

Grid Computing

Security Primer

Paul A. Farrell
Fall 2006

Paul A. Farrell 2006 KENT STATE Grid Computing 1

Introduction to Security

- What do we mean by security anyway?
 - Secure from whom?
 - From systems administrator? From rogue employee? Mr. H. Acker...?
 - Secure against what?
 - Denial of Service? Identity theft? Legally sensitive data acquisition?
 - Or even MPs leaving laptops on the Tube...
 - Secure for how long?
 - “I recommend overwriting a deleted file seven times: the first time with all ones, the second time with all zeros, and five times with a cryptographically secure pseudo-random sequence. Recent developments at the National Institute of Standards and Technology with electron-tunnelling microscopes suggest even that might not be enough. Honestly, if your data is sufficiently valuable, assume that it is impossible to erase data completely off magnetic media. Burn or shred the media; it's cheaper to buy media new than to lose your secrets....”

Paul A. Farrell » 2006 Applied Cryptography 1996, page 225 KENT STATE Grid Computing 2

Introduction to Security

- Secure technology ≠ secure system
 - System using 2048+ bit encryption technology, packet filtering firewalls, PMIs, PKIs...
 - on running laptop in unlocked room
 - ... on PC with password on “post-it” on screen/desk
 - We have heard worse than this, naming no names!
 - Famous quote to muse over:
 - “...if you think that technology can solve your security problems then you don't know enough about the technology, and worse you don't know what your problems are...”
 - » Bruce Schneier, Secrets and Lies in a Digital Networked World

Paul A. Farrell 2006 KENT STATE Grid Computing 3

Goals of Security

1. Prevention
 - prevent attackers from violating security policy
2. Detection
 - detect violation of security policy
3. Recovery
 - stop an attack, assess and repair damage, hopefully continue to function correctly even if the attack succeeds
 - Often involves lock-down until fixed

Paul A. Farrell 2006 KENT STATE Grid Computing 4

Fundamental Terms

- Key terms that are typically associated with information security
 - Data
 - Confidentiality
 - Integrity
 - Availability
 - People and Actions
 - Authentication
 - Authorisation
 - Assurance
 - Non repudiation
 - Auditability/accounting
 - Other
 - Trust
 - Reliability
 - Privacy

All are important for Grids but some applications may have more emphasis on certain concepts than others

Paul A. Farrell 2006 KENT STATE Grid Computing 5

Information (Data) Security

- Confidentiality
 - Securing content of packet during communication to prevent malicious users from stealing the data
 - Usually involves encryption
- Integrity
 - protection of data from modification by unauthorised users
 - can be checked through the use of digital signatures
 - Grid also raises more general questions e.g. provenance i.e. maintaining the integrity of chains or groups of related data
- Availability
 - degree to which a system, sub-system, or equipment is operable and in a usable state

Paul A. Farrell 2006 KENT STATE Grid Computing 6

People Related

- Authentication
 - ensuring users are who they say they are
- Authorisation
 - making a decision about who may have access to data or services
- Assurance
 - confidence that the security system functions correctly
- Non-repudiation
 - ensuring that a user can not deny doing action
- Auditability
 - tracking what a user does to data or services

Paul A. Farrell 2006 KENT STATE Grid Computing 7

Fundamentals - Authentication

- Authentication
 - the establishment and safe propagation of a user's identity in the system
 - e.g. so site X can check that user Y is attempting to gain access to resources
 - Note does not check what user is allowed to do, only that we know (and can check!) who they are
 - Masquerading always a danger (and realistic possibility)
 - Need for user guidance on security
 - Password selection
 - Treatment of certificates
 - Hardware tokens
 - ...
 - Is anonymity required?
- Authentication on the Grid is achieved with Public Key Infrastructures (PKIs)

Paul A. Farrell 2006 KENT STATE Grid Computing 8

Fundamentals - Authorization

- *Authorization*
 - concerned with controlling access to services based on policy
 - Can this user invoke this service making use of this data?
 - Complementary to authentication
 - Know it is this user, now can we restrict/enforce what they can/cannot do
 - Many different contenders for authorisation infrastructures
 - Access Control Lists (ACS)
 - PERMIS
 - VOMS
 - CAS
 - AKENTI
- Authorisation on the Grid must be scalable
 - This means delegation is desirable

Paul A. Farrell 2006 KENT STATE Grid Computing 9

Fundamentals - Assurance

- *Assurance*
 - allow the requester of a service to decide whether a candidate service provider meets the requesters' requirements
 - security, trustworthiness, reliability, or other characteristics
 - can be implemented through certificates signed by a trusted third party

Paul A. Farrell 2006 KENT STATE Grid Computing 10

Fundamentals – Non-repudiation

- *Non-repudiation*
 - ensuring that a contract, especially one agreed to via the Internet, cannot later be repudiated by one of the parties involved
 - In particular that it can be verified that the sender and the recipient were the parties they claimed to be

Paul A. Farrell 2006 KENT STATE Grid Computing 11

Fundamentals - Auditing

- *Auditing/Accounting*
 - the analysis of records of account (e.g. security event logs) to investigate security events, procedures or the records themselves
 - Includes logging, intrusion detection and auditing of security in managed computer facilities
 - well established in theory and practice
 - » Grid computing adds the complication that some of the information required by a local audit system may be distributed elsewhere, or may be obscured by layers of indirection
 - » e.g. Grid service making use of federated data resource where data kept and managed remotely
 - Need tools to support diagnostics
 - Do we need to log all information? (Can We? More pertinent probably)
 - How long do we keep it for?
 - ...
 - Auditing tools are in development for some authorisation infrastructures e.g. PERMIS Secure Audit System

Paul A. Farrell 2006 KENT STATE Grid Computing 12

Fundamentals - Fabric Management

- *Fabric Management*
 - **consists of the distributed computing, network resources and associated connections that support Grid applications**
 - impacts Grid security in these ways:
 - an insecure fabric may undermine the security of the Grid
 - » Are all sites fully patched (middleware/OS)?
 - Can we limit damage of virus infected machine across Grid?
 - » Identify it, quarantine it, anti-virus update/patch, re-instate into VO, ...
 - fabric security measures may impede grid operations
 - » e.g. firewalls may be configured to block essential Grid traffic

Paul A. Farrell 2006 KENT STATE Grid Computing 13

Fundamentals – Trust & Reliability

- Trust
 - Ability to rely on computer-based systems to perform critical functions securely, and on systems to process, store, and communicate sensitive information securely
- Reliability
 - System can be relied on to do what requested when requested

Paul A. Farrell 2006 KENT STATE Grid Computing 14

Fundamentals - Privacy

- Privacy
 - particularly significant for projects processing personal information, or subject to ethical restrictions
 - e.g. projects dealing with medical, health data
 - Privacy requirements relate to the use of data, in the context of consent established by the data owner
 - Privacy is therefore distinct from confidentiality, although it may be supported by confidentiality mechanisms.
 - Grid technology needs a transferable understanding of suitable policies addressing privacy requirements/constraints
 - Should allow to express how such policies can be
 - » defined,
 - » applied,
 - » implemented,
 - » enforced, ...

Paul A. Farrell 2006 KENT STATE Grid Computing 15

Trust – Additional Aspects

- *Trust*
 - **characteristic allowing one entity to assume that a second entity will behave exactly as the first entity expects**
 - **Important distinction between 'trust management' systems which implement authorisation, and the wider requirements of trust**
 - e.g. health applications require the agreement between users and resources providers of restrictions that cannot be implemented by access control
 - e.g. restrictions on the export of software, or a guarantee that personal data is deleted after use
 - therefore a need to understand and represent policy agreements between groups of users and resource providers
 - such policies may exist inside or outside the system, and are typically not supported by technical mechanisms

Paul A. Farrell 2006 KENT STATE Grid Computing 16

Trust – Additional Aspects

- Key concept for Grid security
 - Overall Grid security policy is impossible
 - Sites must integrate local security policies to create Virtual Organisations
 - Essential to have mechanisms which allow trust to be established between participating institutions
- Security Policies should:
 - Be kept and managed by the local site
 - The Grid should aim to integrate existing site policies rather than centralise them.
 - A 'Federation' of trusted sites for VOs
 - Shibboleth??