Challenges for Systems of Systems Security Information and Event Management

Roland Rieke, Fraunhofer Institute for Secure Information Technology SIT

Workshop on Cyber Security and Global Affairs, July 2010

Security Information and Event Management (SIEM) is a key concept to identify security threats and mitigate their impact. Problems encountered by managed security service providers which cannot be adequately addressed by current SIEM solutions comprise insufficient resilience to withstand large scale attacks, inadequate trustworthiness of source data and inadequate disaster recovery capabilities. Furthermore, many current solutions are not able to consider and correlate events from multiple sources originating from different infrastructures and domains. A typical constraint of such systems is the restriction of SIEM to network infrastructure events, and therefore missing *awareness of attacks that exploit complex interrelations between events on different layers* such as physical events (e.g. access to buildings), application level events (e.g. financial transactions), business application monitoring, events in service oriented architectures or events on interfaces to cloud computing applications. Future multi-domain SIEM systems will additionally face new large-scale ICT dependent infrastructures deployed in sectors currently not vulnerable to Internet threats. Examples are new service infrastructures in the e-health sector, smart grids for intelligent power distribution, vehicular ad hoc networks, event-processing infrastructures for the Internet of things. The following approach addresses these challenges.

- We need to *understand the general principles* of systemic intervention, disruption and infection in highly interconnected systems of systems (SoS). For that purpose, the security and privacy requirements as well as proper multi-scale/multi-domain models describing cross-cutting dependencies and the externality each system imposes on the SoS as a whole are required. This input provides the basis for proper *identification* (is this possibly an attack). The externality, that is, the impact that a system's failure would have on others also helps to *predict the effects* of threat prevention, detection, and mitigation strategies, and thus improves the *usability of security*. Not to *sacrifice privacy for security* is a hard goal though, given that the information is needed to identify attacks and attackers.
- Novel concepts, tools and mechanisms are needed for *containment* (avoid spreading of attacks and mitigate malware epidemics) and to assist the affected entities with *erradication* (kill and erase the source and all its offsprings). A scalable variety of containment measures, such as temporary and adequately adjusted quarantine solutions for large-scale ISP networks that deal with infected end-systems, have to be developed and deployed in large scale.
- Collaborative threats could be counteracted by *collaborative analysis and defence strategies*. Scalability requires a collaborative SIEM approach which should not depend largely on centralised rule processing because this is bounding the scalability of the system. A collaborative or federated SIEM approach needs a *trustworthy management infrastructure* including mechanisms to establish and maintain trust relationships and the ability to provide a high degree of trustworthiness in the event collection components. One possibility is to establish holistically protected subnetworks with unforgeability that guarantees the authenticity of generated, processed and stored events which in turn will ensure the non-repudiation of the event source, thus enabling the use of stored events as evidence for prosecution of attackers.
- Concepts to leverage *lessons learned* (what can be learned for future attack identifications and shared with trusted entities) are currently mainly targeted at learning new attack signatures but they should also consider social and financial effects, such as the attackers business models.
- An identification of proper *business cases for cross-domain SIEM* is currently difficult. Once installed, future SIEM systems could provide much improved awareness in an entity's possible or actual unintentional external impact to a disruption of the SoS behaviour as a whole. This can be qualifiable in terms of *legal responsibility* and probably also quantifiable in terms of potential or actual costs.