Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"

CIC
Centro de Investigación en Computación

Laboratorio de Ciberseguridad

Centro de Investigación en Computación(CIC)
Instituto Politécnico Nacional - México.

Cyber security A-15

Dr. Ponciano Jorge Escamilla Ambrosio
pescamilla@cic.ipn.mx
http://www.cic.ipn.mx/~pescamilla/

Cyber Security A-15

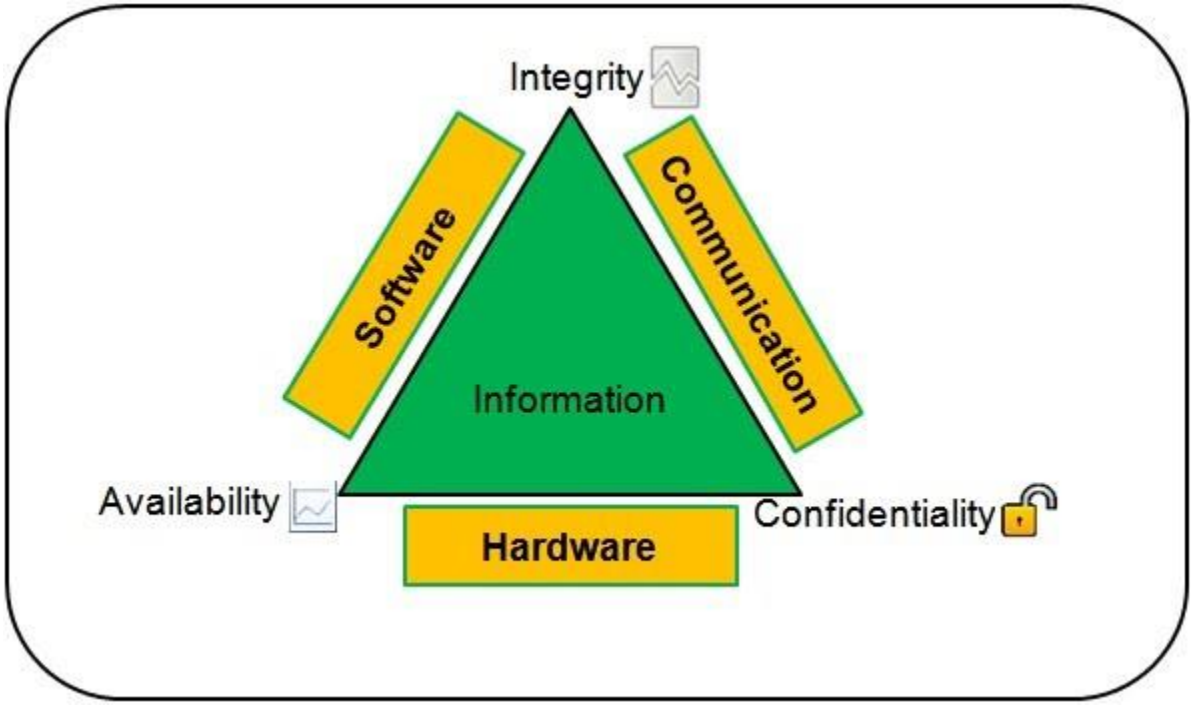
- Instructor
  - Dr. Ponciano Jorge Escamilla Ambrosio
  - pescamilla@cic.ipn.mx
  - http://www.cic.ipn.mx/~pescamilla/
- Class meetings
  - Tuesdays and Thursdays 14:00 – 16:00 hrs.
  - Classroom A3

Cyber Security A-15

2. Ethics in Cyber Security & Cyber Law
   - 2.1. Privacy
   - 2.2. Intellectual property
   - 2.3. Professional ethics
   - 2.4. Freedom of speech
   - 2.5. Fair user and ethical hacking
   - 2.6. Internet fraud
   - 2.7. Electronic evidence
   - 2.8. Cybercrime
   - 2.9. Cyberwarfare

Antecedents

- The ‘CIA’ concept



CIA

- **Confidentiality**
  - "Confidentiality refers to limiting information access and disclosure to authorized users -- the right people -- and preventing access by or disclosure to unauthorized ones -- the wrong people" (http://it.med.miami.edu/x904.xml)
  - The meaning of the confidentiality reflects the basic concept of security which is to protect private or secret information from obtaining by unwanted people.

CIA

- Integrity
  - Integrity can be divided in two aspects, the personality “of being honest and having strong moral principles” and for data resources it means “the state of being whole and undivided” (http://oxforddictionaries.com/)
  - data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle

CIA

- Availability
  - Availability means “assuring information and communications services will be ready for use when needed”
  - Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down

CIANA

- Non-repudiation
  - In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction

- Authenticity
  - In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be

2.1. Privacy

What is Privacy?

"The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Alan Westin: Privacy & Freedom,1967)

Personal information

- Personal information
  - intrinsic physical data
    - Name
    - Date of birth
    - Gender
    - Location data
      - Home address
      - Telephone number

Personal information

- Personal information
  - intrinsic physical data
    - Financial data
      - Salary
      - Bank account balance
      - Credit card number
    - User-created data
      - Confidential correspondence
      - List of personal references
    - Data assigned by other entities
      - Bank account number
      - Social security number

Personal information

- Identifying personal information
  - The subset of personal information that reveals the identity of the entity
- Non-identifying personal information
  - Personal information that not reveals the identity of the entity
    - Information (e.g. salary) that are typically sensitive only when revealed in conjunction with identifying information

Privacy as a process

"Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication…." (Westin, 1967)

Providing confidentiality of personal information

- Two primary techniques (non-identifying personal information)
  - Encryption
    - Personal information may be encrypted so that it may only be seen by intended recipients while it is in transit or while it is in storage
  - Access control
    - Limits who may do what with a given resource
    - Access control allows an entity to explicitly specify which other entities may (or may not) read this information.

Three properties to achieve privacy

- Solicitude
  - Freedom from observation or surveillance
- Anonymity
  - Freedom from being identified in public
- Reservation
  - Freedom to withdraw from communication

Exposure and disclosure of information

- Exposure
  - Communication of identifying information to unintended parties: the identity of the entity is exposed to others
- Disclosure
  - Communication of other types of personal information to unintended parties: this information has been disclosed to others

Exposure and disclosure of information

- Direct exposure/disclosure
  - is the determination of user identity or other personal information by an observer or by another participant in the exchange from the explicit contents of a single transaction or message
- Indirect exposure/disclosure
  - is the determination of user identity or other personal information by inference or from the correlation of the contents of several transactions or messages

Properties for privacy-enabled systems

- Control
  - One must be able to control the type and extent of information revealed to others
- Accountability
  - The act of disclosing information usually implies making its recipients accountable for actions that use that information

Properties for privacy-enabled systems

- Plausible deniability
  - When being asked about something private, a person must be able to plausibly deny noticing or understanding the question instead of appearing to refuse to answer
- Reciprocity
  - The disclosure of personal information is normally not one-sided, but mostly symmetrical: the amount of disclosure from A to B is strongly related to the amount of disclosure from B to A

Properties for privacy-enabled systems

- Utility
  - On a more sociological point of view, there are important questions that must be answered, related to the utility of private data. For example, can the utility of private data be measured and traded? This is a very hard problem as the capabilities of future information systems are highly unpredictable. For example, nobody in 1981 knew that their newsgroup postings would be indexed and easily searchable at Google Groups

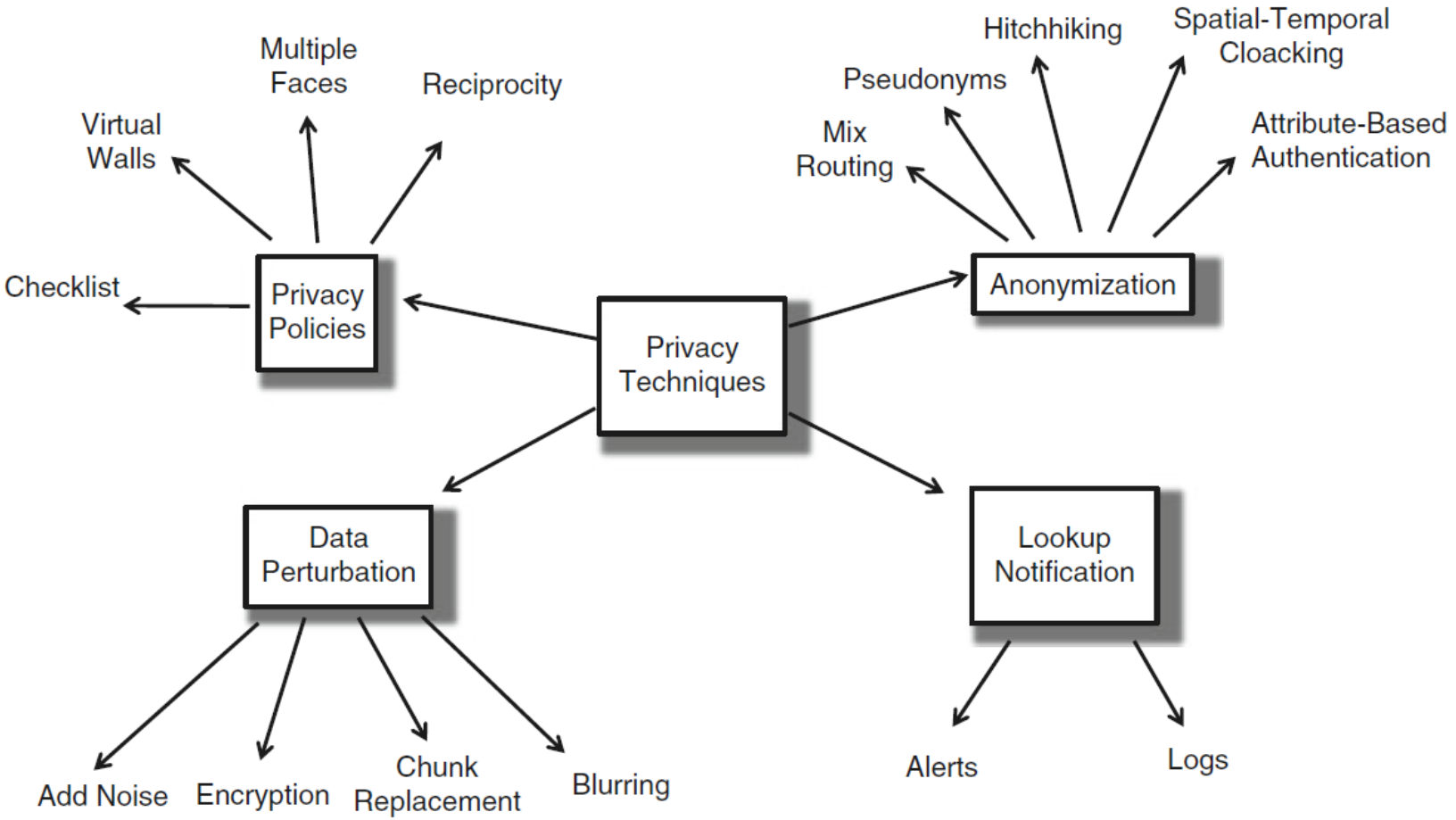
Privacy management techniques

- Privacy policies
  - Applications using this technique allow the user to provide rules (privacy policies) that define to whom and to what extent is his information revealed to others
- Data perturbation
  - This type of technique consists on transforming or partially omitting information before being delivered to the consumer, in such a way that it is impossible to reconstruct the original message while still keeping (some of) its usefulness

Privacy management techniques

- Anonymization
  - Using this technique, the information is delivered intact to context consumers except for its author, which is removed or replaced with one that cannot be used to infer the real author
- Lookup notification
  - This technique consists of providing the user with information of who has consumed his context information and when

Privacy management techniques



Privacy policies

- Checklist
  - It presents the user with a checklist of types of information (e.g., personal bio, photos, location), asking the user to choose who is allowed to see that information
- Virtual Walls
  - The idea is to set up user-defined policies based on the concept of walls around physical places where sensors are deployed. These walls can be configured using a GUI and feature a three-level permission scheme: transparent, translucent, and opaque

Privacy policies

- Multiple Faces
  - Users predefine a small set of disclosure policies, thinking of each one as a different public "face" they might wear
- Reciprocity
  - user A reveals as much of himself to user B as user B reveals to user A. It mimics a common (most of the times unconsciously) behavior in the real world when dealing with privacy issues

Data perturbation

- Add noise
  - This technique perturbs data by adding noise (useless data) before sending it to the server
- Encryption
  - This technique works by encrypting all personal information (e.g., with a symmetric key) transmitted through a secure channel to everyone that is allowed to consume the information

Data perturbation

- Chunk replacement
  - to replace chunks of data with synthetic but realistic samples that have a limited impact on the quality of the aggregated analysis
- Blurring
  - to disclosing something true but not specific enough to reveal sensitive information and it is a well-known human behavior to control privacy

Anonymization

- Mix routing
  - A mix is a message router that forwards messages in such a way that an adversary cannot match incoming messages to outgoing messages.
- Pseudonyms
  - A special type of anonymity is pseudonyms, where an individual is anonymous, but maintains a persistent identity (a pseudonym)

Anonymization

- Hitchhiking
  - The key idea is that a person does not send his location but rather information that he collected at a given location
- Spatial-temporal cloaking
  - an implementation of k-anonymity based on two variables: location and time. Starting with location, it subdivides the area around the subject's position until the number of subjects in the area falls below a certain threshold k (thus achieving k-anonymity), using quad-tree algorithms

Anonymization

- Attribute-based authentication
  - associate data with some non-identifiable attributes of the user (e.g., age, gender) instead of the user himself, thus guaranteeing anonymity

Lookup Notification

- Alerts
  - Applications using this technique provide the discloser of information with immediate visual or audio feedback when someone is consuming that information
- Logs
  - logs represent a less intrusive technique, since they just register all consumptions of personal context information in a log which can be consulted by the information discloser at any time, when he wishes so

Privacy principles

- Organizations and regulatory bodies have produced a large collection of privacy guidelines and privacy principles
  - Bill C-6, the CSA Model Code, the EU Directive on Data Protection, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm–Leach–Bliley Act (GLBA), the OECD Privacy Principles, and the Fair Information Practice Principles