Cybersecurity through an Identity Management System

Elli Androulaki, Maritza Johnson, Binh Vo, and Steven Bellovin

Engaging Data Forum

October 2009
Cybersecurity vs. Privacy

Cybersecurity
online integrity, confidentiality & availability

Privacy
control over personal information distribution

Both growing “online” necessities
sensitive information exchange, i.e. med care logins
financial online activities, i.e. banking, taxation
protected systems, i.e. employee access control

However contradictory
cybersecurity requires accountability and authentication, which result in centralization
“Securing Cyberspace for 44th presidency”
privacy is mostly dealt with through anonymization
This talk is about ...

There is a critical need for combining privacy, accountability, authentication in a deployable identity management system.

Furthermore,

What are the user activities to be addressed?
What are their privacy requirements?

Challenging. Why?

by nature,

centralization enables surveillance
anonymization makes accountability and authentication hard
all the current authorities’ interactions
We suggest an Identity Management System

Related Work:
[B00], [CL01], Idemix, Higgins, PRIME, OpenID
“Real-World”

**In our Threat Model**
- Users may try to cheat
  - lie about income for tax purposes or any other payment related case
  - impersonate or frame another user
  - attempt forgeries
- Banks, Tax/Registration Authorities are “honest but curious”, i.e. may attempt to learn extra information
- Employers may also try to cheat on taxes
- Other services may lie about payments

**In our Requirements**
- Privacy, Accountability, Fairness, Misbehaving parties’ detectability, Deployability
Card Unforgeability
Card non Transferability
User Uniqueness
Privacy preserving demonstration of ...
card-ownership
user-attributes

Card Loss/Compromise Management
strongly authenticated Loss Report
Content Recovery - Card Reissue
Card and card credentials’ Blacklistability
Freezing of subscriptions
Bank Account Management

Single ID-based Registration Entry

Support of two types of accounts
  anonymous, but traceable
  regular

Fair and privacy-preserving Tax reporting

Account privacy maintenance
  w.r.t. bank collaboration with Employers, Merchants, etc.

Account Ownership revocability
  the account’s owner “misbehaves”, is in debt
  the account’s owner dies
Employment

Single ID-based Registration Entry

Fair and privacy-preserving Payments

in proportion to employee’s service
restricting tax-evasions
without leaking bank accounts’ ownership

Access Control in Critical Infrastructure

authenticated: an employee is ...
accurately identified within his company
recognized as a member of his company everywhere else
accountable: a misbehaving employee is traced and fully identified
revocable, when an employee is fired
Taxation and others

Taxation

Single ID-based Registration Entry
Fairness, Accountability, User-Privacy
Maintenance w.r.t. all collaborating entities

Other Online Services, i.e., online subscriptions to magazines, health care, travel agencies.

Single or multiple Registration Entries
User Anonymity and activity unlinkability
Accountability
In conclusion

Need a widespread system to achieve cybersecurity while protecting privacy
We want to provide this with a central ID card system that provides functionality mirroring real world transactions

Future Directions and Ongoing Work involve …
the detailed design of this system
Thank you!

Questions?