Chapter 7.15
A Survey of Attacks in the Web Services World

Meiko Jensen
Ruhr-University Bochum, Germany

Nils Gruschka
NEC Europe Ltd., Germany

ABSTRACT

In the modern electronic business world, services offered to business partners as well as to customers have become an important company asset. This again produces interests for attacking those services either to paralyze the availability or to gain unauthorized access. Though founding on decades of networking experience, Web Services are not more resistant to security attacks than other open network systems. Quite the opposite is true: Web Services are exposed to attacks well-known from common Internet protocols and additionally to new kinds of attacks targeting Web Services in particular. This chapter presents a survey of different types of such Web Service specific attacks. For each attack a description of the attack execution, the effect on the target and partly the results of practical experiments are given. Additionally, general countermeasures for fending Web Service attacks are shown.

DOI: 10.4018/978-1-60566-950-2.ch010

INTRODUCTION

The rising adoption of service-orientation both in industry and academia also triggered a hype on its most prominent realization technique: the Web Services technology (Weerawarana, Curbera, Leymann, Storey, & Ferguson, 2005). Nevertheless, as with all distributed software systems, a wide spread of a particular technology also attracts individuals and organizations that try to exploit such systems for their personal benefits. Thus, in order to cope with such general security threats, every particular technology needs a specialized, appropriate security concept in order to fend attacks and mitigate security-related business risks.

For the particular case of Web Services, a large number of security-related specifications have been released by the leading standardization organizations, each targeting a special aspect of Web Services security. These specifications cover confidentiality and message integrity issues (Nadalin,

Kaler, Monzillo, & Hallam-Baker, 2006), access control and authorization for Web Service invocations (Moses, 2005), reliability for guaranteed message delivery (Ferris & Langworthy, 2005), trust establishment between cooperating organizations (Nadalin, Goodner, Gudgin, & Barbir, 2007; Nadalin & Kaler, 2006) and a lot more.

Nevertheless, the field of security for Web Services includes a lot more issues than what is currently addressed by the existing standards. As an example, the number, types and impact capabilities of known attacks on Web Services raised by far during the last years (Lindstrom, 2004). Apart from general threats like malicious Internet Service Provider employees or hijacked SOAP intermediate hosts, some very skilled, Web-Service-specific attacks have been discovered.

In this chapter, we provide a survey on some of the most severe attack types disclosed yet (cf. Table 1). We give detailed descriptions on the concepts behind the attacks, discuss their potential impact in a real-world SOA, and in the end, a brief summary on appropriate countermeasures is also presented.

The chapter is organized as follows. In the next section, the basic concepts of network based attacks are presented. Then, a list of attacks on Web Services is introduced, followed by an in-depth description on each of these attacks. Each attack description covers the attack idea, the scenario requirements, the vulnerabilities that are to be exploited, and a brief example illustrating the attack concepts. The discussion of potential countermeasures was omitted intentionally in the attack descriptions, as it is briefly done in the succeeding section. More detailed countermeasures can be found in the literature references for the specific attack types. Finally, the chapter concludes with a general statement on the chapter's topics and some future work directions.

Table 1. A list of attacks covered in this chapter

Oversize Payload	Instantiation Flooding
Coercive Parsing	Signature Wrapping
Attack Obfuscation	XML Injection
Flooding Attacks	WS-Addressing Spoofing
State Deviation	Metadata Spoofing

BACKGROUND OF NETWORK ATTACKS

In Figure 1 a typical network and application processing stack for invocations of a Web Service is shown. Every incoming message is first processed by the host's TCP/IP stack. Then, the message is passed to the application server, which commonly includes the Web Service framework. Inside the Web Service framework the message is first parsed and transformed into an in-memory representation (e.g. a DOM tree). After that, the SOAP Message Processing (e.g. WS-Addressing evaluation) and the Security Processing (mainly processing WS-Security extension, e.g. decryption of encrypted message parts or signature validation) is performed. Finally, the Web Service application logic is executed with the Web Service call contained inside the SOAP body.

As shown in Figure 1, a network service can be invoked by arbitrary users including attackers (assuming the service call is not blocked by an external instance like a firewall). Such a network based attack can target on different components inside the network or application processing stack. Well known are attacks targeting the TCP/IP stack or the HTTP handling inside the application server, e.g. Ping-of-Death (Insecure.org, 1996), TCP SYN Flooding (Schuba, Krsul, Kuhn, Spafford, Sundaram, & Zamboni, 1997) or Cookie Poisoning (Haldar, Chandra, & Franz, 2005). Such attacks threaten all services using these components, e.g. Web applications.

Web Services are of course vulnerable to those attacks but additionally to attacks targeting on the Web Service specific processing components. Below, a number of attacks are presented which