(Re-thinking) Security Models
for
Complex Resource Provisioning and
Grid based Applications

Yuri Demchenko
System and Network Engineering Group
University of Amsterdam

1 April 2008, UvA, Amsterdam
Outline

• Background – security research and practice
• Basic uses cases - Extending edge of security practices and theory
  ◆ Collaborative Virtual Laboratory environment
  ◆ Extending User Controlled Security Domain in Virtualised Workspace Service (VWSS)
  ◆ Pilot Job submission and execution in Computer/Cluster Grids
  ◆ Multidomain Complex Resource Provisioning (CRP)
  ◆ UPVN and Multilevel Secure Networks – Area to investigate
• Two basic security models (TCB and OSI/Internet) and related standards
• Policy Obligations – bridging two fundamental security models

• New/(less) known security mechanisms for building integrated security
  ◆ Combining TCB and OSI security models for managed objects/processes
  ◆ Trusted Computing Platform Architecture (TCPA)
  ◆ Identity Based Cryptography (IBC)
Security Research and Practice

- We all know many basic security concepts and models
  - BUT each research project typically brings new problems that require new approaches
  - Good result if it is resulted in proposing and formalising a new model
    - We can use for further projects and development
- Implementing basic concepts in a specific environment or for specific tasks may require extending and sometimes re-factoring existing models
What’s beyond AuthN/Z services - Application vs Security service view

- **Authentication** – first/initial step in accessing a system or handling service request
  - Creating process, invoking service or object
  - Retrieving user attributes
  - In general, creating security context for further command/service execution

- **Authorisation**
  - Applied to user commands/actions, or managed objects
  - Starting/executing process/job/request
  - Creating AuthZ session and AuthZ context
    - Attribute mapping and policy Obligations

- **Managing security and AuthZ context**
  - User AuthZ session – e.g. web browser cookie
  - Process environment – e.g. Unix processes environment
  - Managed Object property – e.g. job, running code permissions, agents
Collaborative Virtual Laboratory Environment

- “Micro” actions in remote instrument control, e.g. surface investigation with electronic microscope
  - Method – AuthZ session management
  - Mechanism – AuthZ ticket (similar to cookie in browser)
- Project/experiment and user centric security
  - Method - Binding project/experiment security context to the signed business agreement
  - Mechanism – Business and/or Trust anchor (BA/TA)
- Experiment workflow and dynamic/changing security context
  - E.g. depending on the experiment stages: specimen scanning, data processing, visualisation, report

Experiment Description as a semantic object defining attributes for the workflow/job, user association in a form of VO, access control policy

Trust domain based on Business Agreement (BA) or Trust Anchor (TA)

This approach can use recently standardised WS-Agreement (WSAG) protocol
Different sides of Security and Trust

- Modern paradigm of remote distributed services and digital content providing makes security and trust relations between User and Provider more complex.
- User and Service Provider – two actors concerned with own Data/Content security and each other System/Platform trustworthiness.
- Two other aspects of security/trust:
  - Data stored vs Data accessed/processed
  - System Idle vs Active (running User session)
- Think about real life analogy:
  - *Diplomatic/President’s visit*
  - *Combat mission*
User-controlled Virtual Workspace Service (VWSS-UC) – Proposed 3 layer model

- Trust Anchors: T0 (TPM) – TA1 (VM/VWSS) – TA2 (Application) – TA# (User)
- WVSS session and Application AuthZ sessions
Grid Security Overview – Major concepts/mechanisms

- Grid is for sharing computing resources and unique resources in the distributed heterogeneous environment by means of resource and user virtualisation
  - Grid Security is built around Web Services Security
- Authentication in the Grid is based on PKI and can use different (user) credentials (PKI, SAML, Kerberos tickets, password, etc.)
- Delegation (restricted and full)
  - Job submission in Grid environment requires (credentials) delegation
  - Implemented using X.509 Proxy Certificate (Proxy or PC)
  - Proxy is generated by the user client based on user master PKC or Proxy
  - Limited delegation chain (typically not more than 10)
- Authorisation is based on VO attributes
  - Simple AuthZ session management by using Proxy or Short Lived Creds (CLC) together with CRL
- Trust is an important component of PKI based AuthN and Delegation
  - Trust relations are represented by a certificate chain
  - Typical Proxy Certs chain
    \[
    \text{PKC (DN1, CA)} \Rightarrow \text{PC (DN2, (ACa) , PKC)} \Rightarrow \text{PPC (DN2, (ACb) , PC)} \Rightarrow \ldots
    \]
  - International Grid Trust Federation GridPMA – http://www.gridpma.org/
Use Case for “gLEExec on the WN” – Pilot Job

Use case that doesn’t fit typical policy based access control in Grids
- Make pilot job subject to normal site policies for jobs

VO submits a pilot job to the batch system
- the VO ‘pilot job’ submitter is responsible for the pilot behavior
  - *this might be a specific role in the VO, or a locally registered ‘special’ user at each site*
- Pilot job obtains the true user job, and presents the user credentials and the job (executable name) to the site (gLEExec) to request a decision on a cooperative basis

Preventing ‘back-manipulation’ of the pilot job
- make sure user workload cannot manipulate the pilot
- project sensitive data in the pilot environment (proxy!)
- by changing uid for target workload away from the pilot
Obligations in Access Control and Management

Obligations in access control and policy based management
- Obligated policy decision
- Provisional policy decision

Access control in Grid and Policy Obligations
- Account mapping
- Quota assignment
- Environment setup/configuration

General Complex Resource provisioning
- Fixed, Time-flexible, Malleable/"Elastic" Scheduling
- Usable Resource

Other/general
- Accounting, Logging, Delegation
Policy Obligation is one of the policy enforcement mechanisms

- **Obligations** are a set of operations that must be performed by the **PEP** in conjunction with an **authorization decision** [XACML2.0]

Obligations enforcement scenarios

- Obligations are enforced by PEP at the time of receiving obligated AuthZ decision from PDP
- Obligations are enforced at later time when the requestor accesses the resource or service
  - Require use of AuthZ assertions/tickets/(restricted proxy?)
- Obligations are enforced before or after the resource or service accessed/delivered/consumed
  - Not discussed in current study/document – refer to OGSA AUTHZ-WG discussions
Proposed Obligations Handling Reference Model

Generic AuthZ service model
PEP – Policy Enforcement Point
PDP – Policy Decision Point
PAP – Policy Authority Point
OH – Obligation Handler
CtxHandler – Context Handler
(S, R, A, E) – components of the AuthZ request
(Subject, Resource, Action, Environment)
Obligations Handling Stages

Obligation0 = tObligation => Obligation1 (“OK?” , (Attributes1 v Environments1))
=> Obligation2 (“OK?” , (Attributes2 v Environments2))
=> Obligation3 (Attributes3 v Environments3)

Obligation0 – (stateless or template)

Obligations are returned by the PDP in a form as they are written in the policy. These obligations can be also considered as a kind of templates or instructions, tObligation.

Obligation1 and Obligation 2

Obligations have been handled by Obligation handler at the SCAS/PDP side or at the PEP side, depending on implementation. Templates or instructions of the Obligation0 are replaced with the real attributes in Obligation1/2, e.g. in a form of “name-value” pair.

- The result of Obligations processing/enforcement is returned in a form of modified AuthzResponse (Obligation1) or global Resource environment changes
- Obligation handler should return notification about fulfilled obligated actions, e.g. in a form of Boolean value “False” or “True”, which will be taken into account by PEP or other processing module to finally permit or deny service request by PEP.
- Note. Obligation1 handling at the SCAS or PDP side allows stateful PDP/SCAS.

Obligation3

Final stage when an Obligation actually takes effect (Obligations “termination”). This is done by the Resource itself or by services managed/controlled by the Resource.
Introducing SCAS as external AuthZ service called from protected environment changes simple security model

- AuthN/AuthZ-glexec flow needs analysis
- Behind each (SCAS) policy should be clear operational model

SCAS is verified to be compatible with the XACML policy and PDP

- XACML uses pluggable security service model (i.e. called from major Service)
- glexec is a kind of gateway/border device
Multidomain Network/Complex Resource Provisioning

Provisioning sequences
- Agent (A)
- Polling (P)
- Relay (R)

Token based policy enforcement
GRI – Global Reservation ID
AuthZ tickets for multidomain context mngt

NRPS – Network Resource Provisioning System
DC – Domain Controller
IDC – Interdomain Controller

AAA – AuthN, AuthZ, Accounting Server
PDP – Policy Decision Point
PEP – Policy Enforcement Point
TVS – Token Validation Service
KGS – Key Generation Service
Multidomain Network Resource Provisioning (NRP)

NRPS – Network Resource Provisioning System
DC – Domain Controller
IDC – Interdomain Controller

Provisioning sequences
- Agent (A)
- Polling (P)
- Relay (R)

Token based policy enforcement
GRI – Global Reservation ID
AuthZ tickets for multidomain context mngnt
T - Token

AAA – AuthN, AuthZ, Accounting Server
PDP – Policy Decision Point
PEP – Policy Enforcement Point
TVS – Token Validation Service
KGS – Key Generation Service
OSI/Internet Security vs TCB Security - Two basic security concepts

Open Systems and Internet
Open Systems Interconnection (OSI)
  Security Architecture
    • ISO7498-2/X.800

Independently managed interconnected system
Trust established mutually or via 3rd party
PKI and PKI based AuthN and key exchange

Concept of the Security Context

Trusted Computing Base (TCB)
Models Bell-LaPadula and Biba
Certification criteria TCSEC/Common Criteria (1984)
  • A1, B1, B2, B3, C1, C2, D

Trust relations

Subjects

Objects

Audit file

Similar model should be proposed for WS SOAP based security services and mechanisms

Layers model for above Application layer are uncertain


OGSA Security Model Components (2002-2006)
- GFD.80 - OGSA version 1.5, Section 3.7 Security Services
- Re-states Web Services Security roadmap

**WS-Security stds specify using SOAP header for security related issues**
- Considered as orthogonal to major service

![Components of Grid Security Model](image-url)
Multilevel Security (MLS)

Originated from Defense community, three classification levels are defined

**Clearance level**
- indicates the level of trust given to a person with a security clearance, or a computer that processes classified information, or an area that has been physically secured for storing classified information.
- Clearance level indicates the highest level of classified information to be stored or handled by the person, device, or location.

**Classification level**
- indicates the level of sensitivity associated with some information, like that in a document or a computer file. The level is supposed to indicate the degree of damage the country could suffer if the information is disclosed to an enemy.

**Security level**
- generic term for either a clearance level or a classification level.
Reference Monitor (RM) Concept

Proposed by J.P. Anderson in the report “Computer Security Planning Study” (1972)

RM property provides a basis for Multi-Level Security (MLS)

- **Complete mediation:** The security rules are enforced on every access, not just, for example, when a file is opened.
- **Isolation:** The reference monitor and databases must be protected from unauthorized modification.
- **Verifiability:** The reference monitor’s correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and isolation.

**RM concept is a basis for TCB certification**
Multi-Level Security Models

Bell–LaPadula (BLP) model
- No write down
- No read up
Focus – Confidentiality
- Mandatory Access Control
Applicability – Data

Biba model
- No write up
- No read down
Focus – Integrity
Applicability – (Open) Data and Control/Mngnt

Known flaw – not protected against insider “worm” virus

TCSEC Common Criteria
- A1 – B3 + formally/mathematically verified design
- B1-B3 – Multilevel security, Formal security model, Mandatory AC
- C1-C2 – Discretionary access control model, auditable user activity
- D – minimal protection
- Currently replaced by ISO 15408 Evaluation Assurance Level (EAL)
TCSEC/ISO Common Criteria

TCSEC Certification Criteria
- A1 – B3 + formally/mathematically verified design
- B3 – Clear security model and layered design, Security functions tamperproof, Auditing mandatory
- B2 – Least-privilege access control model, Certifiable security design implementation, *Covert channels analysis*
- B1 – Labelled security protection, MAC-BLP + DAC
- C2 – Discretionary access control model, auditable user activity
- D – minimal protection

Currently replaced by ISO 15408 Evaluation Assurance Level (EAL)
- EAL1: Functionally Tested
- EAL2: Structurally Tested
- EAL3: Methodically Tested and Checked
- EAL4: Methodically Designed, Tested and Reviewed
- EAL5: Semiformally Designed and Tested
- EAL6: Semiformally Verified Design and Tested
- EAL7: Formally Verified Design and Tested

EAL1-4 – commercial systems, EAL5-7 - special systems (EAL4 circa C2)
- Windows NT (EAL4+) and many routing and Unix systems certified for EAL4
Clark – Wilson Integrity Policy

Criteria for achieving data integrity (primary target for reliable business operation)
- Authentication of all user accessing system
- Audit – all modifications should be logged
- Well-formed transactions
- Separation of duties

Enforcement Rules
E1 (Enforcement of Validity) - Only certified TPs can operate on CDIs

**E2 (Enforcement of Separation of Duty)** - Users must only access CDIs through TPs for which they are authorized.

E3 (User Identity) - The system must authenticate the identity of each user attempting to execute a TP
E4 (Initiation) - Only administrator can specify TP authorizations

Certification Rules
C1 (IVP Certification) - The system will have an IVP for validating the integrity of any CDI.
C2 (Validity) - The application of a TP to any CDI must maintain the integrity of that CDI. CDIs must be certified to ensure that they result in a valid CDI

C3 - A CDI can only be changed by a TP. TPs must be certified to ensure they implement the principles of separation of duties & least privilege
C4 (Journal Certification) - TPs must be certified to ensure that their actions are logged
C5 - TPs which act on UDIs must be certified to ensure that they result in a valid CDI

TP – transformational procedure; IVP – integrity verification procedure; CDI – constrained data Item; UDI - unconstrained data Item
Security technologies for building integrated security

- Combining TCB and OSI security models for managed objects/processes
  - Security context management with AuthZ tickets/assertions
  - Adding security context/attributes to managed objects
    - Revisiting COPS (Common Open Policy Service) protocol
- Trusted Computing Platform Architecture (TCPA)
- Identity Based Cryptography (IBC)
TCG Trusted Computing Platform

Promoted by the Trusted Computing Group (TCG)

- Basis for building and managing controlled secure environment for running applications and processing (protected) content
  - https://www.trustedcomputinggroup.org/home
- Standards for trusted network, client, server and mobile agent
- TMP software stack (TSS) defines API’s for remote access, Identity Mngnt, PKI, Secure e-mail, file/folder encryption, etc.

TCG components

- **Trusted Platform Module (TPM)**
- “Curtained memory” in the CPU
- Security kernel in the OS and security kernel in each application
- Back-end infrastructure of online security servers maintained by hardware and software vendors

**Trusted Network Connect (TNC)** – to enforce security policies before and after endpoints or clients connect to multi-vendor environment
Trusted Platform Module (TPM)

Chip built-in into the computer system or a smartcard chip
- Can be considered as a platform tied “root-of-trust” and used for trusted platform registration and integrity assurance

Provides a number of hardware-based cryptographic functions
- **Asymmetric key functions** for on-chip key pair generation using hardware random key generation; private key signatures; public key encryption and private key decryption
- An **Endorsement key** that can be used by a platform owner to establish that identity keys were generated in a TPM, without disclosing its identity
- **Direct Anonymous Attestation (DAA)** that securely communicates information about the static or dynamic platform configuration, which is internally stored in TPM in the form of hashed values (based on Zero-knowledge cryptography)
- Monotonic counter and the tick counter to enable transaction timing and sequencing
- Protection of communication between two TPM’s
- Secure key/data backup to another TPM
PKI vs Identity Based Cryptography (IBC)

Uses publicly known remote entity’s identity as a public key to send encrypted message or initiate security session

- Initially proposed by Shamir in 1984 as an alternative to PKI
  - Shamir is one of the RSA inventors in 1977 (Rivest, Shamir, Adleman)
- Identity can be email, domain name, IP address
- Allows conditional private key generation

Requires infrastructure different from PKI but domain based (doesn’t require trusted 3rd party outside of domain)

- Private key generation service (KGS)
  - Generates private key to registered/authenticated users/entities
- Exchange inter-domain trust management problem to intra-domain trust
Identity Based Cryptography (IBC)

Available implementations

Voltage Identity-Based Encryption (C based)
- Used in Microsoft Exchange Server

Eyebee by Univ Ireland (Java)
- Tested by us and will be implemented in IDC

Strong motivation for privacy concerned applications
- E.g. patient-doctor communication

1. Encrypt email with the public key of Bob: bob@b.com
2. Bob requests the private master key of the relation alice@a.com and bob@b.com
3. Private master key of bob@b.com

Key Server

Alice
alice@a.com

Send Secure email

Bob
bob@b.com
Multidomain Network Resource Provisioning (NRP)

Provisioning sequences
- Agent (A)
- Polling (P)
- Relay (R)

Token based policy enforcement
GRI – Global Reservation ID
AuthZ tickets for multidomain context mngnt
T - Token

NRPS – Network Resource Provisioning System
DC – Domain Controller
IDC – Interdomain Controller

AAA – AuthN, AuthZ, Accounting Server
PDP – Policy Decision Point
PEP – Policy Enforcement Point
TVS – Token Validation Service
KGS – Key Generation Service
The paper provides a use case for TBN to support Multi-Level Security (MLS) as a concept associated with MAC (Mandatory Access Control: user clearance must match document classification)

- MLS network must ensure dataflow (between applications) binding to the security levels
- Suggests implementation using TCPA, FPGA

Paper (from military domain) by A. Alkassar, C. Stueble
“Security Framework for Integrated Networks”
http://krypt.cs.uni-sb.de/download/papers/AISt_03.pdf
Questions and Discussion
Additional materials
XACML Policy format

- Policy target is defined for the triad Subject-Resource-Action and may include Environment
- Policy may contain Obligation element that defines actions to be taken by PEP on Policy decision by PDP