Cryptography
6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

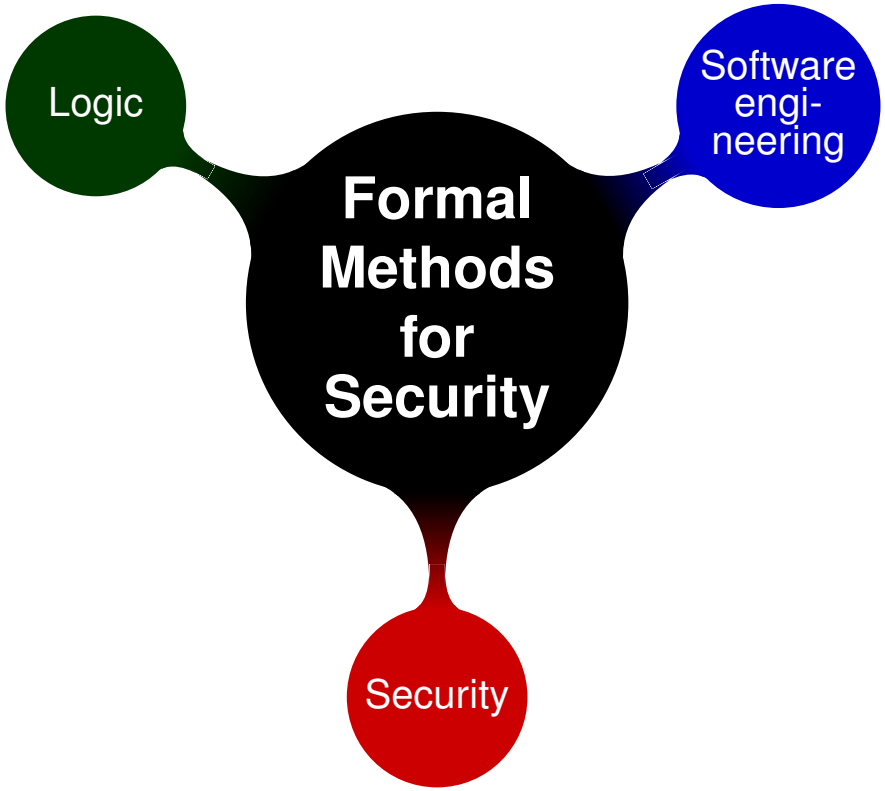
First term 2019/20

Lecture 1

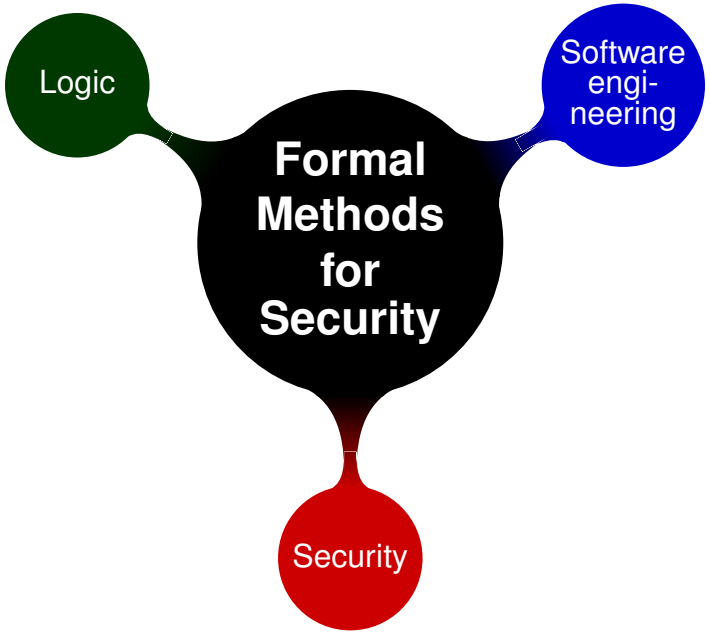
Pleased to meet you

About myself

About myself: Research (and teaching)



About myself: Research (and teaching)



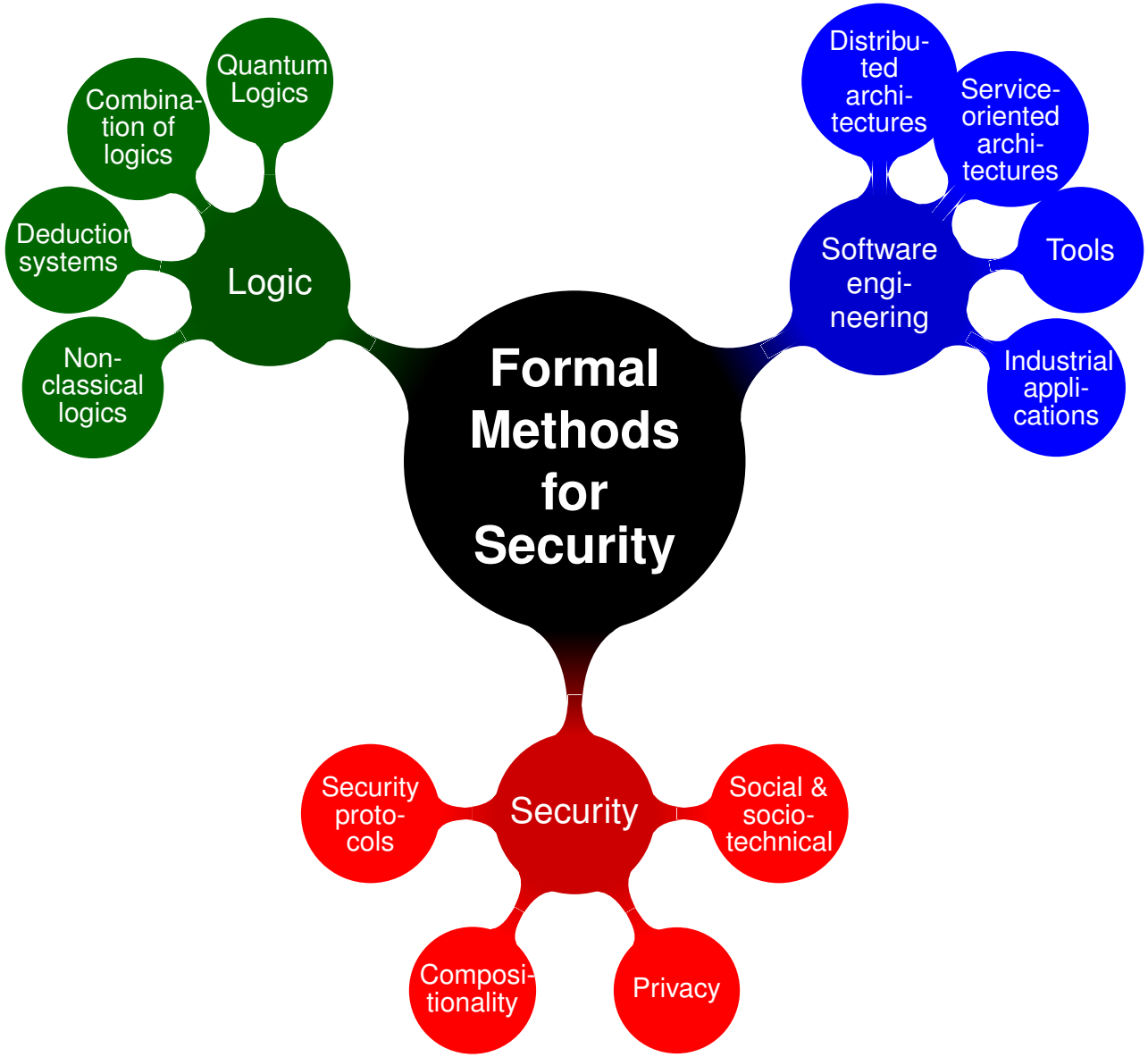
Theoretical research

Formal Methods: Techniques and tools based on mathematics and logic that support the specification, construction, analysis and testing of hardware and software systems.

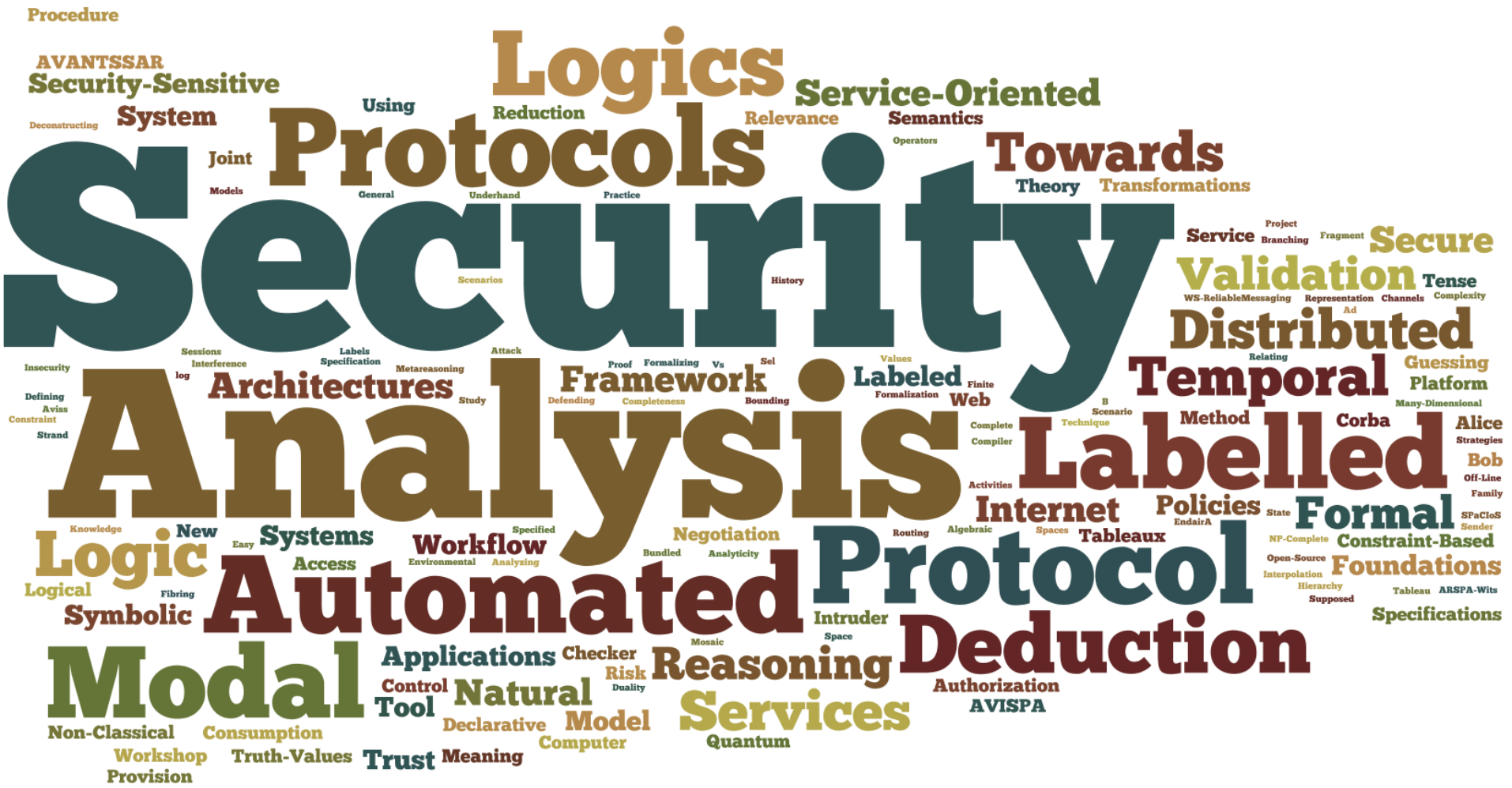
and its application to practical problems

in the small, e.g. security protocols and web applications, privacy, attribution
in the large, e.g. distributed security architectures, cyber-physical systems.

About myself: Research (and teaching)



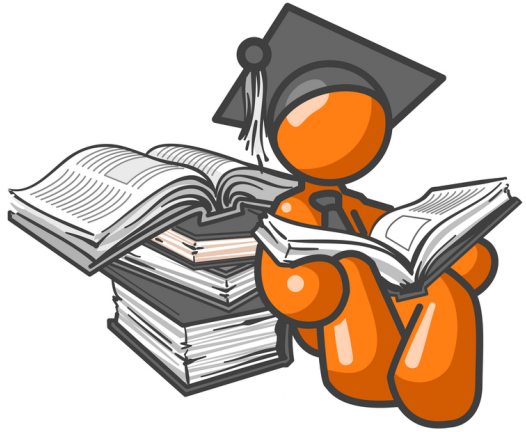
About myself: wordle of my research papers



And you are?

Programmes: BSc, MSci, MSc

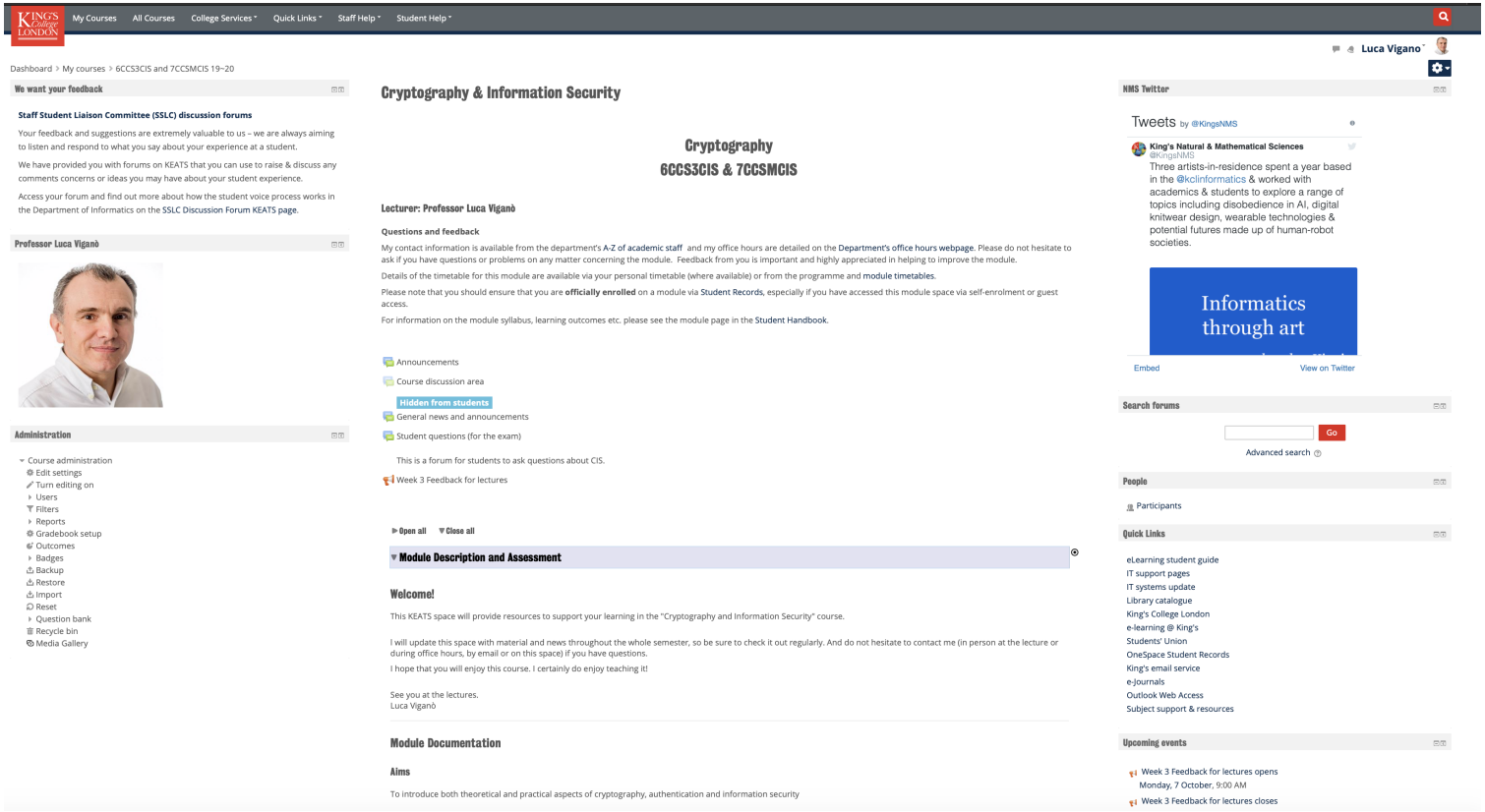
- BSc Computer Science, Year 3
- BSc Computer Science with Management, Year 3
- BSc Computer Science with Management and a Year Abroad, Year 4
- BSc Computer Science with Management and a Year in Industry, Year 4
- BSc Computer Science with a Year Abroad, Year 4
- MSci in Computer Science, Year 3
- BSc Computer Science with a Year in Industry, Year 4
- Mathematics and Computer Science, Year 3
- MSc in Advanced Computing
- MSc in Computing & Internet Systems
- MSc in Computing & Security
- MSc in Computing, IT Law & Management
- MSc in Data Science
- MSc in Web Intelligence
- MSci Computer Science
- ...



Coordinates

Credit level: 6 / 7 **Credit value:** 15 **Exam:** Written examination (2 hours)
KEATS: slides, exercises and general material, news and discussion forum

- Slides available before lectures
- Watch for corrections (new versions with errata lists)
- Student questions and discussion forum



Office: BH(N)7.18 **Office hours:** Thursday 14-16 (or email) **Email:** luca.vigano@kcl.ac.uk

Lecture capture

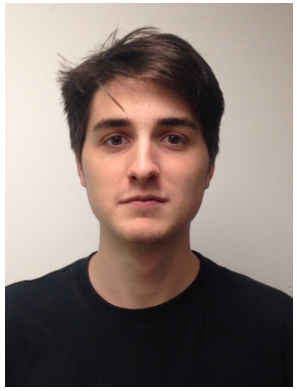
- We provide lecture capture for most modules.
- It is important to use lecture capture wisely:
  - Lecture recordings are a study and revision aid.
  - Watching lectures online is NOT a replacement for attending lectures.
  - Statistically, there is a clear and direct link between attendance and attainment: Students who do not attend lectures do less well in exams.
- Attending a lecture is more than watching it online — if you do not attend, you miss out. You really miss out!

Objectives: for you

Objectives: for me

Format

- Mainly frontal lectures, but tutorials every other week.
- Each of you has been assigned to a weekly slot for the tutorials.
- Meet the team:
  - Professor Luca Viganò
  - Teaching Assistants:



Andrew Cook

Francesca Mosca

Diego Sempreboni

Learning aims & outcomes

- To introduce both **theoretical** and **practical** (and **technological**) aspects of cryptography and information security.
- On successful completion of this module, students should be able to
  - understand the relevant mathematical techniques associated with cryptography;
  - understand the principles of cryptographic techniques and perform implementations of selected algorithms in this area; and
  - appreciate the application of security techniques in solving real-life security problems in practical systems.

Please note that this module contains several advanced mathematical techniques. This should not be a problem for students with a reasonable mathematical background. Explanations are given during the lectures/tutorials and examples are studied in detail.
Nevertheless, an in-depth understanding of these techniques is required for the examination and personal work should be anticipated.

Complementary (and introductory) to other modules in security.

Syllabus and general information

- Basic terminology and concepts:
  - Goals of cryptography, terminology and notation, players
  - Basic cryptographic functions
- Number theory:
  - Congruent modulo n, equivalent class modulo n
  - Integer modulo n (Zn)
  - Multiplicative inverse
  - Relatively prime
  - Euler's theorem
  - Fermat's little theorem
  - EEA (Extended Euclidean Algorithm)
  - CRT (Chinese Remainder Theorem)
- Ciphers:
  - Block ciphers (substitution, transposition, product)
  - Stream ciphers
  - Modes of operation (ECB, CBC, CFB, OFB)
- Cryptosystems:
  - Block cipher: DES (Data Encryption Standard), AES (Advanced Encryption Standard)
  - Public-key: RSA (Rivest-Shamir-Adleman), El Gamal
  - One-way hash function: SHA and MD5 (Message Digest 5)
  - Password hashing and salting

Syllabus and general information

- Key-establishment protocols:
  - Symmetric and asymmetric techniques (Diffie-Hellman, Needham-Schroeder, Otway-Rees)
  - Public-key encryption
  - Basic and advanced Kerberos protocols
- Authentication and identification:
  - Concepts
  - Fiat-Shamir and Feige-Fiat-Shamir protocols
  - Zero-knowledge identification protocol
- Digital signatures:
  - Classification
  - Digital signature schemes: RSA; EI-Gamal; DSA (Digital Signature Algorithm) and DSS (Digital Signature Standard)
- Information Security:
  - Password systems: number of acceptable passwords for a given password policy, exhaustive search password ageing
  - Introduction to viruses, secure communication, social engineering (phishing), firewall, buffer overflow, denial of services

Recommended reading

- Slides will cover all the topics.
- Recommended bibliography (alphabetical order):
  - Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. *Cryptography Engineering*, John Wiley & Sons, 2010.
  - Wenbo Mao. *Modern Cryptography: Theory & Practice*, Prentice Hall, 2003.
  - Alfred Menezes, Paul van Oorschot, Scott Vanstone, A.J. Menezes. *Handbook of Applied Cryptography*, CRC Press, 1996 and 2018). Available online: http://cacr.uwaterloo.ca/hac/.
  - Christof Paar and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010.
  - Bruce Schneier. *Applied Cryptography*, John Wiley & Sons, 1996 (and 20th anniversary edition in 2016).
  - William Stallings. *Cryptography and Network Security. Principles and Practice*, 7th ed., Prentice Hall, 2016.

  These books are recommended only, there's no requirement to buy them.

Calendar

- To be revised as the weeks go by:

Month	Day	Content of Lecture	Tutorial
September	26	Introduction	
October	3	Lecture	Week 6
	10	Lecture	
	17	Lecture	Week 8
	24	Lecture	
	31	~~*Reading week*~~	
November	7	Lecture	Week 11
	14	Lecture	
	21	Lecture	Week 13
	28	Lecture	
December	5	Lecture	Week 15
	12	Revision lecture	

- 5 slide decks (“Lecture 1”, ..., “Lecture 5”), organized thematically.

Outline

1. Motivation
   - What is Information Security?
   - E-Government as an example
2. Dramatis personae of cryptography and information security
3. Two common views of Information Security (and properties/goals)
   - Security as policy compliance
   - Traditional security properties/goals
   - Security as risk minimization
4. Conclusions

Table of contents I

Table of contents I

Information Security

Go to `https://www.polleverywhere.com/lucavigano`

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, ...).

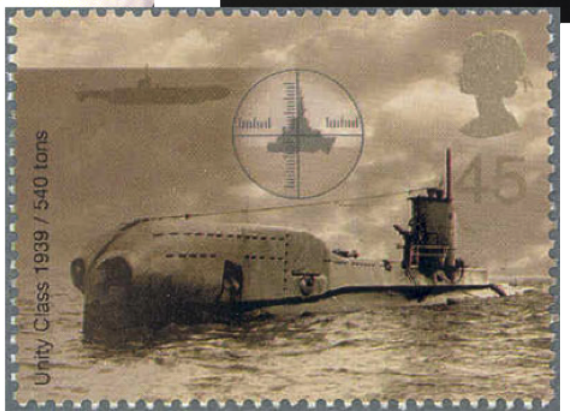
Information Security: a definition

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

Information Security — Past

Go to `https://www.polleverywhere.com/lucavigano`

Information Security — Past



Security primarily a military concern.

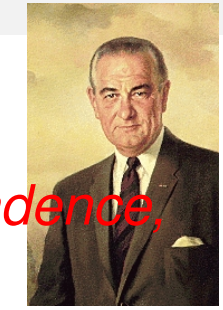
Information Security — Present: Everyone's concern!

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!**

An example: privacy, a fundamental good?



- Lyndon B. Johnson, President of the USA 1963-1969:

  Every man should know that his conversations, his correspondence, and his personal life are private.

- Directive 95/46/EC of the European Parliament:

  Whereas data-processing systems are designed to serve man; whereas they must respect their fundamental rights and freedoms, notably the right to privacy ... In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

  (25.05.2018): **EU General Data Protection Regulation (GDPR)**.

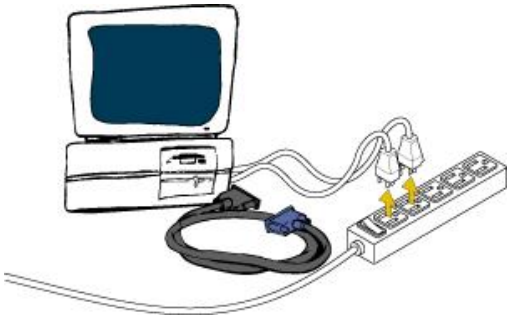
- Scott McNealy, CEO Sun Microsystems, 1999:

  You have no privacy — get over it!

e-Hermitism vs. e-Society

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





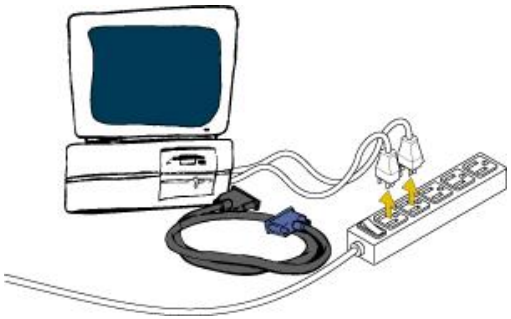
The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards — and even then I have my doubts.

Eugene H. Spafford, Purdue University, often misquoted as

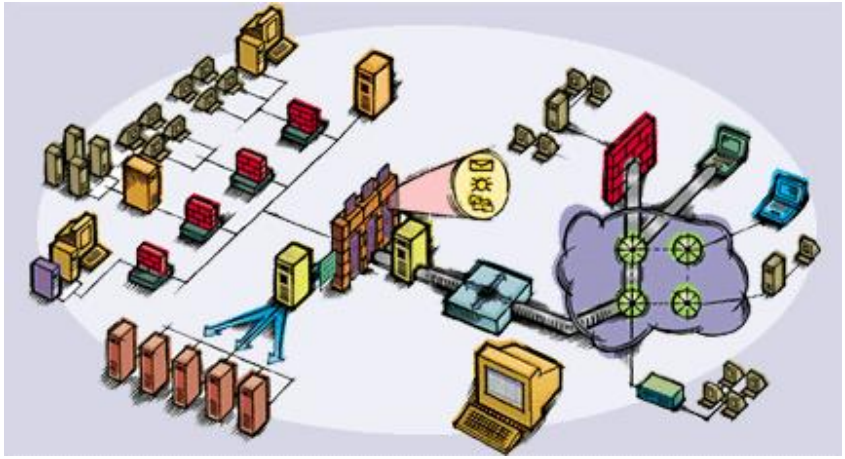
The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it.

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 laypersons and “normal” citizens.

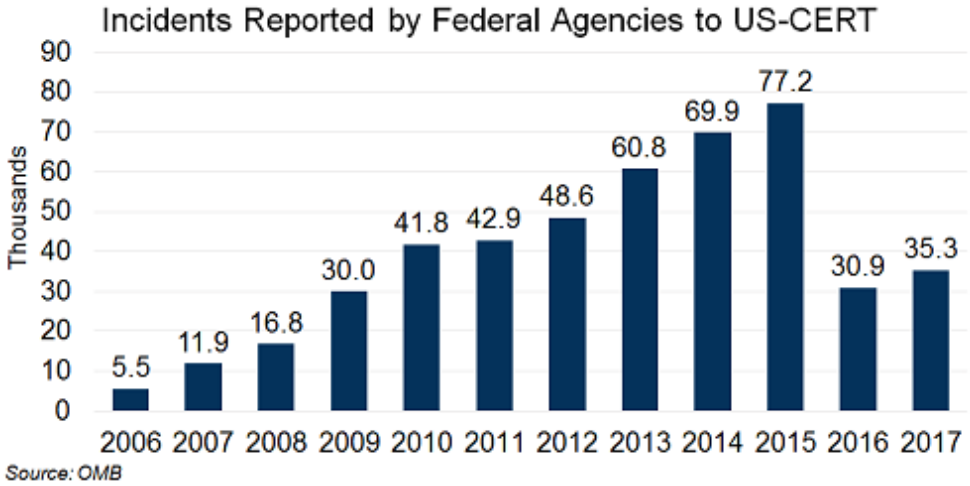
Is your data worth protecting?

- **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?

Security Trends

- *Internet-related vulnerabilities*
  - in the operating systems
  - in routers and other network devices
- *Security incidents*
  - Denial of Service attacks
  - IP spoofing
  - packet sniffing, . . .



Source: Computer Emergency Response Team (CERT)

`www.cert.org`

Where? Everywhere!

Computing: The net is the computer!

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

Where? Everywhere!

Where? Everywhere!

Where? Everywhere!

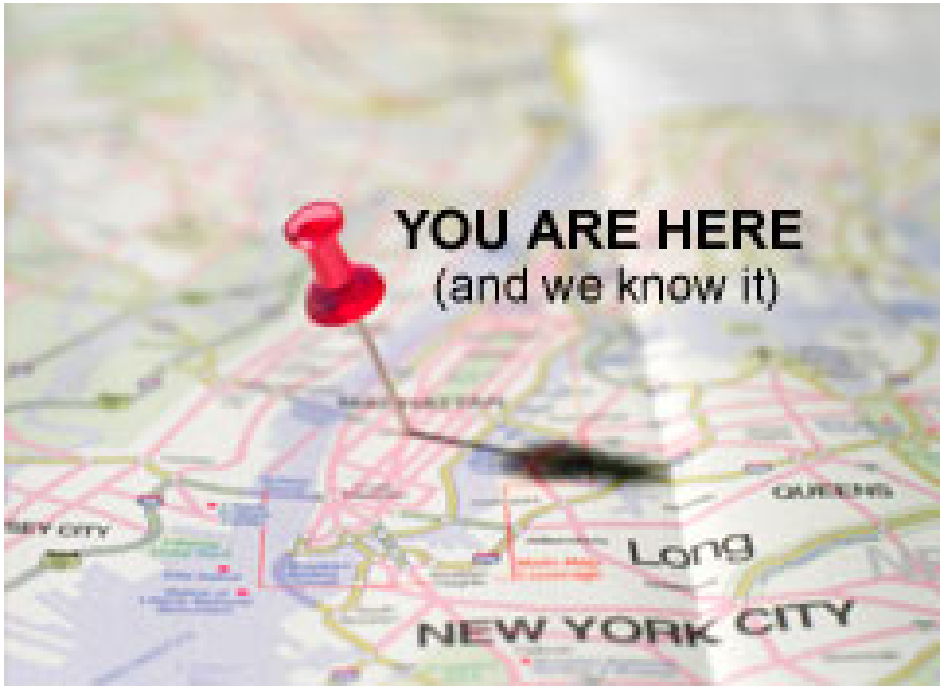
Banking: ATMs, home banking, etc.

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

Where? Everywhere!

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

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

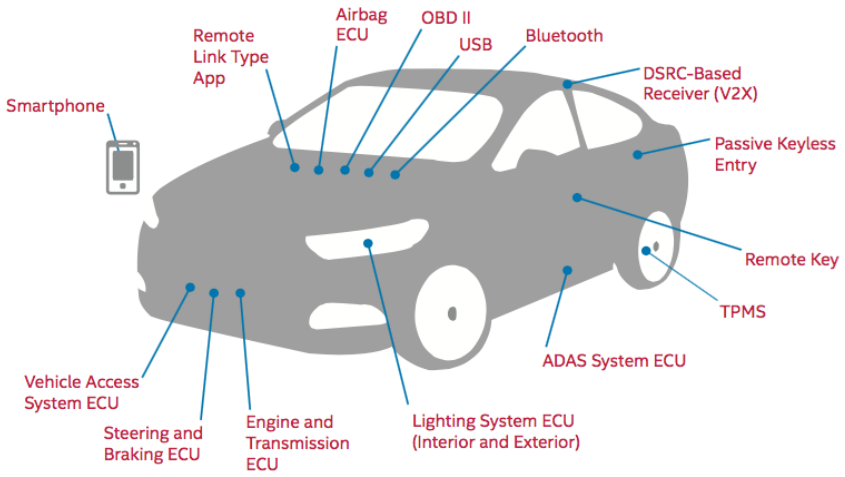


Where? Everywhere!

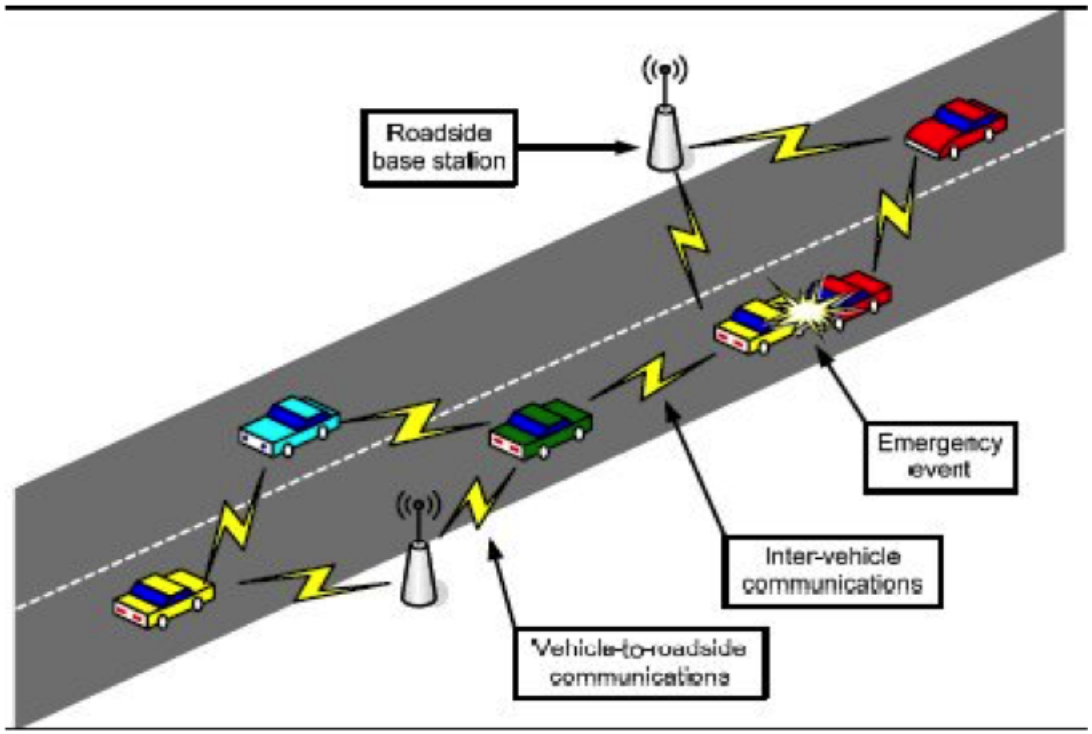
Critical infrastructures: energy, water, finance, industry, ...

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!


Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

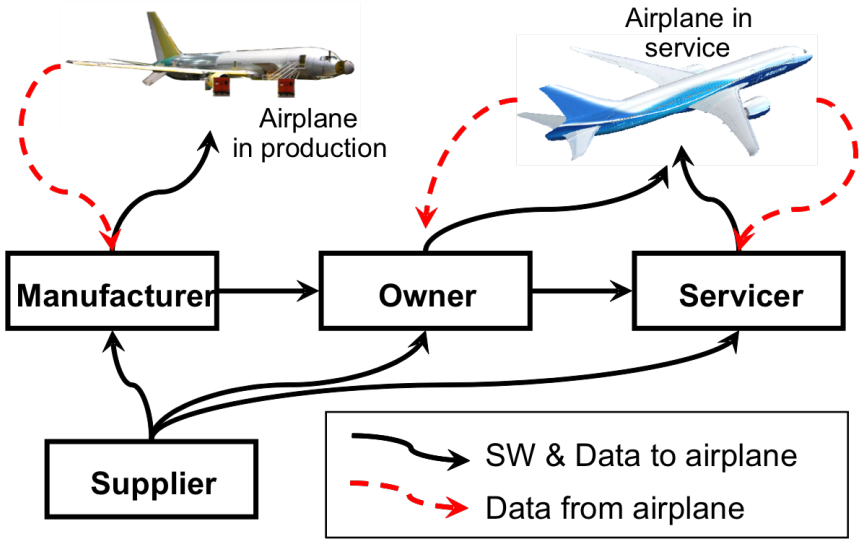
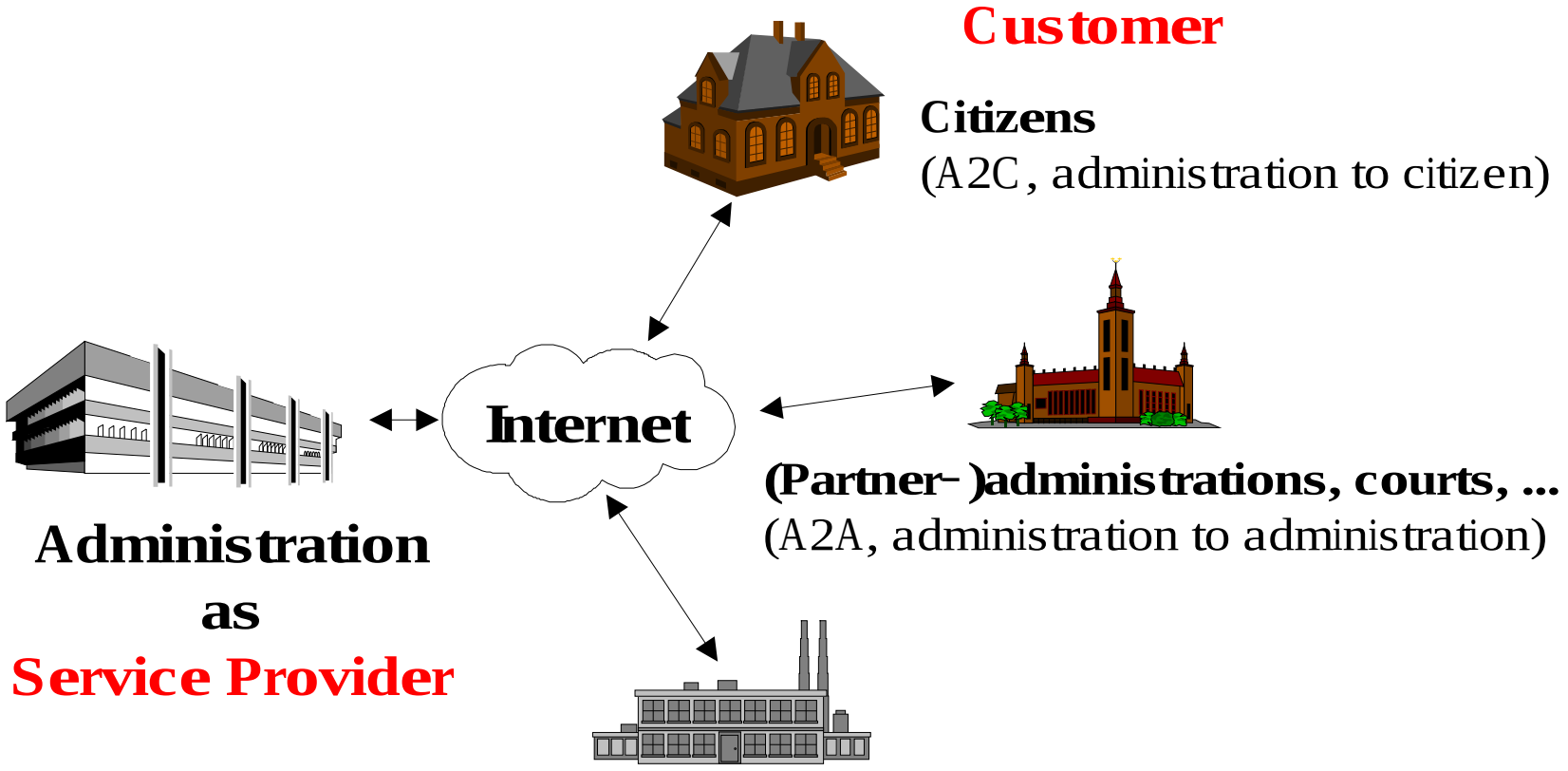

Airplane in service
Airplane in production
Manufacturer
Owner
Servicer
Supplier
SW & Data to airplane
Data from airplane

Table of contents I

What is e-government?

E-government is the use of information technology (in particular the Internet) to create or improve services between customers and governments.

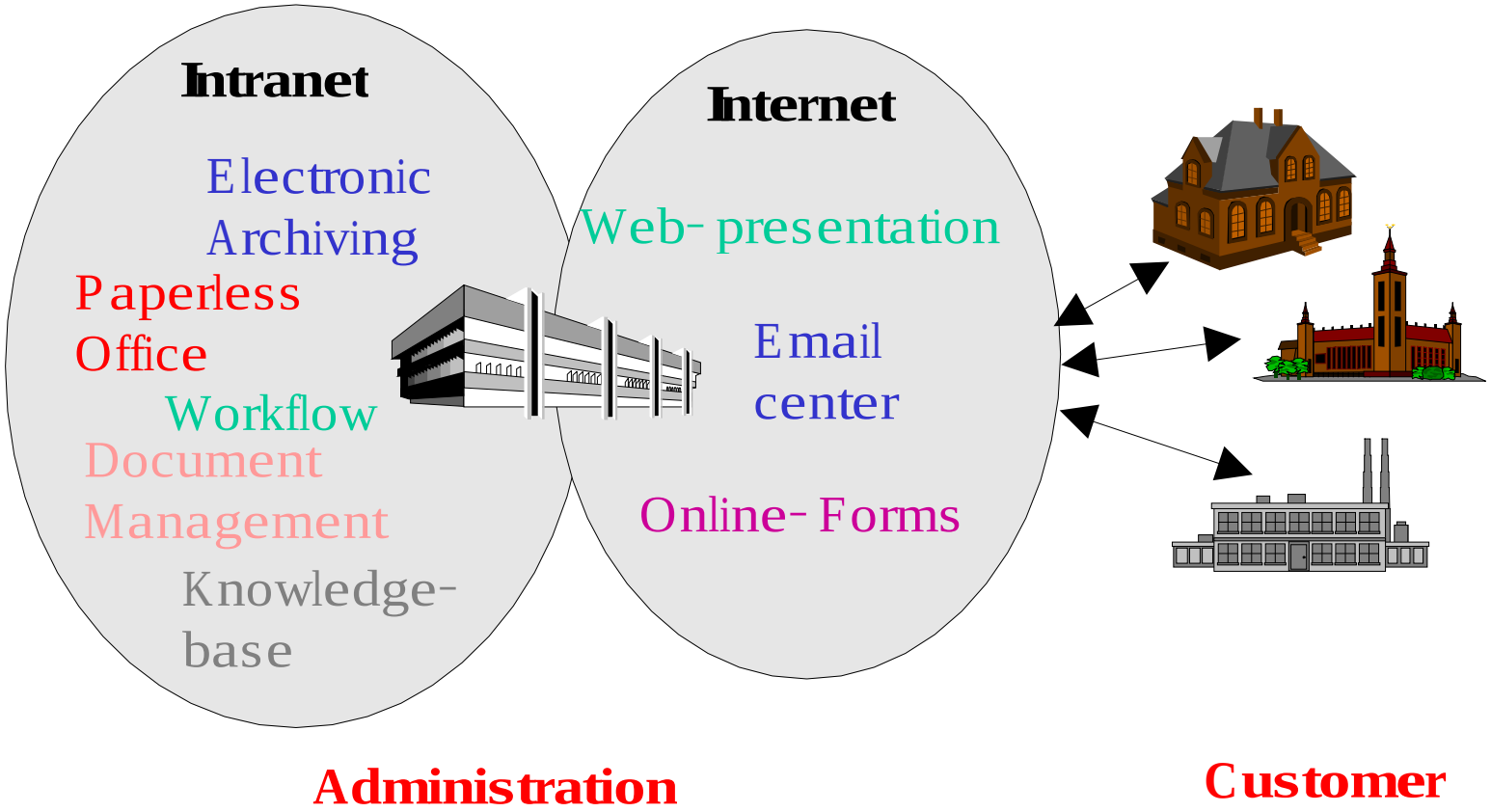


Examples of e-government

- Email correspondence, both informal and official
- Online consultation and virtual information centers
- Electronic applications, taxes, administrative procedures
- Online voting
- . . . and many others!

Similarities to e-business, but with new challenges
(wide-scale coverage, reflection of legal landscape, voting, ...).

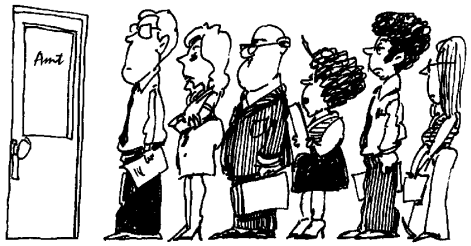
The inner-view of e-government

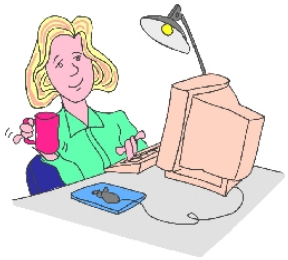


Administration is now open (via web, mail, and application servers) and manages confidential data.

Potentially a win-win situation

- For the citizen





- and for the government

Potential for a tremendous efficiency gain, cost reduction, and service improvement.

But useless without security and trust!

Continent	Only XSS	Only SQL	XSS and SQL	XSS or SQL	None
Africa (61)	14.75 (9)	0.00 (0)	34.43 (21)	49.18 (30)	50.82 (31)
Asia (55)	9.09 (5)	0.00 (0)	76.36 (42)	85.45 (47)	14.55 (8)
Europe (53)	7.55 (4)	0.00 (0)	83.02 (44)	90.57 (48)	9.43 (5)
North America (34)	20.59 (7)	2.94 (1)	52.94 (18)	76.47 (26)	23.53 (8)
Oceania (25)	24.00 (6)	0.00 (0)	28.00 (7)	52.00 (13)	48.00 (12)
South America (17)	17.65 (3)	0.00 (0)	52.94 (9)	70.59 (12)	29.41 (5)

Table 1: Percentages of vulnerabilities in E-Governments for each continent. Number of countries enclosed in parenthesis. Note that some countries are counted for more than one continent, e.g. Russia belongs to both Europe and Asia.

Country category	Only XSS	Only SQL	XSS and SQL	XSS or SQL	None
1st World (32)	6.25 (2)	0.00 (0)	90.63 (29)	96.88 (31)	3.12 (1)
2nd World (31)	9.68 (3)	0.00 (0)	80.64 (25)	90.32 (28)	9.68 (3)
3rd World (50)	18.00 (9)	0.00 (0)	32.00 (16)	50.00 (25)	50.00 (25)
G8 (8)	0.00 (0)	0.00 (0)	100.00 (8)	100.00 (8)	0.00 (0)

Table 2: Percentages of vulnerabilities in E-Governments for different country categories. Number of countries enclosed in parenthesis. Note that not all of the 244 countries are included in the statistic for 1st, 2nd, and 3rd World, we used the countries listed on (nationsonline.org, 2005).

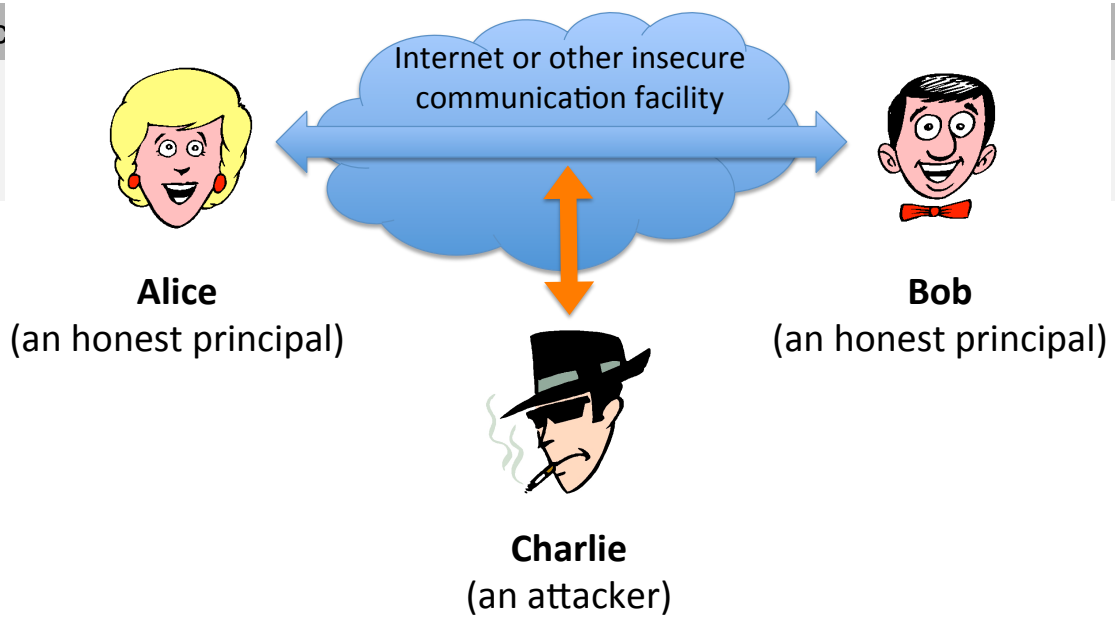
Vulnerabilities in e-governments, V. Moen et al., University of Bergen, 2006.

Table of contents I

Information Security: a definition

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

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)

Table of contents I

Let's consider two common views of Information Security

1. Security as policy compliance.
2. Security as risk minimization.

We shall first consider Information Security from the viewpoint of policies and compliance.

Table of contents I

Which actions are proper?

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

- One perspective is that given by software engineering.
  - Specify what your systems should do.
  - Design and implement systems that meet your specification.
- In case of security, specification stipulates (un)acceptable system behaviors.
- Example (from Internet shopping): Any user may fill their E-shopping cart, but only authenticated users may proceed to the check out.

Policy compliance as secure operation

- For any system

  Specification: What is it supposed to do?

  Implementation: How does it do it?

  Correctness: Does it really work?

- In security

  Specification: Policy

  Implementation: Mechanism (employed in system)

  Correctness: Compliance

Policy compliance in more detail

- Security policy states what system behavior is, and is not, allowed.
- Security mechanisms are used to enforce the policy,
- Returning to analogy with correctness:

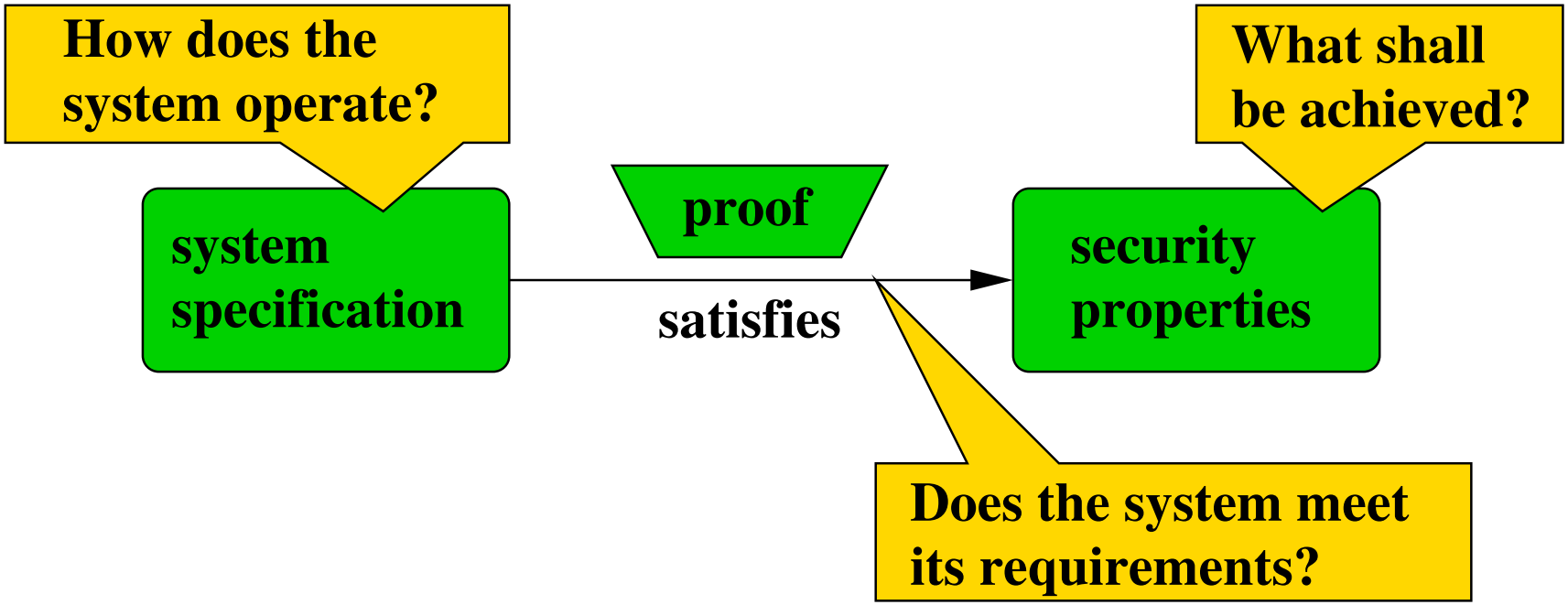
Formal Methods	Security
Specification ϕ	Security property ϕ
Program (or "Model") P	System P employing mechanisms
Correct: $P \models \phi$	Secure: $P \models \phi$

where $\models$ means "satisfies".

- Moreover, ϕ should hold for P in all malicious environments E, roughly $P||E \models \phi$ (i.e., P in parallel with E satisfies ϕ).

Formal Security Models

- Separate what shall be achieved and how this is done.



- Formal specification with formal languages.
- Semantics of languages allow for verification.
  Rigorous validation with mathematical methods.
- We will only see a few brief examples in this course (more in other courses).

Table of contents I

Traditional security properties/goals

- Policies are often formulated to achieve certain standard security properties (also called security goals).
- Common security properties are CIA:

  Confidentiality (Secrecy): No improper disclosure of information.

  Integrity: No improper modification of information.

  Availability: No improper impairment of functionality/service.
- Note that:
  - (Im)proper must be specified individually, for each system.
  - Classical CIA emphasis arose in centralized military context.

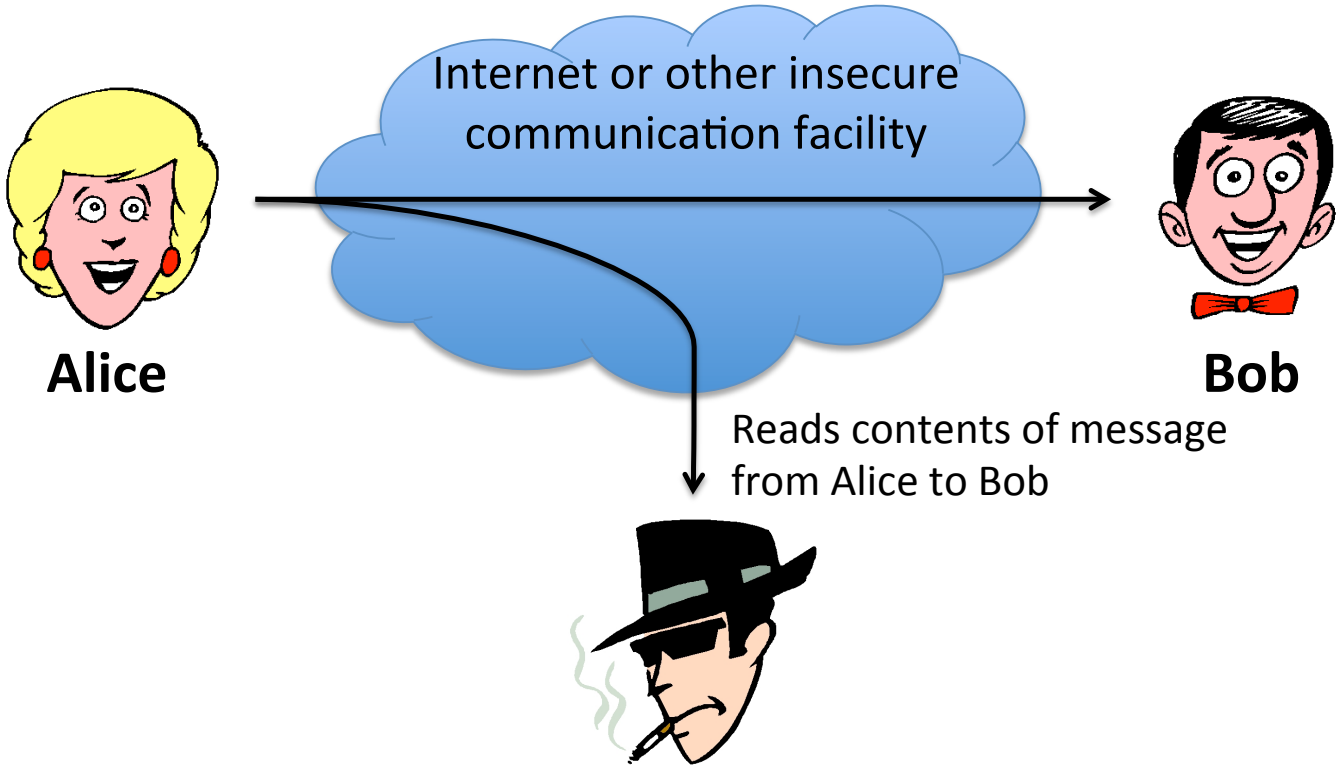
Traditional security properties/goals (cont.)

- Information Security is **CIA**. In other words:
  Confidentiality: No unauthorized access to information.
  Integrity: No unauthorized modification of information.
  Availability: No unauthorized impairment of functionality.
- Note that
  - "Information" includes data and programs.
  - CIA all deal with some form of **authorization** (which requires some form of **authentication** and **access control**).
  - Other security goals can (often) be seen as special cases of CIA.

Security properties/goals: confidentiality (i.e., secrecy)

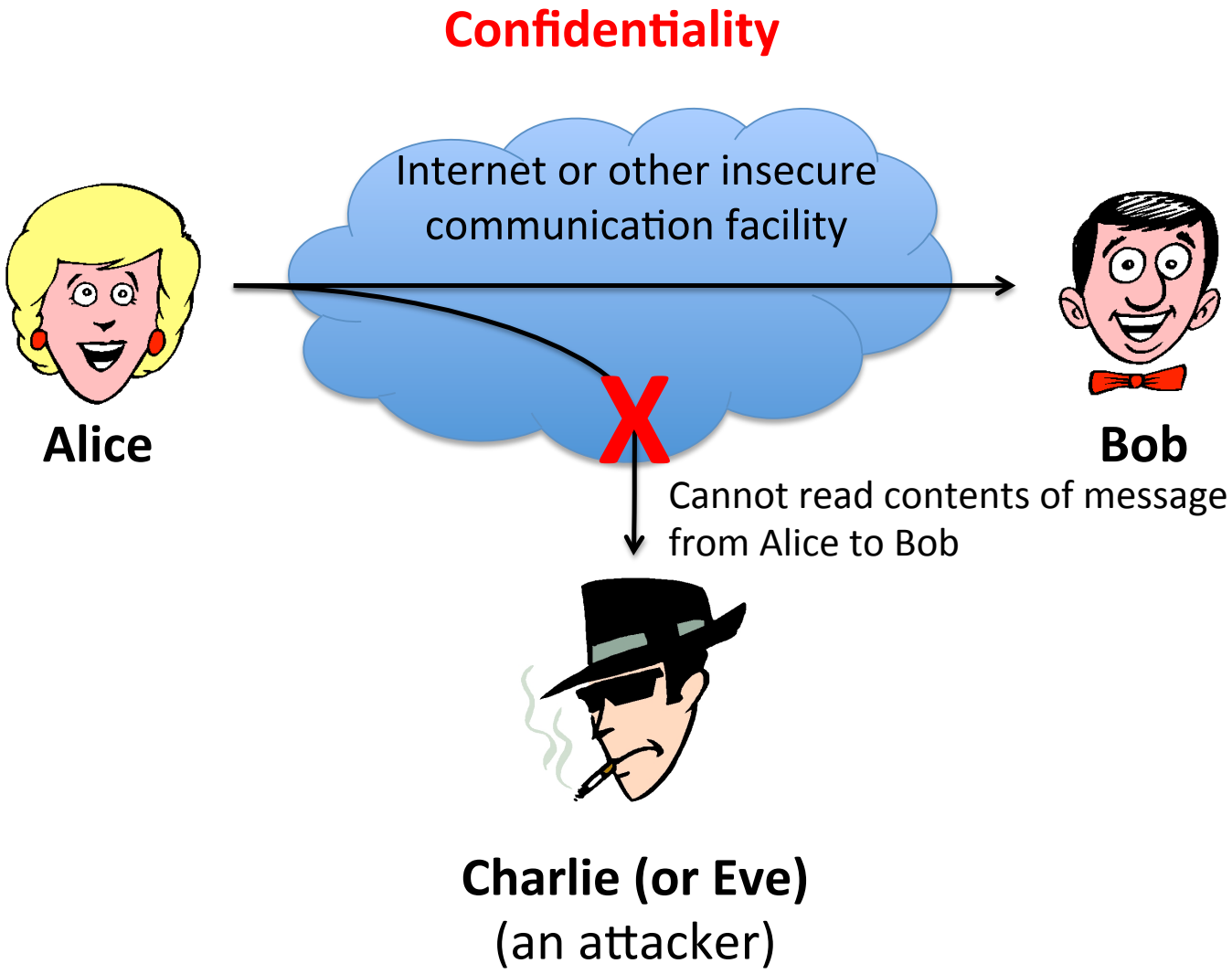
Confidentiality *information is not learned by unauthorized principals*

Attack against confidentiality (passive attack)

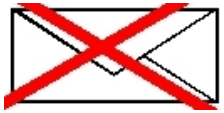


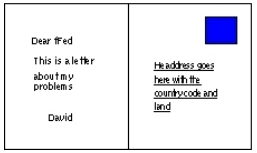
Security properties/goals: confidentiality (i.e., secrecy)

Confidentiality *information is not learned by unauthorized principals*



Confidentiality

Example Email is **not** a letter 

but rather a post card! 

Threat Everyone can read it along the way!

Mechanism Network security, encryption, and access control

Challenges Key and policy management.

Confidentiality, privacy and anonymity

Information is not learned by unauthorized principals

- Confidentiality is sometimes characterised as the unauthorized reading of data, when considering **access control** measures. But in general we are concerned with unauthorized learning of information, which is more subtle to contend with.
- Confidentiality presumes a notion of authorized party, or more generally, a **security policy** saying who or what can access our data. The security policy is used for access control.
- Sometimes: **privacy** pertains to confidentiality for individuals, whereas **secrecy** pertains to confidentiality for organizations, such as commercial companies or governments. Privacy is also sometimes used in the sense of **anonymity**, keeping one's identity private.
- Example violations: your medical records are obtained by a potential employer without your permission; "somebody" knows which websites you are accessings.

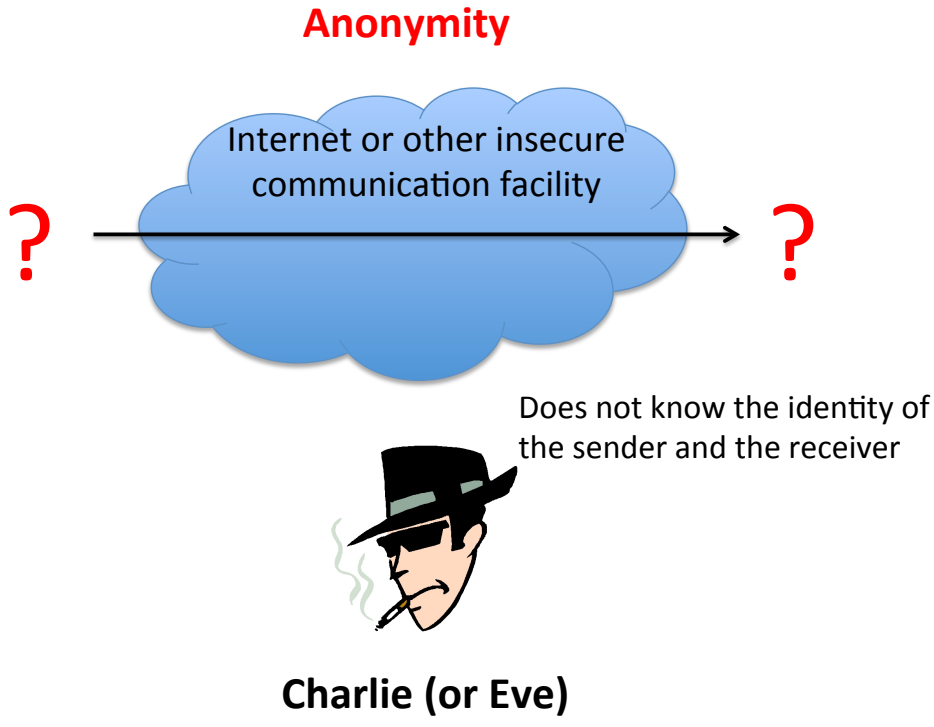
More on privacy and anonymity

Privacy:

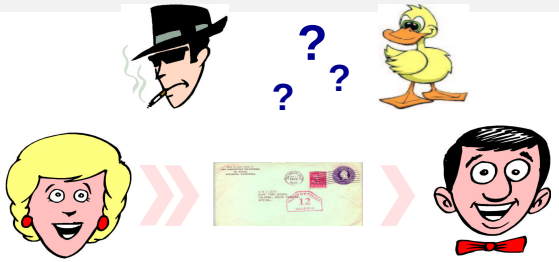
- *You choose what you let other people know*.
- Confidentiality of information that you don't want to share.

Anonymity:

- *A condition in which your true identity is not known*.
- Confidentiality of your identity.



Privacy and anonymity on public networks

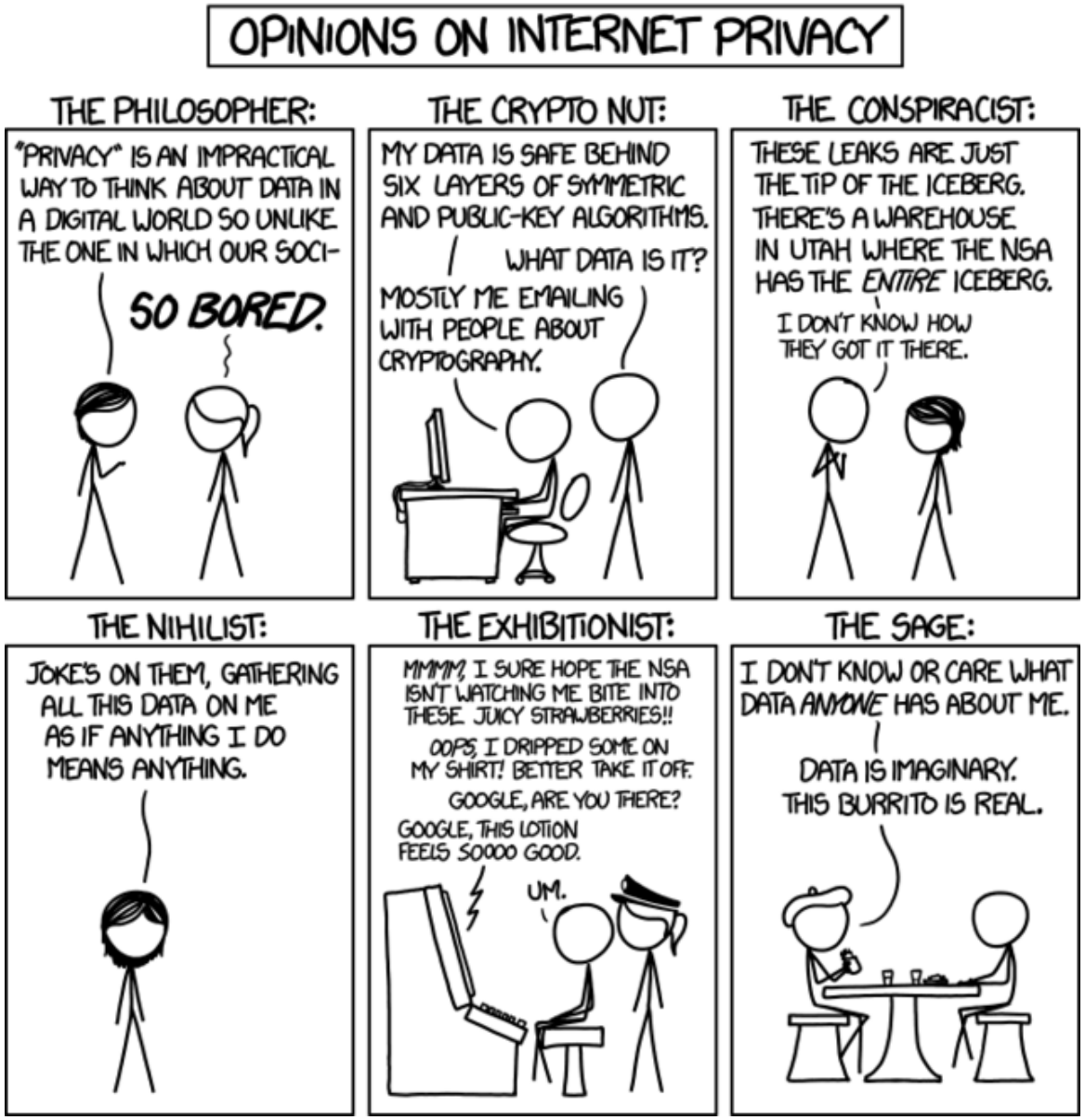


- **Internet is designed as a public network.**
  - Machines on your LAN may see your traffic, network routers see all traffic that passes through them.
  - Email is not a letter but rather a post card! (Everyone can read it along the way.)
- **Routing information is public.**
  - IP packet headers identify source and destination.
  - Even a passive observer can easily figure out *who is talking to whom*.
- **Encryption does not hide identities.**
  - Encryption hides payload, but not routing information.
  - Even IP-level encryption (tunnel-mode IPsec/ESP) reveals IP addresses of IPsec gateways.

Some possible applications of privacy and anonymity

- **Privacy**:
  - Hide online transactions, Web browsing, etc. from intrusive governments, marketers and archivists.
- **Untraceable electronic mail**:
  - Corporate whistle-blowers.
  - Political dissidents.
  - Socially sensitive communications (online AA meeting).
  - Confidential business negotiations.
- **Law enforcement and intelligence**:
  - Sting operations and honeypots.
  - Secret communications on a public network.
- **Blockchain, Cryptocurrencies, Digital cash**:
  - Electronic currency with properties of paper money (online purchases unlinkable to buyer's identity).
- **Anonymous electronic voting**.
- **Censorship-resistant publishing**.
- **Crypto-anarchy**.

Privacy

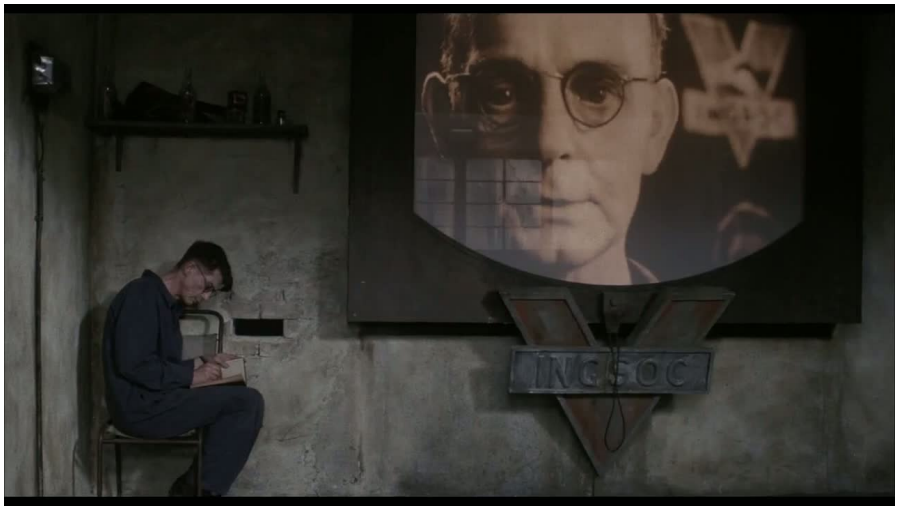

OPINIONS ON INTERNET PRIVACY
THE PHILOSOPHER:
"PRIVACY" IS AN IMPRACTICAL WAY TO THINK ABOUT DATA IN A DIGITAL WORLD SO UNLIKE THE ONE IN WHICH OUR SOCI-
SO BORED.
THE CRYPTO NUT:
MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.
WHAT DATA IS IT?
MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.
THE CONSPIRACIST:
THESE LEAKS ARE JUST THE TIP OF THE ICEBERG. THERE'S A WAREHOUSE IN UTAH WHERE THE NSA HAS THE ENTIRE ICEBERG.
I DON'T KNOW HOW THEY GOT IT THERE.
THE NIHILIST:
JOKE'S ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.
THE EXHIBITIONIST:
MMMM, I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!
OOPS, I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.
GOOGLE, ARE YOU THERE?
GOOGLE, THIS LOTION FEELS SOOOO GOOD.
UM.
THE SAGE:
I DON'T KNOW OR CARE WHAT DATA ANYONE HAS ABOUT ME.
DATA IS IMAGINARY. THIS BURRITO IS REAL.

Extreme Views on Privacy

- Extreme Anti-Privacy: "An honest person has nothing to hide!"

Hey Government... It's me... Butters. Ah I just wanna say, well, well, thanks for watching over me and, and doin' everything you do. ...An and please watch over Mommy, and Daddy, ah an and my friends ... Goodnight, Government. Oh yeah. Ah, and thank you, President Obama, for, for making me feel so safe and looked after. And if it wouldn't be... too much trouble... I'd really like to get a puppy for Christmas this year. 'Night, Government. (South Park S17E01)

- Extreme Pro-Privacy: "Otherwise we have 1984!"



Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork.

- Caution: extreme views tend to be a bit naïve...

Attacker Models

An attacker who controls major parts of the Internet is not realistic

Attacker Models

An attacker who controls major parts of the Internet is not realistic

Attacker Models

An attacker who controls major parts of the Internet is ~~not~~ realistic

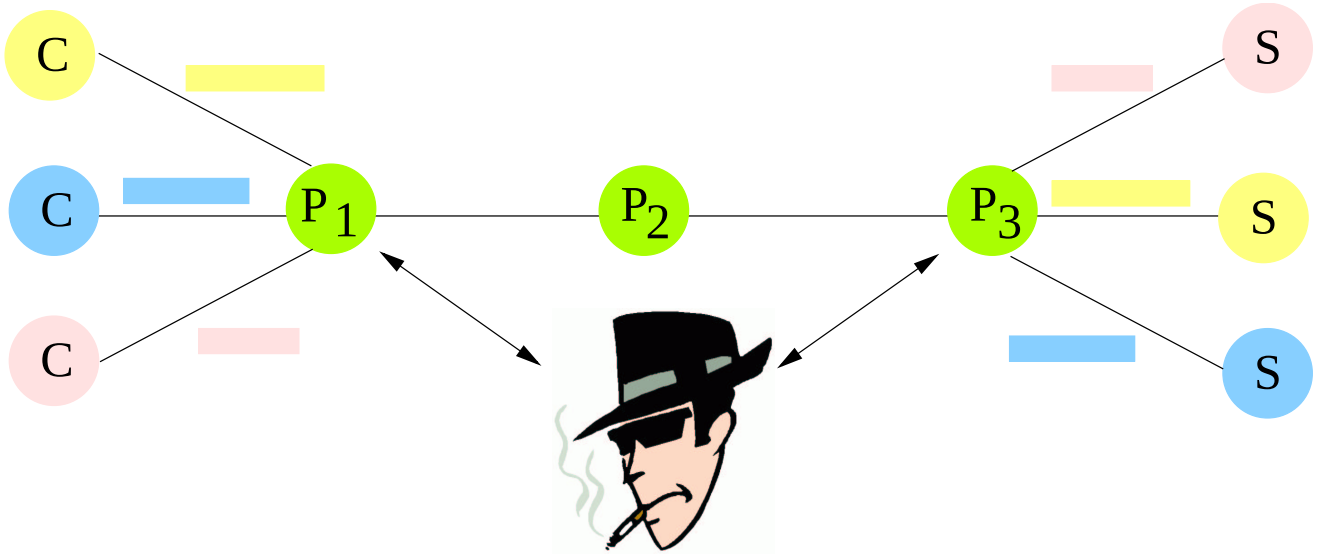
Attacker Models

An attacker who controls major parts of the Internet is ~~not~~ realistic

Why is anonymity difficult?

In a public network:

- Packet headers identify recipients.
- Packet routes can be tracked (traffic analysis).



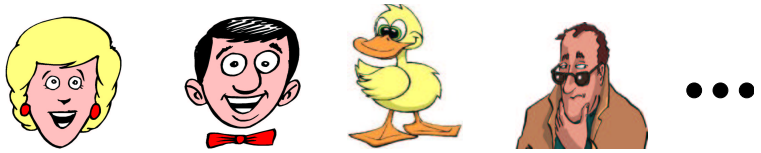
Someone observing P_1 and P_3 can usually break anonymity.

- Payload, even when encrypted, is visible.
- Short delay between messages entering P_1 and P_3.

Challenge is to design technologies to thwart such analysis.

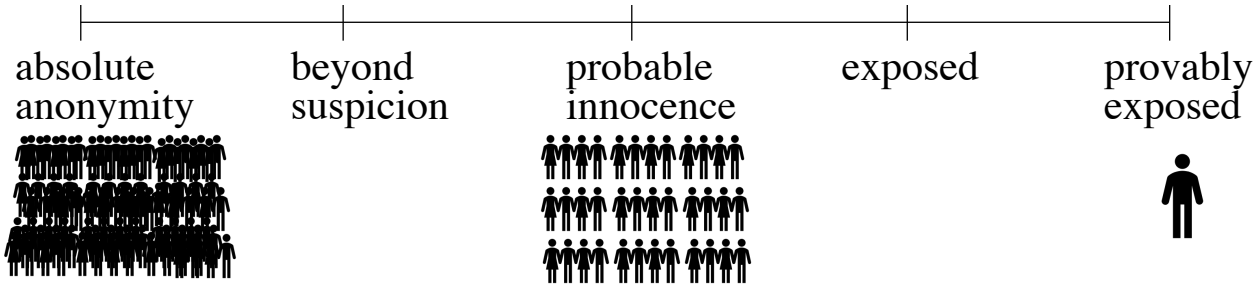
What is anonymity?

- Your actions can be observed (e.g., sending/receiving emails).



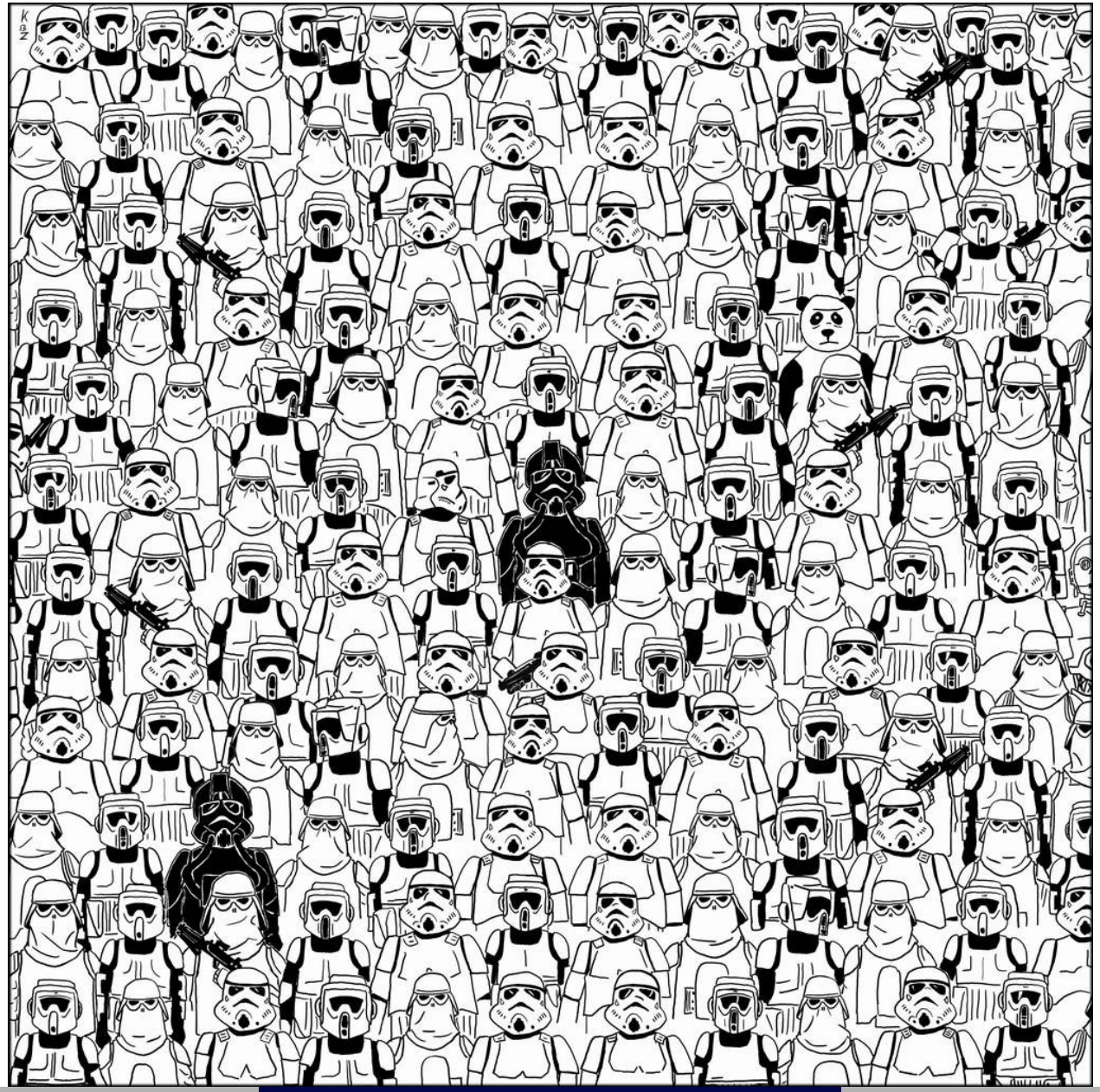
You are only anonymous within a group if your actions (sending, receiving, communication relationships) cannot be distinguished from the actions of anyone else in a group.

- This group is called the **anonymity set**. The larger, the better.



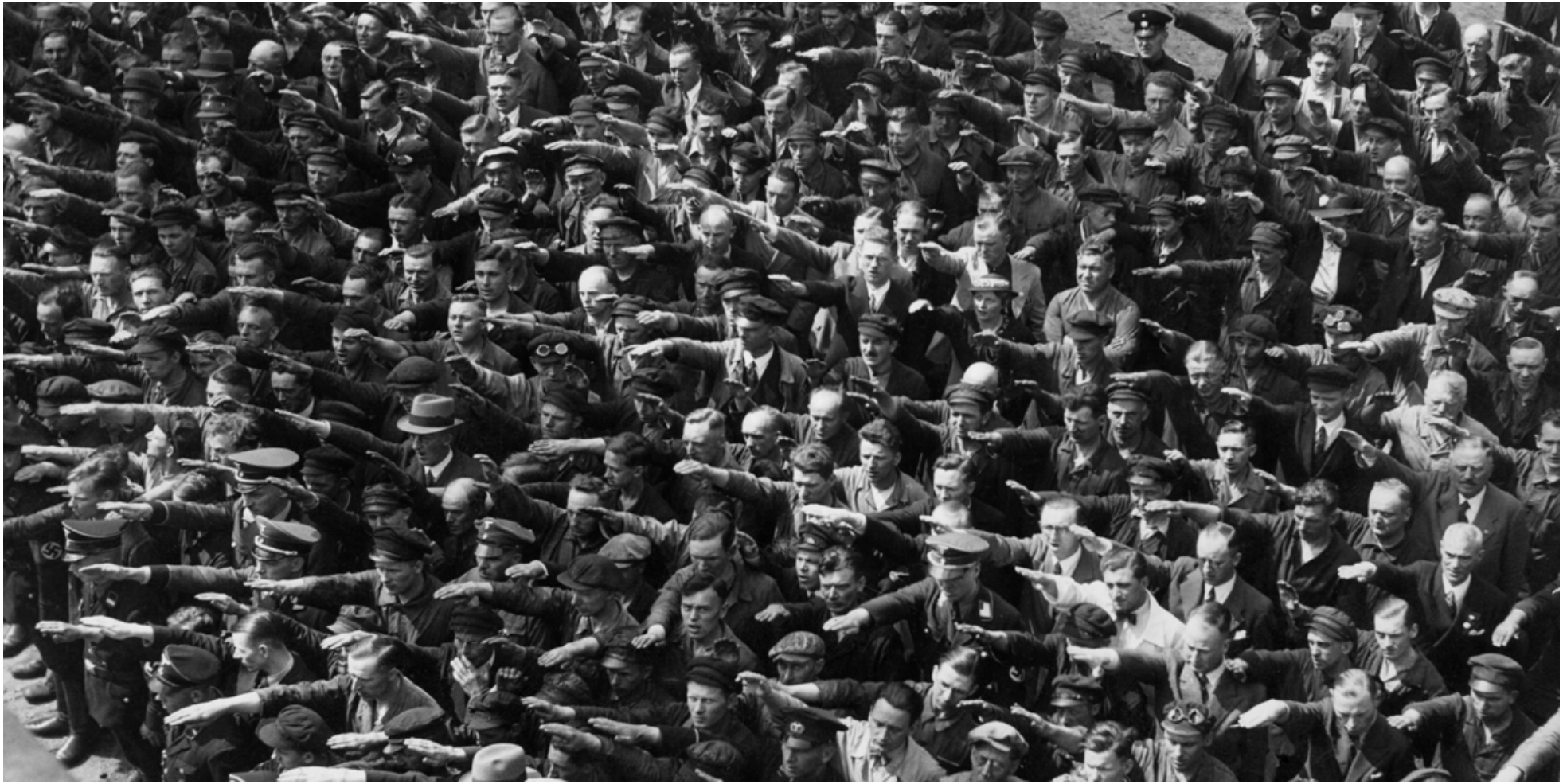
- You cannot be anonymous by yourself!
  - Big difference between anonymity and confidentiality.
- Anonymity is best when anonymizing service attracts many users.
  - All existing technologies have performance/reliability overheads.
  - Usability is central to success.

Anonymity set: find the panda



Anonymity set: the German non-saluter

Launch of a German army vessel in 1936 (a ceremony that was attended by Adolf Hitler himself)



Anonymity set: the German non-saluter

Identity uncertain: August Landmesser or Gustav Wegert?
See online controversy.

Anonymity, unlinkability, unobservability

- Summarizing: **Anonymity** is the state of being not identifiable within a set of subjects.
  - Hide your activities among others' similar activities.
- **Unlinkability** of action and identity.
  - For example, sender and his email are no more related after observing communication than they were before.
- **Unobservability** (hard to achieve).
  - Observer cannot even tell whether a certain action took place or not.

Attacks on anonymity?

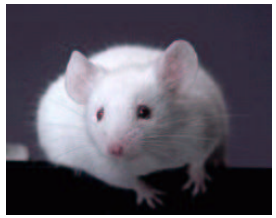
- **Passive traffic analysis**:
  - Infer from network traffic who is talking to whom.
  - To hide your traffic, must carry other people's traffic!
- **Active traffic analysis**:
  - Inject packets or put a timing signature on packet flow.
- **Compromise of network nodes (routers)**:
  - It is not obvious which nodes have been compromised
    - Attacker may be passively logging traffic.
  - Better not to trust any individual node
    - Assume that some *fraction* of nodes is good, don't know which.

Unobservability/Anonymity

- **Requirements:** Anonymize the sender and/or the receiver. Provide confidentiality of principals' identities.
- **Pseudonyms** as a lightweight mechanism.

John Wayne
(**Marion Mitchell Morrison**, born **Marion Robert Morrison**)

Robert Galbraith
(**J.K. Rowling**)



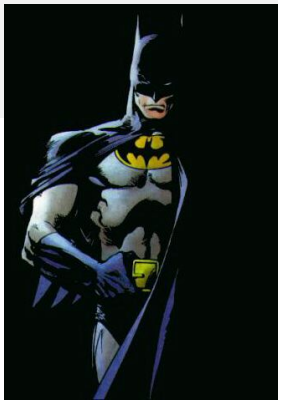
Mouse !!!
Come back − I love you!

Your kissy−bear

Linkage to actual identity only in restricted cases.

- IT equivalent: mail and surf from an ISP account, Hotmail, ...
- Pseudonyms need sometimes to be resolved into the proper (underlying) names.
- But naming and name resolution can be quite problematic.

A naming example



Q: Who is Batman? **A:** Bruce Wayne!

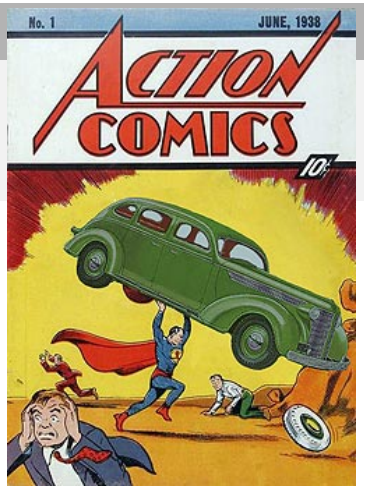
Adam West | Michael Keaton | Val Kilmer | G. Clooney | Christian Bale | Ben Affleck | Will Arnett | R. Pattinson

Q: What do Batman and Michael Douglas have in common?

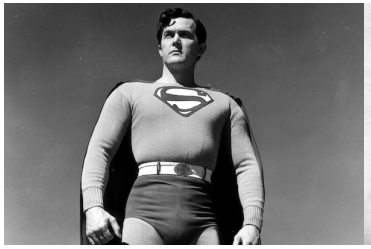
Michael Kirk Douglas.
Son of Kirk Douglas (birth name: Issur Danielovitch Demsky).

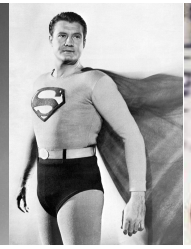
Michael John Douglas, a.k.a. Michael Keaton.
Played *Batman* in the movies *Batman* and *Batman returns*.

A naming example



Q: Who is Superman? **A:** Clark Kent!


Kirk Alyn

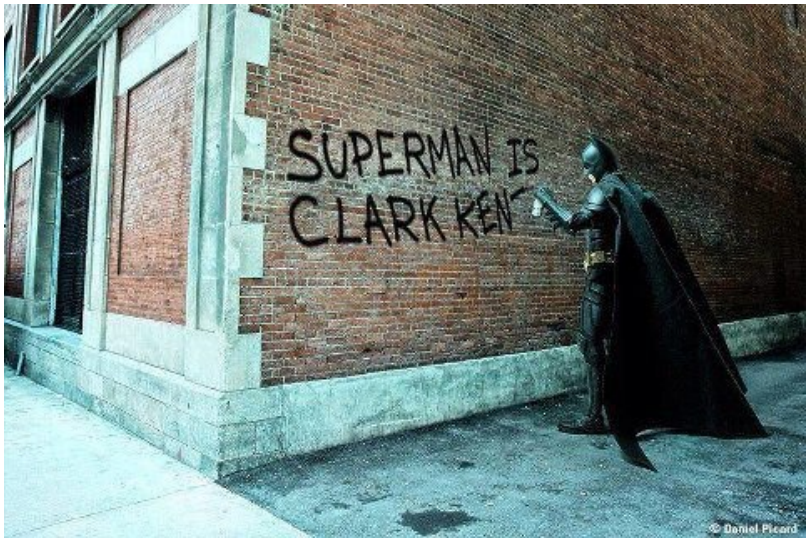

George Reeves


Christopher Reeve


Brandon Routh


Henry Cavill


Channing Tatum



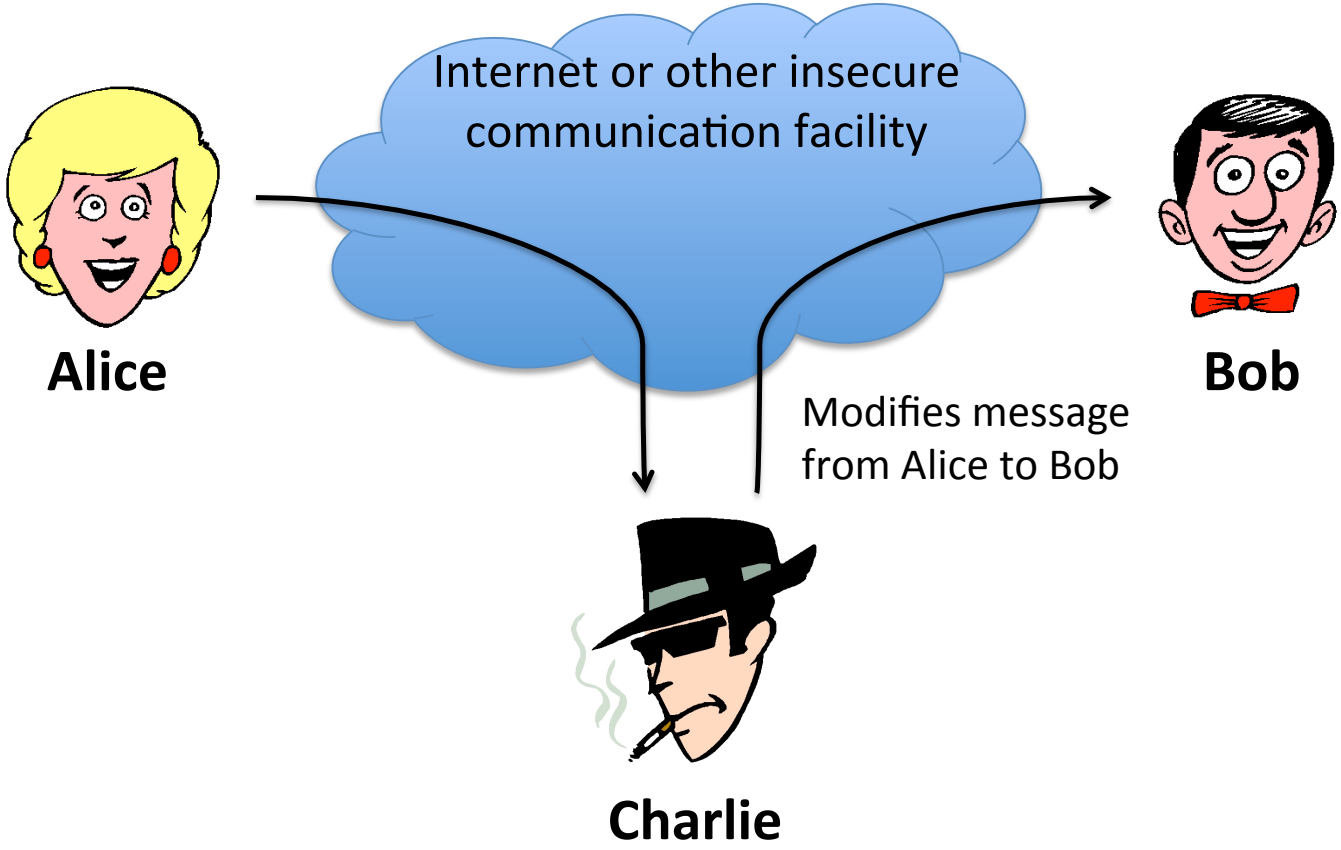
Well... Superman is Clark Kent, but Clark Kent is actually Kal-El.

Name resolution is quite a complex problem, with much on-going research.

Security properties: integrity

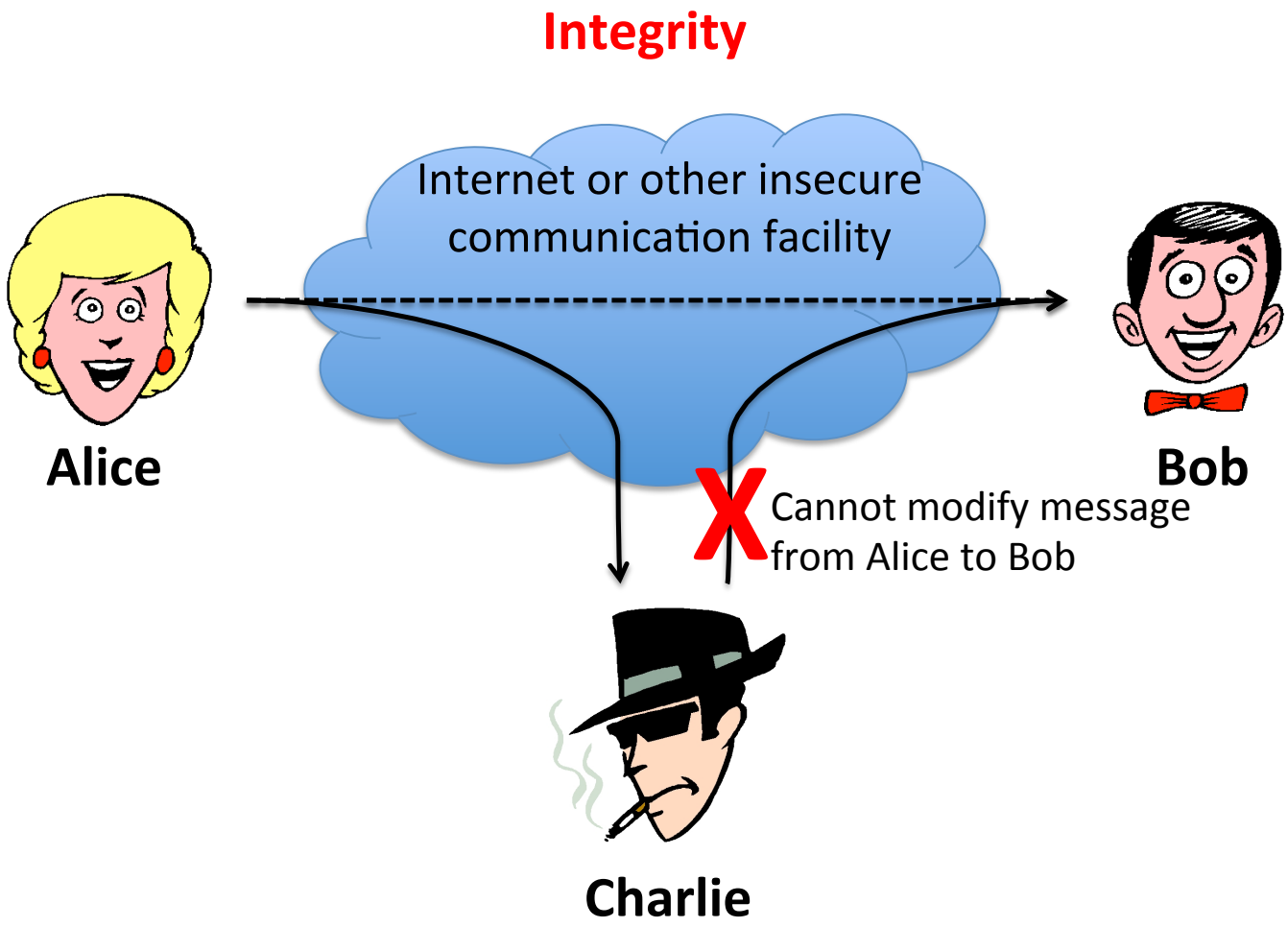
Confidentiality *information is not learned by unauthorized principals*
Integrity *data has not been (maliciously) altered*

Attack against integrity (active attack)



Security properties: integrity

Confidentiality *information is not learned by unauthorized principals*
Integrity *data has not been (maliciously) altered*



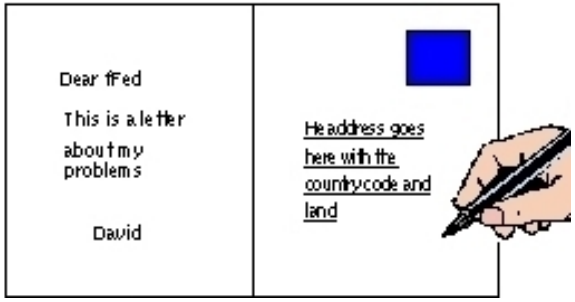
Integrity

Data has not been maliciously altered

- Integrity has more general meanings elsewhere, but in computer security we are concerned with preventing the possibly malicious alteration of data, by someone who is not authorized to do so.
- Integrity in this sense can be characterised as the unauthorized writing of data. Again, this presumes a security policy saying who or what is allowed to alter the data.
- Example violation: an on-line payment system alters an electronic payment to read £ 10,000 instead of £ 100.

Integrity

Example Email (or forms, records, ...)



Threat Unallowed modification/falsification

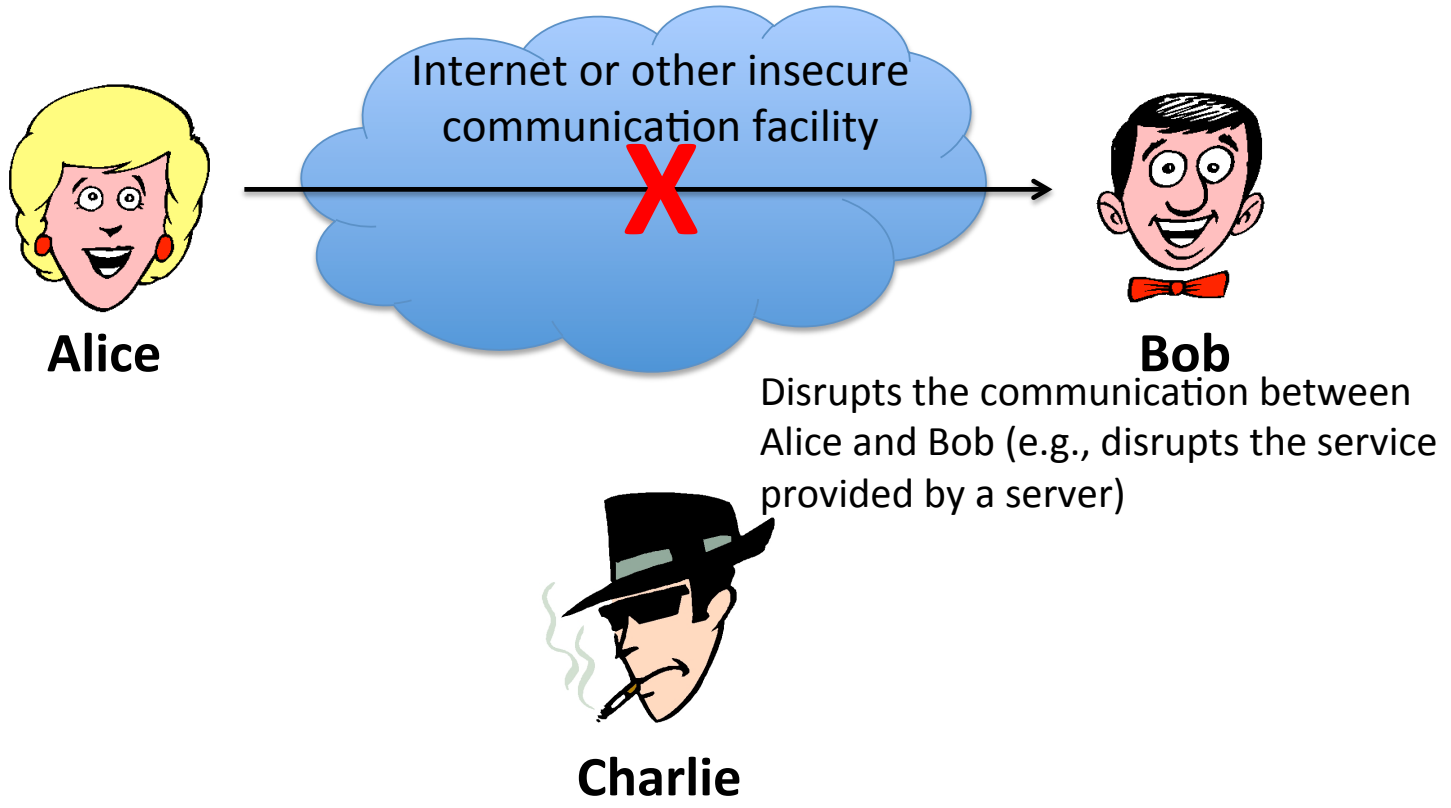
Mechanism Digital signatures and/or access control

Challenges PKI and policy management

Security properties

Confidentiality *information is not learned by unauthorized principals*
Integrity *data has not been (maliciously) altered*
Availability *data/services can be accessed when desired*

Attack against availability



Disrupts the communication between Alice and Bob (e.g., disrupts the service provided by a server)

Availability

Data or services can be accessed in a reliable and timely way

- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infecting a system with a debilitating virus).
- In computer security we're concerned with protecting against the second kind of threat, rather than providing more general forms of fault-tolerance or dependability assurance.
- Ensuring availability means preventing **denial of service** (DoS) attacks, insofar as this is possible. It's possible to fix attacks on faulty protocols, but attacks exhausting available resources are harder, since it can be tricky to distinguish between an attack and a legitimate use of the service.
- Example violations: the deadly distributed DoS (DDoS) attacks against on-line services; interfering with IP routing.

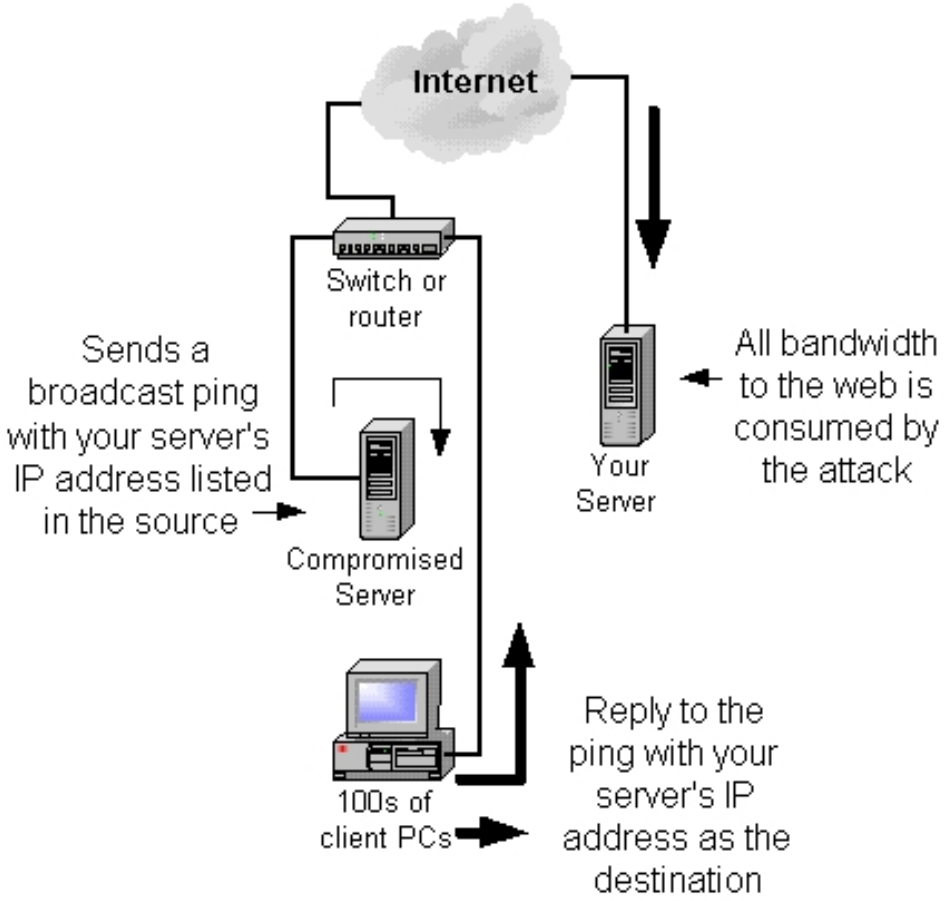
Availability

Example Communication with a server

Threats Denial of service, break-ins, ...

Mechanism Fire-walls, virus-scanners, backups, redundant hardware, secure operating systems, etc.

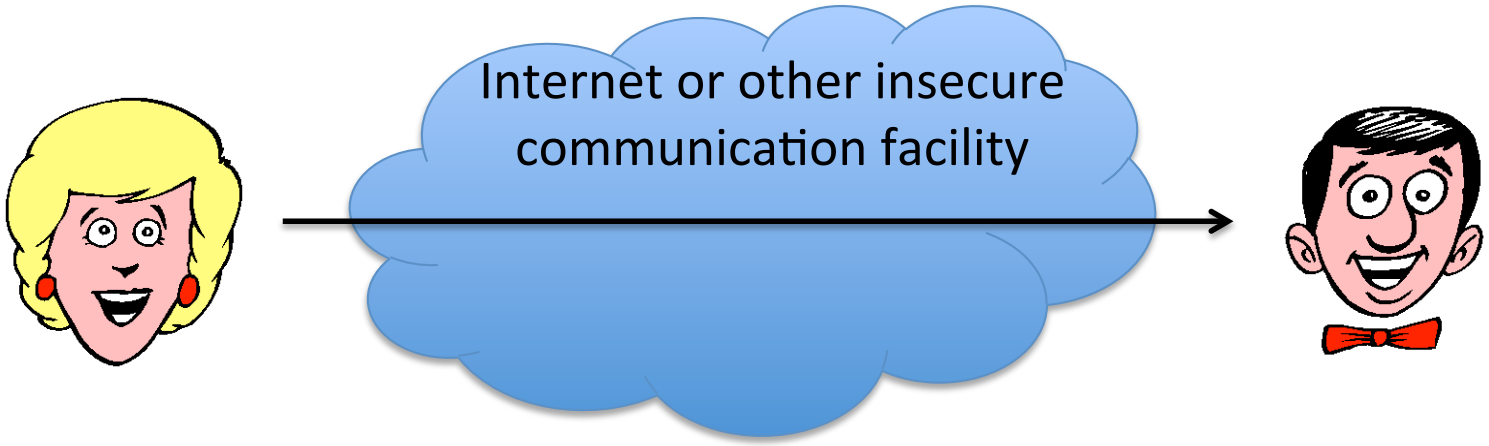
Challenges Difficult to cover all threats (and still have a usable system)



Security properties: accountability

Confidentiality	*information is not learned by unauthorized principals*
Integrity	*data has not been (maliciously) altered*
Availability	*data/services can be accessed when desired*
Accountability	*actions can be traced to responsible principals*

Accountability



Alice
"I sent the message"

Bob
"I received the message"

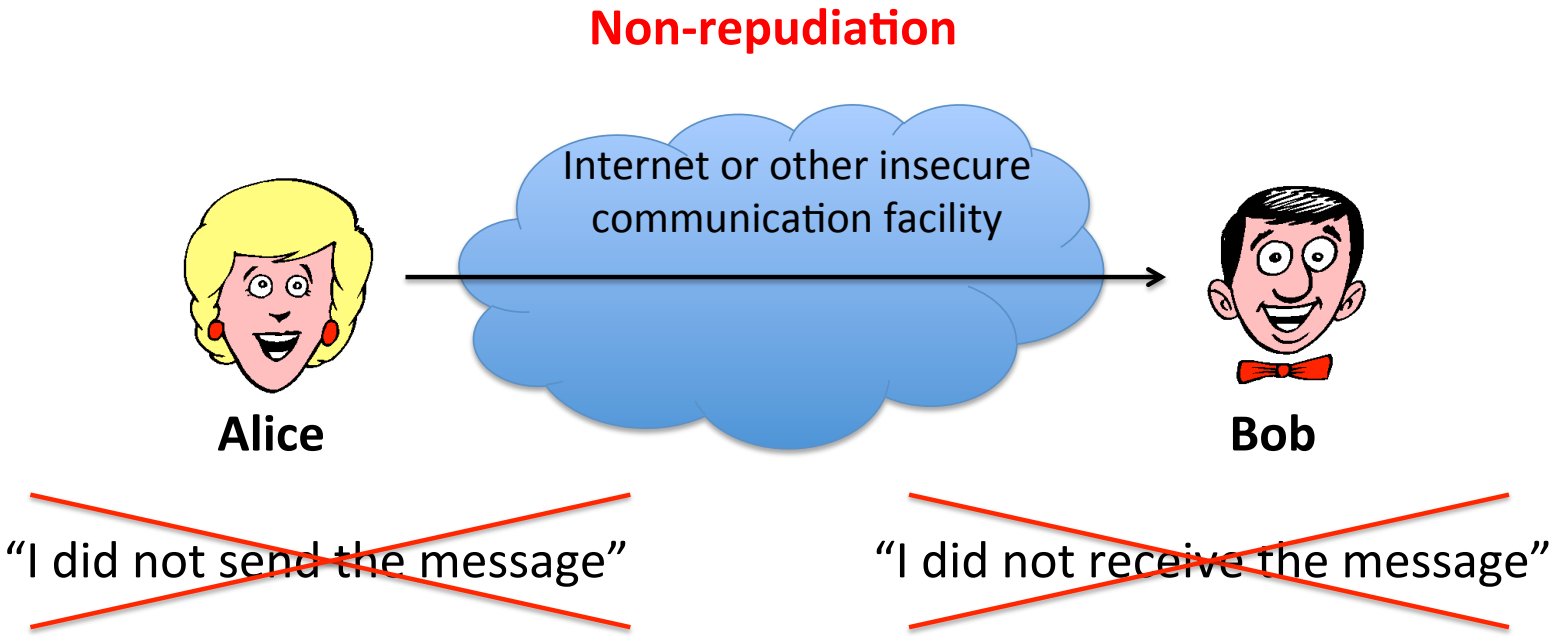
Accountability

Actions are recorded and can be traced to the party responsible

- If prevention methods and access controls fail, we may fall back to detection: keeping a *secure audit trail* is important so that actions affecting security can be traced back to the responsible party.
- A stronger form of accountability is *non-repudiation*, when a party cannot later deny some action.
- Creating an audit trail with machine logs is a tricky problem: if a system is compromised, the logs may also be tampered with. Ways around that problem are to send log messages to an append-only file, a separate server, or even a physically isolated printer.
- Example violation: an audit trail is tampered with, lost, or cannot establish where a security breach occurred.

Security properties: non-repudiation

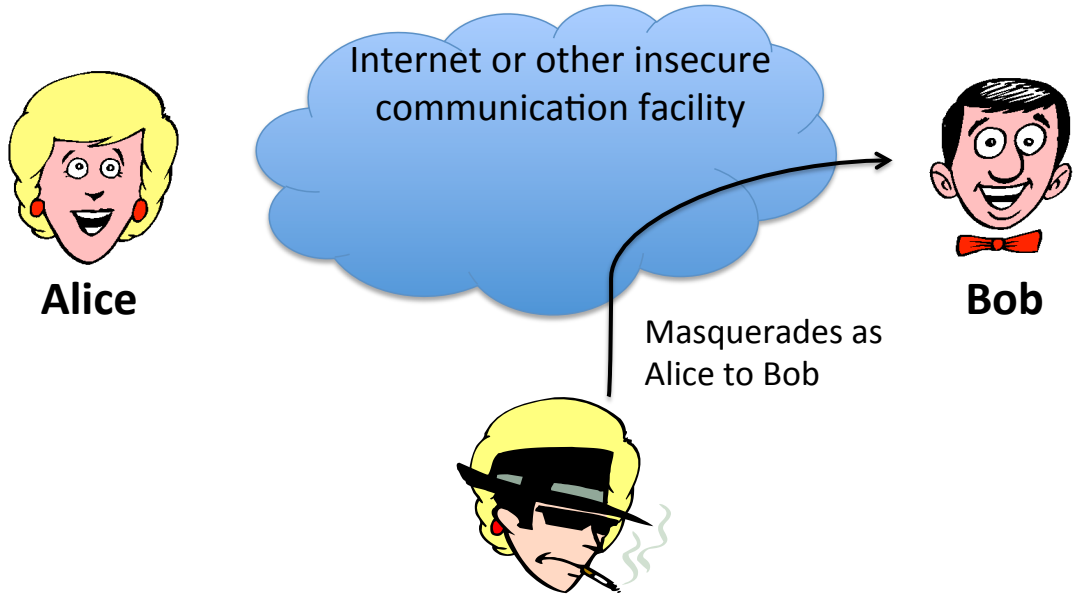
Confidentiality	*information is not learned by unauthorized principals*
Integrity	*data has not been (maliciously) altered*
Availability	*data/services can be accessed when desired*
Accountability	*actions can be traced to responsible principals*
Non-repudiation	*actions done cannot be denied*



Security properties: authentication

Confidentiality	*information is not learned by unauthorized principals*
Integrity	*data has not been (maliciously) altered*
Availability	*data/services can be accessed when desired*
Accountability	*actions can be traced to responsible principals*
Authentication	*principals or data origin can be identified accurately*

Attack against authentication



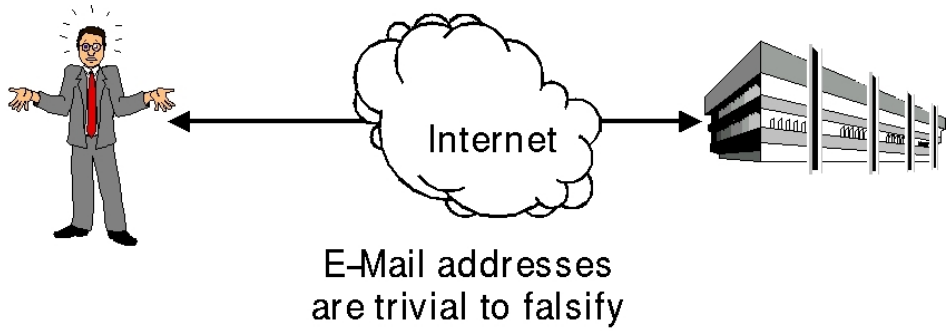
Authentication

Data or services available only to authorized identities

- Authentication is verification of identity of a person or system.
- Some form of authentication is a pre-requisite if we wish to allow access to services or data to some people but deny access to others, using an access control system.
- Methods for authentication are often characterised as:
  - **something you have**, e.g. an entrycard,
  - **something you know**, e.g. a password or secret key, or
  - **something you are**, e.g. a fingerprint, signature, biometric.
- Also, where you are may be implicitly or explicitly checked. Several methods can be combined for extra security.
- Examples of violation: using cryptanalysis to break a cryptographic algorithm and learn a secret key; purporting to be somebody else (identity theft) by faking email, IP spoofing, or stealing a private key and signing documents.

Authentication

Example



Threats Misuse of identity

Mechanisms

- **Individuals:** who one is, what one has, or what one knows.
- **Processes, Data:** cryptographic protocols, digital signatures, etc.

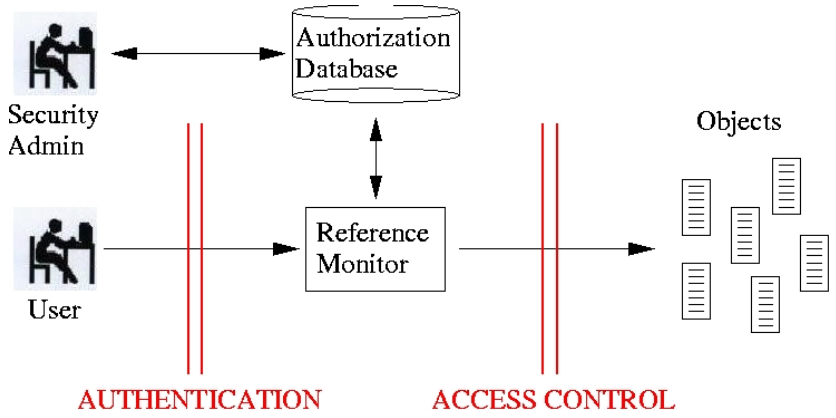
Challenges authentication hardware/mechanisms, protocol design/analysis, PKIs

Authorization

Example Access to data, processes, networks, ...

Threats Unauthorized access of resources

Mechanisms Declarative and programmatic control mechanisms



Challenges Policy design, integration, and maintenance

Security properties

Confidentiality	*information is not learned by unauthorized principals*
Integrity	*data has not been (maliciously) altered*
Availability	*data/services can be accessed when desired*
Accountability	*actions can be traced to responsible principals*
Authentication	*principals or data origin can be identified accurately*

Usually we want to protect all properties in specific ways. Different mechanisms may be used to provide protection, but from the start we must realise that **security is a whole system issue**. The whole system is used in the most inclusive sense: software, hardware, physical environment, personnel, corporate and legal structures.

Usually we will be more restrictive, and security evaluation standards like Common Criteria (see below) are deliberately so, to allow comparison between different security solutions.

Properties versus policies versus mechanisms

- Distinction is fuzzy!
  - Properties generally high-level and abstract.
  - Policy may just be the conjunction of different properties.
  - Alternatively, policy may be more low-level and operational, e.g., comprised of rules like “strong passwords should be used”.
- Mechanisms are concrete, e.g., implementation components.
- Analogy with correctness: specifications at different abstraction levels ranging from “what” (behavior) to “how” (design/code).
- Boundary with other non-security properties also fuzzy.

  Functional correctness: system behaves “properly”.
  Reliability: no accidental failures, even in adverse circumstances.

Example security policy

- A bank may require
  - authenticity of clients (at teller, ATMs, or on the Internet)
  - non-repudiation of transactions
  - integrity of accounts and other customer data
  - secrecy of customer data
  - availability of logging
- The conjunction of these properties might constitute the bank's (high-level) security policy.

Another example: e-voting

- An e-voting system should ensure that
  - only registered voters vote
  - each voter can only vote once
  - integrity of votes
  - privacy of voting information (only used for tallying)
  - availability of system during voting period
- In practice, many policy aspects are difficult to formulate precisely. Other examples: protection against email flooding/spam and monitoring of, and reaction to, suspicious behavior.

Privacy Policies in Voting Systems: two examples

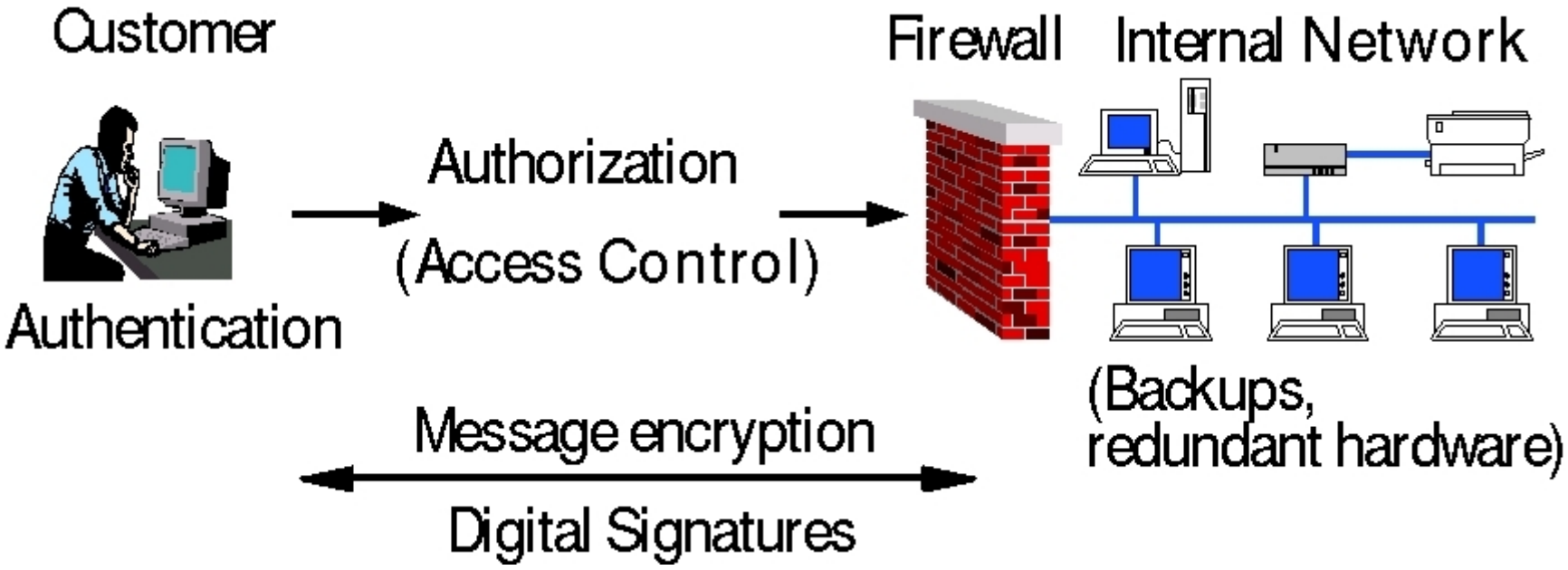
George Caleb Bingham's "The County Election" (1852), pictures the American democratic system in progress. The story takes place in a small Midwestern town in the mid-nineteenth century, when the rituals of voting were still taking shape, particularly on the frontier.

In this crowded composition, Bingham suggests the inclusiveness of a democracy with representatives of every age and social stratum — except, of course, African Americans, who would not enjoy the right to vote until after the Civil War, and women, whose right to participate would not be recognized for another seventy years. The painting reveals other irregularities in the electoral system that would not be tolerated today. Because there was no system of voter registration, the man in red at the top of the courthouse steps swears on the Bible that he hasn't already cast a vote. Because there was no secret (or even paper) ballot, a voter calls out his choice to the election clerks behind the judge, who openly record it in a ledger. Because there were no restrictions on electioneering, the well-dressed gentleman behind the voter — evidently one of the candidates – is free to hand his card to citizens just before they cast their vote. Yet none of this appears to dull the spirit of the voting process.

Privacy Policies in Voting Systems: two examples

Landsgemeinde (“cantonal assembly”) still practiced in 2 Swiss cantons: eligible citizens meet on a certain day in the open air to decide on laws and expenditures by the council, voting by raising their hands (historically, or in Appenzell until the admission of women, the only proof of citizenship necessary for men to enter the voting area was to show their ceremonial sword or Swiss military sidearm, i.e. bayonet).

Security mechanisms (or countermeasures)



We will consider how different mechanisms can be used to achieve goals in the face of threats, and what some of the challenges are.

Challenge: employing adequate mechanisms and demonstrating that the resulting system is secure.

Protection countermeasures

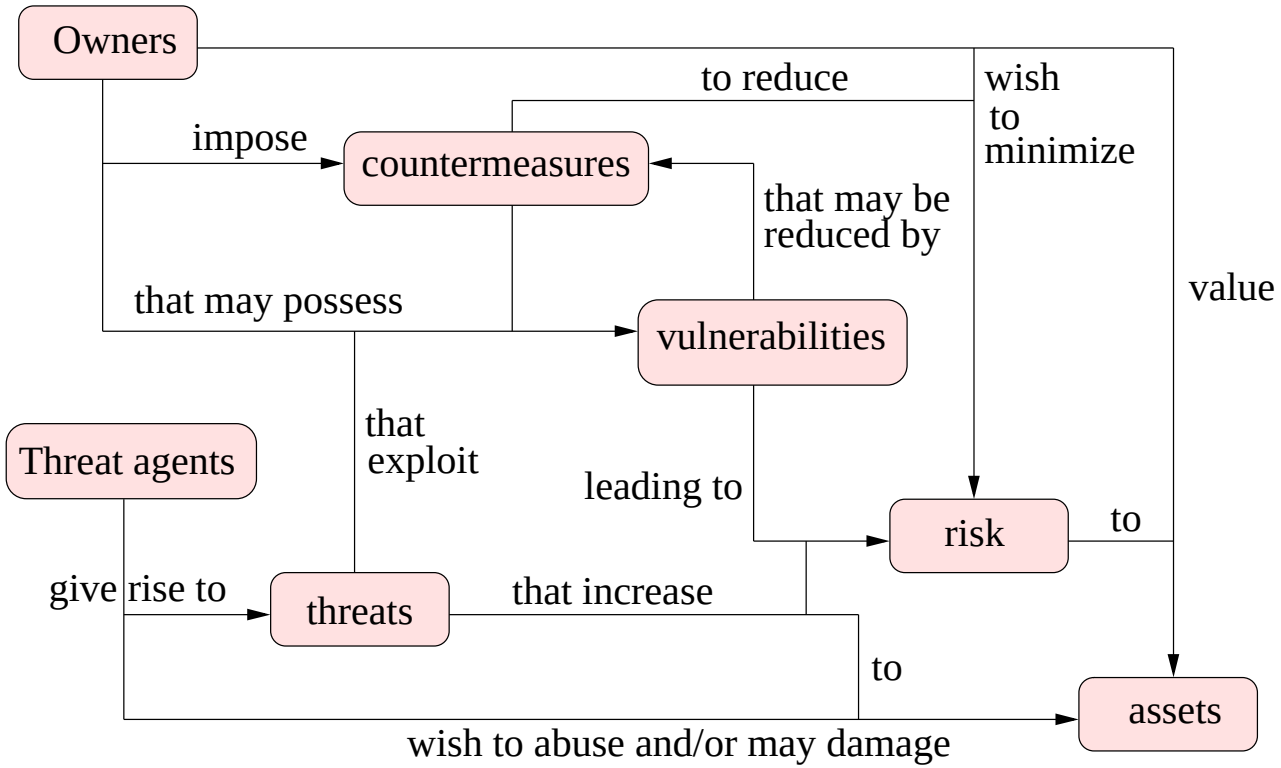
- **Prevention.** We try to prevent security breaches by system design and employing appropriate security technologies as defences. For example, using a firewall to prevent external access to corporate intranets. Prevention is the most important protection measure.
- **Detection.** In the event of a security breach, we try to ensure that it will be detected. This is particularly pertinent in computer security, where "theft" of a file does not imply denial of access for the owner. Logging and MACs (file hashes to detect alteration) are primary methods of detection, although *intrusion detection* systems which actively watch for intruders are becoming more common.
- **Response.** In the event of a security breach, we should have some arrangement in place to respond or recover the assets. Responses range from restoring backups through to informing appropriate concerned parties or law-enforcement agencies.

Summary: security as policy compliance

- Policy/goal oriented view of security, e.g., CIA.
- Definitions themselves don't give rise to a "security process" How do we define policy, analyze threats, come up with mechanisms, demonstrate adequacy of mechanisms, identify tradeoffs and costs, ... ?
- How difficult is the correctness question $P||E \models G$?
  - What constitutes E in practice?
  - And does P behave as expected? Under what assumptions?

Table of contents I

Information Security as risk minimization



Source: Common Criteria.

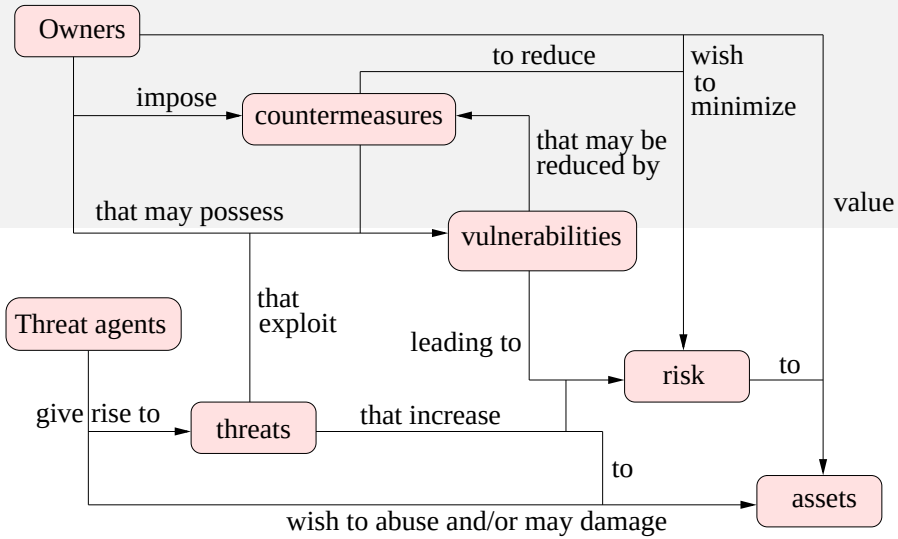
- Classification depicts fundamental concepts and interrelationships.
- Policy (here implicit) defines authorized actions on assets, i.e., what constitutes abuse.

Information Security as risk minimization (cont.)

- Security concerns the protection of **assets** from **threats**. Threats are the potential for abuse of assets.
- Owners value their assets and want to protect them. **Threat agents** also value assets, and seek to abuse them.
- **Owners** analyse threats to determine which ones apply; these are the **risks** that can be costed. This helps the selection of **countermeasures**, which reduce the **vulnerabilities**.
- Vulnerabilities may remain leaving some residual risk; owners seek to minimise that risk, within other constraints (feasibility, expense).

NB: The Common Criteria regards threats related to malicious or accidental human activities; usually we focus on malicious activity.

Information Security as risk minimization (cont.)



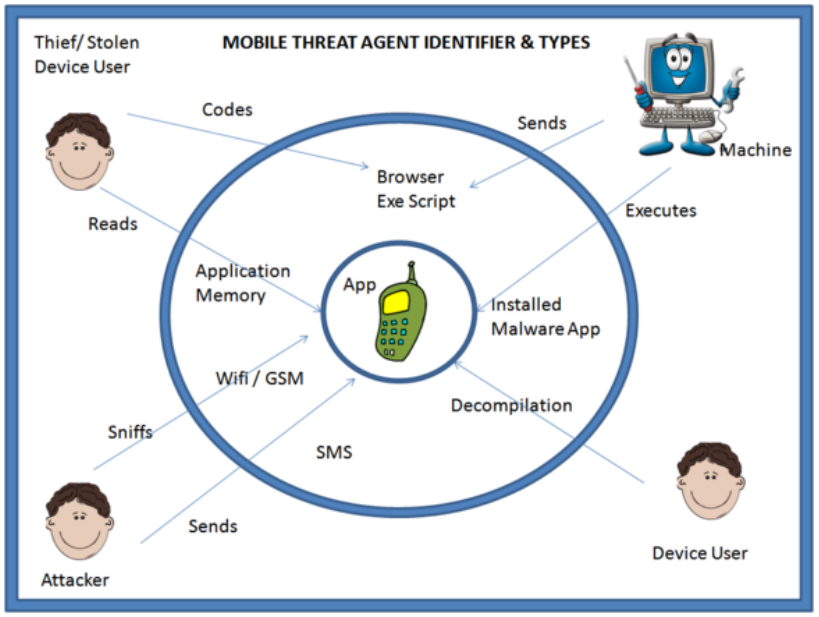
- Focus on risks from vulnerabilities and their exploitation.
- Risk = chance of abuse $\times$ impact.
- Employ countermeasures where most cost-effective.
- Central notion is that of risk.
  In contrast, policy is only implicit in determining what constitutes abuse, i.e., which actions on assets are unauthorized.

Let us first consider typical threats and vulnerabilities and after the essence of risk reduction approaches.

Threat agents

In increasing order of severity

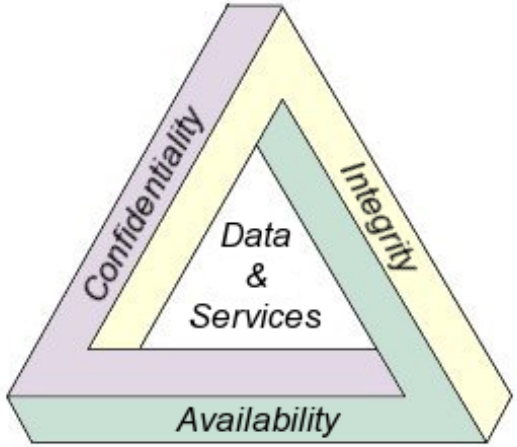
- Employees making unintentional blunders.
- Hackers driven by technical challenge.
- Disgruntled employees or customers.
- Criminals interested in personal gain.
- Organized crime interested in financial gain.
- Organized terrorist groups.
- Foreign espionage agents.
- Information-warfare operations intended to disrupt weapons or command structures.



or

?

Threats



Confidentiality	**Interception**	Unauthorized party gains access to data or services
Integrity	**Interruption**	Service or data becomes unavailable or unusable
Availability	**Modification**	Unauthorized tampering of data or services
	Fabrication	Generation of additional data or activities

Common objectives include: publicity, fraud, theft of intellectual property, destruction, and invasions of privacy as well as intermediate goals such as stealing a password or establishing a backdoor.

Vulnerabilities

- A vulnerability is a weakness that can be exploited by a threat (attack) to cause damage.
- Vulnerabilities often result from interaction in uncertain or hostile environments.

  Physical environment: e.g., laptop in enemy hands.
  Network environment: Internet.
  Software environment: OS, drivers, mobile code, plugins, ...
- Trend is towards increasing vulnerabilities.

  Open infrastructures, distributed administration, importance of quick time-to-market, software/hardware monocultures.

What kinds of vulnerabilities exist in practice?

Here are some examples (but there are much more):

OWASP Top Ten 2017
(Open Web Application Security Project, www.owasp.org)

A1: Injection

A2: Broken Authentication

A3: Sensitive Data Exposure

A4: XML External Entities (XEE)

A5: Broken Access Control

A6: Security Misconfiguration

A7: Cross-Site Scripting (XSS)

A8: Insecure Deserialization

A9: Using Components with Known Vulnerabilities

A10: Insufficient Logging And Monitoring

Authentication vulnerabilities — some details

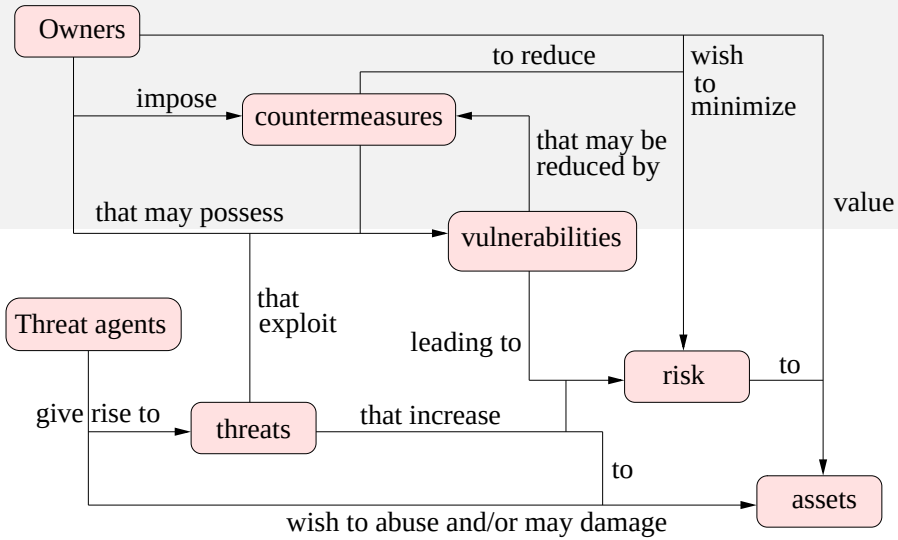
Passwords, pass phrases and/or security codes are used in virtually every interaction between users and information systems. Since properly authenticated access is often not logged, or if logged not likely to arouse suspicion, a compromised password is an opportunity to explore a system virtually undetected. Despite this threat, user and administrator level accounts with poor or non-existent passwords are still very common. As well, organizations with a well-developed and enforced password policy are still uncommon. The most common password vulnerabilities are:

1. user accounts that have weak or nonexistent passwords;
2. user accounts with widely known or openly displayed passwords;
3. system or software created administrative level accounts with widely known, weak, or nonexistent passwords; and
4. weak password hashing algorithms and/or user password hashes that are stored with weak security and that are visible to anyone.

SSL vulnerabilities — some details

- The open-source OpenSSL library provides cryptographic support to the applications that communicate over the network. It is a very widely deployed SSL/TLS protocol implementation, and is used by a large number of vendors. Many of the commonly used POP3, IMAP, SMTP and LDAP servers also have their OpenSSL-based counterparts.
- Multiple vulnerabilities have been found in the OpenSSL library. These vulnerabilities can be remotely exploited to execute arbitrary code at the privilege level of the applications using the OpenSSL library. In some cases, such as the “sendmail”, a successful exploitation may yield root privileges.
- Heartbleed! (See the vulnerability reports.)

Risk analysis and reduction steps



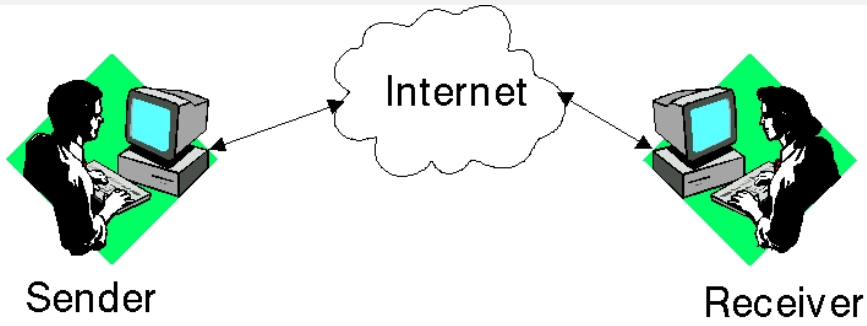
Part I. Analysis of existing risks:

1. Identify assets you wish to protect.
   What are the (information) assets and their functionalities?
2. Identify risks to these assets.
   Requires understanding threat agents and their threats as well as vulnerabilities.

Part II. Analysis of proposed security solution:

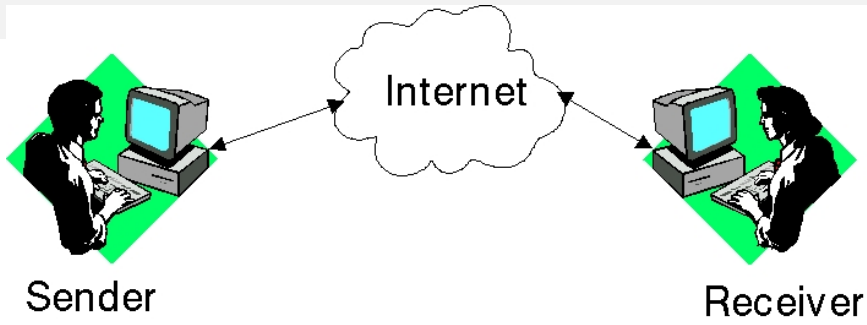
3. How well do proposed countermeasures reduce risk?
4. What other risks and tradeoffs do measures themselves bring?

Example: protecting email



1. What are the information assets?
   Possible answers: mail content (confidentiality, integrity), sender/recipient identities, service availability, ...
2. What are the risks?
   - Others reading or tampering with your mail, observing with whom you communicate, and disrupting service.
   - Chance of abuse depends on who you are, what you send, and how interesting it is to others.

Example: protecting email, analysis of a possible solution



Evaluation of PGP as
a possible good solution:

3. Effectiveness: high provided it is used correctly.
4. New risks and tradeoffs:
   - Key exchange time consuming and requires some sophistication.
   - Users must learn, and properly apply, new mailer functionalities.

Conclusion: PGP is good solution for ensuring confidentiality of sensitive information mailed between knowledgeable partners.

Example: face scanning in airports

Since 9/11, face scanning and matching against databases of known terrorists has been proposed to improve airport security.

1. What are the assets (information or otherwise)?
   Air travelers and those on the ground.
2. What are the risks?
   Terrorists will board planes and may cause harm.
3. Effectiveness: very low.
   Suppose system positively identifies 50% of all known terrorists but has 1% rate of false positives. Suppose there is one terrorist per million. Then for every terrorist recognized, so are 20,000 innocent civilians. At this rate, the security personal will be overwhelmed and stop believing the alarms.

Example: face scanning in airports (cont.)

4. New risks and tradeoffs.
   The face database must be secured. If integrity is not protected, faces can be deleted. If confidentiality not protected, terrorists can determine if they are in database and take appropriate actions (e.g., send an accomplice or change appearance).
   System may instill a false sense of security, lessening overall security. Moreover, it involves high costs and inconvenience.

Huge improvements thanks to advances in Machine Learning.

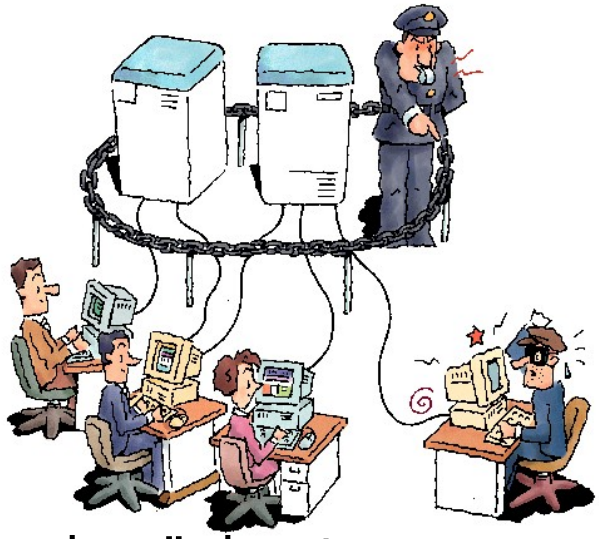
Towards a risk-minimization process

- The risk minimization approach is well established in practice and has an associated process, involving some quantitative or qualitative variant of above.
- Process is also iterative as both vulnerabilities and mechanisms change over time.
- There a number of standard references useful for guiding this. E.g., ISO 17799 (code of practice of Information Security Management).
- Learning risk analysis is an important part of security education.
  - Represents “best practice” as opposed to “best science”.
  - But security in practice is often the sum of many little details

Summary: goals, threats, and mechanisms

- Two different views of security.
  1. Minimizing the risk of abuse.
  2. Building a system that meets a specification.
- In practice, risk minimization is most commonly taken approach.
- Formal approaches are gaining popularity for small to mid-sized technical systems as well as for critical applications.
- There are numerous challenging topics for research and education under both views.

Summary: goals, threats, and mechanisms (cont.)

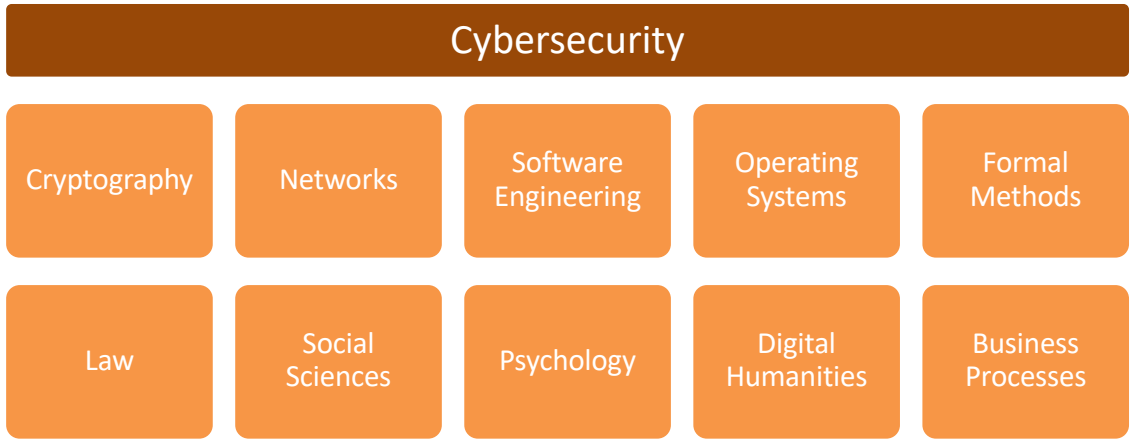


- Standard breakdown. Important for analyzing system security relative to a policy.
- Designing adequate mechanisms is challenging and careful "screening" is not enough.
- History is full of examples of "security breaches" due to poor "security screening".

Table of contents I

Conclusions

- Security is an enabling technology.
- Security is power! E.g., in e-government:
  IT (information technology) processes are used to model and realize government processes. The ability to access and modify data/processes is equal to the ability spy on the most private details of government and its citizens as well as to change the working of the government itself!
- Security is multi-disciplinary



and therein lies, in part, the challenge, excitement, and reward!