Identity Management and Privacy

Panos Papadimitratos

EPFL

Identity Management

SEVECOM

- Identity
  - *Data that uniquely characterize a system entity*
  - System- and context- dependent
  - Partial
- Personal or sensitive data, which warrant special protection or limited disclosure
- Identity Management
  - *Processes for the design of identities and identity attributes for system entities, and the administration of identities and attributes*

Privacy

SEVECOM

- Broad term, with many definitions; hard to define rigorously
- Essentially, privacy means:
  - *To protect individuals' personal or sensitive data from others*
- Communication and networking systems essentially multiply 'opportunities' for users to disclose private information
- Privacy
  - Confidentiality
  - Anonymity
  - Unlinkability

Is privacy an important problem?

SEVECOM

- Almost all cellular mobile telephone users would respond ‘yes’ to the question ‘Are you concerned about your privacy?’
- Almost all web surfers are reluctant to provide personal information (name, email, address etc) unless necessary
- Almost all on-line services (sites) provide a ‘privacy policy’ document/link

Is privacy an important problem? (cont'd)

SEVECOM

- Yet
  - Cell-phone users do/can do almost nothing to protect their privacy than rely to the provider
  - Users are asked for redundant or often irrelevant information when perform a transaction
  - Service providers have their data bases compromised, while companies specialize in collecting data to profile users preferences
- "…the mobile industry has not been particularly active… there is a general lack of understanding of privacy issues within the industry... privacy aspects not being considered in the design phase of many new systems… commercial incentives to protect the user's privacy are small..." [PAMPAS]

Recent and on-going efforts

SEVECOM

- There has been recent interest on privacy
- European and US projects
  - PAMPAS (Pioneering Advanced Mobile Privacy and Security)
  - MODINIS-IDM (Study on Identity Management on eGovernment)
  - PORTIA (Privacy, Obligations, and Rights in Technologies of Information Assessment)
  - FIDIS (Future of Identity in the Information Society)
  - PRIME (Privacy and Identity Management for Europe)
- General focus
  - Internet
  - Vehicular communication systems have been out of the picture (apparently ☺)

Defining Privacy (or aspects of) SEVECOM

- Pseudonym
  - *Identifier different than the actual identity of the entity*
  - Does not carry identity information
    - Could be a partial identity
  - Usually associated with attributes
- Unlinkability
  - *Any two or more objects (e.g., data, services, messages) in a system cannot be correlated with the same entity or a third object*
  - *Any two or more pseudonyms cannot be correlated with the same identity and thus entity*

Defining Privacy (or aspects of) (cont'd)

SEVECOM

- Anonymity
  - Anonymity set: *The set of all entities in a system with similar attributes or with respect to a particular context*
  - Definition 1: *An entity cannot be identified among all entities that belong a particular anonymity set*
  - Definition 2: *The actions of an entity cannot be linked to the entity by a (set of) observers*

Relevant research

SEVECOM

- Protection of Internet communications
  - [Syverson97] Anonymous connections – onion routing
- Protection of commercial transactions
  - [Stubblebine00] Unlinkable serial transactions
- Protection of web-based communications
  - [Reiter97] Crowds – Anonymity for web transactions
  - [Anonymizer] The anonymizer
- Protection of e-mail
  - [Cotrell] Mixmaster – re-mailers
  - [Gulcu96] Email mixing – Babel
- Electronic cash
  - [Chaum93] Blind signatures – untraceable payments
  - [Wayner96] Digital cash

Relevant research (cont'd)

SEVECOM

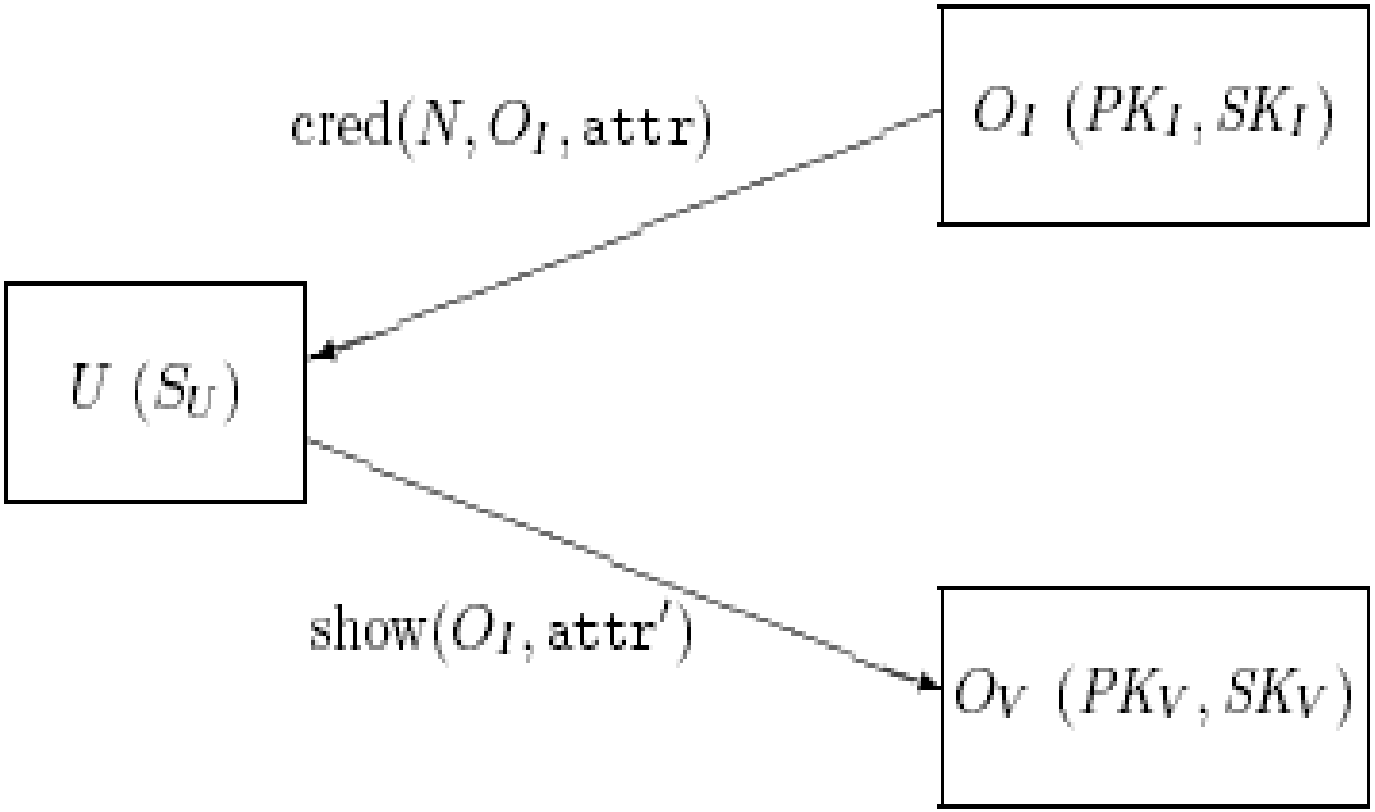
- Anonymous credentials
  - [Chaum81] Pseudonyms - email
  - [Chaum85] Security without identification
  - [Chaum87] Secure and privacy protecting protocol
  - [Damgard88] Credential with provable security against abuse – payment scheme
- Group signatures
  - [Chaum91] Group signatures
  - [Camenisch97] Large groups
  - [Ateniese00] Practical, provably secure
- Zero-knowledge proofs
  - [Goldwasser85] The knowledge complexity of interactive proof systems
  - [Brassard88] Minimum disclosure proofs
  - [Bellare92] Defining proofs of knowledge

Anonymous credential systems

- Example: Idemix
  - Prototype developed within PRIME; based on prior work:
    - [Camenish03] Signature scheme with efficient protocols
    - [Lysyanskaya02] Signature schemes and applications
- Notation
  - User *U*
    - Has a single master secret S_U connected to all pseudonyms and credentials issued to the user
  - Issuing Organization O_I
    - Uses its private key when generating the credential
  - Verifying Organization O_V
    - U uses the public key of O_V when showing the credential
  - De-anonymizing organization O_D
  - User Pseudonym *N*
  - Credential *C*
  - Credential attributes *attr*

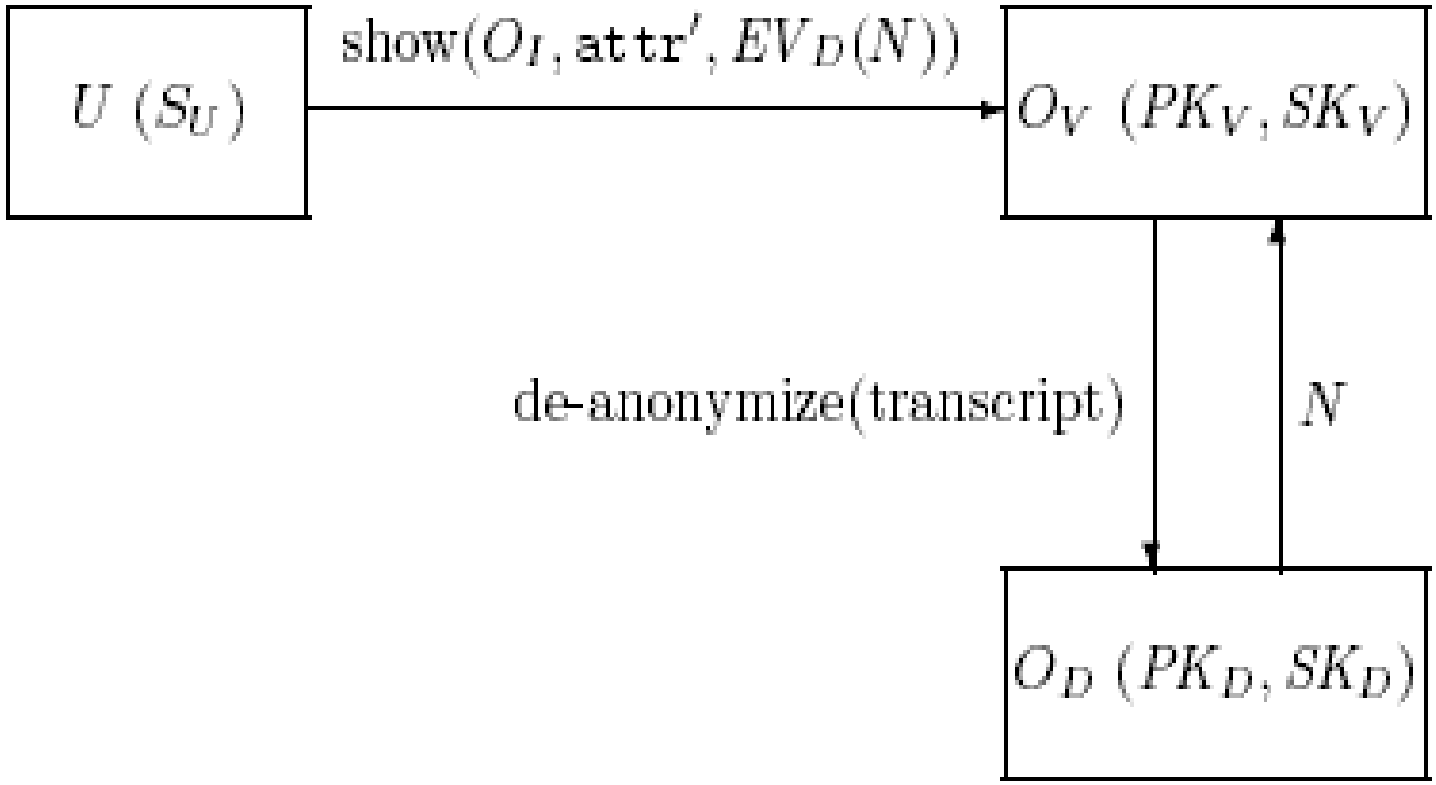
Idemix (cont'd)

- Basic protocols – Idemix



Idemix (cont'd)

- Conditional anonymity - 'de-anonymization'



Current state

SEVECOM

- Vehicular/transportation systems
  - Administered by public organizations
    - Department of Motor Vehicles
    - City or County or State Authorities
  - Participants:
    - Vehicles
    - Drivers
- Rigid identity management processes
- Liability
  - Full anonymity is not sought

Current state (cont'd)

SEVECOM

- Drivers and vehicles already identified in multiple ways
  - Drivers
    - Name, license number, mailing address, date of birth,...
  - Vehicles
    - Vehicle identification number (VIN), registration number, type of the vehicle,…
- Side-observation:
  - Vehicle license plates do not alone disclose the driver's/registrant's name
    - Binding is known to authorities
    - Supposedly not to other drivers
      - **BUT** companies in the Internet sell inverse-lookup of driver names and addresses…

Vehicular communications

SEVECOM

- System participants
  - Users
  - Network nodes
  - Authorities
- Users: individuals that operate vehicles
  - Focus on network operation and device communication
  - Yet, binding users to vehicles is an issue
    - Many-to-many relationship

Vehicular communications (cont'd)

SEVECOM

- Network nodes
  - *Infrastructure*
    - Roadside units
      - Static, quasi-static
    - Mobile infrastructure
      - Public safety vehicles
        - **Police, road assistance, firefighters, ambulances**
      - Buses
  - *Non-infrastructure vehicles*
- Authorities
  - Servers at the wire-line part of the network
  - Infrastructure acting as a gateway to/from the wireless part of the vehicular network

Vehicular communications (cont'd)

SEVECOM

- Relation between "physical" and the VC identities
  - Integration - Adaptation
  - Extension
- Vehicular communications identity
  - "Physical world" set of identity attributes
  - Network identifiers
    - At different layers of the protocol stack
  - Service identifiers/credentials
  - Cryptographic keys and credentials

Similarities between VC and general efforts

SEVECOM

- Protection of sensitive data is equally important
- Precise definition of processes and policies for privacy protection are necessary
- Minimum private (identity) information disclosure, on a need-basis only
- Fine-grained control mechanisms for system entities to regulate the private information disclosure

Similarities between VC and general efforts (cont'd)

SEVECOM

- Accountability, access control
  - Authentication and anonymity/unlinkability
  - Unconditional anonymity will not be acceptable
  - Revocable anonymity or 'de-anoymization'
- Need for multiple credentials per node/system entity
  - Multiple organizations, multiple services
  - Short-lived, context-specific credentials
- Required features for anonymous credentials
  - No sharing
    - Prevent 'passing' of credentials
    - Prevent 'misleading showing' of credentials

Differences between VC and general efforts

SEVECOM

- VC systems are not user-centric
  - Vehicles play a central role
  - Vehicles can be multiply identifiable
    - E.g., Individual subsystems of the vehicle
- VC patterns are not ‘transactional’
  - Potentially any node can be the verifier
  - Broadcast, multicast, anycast
  - Based on context- (e.g., location) or node- (e.g., role, characteristics) specific

Differences between VC and general efforts (cont'd)

SEVECOM

- Frequent/high-rate/continuous communication
  - Periodic
  - Triggered
  - Dependent on network characteristics (e.g., density)
- Beyond the discretion or control of the node or the user to regulate it
  - Safety messages and applications must be 'always-on' without the user being able to select exactly what information to disclose

Differences between VC and general efforts (cont'd)

SEVECOM

- Performance overhead can be critical
  - Example: Idemix
  - Assume:
    - *Infrastructure nodes: No anonymity*; instead, rich description of identity and attributes
    - *Non-infrastructure nodes: Anonymity*
  - With all optimizations in place [Camenish02], one showing of a credential (with expiration date and revocation capability enabled) requires 2.5 sec, or roughly 12 times the period of safety messages

Differences between VC and general efforts (cont'd)

SEVECOM

- Need anonymity at the network layer
  - Not really a difference but a point of caution
- Other considerations
  - Coexistence/inter-operability with other wireless communication systems (e.g., cellular, WiMax (?),…)
- Gradual deployment
  - The 'clean state' advantage may or may not be present

Conclusions

- Within the context of vehicular communications, privacy and identity management are not currently undergoing a standardization process
  - IEEE 1609.2 appears more like a wish list
- Similarities and differences from general approaches
- Unique characteristics
- No self-evidently applicable solution among the available ones
- Assumptions and requirements for privacy and identity management can strongly influence the overall architecture

References

- [PAMPAS] "PAMPAS: Pioneering Advanced Mobile Privacy and Security,"URL: http://www.pampas.eu.org/index.html
- [MODINIS-IDM] "MODINIS-IDM: Study on Identity Management on eGovernment," URL: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome
- [PORTIA] "PORTIA: Privacy, Obligations, and Rights in Technologies of Information Assessment," URL: http://crypto.stanford.edu/portia/
- [FIDIS] "FIDIS: Future of Identity in the Information Society," URL: http://www.fidis.net/
- [PRIME] "PRIME: Privacy and Identity Management for Europe," URL: http://www.prime-project.eu.org/
- [Chaum81] David Chaum "Untraceable electronic email, return addressess, and digital pseudonyms," Comm. of ACM, 24(2): 84-88, Feb. 1981

References (cont'd)

SEVECOM

- [Bangerter04] E. Bangerter, J. Camenisch, and A. Lysayankaya, "A Cryptographic Framework for the Controlled Release of Certified Data," in proceedings of the Twelfth International Workshop on Security Protocols, Cambridge, England, April 2004
- [Camenisch02] J. Camenisch and E. Van Herreweghen, "Design and Implementation of the idemix Anonymous Credential System," in proceedings of the ACM Conference on Computer and Communications Security (CCS),Washington, DC, November 2002
- [Camenisch01] J. Camenisch and A. Lysyanskaya. "Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation," In EUROCRYPT 2001, vol. 2045 of LNCS, pp. 93–118. Springer Verlag, 2001.
- …