Web Services and Grid Security Vulnerabilities and Threats Analysis and Model

Yuri Demchenko, Leon Gommans, Cees de Laat, Bas Oudenaarde
Advanced Internet Research Group, University of Amsterdam
Kruislaan 403, NL-1098 SJ Amsterdam, The Netherlands
{demch, lgommans, delaat, oudenaarde}@science.uva.nl

Abstract

The paper provides an overview of available Web Services security vulnerability models and proposes a classification of the potential Grid and Web Services attacks and vulnerabilities. This is further used to introduce a security model for interacting Grid and Web Services that illustrates how basic security services should interact to provide an attack-resilient multilayer protection in a typical service-oriented architecture. The analysis and the model can be used as a basis for developing countermeasures against known vulnerabilities and security services design recommendations. The paper refers to the ongoing work on middleware and operational security in the framework of the European Grid infrastructure deployment project EGEE and related coordination groups.

1 Introduction

The area of Web Services and Grid security vulnerabilities and threats continues to be new for researchers and developers.

The paper presents an ongoing work that intends in its final result to provide recommendations to the security middleware developers how to address identified specific Web Services and Grid security vulnerabilities, first of all, vulnerabilities of the basic security services that affect Grid applications security, i.e. authentication, authorisation, confidentiality and data protection, remote access and secure communication.

Presented here Grid security vulnerabilities and threats analysis is built upon existing security vulnerabilities models and classifications. It provides a basis for a proposed security model for interacting Web Services and Grids that can be used further in proper security services design and operational procedures development.

The paper Is organized as follows Section 2 provides general overview of existing models and classifications for web application vulnerabilities and refers to the proposed classification of Web Services security threats/attacks. Section 3 extends this analysis to the specific attacks against interacting Grid and Web Services and proposes simple model that groups all attacks depending on their origin and target vulnerability. Section 4 proposes detailed model describing how security services are built into general service oriented architecture and how they interact to provide multilayer security for the Service/Resource. Finally section 5 provides initial suggestions how identified threats and/or attacks can be addressed in security middleware design and operational procedures.

2 General approach and existing models for web application vulnerabilities

The following Vulnerability-Incident life-cycle model provides illustration how vulnerability may become a potential security threat and further develop to an Incident [1, 2]:

Vulnerability => Exploit => Threat =>
Attack/Intrusion => Incident

Vulnerability is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

Exploit is a known way to take advantage of a specific software vulnerability

Threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

Attack is an assault on system security that derives from an intelligent threat**Incident** is a result of successful Attack

An attack is defined as an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. An attack may consist of one or more steps taken by an attacker to achieve an unauthorised result. A successful attack may lead to an intrusion and be

0-7803-9493-3/05/$20.00 © 2005 IEEE

further escalated as an incident.

From the life-cycle above we can understand how an attack is prepared and undertaken by attackers to target the application in general or with the specific vulnerability. The basic steps in attacker methodology are summarized below and illustrated in Fig. 1 [3]:

- Survey and assess
- Exploit and penetrate
- Escalate privileges
- Maintain access or Deny service
- Unauthorised use of Resource (including unauthorised access to information)
- Clean or forge track of activity

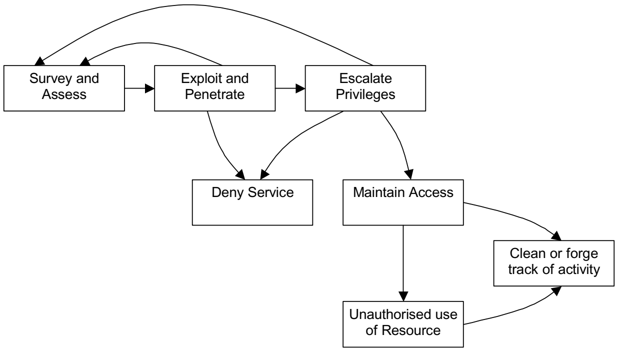

Figure 1. Basic steps for attacking methodology.

There are few known projects and initiatives that focus on vulnerability/threat analysis for web applications providing also recommendations for applications specific countermeasures. The Open Web Application Security Project (OWASP) [4] proposed a commonly recognised classification of the web application vulnerabilities in their document the "Top Ten Most Critical Web Application Security Vulnerabilities". Web Application Security Consortium (WASC) recently released the document on Web Applications threats classification that tends to establish common industry terminology and classification for known vulnerabilities [5]. The Enterprise Vulnerability Description Language (EVDL) proposed by OASIS Web Application Security TC provides detailed breakdown of the major identified vulnerabilities [6]. The guide by Microsoft "Improving Web Application Security: Threats and Countermeasures Roadmap" proposes similar Web Application Security Threats Model and Classification [7].

The Web Services vulnerability analysis and classification proposed by authors in the EGEE MJRA3.4 document [2, 3] summarise earlier works by Forum Systems and Spire Security [8, 9] and extend them with the potential WS-Security vulnerabilities. According to [2], Web Services attacks can be classified in the following way depending on targeted vulnerability groups:

- Web Service interface (WSDL) probing attacks (XWS1)
- Brute force XML parsing system attacks (XWS2)
- Malicious Content attacks (XWS3)
- External Reference attacks (XWS4)
- SOAP/XML Protocol attacks (XWS5)
- XML Security Credentials tampering (XWS6)
- Secure key/session negotiation tampering (XWS7)

3 Security Attacks Groups in Interacting Grid and Web Services

Proposed in this section security threat/attack model intends to address known vulnerabilities and concerns in current Grid middleware implementation. It is based on ongoing work in major European Grid related projects, in particular, EGEE[1] and GridPP[2] [3, 10].

Fig. 2 below provides a general model of interacting Grid and Web Services, represented by the Requestor/User and Service/Resource, and identifies the following threat/attack groups:

UCA - User Credentials Attacks comprise of possible attacks originated from and based on user credentials theft or compromise that may happen as a result of user system compromise or by intercepting user-service communication, if user credentials are not protected enough. These attacks may also be based on improper user authentication/authorisation context handling by the service.

WIA - "Wire" Intelligence Attacks include a wide spectrum of attacks that can happen if service-level communication is not protected enough against eavesdropping and interception. Beside basic service request and response, Web Services communication includes service discovery, AuthN/Z stages, security context negotiation and exchange, including session management. Most threats in WIA group come from potentially uncontrolled environment that messages may pass, especially if end-to-end service communication involves SOAP messages routing and intermediate processing. Communication and messages compromise and manipulation may lead to such classes of attacks as "Man in the middle" (MITM), credentials compromise and/or replay, session hijack, SOAP routing detour, as well as attributes/credentials probing and brute force attacks.

[1] http://egee-intranet.web.cern.ch/egee-intranet/index.html

[2] http://www.gridpp.ac.uk/

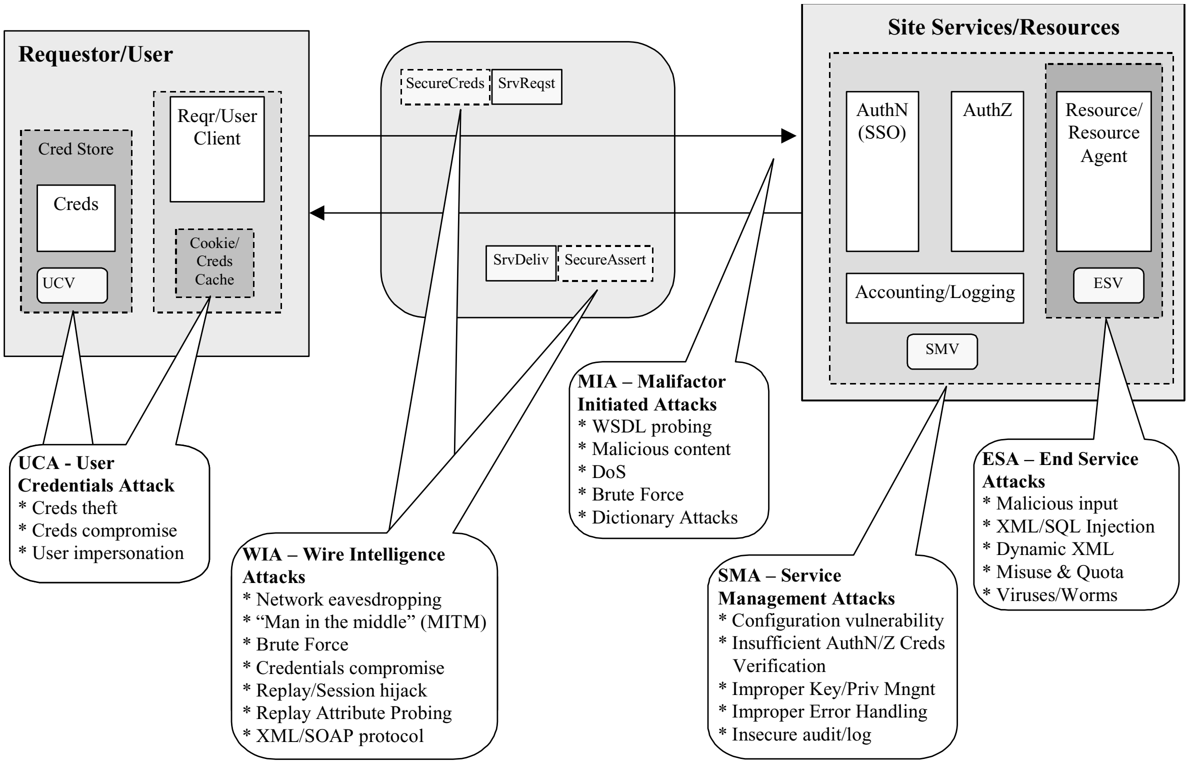

Figure 2. Threats/Attacks grouping in interacting Grid and Web services

MIA - Malifactor[3] Initiated Attacks. This group of attacks can be undertaken by a potential attacker using both traditional and Web Services specific techniques that include WSDL probing, malicious XML content, brute force and dictionary attacks to bay-pass site security services. This group also includes Denial of Service (DoS) attacks that may target all components of the site services stack. It is even more difficult to protect Grid and Web Services because of traditional network and host protection tools, like Firewalls, are transparent to SOAP communications.

SMA - Site Management Attacks include possible attacks that can be caused by improper site security services configuration and management: insufficient AuthN and AuthZ credentials verification including security context verification, improper key and privileges management and control, improper error handling that may disclose internal information about service operation, and also insufficient or insecure logging that may allow an attacker to hide or forge its activity.

ESA - End Service Attacks target known vulnerabilities in the end-service. They use different techniques to construct malicious input content, e.g. XML/SQL injection, external references in XML schema and XML documents, internal and external cross-references with XPath and XSLT instructions. Attacker may intend to violate suggested quota or acceptable use of the resource what can be prevented by proper access control and accounting. End service application can be a target and a mediator of viruses and worms carried over some types of unchecked input, and therefore antivirus protection should also be considered for Web Services applications.

As mentioned before, Web Services and Grid are also susceptible to all underlying network and hosting environment attacks, which protection is reasonably well covered with a spectrum of available products.

Table 1 provides more detailed breakdown of the identified attacks and vulnerability groups together with their mapping to the proposed in [3] Web Services attacks classification.

[3] The person with malicious intents, e.g. intruder or attacker.

Table 1. Threats/Attacks groups in interacting Grid and Web Services

Threats/Attacks groups	Threats/Vulnerabilities	XWS threats mapping
UCA – User Credentials Attacks	• Credentials theft • Credentials compromise • User impersonation	XWS6 – XML credentials tampering XWS7 – Secure key/session negotiation tampering
WIA – "Wire" Intelligence Attacks	• Network eavesdropping • "Man in the middle" (MITM) • Brute force • Credentials compromise • Replay/Session hijack • Replay attributes probing • XML/SOAP protocol	XWS5 – XML Protocol attacks XWS6 – XML credentials tampering XWS7 – Secure key/session negotiation tampering
MIA – Malifactor Initiated Attacks	• WSDL probing • Malicious content • DoS • Brute force • Dictionary attacks	XWS1 – Web Services Interface probing XWS2 – XML parsing system XWS3 – Malicious XML content
SIA – Site Management Attacks	• Configuration vulnerabilities • Insufficient authentication and authorisation credentials verification • Improper key/trust management • Improper privilege management • Improper password/ credentials recovery • Improper error handling • Insecure audit/log	XWS7 – Secure key/session negotiation tampering XWS6 – XML credentials tampering
ESA – End Service Attacks	• Malicious input • XML/SQL injection • Dynamic XML • Resource misuse and quota violation • Viruses and worms	XWS4 – External reference attacks XWS3 – Malicious XML content

4 Resource/Service Security Zones and Multilayer Access Control

In the Grid services architecture (GSA) (as well as in the general Service Oriented Architecture (SOA)), the middleware provides a media for conveying a service request and delivering a service (or its product) in a controlled and secure way to the requestor. In such a model, the service or resource is placed at the back-end of interacting components and sub-systems. Middleware provides the hosting environment and required security services that ensure that service is delivered to the authorised user/entity and in the controlled secure way.

To address identified above vulnerabilities and have an instrument to analyse security vulnerabilities and develop necessary countermeasures against possible attacks, there was a need to create a new security model that represents interacting Grid and Web Services and addresses security issues at multiple application layers/tiers.

Figure 3 illustrates how major access control components interact in a typical GSA/SOA to provide multilayer security protection. It is based on the typical implementation using container or application server for hosting Web Services based applications and provides a structured view of the Resource site security services and how they interoperate. The following security zones are defined for the Resource/Service site:

Zone R0 – zone controlled by the Resource itself that also includes local data storage and local file system; this is the zone of the Resource trust level.

Zone R1 – zone that includes Resource interface or agent and other sub-systems controlled and trusted by the Resource, which can run under administrative privilege. This also includes the policy that is specified by the Resource and stored in the Policy Authority Point (PAP). The Resource agent can also use own access control service that is not exposed in the SOA interactions.

Zone RA and **Zone RAA** – zones protected respectfully by Requestor and request authentication (RA) and authorisation (RAA). AuthN service verifies

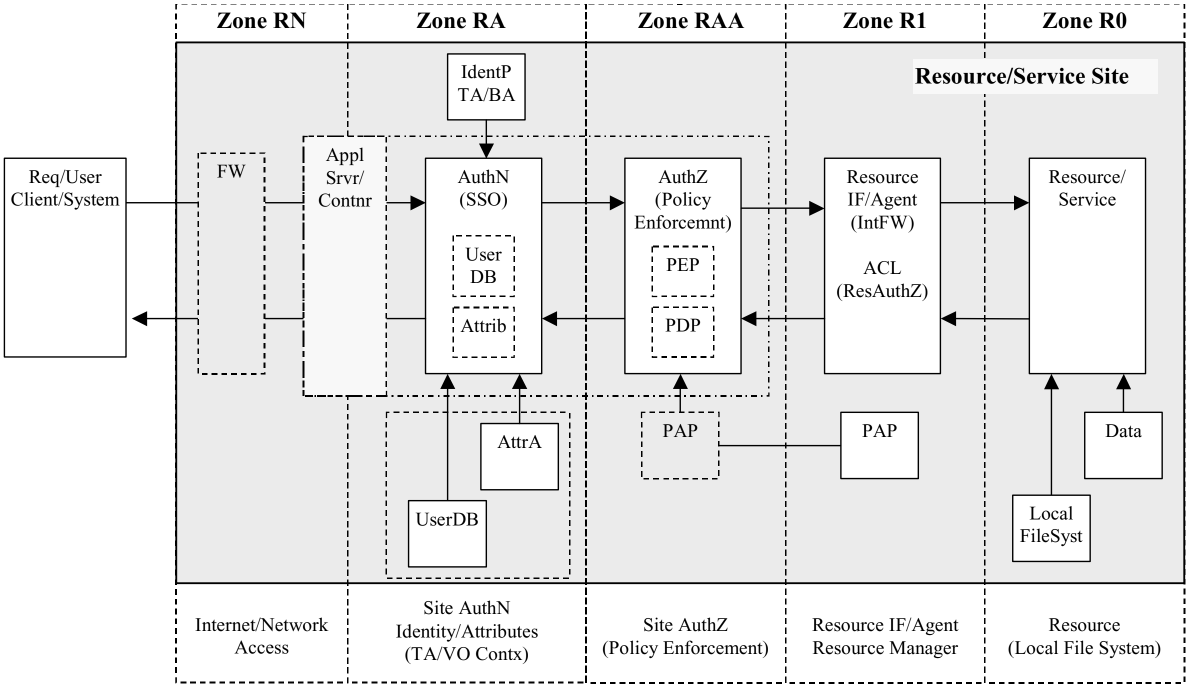

Figure 3. Service/Resource site security zones.

Requestor/request credentials using the database of registered users (UserDB) and may issue associated attributes requesting the Attribute Authority (AA). AuthZ services includes the Policy Decision Point (PDP) as a central policy based decision making authority, the Policy Enforcement Point (PEP) that provides Resource specific authorisation request/response handling and policy defined obligations execution, the PAP as a policy storage.

Zone RN – zone that includes network access facility and actually open to the world; it may also contain the Firewall that is controlled by the Firewall policy and protects the Resource site from the external attacks against the network components and malicious input to the Resource services.

It is important to note that the Requestor or request authentication can be done as a separate procedure before authorisation or as an initial step of the Requestor/Subject verification during authorisation. In the distributed access control infrastructure in order to optimise performance the Authorisation service may also issue authorisation tickets (AuthZTicket) that can be used for granting access to the following similar requests that match AuthzTicket. However, to be consistent, AuthZTicket must preserve full context of the authorisation decision including AuthN context/assertion and policy reference.

Proposed security zones definition can be applied to both distributed and local security services such as Authorisation and Authentication, which relation to the specific security zone should be maintained by proper security context management.

Depending on particular implementation. AuthN and AuthZ services can be implemented as part of application server or servlet container, e.g. in a form of message level filters, SOAP interceptors, etc., or run as an application component or separate services in the container.

Proposed security zone model extends other existing models, such as the URL Security Zones used in Microsoft Internet Explorer security model [12] or security realms concept used in the Java Servlet specification [13] and implemented in the popular servlet container Apache Jakarta Tomcat [14], and provide better granularity required for consistent security analysis of XML Web Services and Grid applications.

5 Addressing Known Vulnerabilities and Threats in Security Services Design and Operational Procedures

Proposed in the previous sections the classification and the model can be used for developing initial recommendations how to address identified Grid and Web

Services vulnerabilities and threats in both middleware security services design and operational security procedures.

It is understood that with wider Web Services and Grid deployment the reality and practice will bring to the surface and reveal new vulnerabilities and possible attacks but at least at this stage most of identified security concerns can be addressed in the design and operations. This is one of the goals of ongoing security coordination activity in the framework of the EGEE project and associated Middleware Security Group (MWSG) and Joint Security Policy Group (JSPG), which is also coordinated with the Open Science Grid (OSG) in US.

Most of mentioned above user and service configuration vulnerabilities (see UCA and SMA groups) can be avoided by the proper design and testing procedures at the development stage or discovered with the proper developed security auditing procedures. Operational procedures must also reflect special rules and procedures for security services deployment and management, first of all, concerning service and user credentials.

Attacks related to malicious input and particularly attacks against XML processing system can be addressed by so-called XML Firewalls, which are currently available from many vendors. XML Firewall provides additional functions to check data authenticity, integrity and validity at the level of inspecting SOAP messages flow [15].

Proposed in the section 4 security model intends to provide a common reference model how security services should interact to provide an attack-resilient multilayer protection for Grid and Web Services.

6 Conclusion

Presented in the paper analysis is actually one of the first attempts to create a security vulnerabilities/treats model of interacting Web Services and Grids. All existing models are mostly concerned with the application security problems at the application side only. Proposed security model addresses security issues at all application tiers by introducing security zones for basic security services that altogether define multilayer service/resource protection.

It is intended that this analysis will create a basis for further discussion and development of more detailed security models of the Grid services in general and security services in particular. Suggested future development includes extending the security model to define user site security zones and user credentials management, adding delegation and distributed authentication and authorisation services

Other specific topic to be targeted in the further security model development is concerned with the trust management in a dynamic policy enforcement infrastructure built around VO and/or transient Grid tasks or jobs.

Proposed security model and threats analysis can also be used for security risk evaluation in real Grid systems and as a basis for Operational procedures revision.

7 References

[1] Shirey R., “Internet Security Glossary”, RFC2828. May 2000. Available at http://www.faqs.org/rfc/rfc2828.txt

[2] Demchenko Y., “Grid Security Incident definition and exchange format”, EGEE MJRA3.4 Deliverable document. Available at https://edms.cern.ch/document/501422/

[3] Demchenko Y., “Web Services and Grid Security Vulnerabilities and Threats Analysis”, EGEE JRA3 Technical document. Available at https://edms.cern.ch/document/632020/1

[4] The Ten Most Critical Web Application Security Vulnerabilities. 2004 Update. - January 27th, 2004. - http://www.owasp.org/documentation/topten.html

[5] Web Application Security Consortium: Threat Classification, Version: 1.00, 2004. Available at http://www.webappsec.org/projects/threat/

[6] Enterprise Vulnerability Description Language (EVDL) v0.1. OASIS Draft, February 2005 - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=was

[7] Improving Web Application Security: Threats and Countermeasures Roadmap. Microsoft Corporation. - June 2003. - 919 p. - http://msdn.microsoft.com/library/en-us/dnnetsec/html/ThreatCounter.asp

[8] Anatomy of a Web Services Attack: A Guide to Threats and Preventative Countermeasures - Forum Systems, Inc., March 1, 2004 - http://whitepapers.itsj.com/detail/RES/1084293354_294.html

[9] Attacking and Defending Web Services, A Spire Research Report, January 2004. - http://www.forumsystems.com/papers/Attacking_and_Defending_WS.pdf

[10] Security Considerations for the Implementation of Unicode and Related Technology. Draft Unicode Technical Report #36. - http://www.unicode.org/reports/tr36/tr36-2.html

[11] Cornwal L., “GridPP Grid Security Vulnerability Detection and Reduction”. - http://agenda.cern.ch/fullAgenda.php?ida=a051137

[12] URL Security Zones, MS Internet Explorer, MSDN. - http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/urlzones.asp

[13] JSR-000154 Java Servlet 2.4 Specification - http://www.jcp.org/aboutJava/communityprocess/final/jsr053/

[14] Tomcat Security overview and analysis - http://www.cafesoft.com/products/cams/tomcat-security.html

[15] A Guide to Securing XML and Web Services. - ZapThink, LLC - January 1, 2004 - http://whitepapers.itsj.com/detail/RES/1073404572_221.html