International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.427-438
http://dx.doi.org/10.14257/ijsia.2014.8.5.37

Contextual Security with IF-MAP

Abdelmajid Lakbabi, Ghizlane Orhanou and Said El Hajji,

Laboratory of Mathematics, Computing and Applications, Department of Mathematical and Computer Sciences, Faculty of Sciences,
University of Mohammed V-Rabat, BP.1014 RP, Rabat, Morocco.
lakbabi@gmail.com, orhanou@fsr.ac.ma, elhajji@fsr.ac.ma

Abstract

The multi-context attacks are serious challenges to security detection process. Actually, each security solution produces a considerable number of security events, heterogeneous and difficult to correlate. Sensors usually work independently making hard to extract security information related to a multi-step attacks. Therefore, correlation and sharing mechanism becomes the key to deal with such challenging IT security threats.

This paper provides an analysis of the current security state and proposes our security architecture based on local and global contextual protections that share security events in a real time IF-MAP approach in response to malicious activities. As to implementation phase we used opensource Omapd as a MAPS central data repository, apache web server and iptables as MAPC clients in perspective to provide real time containment when attacks are detected.

Keywords: *IF-MAP, Security Context, SIEM, Firewall, correlation, Threat*

1. Introduction

The Security is a core requirement for every network to protect its infrastructure and its critical applications. Through this paper, we propose to reduce the attack surface of a protected network by using a new contextual security mechanism [1] that makes possible to share critical events; in perspective to approach a real time reaction against the network applications attacks.

A network security solution is generally based on a large number of security components like Firewalls, Intrusion Prevention/ Detection Systems IPS/IDS, SIEM [2] solutions and others, while each of those security systems keeps its partial information about the network, and there is currently no standardized way to correlate the information from those single distributed sources. This leads to the following weaknesses:

- ❖ Lack of context aware security

The context aware security [3] is the ability of security devices or applications to analyze events in a changing environment, to detect illicit manipulations and to respond accordingly.

- ❖ Insufficient security integration

Figure-1 below shows a conventional security with no interaction. Indeed, in traditional security solutions, each device works independently and reports more or less critical events. Moreover, those events are never or not accurately correlated, and in case the correlation job is done, it unfortunately lacks the ability to respond in real-time and contains live attacks, since the correlation task is almost invoked as a scheduled batch processing.

ISSN: 1738-9976 IJSIA

Furthermore, IT security solutions are in general based on heterogeneous sensors coming from different technologies. To handle this lack of visibility, the majority of security vendors have been focused on proprietary integration between their own solution products using legacy management protocols like (Syslog, SNMP *etc*.,…) that are static and not enough to provide a whole visibility of the attack context by analyzing suspicious connections and reacting to potential deviation from the normal behavior.

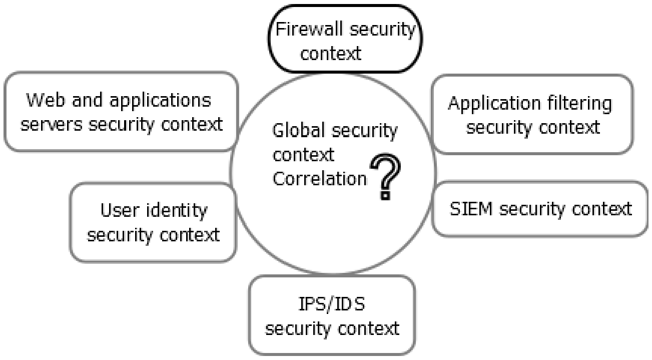
Firewall security context
Web and applications servers security context
Application filtering security context
Global security context Correlation ?
User identity security context
SIEM security context
IPS/IDS security context

Figure 1. Conventional Security with No Interaction

- Basically each sensor entity works on its context with practically no interaction with other sensors of the global security solution.
- No metadata repository to store security events and logs, and consequently there is no correlation work to analyze and state about suspicious traffic.
- No real-time standard or mechanism to collect security information from different sensors sources.
- Lack of intelligent and contextual correlation, then inability to counter distributed or multi-step attacks.

From this situation, some important questions rise:

- With such weaknesses, how is our security being effective?
- Is there a computer or application infected in the network that could potentially spread malware?

On the other side, the attacker has a vast advantage over the defender, since the attacker starts first and has an unpredicted strategy, while the defender should understand that strategy and respond accurately and quickly in a specific application context.

From this perspective, the logical action to take is to reduce the gap between the attack and the containment reaction, to achieve that we propose a security solution based on independent protection technologies that each works on its proper security context then reporting information about given connection behavior in real time

2. New Security-Context Architecture

As a start point, it is capital to determine the perimeter of our proposition. A network security solution is generally based on a large number of security components like Firewalls, Intrusion Prevention/ Detection Systems (IPS/IDS), SIEM solutions. Each of those security systems keeps its own partial information about the network, and there is currently no standard way to correlate the information from those single distributed sources and share it in real time approach.

Our objective is to address such lack of security coordination by the following improvements:

- Each sensor entity works on its context, but should share information when it is facing an attack to report and advise the global security management system and indirectly inform the security enforcement point "PEP" [4] to react and stop the malicious connections.
- Metadata repository is created to store security events, and consequently correlates and states about suspicious activity.
- A real-time standard mechanism is used to share security information among different sensors.
- Intelligent and contextual correlation is performed to counter complex or multi-step attacks.

This target solution can be summarized by the following figure (Figure 2):

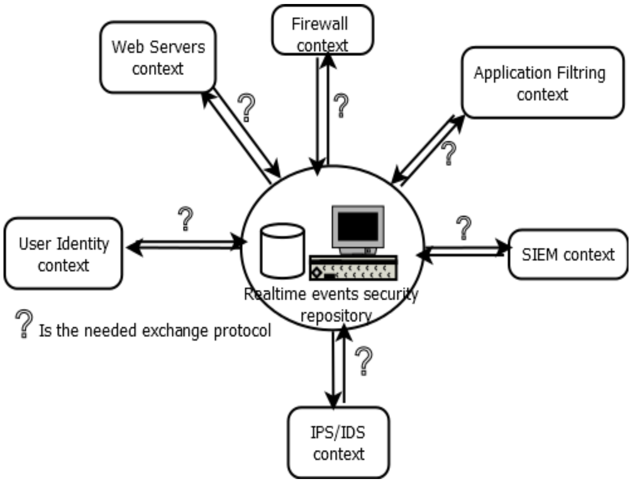
Web Servers context
Firewall context
Application Filtring context
User Identity context
SIEM context
Realtime events security repository
IPS/IDS context
? Is the needed exchange protocol

Figure 2. Modern Concentric Security Interaction

Our proposition is motivated by the following three principal objectives which will be detailed below:

- ❖ Illustrate the importance of securing each type of resource inside its appropriate security context.
- ❖ Correlate the different security events coming from partial contexts to provide the global security context that gives a clear idea about how network resources are being used in real time approach.
- ❖ Share security events and malicious detection in a real time approach using a standard protocol IF-MAP [5].

2.1. Local Security Context

A security context is used by a system to classify resources, such as applications, processes and files. It allows understanding the application environment then enforcing rules for how and by whom a given resource should be accessed. This concept is fundamental and mandatory to build a good security policy; To better illustrate this concept, let’s talk about the security of a web application.

With the evolution of web attacks, for example, classical protection of the perimeter using firewalls become inefficient, because the protection should be done inside the web application context, in order to understand what parameters are vulnerable and lock down the web application flaws consequently. This is named WAF (Web Application Firewall) ad it is a good illustration of the contextual security approach.

Definitely, the better approach to guaranty a good security for given application is to perform the protection inside this application context.

2.2. Global Security Context (correlated context)

Security approach based on local security context will fail to understand and contain multi-context attacks. As an example, let’s take a protection system based on Firewall and intrusion detection/prevention systems. Such security solution is unable to protect network servers and applications, since each local tools fail to understand the whole context of a given access tentative; It assumes that attackers are remote, are network-based, and have a limited privileges; Hence after getting access, malicious users can try an escalation of privilege to gain more authorization and perform forbidden activities; Getting a root access is sufficient to bypass those traditional security, and cause damage on the target system.

In this security model, the target system is considered as a “Black Box”, where the attacker is unable to see into the system, but can only try to manipulate it externally as described by the Top ten OWASP attacks especially the SQL, XSS and RFI [6].

2.3. IF-MAP - The New Security Exchange Mechanism

Are relational databases or directories enough to exchange those contextual security events? Why we need a new protocol? The answer is the challenge to collect and correlate data in real time among many applications and systems which requires the ability to accommodate diverse data types, data relationships and many security entities and find data relation schema to satisfy all security needs.

Conceptually, to contain multi-context attacks, the new proposed approach, use metadata to improve the situational awareness. The idea behind is that attacks will continue to occur even more and more complex.

Consequently, our objective should shift to focus on the user and application behavior, by analyzing the inappropriate uses of applications in the traffic flows to recognize anomalies; From this perspective, we will focus on the integration of the security sensors “Firewall”, log server, and the SIEM server to handle security events and critical parameters in the user session’s context, instead of relying only on the sensors predetermined and static signatures to detect the illicit traffic.

Our motivation is to make network security nodes more effective by introducing intelligent integration of legacy security technologies; this new mechanism will replace SNMP, Syslog, proprietary APIs and custom scripts, and thereby reduce integration complexity and helps to react quickly when deviation from normal behavior occurs. This new standard allows sending automatically populate security events among sensors and a central policy management system in real time which makes accurate reaction possible when attacks are detected.

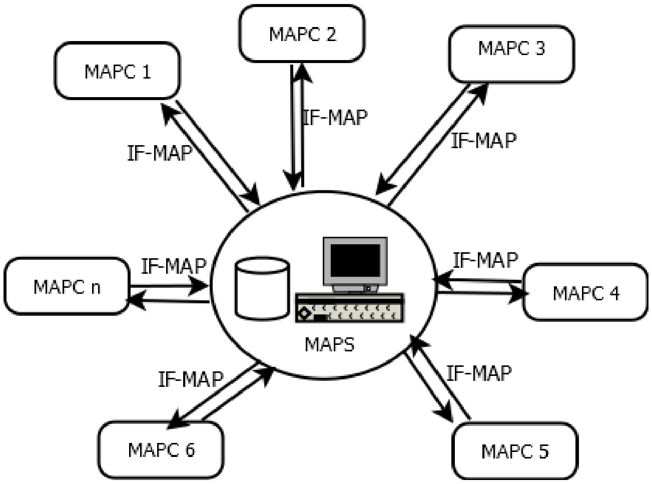

Figure 3. IF-MAP as MAPC/MAPS Exchange Protocol

As shown in the Figure 3, the challenge is the heterogeneous and multi-technology based security, that networks are to let network key security products like IPS, SIEM and the NAC policy [7] servers share events in a nearly real time way, we should adopt a new mechanism using IF-MAP to fill the gap between the attack and the containment, since this protocol has a great potential to enables easy and directly integration into an existing IT infrastructure, with extensions both from schema modifications and client reconfiguration perspectives to enhance security and approach real time reaction to threats.

3. IF-MAP security collaboration protocol

IF-MAP (open standard) stands for Interface for Metadata Access Points. It is a standard based on the web technology and a central database for the IT-systems where we can store and/or retrieve information from in order to get a real-time representation of the security status of the network and its resources.

IF-MAP is based on SOAP (Simple Object Access Protocol) [8] that interacts via HTTPS Request-Response according to client server paradigm. For more security, it uses certificates for each communicating client or server to secure the tunnel. This standard extends the TNC architecture, now providing a standard way to integrate a wide variety of network security devices such as IPS, SIEM servers and firewalls. This allows a smart integration of legacy enforcement check-point to achieve better security.

The IF-MAP defines a standard SOAP-based protocol that network security devices can use to communicate with a shared database called a Metadata Access Point (MAP). Using this protocol and database, the network security devices share information, in real-time, about the users, applications and devices connected to the network: who’s logged into what device, how healthy the device is, whether it’s violating policy. Also, its main purpose is to achieve interoperability for security related data exchange between security components in a network; MAP clients (MAPC) can publish new meta-data to a MAP server (MAPS) and also search for meta-data or subscribe to specific information when new meta-data is published.

3.1. IF-MAP Components

IF-MAP standard that makes possible to exchange metadata in real time. Its main components are:

- MAPS, the IF_MAP server, the central Metadata Access Point that:
    - collects metadata about access decisions
    - can be used to inform dynamic firewall set-up or other network issues
    - interacts with other sensors
- MAPC, the IF_MAP client representing Sensors like Firewall/IPS, log server or SIEM server, etc.

On the other hand, there are two different data types to store in the MAPS: Identifiers and Metadata. Identifiers act as “root hub” for information stored in the IF-MAP server. There are identifiers like Identity, IP address, MAC address, Access Request and Device.

The other type of data is metadata, which has to be linked to at least one identifier but can also connect two identifiers. Each client has to authenticate itself securely to the MAP Server either with username and password or certificate based authentication. All data is transmitted safely with SSL encryption.

3.2. IF-MAP Features for Security

We will present below the main features of the IF-MAP protocol that differentiate it from other existing protocols.

- One-to-many Links

IF-MAP does support one-to-many links; relationships between identifiers are published (at run-time) as metadata tags on links. This if-map feature allows the schema to be run-time dynamic to leads a search method rather than query. This is a key differentiator of IF-MAP from existing standards.

- Search vs. Query

Technical specifications give a clear distinction between search and query which make IF-MAP simple and applicable to security events exchange.

Specifically, query requires a priori knowledge of the schema (including both labels and structure). Because of the emergent structures involved in coordinated computing like security to search and act on changing data structures. Query is applicable to structured databases and directories while search is more appropriate for MAPs.

- MAPs vs Directories

MAPs are distributed, not hierarchical, read/write (dynamic), updatable anywhere, searched while directories are distributed, hierarchical, static and centrally updated, queried like DNS and LDAP.

- Real-time state vs. Historical data

In the security use-cases, systems like Web application Firewall (WAF), Firewall, Intrusion Prevention System (IPS), and Security Event Managers (SEM) subscribe to the MAP and are able to get more information and publish actionable "knowledge" back to the MAP as a result of contextual analytics; Implementation realities including such as persistence, query/search patterns, and computational demands differentiate this standard from historical stores that are suitable for non-transactional systems.

3.3. IF-MAP mechanism and operations

The three basic functionalities of IF-MAP protocol are: Publish, Search, and Subscribe.

The MAPS server is considered as central information security repository where the clients MAPC can perform the following tasks:

- Publish: Clients MAPC can store information for other clients to see on the server MAPS
- Search: Clients can search for published data using search patterns
- Subscribe: Clients MAPC can receive notification when other clients publish new data via the MAPS.

Below Figure-4 illustrates the communication flow between a Map server, a Subscriber and a Publisher.

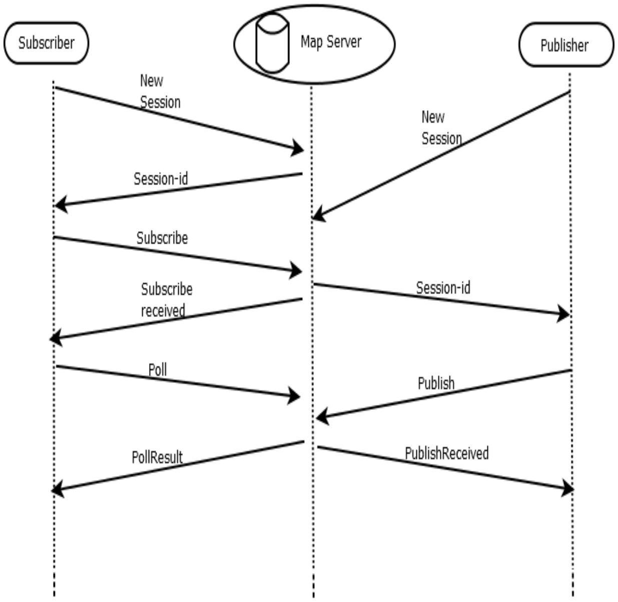

Figure 4. IF-MAP Messages Flow

Such mechanism achieves interoperability for security related data exchange as following:

- MAPC can publish new meta-data to the MAPS
- Search for meta- data
- Subscribe to specific meta-data then
- Get notified when new meta-data is published.

Security notifications are then formatted in xml, encapsulated in SOAP and sent via https, as shown below:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:ifmap="http://www.trustedcomputinggroup.org/2010/IFMAP/2">
<soap:Body>
<ifmap:response>
<pollResult>
<updateResult name="1311">
```

```
<resultItem>
<ip-address type="IPv4" value="192.168.2.102"/>
<mac-address value="03:67:23:45:99:cd"/>
<metadata>
<meta:ip-session
xmlns:meta="http://www.trustedcomputinggroup.org/2010/IFMAP-
METADATA/2"
ifmap-cardinality="multiValue"
ifmap-publisher-id="testsession123"
ifmap-timestamp="2014-06-01T14:53:50+02:00"/>
</metadata>
</resultItem>
</updateResult>
</pollResult>
</ifmap:response>
</soap:Body>
</soap:Envelope>
```

Security event xml formatted is then encapsulated in a soap envelop then sent to destination.

Such scenario as shown in Figure-5 targets getting near real-time visibility into traffic patterns based on user behavior and applications usage [9].

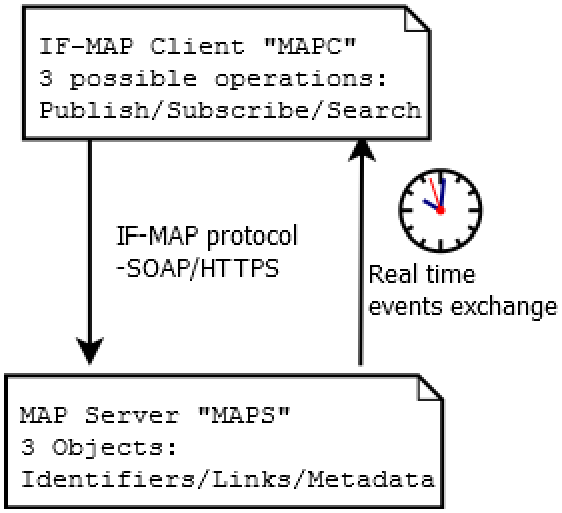

Figure 5. MAPC ←→ MAPS IF-MAP Exchange

MAPC can handle the three operations as described below:

- Subscribe: notify me when (metadata pattern) match
  -MAPC asks to be advised for searches that match when others MAPC publish new metadata
- Publish: notify others security components about changes
  -MAPC Clients store metadata into MAPS for others to consume
- Search: notify me if (metadata pattern) match

The goal is to assess traffic flows in real time and adjust the firewall policy rules to stop attacks; therefore security rules will be injected based on metadata that defines a n-tuple parameters based on (location, source IP address, destination IP address, protocol, destination port, *etc* …) to stop malicious traffic.

IF-MAP "metadata" can be associated with either an identifier or with two identifiers to build security state graph as shown in Figure-6 below.

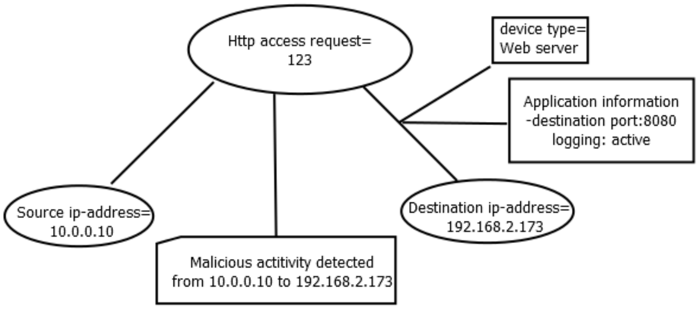

Figure 6. Dynamic Security Graph

These components can act as sensors adding data to the MAPS repository and act upon information received from other components. IF-MAP provides additional properties and security policy configuration changes over the time to contain threats [9]

4. Implementation and Use Case

Our target security architecture aims to implement collaboration between security components in a distributed local and central security context framework as shown below in Figure 7:

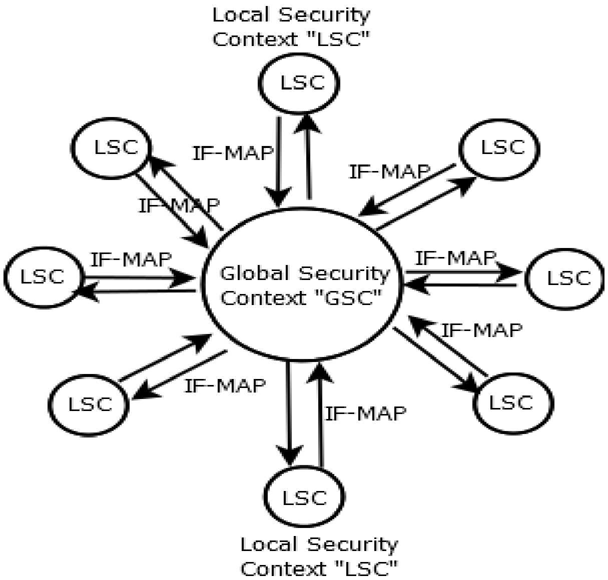

Figure 7. Global and Local Security Context Architecture

To test the local-central security concept, we setup up the following test platform based on open source tools that serves to detect attacks proactively, and then push policy changes to stop penetration in real-time.

- Omapd as a IF-MAP server (MAPS)
- Apache web server with full logging activated
- Iptables firewall as a IF-MAP MAPC
- IF-MAP plug-in installed on the Web server

This leads to stop the RFI scan before further malicious activity can be performed on the target.

In fact, to detect earlier (Remote File Inclusion) scanning activity against vulnerable web servers that supports IF-MAP and can act as MAPC to push the information in real time to the Firewall, then the Firewall can handle this by putting the source IP address in a black-list or just modify the policy access rules to stop the attacker.

Such automated actions to virtually patch vulnerable servers and guarantee their protection in real time without administrator intervention as described below in Figure 8:

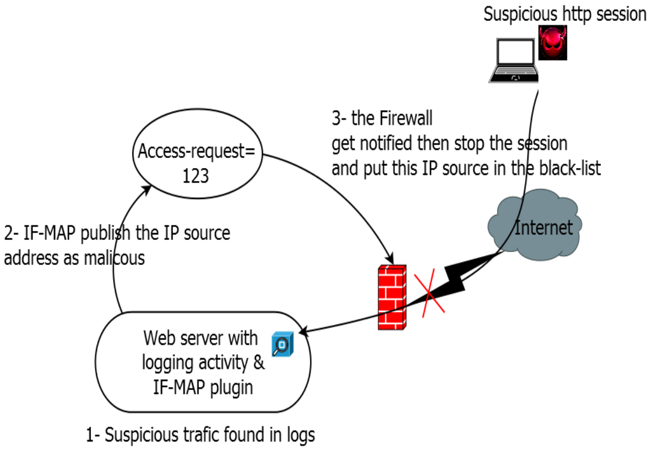
Suspicious http session
3- the Firewall
get notified then stop the session
and put this IP source in the black-list
Access-request=
123
2- IF-MAP publish the IP source
address as malicous
Internet
Web server with
logging activity &
IF-MAP plugin
1- Suspicious trafic found in logs

Figure 8. Suspicious http Session Scenario

When the scan starts, unusual activity entries in the log files are observed:

www[.]<xxx>[.]com/=http:/www.google.com/humans.txt?

www[.]<xxx>[.]com/admin/admin.php?site_url=http://www.google.com/humans.txt?

www[.]<xxx>[.]com/bin/qte_init.php?qte_root=http://www.google.com/humans.txt?

As a reaction to that abnormal behavior, our security platform automatically took the following actions:

1. The log server as a MAPC notify the MAPS to report the RFI scan against the apache web server ; this notification is done via the IF-MAP plug-in as poll action according to (figure-4);

2. The MAPS server build a security event that state the source IP address that makes this http request is suspicious then send it to the iptables firewall as Publish Received IF-MAP primitive (as previously stated in figure-4);

3. The iptables Firewall as a MAPC when it retrieves such update from the MAPS server it takes action by black-listing the attacker IP address as detailed bellow:

```
    for x in `grep -v ^# $BLACKLIST | awk '{print $1}'`; do echo "Denying $x..."
    $IPTABLES -A INPUT -s $x -j DROP
```

Where $BLACKLIST is the suspicious IP addresses sent by the server via IF-MAP plug-in.

5. Conclusion

To protect devices and applications targeted by complex attacks, collaborative security approach between a central point of correlation and local security becomes the solution key, in this perspective we propose a security platform built on a collaborative security approach between a central point of correlation and local security devices and applications, the local security context on each MAPC “device or application” becomes the "source of security events" and contributes to build the global security state in real-time in order to achieve the agility and effectively implement security controls.

Our proposition has the following strong features:

- Deep security is done in local context which the best position to detect violations
- Global security correlation is done in the central point to get better visibility about the global security
- Use an adapted collaboration mechanism local to global context security

That being said, IF-MAP is still not adopted by all security contributors, in case a security component doesn’t support it, own scripts should be build to get the security awareness job done.

Reference

[1] K. Quagliata, “Impact of Security Awareness Training Components on Perceived Security Effectiveness”, PMP, ISACA JOURNAL, vol. 4, (2011).

[2] I. Kotenko, O. Polubelova, A. Chechulin and I. Saenko, “Design and Implementation of a Hybrid Ontological”, Relational Data Repository for SIEM Systems, **(2013)**.

[3] J.-Y. Tigli, S. Lavirotte, G. Rey, V. Hourdin and M. Riviell, “Context-aware Authorization in Highly Dynamic Environments”, IJCSI International Journal of Computer Science Issues, vol. 4, no. 1, **(2009).**

[4] K. Wu and Z. Bai, “A Clientless Endpoint Authentication Scheme Based on TNC”, I.J. Information Technology and Computer Science, vol. 2, **(2010),** pp. 9-16**.**

[5] N. Parthiban, R. Ravi and Dr. B. Shekhar, “Generation of security test to find injection attacks by code review”, IJCSMC, vol. 3, Issue 3, **(2014)** March, pp. 336-343.

[6] A. Lakbabi, G. Orhanou and S. E. Hajji, “Network Access Control Technology Proposition to Contain New Security Challenges”, Int. J. Communications, Network and System Sciences, vol. 5, **(2012),** pp. 505-512.

[7] J. White, J. S. Park, C. A. Kamhoua and K. A. Kwiat, “Game Theoretic Attack Analysis in Online Social Network (OSN) Services”, Conference Proceedings, ASONAM, **(2013),** pp. 1012-1019.

[8] T. Vollmer, M. Manic and O. Linda, “Senior Member, Autonomic Intelligent Cyber Sensor to Support Industrial Control Network Awareness”, IEEE Trans. Industrial Informatics, Internet links, **(2014).**

[9] TNC IF-MAP Binding for SOAP Specification Version 2.2 Revision 9, **(2014)** March 26, http://www.trustedcomputinggroup.org.

Authors

Abdelmajid Lakbabi, a **s**ecurity specialist, Ph.D student of computer science at the University Mohammed V – Agdal, Morocco. He has spent the last 10 years working in network security field, especially the IT security audits and recommendations. With special focus in network access control, firewalling and intrusion preventions technologies, he deliverers technical presentations and trainings at the university and participates with papers and articles on network security.

Ghizlane Orhanou, an Associate Professor in the Computing Sciences Department, Faculty of Sciences, University Mohammed V – Rabat, Morocco. She received Ph.D degree in computer sciences from the University Mohammed V – Agdal, Morocco in 2011. She received in 2001 a Telecommunication Engineer diploma from Telecommunication Engineering Institute (INPT – Morocco). Her main research interests include networked and Information systems security.

Said El Hajji, Professor in the Mathematics Department since 1991 at Mathematical and Computer Sciences, Faculty of Sciences, University of Mohammed V-Rabat. Responsible of the Mathematics, Computing and Applications Laboratory. He received Ph.D degree from Laval University in Canada. His main research interests include modeling and numerical simulations, security in networked and Information systems.