Cryptography
6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

First term 2020/21

Lecture 1.2: What is information security?

Information Security

Computer security deals with the prevention and detection of unauthorized actions by users of a computer system.

- Authorization is central to definition.
- Sensible only relative to a security policy, stating who (or what) may perform which actions.

Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined together.

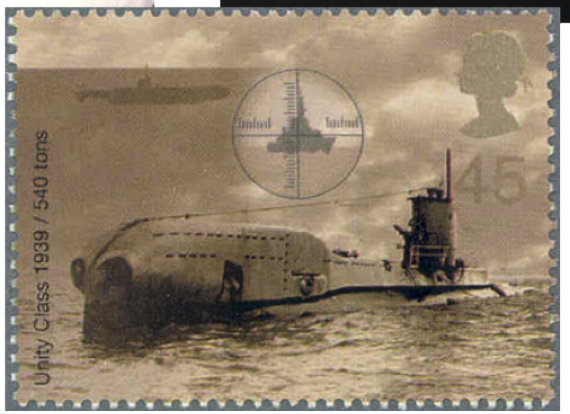
Information security is (perhaps) even more general: it deals with information independent of computer systems.

- Note that information is more general than data. Data conveys information. But information may also be revealed, without revealing data, e.g., by statistical summaries.
- Constitutes a basic right: protection of self (possessions, ...).

Information Security: a definition

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information Security — Past



Security primarily a military concern.

Information Security — Present: Everyone's concern!

Our basic infrastructures are increasingly based on networked information systems:

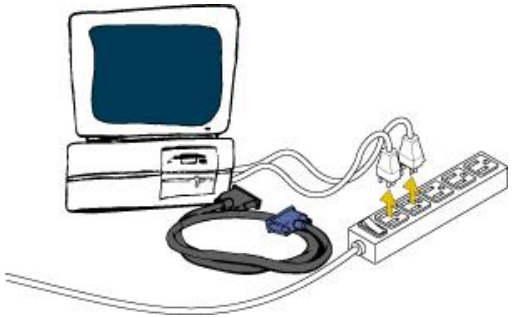
- administration
- business
- communication
- distribution
- education
- energy
- entertainment
- finance
- health
- news
- transportation
- …

Security not just a concern, but an **enabling/disabling factor!**

e-Hermitism vs. e-Society

- The only secure computer is isolated and turned off!
  (*You have no privacy — get over it.*)





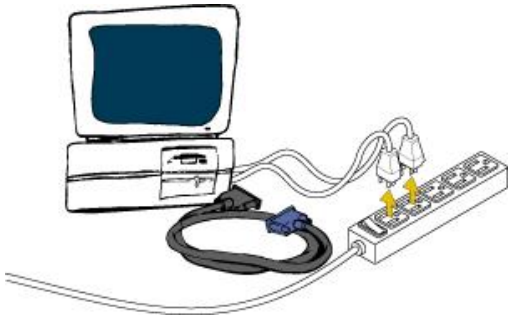
The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards — and even then I have my doubts.

Eugene H. Spafford, Purdue University, often misquoted as

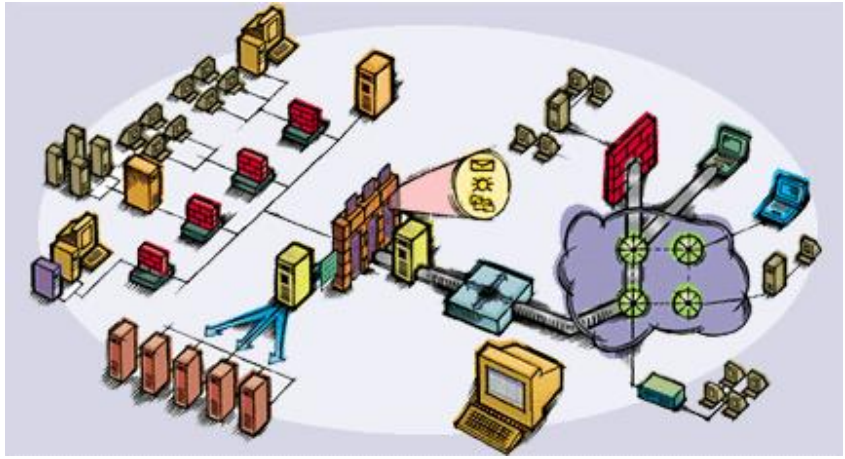
The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it.

e-Hermitism vs. e-Society

- The only secure computer is isolated and turned off!
  (*You have no privacy — get over it.*)



- But we want, and have, an e-society:



Information Security — Who needs it?

- Every one working with “computers”!
- Central to software engineers and system administrators
  - and even executives and politicians
  - as well as hackers, terrorists, and other bad guys.

This year’s trial of the embassy bombings revealed that Bin Laden associates began to use encryption before 1998. Sometimes members of the Al-Qaida confederation have alternatively resorted to simple code words. For instance, “working” is said to mean Jihad, “tools” meant weapons, “potatoes” meant grenades and “the director” was an alias for Bin Laden. Steganographic approaches were also used to communicate in at least three terrorist acts, including the 1998 embassy bombings in Kenya and Tanzania.

Lisa Krieger, Mercury News, Oct 1. 2001

Isis have been using end-to-end encryption and device encryption.

- but fundamental also for laypersons and “normal” citizens.

Is your data worth protecting?

- **Your personal data is interesting**.
  Shopping habits, family status, religion, political party, criminal record, vita/career, health, finances, sports/hobbies, ...

- **Your data is everywhere and computers are good at collecting and using it**.
  - Bank: transfers, investments, credit card purchases, taxes.
  - Telephone: source, time, location.
  - Shopping/travel: from (online) shops, loyalty programs.
  - Entertainment: movies watched in hotels (also $<$ 2 minutes).
- Valuable for sales departments, (future) employers, agencies, etc.
  Valuable for you?

Where? Everywhere!

Computing: The net is the computer!

Must assure selective access to machines, programs, data, computational resources, etc.
Privacy of data, activities, ...

"You're insecure because your data is unsecured."

Where? Everywhere!

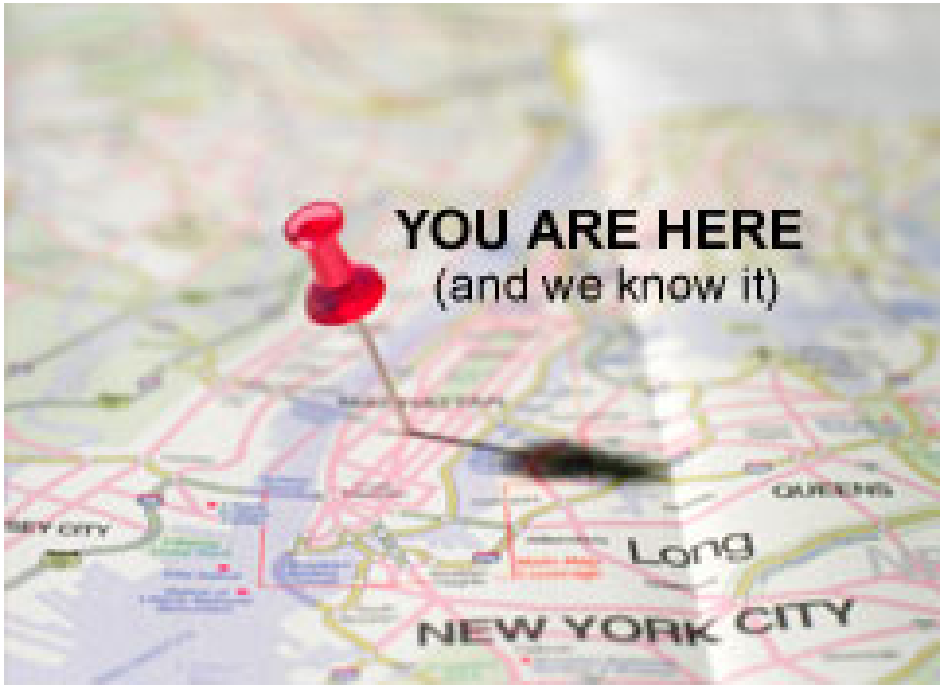
Banking: ATMs, home banking, etc.

Access to accounts, integrity of data, nonrepudiation of transactions, . . .

Where? Everywhere!

Telecommunications: e.g., mobile (GSM) networks

Confidentiality/privacy of communication, location information, . . .

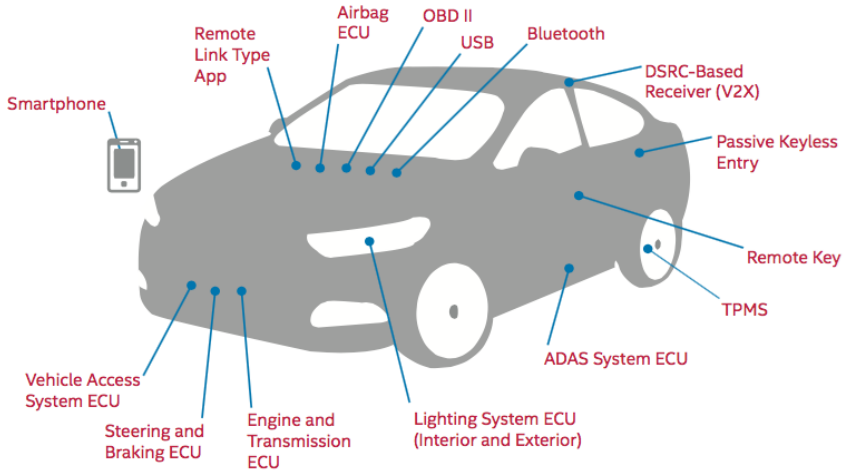


Where? Everywhere!

Critical infrastructures: energy, water, finance, industry, ...

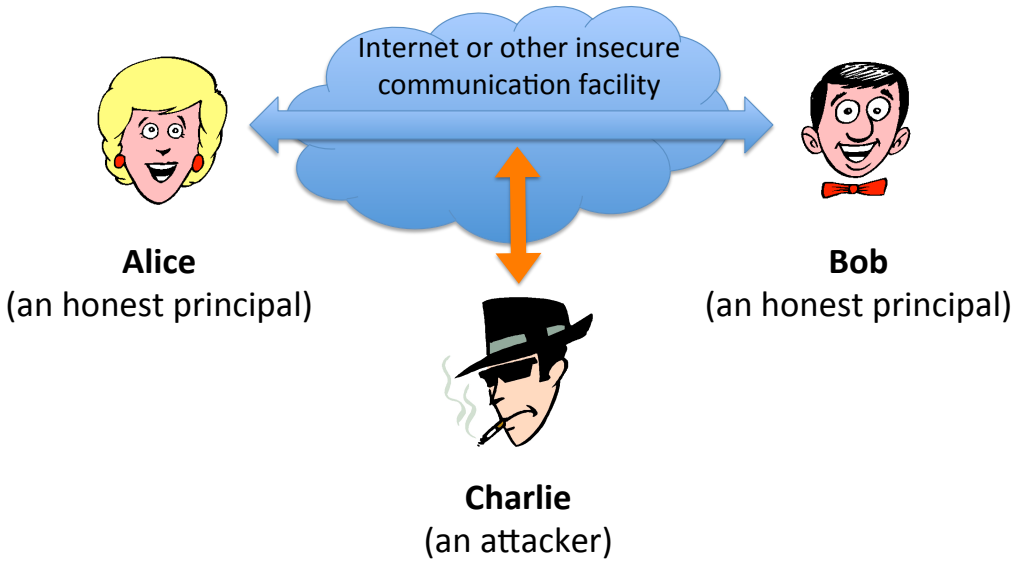
Transport: cars, trains, planes, ...

See, e.g., INTEL's Best Practices white paper on "Automotive Security"; cf. also "How automakers can beef up cybersecurity in the era of the Internet-connected car", TIME magazine, 09/2015.



Cars can be hacked!

What's it all about?

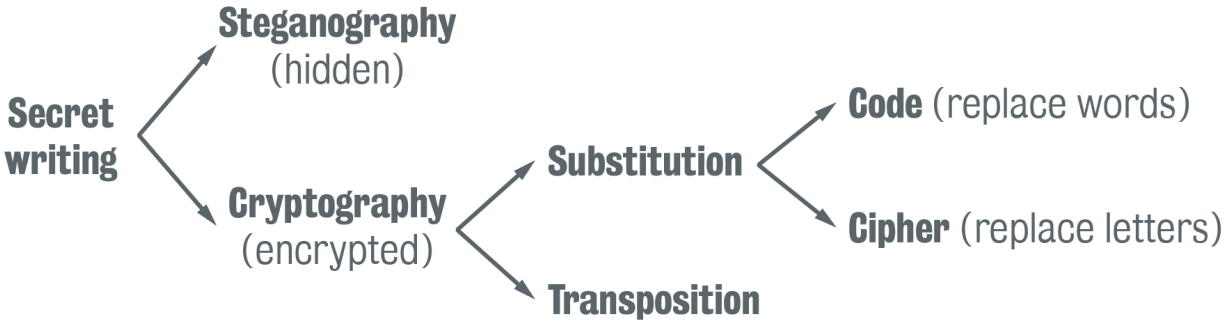


How do we turn an insecure communication facility (like the Internet) into a secure one?

Where (information) security means that one or more security properties (e.g., confidentiality, integrity, authentication, anonymity, unobservability, non-repudiation, availability, etc.) are guaranteed.

Cryptography is an enabling technology.

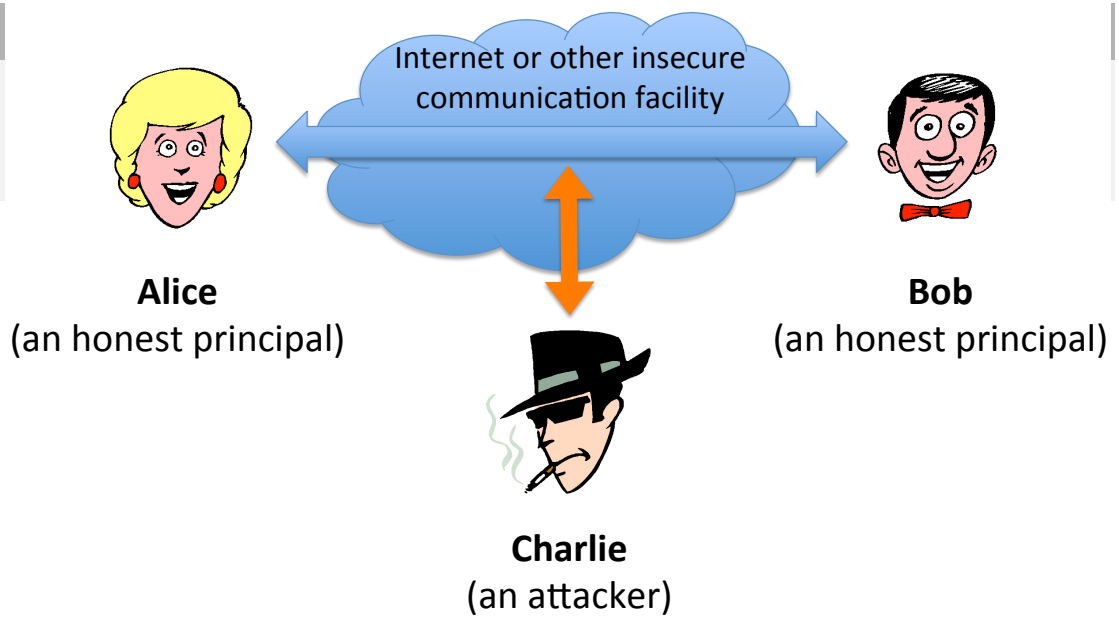
What is cryptography?



- Cryptology: the study of secret writing.
- Steganography: the science of hiding messages in other messages.
- Cryptography: the science of secret writing.
  Note: terms like encrypt, encode, and encipher are often (loosely and wrongly) used interchangeably.
- Cryptanalysis: science of recovering the plaintext from ciphertext without the key.

We will discuss each of these (in some detail).

Agents (principals)



Following a long-standing tradition in (security) protocols, throughout the course we'll consider the following **agents** (a.k.a. **principals**):

- **Honest agents**:
  - **Alice**, **Bob**, **Carol**, ... agents communicating with each other (e.g. client and bank, bank and bank, client and online shop, ...)
- **Dishonest agents (a.k.a. attackers, intruders, ...)**:
  - **Eve**: an eavesdropper (i.e., a passive attacker who only listens)
  - **Charlie**, **Mallory** and **Zoe**: malicious, active attackers
- **Trusted and/or neutral**:
  - **Simon** and **Trent**: (trusted) servers
  - **Peggy** and **Victor**: prover and verifier (zero-knowledge protocols)

Task

- Reflect on how Alice and Bob can actually exchange information "securely" over an insecure medium which is, possibly, under the control of Charlie, an attacker.
  What does it mean for a communication to be "secure"?
  You are allowed to ask a trusted third party for help or use external resources.
- Here, "secure" means that one or more security properties (e.g., confidentiality, integrity, authentication, anonymity, unobservability, non-repudiation, availability, etc.) are guaranteed.
- Think about how you would make communication between Alice and Bob secure.