Chapter 25

On Interoperability Failures in WS–Security: The XML Signature Wrapping Attack

Nils Gruschka
NEC Laboratories Europe, Germany

Meiko Jensen
Ruhr-University Bochum, Germany

Florian Kohlar
Ruhr-University Bochum, Germany

Lijun Liao
Ruhr-University Bochum, Germany

ABSTRACT

The rise in adoption of the Web Services specifications for inter-organizational business processes has led to the development of complex architecture stacks for processing Web Services messages. In particular, the proper use of the WS-Security specification poses a real challenge in terms of manageability and interoperability to adopting companies of today. This chapter is about an example of such complexity causing severe vulnerabilities in terms of security. More precise, it discusses the XML Signature Wrapping attack, which is one of the most severe attack types in Web Services. Starting with a technical description and a real-world attack incident, the chapter explains the rationale and impact of the attack, along with a brief discussion on mitigation and countermeasures.
INTRODUCTION

The last decade has seen a large paradigm shift in computer science. The classic hardware architecture of separate mainframe-style server systems largely moved towards powerful desktops, and nowadays tends to be moved to the Internet (e.g. in cloud computing).

However, along with this paradigm shift, the software design architectures have undergone a reformation as well. Among the broad list of innovations in this field, the software design paradigm of service-orientation turned out to be one of the most impacting ones. Its basic idea is simple: instead of building gigantic, monolithic applications to run a company’s business processes in a closed environment, a business process architect can break the overall process design into smaller units and make each of them separately accessible as services. These services thus provide specific functionalities for business processes in a way that the overall process design merely consists in composing the necessary set of atomic services so that they create the required process functionality.

An additional side-effect of this service-oriented business process design approach consists in that the very same services can be re-used in a set of different business processes if these happen to share some functionality. For instance, a credit card debit service can be re-used for every business process that involves credit card payments to be done.

On the technical side, the paradigm of service-orientation required an initial step: standardization of communication as well. Among the broad list of innovations in this field, the software design paradigm of service-orientation turned out to be one of the most impacting ones. Its basic idea is simple: instead of building gigantic, monolithic applications to run a company’s business processes in a closed environment, a business process architect can break the overall process design into smaller units and make each of them separately accessible as services. These services thus provide specific functionalities for business processes in a way that the overall process design merely consists in composing the necessary set of atomic services so that they create the required process functionality.

An additional side-effect of this service-oriented business process design approach consists in that the very same services can be re-used in a set of different business processes if these happen to share some functionality. For instance, a credit card debit service can be re-used for every business process that involves credit card payments to be done.

On the technical side, the paradigm of service-orientation required an initial step: standardization of communication. Only if both service user and service provider know the very same communication protocols, they are able to interact successfully. Hence, in the early years of the new millennium, the leading software companies like Microsoft, IBM, SAP, Oracle etc. decided to pose a set of specifications for digital communication, and put them to a set of globally accepted standardization organizations (e.g. W3C, IETF, OASIS Open). Based on the syntax of W3C’s eXtensible Markup Language (XML), these specifications emerged to become one of the most used communication protocol for business process communication of today: the Web Services technology.

Web Services specifications are built upon the principle of “divide and conquer” in that they provide separate specifications for separate aspects of communication (also called “separation of concerns”). For instance, the syntactical design of a service request message is defined in the SOAP specification (Box et al., 2000), whereas the list of operations a service provides is declared in an explicit document following the Web Services Description Language WSDL (Christensen et al., 2001). Non-functional properties like security and reliability of message transfer are addressed by additional specifications, namely WS-Security (Nadalin et al., 2006) and WS-ReliableMessaging (Ferris & Langworthy, 2005).

Though this overall approach of having separate specifications for separate tasks in general tends to be a good idea, it turned out that it also has its pitfalls if separate specifications that are supposed to interoperable properly turn out not to do so. This chapter is about such an issue.

In this chapter, we present and discuss the so-called XML Signature Wrapping attack (or short Signature Wrapping). This particular attack pattern works for SOAP-based Web Services communication in presence of a digital signature according to the WS-Security specification. It enables an attacker to trigger Web Service operations on behalf of a legitimate user, impersonating that user in full against the Web Service server, even without the legitimate user knowing about the attack being performed. Thus, this attack belongs to the general class of privilege escalation attacks, as the attacker gains access rights he usually should not have.

Depending on the particular scenario and the attacker’s prerequisites, the impact of an XML Signature Wrapping attack may range from performing simple Denial of Service (e.g. by deleting the legitimate user or cancelling a subscription)
Related Content

Socio-Economic Impacts of Offshore Outsourcing of Information Technology
www.igi-global.com/chapter/socio-economic-impacts-offshore-outsourcing/10058?camid=4v1a

Macro-Economic and Social Impacts of Offshore Outsourcing of Information Technology: Practitioner and Academic Perspectives
www.igi-global.com/article/macro-economic-social-impacts-offshore/1896?camid=4v1a

Extending Care Outside of the Hospital Walls: A Case of Value Creation through Synchronous Video Communication for Knowledge Exchange in Community Health Network
www.igi-global.com/article/extending-care-outside-of-the-hospital-walls/126490?camid=4v1a

Potential Benefits of Analyzing Website Analytic Data
www.igi-global.com/chapter/potential-benefits-analyzing-website-analytic/41209?camid=4v1a