time, and they can be read from a configuration file in plain text, a database or any other mechanism. The rules are handled by the Esper engine. Esper is a Java engine for processing CEP that enables rapid development of applications that process large volumes of incoming messages or events, filters and analyzes events in various ways, and responds to conditions of interest in real-time. When a new incoming event fulfils certain rule, the LDM performs the tasks written in its right part (querying some information from a smart sensor, requesting some configuration service, or even creating a higher level event to forwarding it to the main CEP processor).

In the case that the defined rules require asking for some more information to the sensors, the LDM can ask for this information proactively. The LDM has to ask the RM for the source of the event it is interested in. Then, it sends the request to the selected event source, which forwards the request to the sensor, after translating it into a proprietary command the sensor can understand. Finally, the sensor will respond with the required events.

Conclusions

The CEP adapter introduced in this article is the first step towards a solution for the *cognitive overload* problem explained above. This adapter filters the events received so not all of them are forwarded to higher levels of the system. Some of them are integrated into more sophisticated ones. One of the main features is flexibility. It has been achieved in different degrees depending of the particular issue:

- New sensors can be added to the system. These sensors must provide its events in the SERKET common event format. New incoming sensors could be incorporated to the system on the fly if they are already known. That is, if a class implementing the interface Event Source for that type of sensor, already exists.
- Regarding communication issues, the adapter has been designed as independent from the communication mechanisms as possible. Proxies isolating this kind of issues have been included in every connection between two submodules of the adapter. In this way, although the current CEP adapter is based on JMS in every connection, it would be very easy to change or include a new communication mechanism (sockets, web services etc.) adding the needed proxies.
- The file or data base containing the rules that leads the LDM behaviour can be (and should be) modified as well as the ontology defining the concepts involved, in order to achieve a more sophisticated processing and to include new situations of interest.

On the other side, a CEP Adapter is in charged of certain area of interest. Sensors inside the area are invisible to the rest of the system. Given that areas of interest could be physically organized into a hierarchy, further works lead us to the design of a hierarchy of CEP adapters as well. In such a way that, lower level adapters provide events to the next level ones. So, lower level CEP Adapters would be considered as sensors supplying events to the next level ones. This building-block approach is a good practice to reduce the system complexity and to avoid unnecessary traffic to the main SERKET CEP processor.

Strategic Management of Security Information through an Entropy-Based Alert Correlator

We present an integrated system to process in real time a huge incoming stream of alerts produced by current intrusion detection systems. A key component of this system includes an unsupervised clustering algorithm that combines a temporal sliding window, entropy tests, and expert rules to track the on-the-fly evolution of alert groups.

G. C. Garriga [1]

HIIT Basic Research Unit
Helsinki University of Technology
gemma.garriga@hut.fi

J. L. Balcázar [2]

LARCA Research Group
Universitat Politècnica de Catalunya
balqui@lsi.upc.edu

J. Ballesteros [3]

TISSAT S.A. Avd. Leonardo Davinci 5, 46980, Paterna, Valencia, Spain
fraballo@gmail.com

J. Megias [4]

GMV S.A. Av. Cortes Valencianas, 39, 46015 Valencia, Spain
jmegias@gmv.com

A. Palomares [5]

TISSAT S.A. Avd. Leonardo Davinci 5, 46980, Paterna, Valencia, Spain
apalomares@tissat.es

Introduction

Managing the security of highly complex networks, composed by thousands of networking systems, is an intensive skill-demanding and time-consuming task. It requires processing, analyzing, correlating and understanding every aspect of the network traffic to successfully detect potentially dangerous events that could pose a threat to any protected systems. Subsystems are thus sought that monitor, through specifically tailored sensors, the main communication events of a system (such as network traffic or user commands that account for human-computer communication events), trying and detecting undesired behaviours. Great advances along this line are described in [1, 3, 6, 7, 8, 9].

Managing the security of highly complex networks is an intensive skill-demanding and time-consuming task.

In fact, the security of this traffic is usually monitored by several security systems, with converging objectives but very different ways to address and identify a potential threat. One common approach is based on a pattern-matching analysis, which raises an alert if a previously known attack, present on the IDS installed rules, is detected. Dozens of new detection rules are added daily for those IDSs, demanding the additional effort for security administrators to update rule sets and tuning them at least weekly. Alternatively, anomaly detection is more capable to detect unknown threats, but very prone to offer lots of false positives.

Therefore, usually the millions of daily alerts detected by those different IDSs are not taken into account by the security managers of those networks, leaving IDS's as a forensics-only tool, useful to understand what happened once a successful attack has compromised one or several systems. Actually, in every attempt so far at using the alerts online for preventive system protection, a major intervention of a human guard is still necessary. The reason lies in that, towards detection of *alarming* behaviour, in most cases we have to be content with detecting *unusual* behaviour; and these notions do not coincide. Thus, a relevant line of research aims at reducing, down to manageable rates, the amounts of information to take care of by humans: First, by organizing all the information, storing information about vulnerabilities as they become exposed by attacks, and tracking their evolution and fix history, so that attacks to a vulnerability already corrected do not distract from more urgent matters; our main aim is the construction of such a system. Second, allowing for simultaneously caring for several alerts at once and organizing them into priority layers; this is where we wish our system to contribute to advancing the state of the art. Inferring that alarms are symptoms of the same malicious behaviour (their so-called **root cause**), may be a way out towards better systems [2, 4, 5, 10, 11]. This needs as much domain information as possible, for instance through ontology-based knowledge. Elicitation of the

necessary knowledge, however, remains often the bottleneck. We explore here a different path: we use a very simple and fast timestamp- and IP-based correlation notion that tends to construct large clusters, thus incurring in the risk of mixing several malicious breaches into a single intrusion alarm, but with the advantage of a reduced human inspection load; and we try to make up for the inconvenience by an entropy-based permanent monitorisation of the clusters themselves, splitting them whenever the system finds it likely that several root causes are being mixed into a single set of correlated alerts. The approach is subjected to a preliminary evaluation using the daily data produced by the different IDS's installed in the network system of Valencia's local government, Generalitat Valenciana.

Background

Generalitat Valenciana (www.gva.es) is the local government of Comunidad Valenciana, the third Spanish most developed region. Being one of the Spanish regions most devoted to providing quality e-government services to its citizens, it has a much evolved security consciousness. Besides, their global network provides many relevant horizontal services (both inbound and outbound) that need a state-of-the-art security, like government's Internet communications, citizen's access to e-government processes, public web services, intranet communications, partner and provider collaboration etc. The security of some of these networks is managed by Tissat, a Spanish IT services company that applies R&D to address and solve day to day problems.

It is therefore important to understand that the project had two complementary focuses: First, to enhance Generalitat Valenciana's threat detection capabilities, and hence to be able to protect more thoughtfully its information, and second, to rationalize and ease the work of their security experts, using its expensive skills to do high level work, to understand long-term patterns on security evolution and to be able to promptly respond to any dangerous threat. One of the most important features desired was the capability of grouping similar threat events detected by any IDS/IPS, issue not fully addressed on any commercial or open source tools (it is required that the user to manually configure the rules to correlate and group similar events, causing to share the root problem with IDS/IPS systems: the need of fine tuning the system constantly).

System description

The Security Information Management System used to manage Generalitat Valenciana's common networks has been crafted to be highly modular, with several different evolving services:

- *Vulnerability Management*: Its goal is to automate the management of the vulnerabilities lifecycle, which is composed of the phases of discovery, asset prioritisation, analysis, remediation and verification. At later stages this information will be correlated with threat alerts, therefore making the system able to tell which attacks actually landed on a system vulnerable to them. The base tool to manage vulnerabilities is the formerly open-source system Nessus (www.nessus.org).

- *Threat Management*: Its main aim is to offer an almost-real time console that allows the Security Operations Centre team to view only relevant security events (they are really clusters of alerts) detected by any IDS/IPS, allowing it to react in a timely manner. The base tools used to feed the alert information chosen was SNORT (www.snort.org), an open source IDS with a very actively maintained rule set, used in many kinds of security environments.
- *Malware and Virus Management:* Similar to the Threat Management module, but much more focused on the particular characteristics of Virus, Worms, Trojans and Spyware traffic, providing the ability to detect infection patterns. This system can be fed with any tool that can detect the previously named types of malware, but, in the sake of using open source software, the first one included has been ClamAV (www.clamav.net), an open source virus detection tool.

The underlying system used to support those modules is based on a distributed agent-based environment, with a three tier application that processes the information and offers an interface for users. Those agents control local parsers that import and normalize data (in order to easily add additional tools), opening secure connections to the system's agent-manager module that its responsible for double-checking agent's data, correlating it with the organization's assets inventory and dumping this information to the system's central database. Agents and agent-manager modules are designed to treat millions of events daily.

Data

The data for the system is provided by several IDS's located on different networks, which log millions of events into their local IDS databases. On any network IDS there is a certain set of attributes provided, no matter what tools are used:

- Time of detection: moment when the attack was detected by the systems.
- Source: Where the suspicious event came FROM, always an IP address.
- Target: Where the suspicious event was headed to, always an IP address.
- Event ID: Each tool uses its own proprietary taxonomy and classification.

Time is one of most important attributes for any security correlation attempt, given that it is used to define the relevant time windows. Therefore, it is a must that all IDS's are time-synchronize using NTP (Network Time Protocol). One of the most useful attributes that can characterize an event is the CVE id (Common Vulnerability Exposure, cve.mitre.org): it is a public list of standardized names for vulnerabilities, used both by Vulnerability Assessment Tools (VAS) and IDSs. If this attribute is nonempty, it can provide direct correlation with a specific vulnerability, allowing the system to promptly determine if the attack was successful

(the event CVE id and the vulnerability were the same on the same target). All data logged on into the IDS local database is periodically polled, preprocessing and normalizing information event using a standard event exchange format. This normalization is used to fill in any missed event attributes, to add information about the IDS that sends the event and finally to ease the addition of new IDS technologies: building a parser suffices.

Once the data is preprocessed, it is sent to the system's central database, which consolidates information in order to discard blatantly repeated events. It is only at this point when the adaptive clustering algorithm can be used.

Modelling approach

Formally the traffic of a given network is analyzed by a set of IDSs, namely $\{ids_1, \ldots, ids_n\}$. Attacks against the system manifest themselves as an stream of alerts produced by each IDS, S_i. Each S_i generated by ids_i is an infinite sequence of pairs (a, t), where *a* is an alert and *t* is the occurrence time of such alert, namely the timestamp. Without loss of generality and to simplify the discussion, we consider that all the streams produced by the different IDSs in a network can be collapsed into one single stream of alerts (possibly overlapping in time) $S=\langle\ldots(a,t)(a',t')\ldots\rangle$, $t \leq t'$. The properties of each alert in this stream S identify which IDS detected the event. Given the input stream of alerts S, the output of our algorithm is a stream of alert clusters or alert groups. A cluster or group c is a set of alerts that are close enough according to a certain distance function – e.g. the value of such function is over a certain user specified threshold – and they occur also close enough in time – e.g. one alert in the cluster can reach another in the same cluster within a time window width given by the user. More details about these factors will be provided in the next subsection. The output stream produced by our algorithm will be of the form $O = \langle\ldots(\{c_i\}, t)(\{c_j\}, t')\ldots\rangle$, where $t < t'$, $\{c_i\}$ is the set of clusters of alerts active at time t, and likewise $\{c_j\}$ and time t'.

Essentially, every time we will read a new alert (a, t) from S (or equivalently, the set of alerts with the same time stamp t in S) the current state ($\{c_i\}$, t) will be updated. This updating corresponds to either adding to one cluster in the set $\{c_i\}$ the new information given by a, or creating a new cluster with the single alert a if none of the existing clusters is "close" enough; then, possibly, some clusters will become inactive because they have not been updated with any alert in the recent last time stamps. Moreover, it might happen that some clusters will exhibit entropy high enough to be split in several sub-clusters.

Technical details

The following are important technical elements to consider:

Vulnerabilities of the system – The network is commonly scanned in the search of vulnerabilities. Names of vulnerabilities come standardized in a CVE identifier. Unfortunately, running a vulnerability scan is not possible at all times as it consumes network bandwidth and it is usually very costly. Also, the scope of these scans is limited.
Alert – An alert corresponds to an event generated by an IDS to notify a potential breach in the system.
Window – A window sliding over the input stream of alerts will define the notion temporal closeness between events. Formally, at a time t a window of width w is defined as the interval [t − w, t], so that at the current state $O = \langle\ldots(\{c_i\}, t)\ldots\rangle$, the set of clusters $\{c_i\}$ is active, meaning that each cluster contains at least one alert that occurred within the current window. On the other hand, a cluster will get outdated, and thus it will be ready to become inactive and "leave the window", when it has not been updated with any alert within the defined window interval.
Cluster of alerts – This corresponds to a set of alerts which share certain similarity. The centroid of a cluster is updated every time a new alert a is added to the cluster: the centroid will be updated with the most similar field/s shared with the new alert a.

Similarity function for alerts – A similarity function *f* for alerts is necessary to construct clusters. The similarity of an alert a read from S w.r.t. an active cluster c with alert centroid a will be defined by *f*(a,a') in [0..1]. If *f*(a,a') is over a user specified threshold then the alert a will be added to the cluster.

The similarity function is specified for this application according to the expert rules. Similar alerts must occur close enough in time; this will be checked through the window condition: the window width is provided by the user. A second set of criteria analyzes in which cases two sources might be considered similar, and two targets might be considered similar. To compare IP addresses we use cosine similarity:

$$\cos(IP, IP') = \frac{IP \cdot IP'}{\|IP\|_2 \|IP'\|_2}$$

where $IP \cdot IP'$ denotes the dot-product of the two vectors. If two IP addresses are identical then the cosine similarity will be 1. To compare two port numbers we simply perform a ratio between them.
It is necessary to establish priorities when comparing fields between alerts: source port is less important than target port, which is less important than the target IP, which at the same time is less important than the similarity of the source IP. Also, in case two alerts share exactly the same CVE id (if it exists) then similarity should be always 1. The combination of these values is not trivial and decisions have to be taken, e.g. similarity of 1 in IP source would indicate that those two alerts are indeed very similar and represent an intrusion together, but on the other hand, if any of the fields obtains similarity 1, then it is worth trusting in the highest similarity of the four fields. We combine all these rules of experts into a similarity function *f* which is symmetric.

Entropy – In real world conditions or for certain user-specified parameters, clusters might become disperse, i.e. not showing any coherence in the alerts contained in the cluster. For example, if the similarity threshold is not high enough, then many alerts will would grouped together even if they are not really similar; or, if the specified window width is too wide, then clusters may become active during too prolonged periods of time thus favouring the addition of new alerts that increase the disorder; or also, if the expert rules are not sufficient then clusters might not be too concentrated. In such situations, it is useful to split the cluster into a subset of other clusters that exhibit less disorder and less number of alerts.

The Shannon entropy measure (typically used in information theory) will be used here to evaluate the level of disorder that there is in a cluster. Given a cluster c, the entropy will be computed over the set of source IP addresses of the alerts in the cluster, and also over the set of target IP addresses of the alerts in the cluster. Eventually we will assign the maximum of those two values to designate the entropy of the cluster, i.e.:

$$H(c) = \max\{H(IP_{source}), H(IP_{target})\},$$

where

$$H(IP_{source}) = \sum_i -p_i \log_2 p_i ,$$

with index i ranging through the different source IP addresses and p_i being the probability of the address IP_i in the cluster c, computed simply as the ratio of occurrences in the cluster. An entropy score over a user-specified threshold for a cluster c shows the need of splitting the cluster c into as many sub-clusters as different IP addresses (either source or target, depending on the one contributing to H(c) with the maximal entropy).

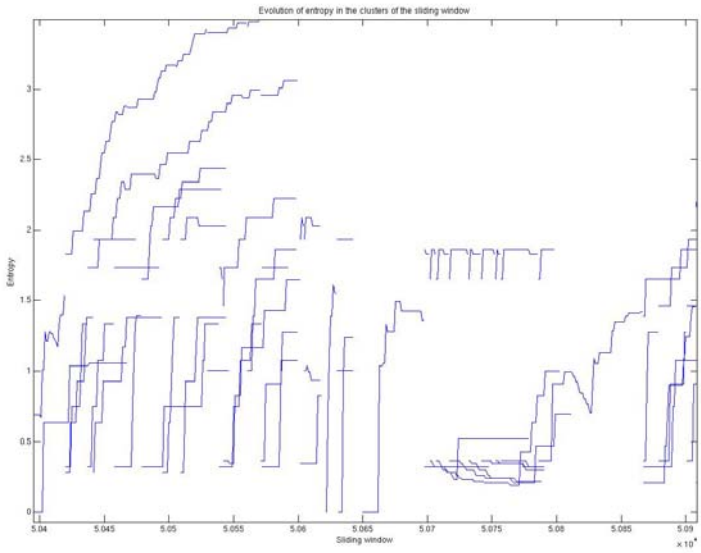


Figure 1: Snapshot of the entropy evolution of active clusters: x-axis represents the time evolution and y-axis is entropy. Each continuous blue line represents the entropy evolution of an active cluster within this time interval snapshot. The minimum entropy threshold was set to 3.5 in this experiment, so when a cluster reaches this limit, then the entropy value immediately drops (meaning that the cluster is split into several others with less entropy). Also note that for some clusters the entropy might decrease at some point of the evolution. This is because the cluster is getting more compact, instead of getting more disordered

Preliminary empirical evaluation

In this section we present a preliminary empirical evaluation of the entropy based alert correlation approach. We will test our approach on the alerts generated during the day 12/27/2006 in the networking system of Generalitat Valenciana. This corresponds to 75,821 alerts, roughly 6Mb of data. Distance between alerts is measured here in seconds. The methodology of these first experiments consists in varying the three input parameters: window width, similarity threshold and entropy threshold. A snapshot of the entropy evolution for the active clusters is depicted in Figure 1.

In next Figures 2 and 3: The first plot is the number of active clusters at time t (y-axis) versus time t (x-axis). The second plot is the total number of alerts in the active clusters at time t (y-axis) versus time t (x-axis). The third plot is the average number of alerts per active cluster at time t (y-axis) versus time (x-axis). The fourth plot is the maximal entropy from all active clusters at time t (x-axis) versus time (y-axis).

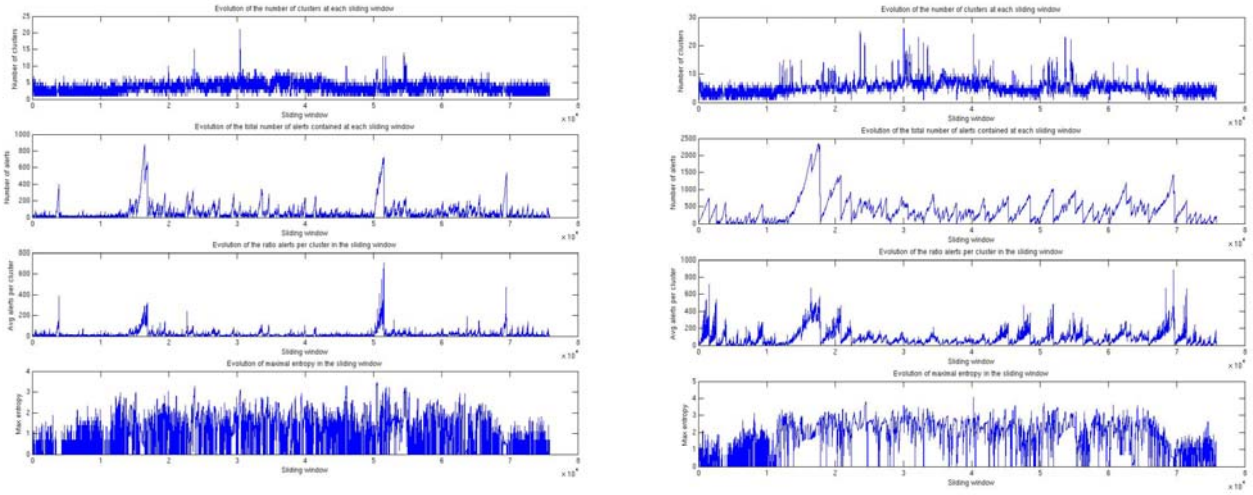


Figure 2: Comparing the state evolution of clusters through time with a tight window width (7 seconds, left) versus a wide window width (20 seconds, right). Rest of parameters: min similarity 1.0 and min entropy threshold 3.0. Observe that with wide window width, the clusters stay active longer thus producing higher accumulations of clusters (peaks of the second plot), and also these are clusters with much more alerts.

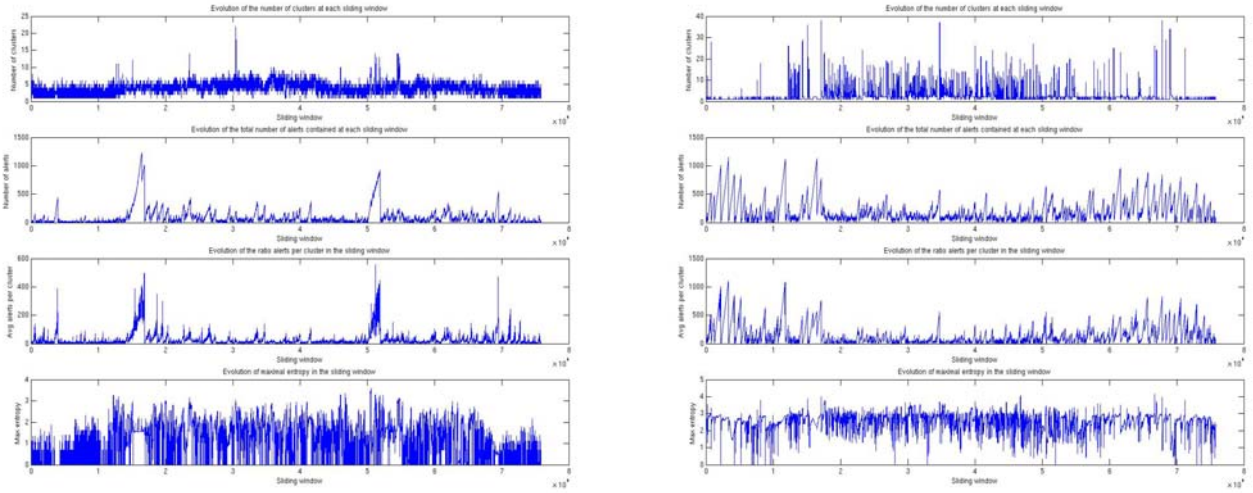


Figure 3: Comparing the state evolution of clusters through time with a strict similarity threshold (1.0, left) versus a loose similarity threshold (0.7, right). Rest of parameters: window width is 9 seconds and minimum entropy threshold is 3.0. Observe that with a loose similarity, the number of alerts in clusters tends to increase. Also the number of clusters per time t is high for similarity 0.7, as alerts updated clusters very easily, and this gives those clusters the chance of being active at least in the next 9 seconds marked by the window width.

CASE STUDY	TYPE	FREQUENT SOURCE PORT	FREQUENT TARGET PORT	CLASS
1	WEB SURFING		80 or 443	AUDIT
2	HTTPD RESPONSE	80 or 443		AUDIT
3	DNS ANY REQUEST		53	AUDIT
4	DNS ANY RESPONSE	53		AUDIT
5	SMTP SENDING		25	AUDIT
6	SSH CONECTION		22	AUDIT
7	TCP PORT SCAN			ATTACK
8	DENIAL OF SERVICE			ATTACK
9	NET SCAN			ATTACK

Table 1: Description of the 9 different types of clusters are classified by the experts during the experiments. For some types of clusters we show as well the frequency source/target port associated to the cluster type. Last column (class) corresponds to the classification of the cluster (either audit or attack) given by the experts.

Discussion

Analysis of the outcome of the experiments described (and of further experiments omitted) reveals some interesting considerations. Regarding the time window, we find a rather strict linearity between its length and the number of false positives and false negatives: as expected, but confirmed with a linear dependency on the data obtained, larger windows improve substantially the quality of the detection rate. Of course, larger windows also imply higher resource consumption, so each particular application will need some tuning effort to find the largest window width acceptable for the installation.

Similarity threshold and entropy threshold are harder nuts to crack. No linear correlation is found, but it can be observed that the optimal results are found in specific intervals: [0.7,1] for similarity (which is not surprising) and [2,3] for the entropy: along these intervals, the best ratios with respect to false positives and false negatives were usually found, but little more can be said. These are useful guidelines to tune this algorithm for an actual SIM system.

In our several real-world simulations on the networking systems of Generalitat Valenciana we found that a window width of 300 seconds, together with a similarity of 0.7 and entropy threshold set to 2, were the parameter values preferred by the security experts. The intuition for enlarging so much the window width is the following: we found that for small window widths some of the clusters were removed from the window too early in the process; yet, these clusters would reappear some seconds later containing a very similar bunch of alerts. Indeed this corresponds to observing very big cluster that can never fit into a too small window and thus, is split into several smaller overlapping clusters as the too small window slides through. The set of different type of clusters we found with these parameters can be seen in Table 1.

Even if these parameters are not easy to optimize, one sees there is a very stable behaviour of the algorithm, with a certain ``continuity'' whereby the outcome of slight changes in the parameter settings is reflected in rather stable output. However, it must be noted that the level of abstraction of the algorithm with respect to the network under surveillance is not high, and this results in a high variability of the results of the algorithm with respect to the network on which it has been implemented. Thus, relatively little changes in the network may easily result in a substantial loss of performance and a need of retuning the system.

Future work

This framework offers several opportunities for improvement, given that the strategy of letting clusters grow and inducing them to split under specific entropy considerations indeed gives very good results as of decreasing the load of information to be handled by the security experts in charge.

First, beyond adjustment of parameters, variations in the very similarity function could be explored, since our decision here for starting this work was a rather simplistic one.

One additional major issue is the possibility of using the information derived along the clustering to rank the priority of the groups of alerts, in that evolution of the corresponding cluster may suggest alerts that require immediate attention in much higher degree than others. Data coming from the vulnerabilities database must be treated also, since, for instance, an attack that clearly targets a vulnerability that has been recently fixed is of much less priority than even mild potential attacks to an existing vulnerability.

Acknowledgements

This work was supported by Spanish Government under the MITYC grant PROFIT FIT-360000-2005-46. The main part of this work was done while the first author worked at the Universitat Politècnica de Catalunya, Barcelona, Spain.

References

1. T. Bass. Intrusion detection systems and multisensor data fusion. Commun. ACM, 43(4):99–105, 2000.

2. F. Cuppens. Managing alerts in a multi-intrusion detection environment. In 17th Annual Computer Security Applications Conference, page 22, 2001.

3. H. Debar, M. Dacier, and A. Wespi. Towards a taxonomy of intrusion detection systems. Comput. Networks, 31(9): 805–822, 1999.

4. H. Debar and A. Wespi. Aggregation and correlation of intrusion-detection alerts. In 4th Int Symp on Recent Advances in Intrusion Detection, pages 85–103, 2001.

5. K. Julisch. Clustering intrusion detection alarms to support root cause analysis. ACM Trans. Inf. Syst. Secur., 6(4):443–471, 2003.

6. T. Lane and C.E. Brodley. Sequence matching and learning in anomaly detection for computer security. In AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management, pages 43–49, 1997.

7. W. Lee and S.J. Stolfo. A framework for constructing features and models for intrusion detection systems. ACM Trans. Inf. Syst. Secur., 3(4):227–261, 2000.

8. W. Lee, S.J. Stolfo, and P.K. Chan. Learning patterns from unix process execution traces for intrusion detection. In AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management, pages 50–56, 1997.

9. W. Lee, S.J. Stolfo, and K. Mok. A data mining framework for building intrusion detection models. In IEEE Symp. on Security and Privacy, pages 120–132, 1999.

10. A. Valdes and K. Skinner. Probabilistic alert correlation. In 4th Int Symp on Recent Advances in Intrusion Detection, pages 54–68, 2001.

11. F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer. A comprehensive approach to intrusion detection alert correlation. IEEE Trans. Dependable Secur. Comput., 1(3):146–169, 2004.

2nd International Workshop on Critical Information Infrastructures Security

For second consecutive year the CRITIS Workshop has been a meeting point for CIIP international experts coming from industry, government and academia. The Workshop has provided an interesting opportunity for presentation and discussion of the main aspects of CIIP research, sharing new ideas and experiences.

Javier Lopez (right)

CRITIS'07 Program Co-Chair

University of Malaga
Computer Science Department
Tel: +34-952131327 or +34-952134186
jlm@lcc.uma.es

Bernhard Hämmerli (left)

CRITIS'07 Program Co-Chair
(affiliation see first page)
bmhaemmerli@acis.ch

The Second International Workshop on Critical Information Infrastructure Security (CRITIS 2007) was held on October 3-5, at Benalmadena-Costa (Malaga) in Spain, in conjunction with ITCIP (Information Technology for Critical Infrastructure Protection). The main objective was to bring together experts from diverse CIIP-related research areas, that is, professionals from private companies, universities and public administrations in order to discuss interesting security issues of Critical Information Infrastructures.

The workshop attracted 80 participants, thus increasing audience in comparison with CRITIS 2006, hold in Greece. From the 75 papers submitted, and after a strict and rigorous reviewing process, only 29 of them were selected for presentation during the event. All these research contributions have demonstrated the great interest of the community for advancing in the topic and solving many of the problems still open in the field.

CRITIS 2007 received submissions from all over the world, resulting on a high-quality program with the participation of four recognized and distinguished invited speakers.

A high-quality scientific program

The workshop had the honour of including in its program four invited talks by distinguished speakers: Jaques Bus (European Commission, INFSO Unit "Security"), Adrian Gheorghe (Old Dominion University, US), Paulo Veríssimo (University of Lisbon, Portugal), and Donald Dudenhoeffer (Idaho National Labs, USA).

A. Gheorge presentation was entitled "*Critical Information and Critical Infrastructures. How do they relate?*". In the talk, Prof. Gheorge pointed out that it was necessary to understand the concept of critical information under critical and complex systems in order to respond quickly to any impact, and to get the system back to its performance capability. This presentation also described the problems (threats and interdependencies) in this type of systems.

The second invited speaker, Prof. Veríssimo presented "*The tangled webs of Critical Information Infrastrutures*". In this talk, he commented the need of achieving resilience in CI, which is exposed to multiples types of threats, and pointing out that it is necessary to research new or better methods to protect such infrastructures.

Then, D. Dudenhoeffer presented *"Critical Infrastructure Interdependency Modelling and Simulation: Current Practices and Challenges"*, where he provided a technical background for research in interdependency modelling, and discussed challenging aspects in this area. The last invited talk, by J. Bus, was entitled *"Emerging Technology Challenges in the Protec-*

tion of Critical Information Infrastructures", where several very interesting aspects about CIIP were presented along with the current plans of European Union for the FP7.

An interactive panel

CRITIS'07 included an extremely interesting panel chaired by Jacques Bus. The title of the panel was *"Resilient Critical Information Infrastructures: a myth or a realistic target?"*, and the audience could enjoy the following panellists: Mike Corcoran (CPNI, UK), Antonio Diu (AIA, Spain), Claudia Eckert (Fraunhofer SIT, Germany), Saifur Rahman (Virginia Tech, USA) and Marc Tritschler (KEMA, UK).

Jacques Bus chaired an interactive and interesting panel, where were debated very current aspects of CIIP.

The main idea of the panel was to discuss aspects about system, organisational and business resilience, as a new paradigm. Also, the latest progress in technologies, policy, software development and researching practices as well as the international contributions and activities were put in place. Attendees to the workshop participated actively in the debate with the panellists and discussed about the motivating ideas under examination.

Research talks

The scientific program was structured into nine sessions, each one dealing with specific issues of CI. For example, the first session was focused on R&D agenda, where U. Bendish et. al gave details from the CI2RCO project, and A. Stefanini et al. exposed ICT vulnerabilities of the power grid.

The second and third sessions focused on communication risk and assurance. S. Wolthusen et al. proposed several algorithms to analyze cyclical interdependencies in CI and a three-dimensional framework to represent the graph-based model with their geospatial interdependencies and interactions in a specific area of interest. Also, K. Watanabe et al. suggested a conceptual framework for information system risk management corresponding to financial sector. W. Kanoun et al. proposed a risk assessment for improving the reaction in intrusion detection systems. F. Baiardi presented a prototype (Vinci) to manage CI through virtual network communities. Y. Murayama et al. described their studies about the sense of security (Ashin) perceived by the society, and finally R. Páez et al. introduced an IDS based on Agents.

The fourth session mainly discussed on code of practice and metrics. It started with D. Cerotti et al., who presented a way of representing the CRUTIAL project domain by means of UML diagrams. H. Dellwing et al. proposed an expert system (CRIPS) to mitigate the danger in emergency situations. G. Braendeland et al. described a way of representing the mutual dependencies by means of CORAS diagrams, and R. Setola et al. exposed a methodology to estimate input-output interoperability model parameters in crisis period.

The main focus of the fifth session was information sharing and exchange, where D. Chan et al. presented an efficient access control for secure XML query processing, and I. Dionysiou et al. proposed a trust management framework for CI.

The sixth session focused on continuity of services and resiliency, and began with G. Kambourakis explaining a method capable of detecting DNS attacks. G. Maciá et al. described a low-rate denial of service attack against application servers (LoRDAS). S. Delamare et al. defined an approach to improve resilience by means of a routing overlay in an autonomous system. Finally, D. Martínez et al. presented a framework capable of defining operational plans to provide dependability and security.

The seventh session focused on SCADA and Embedded Security, where J. Paulo et al. proposed a new method based on Kohonen maps to improve security tests on automation devices. W. Boyer et al. described their security technical metrics for control systems, and finally K. Kawano presented a security architecture based on segmentation.

The next session discussed on threats and attacks modelling, and began with U. Larson et al. describing a general model for attacks manifestation generation. J. García presented a survey on detection techniques to prevent cross-site scripting attacks on web applications. J. Mallios defined an abstract model for describing SPIT attacks. Finally, S.Schmidt exposed a malware detector placement game for intrusion detection.

The final session focussed on information exchange and modelling. J. Sarriegi began with a methodology to develop simulation models for information security management. C. Ferigato presented a platform for information exchange on protection of CI. Finally, the conference concluded with F. Flentge presenting a standardised language for cross-sector information exchange.

Further information

The post-proceedings of CRITIS'07 will be published by Springer in the Lecture Notes in Computer Science series during the first half of 2008. Further information about this and other issued can be found on the website of the event <http://critis07.lcc.uma.es>

ECN-8: Selected Links and Events

Actual Upcoming CIIP Conferences in Europe

- January 15th, 2008: ICT Trust and Security Day: cistrana.org/events/index_security_seminar.htm
- IST events, http://europa.eu.int/information_society/newsroom/cf/newsbytheme.cfm?displayType=calendar&tpa_id=7
- 5th International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment DIMVA of GI SIG SIDAR, July 10-11, 2008 – Paris, France www.dimva2008.org
- 4th International Conference on IT-Incident Management & IT-Forensics www.imf-conference.org
- 3rd International Workshop on Critical Information Infrastructures Security, Call for Paper critis08.dia.uniroma3.it
- INFSO D4 events, http://cordis.europa.eu/ist/trust-security/events.htm

European Projects or Projects with Articles in this Issue

- European Finance Forum: www.europeanfinanceforum.org
- IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems: www.irriis.eu
- Federal Strategy Unit for IT FSUIT http://www.isb.admin.ch/org/index.html?lang=en
- Institute for Internet Security, www.internet-sicherheit.de www.if-is.net
- Federal Office for Information Security (BSI), www.bsi.de/english/index.htm

E-Reports

- Reports to the article "SCADA Cyber Security, Critical Infrastructures' Achilles Heel?" can be requested on: http://www.s21sec.com/default.aspx?HIVEDATA=dW2z6ApW38XBhw8gB2U%2FUt58IVxnzmfIKSajF7JoZk%2Beu3%2Bw2Hl%2B4PAsozAswU%2FwfMmeRMWLI2ioGTTBH78h3%2FeU%2BDISajHmHdZVfBSu%2Fu4%3D
- Links related to the article "Strategic Management of Security Information through an Entropy-Based Alert Correlator":
  www.nessus.org: Vulnerability Management
  www.snort.org: Threat Management
  www.clamav.net Malware and Virus Management
  cve.mitre.org Common Vulnerability Exposure (Naming Convention)

CRITIS'08

3nd International Workshop on Critical Information Infrastructures Security

October 13-15, 2008, Frascati (Rome), Italy

Program Co-Chairs
Roberto Setola, Univ. CAMPUS Bio-Medico, Italy
Stefan Geretshuber, IABG, Germany

General Co-Chairs
Sandro Bologna, ENEA, Italy
Stefanos Gritzalis, University of the Aegean, Greece

Honorary Chair
Salvatore Tucci,
Prime Minister Office,
Università Roma Tor Vergata, AIIC, Italy

Sponsorship Co-Chairs
Marcelo Masera, IPSC, Italy
Stefano Panzieri,
Università di Roma Tre, Italy

Local Organization Chair
Emiliano Casalicchio,
Università di Tor Vergata, Italy

International Program Committee
Fabrizio Baiardi, Italy
Robin Bloomfield, UK
Stefan Brem, Switzerland
Donald D. Dudenhoeffer, US
Myriam Dunn, Switzerland
Claudia Eckert, Germany
Urs Gattiker, Switzerland
Erol Gelenbe, UK
Adrian Gheorghe, US
Eric Goetz, US
John Griffin, US
Nouredine Hadjsaid, France
Bernhard M. Haemmerli, Switzerland
Raija Koivisto, Finland
Rüdiger Klein, Germany
Javier Lopez, Spain
Eric Luiijf, Netherlands
Angelo Marino, European Commission
Simin Nadjm-Tehrani, Sweden
Eiji Okamoto, Japan
Andrew Powell, UK
Kai Rannenberg, Germany
Michel Riguidel, France
William H. Sanders, US
Sujeet Shenoi, US
Giovanni Ulivi, Italy
Paulo Veríssimo, Portugal
Stephen D. Wolthusen, UK
Stefan Wrobel, Germany
Jianying Zhou, Singapore

Organization Committee
Susanna Del Bufalo, Italy
Stefano De Porcellinis, Italy
Annamaria Fagioli, Italy
Emanuele Galli, Italy
Bernardo Palazzi, Italy
Federica Pascucci, Italy

In the last years we observed dramatic changes in technological infrastructures that found the base of developed countries. For a lot of economical, social, technological and political reasons that are generally referred to as globalisation and liberalisation, they become more and more interoperable, integrated and interdependent. These phenomena and the actual socio-political instability, pose new and very hard challenges for the management and protection of these systems and, more specifically, imposes the development of innovative strategies to guarantee their service continuity. The abundance of services of modern infrastructures is no more thinkable without ICT that therefore has become a key-resource. At the same time ICT is considered as one of the most vulnerable elements of the whole system.
CRITIS'08 wants to bring together experts from science, industry and public authorities involved in management, supervision and protection of critical infrastructures to provide an interdisciplinary and multi-faceted view about third millennium security strategies for Critical Information Infrastructures.
Authors are solicited to contribute to the workshop by submitting articles that illustrate research results, R&D projects, surveying works and industrial experiences that describe significant advances in the following (non-exclusive) areas of Critical Information Infrastructures

- Modelling and Simulation of Critical Infrastructures
- Interdependency Modelling and Analysis
- Network and Organizational Vulnerability Analysis
- Threats and Attack Modelling
- SCADA/DCS and Control System Security
- Self-healing, Self-protection, Self-management Architectures
- Situation Awareness and Response Optimisation
- CIIP Policy and Cross-Border Issue
- R&D Agenda, Benchmarking and Survey

Instructions for paper submission
All submissions will be subjected to a thorough **blind review** by at least three reviewers. Papers should be up to 12 pages in English, including bibliography and well-marked appendices. As in the case of CRITIS'07, post-proceedings are planned to be published by Springer in the Lecture Notes in Computer Science series. Pre-proceedings will appear at the time of the conference. At least one author of each accepted paper is required to register with the workshop and present the paper.
To submit a paper, select the *Paper Submission* option in the menu and note the following. The submitted paper (in PDF or PostScript format), which should follow the template indicated by Springer, must start with a title, a short abstract, and a list of keywords. However, it should be anonymous with no author names, affiliations, acknowledgements, nor obvious references.
Revised and/or extended versions of outstanding papers from the conference will be published, on the base of their arguments, in a special issue of the *International Journal of Critical Infrastructure Protection (Elsevier)* or in a special issue of the *International Journal of System of Systems Engineering (Inderscience).*

Important dates
Submission of papers: May 15th, 2008
Notification to authors: July 15th, 2008
Camera-ready copies: August 31th, 2008

http://critis08.dia.uniroma3.it

IMF 2008
4th International Conference on
IT-Incident Management & IT-Forensics

September 23 - 25, 2008
Mannheim, Germany

www.imf-conference.org/
mailto:2008@imf-conference.org

Conference of **SIG SIDAR**
of the **German Informatics Society (GI)**.

Call for Papers: see www.imf-conference.org

Information technology has become crucial to almost every part of society. IT infrastructures have become critical in the world-wide economy, the financial sector the health sector, the government's administration, the military, and the educational sector. Although security usually gets involved into the design process of IT systems nowadays, the process of maintaining security in the operation of IT infrastructures, in most cases, still lacks the appropriate attention. The capability to manage and respond to IT security incidents and their forensic analysis are not well established. The quickly rising number of security incidents worldwide makes the implementation of incident management capabilities essential.

The scope of IMF 2008 is broad and includes, but is not limited to the following areas:

IT-Incident Management

- Purposes of IT-Incident Management
- Trends, Processes and Methods of IT-Incident Management
- Formats and Standardization for IT-Incident Management
- Tools for the IT-Incident Management
- Education and Training, IT-Incident Management Awareness
- Determination, Detection and Evaluation of Incidents
- Procedures for Handling Incidents
- Problems and Challenges when establishing CERTs/ CSIRTs
- Sources of Information/ Information Exchange/ Communities
- Dealing with Vulnerabilities (Vulnerability Response)
- Current Threats
- Early Warning Systems
- Organizations (National CERT-Associations, FIRST, TF-CSIRT, TERENA / TI, etc.)

IT-Forensics

- Trends and Challenges in IT-Forensics
- Methods, Processes and Applications for IT-Forensics .(e.g. Networks, Operating Systems, Storage Media, ICT Systems)
- Evidence Protection in IT-Environments
- Standardization of Evidence Protection Processes
- Data Protection and other legal implications for IT-Forensics
- Methods in Investigation
- Legal Relevance of IT-Forensics Investigations
- Tools for IT-Forensics
- IT-Forensics Readiness
-

IMPORTANT DATES

June 1, 2008:	Deadline for Submissions
June 23, 2008:	Notification of acceptance or rejection
July 14, 2008:	Final paper camera ready copy due
September 23-25, 2008:	IMF 2008 Conference

Call for Paper:
Fifth Conference on Detection of Intrusions and Malware & Vulnerability Assessment

July 10-11th, 2008, Paris, France

Conference of SIG SIDAR of the German Informatics Society (GI)

The annual DIMVA conference serves as a premier forum for advancing the state of the art in intrusion detection, malware detection, and vulnerability assessment. Each year DIMVA brings together international experts from academia, industry and government to present and discuss novel research in these areas. DIMVA is organized by the special interest group Security - Intrusion Detection and Response of the German Informatics Society (GI). The conference proceedings will appear in Springer's Lecture Notes in Computer Science (LNCS) series.

DIMVA solicits submission of high-quality, original scientific work. DIMVA's scope includes, but is not restricted to the following areas:

Open Call for Paper (to Feb 4, 08)

Intrusion Detection

Approaches
Implementations
Prevention and response
Result correlation
Evaluation
Potentials and limitations
Operational experiences
Evasion and other attacks
Legal and social aspects

Malware

Techniques
Detection
Prevention and containment
Evaluation
Trends and upcoming risks
Forensics and recovery

Vulnerability Assessment

Vulnerabilities
Vulnerability detection
Vulnerability prevention
Classification and evaluation

DIMVA particularly encourages papers that discuss the integration of intrusion, malware, and vulnerability detection in large-scale operational communication networks. More information see www.Dimva2008.org.

Important Dates

Deadline for paper submission: February 4th, 2008 **(firm deadline)**
Notification of acceptance or rejection: April 8th, 2008
Final paper camera ready copy: April 25th, 2008

Organizing Committee

General Chair: Hervé Debar, France Telecom R&D, France (info@dimva.org)
Program Chair: Diego Zamboni, IBM Zurich Research Lab, Switzerland (pc-chair@dimva.org)
Sponsor Chair: Ludovic Mé, Supélec (sponsor-chair@dimva.org)
Publicity Chair: Tadeusz Pietraszek, Google, Switzerland (publicity-chair@dimva.org)