Definitions and understanding of
—information security
--cryptology or cryptography
--trusted computing
--privacy
--

Xuejia Lai
Dept. of CS, Shanghai Jiao Tong Univ.
lai-xj@cs.sjtu.edu.cn
2012-12-07

Need for theory of IT-security

- Issues in Information security
  - Scientific like
    - Confidentiality
    - Authentication
    - Access control
  - More engineering
    - Virus protection
    - Intrusion prevention
    - Copy-right protection
    - Content filtering

What is information security?

- We are all working on information security, but what is information security?

The ISO definition:

Information security is about preserving of confidentiality, integrity and availability of information. - ISO 17799/ BS 7799

This definition is not satisfactory:

- cryptography (only a small part)
- +availability (beyond security)

The right definition

- Information theory is the science of communication in the presence of noise (Shannon).
  - 信息论研究噪音干扰下的通信.
- Cryptology is the science of communication in the presence of adversaries (Rivest).
  - 密码学研究有对手参与的通信.

Information security is the science of information system in the presence of adversary.

信息安全研究有对手存在的信息系统

☆1.Security is a part of information system1.9

- **Definition:** ***Information security is the science of information system in the presence of adversary.***
  - **Our goal is still information processing, so we are dealing with communication, storage, computer system, …,etc.**
  - **Security is a (not essential) part of information system.**
  - **Remember the original purpose in developing security (eg. SAV kills WinXP), Do not setup security just for security’s sake.**
- **There exists 100% security (no adversary)**

2. Security is becoming necessary

- **Security is becoming necessary** because the presents of adversary – is increasing:
- IT-techniques is spreading in our life
- The threshold for making damage if getting lower
- Outside enemy and Insider, even ourselves
- Attacks become organized actions, not only individual activity - APT

crossing

- Information security involves mathematics, physics and other basic sciences; computer science and technology, communications engineering, electronics and network technology and other applied sciences, law, management, psychology, ethics, sociology and other humanities. therefore, information security has multidisciplinary characteristics. from the point of view of technology , information security related to software technology, communications technology, also with the security services, security management, and is closely related to public information ….

- Information security ---we do everything,but nothing better?

5. Distinctive merit of security : one-way

- Information security is different from other general systems in:
  - – Basic idea: one way function – easy to use and hard to break.
- Equivalent definition: Information security is the technique for one-wayness
- Examples. (you don’t see these in other areas):

  Ciphers, hash functions, random numbers

  Digital signature, Zero-knowledge proof

  Number theory, Elliptic Curves

  Firewall, VPN,…

different from general systems

- Argument to single out information-security from other research subjects: we concentrate on “the hard part” of a problem.
- Different object:
  - Security studies how to make adversary hard to break;
  - Others study how to make a system easy to use efficiently
- Different tools:
  - One-way functions
  - Difficulty and complexity

6. Independence as a discipline

- **Definition：** *Information security is the science of information system at the presents of adversary.*
- **Information security can be an Independent research subject because：**
  - **Research object：** *information system with the presents of adversary*
  - **Special : one-wayness**
- **Relationship with other research subjects：**
  - *information system with the presents of adversary*
  - **NOT "do everything, but nothing better"**

7. Sub-disciplines

Information security

information system with the presents of adversary

one-wayness

crypto	network	computer	warfare

Typical information system

Empathy?

One-way function

Crypto = one way function

- Oneway function f: X ->Y, given x, easy to compute f(x); but for given y in f(X), it is hard to find x, s.t., f(x)=y.
  - Prob[f(A(f(x))=f(x))] < 1/p(n)   (TM definition, existence unknown)
  - Example: hash function, discrete logarithm;
- Keyed function f(X,Z)=Y, for known key z, it is easy to compute f(.,z)
  - Block cipher
- Keyed oneway function: f(X,Z)=Y, for known key z, it is easy to compute f(.,z) but for given y, it is hard to x,z, s.t., f(x,z)=y.
  - MAC function: keyed hash h(z,X), block cipher CBC
- Trapdoor oneway function $f_T(x)$: easy to compute and hard to invert, but with additional knowledge T, it is easy to invert.
  - Public-key cipher; RSA: $y=x^e$ mod N, T: N=p*q

8. Related phenomenon

- Well accepted
  - Quantum computing/ cryptography – can be used to solve / establish hard problems
  - DNA: similar – DNA cipher uses new hard problem, DNA computing can solve hard problem
- Not well established yet
  - Chaos theory: what is the difficulty and one-way?
  - Fuzzy computing: similar, things we don't understand are not necessarily difficult.
  - (although both may be used in random number generation)

IT-security

- **Information security is the science of information processing in the presents of adversary.**
  - **Our subject is still information processing, so we are dealing with communication, storage, computer system.**
  - **Security alone is not really needed.**
  - **Security is necessary because of the presents of adversary, i.e., if there exist threats to system.**
  - **Foundation – one way function – easy to use and hard to break.**
  - **Differ from other study topics: 1-way, difficulty of attack, …**

IT-security and Cryptography

- **Issues in Information security**
  - **Scientific like**
    - **Confidentiality**
    - **Authentication**
    - **Access control**
  - **More engineering**
    - **Virus protection**
    - **Intrusion prevention**
    - **Copyright protection**
    - **Content filtering**

Cryptography

Cryptology
(from the Greek for 'hidden word')

Cryptography –密码编码学
Code making

Cryptanalysis-密码分析
Code breaking 破译

Confidentiality
Secrecy, privacy

Authenticity
Data
entity

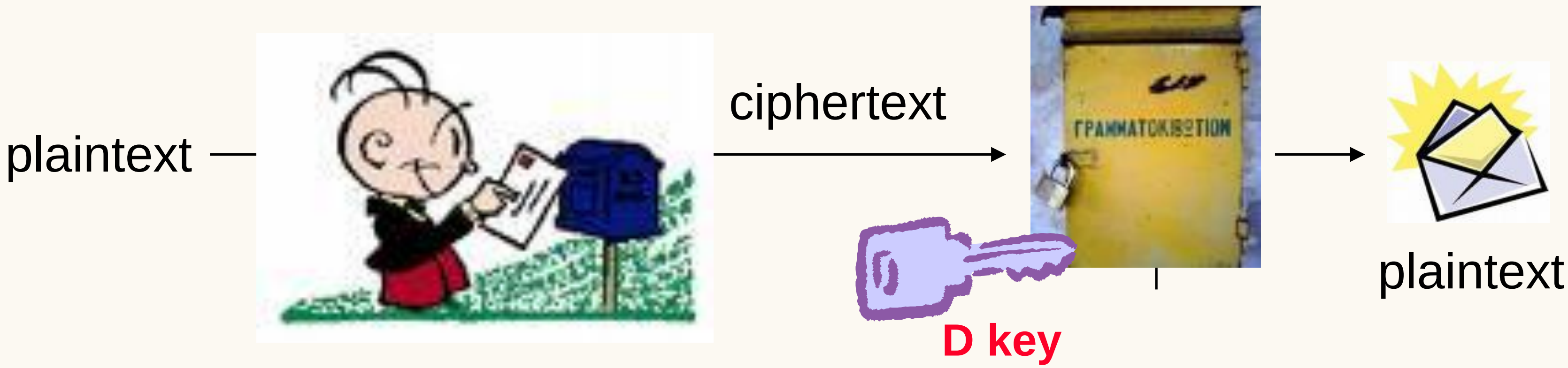
Integrity
Random number

Confidentiality and authenticity are independent attributes of a cryptosystem

Confidentiality

– Confidentiality : information is not disclosed to unauthorized individuals, entities, or processes. [ISO]

– Mechanism to achieve confidentiality--Encryption:



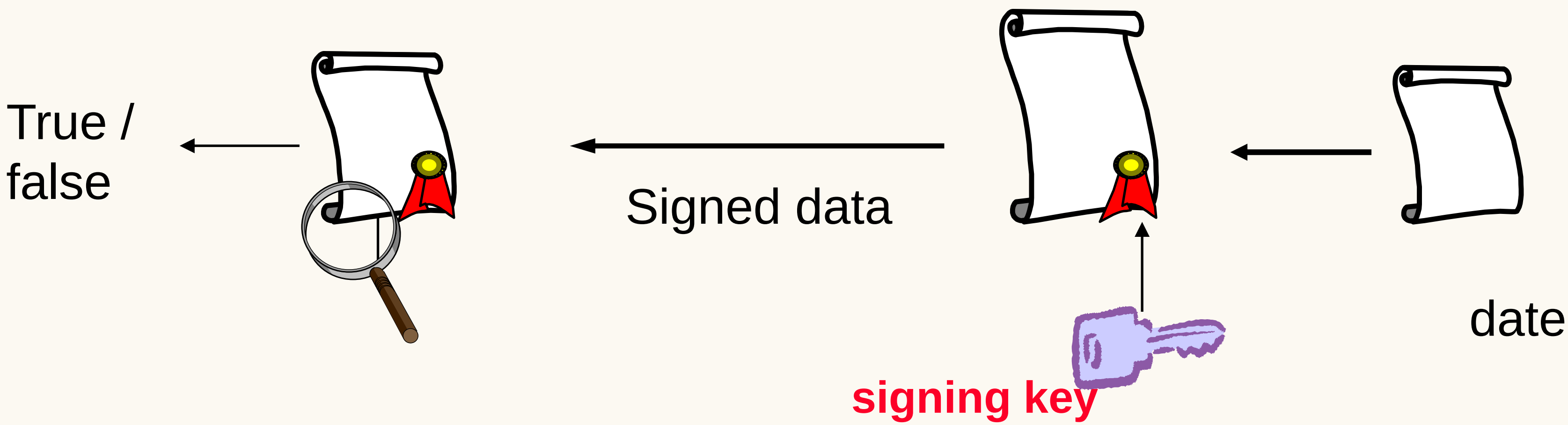
Only the user knowing the decryption key can recover plaintext

–"who can *read* the data"

Authenticity

– Authenticity: assurance of the claimed identity of an entity. [ISO]

– Example: ID-card, password, digital signature



Only the user knowing the secret-key can generate valid signature

"who *wrote* the data"

Extended Cryptography

- who can read the data in the future
  - Confidentiality
- who wrote the data in the past
  - Authenticity
- who has read the data in the past
  - Content protection, …?
- who can write the data in the future
  - Virus, DoS, Spam, …?

We may need tools beyond math and computer
--quantum money, biologic computing

Privacy

- How to define privacy?
  - K-anonymity
  - Differential privacy

- Privacy $\neq$ confidentiality
- Is there some adversary?
- Do we need one-wayness?

Public Standard vs. secret system

2 sides of a sword:

Public standard

- compatible with other entities, Independent of providers
- confidence and trust in systems
- Up to date techniques / fast reaction to incidents
- Security should not depend on the secrecy of the system

Secret System

- it could be more difficult to break the system, because adversary has less knowledge of the system in use
- Support from the provider, Insurance by the authority

Develop system : assume enemy knows everything except the key.

Use of system: hide as much as possible

☆Define difficulty: Turing-Machine complexity

Turing-Machine complexity is

– uniform (one algorithm for every input length) and
– Asymptotic (complexity is about f(n) when n $\to\infty$)

- If P = NP, then we can solve many problem in polynomial time; does this means we cannot have provably secure system?
  - Answer: no
  - If we a cipher that encryption complexity is n, but attack needs at least n^3 , then this would be enough for many practices
- If P ≠ NP, do we have provably secure system?
  - Answer: no.

∵ attacker works only on one fixed-size problem

E.g. even if TM-complexity of factoring is exponential, to factor a specific integer can still be easy. To break a given RSA, you need only to factor one integer, not every integer.

∵ Example: there exist problem, for which the uniform complexity is super exponential, but the fixed length complexity is linear [Cohen}.

Difficulty and complexity

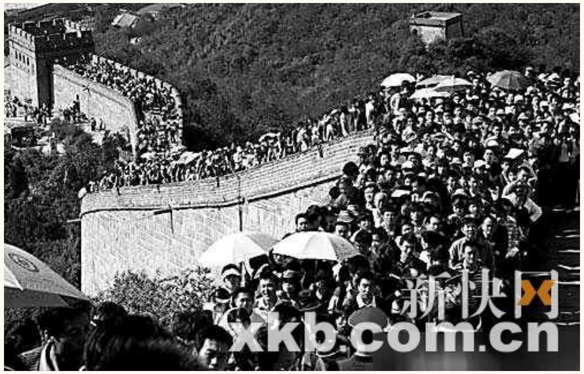
- ‘the problem of cipher design is essentially one of finding difficult problems’ [Shannon 49]
- Our goal: proving that “to break the system needs at least this much work“
- “finding difficult problems” requires to define difficulty – complexity.
- Turing machine complexity does not meet our requirement (but still useful)
- Gate-complexity – right definition but current results are not useful.
- Lots of researches and results but far from our goal.

Computation power

- Heisenberg uncertainty relation
  - the number of elementary logical operations per second that can be performed by that amount of energy, E,

$$2E/(\pi*\underline{h}) , \underline{h} = 10^{-34}$$

- Using total energy in the whole universe
  - Max. number of operations: $10^{120} \approx 2^{400}$.
  - Max number of bits storage: $10^{90} \approx 2^{300}$



- Today's world computation power $<2^{120}$
  - #operations/second $< 2^{40}$
  - #computers < 7,040,045,902 *100 $< 2^{40}$ (2012-09-18)
  - #seconds in 30,000 years $<2^{40}$