Trust in LargeScale Computational Grids: An SPKI/SDSI Extension for Representing Opinion

Jose de Ribamar Braga Pinheiro Junior
Alexandre C. T. Vidal
Fabio Kon

Department of Computer Science
University of São Paulo, Brazil

4th International Workshop on Middleware for Grid Computing - MGC 20066

Outline

Overview
Security

- Securing information access is a hard task
- Security technologies were created to make it difficult for unauthorized users to access information
- People and software agents that have legitimate rights could use their prerogatives to execute forbidden actions
- It would be important to consider the relationship between subjects, including the interation history

Overview
Security in Grids

- A Grid may encompass many institutions and different administrative domains
- It may also contains thousands of users and machines
- The environment is dynamic, with users and resources joining and leaving at any time
- Centralized solution is not desirable

Overview
Trust Chains

- Trust chains provide decentralized resource access control
- Based on mutual trust relations
- Each subject is a certification authority
- Can provide access rights to other subjects
- These rights can be delegated, creating a trust chain

Overview
SPKI/SDSI model

- SPKI/SDSI: implementation of trust chains
- Users can create authorization certificates in behalf of other users
- Users can delegate authorization certificates
- When a subject decides that another one is reliable, he has to have total certainty about this
- It would be better to have intermediate levels of trust

Outline

Jøsang model.

- Opinion ω about an statement
- $\omega = \{b, d, u\}$ where $b + d + u = 1, \quad \{b, d, u\} \in [0, 1]^3$
- b, d, and u represent belief, disbelief, and uncertainty
- There are 3 well defined states
- Operators to manipulate opinions

CONJUNCTION Operator

When need opinion about two independent statements

$\omega_p^A = \{b_p^A, d_p^A, u_p^A\}$ and $\omega_q^A = \{b_q^A, d_q^A, u_q^A\}$

$\omega_{p\Lambda q}^A = \omega_p^A \Lambda \omega_q^A = \{b_{p\Lambda q}^A, d_{p\Lambda q}^A, u_{p\Lambda q}^A\}$

where:

$$\begin{cases} b_{p\Lambda q}^A = b_p^A b_q^A \\ d_{p\Lambda q}^A = d_p^A + d_q^A - d_p^A d_q^A \\ u_{p\Lambda q}^A = b_p^A u_q^A + u_p^A b_q^A + u_p^A u_q^A \end{cases}$$

RECOMMENDATION Operator

Subject B recommends his opinion about an statement p to subject A

$$\omega_B^A = \{b_B^A, d_B^A, u_B^A\}$$

$$\omega_p^{AB} = \omega_B^A \otimes \omega_p^B = \{b_p^{AB}, d_p^{AB}, u_p^{AB}\}$$

$$\text{where:} \quad \begin{cases} b_p^{AB} = b_B^A b_p^B \\ d_p^{AB} = b_B^A d_p^B \\ u_p^{AB} = d_B^A + u_B^A + b_B^A u_p^B \end{cases}$$

CONSENSUS Operator

Combination of two subject beliefs about an statement

$\omega_p^A = \{b_p^A, d_p^A, u_p^A\}$ and $\omega_p^B = \{b_p^B, d_p^B, u_p^B\}$

$\omega_p^{A,B} = \omega_p^A \oplus \omega_p^B = \{b_p^{A,B}, d_p^{A,B}, u_p^{A,B}\}$

where:

$$\begin{cases} b_p^{A,B} = (b_p^A u_p^B + b_p^B u_p^A)/(u_p^A + u_p^B - u_p^A u_p^B) \\ d_p^{A,B} = (d_p^A u_p^B + d_p^B u_p^A)/(u_p^A + u_p^B - u_p^A u_p^B) \\ u_p^{A,B} = (u_p^A u_p^B)/(u_p^A + u_p^B - u_p^A u_p^B) \end{cases}$$

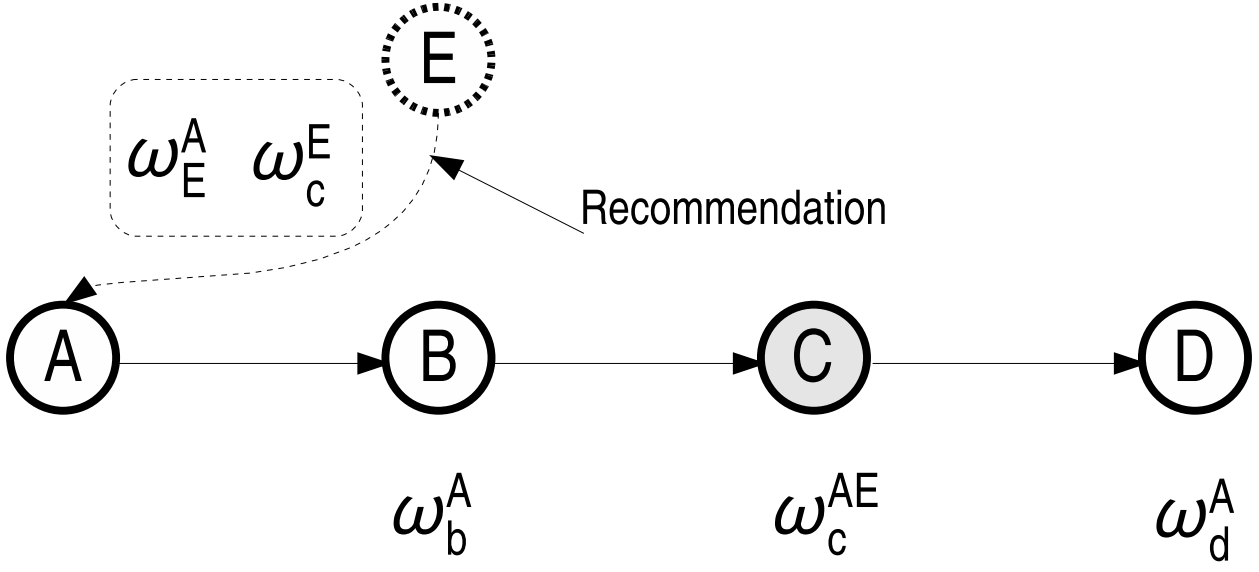
Outline

Using the model with trust chains

- Introduce the concept of opinions in trust chains
- Opinions are used to determine trust between subjects
- A subject can validate a trust chain using the consensus of its opinion about all the subjects in the chain

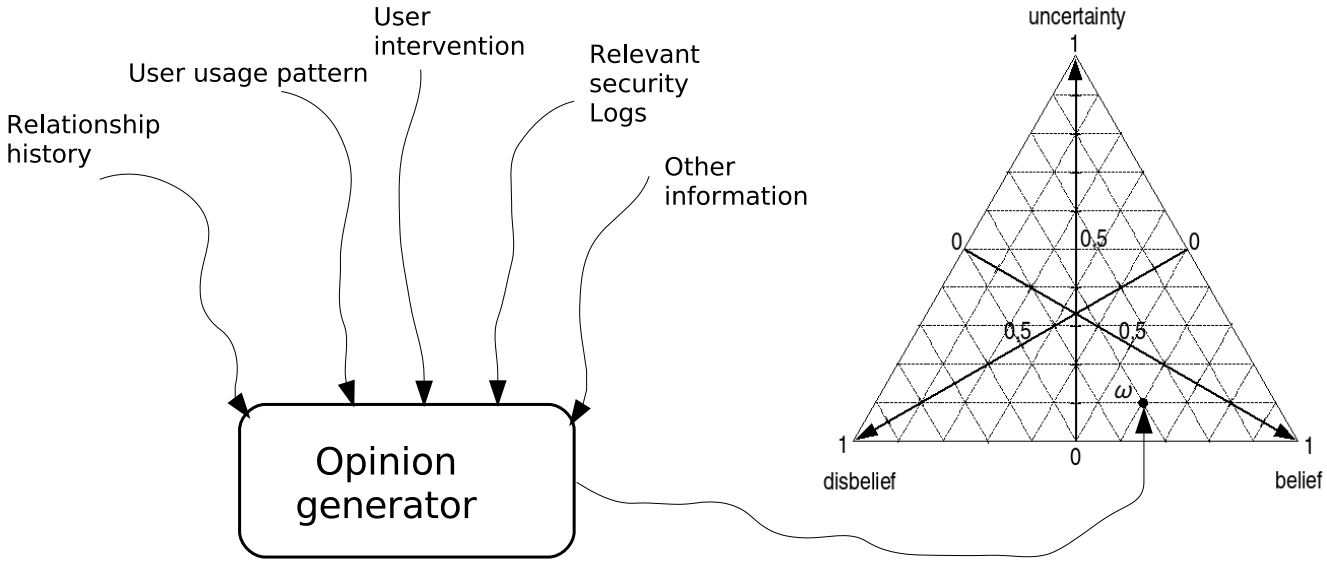
Subject E recommends C to A

- Subject A needs to validate the trust chain but his opinion about C is uncertain
- Subject E recommends his opinion about C to A

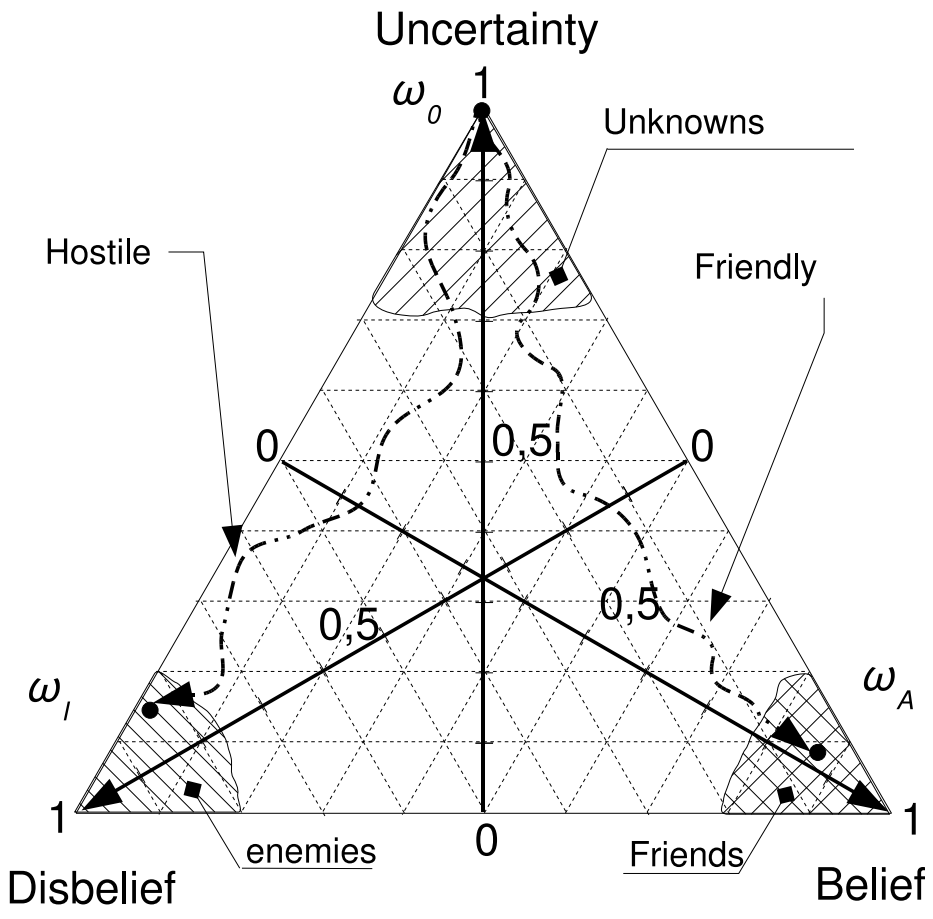


Opinion generator

- Need some mechanism to automatically generate opinions between subjects
- Should also allow manual user intervention



Opinion changing



Outline

Opinion Certificate

- Added new kind of certificate: *opinion certificate*
- *issuer* - is the subject that gave the opinion, he is the certificate owner
- *subject* - is the entity that received the opinion
- *opinion* - is the opinion represented using the model
- *validity specification* - represents the validity of the certificate

Advantages of Opinion Certificate

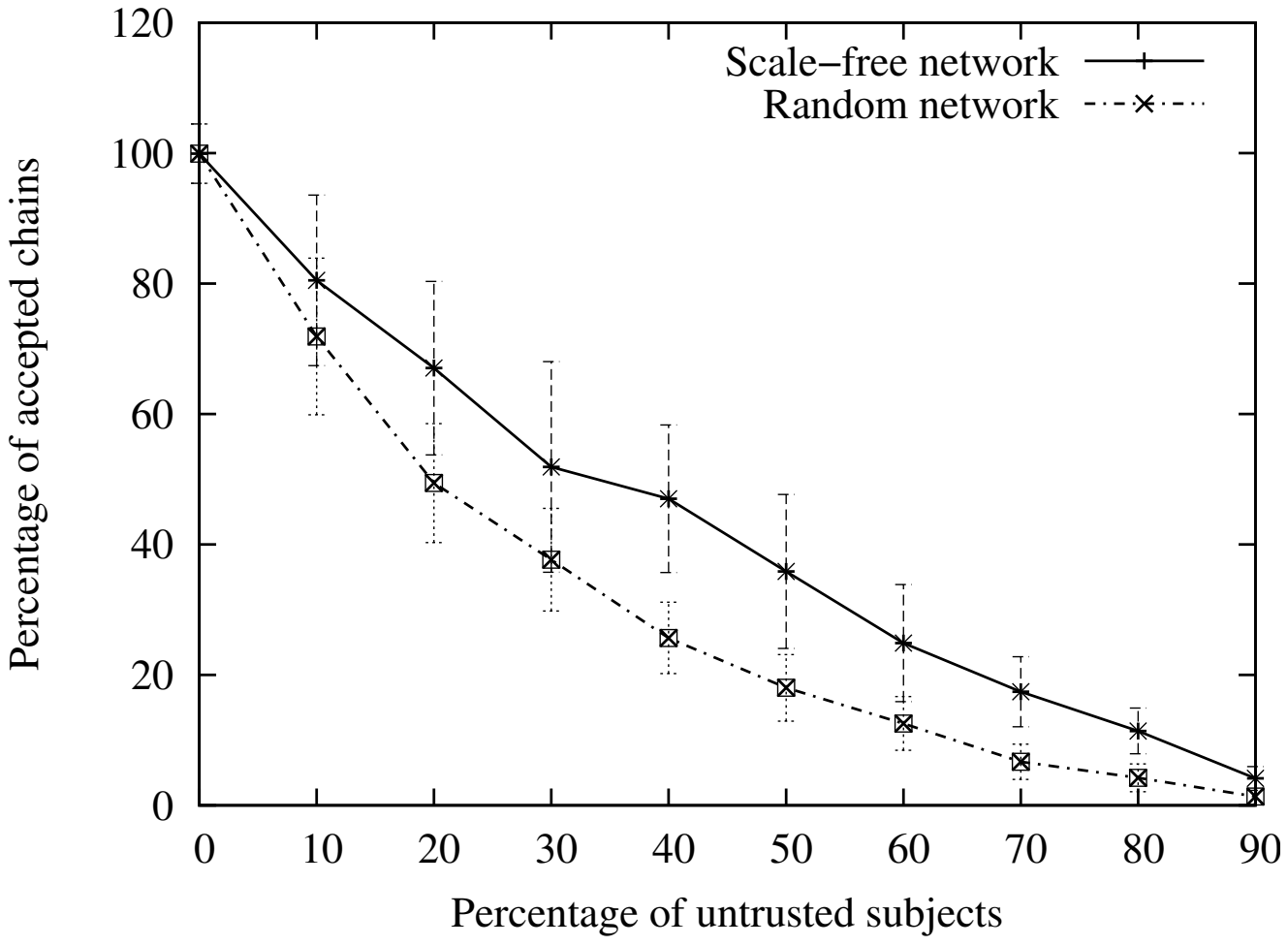
- Opinion composition allows chains to be verified considering non-binary opinions of all related subjects.
- Long chains could usually results in unfavorable opinions
- Non-binary opinions may be used to have an access control list with fine granularity.

Outline

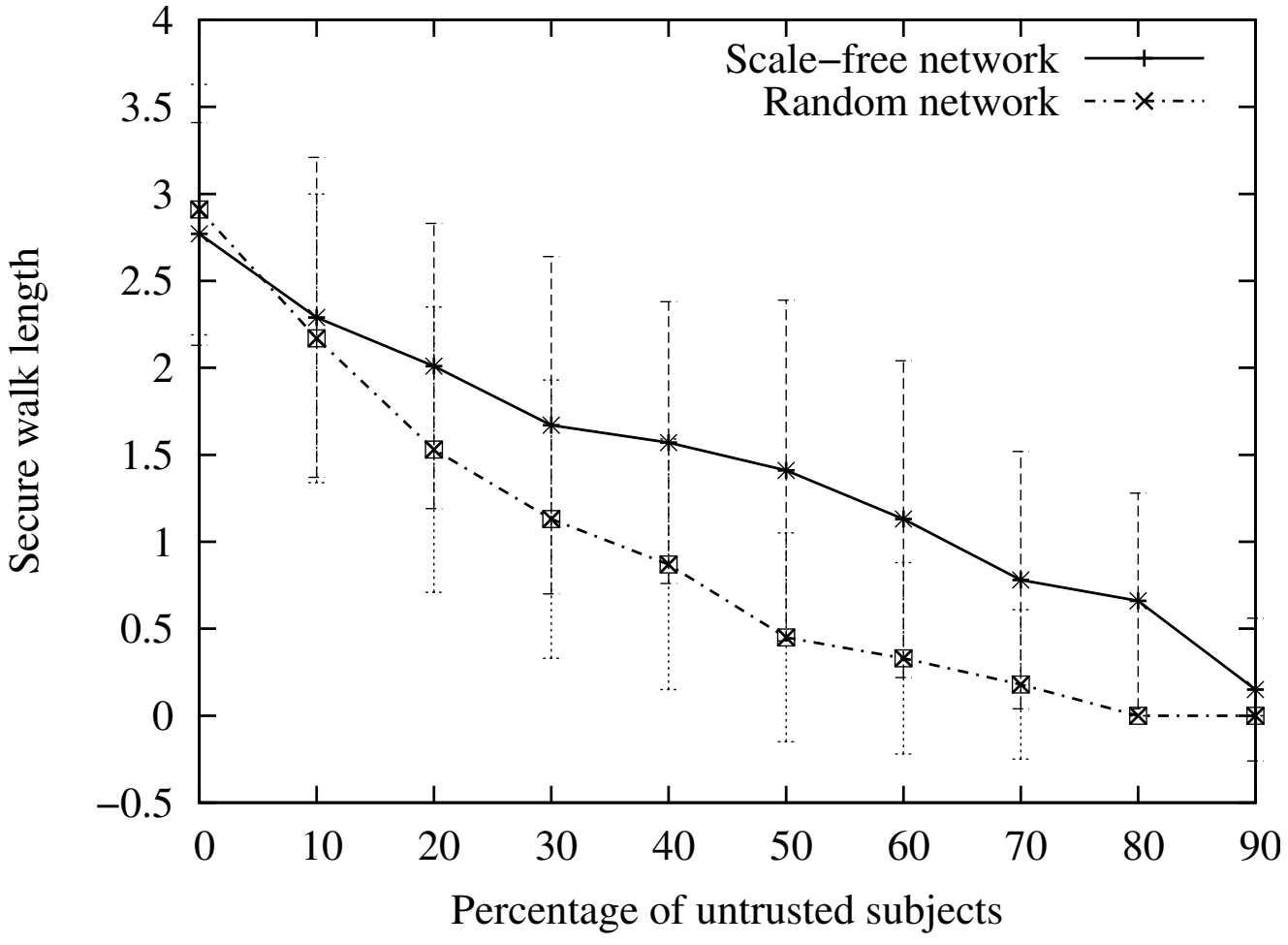
- Bamboo Simulator
- 100 subjects, each controlling a single shared resource
- Random and Free-scale network topologies
  - Free-scale contain high-connectivity hubs
  - Present in web pages, power grids, social interactions
- Simulation have subjects performing legitimate and ilegitiamate action
  - Actions change the opinion of one subject about another

- Steps
  - Initial opinions of 100% uncertainty
  - Subjects delegate their resources randomly
  - Subjects perform resource accesses, modifying opinions
  - Subjects delegates their resources again, creating new trust chains
  - Trust chains are verified to check which ones are acceptable
- Accepted chains versus percentage of untrusted subjects
- Secure chain length versus percentage of untrusted subjects

Accepted chains versus percentage of untrusted subjects



Secure chain length versus percentage of untrusted subjects



Concluding Remarks

- New concept to the initial SPKI/SDSI model: the subjectivity.
- Subjectivity allows SPKI/SDSI to be used in highly dynamic environments such as computational grids
- Jøsang's model seems adequate for represeting opinions

- Need to verify whether the mathematical operations are sufficient
- Implementation of a grid security middleware using the SPKI/SDSI extension
- Finer granularity in security policy definitions

Questions

Trust in LargeScale Computational Grids: An SPKI/SDSI Extension for Representing Opinion

Jose de Ribamar Braga Pinheiro Junior
Alexandre C. T. Vidal
Fabio Kon

Department of Computer Science
University of São Paulo, Brazil

4th International Workshop on Middleware for Grid Computing - MGC 20066