Protecting Communication in SIEM systems

Valerio Formicola – Università di Napoli "Parthenope"

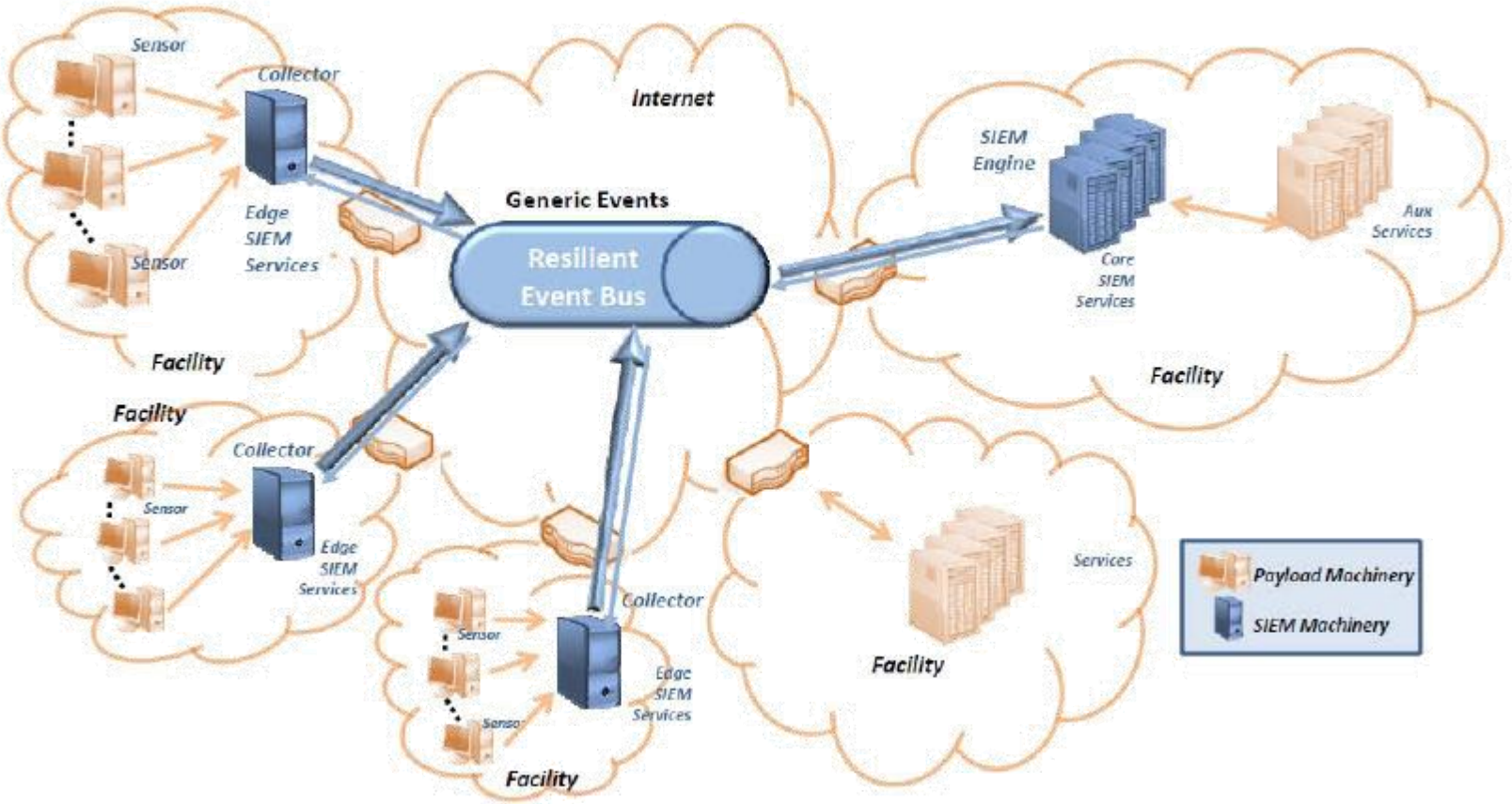
Winter School: Hot Topics in Secure and Dependable Computing for Critical Infrastructures

SDCI 2012

January 15th - 19th, Cortina d'Ampezzo, Italy

Project description

A Security Information and Event Management (SIEM) deployment

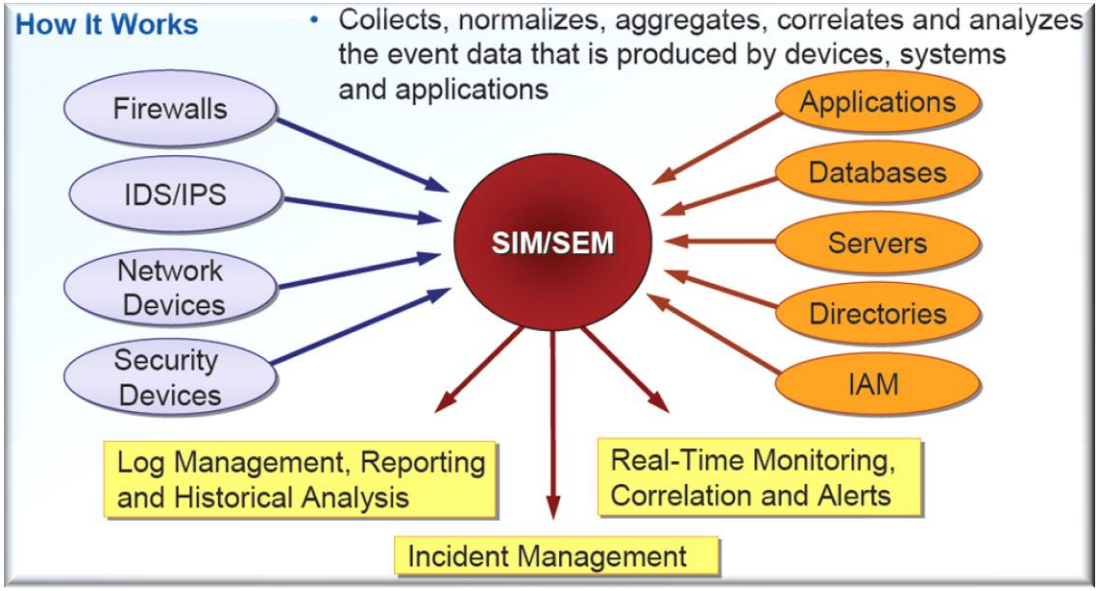


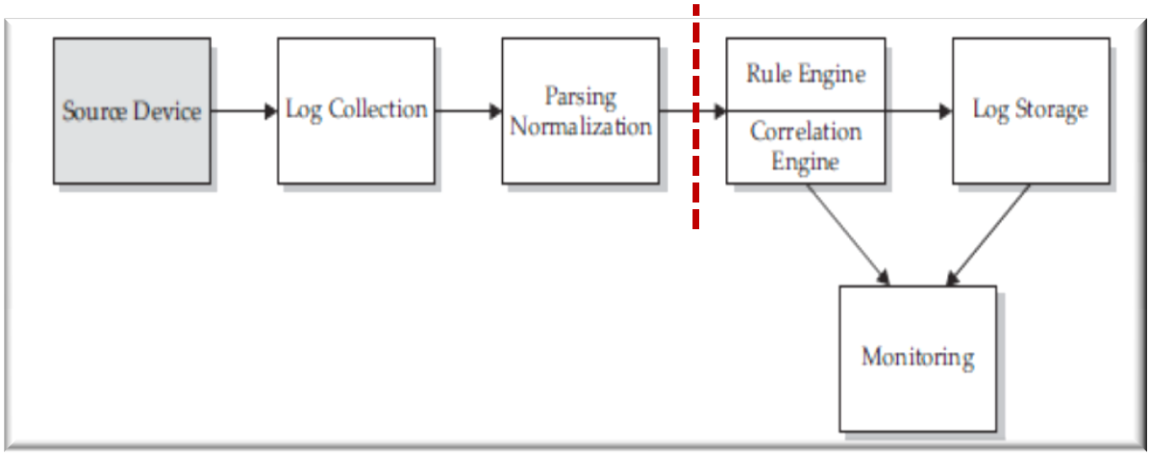
Design a solution for the protection of the communication between the collectors and the correlation engine.

SIEM systems

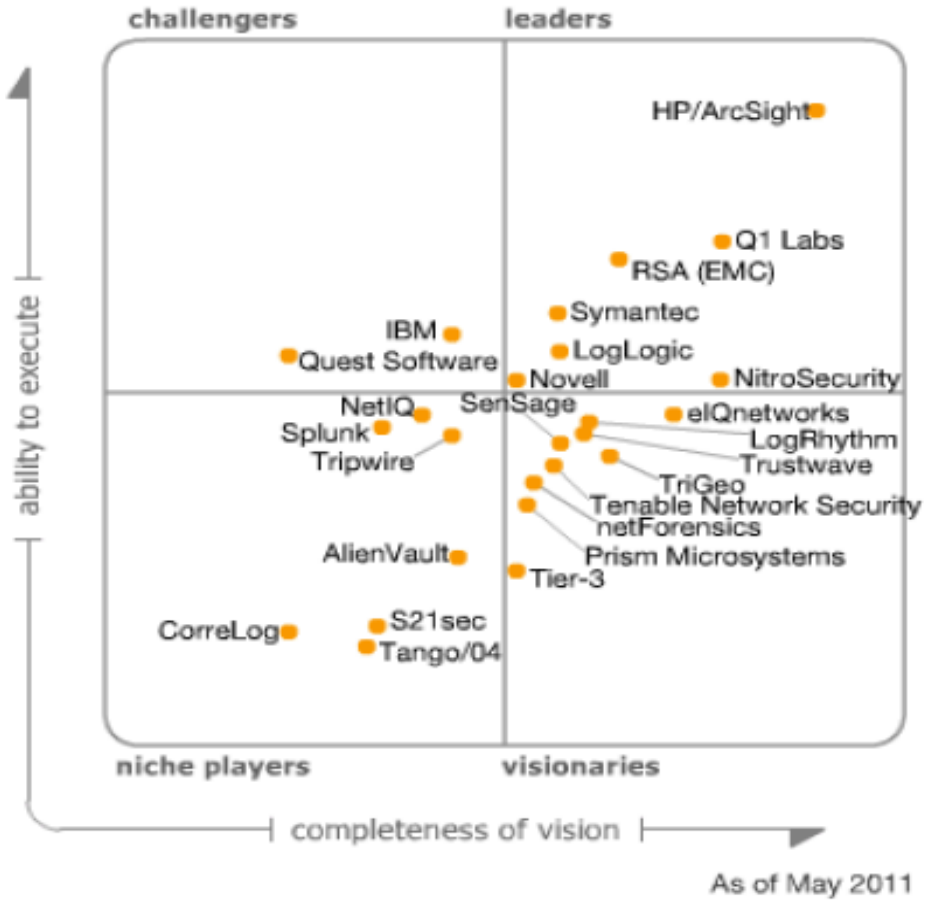
SIM + SEM = SIEM

SIM: log management and compliancy report (i.e. ISO 27001-2, PCI DSS, NERC, …)
SEM: real-time monitoring and incident management

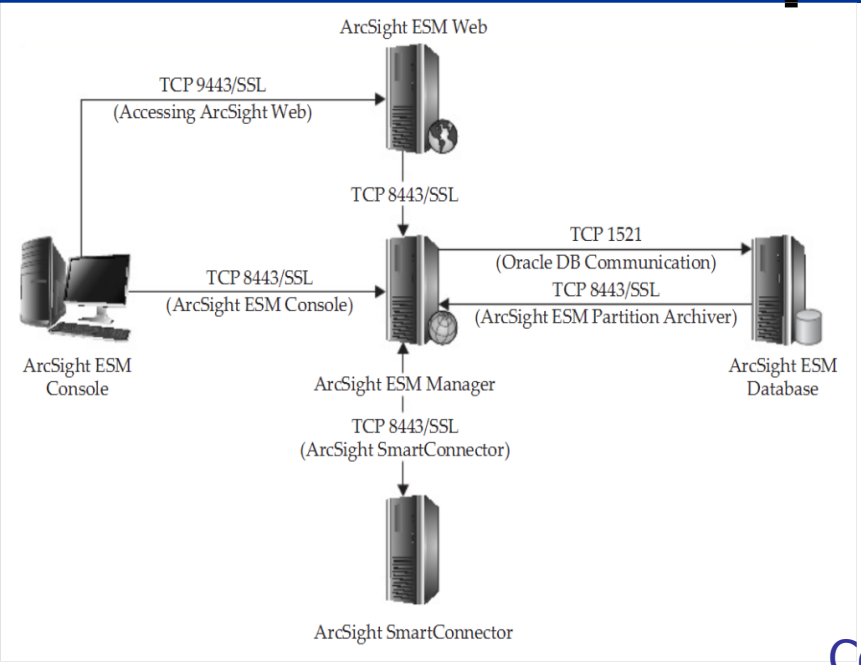


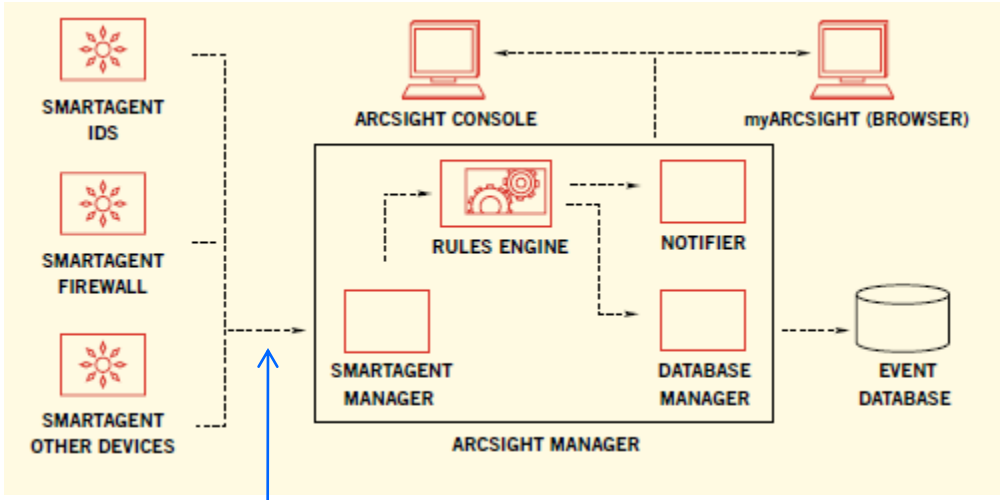


Market analysis of SIEM products



ArcSight Enterprise Security Manager (ESM): deployment





Common Event Format (CEF)

Every path between components is protected with encryption and authentication.

Communication between ArcSight ESM and ArcSight Connectors, ArcSight Consoles and Web Browsers is encrypted with 128-bit SSL encryption and 1024-bit key exchange. ArcSight ESM also supports authentication techniques such as RADIUS, LDAP, Active Directory, Two-Factor Authentication, and Public Key Infrastructure.

ArcSight protects communications by focusing on C-I-A properties.

Moreover components must be synchronized by means of NTP

ArcSight ESM: protecting communications

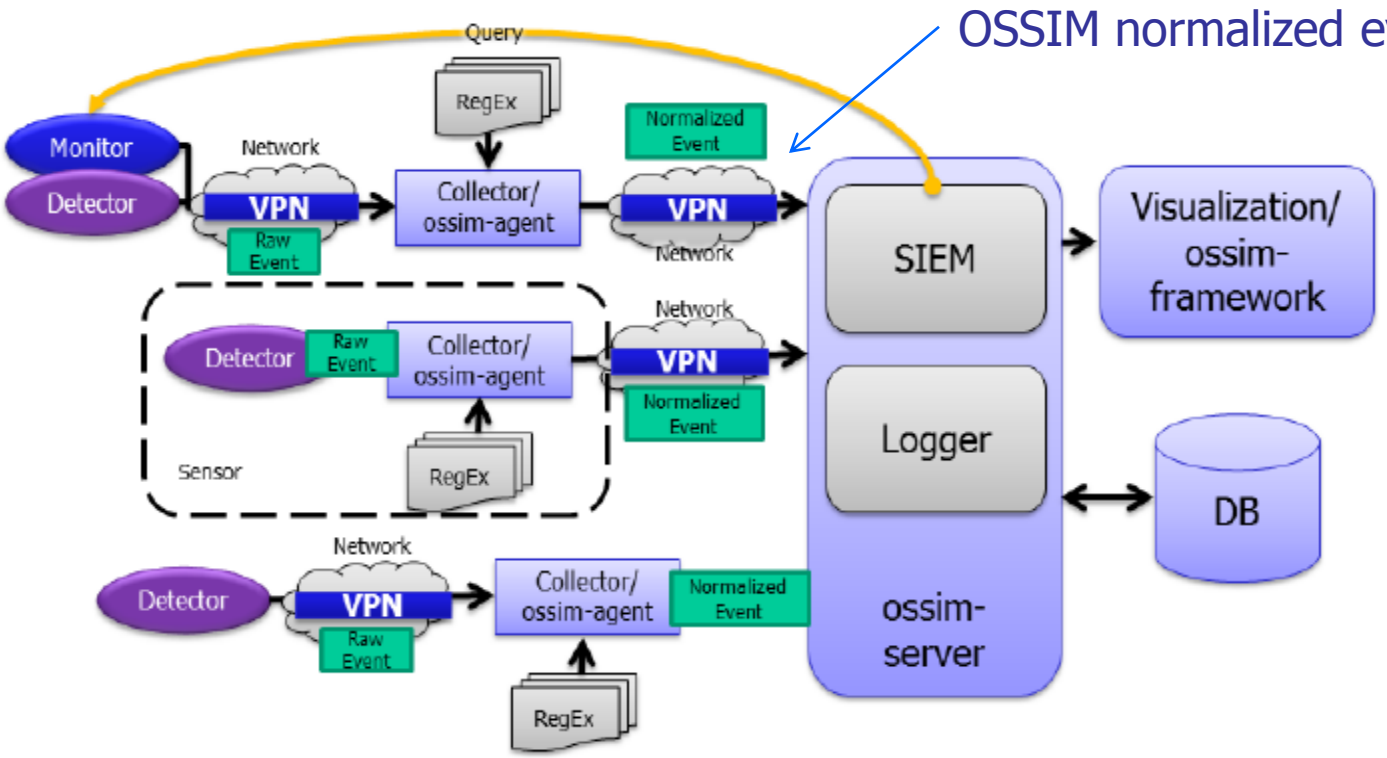
Confidentiality – ArcSight Connectors use a 128-bit encrypted SSL connection to communicate event data between other components such as ArcSight Logger and ArcSight ESM. The connector can be installed directly on the end device or within a protected DMZ to further protect the confidentiality of the log data.

Integrity – ArcSight Connectors normalize security event data in accordance with the *NIST 80092 standards* and 100% of the data from the original event is preserved and no data is changed during normalization. Additionally, ArcSight establishes chain of custody by appending a timestamp from each ArcSight component that processes the event.

Availability – ArcSight Connectors provide local caching at remote sites, which mitigates the impact of a connectivity loss between remote offices and central log aggregation points that would otherwise lead to a loss of critical event data that may be the missing link in an audit or investigation*. Connectors support automated failover to a secondary centralized ArcSight destination (Logger or ESM) in the event that the primary destination is unavailable. Logs are transmitted and stored reliably - to ensure that critical events (such as logs that indicate compliance violations) are not dropped or lost due to saturated transmissions links, lack of buffers at the source, or unreliable transport protocols.*

Availability 2 – ArcSight ESM is architected for high availability through the use of discrete components, automatic component restart, and cached event queues. *For example, if the Manager is restarted for some reason, ArcSight SmartConnectors simply cache events to send when the Manager is running again.* Likewise, the Manager will automatically suspend and resume operations in the event of Database failure. The storage system underlying the ArcSight Database component is the largest single failure point in the ArcSight ESM system. For this reason, and for any production system, ArcSight recommends a high-reliability RAID or SAN subsystem with tens of spindles, striping and redundancy. Other storage clustering solutions are available, ranging from Oracle Cluster File System (OCFS) to solutions from Veritas and EMC AutoStart.

AlienVault OSSIM: deployment and communications

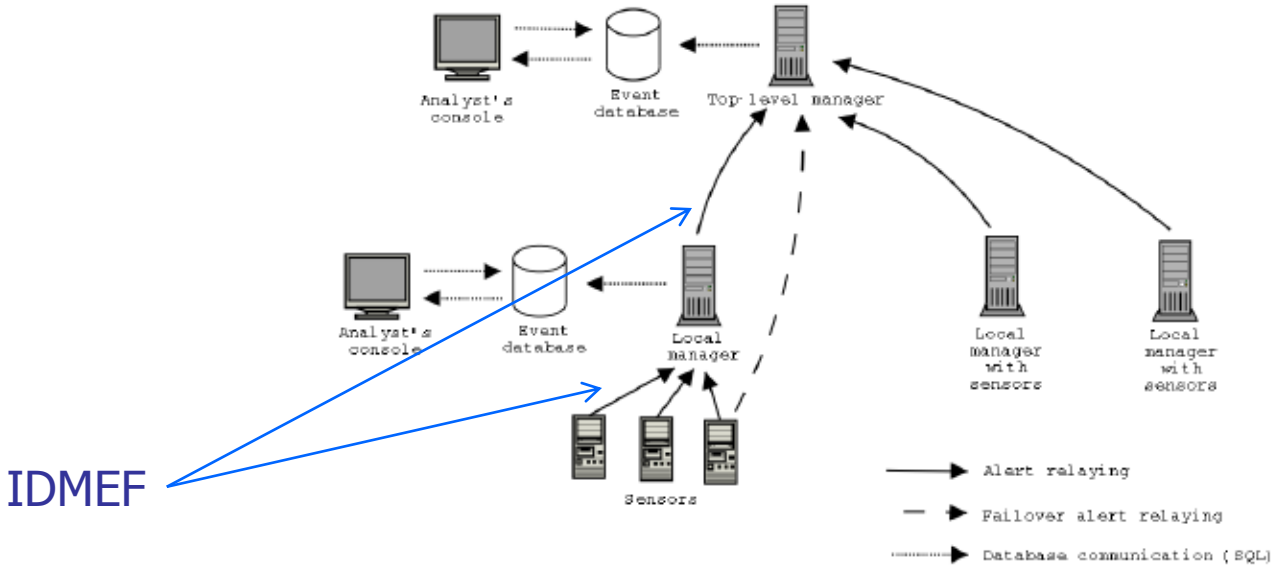


Communications may be protected by means of VPNs (typically ssh, ssl channels, IPSec).

Agents (Collectors), Probes and other components *may* be synchronized by means of NTP.

6Cure Prelude: deployment and communications

Components: Prelude Manager, Libprelude, LibprelueDB, Prelude-LML, Prelude-Correlator, Prewikka Interface, Prelude-PFLogger



Libprelude ensures that re-transmission of data is performed if an interruption occurs between any of the components in the system.

In cases when a connection to a manager is lost, the library provides a transparent mechanism which makes periodic reconnection attempts (using exponential backoff).

Libprelude can communicate with Prelude Manager over an UNIX socket (within the same host), encrypted TCP connection (using OpenSSL, preferred for communication with remote host) and unencrypted TCP connection

GAP analysis: scenario description

The edge networks can be very heterogeneous and expose Correlation components to several kinds of threats and failures.

The networks between the Collectors and the SIEM engine can be very heterogeneous, large-scale, multi-tenant, …

What gives a correct analysis (from communication perspective)?

- Correct values in the messages: the log content and a trusted time reference for meaningful correlations
- Message Order
- Timeliness (transmission): both for near real-time analysis and effective correlation process

Which kinds of failures we have to consider?

- Intermediate nodes forward wrong messages (failures or forged messages)
- Messages are re-played, re-ordered, dropped, delayed at intermediate nodes

Are TLS/SSL, IPSec, the protection mechanisms and the communication solutions adopted by the SIEM vendors able to face such issues?

GAP analysis: SSL and IPSec

•**Confidentiality.** IPsec and SSL can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key—a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.

•**Integrity.** IPsec and SSL can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a keyed cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

•**Peer Authentication.** Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host. SSL authentication is typically performed one-way, authenticating the server to the client; however, SSL VPNs require authentication for both endpoints.

•**Replay Protection**. The same data is not delivered multiple times, and data is not delivered grossly out of order.

•**Traffic Analysis Protection**. A person monitoring network traffic cannot determine the contents of the network traffic or how much data is being exchanged. IPsec can also conceal which parties are communicating, whereas SSL leaves this information exposed. Frequency of communication may also be protected depending on implementation. Nevertheless, the number of packets being exchanged can be counted.

•**Access Control.** IPsec and SSL endpoints can perform filtering to ensure that only authorized users can access particular network resources. IPsec and SSL endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.

1. These protocols don't focus on providing timely messages delivery (specifically *application level delivery deadline*), which is a key feature for a SIEM's quality -> they do the best of the underlying network (especially for SSL, which is the widely adopted solution)
2. Time reference in such systems is considered a trusted part.
3. No mechanism has been considered to protect from intermediate malicious nodes (or some other Collectors), especially important in large-scale systems
4. Vendors adopt point-to-point communications and do not abstract an Event Bus layer: they suppose to have strictly coupled components

A solution for a Reliable Event Bus

How does an Event Bus work?

When a module wishes to communicate with another module or other modules, it places a message on the Event Bus. The Event Bus takes care of delivering the message to the recipients.

Communication paradigms:

•Publish-Subscribe: Modules may subscribe to certain message types. Whenever a module publishes a message to the bus, it will be delivered to all modules that subscribed to its message type.

•Broadcast: The message will be delivered to all (other) modules.

•Point-to-point: The message has one and only one recipient.

Reliable Event Bus: an Event Bus addressing requirements in terms of

Confidentiality and Integrity properties

Fault Tolerance: i.e. Byzantine fault protection mechanisms

Delivery time constraints

Message ordering

Reliable Event Bus solution

We can consider a REB as an **overlay network**: the infrastructure is built on the underlying, unreliable network:

the components in charge of "providing" access to this overlay are the Collectors – or better, the additional services they could provide to the framework, a part of SIEM functionalities.

Design and implementation ideas:

•Event Bus: **JMS** message system can be considered as messaging system, based on publish-subscribe mechanisms

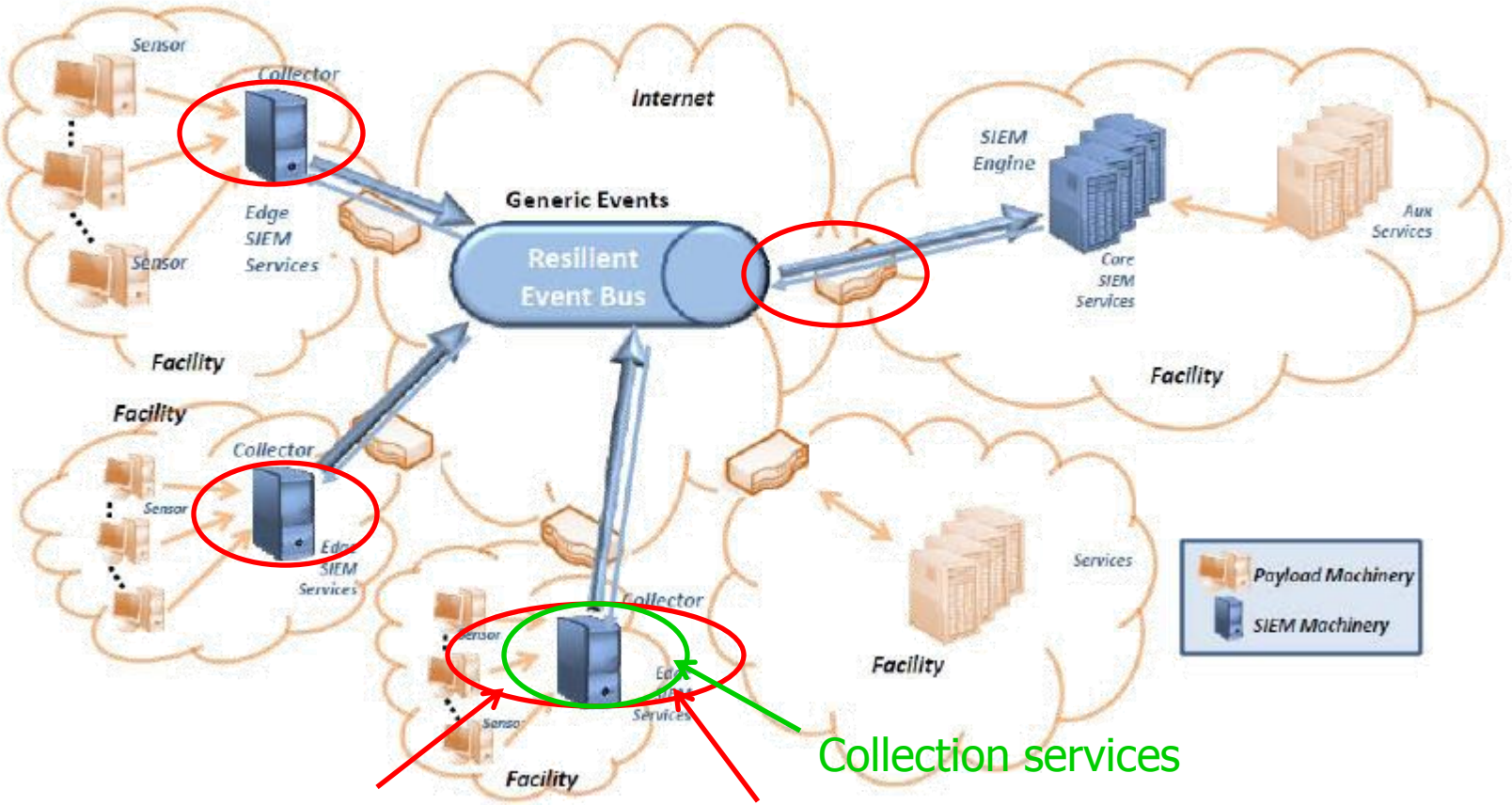
•**SSL and IPSec** - in charge of implementing several configurable mechanisms to guarantee Confidentiality, Integrity and Authenticity – can be placed at the ends of the communication: OpenSSL and the IPSec framework can do the job

•Byzantine faults in intermediate nodes can be protected by **application layer protocols** based on consensus mechanisms and broadcasting; moreover more complex mechanisms can be considered to offer message order delivery:

i.e. the Byzantine Paxos solution presented by Prof. Nuno Neves in his presentation, shows that we can also have time constraints, by using proper timers in the algorithm mechanisms

•A reliable timestamp mechanism must be provided in order enforce trustworthiness in the time reference (**GPS + NTP**?...)

Reliable Event Bus solution



References

- NIST – Guide to SSL VPNs – Recommendations of the National Institute of Standards and Technologies
- SANS Institute InfoSec Reading Room – Prelude as a Hybrid IDS Framework
- K. Zaraska - Prelude IDS: current state and development perspectives
- J. Casal – OSSIM fast guide
- Gartner GAS Core Research Note – Critical Capabilities for Security Information and Event Management Technology 2008
- ArcSight – Audit Quality SIEM solution – 2008
- Khan Consulting Inc. – Computer Security Log Files as Evidence – An Evaluation of ArcSight ESM
- Gartner - The Gartner Security Information And Event Management Magic Quadrant 2010: Dealing with Targeted Attacks
- Miller, Harris, Arper, Vanyke, Blask – Security Information and Event Management (SIEM) Implementation - McGraw Hill
- Nuno Neves (FFCUL), MASSIF Project FP7-257475 - D5.1.1, Preliminary Resilient Framework Architecture - 2011