SAyI: Scalable Authentication Infrastructure

Wenyuan Fei and Jon A. Solworth
http://www.ethos-os.org
UIC COLLEGE OF ENGINEERING
UNIVERSITY OF ILLINOIS AT CHICAGO
Department of Computer Science

Introduction

- Internet consists of multiple organizations
- Thus Internet authentication is inherently distributed
- There is no central database holding credentials for all entities
- The entities involved in an Internet authentication are:
  - **Relying party**: the entity provides services to other entities on Internet
  - **User**: the entity which request services and are authenticated by relying party
  - **Trusted Third Party (TTP)**: the entity which signs user's key. The information it provides are certificates which are in form of:

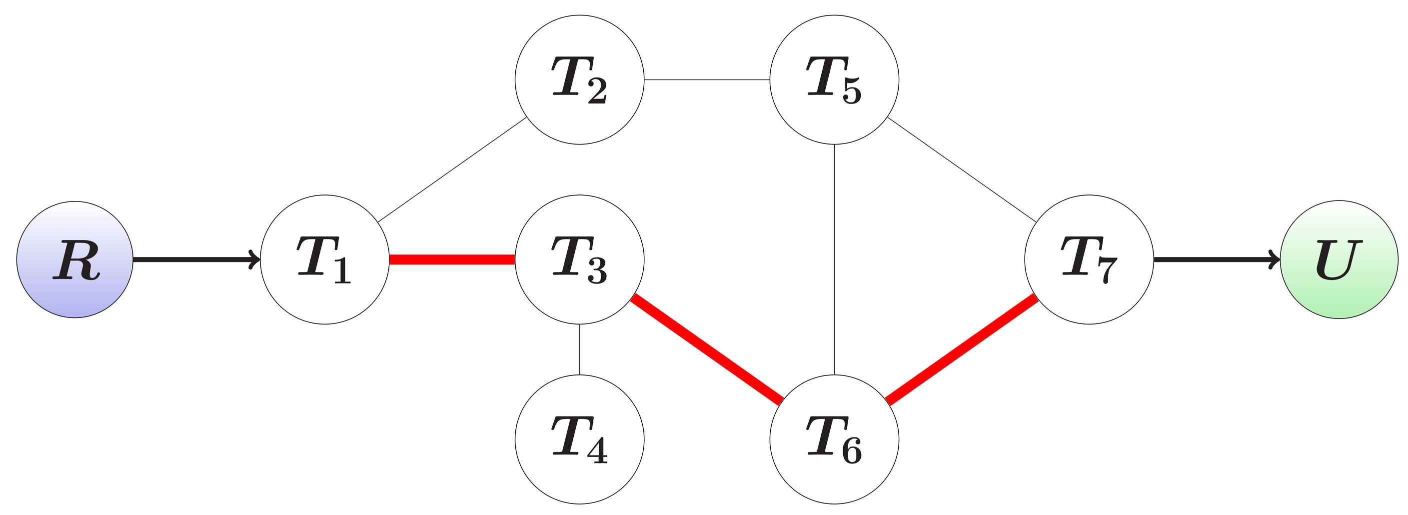
TTP t says x's key is key_x

An Authentication

- The user contacts the relying party and provides a public-key authenticator
- The relying party authenticates the user, relying on:
  - the authenticator from the user
  - authentication information from TTPs

Trust Model on Internet and Its Risk

- The whole Internet can be viewed as a graph in which:
  - each organization is a node
  - trust relationships among organizations are edges
  - each edge can be considered as a certificate
- **certification path** is a path in the graph which connects relying party with user
- To authenticate a user, the relying party needs to find a certification path
- Graph search is required in order to find a path
- For example, T_1, T_3, T_6 and T_7 is a certification path from relying party R to the user, where R knows T_1's public key and T_7 signs user U's public key

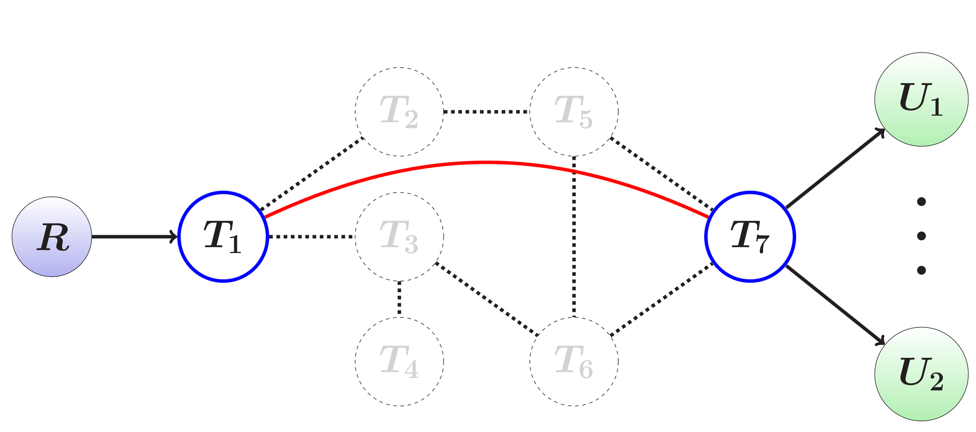


Issues of Internet Authentication

- Risk of trusting on Internet:
  - The relying party bears the risk of a mis-authentication
  - Authentication accuracy is depended on TTPs
  - One relying party's adversary is not necessarily another's
  - A **strong trust model** is needed which allows each relying party to specify the TTPs used in an authentication
  - X.509 and SDSI/SPKI support strong trust model, but not efficiently
- Cost of Internet Authentication
  - Certification path construction requires irrelevant certificates to be fetched and evaluated
  - The more irrelevant nodes are visited, the more bandwidth is needed

SAyI Strategy

- A group is set of users with similar privileges
- Relying party defines **groups** using TTPs it trusts for that authentication
- Allows different quality authentication for different purposes
- SayI only fetches certificates relative to group
- R trusts T_1 and T_7 to provide group information
- T_1 and T_7's public key are fetched by R
- Users' key are signed by T_1 and T_7
- No need to visit T_3 and T_6 or other nodes in the graph.

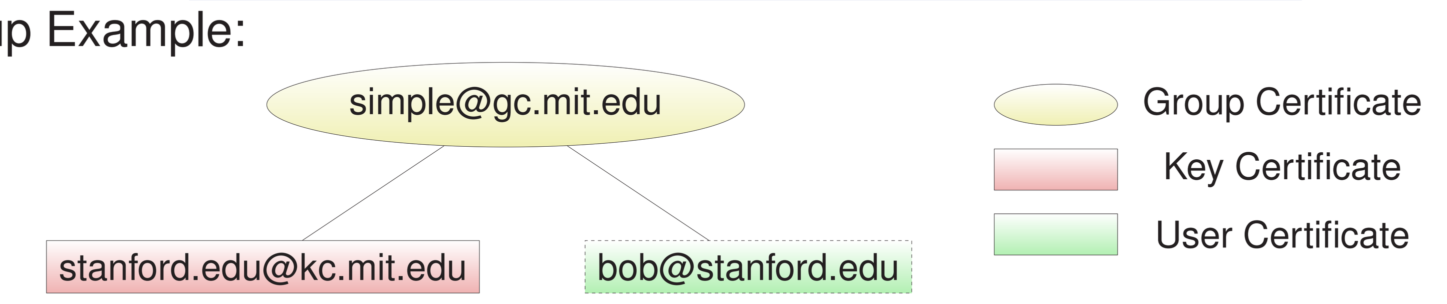


SAyI Groups

- Building Group:
  - Relying party needs to decide which Trusted Third Parties (TTPs) are going to be used
  - TTP decides the users in the group
- Groups can be specified by certificates, and SAyI has 3 types of certificates:
  - **Group**: specifying key names, user names and other group certificate names.
  - **Key**: containing a public key of a TTP
  - **User**: associating user's name with its public key

Type	Name	Example
Group	*l*@gc.*d*	friends@gc.smith.org
		smith.org provides a group of her friends
Key	*l*@kc.*d*	ydom.com@kc.xdom.com
		xdom.com asserts ydom.com's key
User	*l*@*p*	bob@usenix.org
		the user known as bob at usenix.org

- A Group Example:



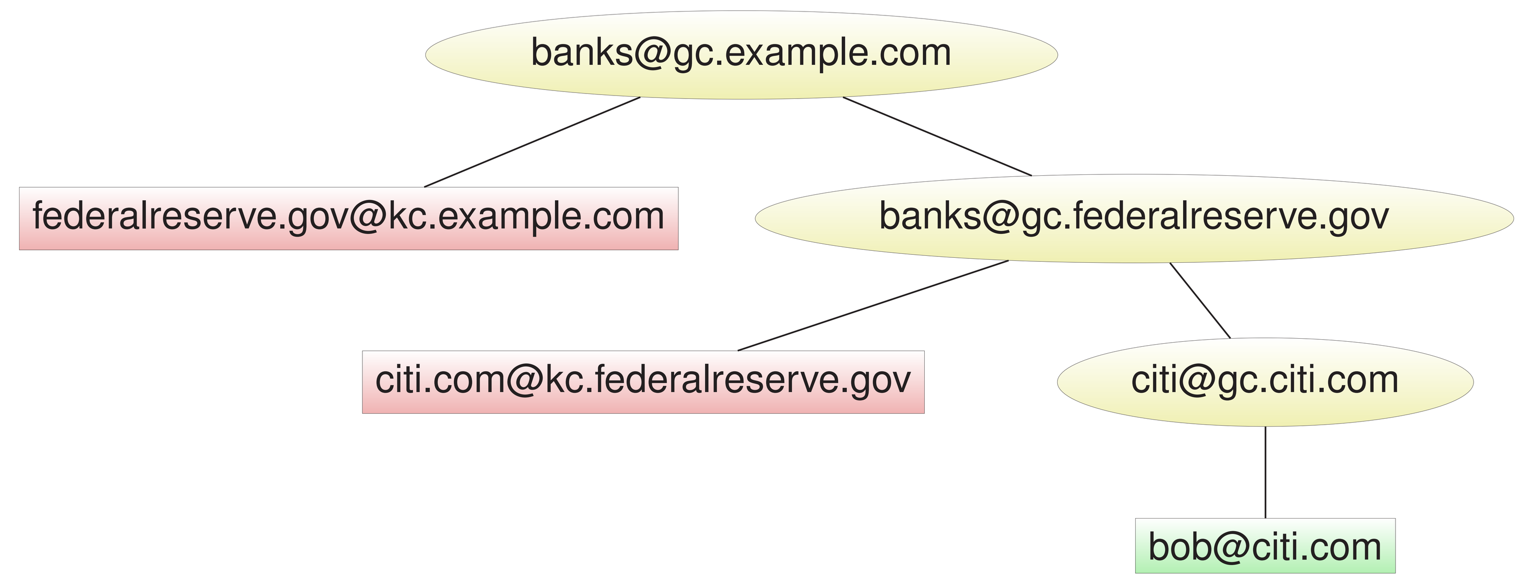
The groups consists of a group certificate of mit.edu, a key certificate for stanford.edu referenced by mit.edu, and a user certificate for bob from standford.edu

SAyI Algorithm

- SAyI architecture:

- SAyI's authentication involves:
  - The user contacts relying party for service with a user certificate supplied
  - Relying party asks cache to fetch the group information which the user belongs to
  - The cache recursively fetch all key and group certificates in the group
  - Relying party requests certification path from the cache in order to verify the user certificate
  - The certification path is finally returned to relying party from cache

Example of How the Algorithm Works



- **Bob** contacts relying party R for service with user certificate bob@citi.com
- R requests cache to fetch certificates in group starting from banks@gc.example.com
- R requests from cache for certification path banks@gc.example.com, federalreserve.gov@kc.example.com, banks@gc.federalreserve.gov, citi.com@kc.federalreserve.gov, citi@gc.citi.com
- Finally, R gets the whole certification path to verify bob@citi.com

Evaluation & Conclusion

Groups	Publishers	Inter-mediaries	Simple Certs	Simple Bytes	Simple Time (sec)	Segmented Certs	Segmented Bytes	Segmented Time (sec)
Universities	9,290	400	1,201	787,190	10.36	801	378,155	7.24
Banks	13,771	400	1,201	1,038,126	12.27	801	431,927	7.65
Hospitals	18,000	400	1,201	1,274,950	14.08	801	482,675	8.03
Municipal Gov.	36,722	2,000	6,001	3,388,982	30.21	4,001	1,772,939	17.88
Small Group	154	6	19	13,170	4.45	13	6,119	4.40
Mega Group	5,000,000	2,000	6,001	281,332,550	2,150.75	4,001	61,332,275	472.28
Internet	200,000,000	280	841	11,200,193,750	85,455.05	561	196,835	5.85

- Bandwidth cost and latency are given for SAyI
- SAyI is compared with a X.509 PKI consisting of 160 organizations, and it shows 8.75 fold speed-up and a 20 fold reduction in bandwidth cost.