WG Intrusion and Fraud Detection for Web Services

Marc Daciér, Ulrich Flegel (chair), Ralph Holz, Norbert Luttenberger

Motivation

Web services (WS) technology bears the promise to finally bring the power of SOA middleware to the road on a large scale and across organizational domains. Big players such as Google, Amazon, SAP, and IBM have already adopted the technology. European funding agencies are strongly believing and heavily investing into WS-related technological developments and application scenarios. We expect a growing adoption and widespread use of Web services for different application areas, among them e.g. value added service composition, Web 2.0-enhanced communication systems (e.g. based on Ajax), and focused service offerings from specialized small or medium sized enterprises (SMEs).

Definitions

By the term Service-oriented Architecture (SOA) we denote a paradigm for the architecture of distributed systems, where loosely-coupled software components are encapsulated as services that can be accessed via interfaces that are published in a formal notation such that clients can easily make use of such services. WS technology is the most prominent technology for implementing a SOA. Web services come with OS- and programming language-independent XML-encoded messages, a formal service description written in the XML-based Web Service Description Language (WSDL) and other numerous standards (sometimes playfully abbreviated as WS-*) on security, composition, trust, federation, etc.

State-of-the-Art

More and more technical aspects of WS technology are being standardized, among these standards for security and security policy. Many research groups directly focus on insufficiencies of the existing standards. Still, these standards do neither address the availability of Web services, nor intrusion detection, nor fraud detection. A visible trend in the amount of work invested is applications of formal methods for model driven policy generation and verification. Another cluster of interest revolves around the problem of securing service choreography and orchestration. Finally, a lot of work is seen in the area of authorization modeling and enforcement. As a main conclusion we observe that the overwhelming amount of work addresses threat prevention. Reactive aspects have to date been largely ignored, such as detecting and mitigating at-

Dagstuhl Seminar Proceedings 08102
Perspectives Workshop: Network Attack Detection and Defense
http://drops.dagstuhl.de/opus/volltexte/2008/1498

tacks and fraud at the service layer of the computing system. A more complete study of the state of the art has been delivered by Flegel [1].

Future Directions

Clearly, there is an urgent need for methodologies and tools to counter intrusions and fraud geared towards Web services. We state that this need is urgent even though vulnerabilities of Web services are not yet exploited on a large scale. A careful analysis of potential attacks against Web services as carried out e.g. by Jensen et al. immediately shows that Web services are very vulnerable especially against DoS attacks [2].

On the other hand, while Web services and technology not only open a new window for vulnerabilities, they also offer unprecedented opportunities for the detection of intrusions and fraud. The novel idea we propose is to leverage available formal descriptions of system behavior, such as provided formal interface and policy descriptions, to generate models of acceptable behavior and detect deviations thereof by dedicated security services. Detection is comprehended as a part of the life cycle of Web services, influencing the trust evaluation of services and thereby guiding service selection. As service providers realize that their services are used less frequently as a consequence of lax internal and external security, they may implement better safeguards in order to re-gain the trust of the user community.

Challenges

- Extend WS policy specifications beyond confidentiality and integrity to enable intrusion and fraud detection
- Enable transformation of formal WS descriptions into systems for deviation detection to leverage existing specifications
- Investigate existing IDS approaches to re-use available technology for the WS environment
- Design methods for the integration of service policies across domains to monitor composite services
- Find new efficient XML processing methods and algorithms to counter the effects of resource exhaustion attacks

Recommendations

We recommend establishing a new DFG-funded priority program on communication security. WS availability and WS-oriented intrusion and fraud detection should be an important part inside such a research program.

References

[1] Flegel, U.: Web Services Security: State of the Art, Deliverable D.TEXO.8.1, BMWi funded project Theseus/TEXO, Karlsruhe, November 2007. Available via the author.
[2] Jensen, M., Gruschka, N., Herkenhöner, R., Luttenberger, N.: SOA and Web Services: New Technologies, New Standards - New Attacks. In: The 5th IEEE European Conference on Web Services (ECOWS 2007), Halle (Saale), Germany, November 2007, 26-28.