AON and Grid Security: XML Web Services vulnerabilities and threats analysis

RIPE51 – October 10-14 2005, Amsterdam

Yuri Demchenko <demch@science.uva.nl>
Advanced Internet Research Group
University of Amsterdam

Outline

- Motivation
- Background: Projects and Technologies
- Addressing Web Services and Grid vulnerabilities in Grid projects
- Existing classifications and models
- Proposed security threats classification and models
- Additional information (reference)

Motivation behind this presentation

- Attract attention to the new open security problem area
  - Grid and Web Services are moving to infrastructure level services
  - New end-to-end (or application-to-application) security model is identity/credential based
    - Potentially exposed to identity theft attacks and can provide really wide possibility for using compromised credentials
- Research/Grid community sees the problems but doesn’t have enough manpower and operational services focus
  - Wider awareness among networking community and ISP’s may help

Background – Projects and Activities

- EGEE (Enabling Grid for E-sciencE - http://egee-intranet.web.cern.ch/egee-intranet/) project is building the first operational worldwide infrastructure
  - For Large Hadron Collider (LHD) in CERN that since 2007 will start generating huge amount of information – about 15 Petabytes per year to be made available to nearly 2000 physicists worldwide
  - Tight cooperation with another int'l project LCG (LHC Computer Grid) and USA Open Science Grid initiative (OSG)
- Wider cooperation and outreach
  - Biomedical applications
  - National Research Networks
  - Industry partners
- Joint Security activity in EGEE/LCG/OSG
  - JRA3 (Security) and Middleware Security Group (MWSG)
  - Joint Security Policy Group (JSPG)
  - Grid Vulnerability Group (closed)

Background - Web Services and Computer Grids

- Web Services as a platform for Service Oriented Architecture (SOA) are mostly message-based and stateless
  - State and flow management are considered beyond the scope
- Computer Grids are defined as ***coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations***
  - More data and user centric and require transient/stateful processes management
  - Require (dynamic) resource and user associations
- Web Services and Networks: Similarities and Differences
  - Messaging level services are similar to networking
    - XML Routing and Session Management: WS-Addressing, WS-Routing, WS-ReliableMessaging, WS-SecureConversation, and WS-Security functionality for AuthN/AuthZ
  - Point-to-point networking model vs end-to-end Web Services model
    - Consequently, data/user centric end-to-end security model

New technology adoption by industry – trends and observations

- Industry is moving to adoption of new technology and building more business processes oriented infrastructure
  - Message and Service oriented (middleware) infrastructure
- Messaging and XML processing Middleware
  - XML/Messaging Accelerators, Concentrators and Firewalls
    - DataPower, Forum Systems, Sarvega
  - Enterprise Service Bus (proposed by Sonic Software)
    - One of successful marketing presentations of the emerging SOA infrastructure
- Traditional network equipment companies are moving to the new area to deliver flexible, secure accelerated solution for WS enabled Data Centers
  - Cisco Application Oriented Network (AON)
    - Applications and Service oriented middleware and infrastructure
  - Nortel and Juniper WS enabled networks
    - Nortel Application Switch supports SOAP and WS-Security
    - Juniper Application Acceleration platform supports XML processing
- Big ISP's and Data Centers are joining in XML based services adoption

Web Services and Grid security model

- End-to-end (or application-to-application) and data-centric security model
  - In contrary to point-to-point (host-to-host) and host-based security models in networking
    - With new attacking tools and spyware host based and p2p security model is proven to be vulnerable to credentials compromise
    - "Year 2004 is marked as the year when we lost our desktops" [somebody]
  - Currently used VPN and "secure channelling" in service/message oriented applications doesn't provide end-to-end messages security
- Security services re-use (in SOA) requires explicit security context management
  - POSIX/host based security uses security context implicitly as process privileges
- WS and Grids potentially exposed to the new kind of attacks
  - **"white collar" attacks**, in contrast to ordinary "blue collar" attacks, target vulnerabilities in applications to gain access to most valuable resources
    - Term coined by the EGEE Joint Research Activity (JRA3) group
  - Attracts another category of malifactors more interested in services/resources misuse

Current status with XWS/Grid Security Vulnerabilities analysis

Grid Operational Centers know major security vulnerabilities

- Those that are *actually* obvious
- We can expect more will be discovered when we apply regular security vulnerability analysis and risk assessment

(Already perceived) Problems

- There is no common approach/model for analysing security vulnerabilities in Web Services and Grids
- All security models and methodologies are complex and multifaceted
    - ◆ Grid is new but not unique – can benefit from already existing experience in other areas

Known Vulnerabilities and Threats Classifications

OWASP (Open Web Application Security Project) – 2003-2004

- http://www.owasp.org/documentation/topten.html

EVDL (Enterprise Vulnerability Description Language)

- OASIS WG - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=was

Web Applications Security Threats Model by Microsoft

- http://msdn.microsoft.com/library/en-us/dnnetsec/html/ThreatCounter.asp

XML Web Services Security Vulnerabilities/Threats classification (XWS)

- Proposed in MJRA3.4/MJRA3.6 and discussed in MJRA3.5 EGEE deliverables
  - 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/
- For service end-point, user client, and interacting services

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 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

XML Web Services threats/ attacks classification (1)

XWS1 – Web Services Interface probing

- WSDL scanning, WSDL parameters tampering, WSDL error interface probing

XWS2 – XML parsing system

- Recursive XML document content, oversized XML document

XWS3 – Malicious XML content

- Malicious code exploiting known vulnerabilities in back-end applications, viruses or Trojan horse programs, XSLT, malicious XPath or XQuery built-in operations, malicious Unicode content

XWS4 – External reference attacks

- Malicious XML Schema extensions, namespace resolution manipulation, external entity attacks

XML Web Services threats/ attacks classification (2)

XWS5 – SOAP/XML Protocol attacks

- SOAP flooding attack, replay attack, routing detour, message eavesdropping, “Main-in-the-middle” attack

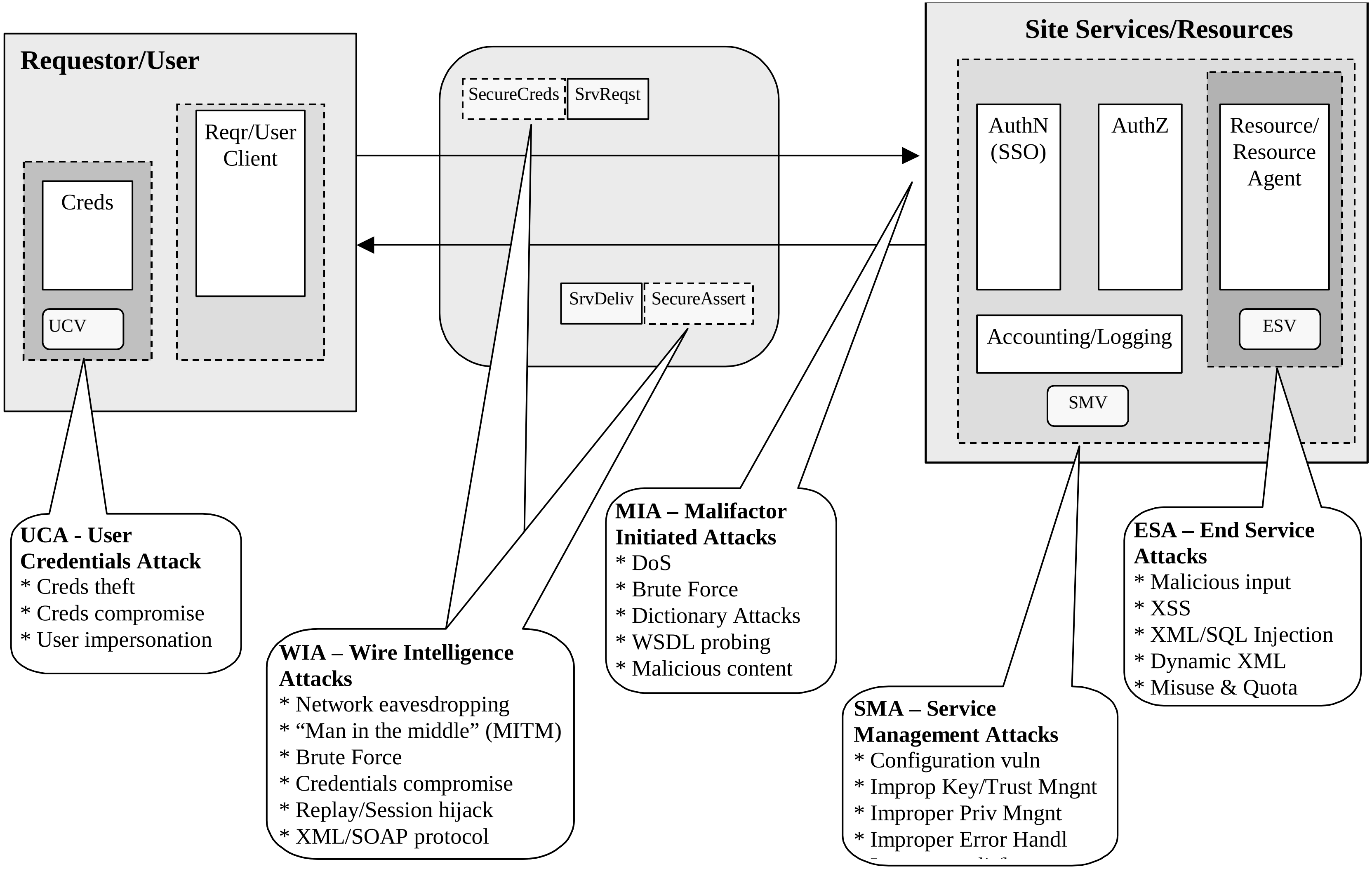
XWS6 – XML security credentials tampering

- XML Signature manipulation, secure XML content manipulation, Unicode content manipulation, XML credentials replay, application session hijacking

XWS7 – Secure key/session negotiation tampering

- Poor WS-Security implementation, poor key generation, poor key/trust management; weak or custom encryption

Threats/Attacks grouping in interacting services



UCA - User Credentials Attack
- Creds theft
- Creds compromise
- User impersonation

WIA – Wire Intelligence Attacks
- Network eavesdropping
- “Man in the middle” (MITM)
- Brute Force
- Credentials compromise
- Replay/Session hijack
- XML/SOAP protocol

MIA – Malifactor Initiated Attacks
- DoS
- Brute Force
- Dictionary Attacks
- WSDL probing
- Malicious content

SMA – Service Management Attacks
- Configuration vuln
- Improp Key/Trust Mngnt
- Improper Priv Mngnt
- Improper Error Handl

ESA – End Service Attacks
- Malicious input
- XSS
- XML/SQL Injection
- Dynamic XML
- Misuse & Quota

Threats/Attacks grouping (1)

WIA – “Wire” Intelligence Attacks

- Network eavesdropping
- “Man in the middle” (MITM)
- Brute Force
- Credentials compromise
- Replay/Session hijack
- XML/SOAP protocol

MIA – Melifactor Initiated Attacks

- Denial of Service (DoS)
- Brute Force
- Dictionary Attacks
- WSDL probing

UCA – User Credentials Attacks

- Credentials theft
- Credentials compromise
- User impersonation

Threats/Attacks grouping (1)

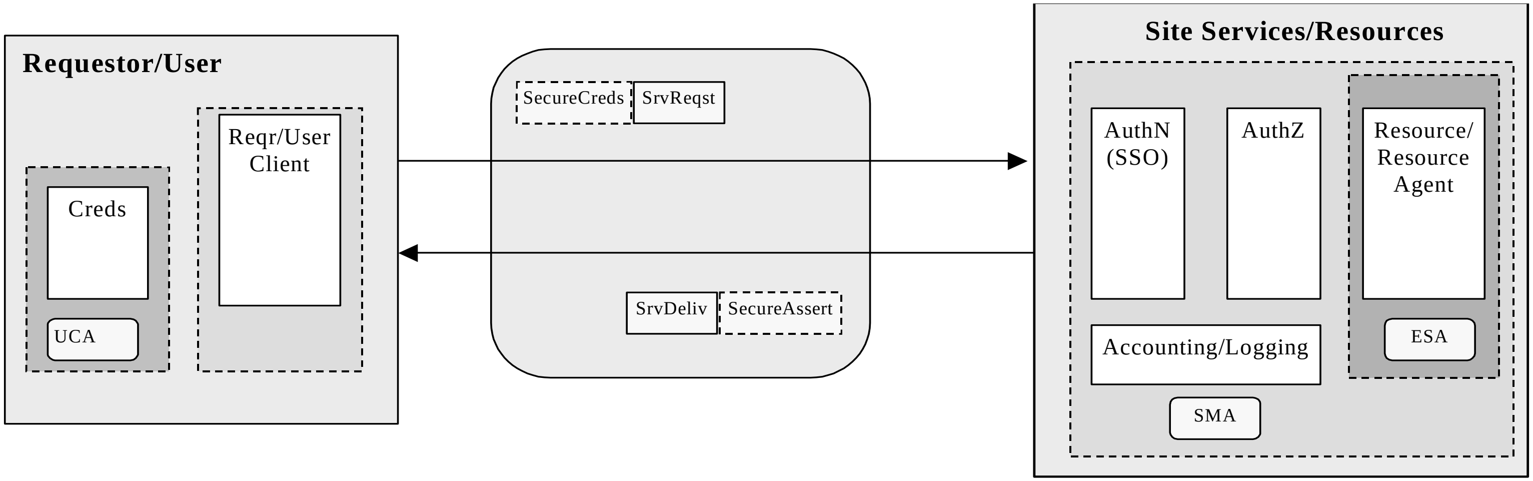
SIA – Site Management Attacks

- Configuration vulnerabilities
- Improper Key/Trust Management
- Improper Privilege Management
- Improper Error Handling
- Insecure audit/logging

ESA – End Services Attacks

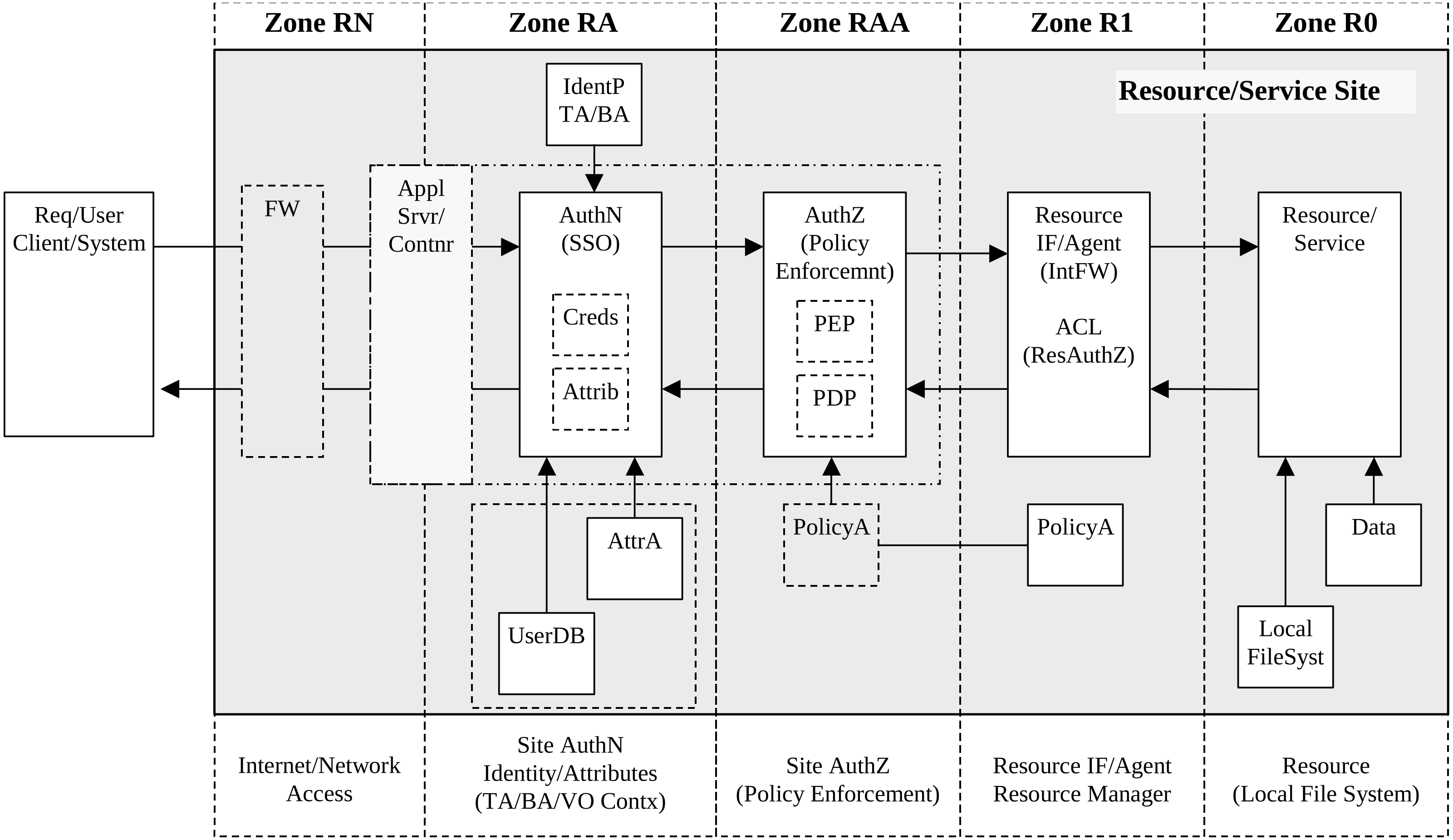
- Resource misuse and quota violation
- Malicious input
- Dynamic XML
- XML/SQL Injection
- [Cross-site scripting (XSS)]

Security models for interacting Grid/XWS services

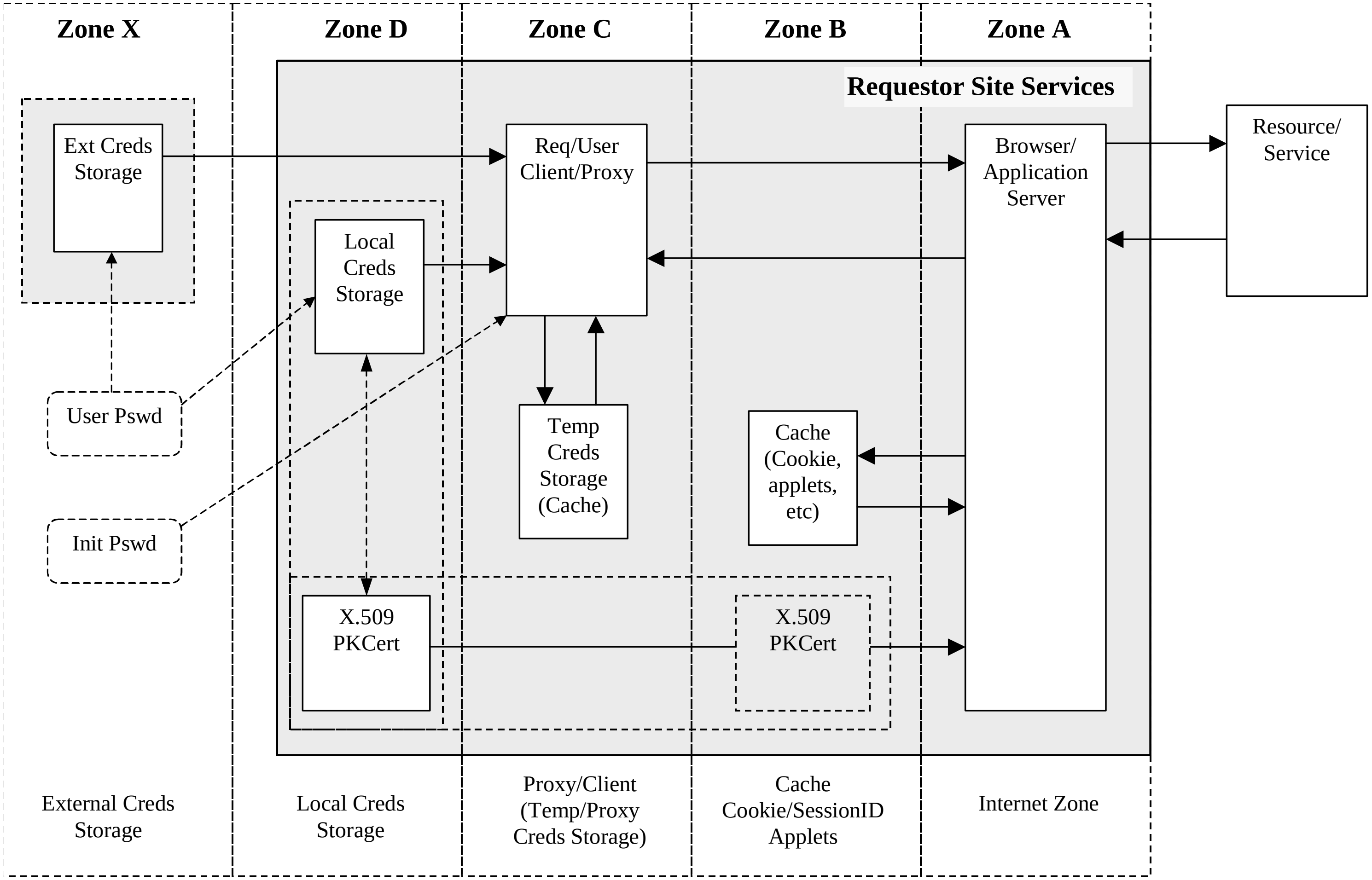


- Requestor/User site security zones
- Service/Resource site security zones

Service/Resource site security zones



Requestor/User site security zones



Example use of the proposed security models

EGEE2 Security Architecture (2006-2007)

- Message level security
- To implement dynamic trust and security context management
- Dynamic Virtual Organisations (VO) security associations

Collaboratory.nl project (CNL) – run by the Consortium of leading Dutch industry companies

- Providing secure remote access to unique analytical equipment
- Job-centric security model for Open Collaborative Environment
  - Distributed security services model and Dynamic trust management based on VO concept

NextGrid – 2004-2006

- Dynamic trust management architecture

Summary and expected development

Expected positive feedback and possible contribution from the networking/infrastructure community to address perceived XML/WS based vulnerabilities at middleware infrastructure level

Proposed Security vulnerabilities and attacks classification and security model provides an input to further analysis of existing and to be discovered XWS/Grid vulnerabilities

- Intended goal of the EGEE Vulnerability Group

Additional materials

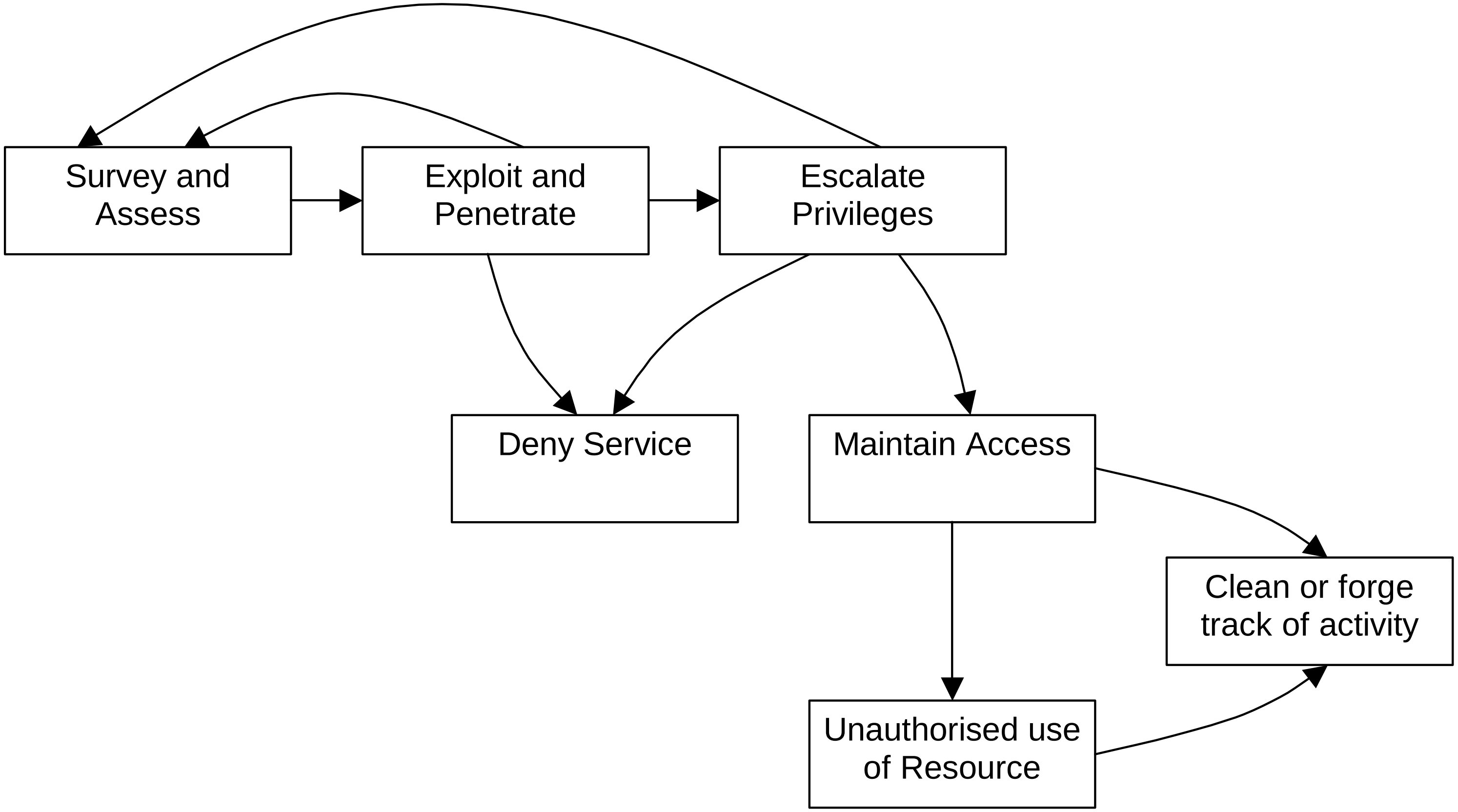
- Users vs hackers
- Basic steps in attacking methodology
- Top Ten OWASP Vulnerabilities
- Application security layers and Host security components
- WS-EveryWhere

Users vs hackers

Users go regular route

Potential hackers use any possible opportunity to bypass

Basic steps in attacking methodology



Top 10 OWASP vulnerabilities

A1 - Unvalidated Input

A2 - Broken Access Control

A3 - Broken Authentication and Session Management

A4 - Cross Site Scripting (XSS) Flaws

A5 - Buffer Overflows

A6 - Injection Flaws

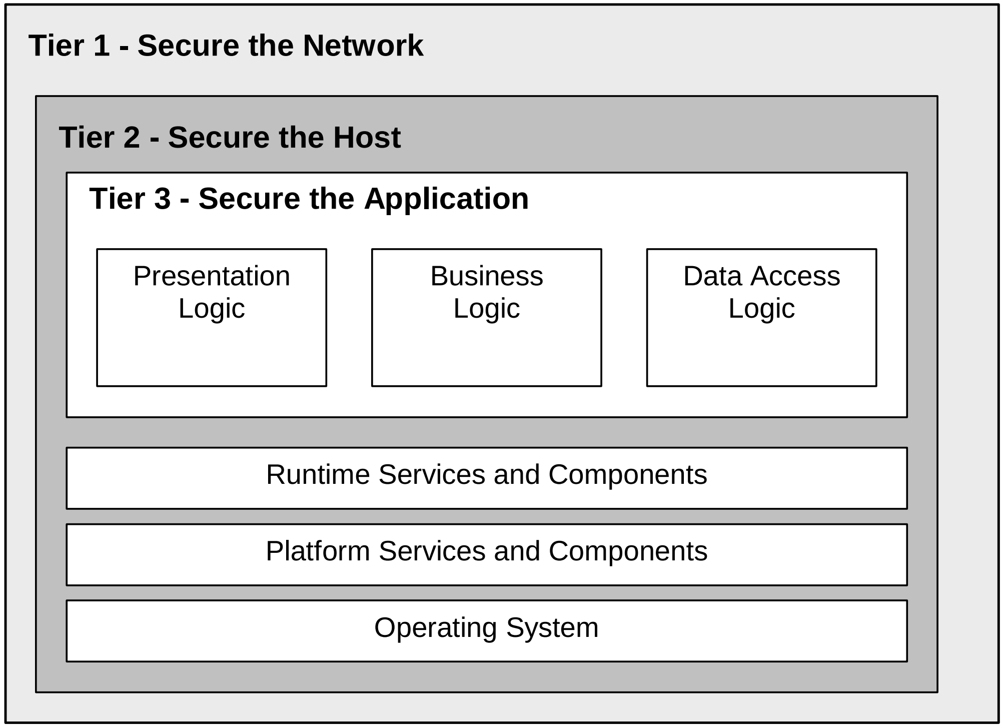
A7 - Improper Error Handling

A8 – Insecure Credentials Storage

A9 - Denial of Service

A10 - Insecure Configuration Management

Application Security Layers


Tier 1 - Secure the Network
Tier 2 - Secure the Host
Tier 3 - Secure the Application
Presentation Logic
Business Logic
Data Access Logic
Runtime Services and Components
Platform Services and Components
Operating System

Grid and application security must be build on solid base of lower layers

Grid middleware constitutes Tier 3 layer and must protect actual applications from possible attacks

Host security components

Protocols and Ports that provides network access and communication services for applications.

Common OS Services

Files and Directories

User Accounts and privileges

Registries

Auditing and Logging

Patches and Updates management

So, any WS-Alternative to WS-EveryWhere ?

Quoted from "The Loyal WS-Opposition" (2004/09/18) at
http://tbray.org/ongoing/When/200x/2004/09/18/WS-Oppo

So here's what I'm going to do. I'm going to stay out of the way and watch the WS-visionaries and WS-dreamers and WS-evangelists go ahead and WS-build their WS-future. Because I've been wrong before, and maybe they'll come up with something that WS-works and people want to WS-use. And if they do that, I'll stand up and say "I was WS-wrong."

BUT do we have WS-Alternative to:

- Services and runtime decoupling and integration?
- End-to-end and Message/Document/Data centric security model?
- Customer driven or provider independent security model?
- Ontologies/Semantics/Namespace context management?