Principles of Computer Security

Alvin Lin

January 2018 - May 2018

Privacy

Privacy is a concept that overlaps with security, especially confidentiality. There has been a dramatic increase in the scale of information that is collected and stored for law enforcement, national security, and economic incentives. Individuals have become increasingly aware of access and use of personal information and private details about their lives. Concerns about the extend of privacy compromise have led to a variety of legal and technical approaches to reinforcing privacy rights.

The Evolution of Privacy

In the past, we didn't have a lot of the protections we had. Phone numbers were freely published, and there weren't many restrictions on the sharing of personal information. Personal information categories:

- Social security number
- Address
- Phone number
- Date of birth
- Religious affiliation
- Military address

Personally identifiable information (PII) allows other to track and find an individual and can be used for illegal or criminal activities. Information that is **sensitive** can

be used to harm or inconvenience an individual. **Direct identifiers** allows information to be directly tied to an individual, and **quasi-identifiers** can be combined with other information to identify an individual. Information that is not personally identifiable can become personally identifiable in this way if it is combined with other acquired information.

Protecting PII

Student information is protected by the **Family Education Rights and Privacy Act (FERPA)**. Protected health information must be in compliance with the **Health Insurance Portability and Accountability Act**. Personally identifying information in general is protected by varying laws in each state. Businesses, charities, and governments who handle sensitive information are responsible for protecting sensitive information. We have to be aware because personally identifiable information lurks sometimes where we least expect it and anonymization is not enough.

European Union Directive on Data Protection

This directive was adopted in 1998 and states that members must protect fundamental privacy rights when processing personal information. It was organized around the following principles:

- Notice
- Consent
- Consistency
- Access
- Security
- Onward transfer
- Enforcement

United States Privacy Initiatives

The Privacy Act of 1974 dealt with personal information collected and used by federal agencies. It permitted individuals to determine the records kept on them, forbid records being used for other purposes, and obtain access to records, and correct

and amend records appropriately. This act ensured agencies would properly collect, maintain, and use personal information. It created a private right of action for individuals.

Code of Practice for Information Security Management (ISO 27002)

- Organizations must develop and implement a data policy for the privacy and protection of personally identifiable information.
- They must communicate the policy to all persons who process personally identifiable information.
- They must develop appropriate management structure and control to comply with this policy and relevant legislation/regulations.
- They must appoint a responsible person (a privacy officer) to guide managers, users, and service providers on their individual responsibilities and specific procedures.
- Their responsibility for handling personally identifiable information and awareness of privacy principles must following relevant laws and regulations.
- They must implement appropriate technical and organizational measures to protect personally identificable information.

Properties of Privacy

- Unobservability: A user may use the resource or service without others being aware of its use. Germany views unobservability essential to constitutional rights.
- Anonymity: A user may use the resource or service without disclosing their identity. The service should protect the user identity. This makes it harder to establish trust between the system and users.
- Unlinkability: A user may use the resource or service multiple times without others being able to link the uses together.
- Pseudonymity: A user may use the resource or service without disclosing their identity, but can still be accountable for that use.

None of these properties can be implemented totally. Any interaction between a user and a security system leaks information about users. The main threat is that attacks can collect long-term user data and use statistical methods to deanonymize users.

Privacy and Data Surveillance

The demands of homeland security and counterterrorism have imposed new threats to personal privacy. Police and intelligence agencies are now aggressive in using data surveillance to fulfill their missions. Private organizations are also exploiting their abilities to build details profiles of individuals through the Internet, increases in electronic payments, cell phones, and other mobile devices. Both policy and technical approaches are needed to protect privacy when both government and nongovernment organizations seek to learn as much as possible about individuals.

K-Anonymity

Can private data about people be shared with researchers with guarantees that individuals cannot be re-identified while the data is practically useful? The k-anonymity protection model allows for data to be released only when any one person cannot be distinguished from at least k-1 individuals whose data is also in the release.

Differential Privacy

Differential privacy approaches only allow queries where the result is claimed to have strong, provable privacy guarantees.

> You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech