Security vs. Privacy:
Revisiting the AAA Fundamentals

Yves Deswarte
desparte@laas.fr

LAAS-CNRS
Toulouse, France

Security & Privacy:
Two Fundamental Rights

Universal Declaration of Human Rights, UN, 1948

- **Article 3.**
  Everyone has the right to life, liberty and security of person.

- **Article 12.**
  No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
Information System Security (ISS) & Privacy Protection

- Privacy Protection = confidentiality of personal information

- Confidentiality: one of the basic security properties
  
  
  \[ CIA = \text{Confidentiality, Integrity, Availability} \]

- ISS provides the means to protect privacy
  - AAA : Authentication, Authorization, Accounting

- But...

...the devil lies in the details
...the devil lies in the details

- Some security techniques
  - Audit, evidence collection
  - Traceability
  - Strong authentication, ...

... are threatening privacy!

- Imbalances:
  - Honest citizens are more observed than criminals
  - Companies collecting illegal personal data are stronger than their victims: personal data = currency
  - One-sided contracts: ex. Facebook, Google, Apple...

- Self-censorship --> liberty reduction

Privacy

Privacy (noun)

- the state or condition of being free from being observed or disturbed by other people: she returned to the privacy of her own home.
- the state of being free from public attention: a law to restrict newspapers’ freedom to invade people’s privacy.
1\textsuperscript{st} Principle to protect privacy

- **"Sovereignty"**: keep control of your personal data, they belong to you!
  - store them on a personal device (smartcard, smartphone, tablet, laptop...)
  - if you disclose your data to another party, impose **obligations** on their use
    - Erasure on demand (*right to be forgotten*)
    - Expiration date
    - Notification in case of transfer or unexpected use
    - etc.

2\textsuperscript{nd} Principle to protect privacy

- **Personal data minimization**
  - transmit only the data needed by those entrusted to:
    - perform the agreed task (and only to them)
      - "need-to-know"
    - destroy it after use (*right to be forgotten*)

- ... in "cyberspace" like in the real world

- ...with limits: some personal data need to be transmitted to judicial authorities in case of dispute or enquiry (e.g., money laundering) "pseudonymity" rather than total anonymity

- Links: minimization $\leftrightarrow$ purpose: "legitimate"
  collected data: "not excessive"
Security Technologies and Privacy

- **AAA**: Authentication, Authorization, Accounting
  - **Authentication**: each user is to be identified safely
    - Identification + Identity Verification
  - **Authorization**: each user can only perform operations authorized for her/him
    - Manage and verify rights for each identity
  - **Accounting**: each user is kept liable for her/his acts
    - Audit: collect evidence by identity

“Virtual” Identity

- **Identity** = representation of a person in an information system

- In general, it contains:
  - External identifier, corresponding to only one person (e.g., login name)
  - Authentication information (e.g., password, public key, zero-knowledge proof data, biometric reference, ...)
  - Other information linked to the person
    - **Data**: civil identity, credit card number, mail address, phone number, e-mail@, ...
    - **Meta Data**: internal identifiers (e.g., uid, gid, ...), privileges, roles, groups, IP@, MAC@, ...

- **Remark**: a single person may have several (partial) virtual identities
Identification & authentication

- **Identification** = retrieve the identity of a person among all registered persons
  - User: provides the external identifier

- **Authentication** = verification that the identity corresponds to the user who presents:
  - Something s/he knows (e.g., password)
  - Something s/he owns (e.g., smartcard)
  - Something s/he can do (e.g., manuscript signature)
  - Something s/he is (biometry, e.g., fingerprint)

What is the Identity used for?

- **Authorization**: assign different privileges to different users
  - Right management:
    - Grant rights to each user
    - Enable/disable actions according to these rights
    \(\Rightarrow\) Without an identity, a user has only minimal rights

- **Accounting**: keep each user liable for her/his acts
  - Identify a posteriori who has committed something bad
    - Requires a different identity for each user
    - Requires recording sensitive actions that are attempted by each user (Audit)
    \(\Rightarrow\) Without an identity, a user can only perform actions that cannot be harmful
But...

... authentication and accounting are infringing “minimization” and “sovereignty”

- If you need to present your identity to exercise your rights → personal data disclosure
- You cannot control how are used your personal data collected for accounting!

Identity and Privacy

- Identity = any representation of a person in an information system (not only “users” !!!)
  - Patients, personnel, clients, …

- Identity is a personal information!
  - Sovereignty: the person should keep control on it
  - Minimization: as little information as possible

⇒ No identification without consent!
  - fingerprint, DNA, video-monitoring, RFID…
  - IP addresses, Caller-ID, …
Multiple virtual identities

- Reduce/control links between the person and the personal data (control the *linkability*)

- Basic rule: for public access, anonymity

- But for customized / privileged access, *pseudonyms*
  - Preferences (e.g., weather forecast)
  - Different "roles" \(\rightarrow\) different pseudonyms
    - E.g., tax payer and elector
  - Pseudonym lifetime: related to linkability
    \(\rightarrow\) one-time pseudonyms
  - Authentication strength: related to identity stealing risks (and liability)

- *Multiple virtual identities managed by the user vs. “single-sign-on”* e.g., IdNum, Liberty Alliance, OpenID

---

Authorization

- Today on the Internet: client-server
  the server grants or denies privileges to the client
  according to her/his claimed identity (possibly
  verified by authentication mechanisms)

- The server needs to store personal data
  -> evidence in case of dispute

- These data can be used for other purposes:
  client profiling, direct marketing, client data trading,
  blackmailing, ...: personal data = currency

The client-server scheme is obsolete!

- Internet transactions spread among more
  than two parties (e.g., e-commerce)

- These parties can have different (or even
  opposite) interests: mutual suspicion

- Harmful for privacy:
  infringing the “need to know” principle
Authorization without identity?

- Prove your rights without disclosing your identity
  - Anonymous credentials

- Examples
  - Subscription cards, association membership, ...
  - Driving license, identity card, elector card, ...

- Multiple certificates?
  - ex: SPKI: attribute certificates / authorization certificates
  - ... but linkability: public key!

Idemix anonymous credentials
Group Signature

1 public key for signature verification

\[ K_v \]

\[ K_s(1) \]
\[ \vdots \]
\[ K_s(n) \]

n private keys for signature generation

\[ \text{challenge} \]

\[ [\Sigma]_{K_v} = ? = \text{challenge} \]

Accounting

- The Authority maintains a directory (authenticated user, signature key)
- The server records the signatures -> audit log
- From the signature, the Authority can recognize the signer -> anonymity lifting
A new scheme for AAA

- Separate authentication and authorization enforcement
  - Credential Issuing Authority: authentication + right granting → anonymous credential
  - Server: verifies the validity of the anonymous credential and enables the authorized actions

- Separate evidence collection and accounting
  - Server: audit the actions → log the credentials
  - Credential Issuing Authority: if case of evidence of wrong doing, lifts the credential anonymity

→ the anonymous credential should not be transferable (nor forgeable...)

Non transferability?

- Idea: a personal device (smartcard) + biometric recognition
**Conclusion**

- It is possible to enforce both security and privacy by the same technology.

It is possible:

- To prove rights without disclosing identity
- To develop Privacy-Enhancing Technologies that do not provide impunity to criminals
- To develop Security Technologies that do not invade privacy

**Recommendations**

- Analyze privacy impact as soon as inception of a new technology: “Privacy by Design”, else “Privacy by disaster”
  - Privacy by Design, Privacy by Default, Privacy Impact Analysis
  - Right to be forgotten

- Take the opportunity of new services installment to provide privacy benefits
e.g., German electronic identity card --> certified pseudonyms

- Respect the sovereignty and data minimization principles

- Develop new personal devices to facilitate privacy:
e.g., personal data storage, identity management, e-Cash, …