



Towards a Distributed Authentication System in Coordinated Mobile Virtual Organizations



Genge Bela¹
dr. Haller Piroska²



- ^{1, 2} Faculty of Engineering, "Petru Maior" University of Targu Mures
- Email: ¹ bgenge@engineering.upm.ro, ² phaller@upm.ro



Virtual Organizations



Structure:

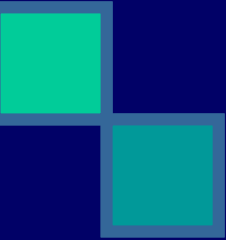

- Semi-independent autonomous individuals
 - Departments
 - Organizations
- 

Main Goal:

- Resource sharing

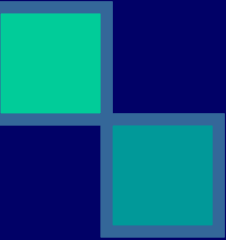


Existing access control possibilities


- 
- Simple firewall – port/IP filtering
 - Dynamic firewall – + sequence of bytes
 - X.509 certificates to authenticate user at each resource
- 



Firewalls

- 
- Provide network package filtering on Data Link, Network or Transport level
 - Provide protocol filtering with the use of proxies

Problems:

- 
- Simple firewall: VO nodes may not be reached because of port filters
 - Dynamic firewall: the use of a sequence of bytes may be discovered + the firewall is a central point of failure




Certificate hierarchy

- Anyone can check the authenticity of a certificate
- If the CA is offline, no new certificates may be issued but authentication of existing users may continue

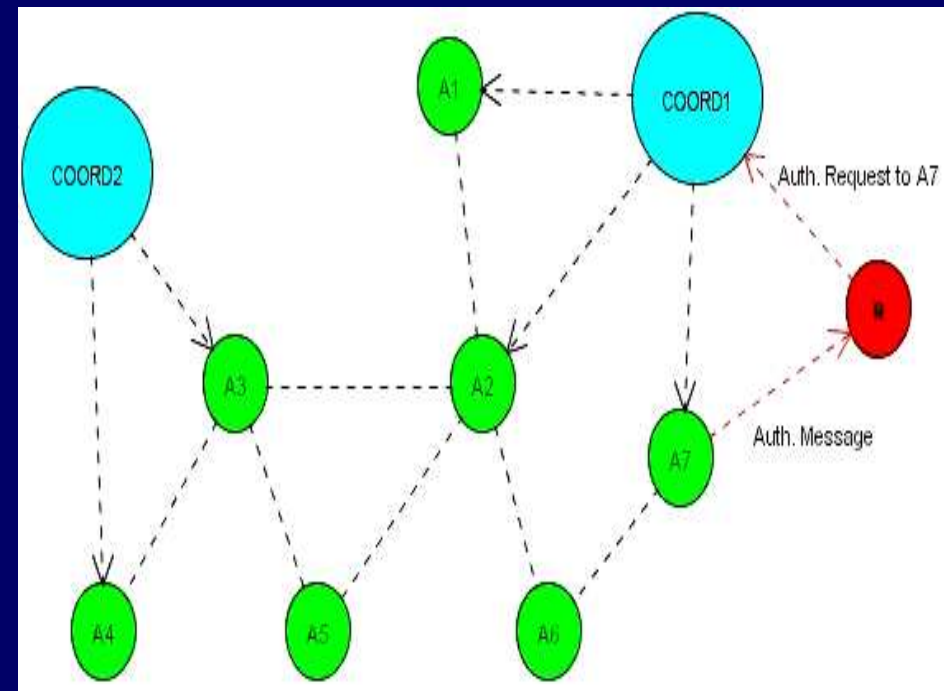


Problems:

- Key distribution (PKI – hierarchy of certificates, Maille – hierarchy + key distribution through peers, Phobos – hierarchy + key request from neighbors)
 - Compromise of the CA -> all certificates must be revoked
 - One CA leads to a monopole on the market
 - At each server, a user must be authenticated with the same hierarchy/public key algorithm
- 

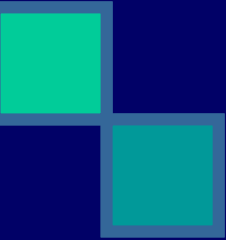

Proposed authentication model

- Initial authentication through the use of Coordinators
- No Key distribution using existing linked servers and 3rd party authentication protocols
- High mobility of nodes through the use of decentralized authentication



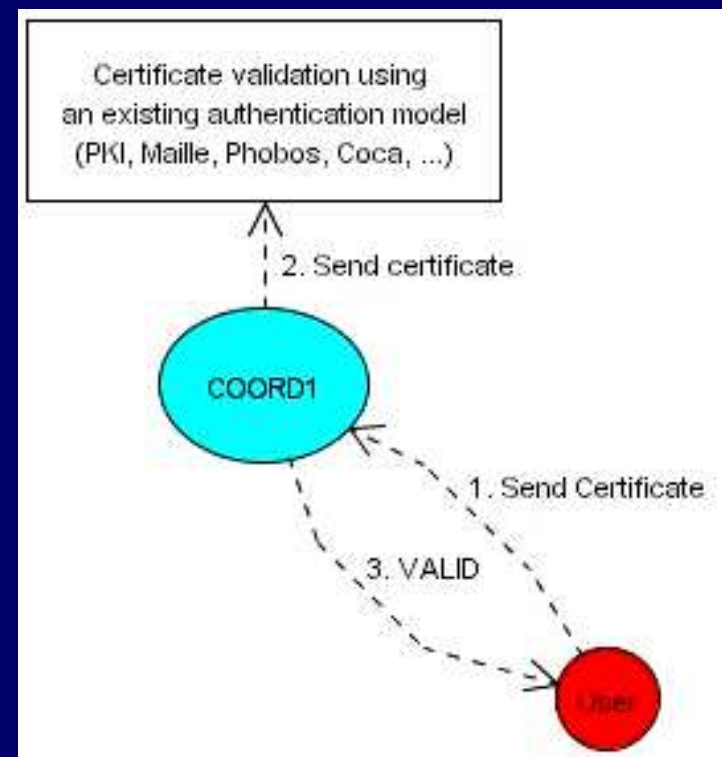


Initial access through the use of Coordinators

- 
- Certificate based authentication of nodes
 - “Coordinating” the user to the proper server
 - Authenticating the user on selected server
- 

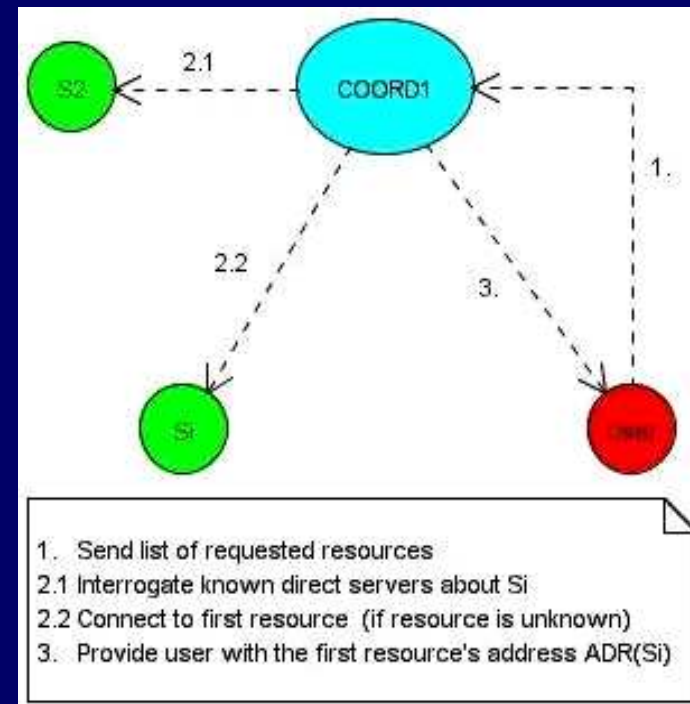
Initial authentication

- Based on existing certificate hierarchy and key distribution models
- Goal: verify the validity of certificate (expiration date, revocation, ...); establish a session key



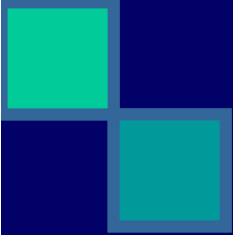

Coordination process

- Receive list of requested resources
- Interrogate existing connections about requested resources
- Create new connections if no first resource is available





Introducing “new” nodes to the system

- 
- 3 party authentication protocol for key distribution
 - Use of symmetric algorithms for efficiency
 - Use of timestamps as “nonces” to prevent replay attacks
 - Minimize the “contribution” of the new node to the authentication process (nonce and key generation)
 - Generated session key position must be strategically placed to minimize type confusion attacks
- 

Proposed authentication protocol

Step 1:

$B \rightarrow S : \{A, T_b, R_b\} \{SKey(B)\}$

Step 2:

- $S \rightarrow A : \{B, R_s, k_{ab}, L, T_s\} \{SKey(A)\}$
- $S \rightarrow A : \{k_{ab}, R_{s1}, T_s\} \{SKey(B)\} \% V_a$

Step 3:

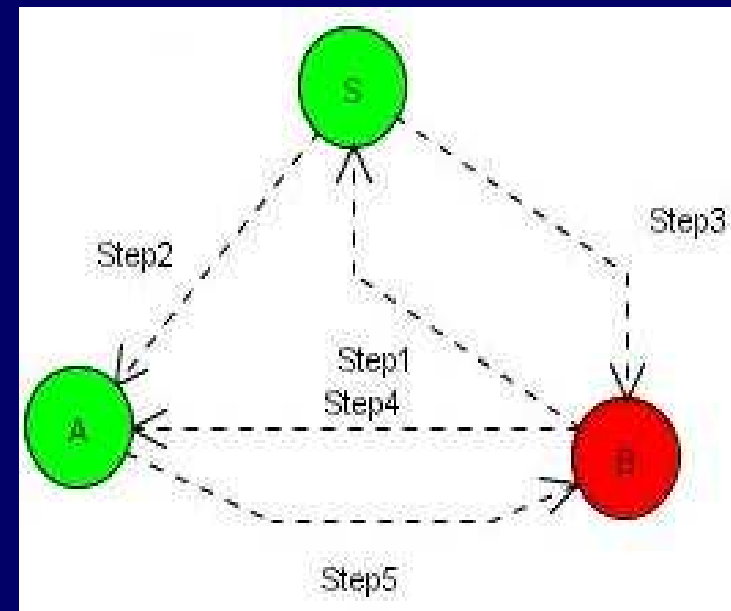
- $S \rightarrow B : \{A, R_{s1}, k_{ab}, L, T_s\} \{SKey(B)\}$
- $S \rightarrow B : \{R_b - 1\} \{k_{ab}\}$
- $S \rightarrow B : \{k_{ab}, R_s, T_s\} \{SKey(A)\} \% V_b$

Step 4:

$B \rightarrow A : \{B, V_b \% \{k_{ab}, R_s, T_s\} \{SKey(A)\}\} \{k_{ab}\}$

Step 5:

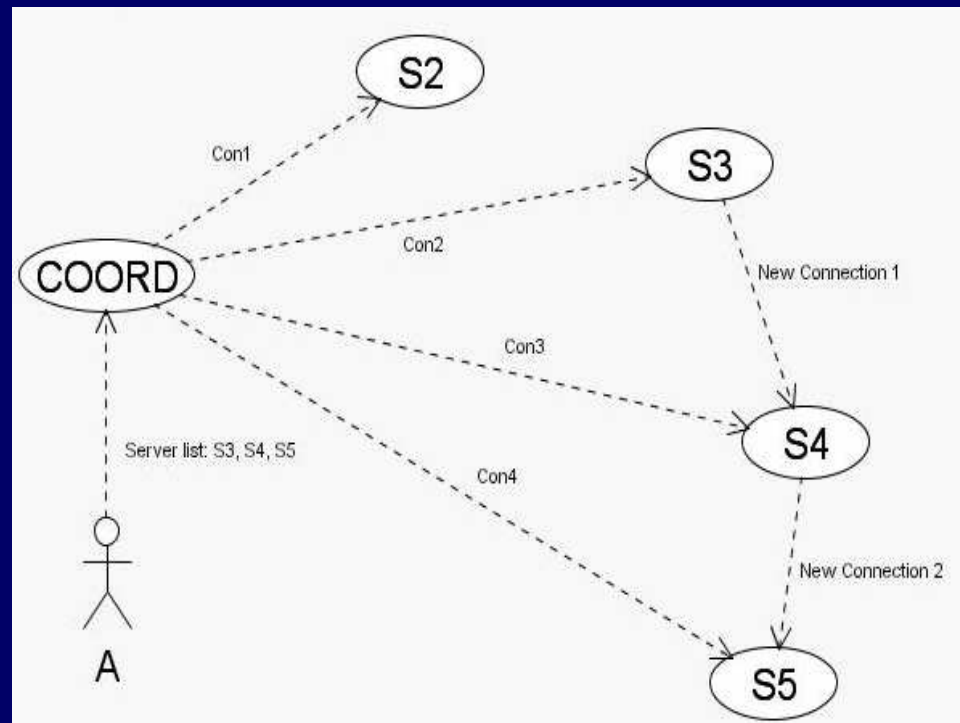
$A \rightarrow B : \{A, V_a \% \{k_{ab}, R_{s1}, T_s\} \{SKey(B)\}\} \{k_{ab}\}$



- S – Coordinator
- B – “new” node
- A – Target node

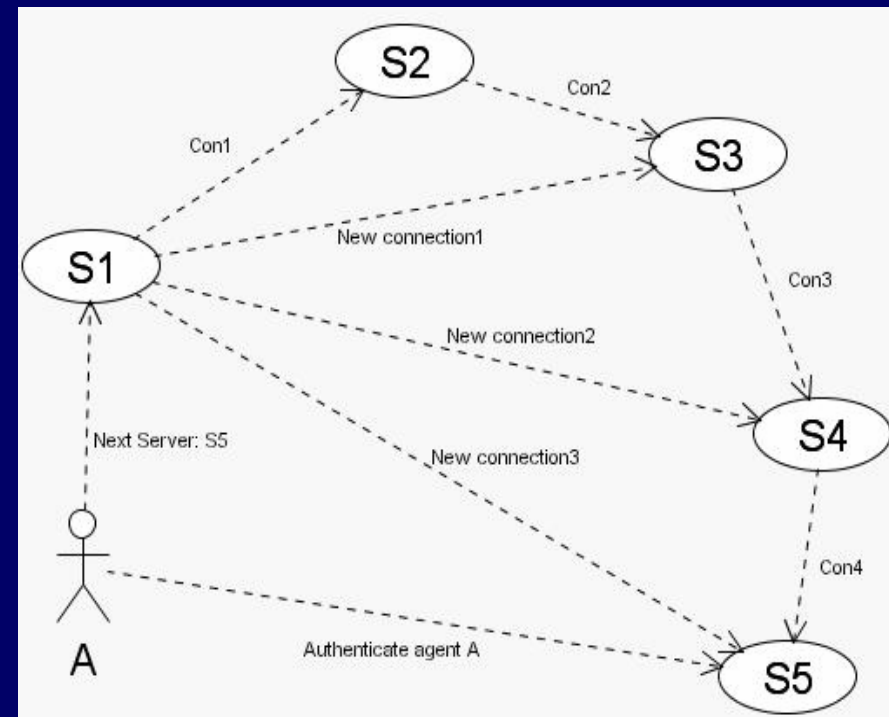
“Next node” access possibilities (a)

- Coordinator will create server links
- User 'A' will be authenticated at S4 by S3 and at S5 by S4



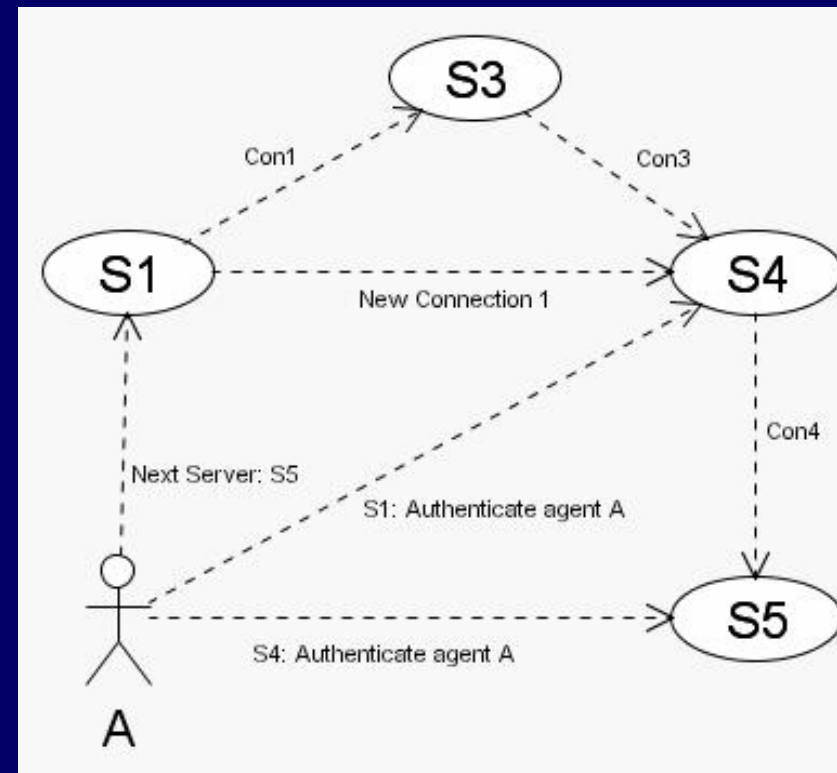
“Next node” access possibilities (b)

- Initial node S1 will authenticate himself at each intermediary node
- Finally, S1 will auth. A at S5




“Next node” access possibilities (c)

- S1 will authenticate 'A' at S4
- S4 will authenticate 'A' at S5





Problems and future work

- If node S is compromised, any node may be authenticated
 - A broken link will lead to the use of a coordinator
 - A node should have more than one link at a time or use passwords that have a certain time limit
 - To reach a next node, a client must pass through intermediary nodes
 - Frequently used links should not be broken!
 - Determining the “next node”
 - Use of adapted routing protocols
- 



Thanks for you're attention!



Questions?



Presented by: Genge Bela

Email: bgenge@engineering.upm.ro