Management of Security Information and Events in Future Internet

Andrew Hutchison, T-Systems South Africa
Roland Rieke, Fraunhofer Institute for Secure Information Technology

Workshop on Cyber Security and Global Affairs, 2011

> "*Systems Come in Threes!*
> *. . . a* judgemental system*, is involved in determining whether any particular activity (or inactivity) of a* system *in a given* environment *constitutes or would constitute - from its viewpoint - a failure.*"
> (Brian Randell, IFIP WG 10.4, Guadeloupe, 2007)

Changes and Developments. *Security Information and Event Management (SIEM)* is a key concept to identify security threats and mitigate their malicious impact. Traditional SIEM deployment occurs *within* a corporate infrastructure or it is provided by an external service provider. In such a Managed Enterprise Service Infrastructure, which is typically based on a managed IT outsource environment where events from multiple sources are collected centrally, it is also generally the case that SIEM deployment is within the realm of the provider organization and that events only pass via internal customer or service provider links. However, the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) paradigms are driving a complete re-think of the models whereby organizations deploy and manage their own infrastructure for many aspects of their computing needs.

Furthermore, Future Internet SIEM has to address the connection of *Cyber-Physical Systems (CPS)* via the Internet which extend existing critical infrastructures and form totally new types of planet-scale coaction structures.

Vision. The drive to use IaaS and PaaS paradigms implies a need to consider the implications for *deployment of SIEM in the cloud*. Following this trend, organizations could avoid Capex investments to deploy their own analysis modules, through contracting an Opex based SIEM service based on a fixed or variable monthly fee. Through the likely shift of SIEM service provision, from stand-alone organizational environments to a shared cloud processing facility, there are opportunities to make inter-organisational analyses. This in itself raises many issues in terms of *ensuring privacy and integrity of the events* of any particular company, while still gaining the benefit of being able to spot cross-company trends. The *security of a cloud based service is also critical*, and a likely stepping stone towards Public based services is that Private cloud services, from reputable large service providers, will be the preferred deployment model. In this mode, service providers have full oversight and control over event processing, while customers benefit from a lower cost, on-demand, scalable service.

Challenges. Most important, by its very nature, the SIEM itself in a hostile and unpredictable environment is a potential target for an attacker. To prevent for example the interception or blocking of SIEM event feeds, an Internet based SIEM cloud type service would have to provide quality of service guarantees to *ensure reliable and timeous arrival of security event information* from the sensors. The debate on *Internet net-neutrality* could also refer here since there could be a case for expediting *control traffic* such as SIEM event feeds.

Ideally, the SIEM system should be able to analyze upcoming security threats and violations in order to trigger remediation actions even before the occurrence of possible security incidences. Therefore, new process and attack analysis and simulation techniques are needed in order to be able to relate security relevant events and evaluate them with respect to given security requirements.

The emerging trend for the use of meshed wireless communication to connect *cyber-physical systems* to critical infrastructures and to the Internet as a whole also has to be addressed in Future Internet and Internet of Things (IoT) SIEM. This large scale connectivity, not only of sensors but also of actuators, enables totally new types of remote attacks against critical services and infrastructures with *potentially very high impact and Societal cost.* Novel adaptive response technologies are therefore needed to enable anticipatory impact analysis, decision support and to provide impact mitigation by adaptive configuration of countermeasures such as policies.

Solutions and implied RTD needs. The project MASSIF (*MAnagement of Security information and events in Service InFrastructures*), a large-scale integrating project co-funded by the European Commission, addresses these challenges. The vision of creating a next-generation Security Information and Event Management environment drives the development of an architecture which provides for *trustworthy and resilient collection of security events* from source systems, processes and applications. A number of novel inspection and analysis techniques are applied to the events collected to provide *high-level situational security awareness*, not only on the network level but also on the service level where high-level threats such as money laundering appear. An *anticipatory impact analysis* will predict the outcome of threats and mitigation strategies and thus *enable proactive and dynamic response.* The balance between the amount of processing, normalization, aggregation and analysis at *edge collectors* of an SIEM system, and the work done at the central *nerve centre* are also topics which would have to be re-considered in the context of an Internet type deployment of an SIEM system. A scalable distribution of acquisition and parallel processing, and seamless function-splitting between core engines and edge collectors, is needed.

Conclusion. In essence though, the evolving Internet provides many new questions for SIEM deployment, and from an SIEM perspective reinforces the importance of having an Internet with security and possibly differentiated service for *high priority* and *trustworthy* control traffic such as the events from an SIEM. The commercial models also change since a *service fee* needs to evolve to scale up/scale down and pay-per-use models.