Internet and Security: Dream or Reality

Roman Špánek

Seminář KEG

Content

- Security and the (Future)Internet
- Basic approaches
- Reputation based approaches
- Attacks
- Our work

Security - Basics

- Cryptographic
  - mathematical techniques for keeping data protected from adversaries
  - **Authentication:** Data were created by a particular user who claims it
  - Security stands on cryptographic techniques

Cryptoghraphic Attributes

- Confidentiality
  - Content is not revealed to any non-authorized entity
- Integrity
  - Data cannot be altered by any non-authorized entity
- Authentication
  - Entity authentication: verification identity of communicating entities
  - Data authentication: guarantees origin of data
- Non-repudiation
  - Guarantees entity responsibility for a particular action (sending a message, receiving a message etc.)
- Availability
  - Services are ready when required

Cryptographic Primitives

- Symmetric key cryptography
- Asymmetric key cryptography
- Message digests

The State of the Art

- Internet, cell phones, social networking, … new technologies for advanced communication between human beings
- Communication has been one of the main driving force of human evolution
- Is security really necessary?
  - Social networks (facebook, twitter, etc.)
  - eBusiness
  - …

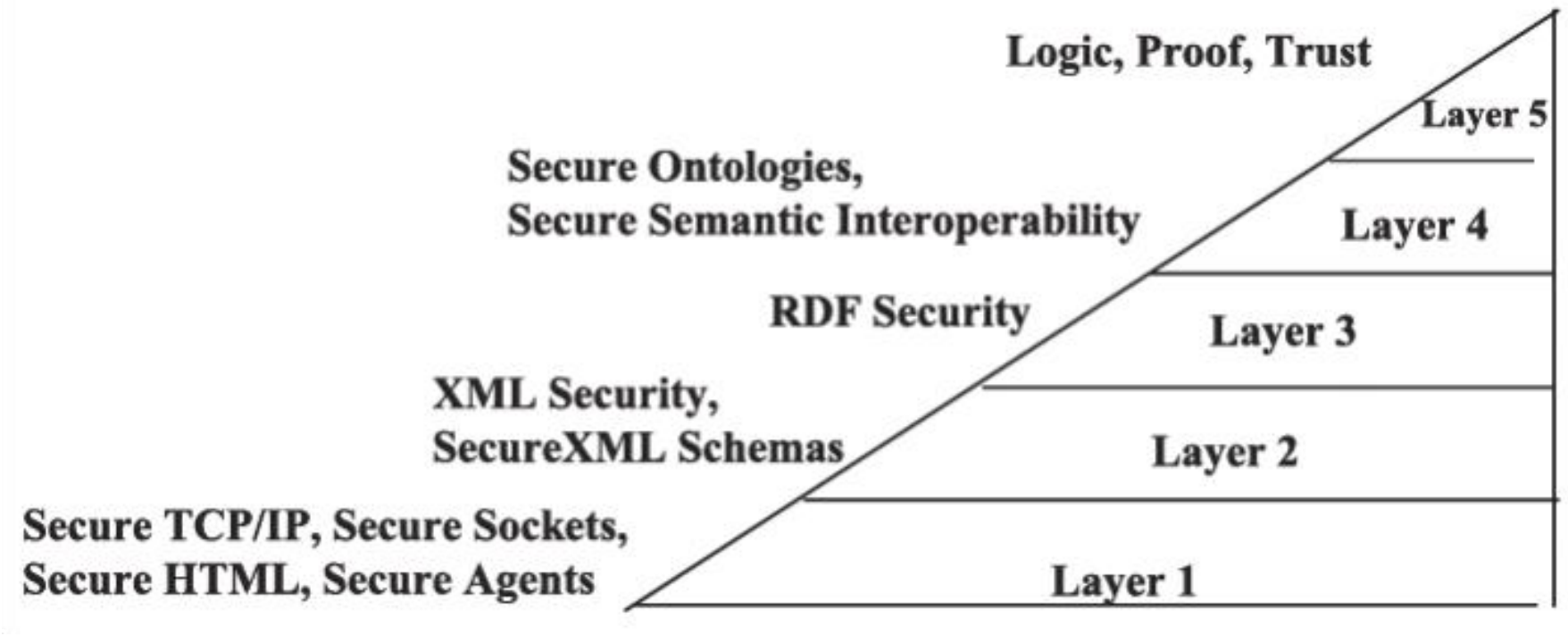
How to solve security?

- Security system should be
  - Flexible
  - Semantically rich
  - Simple as possible to enable automation
- Demands might be in contrary to themselves

How to solve security?

- KERBEROS
- PKI (Public Key Infrastructure)
- PGP (Pretty Good Privacy)
  - adopts the web of trust approach
  - no central authority which everybody trusts
  - individuals sign each other's keys and progressively build a web of individual public keys interconnected by links formed by this signatures.
- Is it flexible and usable for distributed system like Web?

Security and the Semantic Web



XML Security

- XML digital signatures
  - Content has not been altered
- XML encryption
  - Content cannot be read by an unauthorized entity
- X.509 Public Key Certificates

Reputation and Trust

- Reputation and trust have been important for humans since the dawn of our evolution (cooperation, establishment of contacts).
- **Reputation:** is pubic meaning on a person, group, organization, source, etc.
- **Trust**: can be derived from reputation of one side to another inside a given context

Reputation and Trust

- P2P networks
  - eCommerce (wBay, Amazon, uBid, and Yahoo)
  - Reducing transaction-specific issues, etc.
- inauthentic content (pollution) in file sharing networks
- Wikipedia
- …

Trust Management Systems

- Policy Based
- Reputation based
- Social network based

Policy based

- In the context of open and distributed architectures and computational grids
- problem of authorization and access control in open systems
- trust management mechanisms employing different policy languages and engines for specifying and reasoning on rules for the establishment of the trust.
- limited to verification of credentials and restricting access to resources according to policies defined by a resources owner.

Policy based

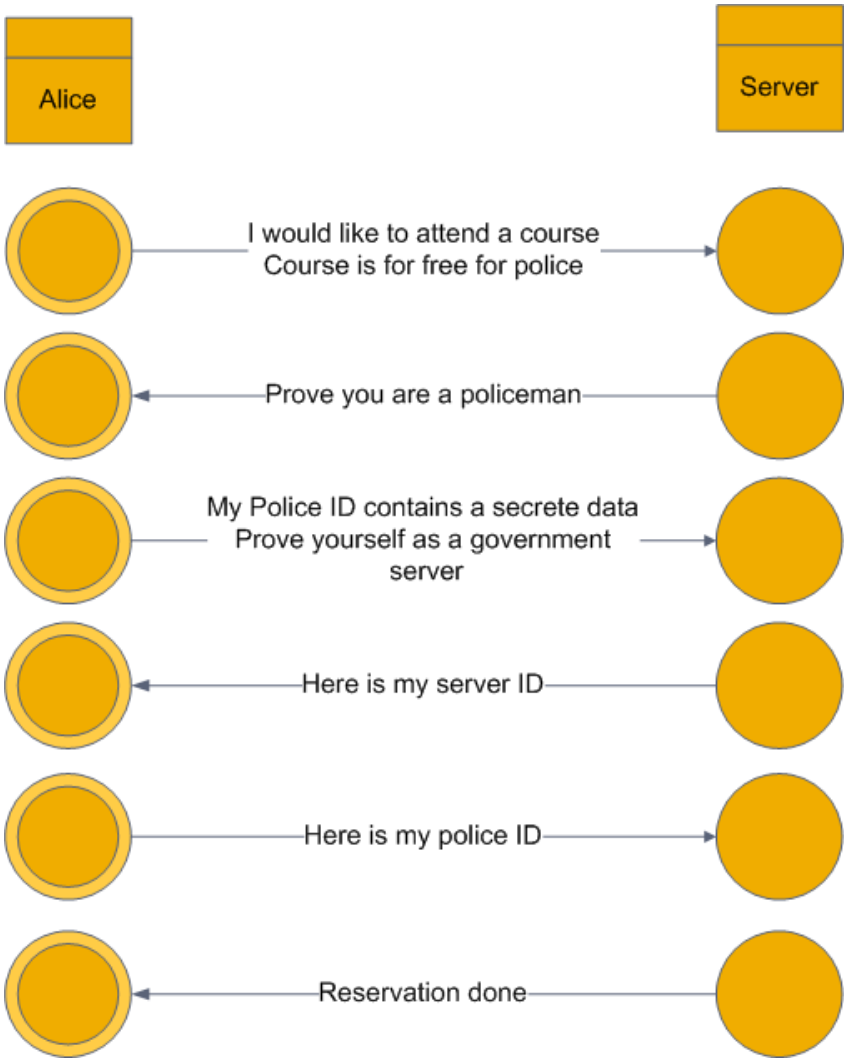
- Extensible Access Control Markup Language (XACML)
  - Policy language
- Role Based Access Control (RBAC)

Policy based

- The Platform for Privacy Preferences (P3P)
  - enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents.
  - P3P user agents will allow users
    - to be informed of site practices
    - to automate decision-making based on these practices when appropriate.
    - users need not read the privacy policies at every site they visit.

Policy based and Negotiation Example

- Example situation of negotiation between a user (Alice) and a server(Government server)



Reputation based approaches

- Means to build a trust between source/service provider and customer by utilizing former transaction, behavior, etc.
- Currently used by many portals
  - eBay,
  - aukro.cz,
  - …

Social-network based

- Using social networks for inferring trust
- Friend-of-my friend is also my friend approach
- Indirect reputation
- Virtual Organization
- Virtual Communities
- Social Web
  - Friendster,
  - Facebook
  - MySpace,
  - LinkedIN,
  - …

Regret

- Reputation is divided into 3 dimensions:
  - Social (friend of my friend is also my friend)
  - Individual (used for direct communication)
  - Ontological (other reputation, based on behavior, aims, shared data, etc.)

NodeRanking

- Very similar to page rank
- Each node in network propagates portion of its own reputation to its neighbors
- Node reputation is given by reputation of its neighbors

Virtual Organization/Communities

- **Virtual Organization (VO)** is a temporary or permanent coalition of geographically dispersed individuals, groups, organizational units or entire organizations that pool resources, services and information to achieve common objectives and that have precisely described mechanisms and rules when and what to share.
- Used in Computation Grids

Lifetime of VO

1. Establishment of VO (Discovery & Formation)
   - Requirements on new members are set
   - Members satisfying the requirements are accepted to VO, accepted members receive:
     1. Credential to access other members
     2. Interaction & coordination information
     3. VO agreements and policies
     4. Other configuration (contacts, etc.)
2. Normal operation
3. Dynamic addition of an organization
   - Addition of a new resource needed by VO members
4. Dynamic removal of an organization
5. Replacement (steps 3 and 4)

Security Systems for Grids

- Property based certificates
  - PRIMA
  - VOMS
  - CAS
  - X.509 attribute certificates

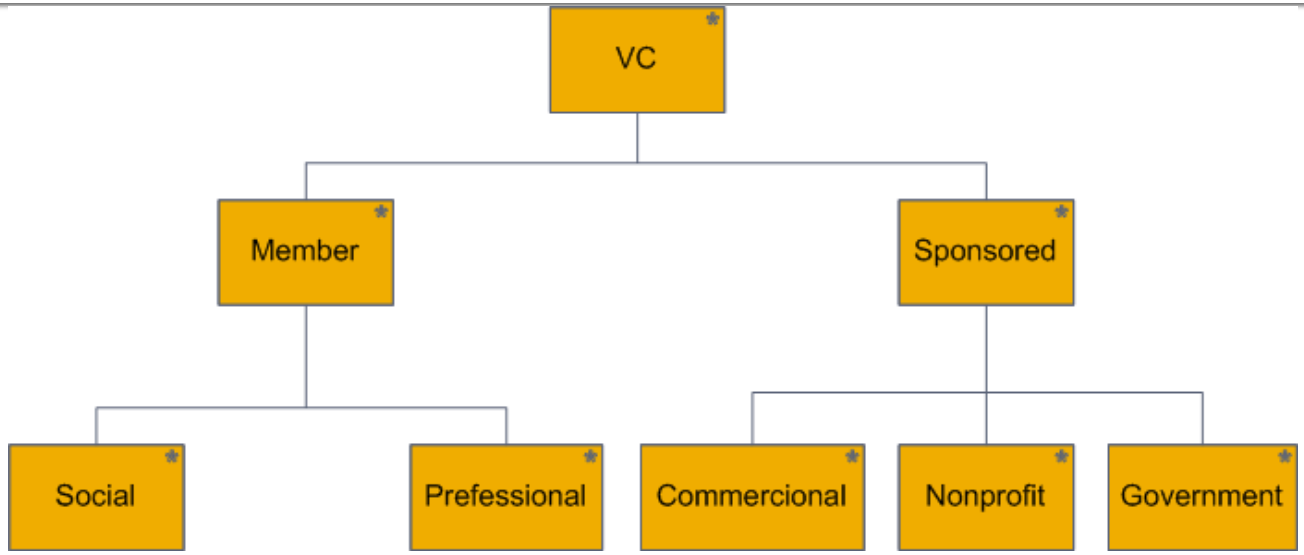
Security Systems for Grids

- **Virtual Organization Management Service (VOMS)**
  - Attribute based access control.
  - The client retrieves a pseudo certificate consisting of client attributes (e.g. groups and roles) from VOMS servers and stores them in a non-critical extension of a common proxy certificate.
  - These proxy certificates are used to access the resource.
- **PERMIS** aimed creation of an X.509 role based Privilege Management Infrastructure.
  - PERMIS has ability to accommodate diverse access scenarios.
  - PERMIS primary consists of two subsystems:
  1. the privilege allocation subsystem issuing a user X.509 certificate and storing it in LDAP (Lightweight Directory Access Protocol) directories.
  2. the privilege verification subsystem which hauls the user certificates from a pre-configured list of LDAP.

Security Systems for Grids

- **AKENTI**
  - three types of certificate stored in an XML format:
    1. attribute certificates binding an attribute-value pair,
    2. use-condition certificates indicating lists of relational expressions of required attributes to access rights,
    3. policy certificates consisting of trusted Certificate Authorities CAs and stakeholders issuing use-condition certificates and lists of URLs where attribute certificates can be retrieved.
  - Clients are then authenticated on their X.509 certificates.
- **System for Privilege Management and Authorization (PRIMA)**
  - accommodates attribute X.509 certificates to enforce privilege and policy statements.
  - Both certificates issued by a resource administrator and a stakeholder are used by a client to the resource Policy Enforcement Point (PEP).
  - PEP validates the attributes and verifies with the resource Policy Decision Point (PDP) if the issuers are authoritative for user's presented privileges.
  - All acknowledged privileges are gathered by the PEP and further presented to the PDP for verification against the access control policies.
  - PDP simply returns an authorization decision and a set of access recommendations (e.g. file accessible, user's quotas) for setting up a local account.

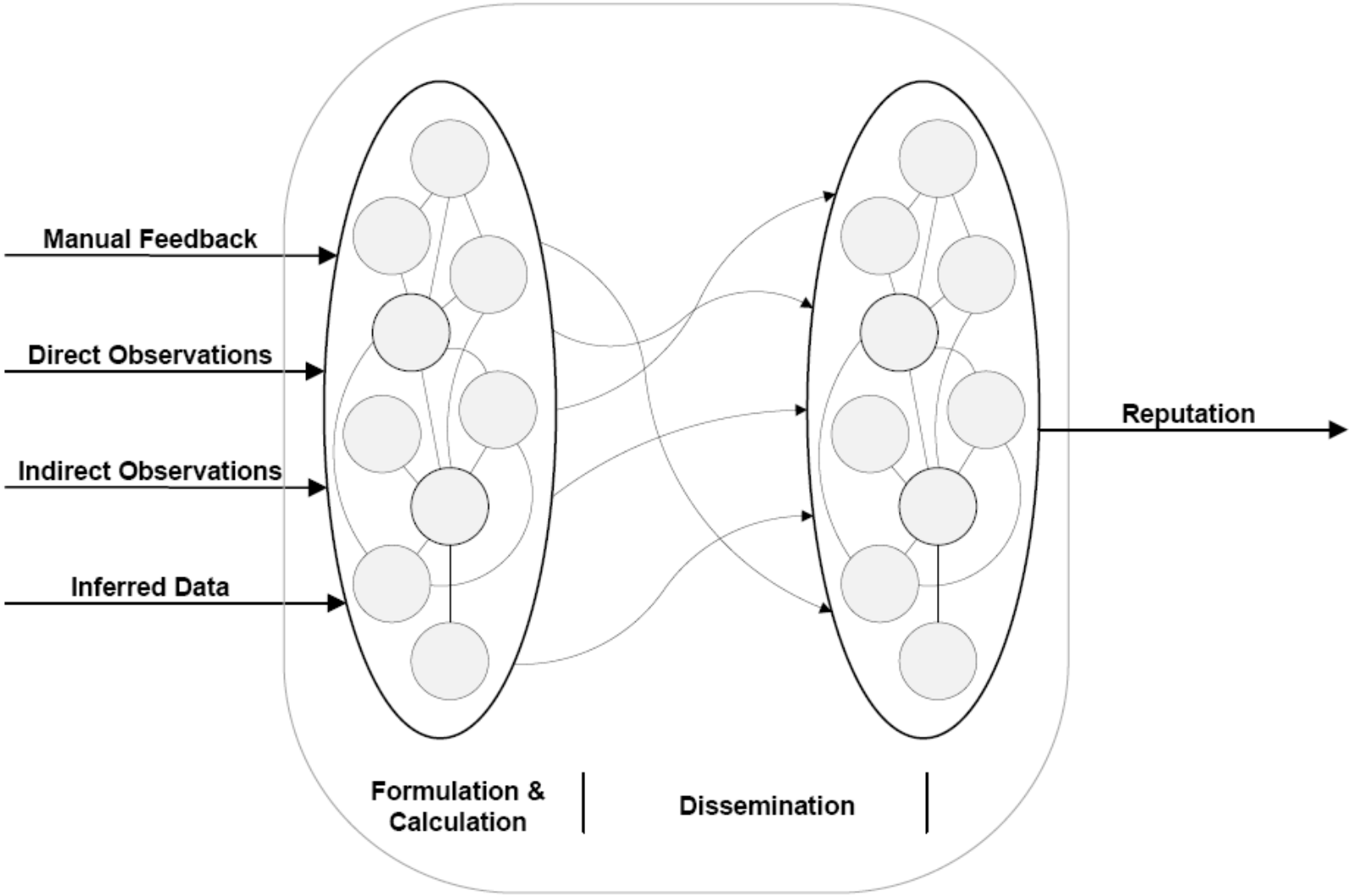
Virtual Communities



- Very popular on so called *social web*
- Attributes:
  1. Purpose: one common intension, more different intensions
  2. Place: access is limited to invitation, who may be a community members, etc.
  3. Platform:
     1. synchronized communication (chat)
     2. Asynchronously (email)
     3. Hybrid
  4. Profit Model (makes VC any profit?)

Basics for Building Reputation System

- **Formulation.**
  - mathematical model of the reputation metric
  - accept positive, negative combined feedback information.
- **Calculation**.
  - Algorithm calculating the mathematical formulation for a given set of constraints
- **Dissemination**.
  - Participants can obtain the reputation given by the calculation.
  - storing the values
  - disseminating values to participants (DHT, communication protocols).


Manual Feedback
Direct Observations
Indirect Observations
Inferred Data
Reputation
Formulation & Calculation
Dissemination

Components of formulation:

- Source of information
  - Manual
    - Human feedback (user rating)
    - we need a transformation from qualitative into quantitative metric (Bayesian procedures, Fuzzy logics)
  - Automatic
    - Direct observation (success x failure, cheating, etc.)
    - indirect observation (second-hand observation)

Components of formulation:

- Type of feedback
  - Positive
  - Negative
  - Both

Components of formulation:

- Reputation metric
  - Binary
  - Discrete (various degree in order to allow more flexibility)
  - Continuous (implemented as real numbers)
  - Conversion from continuous to discrete
  - Symmetric
    - PageRank (one global values know to all entities)
  - Asymmetric
    - Each node have its own individual view on the system

Calculation

- May be a complicate with respects to constraints given by an environment .
- Should be resilient against manipulation with input data
- Calculation Structure:
  - Centralized(eBay) – single point of failure
  - Distributed (convergence problem, …)
- Calculation Approach:
  - Deterministic model (centralized structure, asymmetric formulation structure)
  - Probability model (Markov models, Bayesian models,…)

Dissemination

- Prevent alternation calculated values during dissemination
- Dissemination Structure:
  - Centralized (eBay)
    - Single point (may be implemented as a cluster) stores and disseminates values
    - Single point of failure, single point to be attacked
- Distributed
  - each participant is responsible for some portion of the calculated reputation values.

Dissemination

- Dissemination approach:
  - Deterministic (DHT,..)
  - Probabilistic (probabilistic broadcast, flooding,..)
- Storage:
  - Short-time (volatile memories)
  - Long-time (non-volatile memories – storage security)
- Dissemination Redundancy:
  - Trade off between transmission efficiency and resilience against message modification.
  - Multiple messages are sent to provide resilience against message altering

Attacks against Reputation Systems

- Open infrastructure allows **inner (from inside)** and also **outer (from outside)** attacks
- **selfish** or **malicious**
- **Alone** or **synchronized** by a **group** of attackers

Attacks

- Self-Promoting
- Whitewashing
- Slandering
- Orchestrated
- Denial of Service

Self-promoting

- Attackers manipulate their own reputation by falsely increasing it.
- Node falsely augment their reputation.
- Node generates **positive feedback** for itself or by attacking **dissemination** of reputation
- Attack may be done by a group of collaborating nodes generating positive feedback to themselves
- System vulnerable:
  - With positive feedback only
  - With no mechanism for data (feedback) authentication
  - With no need for proof of interaction
- Solution:
  - Require accountability, proof of transactions, system preventing nodes to have multiple identities
  - Identify attackers that communicate within isolated groups/cliques (it is known to be NP hard)

Whitewashing

- Attackers abuse system for a short-time – degrade of reputation
- Attackers leave the system and enter it with a new reputation
- System vulnerable:
  - Systems with negative feedback only (new participants have almost the same reputation as well behaved nodes)
  - Systems with positive & negative feedback if based only on long term evaluation == **behavior oscillation**
- Solution:
  - System cannot assign similar reputation to newcomers and to nodes with long-term good behavior
  - Only limited history is considered
  - System preventing node to gain multiple identities

Slandering

- Attackers falsely produce negative feedback about other nodes
- Can be done by a coalition of attackers
- System vulnerable:
  - System with no authentication of origin of the feedback
- Solution:
  - System should make a trade off between in sensitivity to negative feedback
  - Validate that feedback is tied to a real transaction

Orchestrated.

- Group or one attacker use different methods and strategies, change behavior over time periods, etc.
- Oscillation attack:
  - Concluders dive themselves into two teams
  - One behave honestly for some period of time to gain reputation and to reduce decline of reputation of the second team
  - Second behave dishonestly and try to get as much as possible from dishonest behavior
  - After some time roles are exchanged
- System vulnerable:
  - When there are several concluders for each role in the system
- Solution:
  - Use a graph techniques in order to reveal groups of concluders

Denial of Service

- System vulnerable:
  - Centralized systems
- Solution:
  - Distribution of calculation and dissemination

Defense Strategies

- Sybil attack (Preventing multiple identities)
  - Require some payment for each identity (computation power, storage, etc.)
  - Bind digital identity with some real world identity (IP address, cell phone numbers,…)
  - Create a web of trust and use social network strategies in order to identify multiple identities
  - Use a graph algorithms to detect multiple identities and prevent Sybil attack

Mitigating Generation of False Rumors

- Bind feedback with a concrete transaction by using a cryptographic algorithms (certificates and signatures)
- Coalition of attackers may overcome this solution

Mitigating of Spreading of False Rumors

- System using only direct information can limit this
- On the other hand, it cannot be used in large system where just several nodes communicate
- Rely on pre-trusted identities to reduce the effectiveness of fabricated or altered information
- Use Bayesian framework, where misbehavior is modeled by a Beta distribution

Preventing Short-term Abuse of the System

- Misused system and them exit to avoid consequences
- Solution:
  - Newcomers should have lower default reputation
  - Newcomers must provide more services that they receive for some time since they get their initial reputation

Our results

- **SecGrid**
  - Phd. Thesis
  - R. Špánek, Self-organizing and Self-monitoring Security Model for Dynamic Distributed Environments
- **Reputation system evaluating quality of web sources**
- **Reputation system for MediGRID**

Děkuji za pozornost