

## Featured this month:

### Developing world, developing problems

**B**ot net infections may be bad enough in the developed world, but the signs are that we are due for an explosion of bot net malware activity in the developing one. A mixture of new broadband connections and unpatched PCs is creating a perfect storm in which a new community of computers will be ripe for infection and exploitation.

In particular, Asia is becoming a target for cyber criminals, and ISPs in the region are perfectly positioned to learn from the West's mistakes in the past. Mark Sunner, chief security analyst at MessageLabs, takes a look at malware infections by geography, and crunches the numbers.

*Go to Page 4...*

### Managing both careers and risks

**C**areer choices for people in information security are growing, while the profile of the people choosing this career is changing. For employers, there is growing recognition that information security can no longer be managed by the generalist. Just as individuals must take control of their own careers, companies also must support and develop the people they rely on to provide the most effective information security programme.

To manage careers as well as risks, all information security managers should formalise professional development with a workforce plan that maps requirements and encourages the interest of individuals, while focusing on opportunities across the business. John Colley of (ISC)<sup>2</sup> discusses effective career management techniques in the security industry.

*Go to Page 7...*

### SQL attackers strike again

**Y**et more SQL injection attacks have swept the internet. Hundreds of thousands of web sites were hit, including those operated by the UN and UK government. Websense identified the attack, which uses injected JavaScript to access the domain nihoarr1.com. They JavaScript file is loaded from that domain, which in turn loads a .HTM file accessing several other exploits.

Initial reports suggested that the attacks exploited a vulnerability that Microsoft had announced in IIS, but in a blog post, F-Secure later suggested that it was more to do with badly written ASP code. Microsoft staff clarified the situation: "The attacks are facilitated

by SQL injection exploits and are not issues related to IIS 6.0, ASP, ASPNet, or Microsoft SQL technologies," said an executive on the Microsoft Security Response Centre blog.

The Department of Homeland Security's web site was also compromised by the attack, which uses a single string of text written in hexadecimal code.

Based on an analysis of tools found at the offending domain, Websense believes that the attack is linked to a previous SQL injection that infected thousands of web sites in March, in which a different domain served up 12 attacks to browsers sent to it via hacked websites.

## Contents

### NEWS

SQL attackers strike again	1
Researchers crack bot net secrets	2
BERR: More work to do on security	2
Symantec: Spammers using AdWords	20
Mozilla serves up infected files	20

### FEATURES

#### Developing world, developing problems

Broadband connections in developing countries are putting new communities in the path of bot net malware. Mark Sunner of MessageLabs investigates.	4
--	---

#### Managing both careers and risks

John Colley, managing director, EMEA for (ISC) <sup>2</sup> , explores the options for companies trying to find and retain skilled staff.	7
---	---

#### Treating employees as a threat

Kurt Roemer, chief security strategist at Citrix explains why your best employee could still unwittingly be your worst enemy.	9
---	---

#### Vulnerability management at the crossroads

Organisations embracing vulnerability management best practices have not always enjoyed the expected gains. Iván Arce of Core Security Technologies explains why.	11
---	----

#### Collective intelligence approaches to malware recognition

Desktop malware detection has its place, says Iñaki Urzay, chief technology officer of Panda Security.	14
--	----

#### Security for safety in railways

Dario Forte describes the development of a new security system to support the modernisation of the Italian rail traffic management infrastructure.	17
--	----

### REGULARS

News in brief	3
Events	20

# Security for safety in railways

Dario V Forte, CISM, CFE, founder and CEO Dflabs

Industrialised nations base their organisation and development on increasingly complex and computerised infrastructures. Much of these infrastructures are critical to a country's security and vital functions, (healthcare, law enforcement, energy production and distribution, transportation, etc.) and is thus known as critical national infrastructure (CNI). These functions and their infrastructure are subject to risks of various kinds, including malfunction, natural disaster, and intentional attack. Such risks may directly or indirectly compromise their ability to satisfy the needs for which they were developed, and are thus accorded an enhanced level of protection.

In the transportation sector, and specifically regarding the Italian Railway Signal System, the development and introduction of the new interoperability system RTMS/ERTCS (Rail Traffic Management System/European Rail Traffic Control System) plays a role of fundamental importance. The objective of this system is to transform the Italian railway system into a high speed/high capacity system. This new technological infrastructure is an innovative rail signal infrastructure that will allow the Italian rail network Rete Ferroviaria Italiana (RFI), to respond to the new dictates of European integration and the increasing demand for high speed transportation.

The development of the RTMS/ERTCS system has placed the Italian railways and Italian industry in a position of world leadership, but has also brought with it the risks associated with the use of ICT infrastructure. We are all well aware of the risks to infrastructure from malfunctions, human error or intentional acts of sabotage. The issue of information security becomes very complex in this context. Even if the safety of the transportation system is maintained, the occurrence of an adverse event may significantly affect its continuity of operation, causing not only delays and inconveniences in the circulation of trains, but also financial losses and damage to the image of companies in the sector.

## Implementing information security

Via its Comunità Sicurezza (Security Community), Finmeccanica has recently

implemented the SeSaR (Security for Safety in Railways) corporate project, cofinancing it within a larger project called MindSh@re.

Before we illustrate the idea behind the SeSaR Project, we have to ask the question, how is information security achieved? A brief but exhaustive answer can be provided: achieving information security means developing incident prevention, detection and response measures.

Prevention entails a set of defence techniques and countermeasures that make a system able to resist attacks and attempts at compromising it. However, this can only be achieved at some effort and expense. To be effective, prevention has to be protracted indefinitely, requiring an unflagging organisational commitment, continual personnel training, and constant upgrading of countermeasures.

***"To be effective, prevention has to be protracted indefinitely, requiring an unflagging organisational commitment, continual personnel training, and constant upgrading of countermeasures"***

When prevention fails to prevent, the next operation is to detect what happened. Since new malicious codes are capable of self mutation when they replicate, and zero-day attacks can make countermeasures ineffective, an adequate defense architecture must have tools that are able to carry out real-time analysis of logs memorised on the computer and on network defence apparatus.



Dario Forte

After detecting what prevention has failed to prevent, the ultimate task is to respond to it. Obviously at this point it may be very difficult to ensure that the incident will not cause malfunctions, breakdowns or interruptions of service.

The objective of the SeSaR project has been to research and develop a tool that unites the two priority security activities: prevention and detection. The concept behind this tool is the ability to discover the new, the unusual and the anomalous.

The concept has assumed concrete form in a hardware/software platform with the following functional components:

**Prevention:** the integrity of the system is constantly monitored and verified in real time.

**Detection:** logs regarding critical and defense systems are correlated and analysed constantly in real time, searching for significant concatenations of events or modifications to the system.

**Operator interface:** a simplified interface composed of a console and a synopsis panel gathers and summarises information, providing clear and exhaustive indications of any detected anomalies so as to allow immediate response measures to be undertaken.

## Project context

The applicative environment of the SeSaR project is the technological infrastructure of the RTMS/ERTCS Signal System used on the Rome-Naples high speed rail line. The Rome-Naples high speed system is composed of several components. A central level known as the central satellite post, or Posto

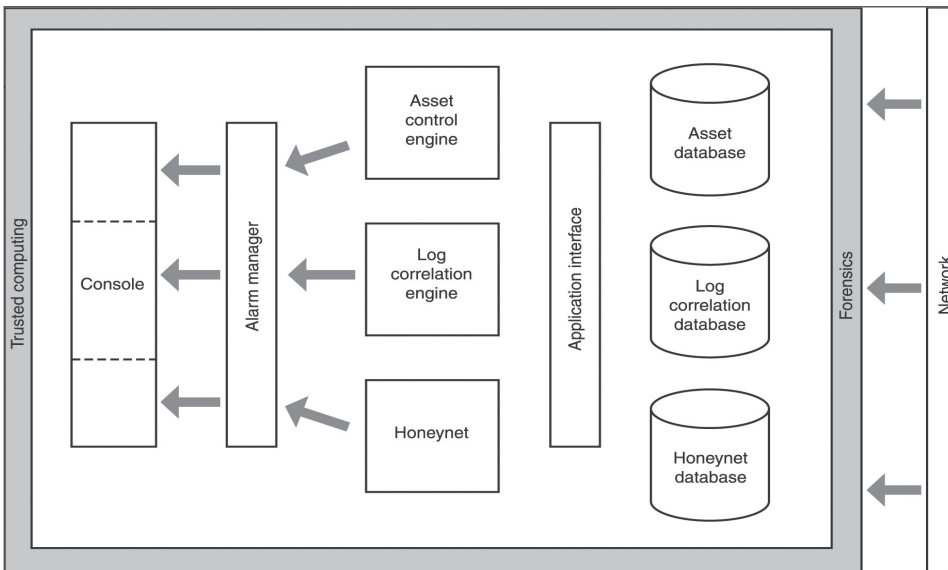


Figure 1: Functional components of SeSaR.

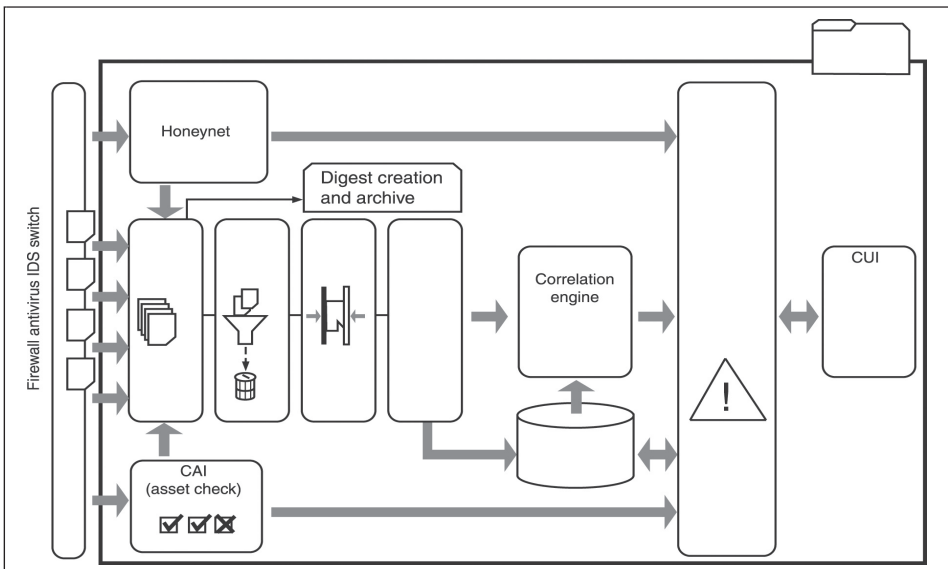


Figure 2: SeSaR Architecture.

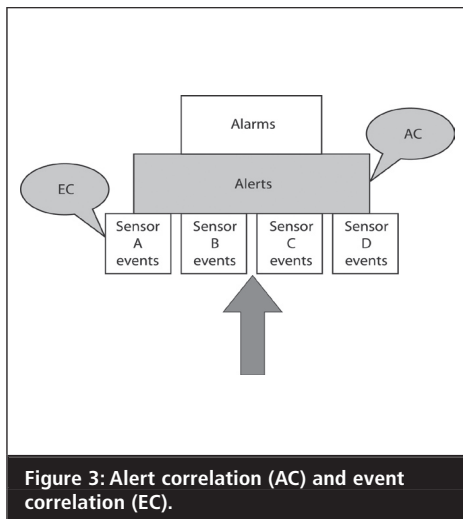


Figure 3: Alert correlation (AC) and event correlation (EC).

SeSaR offers a number of specific and innovative aspects. It constitutes a non-invasive defense system, and it works independently of the ICT infrastructure and operating systems (Unix, Linux or Windows). It also constitutes a multi-level defense system, carrying out checks and verifications on different levels and in different areas of computer security, such as asset control, log correlation, and integrated and interacting honeynets. And finally, it can implement trusted computing functions and thus constitutes a reliable and trusted defence system.

In particular, the SeSaR system has the following principal functions, as illustrated in figure 1:

- Real-time asset control of the entire ICT infrastructure
- Real-time correlation of logs collected by security devices and critical systems
- Honeynet functionality, facilitating the identification of intrusions or aberrant behavior via the creation of ICT ‘bait’ and ‘traps’
- Forensics functionality, so that the data collected during investigation of an attack can be assigned a digital signature and timestamp. This gives it value as evidence in a court of law, while creating trust in the system via integrity checks.

SeSaR was developed from an idea conceived by Finmeccanica companies ANSALDO STS and Selex SI in response to an initiative of the MindSh@re corporate project, and is being developed in line with the needs and indications of a major client, the Italian Rail Network (RFI). The initiative embodies a very productive and rewarding collaborative effort between the two Finmeccanica companies, who are pooling their knowledge on information security, a theme which is broadly applicable within their respective production systems. The companies are availing themselves of external specialised collaborators such as the Biophysics and Electronics Department of the University of Genoa under Prof. R. Zunino and other academics such as the author and Prof. G. Sciutto.

## Architecture and functionality

SeSaR architecture is modular and web-based. The components can work independently or in an integrated framework. The user accesses the functions and services via a simple browser. The principal components of the SeSaR architecture are illustrated in Figure 2 and described below.

### System Asset Check (CAI, green)

This component checks the integrity of the hardware/software systems at the central post and the peripheral posts in real time in order to detect and identify intrusions or missing hardware or software elements. The operation mode entails real-time checking of the functional status of the systems (via SNMP interrogations of the network devices to which the systems are connected) and comparison with the nominal configurations memorised in the database. If any discrepancies are detected an alarm is generated at the console and at the synoptic panel.

### System Log Correlation (CLI, blue)

This component represents the brain of the system. Its function is to automatically detect anomalies. This detection is not intrusive; it is accomplished on the basis of information, data and events coming from perimeter defense devices (firewalls), content filtering devices (antivirus programs), critical systems and the other two components, CAI and the honeynet. As illustrated in figures 2 and 3, this requires a chain of correlation steps (from Log Correlation to Alarm Management) and can be divided into two distinct

phases: alert correlation (AC) and event correlation (EC).

### **“SeSaR represents an important step in the applicability of information security systems to diverse sectors”**

In event correlation, the events from each individual sensor (e.g. the firewall) are analysed and filtered with the purpose of extracting useful information in order to generate alerts (as per the following steps in figure 2: log collection, filtering, aggregation, metadata creation, correlation engine). In alert correlation, the alerts from each sensor are correlated and translated into alarms according to specific threshold levels (alarm management step in figure 2). The alarm is then sent to the console and to the synoptic panel where it can be assessed by the operator.

### Honeynet (Yellow)

This component is dedicated to the identification of intrusions or anomalous behaviors on the part of internal users and works by creating ‘traps’ within dedicated and properly monitored networks known as honeynets.

Three functions are performed:

- Data capture, dedicated to the collection of incoming traffic to the ‘trap’
- Data control, dedicated to checking and filtering the information to determine whether it is allowed or unauthorised
- Data analysis, dedicated to the analysis of activities performed on the honeynet

### Operator console and synoptic panel

The alarms generated by the above components are collected and displayed to the operator both in text

format (console) and in graphic format (synoptic panel).

## Conclusions

SeSaR represents an important step in the applicability of information security systems to diverse sectors. It adequately responds to the demands imposed by interconnected networks and commercial ICT platforms with heterogeneous software components. It represents a valid countermeasure to threats to and potential vulnerabilities of these infrastructures.

SeSaR is currently being developed per specific interest by the Italian Rail Network (Rete Ferroviaria Italiana – RFI) and specifically for the Rome-Naples High Speed line. However, given its special features and platform-independent architecture, SeSaR is a prototype that can be applied in other contexts, particularly to systems that were initially developed to be platform-centric but that now need to open up, publish their services and interoperate with other systems.

### About the author

*Prof. Dario Forte, CFE, CISM, former police detective and founder of DFLabs, has worked in information security since 1992. He has been involved in numerous international conferences on information warfare, including the RSA Conference, Digital Forensic Research Workshops, the Computer Security Institute, the US Department of Defense Cybercrime Conference, and the US Department of Homeland Security (New York Electronic Crimes Task Force). He was also the keynote speaker at the Black Hat conference in Las Vegas. He provides security consulting, incident response and forensics services to the Italian Government, law enforcement agencies and private companies. [www.dflabs.com](http://www.dflabs.com)*



## A SUBSCRIPTION INCLUDES:

- 12 printed issues
- Online access for 5 users
- A three-year archive of back issues
- Free delivery

[www.networksecuritynewsletter.com](http://www.networksecuritynewsletter.com)