# Identity Federations: Security Analysis

**Rémi Mollon**

*CERN Computer Security Team*

FIM4R Meeting

Espoo, Finland – October 2nd, 2013

# Scope

- Centre of Excellence model
  - Defining requirements for FIM
- Beginning of risk analysis
- From a generic point of view
  - Implementation independent

# Identity Federations

- Group of...
  - Identity Providers – IdPs
  - Service Providers - SPs
- Common
  - Identity management
  - Attribute management
  - Policies

# Trust Framework

- Between IdPs and SPs
  - … and users!
  - Establishment of common policies and obligations
  - Proper user authentication by IdP
  - Proper use of user attributes by SP
- Malicious entity breaks trust chain
  - Traceability should be ensured

# Different Approaches

- User-centric Federation
  - Open environment
  - “Public” services
- Provider-centric Federation
  - Circle of trust
  - Defined group of IdPs and SPs
  - Agreed common policies
- Mixed Federation
  - Guest IdPs

# Authentication

- Done by corresponding Identity Provider
  - Single point of failure for a group of users
- Single password for all services
  - Wide impact in case of compromised passwords
  - Revocation mechanism is paramount
- Stronger authentication for sensitive services

# Single Sign On

- Auto-log on once authenticated against IdP
- Determination of the corresponding IdP
  - « Where Are You From » (WAYF)
- Be careful with logout
  - Auto log on even after service logout
  - IdP logout may not logout from services
  - Session timeout

# Attribute Provider

- Consistent handling in a given community
  - IdP independent
- Very sensitive entity
  - Single point of failure
- Who is responsible for it?
- Compatibility with existing systems

# Levels of Assurance – IdPs

- Physical identity checks
  - Vouching, passports
- Authentication strength
  - Password rules (including recovery)
  - Simple password vs multi-factors
- Identity life cycle
- Accreditation mechanism
  - Requirements clearly defined in policies
- Lowest level for open third-parties' IdPs

# Levels of Assurance – SPs

- Appropriate security measures in place
- Restrict user attributes access
  - By groups according to sensitiveness/purpose
  - Need-to-know
- Accreditation mechanism
  - Requirements clearly defined in policies

# Malicious Identity Provider

- Access to users' attributes
- Misuse of SPs resources
  - Impersonate users
  - Fake users

# Malicious Service Provider

- Misuse of users' attributes
  - Data mining, targeted attacks
- Phishing attacks
  - Redirection to fake login page
- Cross-Site Request Forgery attacks
  - Actions on other services using user credentials

# Privacy

- Easy correlation of users' activities
- Access to users' attributes
  - SPs may not need all of them
  - Clear statement for users
  - Mechanism to restrict access
  - Should be part of service-specific policies
  - Third-party attribute provider

# Data Protection Laws

- International federations
  - Laws may differ between countries
  - Confidentiality of attributes
- Policies should take them into account
  - Not easy to enforce technically

# Independent Partners

- Different needs and obligations
- Heterogeneous technologies
  - Need of (credentials) translators
  - Implementation issues
- Compatibility may not be complete

# Young technology

- Implementation and configuration issues
- (Mis)understanding from the users
  - Good practices
- To be reviewed:
  - Security Procedures
  - Incident Response

# Conclusions

- Trust/Accreditation model to be determined
  - e.g. International Grid Trust Federation model
- Privacy issues
  - Complex in international environment
- Interoperability
- New environment
  - Security implication need to be understood

# Questions?

- Thank you for your attention!