AN ARCHITECTURAL BLUEPRINT FOR A NATIONAL CYBER ATTACK INFORMATION SYSTEM

Florian Skopik, Arndt Bonitz and Roman Fiedler

[1] *firstname.lastname@ait.ac.at*
The Austrian Institute of Technology, Safety and Security Department
2444 Seibersdorf, Austria

The landscape of critical infrastructures has changed dramatically in recent years. Critical infrastructures are now provided by not only a small number of national organizations, but also private companies. This situation has led to a diverse field of interconnected providers, with varying quality and security standards, providing a large attack surface for malicious activities. To counter these new threats in the cyber-security domain, collaborative protection approaches, such as cyber defence centres, are established all over Europe. In the project CAIS, we develop an architectural blueprint for the technical infrastructure of such a collaborative defence approach, and survey technologies feasible for implementation.

GOALS OF PROJECT CAIS

A multitude of research questions arise in the domain of critical infrastructure protection:

- **Attack Detection:** How can coordinated attacks be discovered? More precisely, how can we find out if systems across organizations are attacked simultaneously?
- **Situational Awareness:** How can governmental authorities properly be informed about these issues in case a critical infrastructure is being attacked?
- **Mitigation and Remediation:** How can unconcerned companies be warned and their defence systems be updated efficiently to prevent spreading attacks?

GENERAL DESIGN OF A REFERENCE ARCHITECTURE

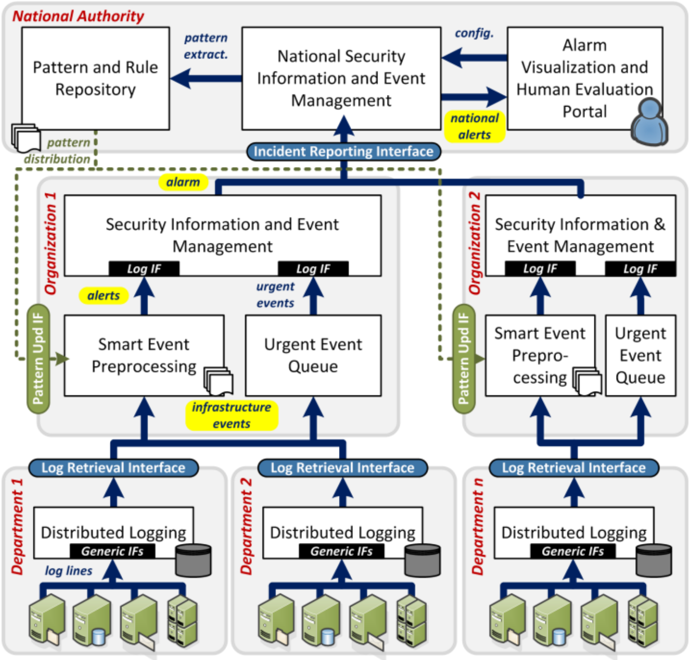

Fig.1: CAIS reference architecture

We constructed a reference architecture (Figure 1) which helps to identify concrete applicable technologies to implement an effective Cyber Attack Information System (CAIS). In particular, distributed logging is used to capture (technical) events from all relevant machines and services, including, firewall entries, application server logs, and DNS queries. Since the overall system must be highly scalable and data privacy is a major concern, each department is performing this step on its own. On the organizational level, smart event preprocessing is applied to events (e.g., filtering, ranking, correlation). This step massively reduces the amount of data for the next steps by getting rid of all irrelevant events, i.e., events that are not further handled by company policies. Furthermore, this component already allows to generate low-level alerts (e.g., multiple login failures on a single machine, etc.). The remaining events are fed into a security incident and event management solution

(SIEM), where event streams are analysed and high-level alarms generated in case of potentially malicious activities (e.g., multiple login failures across several machines, etc.).

The major novelty in this approach lies in the fact that evaluated alarms are being forwarded to a national body. Messages are encoded in either the format IODEF [1] or X-ARF [2] and thus already normalized according to predefined categories and ontologies. In case of multiple reported incidents of similar type or critical infrastructures are concerned, a national alert is generated. Additionally, the national body is predestined to act as a central point of coordination to distribute new search patterns, filters, and correlation rules to allow single organizations to tweak their anomaly detection engines and filter adverse traffic.

RESULTS AND CONCLUSIONS

The aim of the national project CAIS is to build a prototype of the presented architecture and evaluate its feasibility. We decided to utilize the open-source SIEM solution OSSIM [3], which is based on a collection of well-known open source tools. OSSIM also features an own correlation engine, the ability to create and report alarms and a graphical, web-based interface. The alert functionality of OSSIM fits nicely in the general architecture of the Cyber Attack Information System: alerts can be generated from all kinds of input events, such as firewall events, snort messages, correlated alarms or any other syslog entries. An alert can contain arbitrary information, such as the systems involved and used protocols. An alert can be propagated either via an integrated e-mail interface or can be passed to another application. With the latter option it is possible to call a script, which sends all alarms over a PGP secured mail interface to higher level SIEM solutions, such as a National SIEM.

We make use of OSSIM's extensibility to integrate new features into the SIEM: A smart event preprocessing queue and a special urgent event queue. The smart event preprocessing queue is used as a method to detect anomalies in log events. While OSSIM also provides a method to detect malicious activity in log files, the configuration is usually time consuming and requires a detailed knowledge of the monitored infrastructure. System-specific rules for correlation need to be added manually, the anomaly detection tools included (i.e. the IDS component snort or the ARP monitoring tool arpwatch) also require manual configuration. This anomaly detection component can also be used as an additional input for the correlation engine of OSSIM. For instance, if the integrated IDS triggers a security event and the anomaly detection component detects an unusual activity, OSSIM can correlate both events and generate an alarm. Since the anomaly detection is running with a short time delay, the urgent event queue has been added to the concept. It directly conveys log messages from the distributed logging solutions to the OSSIM correlation engine. Both components, the preprocessor and the urgent event queue are connected to a distributed logging engine

The default OSSIM image is based on Debian Linux. Debian uses the Advanced Packaging Tool (APT) for the retrieval, configuration, installation and updating of software packages. APT relies on repositories, were software, libraries and other components are stored and can be accessed by the APT client tools. OSSIM makes also use of APT for installing new or updated correlation rules from their repositories to a system. Of course, it is possible to add other repositories to an installation. A national body could also host their own repositories to distribute new correlation rules to installations in the field.

Acknowledgements

This work was partly funded by the Austrian security-research programme KIRAS and by the Austrian Ministry for Transport, Innovation and Technology in course of the project CAIS.

References

[1] Danyliw, R., Meijer, J., Demchenko, Y.: Rfc 5070: The incident object description exchange format (December 2007), available online: http://www.ietf.org/rfc/rfc5070.txt

[2] x-arf.org community: Extended abuse reporting format v0.2 (February 2013), available online: http://www.x-arf.org/specification.html

[3] AlienVault: OSSIM: the open source SIEM, homepage, available online: http://communities.alienvault.com