Web Services and Grid Security Vulnerabilities and Threats Analysis and Model

Vulnerability-Incident life-cycle

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

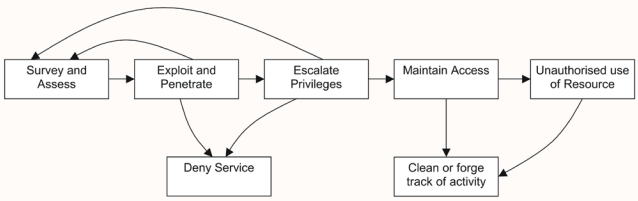
Vulnerability is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

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

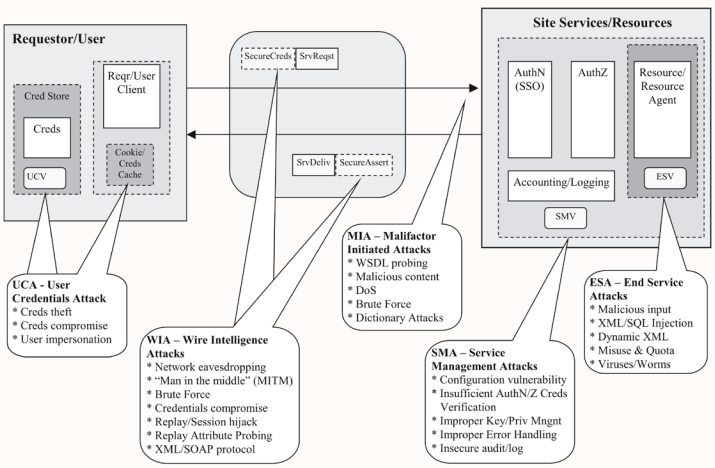
Threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

Attack is an assault on system security to evade security services and violate the security policy of a system.

Incident is a result of successful Attack.



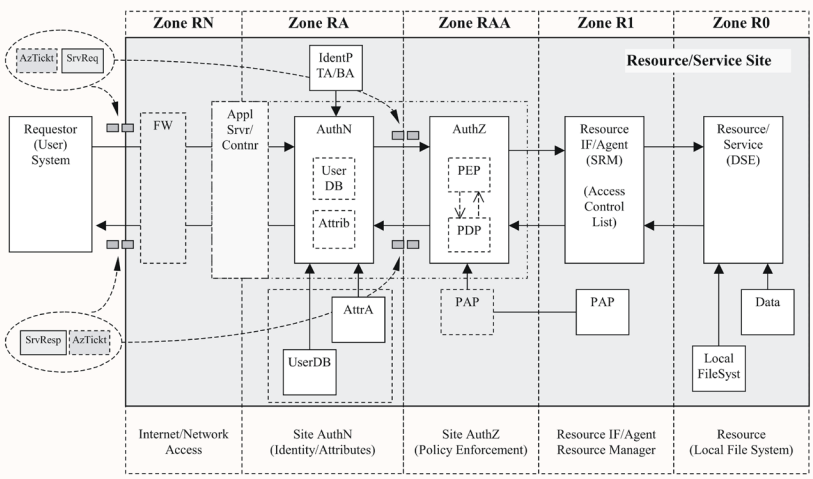
Attacks grouping in interacting Grid and Web services



Web Services threats classification and their mapping to attack groups

Category of threats/attacks	Threats	Suggested mapping to attack categories
XWS1 – Web Services Interface probing	WSDL scanning, WSDL parameters tampering, WSDL error interface probing	MIA – Malifactor Initiated Attacks
XWS2 – XML parsing system	Recursive XML document content, oversized XML document	MIA – Malifactor Initiated Attacks
XWS3 – Malicious XML content	Malicious code exploiting known vulnerabilities in back-end applications, viruses or Trojan horse programs, malicious XPath or XQuery built-in operations, malicious Unicode content	MIA – Malifactor Initiated Attacks ESA – End Service Attacks
XWS4 – External reference attacks	Malicious XML Schema extensions, namespace resolution manipulation, external entity attacks	ESA – End Service Attacks
XWS5 – SOAP/XML Protocol attacks	SOAP flooding attack, replay attack, routing detour, message eavesdropping, "Main-in-the-middle" attack	WIA – "Wire" Intelligence Attacks
XWS6 – XML security credentials tampering	XML Signature manipulation, secured XML content manipulation, Unicode content manipulation, XML credentials replay, application session hijacking	UCA – User Credentials Attacks WIA – "Wire" Intelligence Attacks SIA – Site Management Attacks
XWS7 – Secure key/session negotiation tampering	Poor WS-Security implementation, poor key generation, poor key/trust management; weak or custom encryption	UCA – User Credentials Attacks WIA – "Wire" Intelligence Attacks SIA – Site Management Attacks

Service/Resource Security zones



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 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.

Note: Access control components interaction in a typical OGSA/SOA to provide multilayer security protection requires explicit security context management because of message based and stateless character of Web Services as a SOA platform (in contrary to POSIX/host based security using process privileges implicitly)

Related EGEE/LCG activities and technical documents

XML Web Services Security Vulnerabilities/Threats classification (XWS) is the result of EGEE JRA3 Security deliverable MJRA3.4/MJRA3.6 and MJRA3.5

- Web Services and Grid Vulnerabilities and Threats Analysis - https://edms.cern.ch/document/632017/
- Grid Security Incident definition and exchange format - https://edms.cern.ch/document/632020/
- Secure Credential Storage - https://edms.cern.ch/document/638872/

EGEE JRA3: Security - http://egee-jra3.web.cern.ch/egee-jra3/
EGEE Technical Page - http://egee-intranet.web.cern.ch/egee-intranet/
Joint Security Policy Group (JSPG) - http://proj-lcg-security.web.cern.ch/proj-lcg-security/

Future developments

Proposed Security vulnerabilities and attacks classification and security model intends to provide an input to further analysis of existing and to be discovered Grid and Web services vulnerabilities, in particular, extend the security model:

- to define user/site secure credentials protection zones,
- add delegation and distributed authentication and authorisation services,
- trust management in a dynamic policy enforcement infrastructure built around VO and/or transient Grid tasks or jobs.

UvA Universiteit van Amsterdam

Yuri Demchenko
Leon Gommans, Cees de Laat
Bas van Oudenaarde

Advanced Internet Research Group

eGee Enabling Grids for E-sciencE