Paper

The INTERSECTION Framework: Applied Security for Heterogeneous Networks

Adam Flizikowski[a], Mateusz Majewski[b], Maria Hołubowicz[b], Zbigniew Kowalczyk[c], and Simon Pietro Romano[d]

[a]Istitute of Telecomunications, University of Technology and Life Science, Bydgoszcz, Poland
[b] ITTI Ltd., Poznań, Poland
[b]Polska Telefonia Cyfrowa, Warsaw, Poland
[d] Computer Science Department, Universita' di Napoli Federico II, Napoli, Italy

Abstract—Inherent heterogeneity of the networks increases risk factor and new security threats emerge due to the variety of network types and their vulnerabilities. This paper presents an example of applied security framework – the INTERSECTION. By referring to the ISO/IEC security standards and to the FP7 INTERSECTION project results, authors underline that in the processes of managing and planning security, investigating technology and business governance should be at least as important as formalizing the need for decisions on security cooperation between operators. INTERSECTION provides security mechanisms and introduces capability possible only with a management solution that is at a higher level than that of any of the connected systems alone.

Keywords—IDMEF, IDS, IPFIX, security framework.

1. Introduction

Information technology industries as well as telecommunication operators are seeking efficient and comprehensive security solutions. This crucial task not only aims at providing protection against malicious or sometimes inadvertent attacks – it must also address the business requirements for confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of information and services. Still, an information system is as secure as the weakest element of the system. In many cases network security consists of building blocks provided by vendors specializing in a single aspect of security. This is why interoperability should be considered. Basic interoperability could be achieved by deploying standard protocols for data exchange between security components. Intelligence of the system could be further enhanced with implementation of a management component capable of aggregating such information and able to link otherwise unrelated events into a big picture view. Such a system may provide comprehensive and efficient security defense even in the case of zero-day exploits. Furthermore, the heterogeneity of networks should be taken into consideration, as it may add new vulnerabilities or open otherwise independent networks to new threats.

At the same time another perspective of the same situation can be observed – there is a value in having access to additional monitoring data for correlation in a security framework. Turning adverse situation of supporting various and complex connections between networks into an advantage of high level managed security solutions capable of preventing complex attacks from spreading into multiple networks and geographic areas may be especially interesting to telecom service provides. This task is the aim of the European research project INTERSECTION. Additionally the project focuses on developing new anomaly detection algorithms that can be used with the traffic correlation engine to predict the network behavior and prevent malicious users from accessing the network, stealing information or disrupting a service. By detecting zero-day exploits and automated remediation the security level is further improved. This paper is divided into sections organized as follows: Section 2 is a summary of the related work in the field of security frameworks. Section 3 describes the various ISO standards addressing telecommunication security management and intrusion detection framework architecture. Section 4 describes the impact of known network threats (like viruses) on companies network and some information about anomaly detection techniques. Section 5 describes the idea of INTERSECTION and protocols used in framework. Section 6 describes the plausible test scenarios for demonstrating the INTERSECTION capabilities. Section 7 introduces idea of converged security. Section 8 then presents security as a service concept. We conclude in Section 9.

2. Related Work

In order to align the described INTERSECTION framework with current state of the art research authors have reviewed most related papers. The areas covered by analyzed papers span from describing technical solutions for improving security: [1], [2], through business perspective: [3], [4], [5] finally to evaluation criteria. In [3] author describes ten aspects that should be taken into account

when planning information security. It is interesting to note that infrastructure, tools and supporting mechanisms are the last items on the list of important factors to include. According to author, even more important then security mechanisms is the need for corporate governance responsibility (security is a business issue and not technical issue) as well as enforcement of information security compliance and monitoring.

According to the autor, the latter are absolutely essential. Framework for unified network security management is presented in [1]. This paper defines architecture of a unified security management system for security framework for converged networks. The framework is based on the following principles: coordination of heterogeneous detection tools performing vulnerability and multistage attack analysis visualization and delivering strategic responses across network boundaries. The architecture of the security framework consists of 3 layers: scanning, modeling and application. Scanning layer is monitoring traffic data from different types of network; it analyzes the data by using vulnerability information and database in order to provide security assessment. The modeling tier provides a functional representation of weaknesses found on networks in the form of requirements and impact. The application tier provides a view of the security features of the network to help identifying potential threats to an enterprise. It provides analytical and correlation tools which can be visualized to provide administrators with information that allows to take effective decisions against security threats.

Similarly Onwubiko *et al*. in [2] propose integrated security framework. The framework defines four types of components: sensor components that contribute evidence about security related events, analysis components that implement autonomous software agents capable of synthesizing evidence, an abstract "security space" through which components communicate and finally response components that implement countermeasures. Response components can be configured to incorporate human decision-making in protecting networks. The logical components of the framework are realized on physical network nodes. A physical network node may realize one or more logical components and may interact with one or more security spaces. The above framework follows the generic model for intrusion detection presented in [6].

Hunter in [4] presents the Tivoli case to create an integrated framework approach and the problems found when the company had to interoperate with other management products not embraced by the framework. He underlines that integration is required and that there is a need for standards and protocols that allow different vendors to inter-operate rather than having dedicated integration frameworks. In addition, the idea of autonomic-management is presented, even though the preliminary stage is to identify potential security threats in advance and to alert security managers so that proactive action can be taken. The longer term objective of the Tivoli case is to provide self healing security management and to fix problems automatically.

On the other hand authors in [5] show that although conventional security solutions have been implemented as standalone systems, designed for solving very specific regional problems it is feasible to create integrated security infrastructure with capabilities for dynamic and automatic interaction between heterogeneous security devices. Presented solution combines firewall, intrusion prevention system (IPS), vulnerability scanners and honeypot technologies to assure a security infrastructure. Each component collaborates with the others in order to choose the best action and to launch adequate countermeasures. Exchange of security events between individual security components allows automatic corrective action without user intervention, while keeping the ability to adapt to an evolving environment. Another possibility for improving security level within large organizations is outsourcing.

Author in [7] state that security falls within the area that does not lend itself well to outsourcing because it is too closely tied to the running of the business. Moreover, Gartner suggests that outsourcing security is not appropriate for everyone and has developed decision framework to determine whether in-house or outsourced security is more appropriate [7]. The typical scope of security outsourcing extends to: monitoring security architecture, continuous configuration of security infrastructure, prevention and recovery of incidents. According to the author the major benefit of outsourcing is achieved when the scope of threats is much larger than a company (operator) can provide in its own right. Even if a company has resources to continuously monitor all the events being generated it can only correlate those events happening within its own perimeter.

3. Security Management Standards

The International Organization for Standardization offers suite of standards responsible for providing detailed guidance on the security aspects of the management, operation and use of information system networks, and their interconnections. Security requirements have been gathered in the ISO/IEC series of standards addressing the following areas:

- (ISO/IEC 18028-1) establishes network security requirements and introduce possible control areas and the specific technical areas,
- (ISO/IEC 18028-2) defines a standard security architecture,
- (ISO/IEC 18043) defines the methods for selecting, deployment and operations of intrusion detection system,
- (ISO/IEC 7498-2) the security issues that have to be address within a security system.

Identification and analysis of the communication related factors that should be taken into account to establish network security are the scope of the ISO/IEC 18028-1 stan-

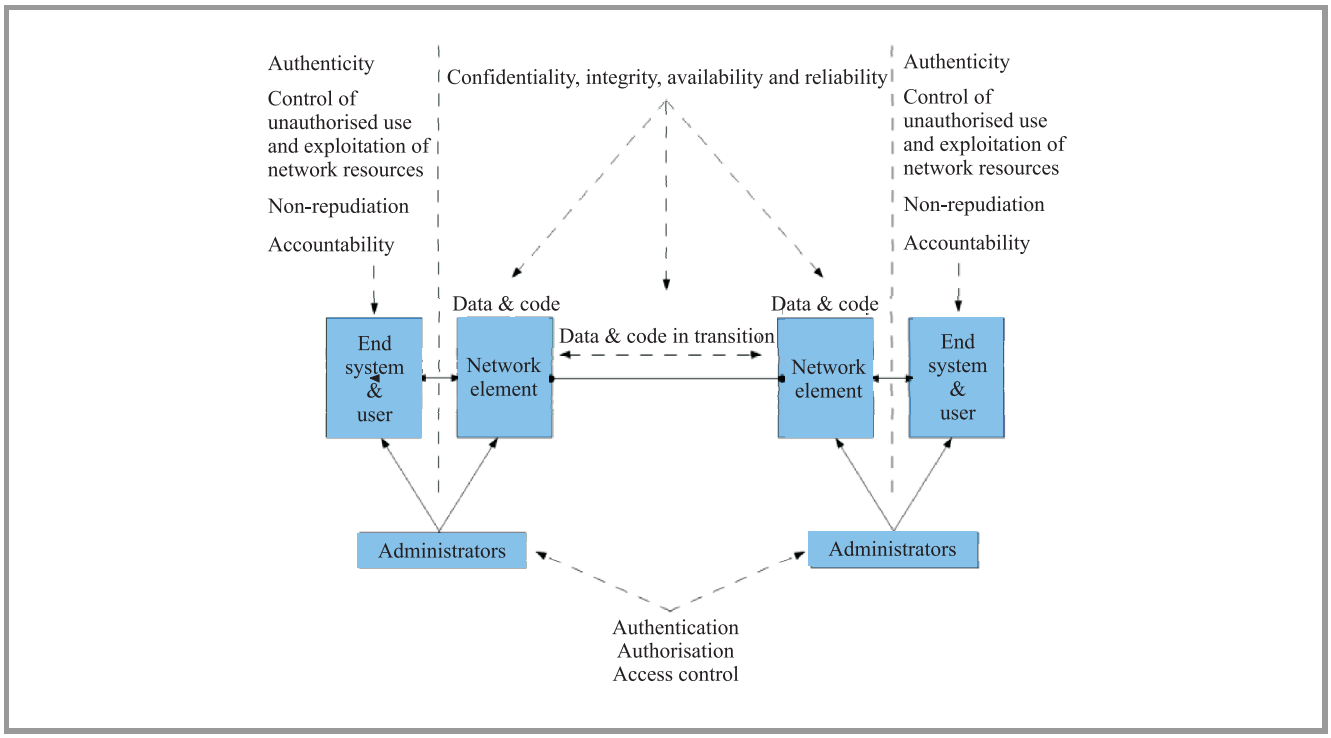


Fig. 1. Conceptual model of network security risk areas [8].

dard. These factors and the corresponding areas of risk are depicted in the Fig. 1.

The results of security risks assessment of a network connection depend on the type and number of networks communicating (e.g., WAN, WLAN, broadband, radio). Selected key risk factors for each type of network are shown in Table 1. When referring to Table 1 one should distinguish between threats and key risk factors. WLAN will certainly be vulnerable to DoS attacks but the impact of such is more severe in WAN or broadband. The same applies for wireless networks. Although radio networks share the same primary security risk with WLAN, there are more prone to disruption due to the possibilities of jamming the system and affecting a considerably greater number of users. Columns in the Table 1 represents the key risks related to particular network whereas speaking about connection that uses for instance WLAN and WAN one should intersect risk factors from both networks. Each risk factor represents certain threat to the system.

Table 1
Key risk factors according to connection type [8]

Risk	WAN	WLAN	Radio	Broadband
Intrusion	+			
DoS	+		+	+
Eavesdropping		+	+	
Unauthorized access		+		
Misconfiguration		+		+
Flawed WEP or TKIP		+		
Session hijacking			+	
Propagation of malicious code				+
UL/DL of unauthorized access				+

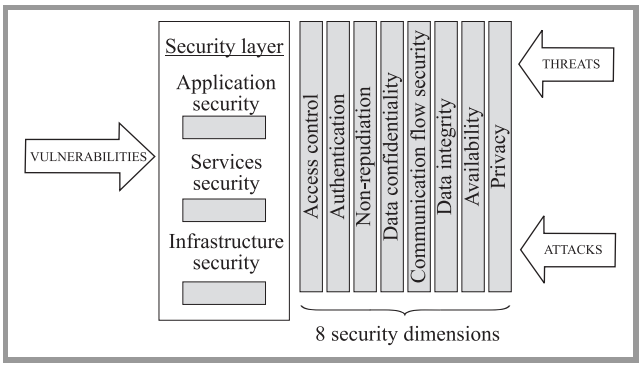


Fig. 2. Security conceptual architecture [10].

According to the ISO 7498-2:1989 specification [9] various threats may be grouped and categorized as follows:

– destruction of information and/or resources (I),

– corruption or modification of information (II),

– theft, removal of loss of information and other resources (III),

– disclosure of information (IV),

– interruption of services (V).

Particular threats should be addressed by defining a set of principles that describe a security structure for the end-to-end security solution. According to ISO/IEC 18028-2 the most generic security framework aimed at combating broad range of threats can rely on the eight-dimensional model as presented in Fig. 2. The figure depicts the concept of protecting a network by defining security dimensions at each security plane of each security layer to provide comprehensive security solutions. Thus according to [10], to be resilient, an end-to-end security solution must address the spectrum of depictured areas and dimensions. Protection elements have to be placed throughout the network to protect the company from malicious attacks. The target coverage of threats by the well established security dimensions in an organization is presented in Table 2.

Table 2
Threats and security dimension relation [10]

Security dimension	Security threat				
	I	II	III	IV	V
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data confidentiality			Y(*)	Y(*)	
Comm. flow security			Y	Y	
Data integrity	Y(*)	Y(*)			
Avaliability	Y(*)				Y(*)
Privacy				Y	
(*) feasible with IDS.					

Network security is achieved by addressing a specific group of threats (column name refers to the numbering in the threat list above) with a security component or system that provides functionalities described by given dimension (row). When mitigating particular risk with the proper countermeasure a certain level of security is achieved – which can further be extended by applying more mature solutions and robust security components. A practical way to enhance the security level is to introduce an intrusion detection system (IDS) in the network. IDS will, by definition, cover certain threats in the context of eight-dimensional security model (Table 2). According to [11] generic IDS should address the authentication, integrity, confidentiality and availability dimensions as indicated by Table 2. It is worth noticing that by addressing only four out of eight security dimensions IDS can cover a complete spectrum of security threats. A generic model for IDS defined by [11] is presented in Fig. 3.

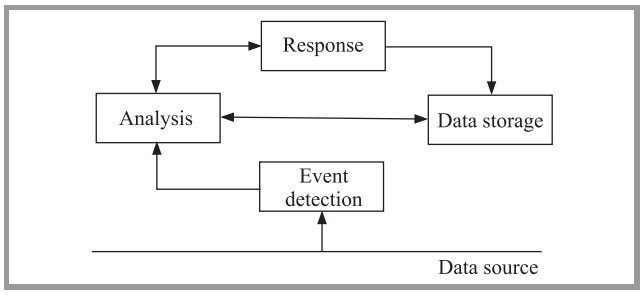


Fig. 3. Generic model of intrusion detection [6].

The event detection module will gather data scattered around the network; this will include information about interfaces, traffic, active users and system logs. Data correlation will take place inside the analysis block, where patterns of properly functioning network will be defined. All data is stored in a data storage module. If an IDS works in anomaly detection mode the system can compute the traffic profiles for normal behavior and compare it to ongoing traffic to determine possibility of an attack. Once the attack is detected the IDS can in turn scan set of available countermeasures and with a presence of a response module – reconfigure the network devices or interfaces to slow down the attack, thus providing enough time for the system administrator to trace the intrusion source. A secure network may contain single IDS as well as multiple IDSes spread through the network. Hierarchical architecture is proposed in [11] for multiple IDS management as shown in the Fig. 4.

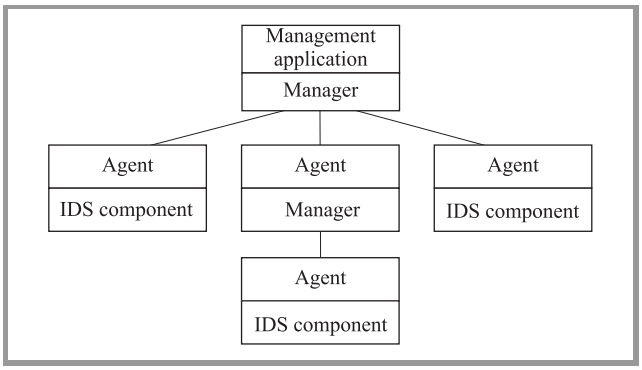


Fig. 4. An intrusion detection management model [6].

The more data is gathered from agents for analysis the more reliable decision can be made by manager and an ongoing attack may be detected in less time. Thus according to [6] it could be beneficial for operators to share data on intrusion information and interconnect their IDS. The ISO/IEC 18043 advises such solution but also points out that operators are not willing to give their knowledge of intrusions that have affected their IT systems to the public, as it could reveal their business operations. This is even more important when we take zero day exploits under consideration. Well known worms like Witty or Slammer [12] have caused tremendous financial losses to many companies around the world. Would the worms be more destructive and target mostly critical infrastructure networks their impact could be far more severe. The next section provides use-case rationale for developing applied security infrastructure that is capable of aggregating and linking otherwise unrelated events into a big picture view to increase protection level.

4. Rationale for INTERSECTION

On the 25th January 2003 a virus called Slammer (sometimes also Sapphire) started infecting hosts by exploiting a buffer-overflow security hole in computers connected to Internet that were running the Microsoft SQL server and Microsoft SQL server desktop engine (MSDE) 2000 [12]. Once a host was infected the worm started scanning random IP addresses to spread further. Figure 5 presents the number of packets send by Slammer from infected locations during the first 12 hours after activation. Because Slammers behavior was highly anomalous (e.g., regarding amplified traffic envelope) it could be detected by a method called network telescope [12]. Success in suppresing the virus was achieved by analyzing intrusion detection system logs gathered from attacked companies and history of events collected by NMS systems.

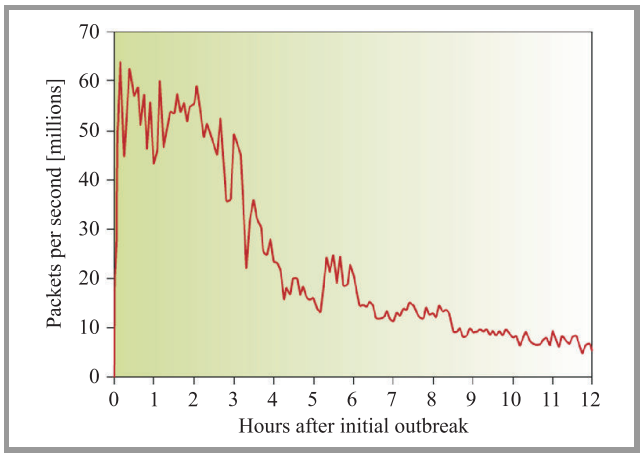


Fig. 5. The response to Slammer during the 12 hours after its release [12].

Would the infected systems been able to exchange information between different companies IDS the worm could have had respectively smaller impact and could have been suppressed from spreading worldwide. The distributed IDS could sufficiently increase the security of network operator infrastructures engaged in a supporting communication with malicious traffic in-band. The data for analysis could be spread through the network so if one operator would face the attack another one could benefit from his experience by exchanging information about pattern of anomalous (attacked) traffic between IDS. The INTERSECTION framework among other goals aims at proposing new anomaly detection algorithms as well as investigation of known algorithms [13] and providing a security framework that interconnects different network operators, which in turn allows exchanging traffic flow information between them. This could lead to enhancing the current security solutions by the factor proportional to the synergic effect of information exchange between operators.

5. A View on INTERSECTION

The aim of the INTERECTION project is to come up with specifications of an integrated framework for security and resiliency in complex and heterogeneous communication networks. Three objectives have been identified during the architecture process:

- to define what data must be shared among security systems of critical infrastructures and to specify hierarchy of communication and rules for data access,
- to design an integrated framework for securing networked systems,
- to specify appropriate protocols enabling communication between security systems in order to assure interoperability in an inter-domain environment.

Figure 6 presents a general overview of the proposed INTERSECTION framework. The INTERSECTION framework includes the following components for: monitoring, detection, reaction, remediation, visualization, and topology discovery. Integration of these components and exchange of information between modules collecting data from heterogeneous environments leads to improved network protection and security for participating systems. Monitoring, detection, reaction, and remediation components cooperate in real time and in automated fashion. These modules gather data from probes and network elements, analyze it, detect intrusions and anomalies, and select the most suitable reaction (e.g., reconfiguration of network components).
Remediation module is responsible for taking appropriate action in order to prevent similar attacks in the future. A network must operate at least one remediation point (e.g., at a gateway) in order to effect remedies, but may operate several if appropriate (e.g., one per border router) or additional that actually exist in neighbor networks (provided co-operation of those networks). The INTERSECTION framework also includes offline functions aiming at using data coming from the network, or provided by the real-time elements, to help the human operator in analyzing the network state and to evaluate configuration changes implemented by remediation module. The offline functions include topology discovery, visualization and anomaly detection. It is also important to highlight the relevant protocols used for data exchange within INTERSECTION. These include: IDEMF and IPFIX. A short description of each protocol is provided in the next two subsections.

5.1. IDEMF

IDMEF is an XML domain specific language (DSL) for intrusion detection systems. Its purpose is to provide an homogeneous environment to improve the network security.

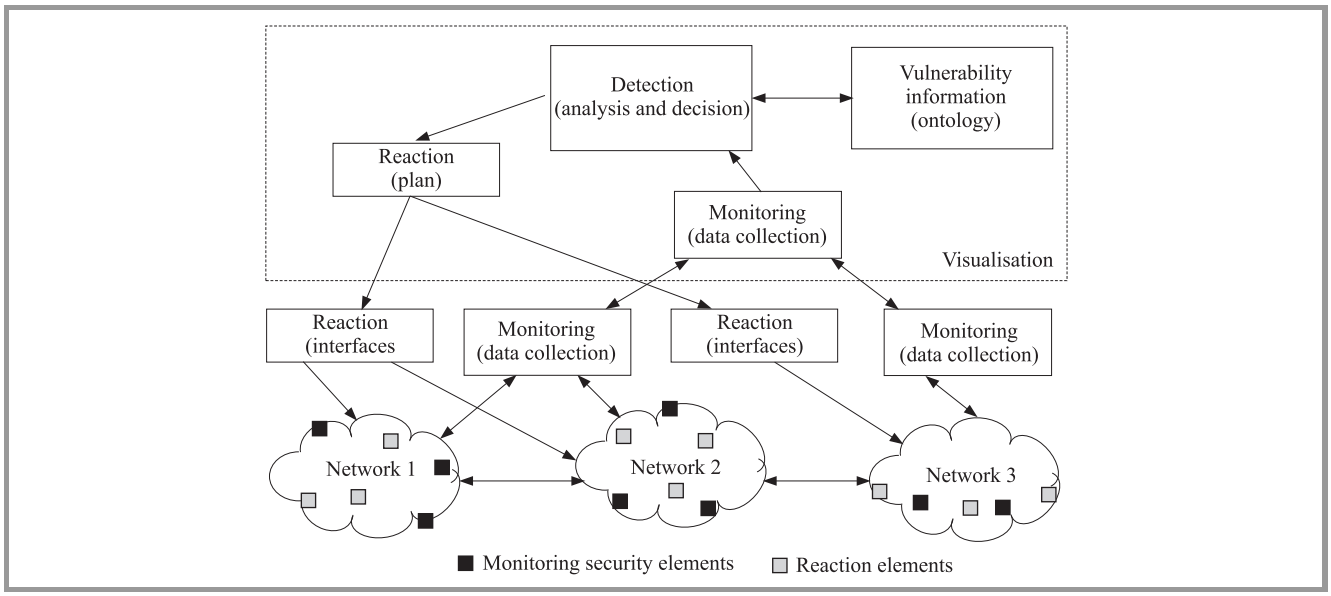


Fig. 6. INTERSECTION framework.

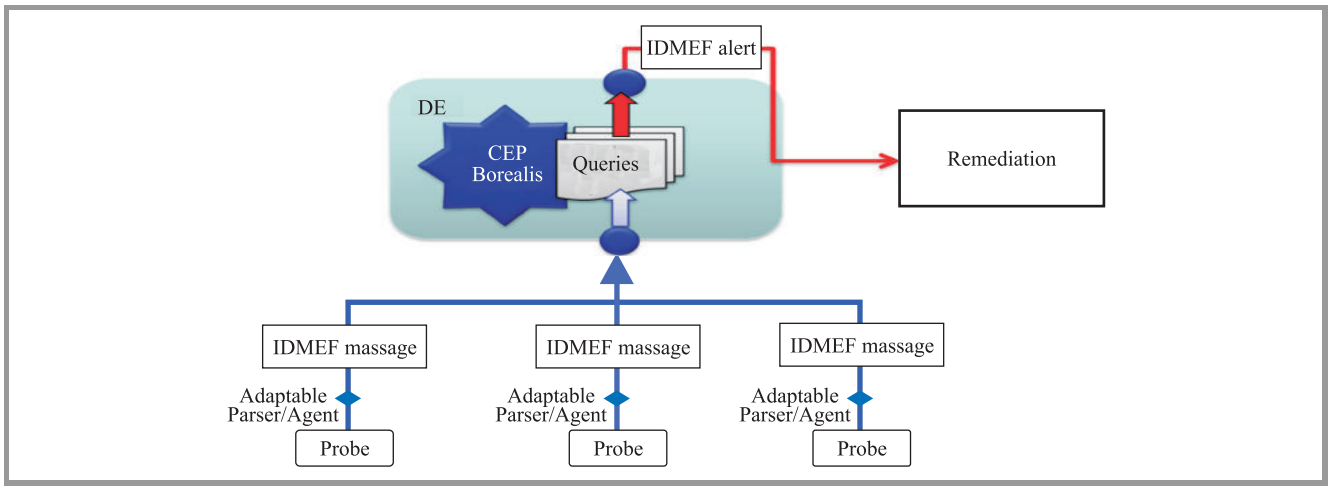


Fig. 7. Usage of IDMEF in INTERSECTION.

Figure 7 shows how IDMEF format is used in INTERSECTION. The decision engine (DE) aggregates events gathered from multiple probes (Host IDSes, Network IDSes, DB monitors, etc.). Correlation of these events is performed by complex event processor (CEP), namely Borealis correlation engine, developed jointly by Brandeis University, Brown University and MIT.
IDMEF messages are used to transmit information from the probes, and to send alerts to the remediation component.

5.2. IPFIX

IPFIX is an IETF working group standard [14]. It was created from the need for a common, universal standard for exporting the Internet protocol flows information from routers, probes, and other devices that are used by mediation systems and network management systems to facilitate services such as measurement, accounting and billing.

Within INTERSECTION IPFIX was used for the measurement task – a task that can be initiated by one of three components: measurement controller, IDS or visualization. Probes in INTERSECTION are called OpenIMP probes. Figure 8 shows that the monitoring system uses multiple measurement units (probes), which are distributed within the network and passively monitor network traffic. In addition, the monitoring system includes a postprocessor, collector, management and control interface.
The following section describes the proposed test scenarios within INTERSECTION project.

6. Test Scenarios

The INTERSECTION defined the suite of test scenarios to evaluate performance and detection, remediation and visualization capability of the proposed framework. This

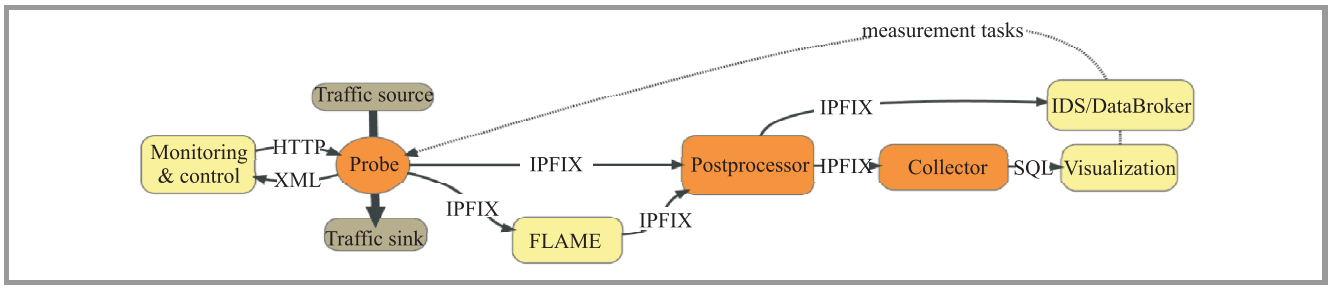


Fig. 8. Role of IPFIX in INTERSECTION.

section enumerates five different demo scenarios that have been designed to show how the INTERSECTION framework can effectively detect and resolve attacks by analyzing different pieces of information obtained from different networks. Furthermore, some scenarios show how the INTERSECTION framework is capable of detecting attacks by correlating data that, when analyzed separately would not provide enough information to detect the attack and to correct the system configuration settings. Each one of the five scenarios has been designed to be run over an interconnected infrastructure, the INTERSECTION demo network presented in Fig. 9, which is setup by the project partners. This interconnection of networks is necessary since an important premise, when designing the demo scenarios, was heterogeneity. In fact, the heterogeneity in the demo scenarios is addressed in the following ways:

- Each demo scenario involves at least two demo labs of different access technology interconnected, thus showing that the designed INTERSECTION framework can deal with access network heterogeneity. The interconnected infrastructure of the different demo labs, called INTERSECTION demo network, consists of five laboratories of different communication technologies (including satellite, wireless and wired networks) connected in a full-mesh network.
- Demo scenarios show how the INTERSECTION framework combines detection techniques from different access technologies with other detection techniques independent from the access technology, thus providing a richer framework for detection of attacks. Even if the attack exploits a vulnerability related to a specific access technology, information from other networks can contribute to the detection of the attack.

The demo scenarios are based on exploiting specific vulnerabilities that are currently present in networks. In summary, a demonstration case is a realistic story about how a vulnerability of a certain technology or equipment can be exploited, how the attack will be detected, how some mechanisms will be activated to solve the attack and how this process of detection and remediation can be shown to the network administrator through a visualization framework. Unlike a usual attack scenario, in these demo cases the attack is not detected by just analyzing the network where the

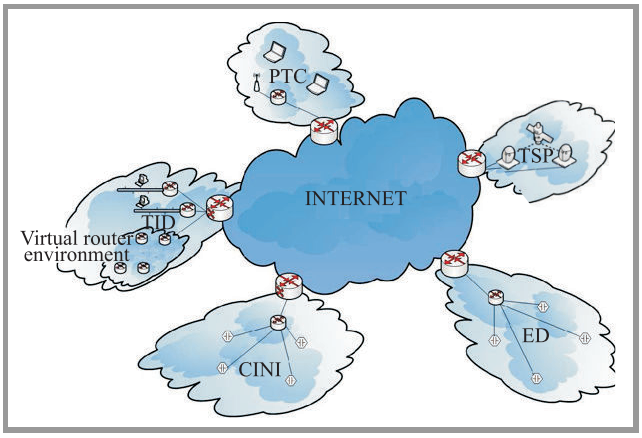


Fig. 9. he INTERSECTION demonstrator.

attack is performed, but by correlating the information from different networks involved in the monitored environment. The demo scenarios investigated by the INTERSECTION project are:

- loss of access to a content provider by hijacking prefixes of its corresponding autonomous system,
- satellite PEP spoofing,
- multistage attack on high profile roaming user and his network,
- injection of bogus packets in a wireless sensor network,
- distributed denial of service attack.

One of the INTERSECTION objectives is to show the applicability of the advanced decision support tools for mitigation, response and recovery in a heterogeneous environment. For this reason, a set of the aforementioned demo scenarios have been identified. Even though INTERSECTION is a research framework it is designed to be deployed by any operator already using commercial solutions that are incorporating IDMEF and IPFIX protocols.

7. Towards Converged Security

Numerous network security systems are currently available on the market. Authors envisage two categories of systems:

– systems that can manage one or more security areas, but not the end-to-end security environment of the organization,

– systems that have the capability of aggregating information from multiple sources and managing the whole environment.

First branch of systems include (but is not limited to) network access control, self-defending networks, and security gateways whereas the second is focused on so called management solutions. The latter include COTS products used for collecting, maintaining and reporting network traffic providing services such as centralized log system, user notification, activity monitoring. It can be seen that INTERSECTION does not address all security issues like privacy, communication flow security, non-repudiation and access control required for a complete security management system. However, a strong correlation of INTERSECTION to standard protocols for data exchange and proposed strategy for interconnecting networks of independent operators and their customers shows the way towards unified approach to network security in our highly interconnected world. One way to evaluate security solution is to map it against the security maturity model. Attributes such as company size, industry regulations, liability, technical complexity, culture, risk tolerance, and the level of dependence on physical and logical assets all create distinct requirements for risk management and security convergence. However, there are several attributes common to a mature, converged security organization. In [15] maturity attributes of a company are presented (Table 3).

Table 3
Converged security maturity attributes – excerpt from [15]

Maturity attribute	Defense-in-depth
Immature (ad hoc)	There is no formal security structure
Aware (repeatable but intuitive)	Security is focused on perimeter defense
Management and risk-based (defined)	Safeguards extended beyond the perimeter, but remain technically focused
Common (optimized)	There is true defense-in-depth encompassing people, policy, and processes with technology. Thrid-party and mobility issues are included

INTERSECTION framework, while not covering some of the aspects of the converged rank in maturity model in some way may stretch the model beyond current definition. INTERSECTION framework envisions participation in a solution that not only includes internal policies and processes of an organization but provides enhancements and introduces capability possible only with a management solution that is at a higher level than any of the connected systems alone.

8. Security as a Service

As the software paradigm shifts towards cloud computing the more important it appears not only to provide means for better security but also to incorporate security solutions that span across domains and gain from the knowledge/experience of "first" victims in order to protect others. In computer networks there is a problem of extremely high speed of data/message exchange between host/networks during attack. The so called zero-day exploits are the effects of malicious activity of attackers that may affect huge number of network users (from individual to corporational). Thus important dimensions for improved threat detection and prevention (also tolerance) are time and knowledge. Time factor covers the time period to detect malicious activity as well as time to find and apply countermeasures best matching to the context. On the other hand knowledge sharing is essential in keeping security best practices up to date each time security flaw is detected and providing framework for building and exchanging rules to apply (e.g., in the context of security threat) remediation policy of an organization. Some aspects limiting the proper take-off of the 3S paradigm are related to both business view (security maturity of an organization, information exchange strategy) and regulatory framework of a given country (obligation for anonymization of logs). Deployment of INTERSECTION enables implementation of the paradigm of security as a service external to an organization. One can imagine that monitoring and decision engines are located outside of a company network and managed by trusted third party.

9. Conclusions

The growth of Internet connectivity results in increased security requirements for enterprises to achieve services availability as described by SLA agreements (for end users and between operators). Inherent heterogeneity of the networks increases risk factor and new security threats emerge due to the variety of network types and their vulnerabilities. The solution proposed by INTERSECTION aims at providing security-level interoperability between many operators using different network technologies and different security solutions. The real benefit of exploiting INTERSECTION as an example of applied security framework paradigm can be capitalized if the key operational assumptions are fulfilled. The network owners and service providers should agree on the need to foresee security related data exchange as an important substrate of a successful security policy. The wide spread of malicious code that is remotely com-

manded to trigger distributed DoS attacks at any time decided by a hacker, calls for the real cooperation that is fostered by telecommunication regulatory institutions. Currently the Polish telecommunication law for instance states that cooperation between telecommunication operators is the obligation of the operator only at times of crisis situations [16]. So it is up to the operator to make its internal information accessible for other operators. The continual improvement (as a business process) of individual organizations security infrastructure is essential but there is an even more important aspect in holistic security supremacy that is only possible when security information exchange requirement is fulfilled. It should be at least as important to investigate technology and business governance as to formalize the need for decisions on security cooperation in the process of managing and planning security. From this perspective the meaning of the attribute of converged security maturity of an organization is stretched as INTERSECTION provides enhancements and introduces capability possible only with a management solution that is at a higher level than any of the connected systems alone.

Acknowledgements

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 216585 (INTERSECTION Project).

References

[1] J. Dawkings, "A framework for unified network security management: identifying tracking security threats on converged networks", *J. Netw. Sys. Manag.*, vol. 13, no. 3, 2005.

[2] C. Onwubiko, A. P. Lenaghan, L. Hebbes, "An integrated security framework for assisting in the defense of computer networks", in *Proc. Mobile Future 2006 and the Symposium on Trends in Communications SympoTIC'06*, 2006, pp. 52–55.

[3] B. Von Solms, "The ten deadly sins of information security management", *Comp. Secur.*, vol. 23, pp. 371–376, 2004.

[4] P. Hunter, "Lack on integration undermines IT security", *Netw. Secur.*, vol. 2003, no. 1, pp. 5–7, 2003.

[5] M. Sourour, B. Adel, and A. Tarek, "Ensuring security in depth based on heterogeneous network security technologies", *Int. J. Inf. Secur.*, vol. 8, no. 4, pp. 233–246, 2009.

[6] Technical Report ISO/IEC TR 15947 "Information technology-security techniques-IT intrusion detection framework. Part 1: Network security management", 2002.

[7] M. Withworth, "Outsourced security – the benefits and risks", *Netw. Secur.*, vol. 2005, no. 10, pp. 16–19, 2005.

[8] International Standard ISO/IEC 18028-1 "Information technology-security techniques-IT network security. Part 1: Network security management", 2006.

[9] ISO 7498-2:1989 – CCIT Rec. X.800 (1991).

[10] International Standard ISO/IEC 18028-2 "Information technology-security techniques-IT network security. Part 2: Network security architecture", 2006.

[11] International Standard ISO/IEC 18043 "Information technologu-security techniques-selection, deployment and operations of intrusion detection systems", 2006.

[12] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Stainford, and N. Weaver, "Inside the Slammer worm", *IEEE Secur. Priv.*, vol. 1, no. 4, p. 33–39, 2003.

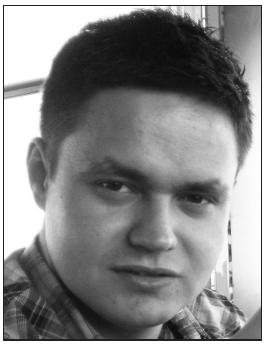
[13] Ł. Saganowski, M. Choraś, R. Renk, W. Hołubowicz, "A novel signal-based approach to anomaly detection in IDS systems", *Lecture Notes in Computer Science*, vol. 5495, pp. 527–536, 2009.

[14] Request for Comments RFC 5101, "Specification of the IP flow information export (IPFIX) protocol for the exchange of IP traffic flow information", 2008.

[15] K. Anderson, "Convergence: a holistic approach to risk management", *Netw. Secur.*, vol. 2007, no. 5, pp. 4–7, 2007.

[16] *Polish Telecommunication Law*, act from 16th July 2004.

Adam Flizikowski obtained his M.Sc. from University of Technology and Agriculture in Bydgoszcz, Poland, in 2000. Since 2003 he holds a research position of professor assistant at the University of Technology and Life Sciences. He also had managed projects dealing with telecommunication aspects like end to end QoS management, policy based networking, mobile service automated evaluation, methodology of evaluation of video servers and STB platforms, and so on. He has working experience with IT system design methodology and especially applied ontology based systems. Currently he works on dissertation on admission control in 4G WiMAX networks.
e-mail: adamfli@utp.edu.pl
Istitute of Telecomunications
University of Technology and Life Science
Prof. Kaliskiego st 7
85-796 Bydgoszcz, Poland



Mateusz Majewski obtained his M.Sc. from University of Technology and Agriculture in Bydgoszcz, Poland, in 2009. Since 2008 he has been working in the ITTI Ltd. in Poznań. In the recent years he participated in EU projects as a junior consultant. During the years he was involved in projects covering such topics as QoS aspects in wireless networks, simulation methodologies, security framework and applied security.
e-mail: mateusz.majewski@itti.com.pl
ITTI Ltd.
Rubież st 46
61-612 Poznań, Poland

Maria Hołubowicz obtained her M.Sc. from Poznań University of Technology, Poland, in 2009. She has been working in ITTI Ltd. in Poznań since 2007. She has contributed to the preparation of a number of proposals to FP7 ICT and Security calls. She has participated in EU projects as a junior consultant and in projects that involve GUI design, knowledge based systems, network security systems and ontology design for knowledge based systems for EDA projects.
e-mail: carolina@itti.com.pl
ITTI Ltd.
Rubież st 46
61-612 Poznań, Poland

Zbigniew Kowalczyk obtained M.Sc. and MBA from Kozmiński University in Warsaw. Since 2000 he has worked as an IT Architect, IT Consultant, and Project Manager for Compugen of Richmond Hill (Canada). He holds number of professional certifications, including PMP and CISSP. Since the beginning of 2009 he is involved in EU projects as part of the team of Polska Telefonia Cyfrowa (PTC). He contributes to Tuesday Technology Report, a bi-monthly electronic newspaper, writing on IT security trends and issues.
e-mail: zkowalczyk@era.pl
Polska Telefonia Cyfrowa
Jerozolimskie Av. 181, B2.13
02-222 Warsaw, Poland

Simon Pietro Romano received the degree in computer engineering from the University of Napoli Federico II, Italy, in 1998. He obtained a Ph.D. degree in Computer Networks in 2001. He is currently an Assistant Professor at the Computer Science Department of the University of Napoli. His research interests primarily fall in the field of networking, with special regard to QoS-enabled multimedia applications, network security and autonomic network management. He is currently involved in a number of research projects, whose main objective is the design and implementation of effective solutions for the provisioning of services with quality assurance over Premium IP networks. He is member of both the IEEE Computer Society and the ACM.
e-mail: spromano@unina.it
Computer Science Department
Universita' di Napoli Federico II
Via Claudio 21
80125 Napoli, Italy