

Title / Titel

## **No quality without security - SOA Security is more than Web Service Testing**

---

Speaker(s) / Referent(s)

Schinner, Alexander A.;

Kopriva, Dominik / T-Systems GEI GmbH, Germany (DE)

---

To whom is the presentation addressed? / An wen richtet sich der Beitrag?

Decision makers, Software and Test managers, Test engineers

---

Keywords / Stichwörter

SOA, Security Testing, Secure Programming, Security Management

---

Abstract / Zusammenfassung

“The whole is greater than the sum of its parts” - SOA and Services

Can we assume that a SOA based system is secure if all services are tested for security? We think the answer is &quot;NO&quot;. So we will present in this talk additional security aspects which should be tested:

Services and Web Services

First we will give a short overview on security relevant aspect of a Service Oriented Architecture (SOA). Also, SOA promises significant benefits to today's organizations due to unprecedented flexibility and reuse of service those systems are, technically speaking, only a collection of services - internal and external to an organization - which communicate with each other. The technology of Web Services is the most likely connection technology and is heavily based on XML to create a robust connection.

Web Services and Security

For two reasons it is crucial to remember that SOA is not equal to Web Services: First service-oriented architectures are nothing new; CORBA, DCOM and other protocols have long provided similar functionality and ideas while other technologies can be used to build a service-oriented architectures. Second, and this will be the main focus of this presentation, even in a Web services based system, there are many more aspects for security testing than testing for XML, SOAP, WSDL and UDDI flaws.

Security and Testing

First, we will discuss underlying security mechanisms like encryption and decryption algorithms, key generation algorithms and basic protocols to secure a network below the application.

Second, we will point out that a Web Service is based on standard technologies, so infrastructure, operating system, the application server and all other underlying technologies must be tested for

---

security. We will explain different technologies to do these tests.

Third, we will discuss different aspects of identification, authentication and authorization in SOA environments and their influence on security testing.

Fourth, it is important to a look on the business process layer. Security on the organizational level combined with Government and Regulatory compliance, will require security testing activities to be incorporated into the entire project life cycle.

#### Summary

SOA will raise the necessity of Security testing. Testing only services themselves is not enough to answer management's question: "Is the data safe as it travels through internal and external networks?"

---

#### Biography / Biografie

Dr. Alexander Schinner is an experienced security consultant and penetration tester at T-Systems GEI GmbH. Before that, he has been the lead intrusion analyst at a German company which focuses on firewalls and intrusion detection systems for high security environments. Starting in the early 1990's, Dr. Schinner began to work in the areas of high performance computing and security. He focused on different projects, such as hardware based antivirus systems, parallel computers and fuzzy logic development systems. He held a teaching position for network engineering and microcomputer technology at Magdeburg university of applied sciences. At this time, he also built one of Germany's then largest Linux Beowulf Clusters, entering rank 23 on the worlds Top 500 Cluster List. Dr. Schinner holds the CISSP, the GIAC Certified Intrusion Analyst and the GIAC Certified Forensic Analyst.

---

#### Contact information / Kontaktinformationen

Schinner, Alexander A.  
T-Systems GEI GmbH  
Security COnsulting  
Dachauerstr. 651

80995 München  
Germany

---