Introduction to the security of ICT systems

Antonio Lioy

< lioy @ polito.it >

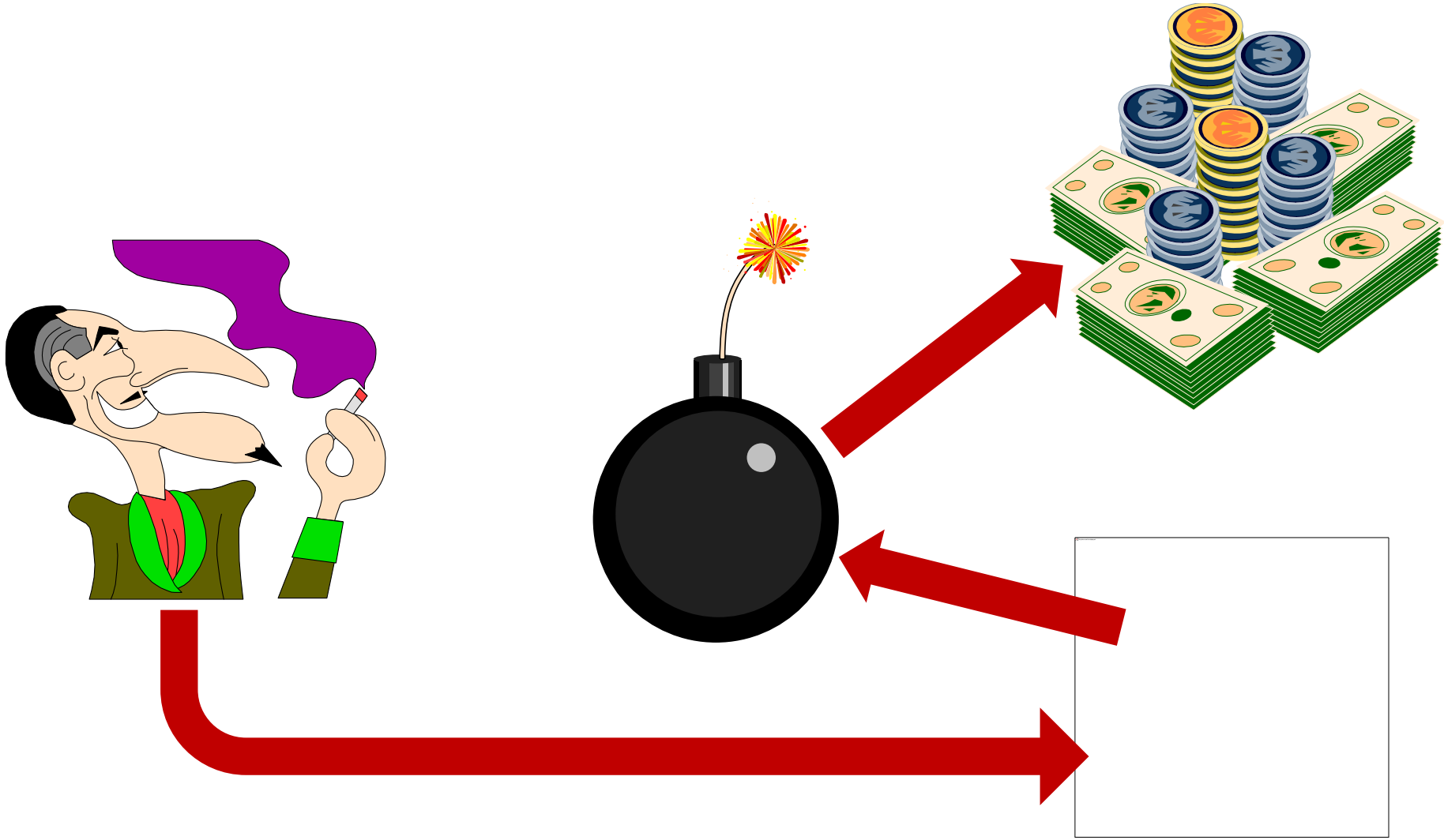
Politecnico di Torino

Dip. Automatica e Informatica

Agenda

- **introduction to information security:**
  - evolution of ICT systems and the security problem
  - problems and vocabulary of ICT security
  - technological attacks (sniffing, spoofing, …)
  - non-technological attacks (social engineering)

Why is security an important issue?



Possible consequence of a successful attack

- **financial loss**
  - direct (e.g. fund transfer)
  - indirect (e.g. value of share, fine by privacy authority)
- **recovery cost**
  - take the system back to normal operations
  - improve the system to avoid new attacks
- **productivity loss**
  - processes are stopped or delayed
- **business disruption**
  - customers may look to alternative suppliers
- **reputation damage**
  - difficult to regain trust

Complexity of the ICT scenario

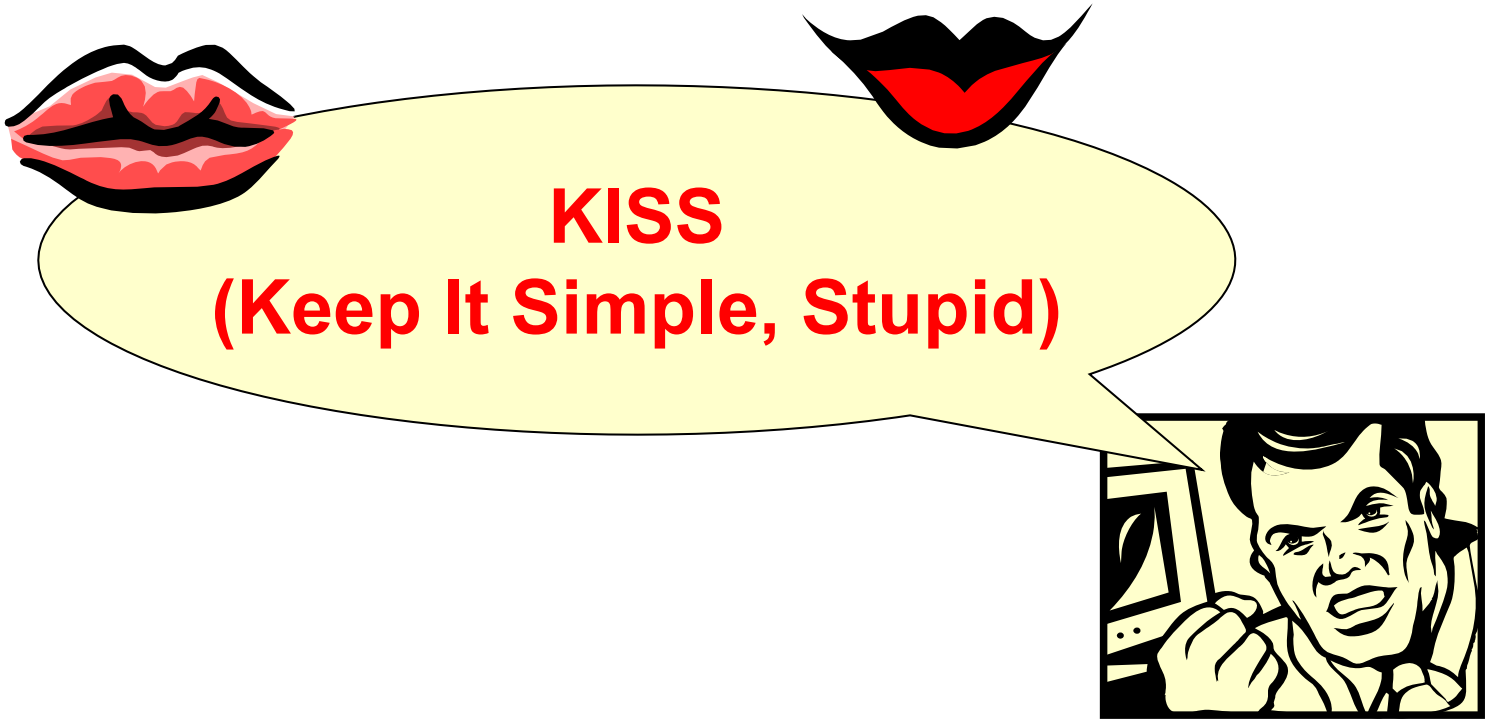
- **"personal" devices**
  - desktop, laptop, tablet, smartphone, …
  - smart TV, fridge, car, …
- **communication networks**
  - data-only networks (no separate analogic phone network)
  - wired and wireless networks
  - mobility
- **distributed services**
  - outsourcing, hosting, farming, cloud, IoT
  - both for the computation functions and the storage ones
- **programming increasingly complex**
  - stratification, framework, language mix, …

Complexity is an enemy of security

FIRST AXIOM OF ENGINEERING
The more complex a system is, the more difficult its correctness verification will be (implementation, management, operation)

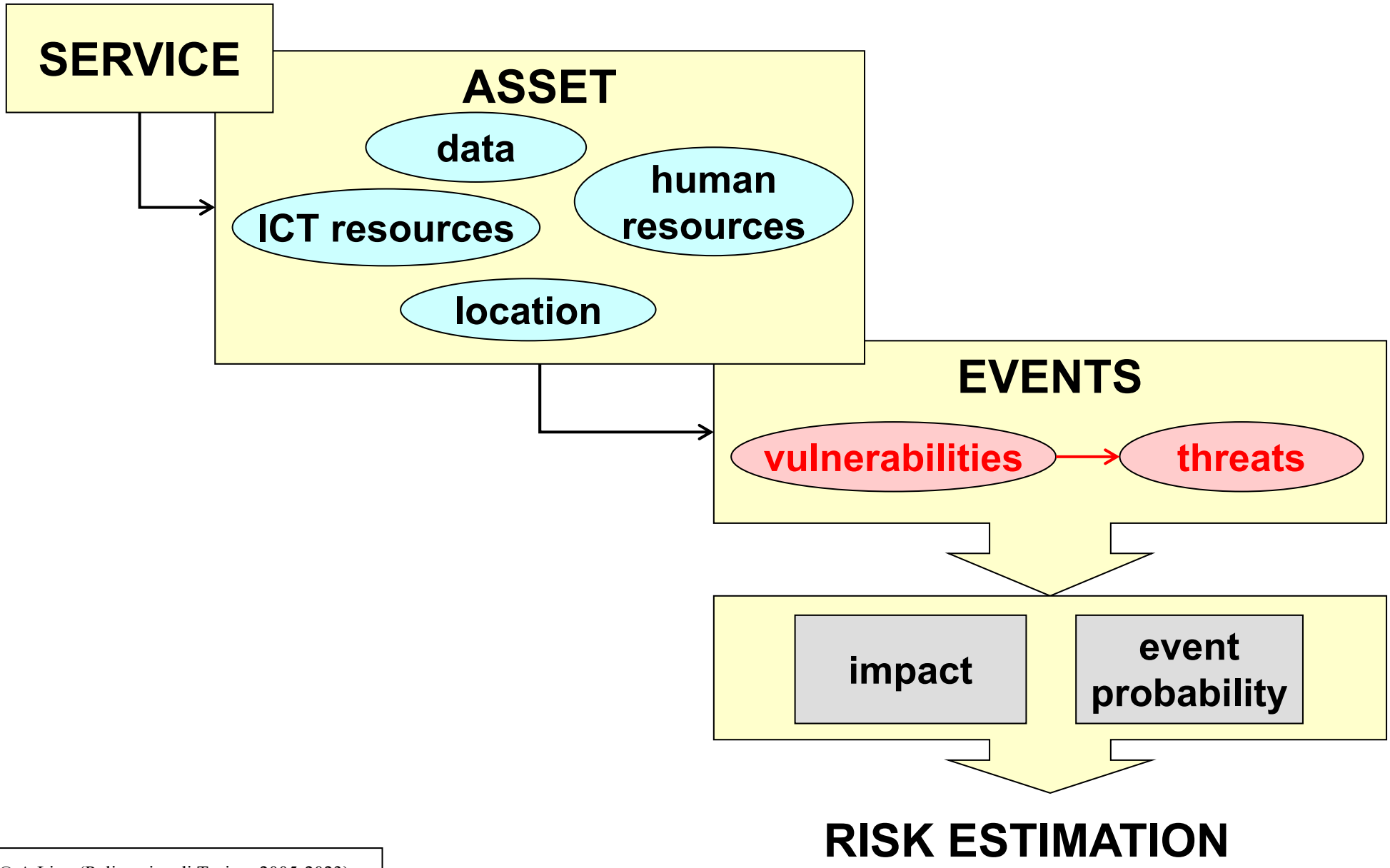
- example: the number of bugs in program is proportional to its number of lines of code
- the complexity of the current information systems is in favour of the attackers that can find attack paths increasingly ingenious and unforeseen by the defenders

The kiss rule



example: software complexity – https://tonsky.me/blog/disenchantment/

Risk estimation



Terms

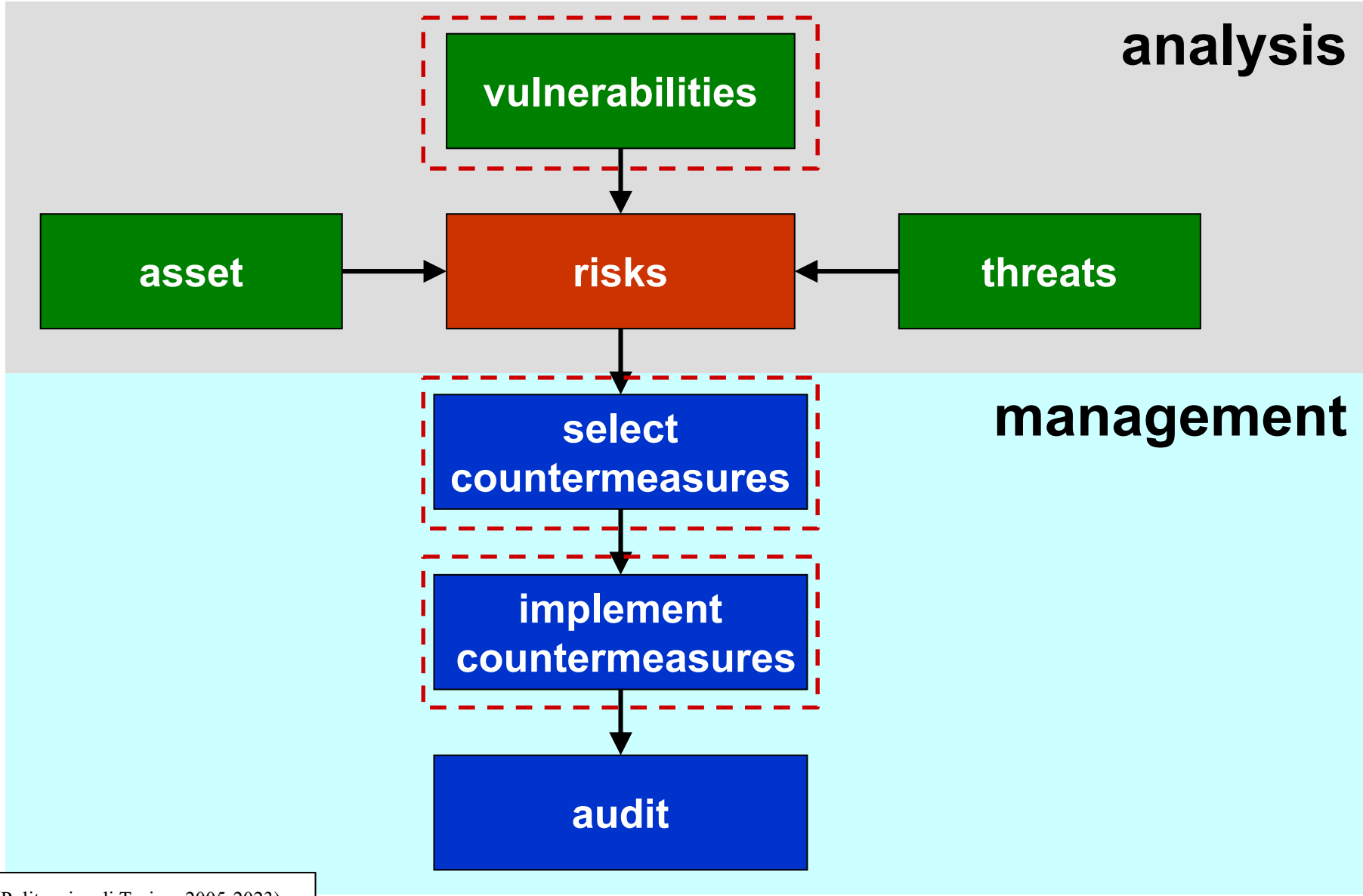
- **ASSET = the set of goods, data, and people needed for an IT service**
- **VULNERABILITY = intrinsic weakness of an asset**
  - e.g. pwd = login; sensible to flooding
- **THREAT = possible deliberate action / accidental event that can produce the loss of a security property by exploiting a vulnerability**
  - it depends upon the specific environment and/or operating conditions
- **ATTACK = threat occurrence (deliberate action)**
- **(NEGATIVE) EVENT = threat occurrence (accidental event)**

Risk management

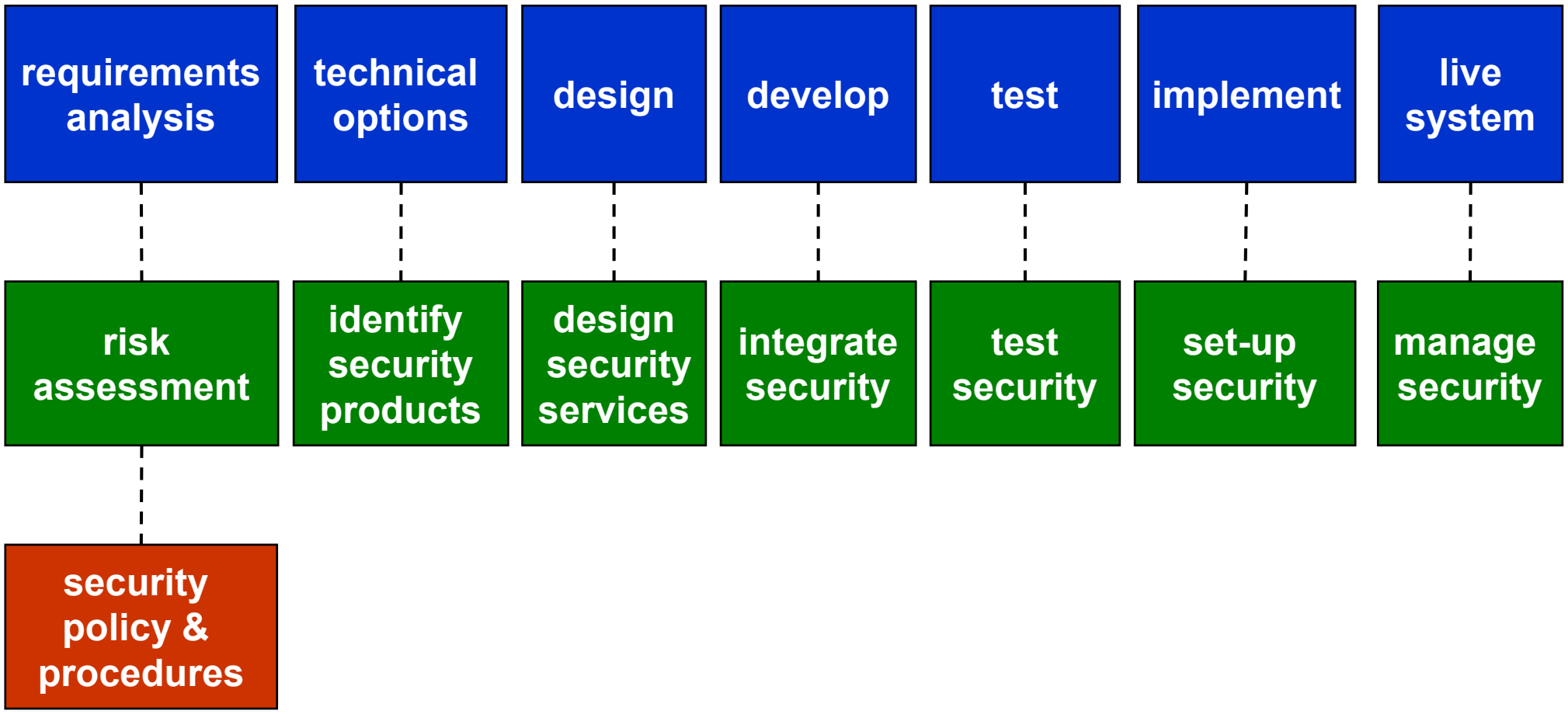
- **(far too) many risks will be identified**
- **need to prioritize them keeping into account not only the impact but also the available time and budget:**
  - address the most important risks (first, then second, then …)
  - … or try to maximize the number of risks covered
- **a risk assessment matrix (or risk heat map) may be useful:**

	improbable (1)	remote (2)	occasional (3)	probable (4)	frequent (5)
catastrophic (5)	5	10	15	20	25
significant (4)	4	8	12	16	20
moderate (3)	3	6	9	12	15
low (2)	2	4	6	8	10
negligible (1)	1	2	3	4	5

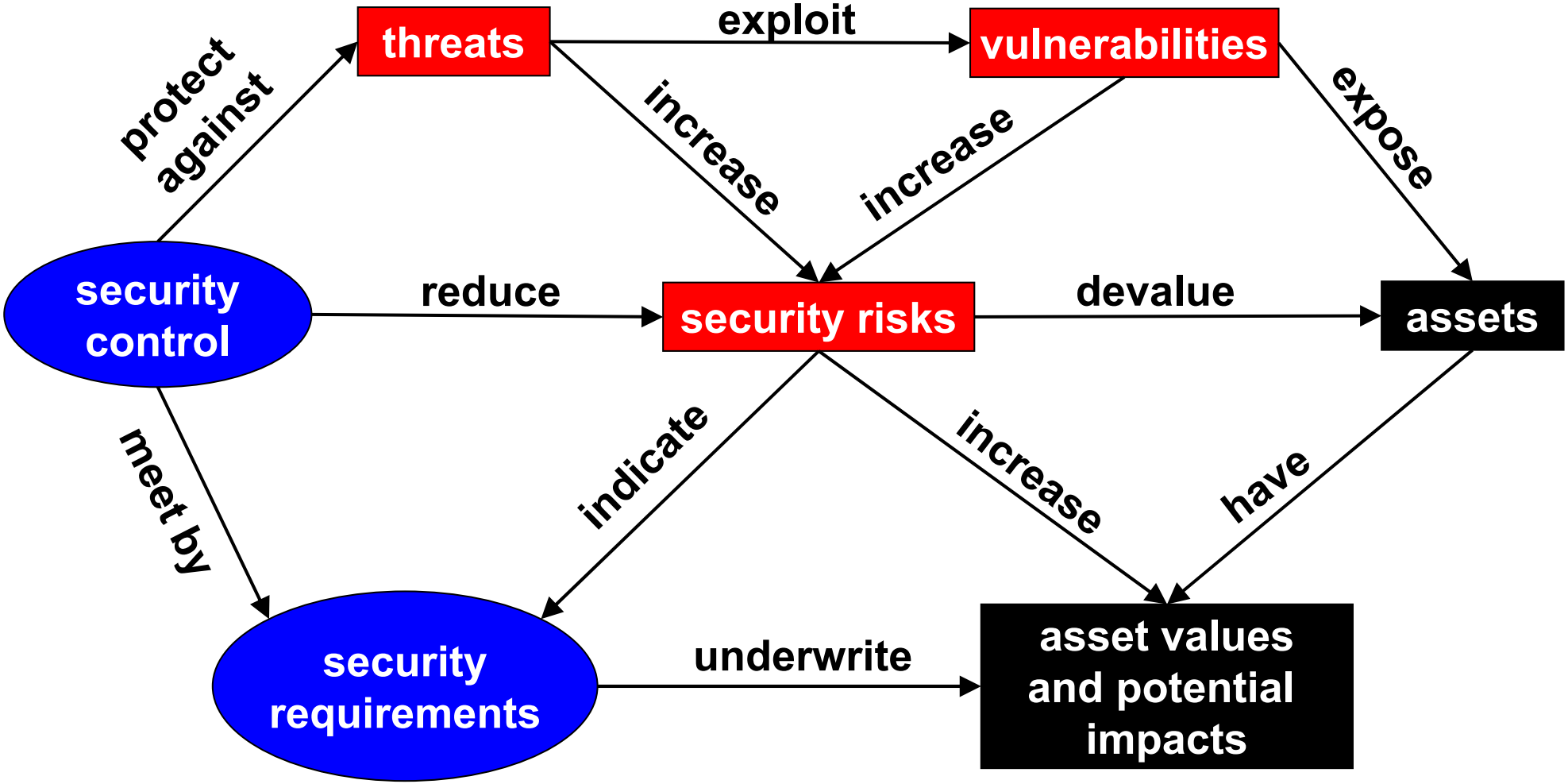
Analysis and management of security



Security in the lifecycle of a system



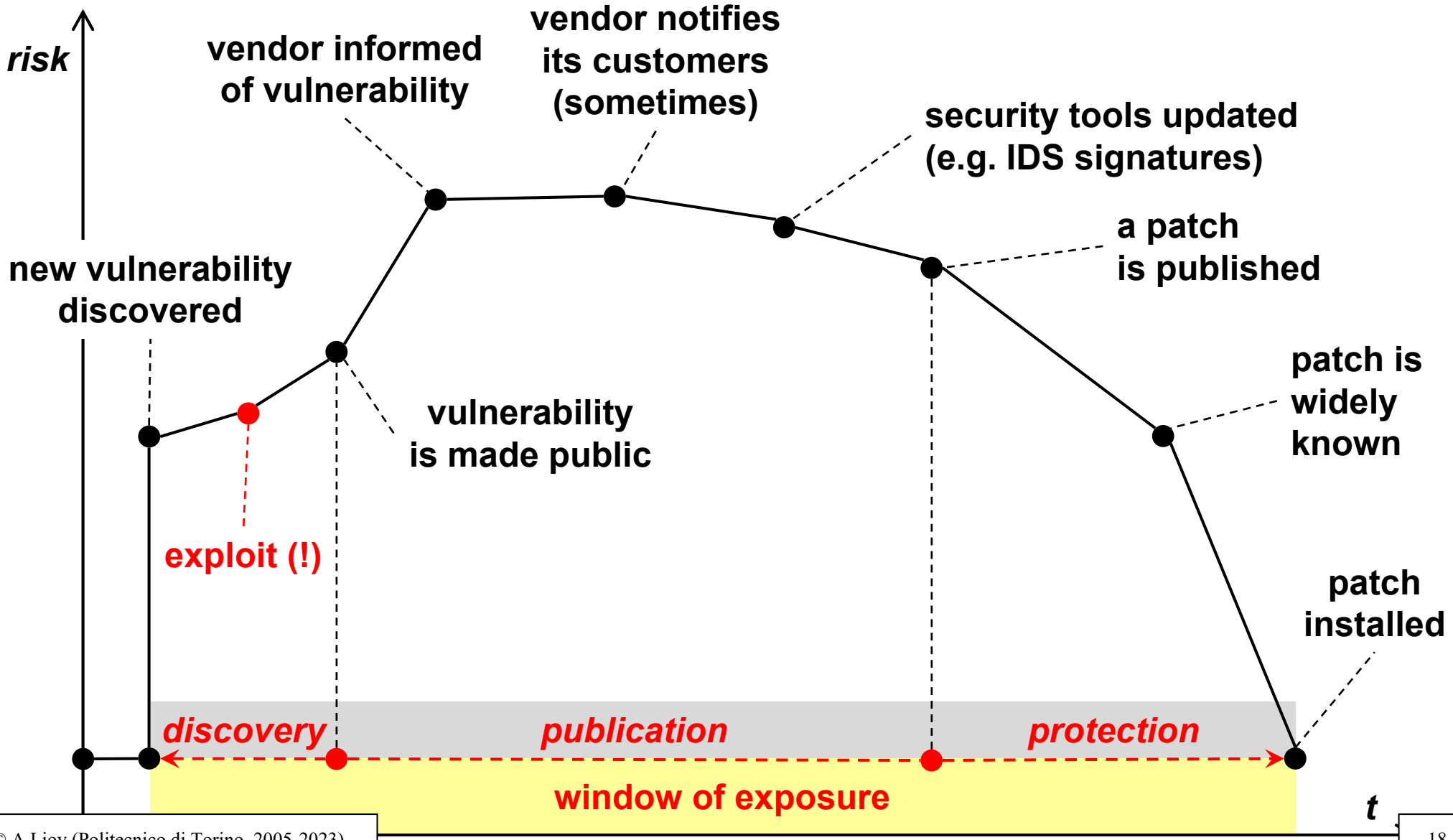
Relations in the security field



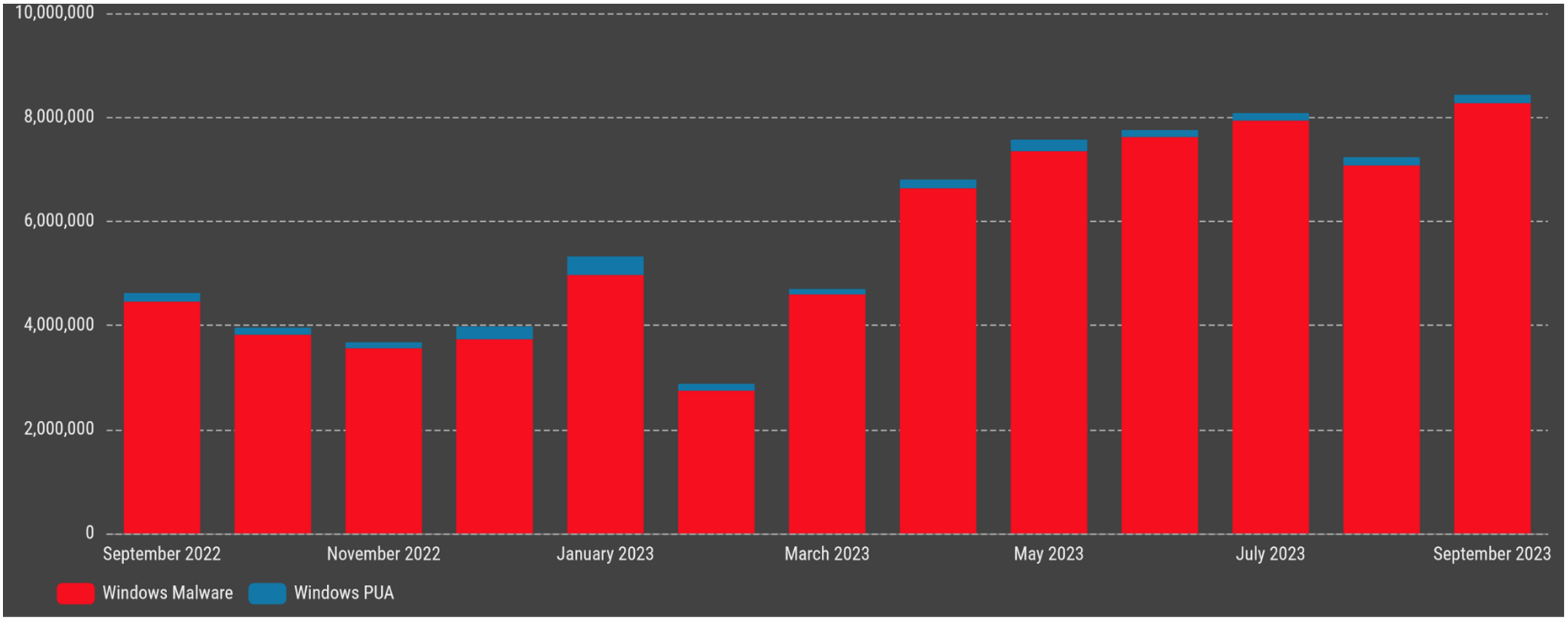
Some terminology

- **incident**
  - a security event that compromises the integrity, confidentiality, or availability of an information asset
- **(data) breach**
  - an incident that results in the disclosure or potential exposure of data
- **(data) disclosure**
  - a breach for which it was confirmed that data was actually disclosed (not just exposed) to an unauthorized party

Window of exposure

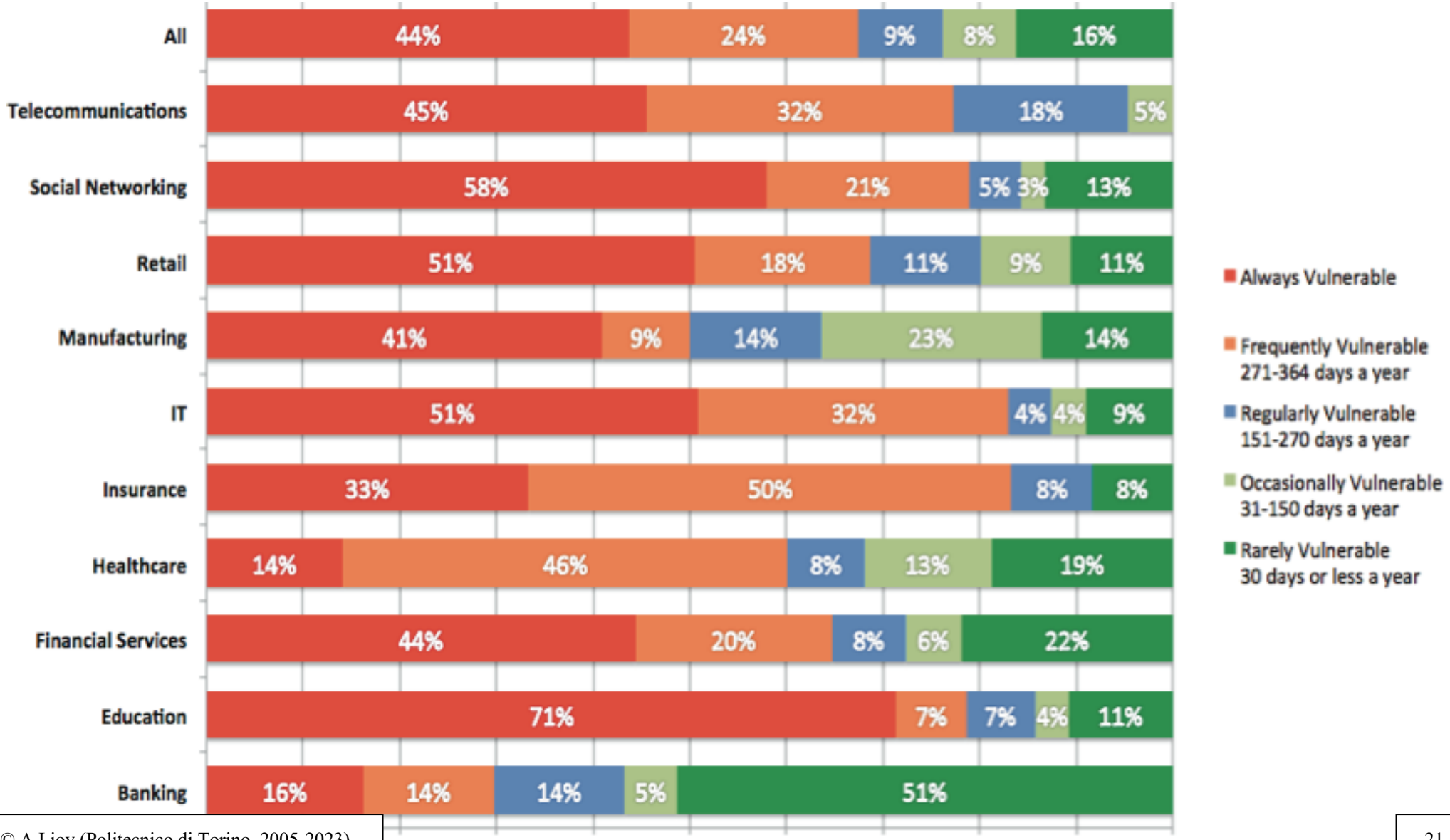


State of the art: new attacks (malware)



www.av-test.org
30.9.2023

WOE: server web (2010)

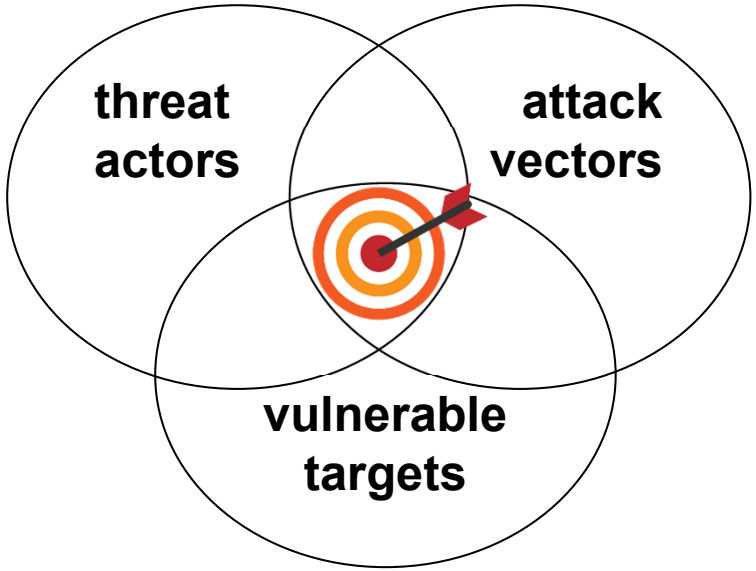


WOE: responsible disclosure

- **an example: https://www.zerodayinitiative.com/advisories/ZDI-18-1075/**
- **This vulnerability is being disclosed publicly without a patch in accordance with the ZDI 120 day deadline:**
  - 8-may-18, ZDI reported the vulnerability to the vendor and the vendor acknowledged the report
  - 14-may-18 the vendor replied that they successfully reproduced the issue ZDI reported
  - 9-sep-18, the vendor reported an issue with the fix and that the fix might not make the September release
  - 10-sep-18, ZDI cautioned potential 0-day
  - 11-sep-18, the vendor confirmed the fix did not make the build
  - 12-sep-18, ZDI confirmed the intention to 0-day on 20-sep-18

Cyber threats schema

- **three main components**
  - threat actors (and their motivation)
  - attack vectors (vulnerabilities and context)
  - vulnerable targets (value for owner and attacker)

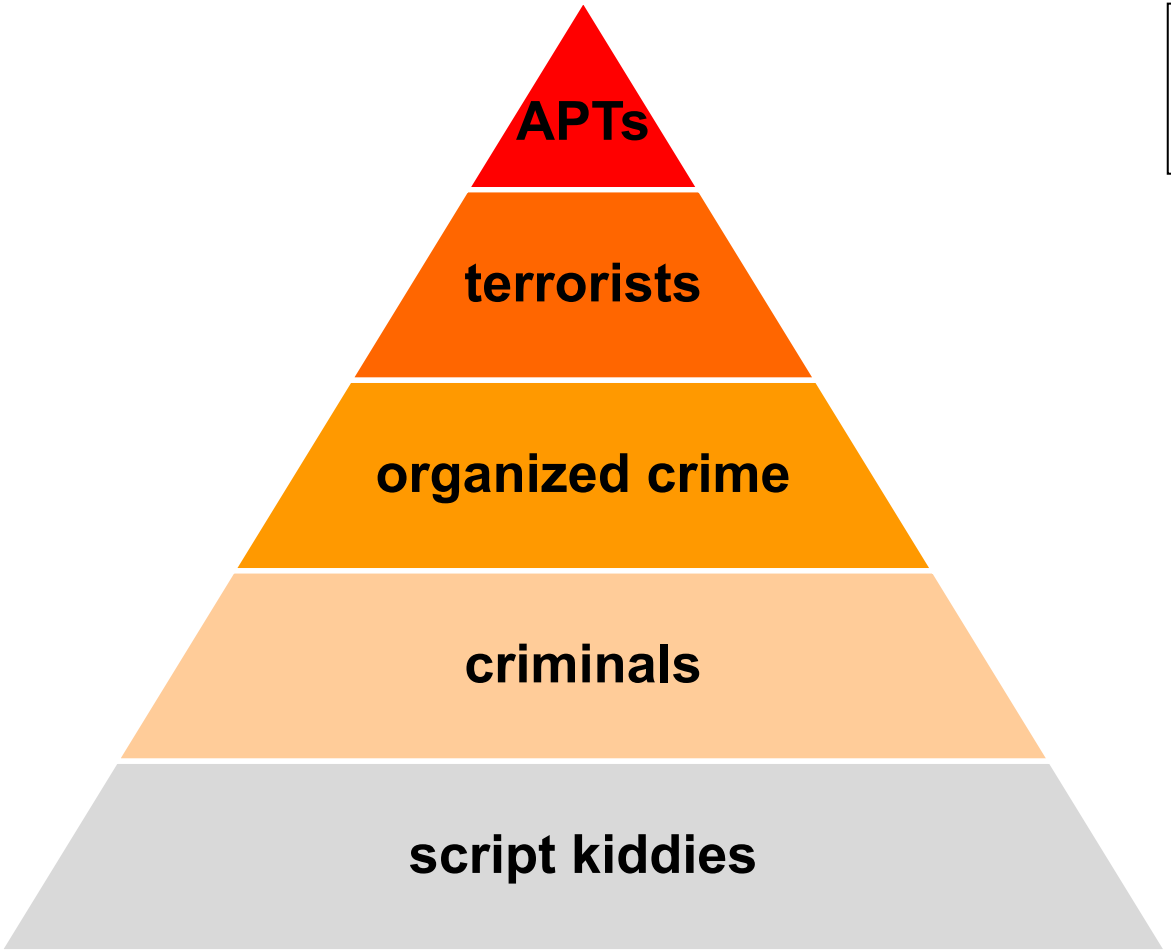


Motivations: MICE

- **M is for MONEY**
  - direct transfer, blackmail, … or indirect (e.g. data reselling)
- **I is for IDEOLOGY**
  - political, religious, hacktivism, …
- **C is for COMPROMISE**
  - individuals with no choice due to blackmail or threat against their families or themselves
- **E is for EGO**
  - "we do it because we can"
  - bragging around and positive reputation

Cyber threats: threat actors

- many actors and motivations



Advanced Persistent Threats (nation-state, stealthy, …)	
disrupt and/or intelligence for physical attacks	
profit, for themselves or others (CaaS – Crime-as-a-Service)	
profit (direct / indirect)	
fun (and bragging)	

(Cybersecurity) Standardization bodies (I)

- **ISO (International Organization for Standardization)**
- **ITU-T (International Telecommunication Union, Telecommunication standardization sector)**

- **ISOC (Internet Society)**
  - IETF (Internet Engineering Task Force)
  - IRTF (Internet Research Task Force)

- **NIST (National Institute of Standards & Technology)**
- **ANSI (American National Standards Institute)**

(Cybersecurity) Standardization bodies (II)

- **ETSI (European Telecommunications Standards Institute)**
- **CEN (European Committee for Standardization)**
- **CENELEC (European Committee for Electrotechnical Standardization)**

- **BSI (British Standards Institution)**
- **UNI = Italian national body for standards (unification)**
  - UNINFO = UNI body for information technologies and their applications

- **generically named SDO (Standards Developing Organization), or SSO (Standards Setting Organization)**

What is security?

Security is a process, not a product

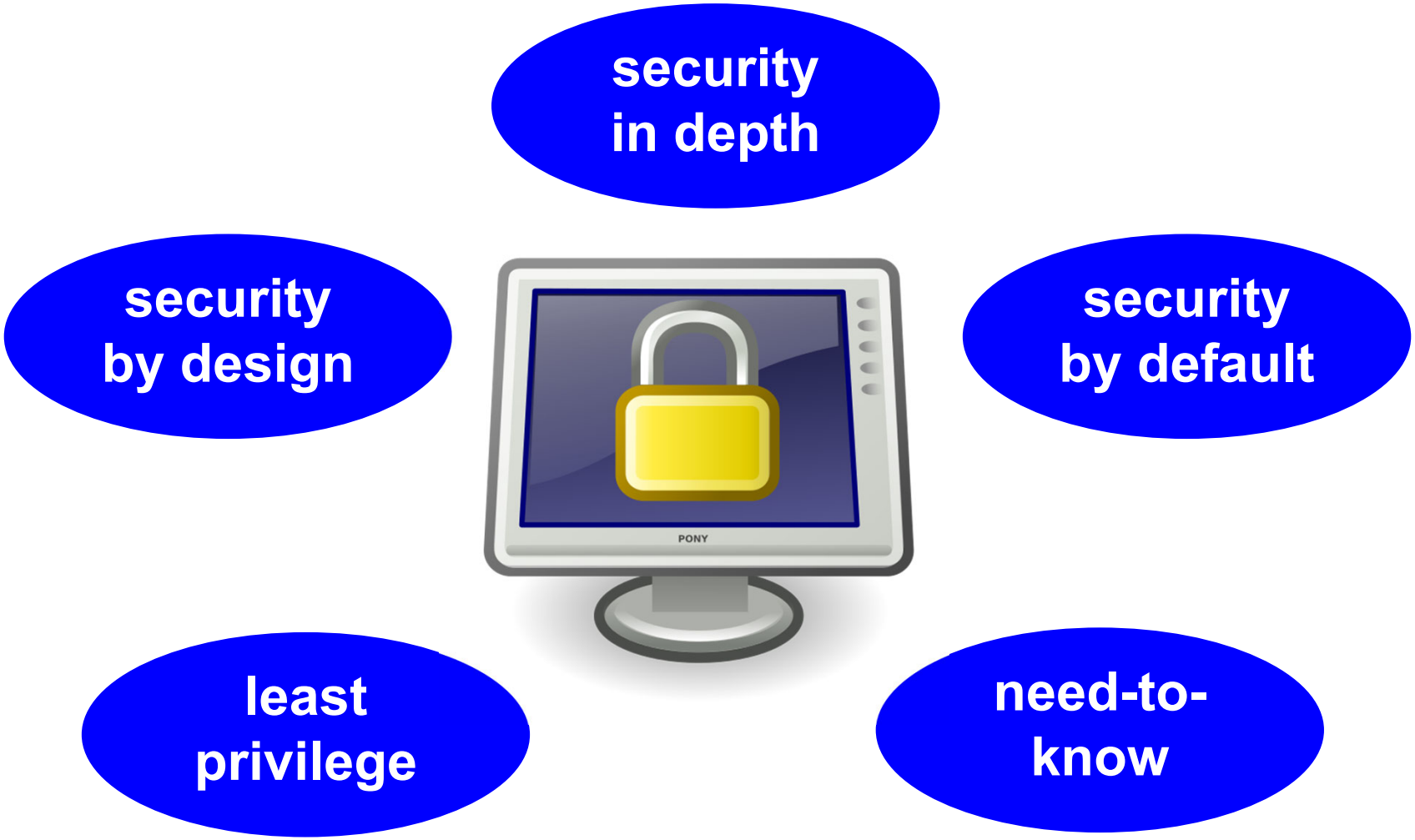
(Bruce Schneier, Crypto-Gram, May 2005)

Computer Security: Will We Ever Learn?

If we've learned anything from the past couple of years, it's that **computer security flaws are inevitable**. Systems break, vulnerabilities are reported in the press, and still many people put their faith in the next product, or the next upgrade, or the next patch. "This time it's secure," they say. So far, it hasn't been.

Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. **The trick is to reduce your risk of exposure regardless of the products or patches**.

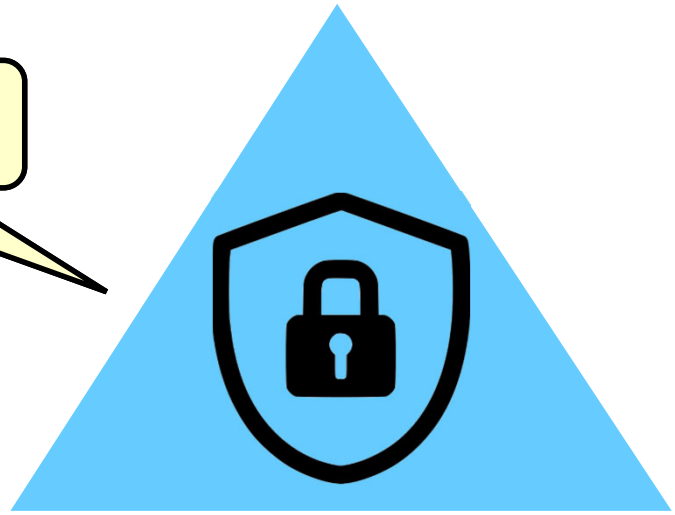
Some security principles



Security and C.I.A.

NO, not this one

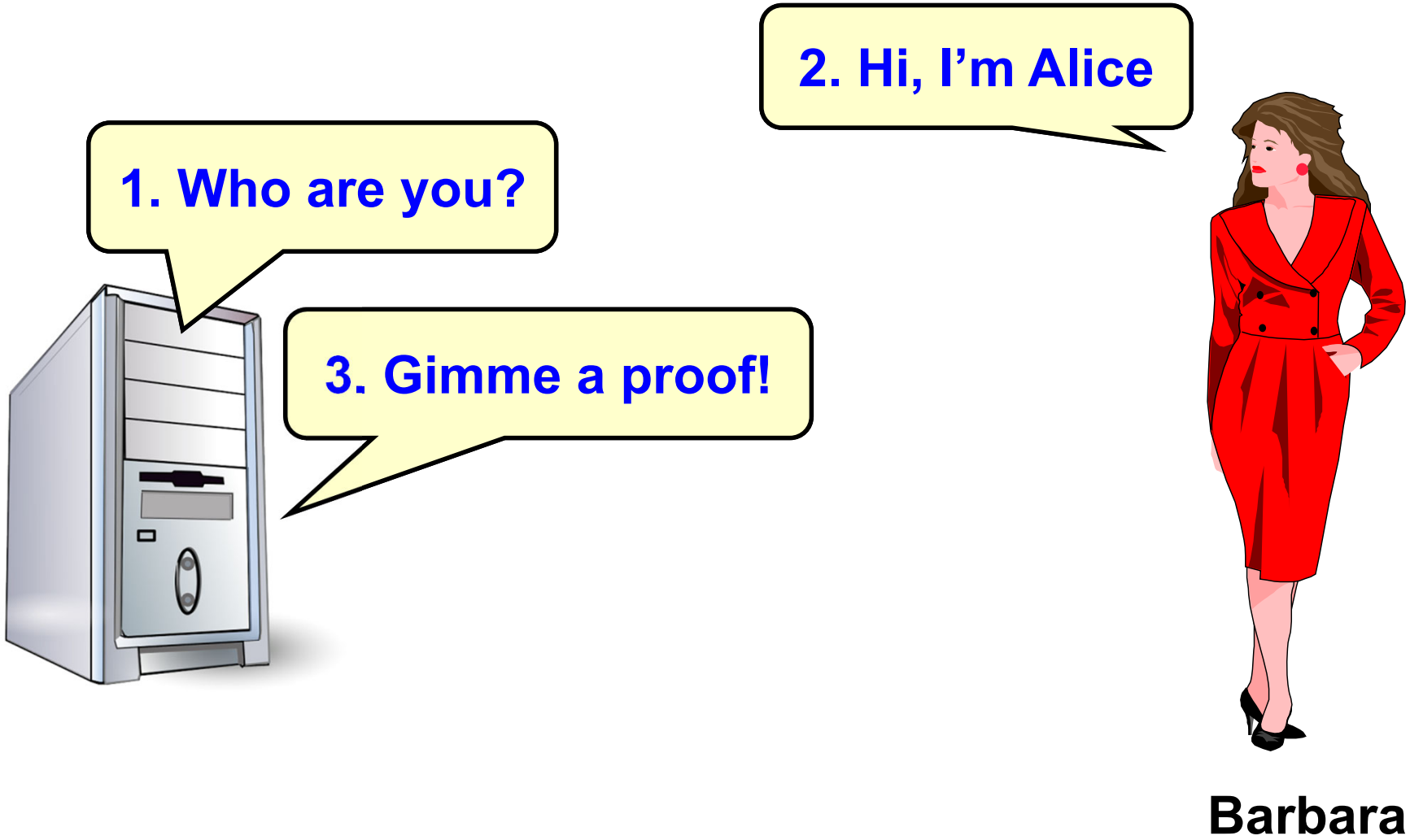
YEP, this one



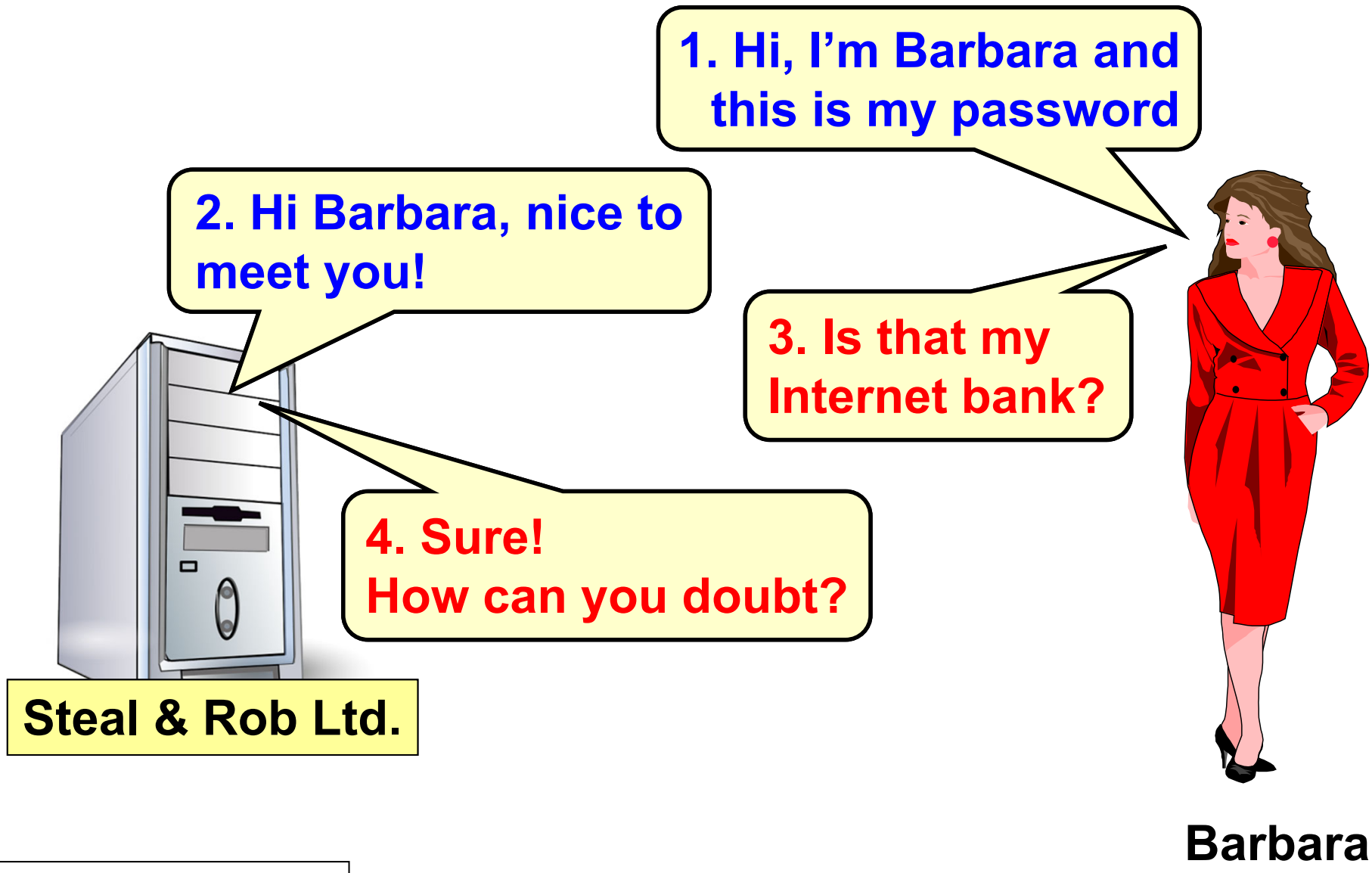
(abstract) security properties / services

autenticazione (semplice / mutua)	*(simple / mutual) authentication*
autenticazione (della controparte)	*(peer) authentication*
autenticazione (dei dati)	*(data / origin) authentication*
autorizzazione, controllo accessi	*authorization,* *access control*
integrità	*integrity*
riservatezza, confidenzialità	*confidentiality, privacy, secrecy*
non ripudio	*non-repudiation*
disponibilità	*availability*
tracciabilità	*traceability, accountability*

Peer authentication (single)



Peer authentication (mutual)



Data origin authentication

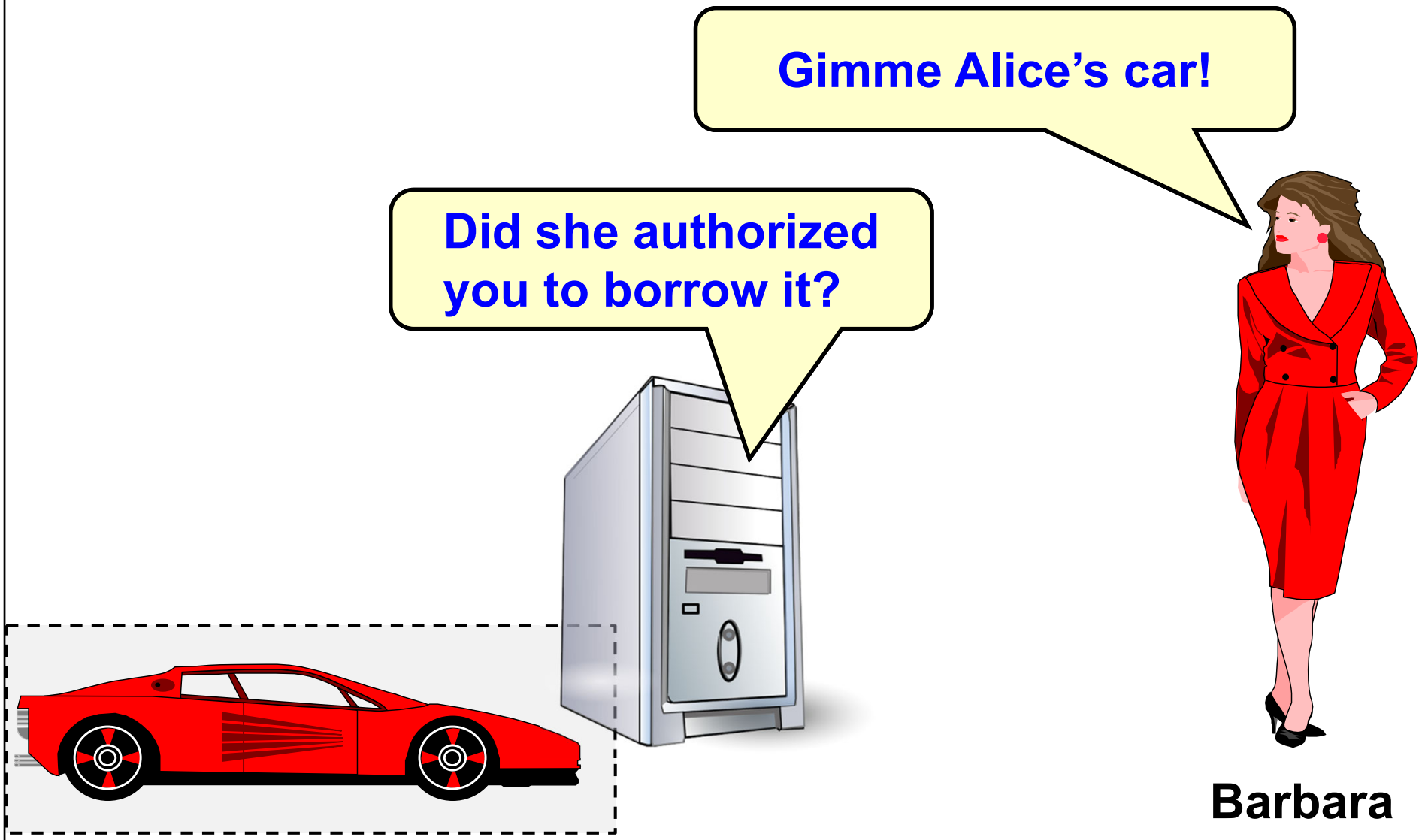
Increase by 30% the salary of Prof. Lioy

The Rector

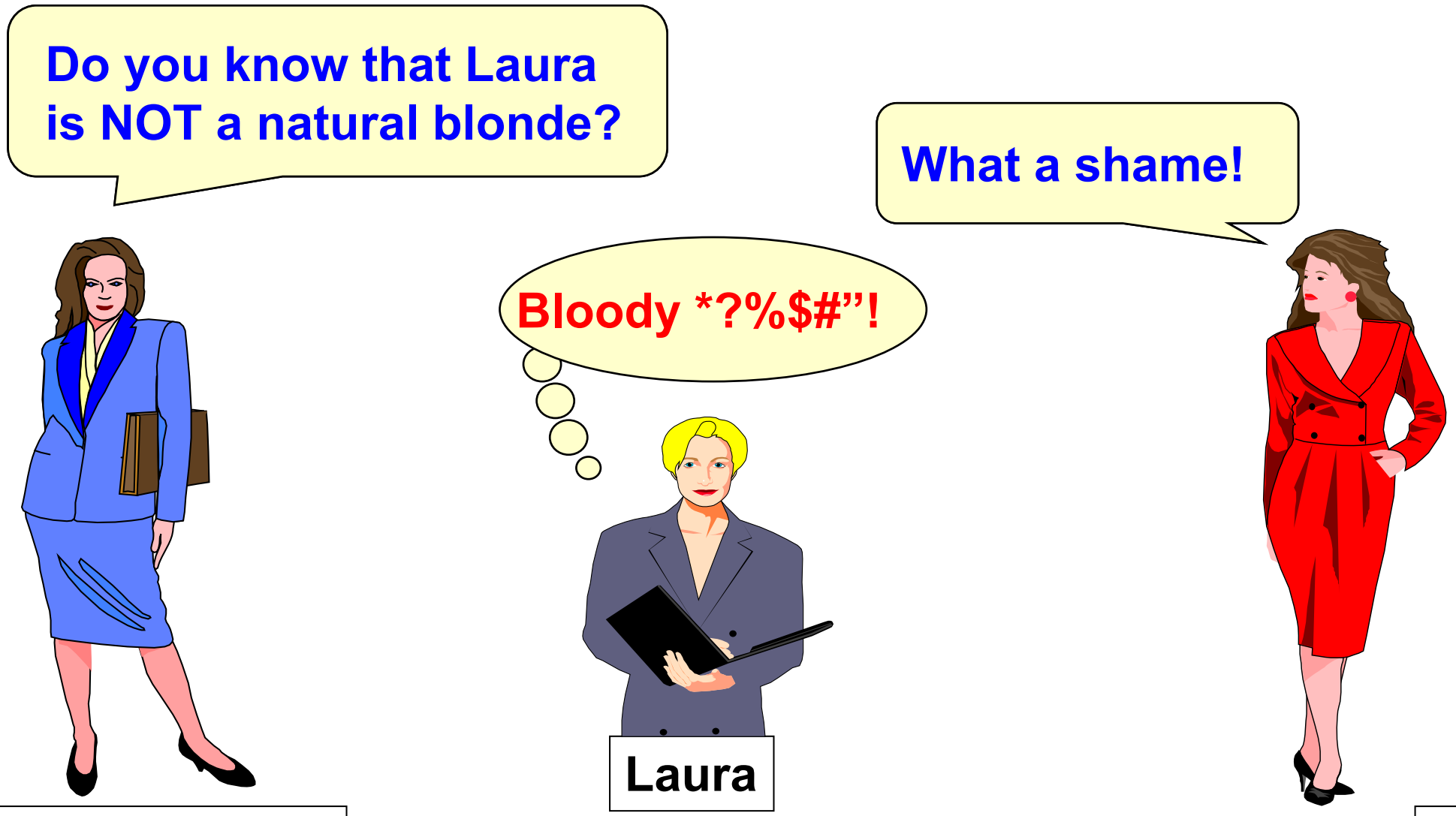
Non-repudiation

- **formal proof – acceptable by a court of justice – that gives undeniable evidence of the data creator**
- **several facets:**
  - (sender/author) authentication
  - integrity
  - (sender/author) identification
  - . . .
- **beware!**
  - normally associated not only to technical aspects but also to a specific procedures performed voluntarily
  - we (almost) never have non-repudiation with protocols or procedures that perform automatic actions on user's behalf

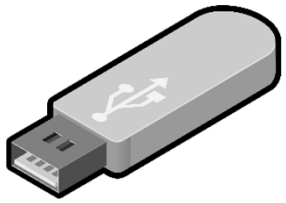
Authorization (access control)



Privacy (communication)



Privacy (data, actions, position)



www.p***hub.com

black_money.xls

Torino, cell 2455

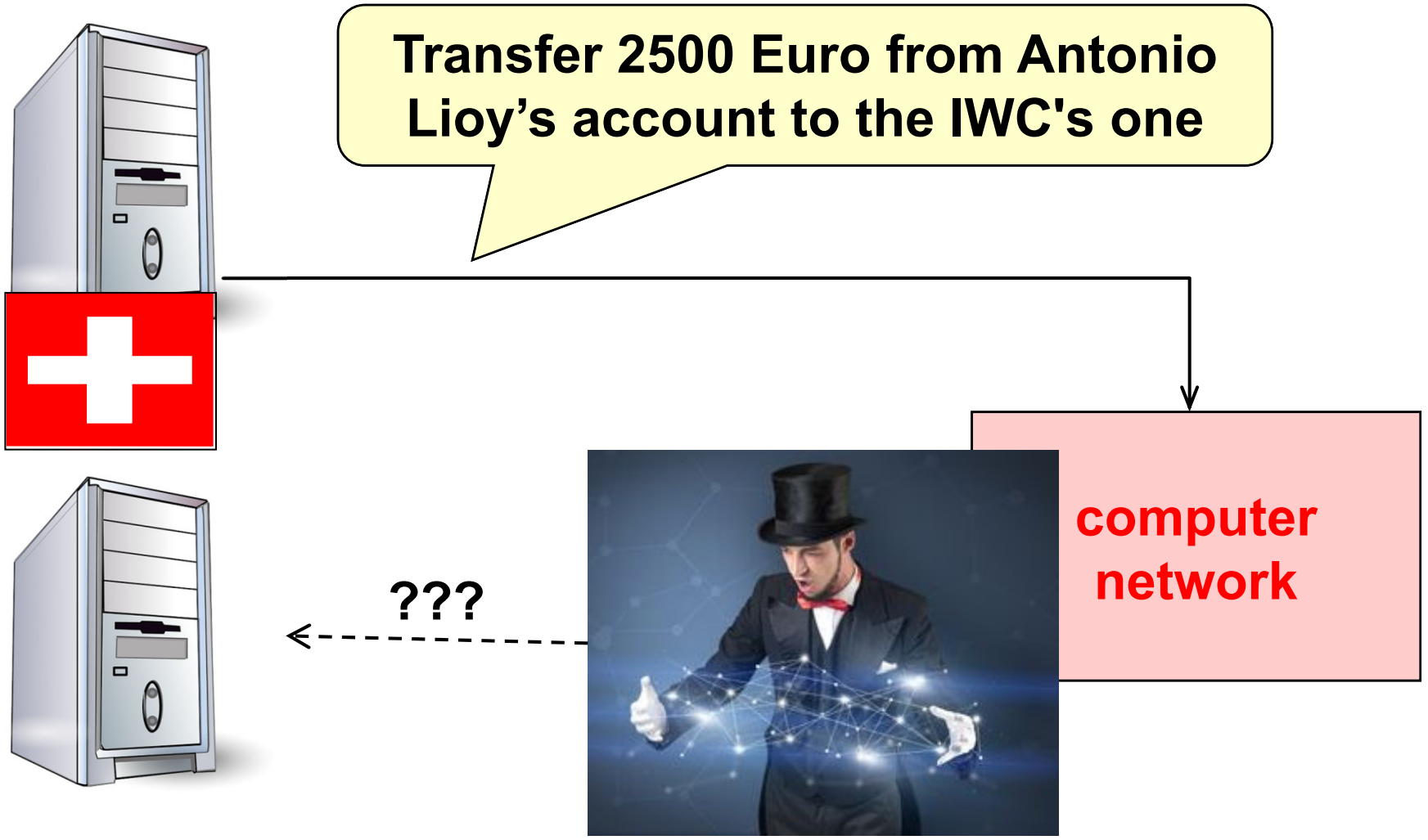
Integrity (data modification)

Pay 1,000 Euro
to Antonio Lioy

computer
network

Pay 10,000 Euro
to Antonio Lioy

Integrity (data cancellation/filtering)



Replay attack

Pay 1,000 EURO
to Antonio Lioy

computer
network

Pay 1,000 EURO
to

Pay 1,000 EURO
to

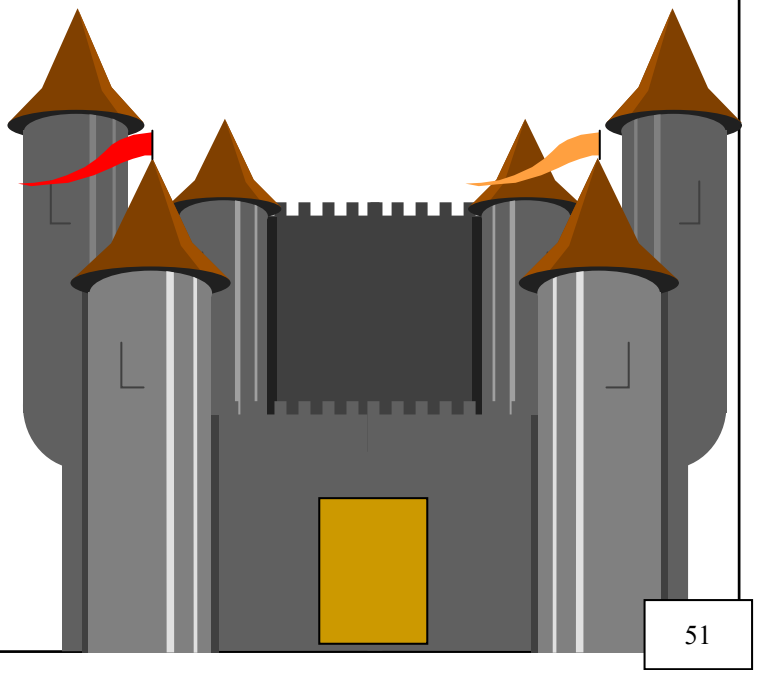
Pay 1,000 EURO
to Antonio Lioy

Data protection

- **for each security property consider always the three cases of data protection:**
  - "data in transit"
    - when data are transmitted over a communication channel
  - "data at rest"
    - when data are stored in a memory device
  - "data at work"
    - when data are in RAM for use by a process

Where is the enemy?

- **outside our organization**
  - boundary / perimeter defence (firewall)
- **outside our organization, with the exception of our partners**
  - Extranet protection (VPN)
- **inside our organization**
  - LAN / Intranet protection (?!)
- **everywhere!**
  - application-level protection
  - data protection
  - in other words … ZTA (Zero Trust Architecture)



Threat model: where is the enemy? which actions can it perform?

- **MITM (Man-In-The-Middle)**
  - sitting between the two peers A and B
- **MATE (Man-At-The-End)**
  - inside one peer
- **MITB (Man-In-The-Browser)**
  - inside one specific component of one peer (typically the web browser)

- **passive attacker**
  - can only read the data / traffic
- **active attacker**
  - can read but also modify, delete, or create data / traffic

Stolen laptop / smartphone

- not only an economic loss to replace the stolen device …
- but also the loss of data that become unavailable (backup?) …
- or the spreading of restricted information

Scoop of a Global Post reporter in the town between Pakistan and Afghanistan

US PCs sold at the Peshàwar market

Computers of the US army with restricted data sold for 650$ along the road where Nato troops are attacked by the talebans. … Still full of classified informations, such as names, sites, and weak points. (corriere.it, 9/2/09)

Basic problems (technological)

- **the networks are insecure:**
  - (most) communications are made in clear
  - LANs operate in broadcast
  - geographical connections are NOT made through end-to-end dedicated lines but:
    - through shared lines
    - through third-party routers
- **weak user authentication (normally password-based)**
- **there is no server authentication**
- **the software contains many bugs!**

Some classes of attacks

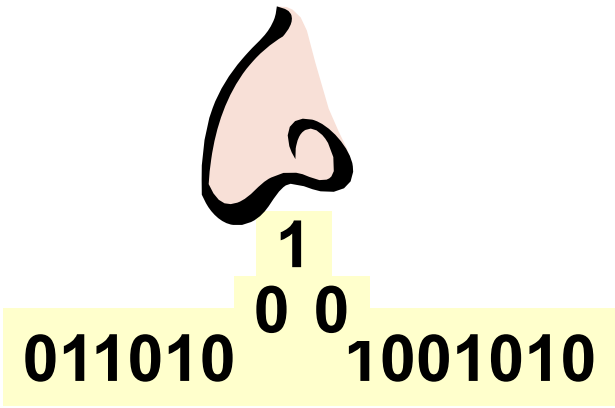
- **IP spoofing / shadow server**
  someone uses the address of another host, to take its place as a client (and hide its own actions) or as a server
- **packet sniffing**
  the content of network packets (e.g. passwords and/or sensitive data) are read by (unauthorized) third parties
- **connection hijacking / data spoofing**
  data inserted / modified / cancelled during their transmission
- **denial-of-service (distributed DoS)**
  the functionality of a service is limited or disrupted (e.g. ping bombing)

IP spoofing (masquerading)

- **forging the source network address**
- **typically the level 3 (IP) address is forged, but it is equally easy to forge the level 2 address (e.g. ETH, TR, ...)**
- **a better name would be *source address spoofing***
- **attacks:**
  - data forging
  - (unauthorized) access to systems
- **countermeasures:**
  - do NEVER use address-based authentication

Packet sniffing (eavesdropping)

- **reading the packets addressed to another network node**
- **easy to do in broadcast networks (e.g. LAN) or at the switching nodes (e.g. router, switch)**
- **attacks:**
  - allows to intercept anything (password, data, ...)
- **countermeasure:**
  - non-broadcast networks (!?)
  - encryption of packet payload



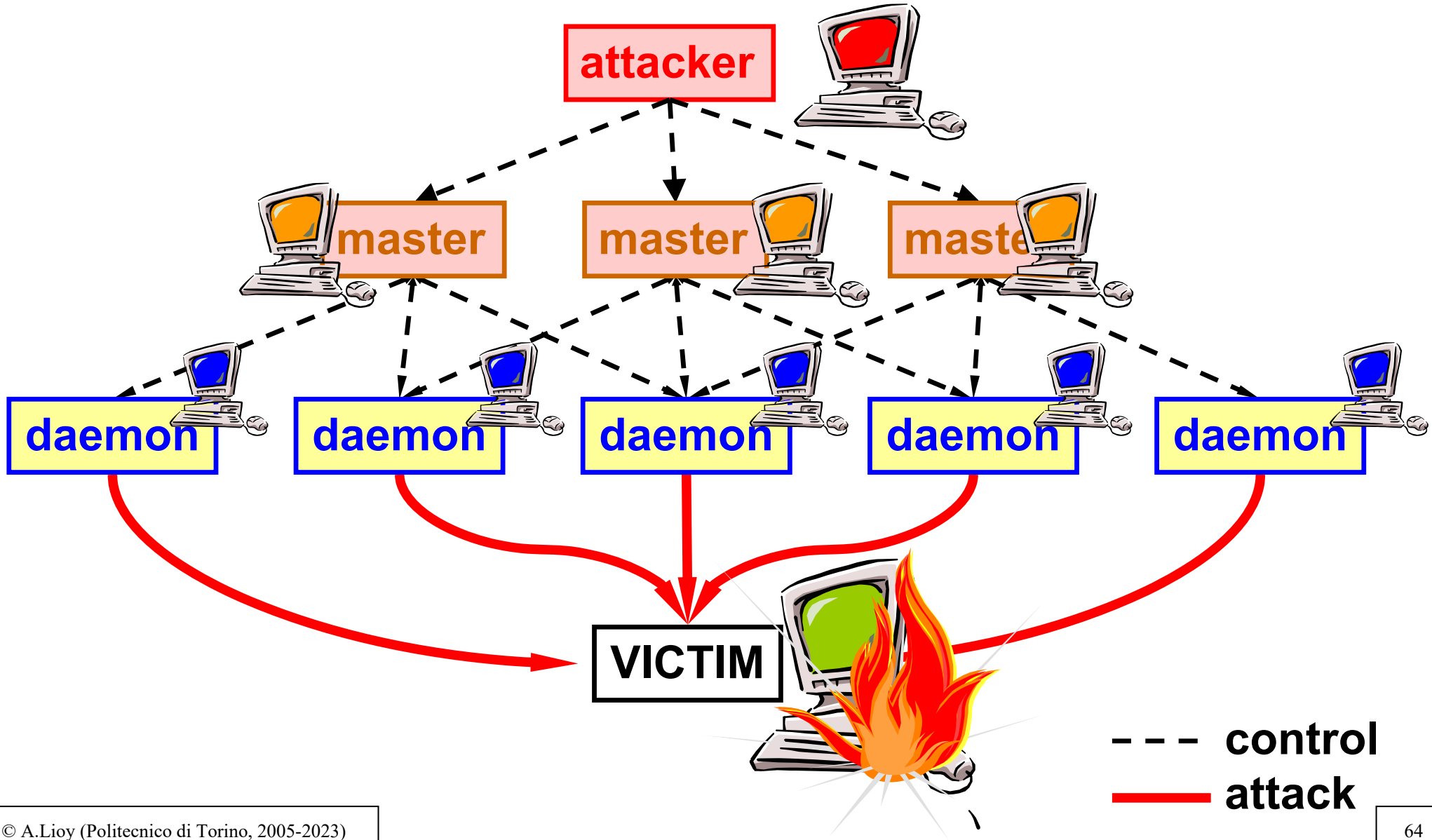
Denial-of-service (DoS)

- **keeping a host busy so that it can't provide its services**
- **examples:**
  - mail / log saturation
  - ping flooding ("ping bombing")
  - SYN attack
- **attacks:**
  - block the use of a system / service
- **countermeasures:**
  - none!
  - monitoring and oversizing can mitigate the effects

Distributed denial-of-service (DDOS)

- **software for DoS installed on many nodes (named daemon, zombie or malbot) to create a Botnet**
- **daemons remotely controlled by a master**
  - C&C (command & control) infrastructure
  - C/S or P2P communications
  - encrypted or "covert" channels (e.g. UDP over ICMP)
  - auto-update capability
- **effect of the base DoS attack multiplied by the number of daemons**

DDoS attack



DDoS: improving the attack

- **use a "reflector"**
  - to hide the attacker's tracks
  - to multiply the attackers (e.g. smurfing, fraggle)
- **use an amplification factor N:1**
  - depends on the attack protocol used,
  - look for a reflector server with |response| >> |request|
  - easy with datagram (e.g. ICMP, UDP) but possible also with stream under certain conditions (e.g. self-attack HTTP)
  - e.g. typical DNS amplification 70:1 but NTP amplification can be 20-200:1

Feb 8th, 2000, 10:30am (PST) @ Yahoo Server Farm

- "the initial flood of packets, which we later realized was in excess of 1G bits/sec, took down one of our routers …"
- "… after the router recovered we lost all routing to our upstream ISP …"
- "… it was somewhat difficult to tell what was going on, but at the very least we noticed lots of ICMP traffic …"
- "… at 1.30pm we got basic routing back up and then realized that we were under a DDoS attack"

- later the attack was traced back to the 15-years old Canadian boy Michael Calce (a.k.a. MafiaBoy)

http://packetstorm.decepticons.org/distributed/yahoo.txt

DDoS towards "Krebs on security" blog

- September 27th, 2016
- 665 Gbps
- botnet of IoT devices (or claiming to be such)
- no use of reflectors or amplification factors, just millions of devices performing perfectly valid requests
- blog protected by Akamai, but on 27/9 it gave up (double of its sustainable traffic) and decided to make the blog unreachable
- unknown reason of the attack, perhaps connected to Krebs' analysis of similar attacks and takedown of the DDoS-for-hire service vDOS, and the arrests of two people founders of the service (POST request attacks included the string “freeapplej4ck,” the nickname of one vDOS co-owners)

Shadow / fake server

- **host that manages to show itself (to victims) as a service provider without having the right to do so**
- **techniques:**
  - request sniffing and response spoofing (difficult: shadow server must be faster than the real one, or this one must be unable to respond, e.g. due to DDoS)
  - wrong mapping (easy: routing or DNS manipulation)
- **attacks:**
  - issue wrong answers, providing thus a “wrong” service to victims instead of the real one
  - capture victim’s data provided to the wrong service
- **countermeasures:**
  - server authentication

Connection hijacking / MITM

- **also named *data spoofing***
- **attacker takes control of a communication channel to insert, delete, or manipulate the traffic**
- **logical or physical MITM (Man In The Middle)**
- **attacks:**
  - reading, insertion of false data and modification of data exchanged between two parties
- **countermeasure:**
  - secrecy, authentication, integrity, and serialization of each individual network packet

Trojan

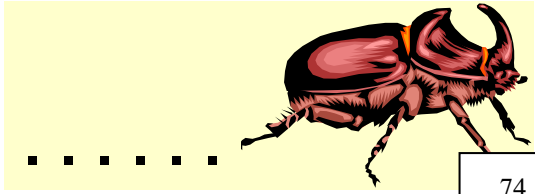
- **Trojan (horse)**
  - program containing a dangerous payload
- **network channels more protected …**
- **… but user terminals less protected**
  - Smartphone, smart-TV, …
  - IoT (Internet-of-Things)
  - "ignorant" users
- **classic attack tools (e.g. keylogger as part of a game) and modern ones (e.g. browser extension)**
- **often used to create a**
  - MATE = Man-At-The-End
  - MITB = Man-In-The-Browser

Zeus

- **also know as Zbot**
- **currently a major malware + botnet**
- **discovered (born?) on 2007, sold (?) on 2010**
- **can be used:**
  - directly
    (e.g. MITB for keylogging or form grabbing)
  - indirectly, to load other malware
    (e.g. the CryptoLocker ransomware)
- **very difficult to discover and remove**
  - hides itself with stealth techniques
  - about 3.6 M active copies just in the USA

Software bug

- **even the best software (either off-the-shelf or custom) contains bugs that can be used for various aims**
- **easiest exploit: DoS**
- **example: WinNT server (3.51, 4.0)**
  - telnet to TCP port 135
  - send 10 random characters, then CR and disconnect
  - server unavailable!
    (100% CPU load even though no useful work is done)
  - http://support.microsoft.com/kb/162567
  - solution: install SP3

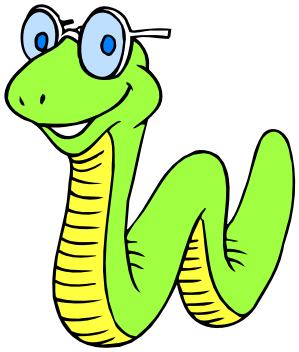


Virus & Co. (malware)

- **virus**
  - damages the target and replicates itself
  - propagated by humans (involuntarily)
- **worm**
  - damages the target by replicating itself (resource saturation)
  - automatic propagation
- **Trojan (horse) = malware vector**
- **backdoor = unauthorized access point**
- **rootkit = privileged access tools, hidden (modified program, library, driver, kernel module, hypervisor) and stealth**
- **PUA (Potentially Unwanted Applications)**
  - it's a sort of grayware, not directly dangerous

Virus and worm (malware)

- **requires complicity (may be involuntary) from:**
  - the user (gratis, free, urgent, important, …)
  - the sys manager (wrong configuration)
  - the producer (automatic execution, trusted, …)
- **countermeasures:**
  - user awareness
  - correct configuration / secure sw
  - install antivirus (and keep updated!)



Malware food chain

business opportunity (vulnerability)

malicious code

vulnerability marketplace

Hall of fame

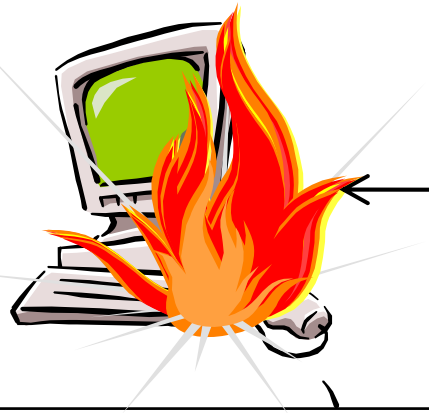
. . .

. . .

bug bounty!

malware toolkit market

VICTIM

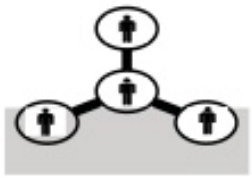


malware distributors (spam, web, …)

Zeus

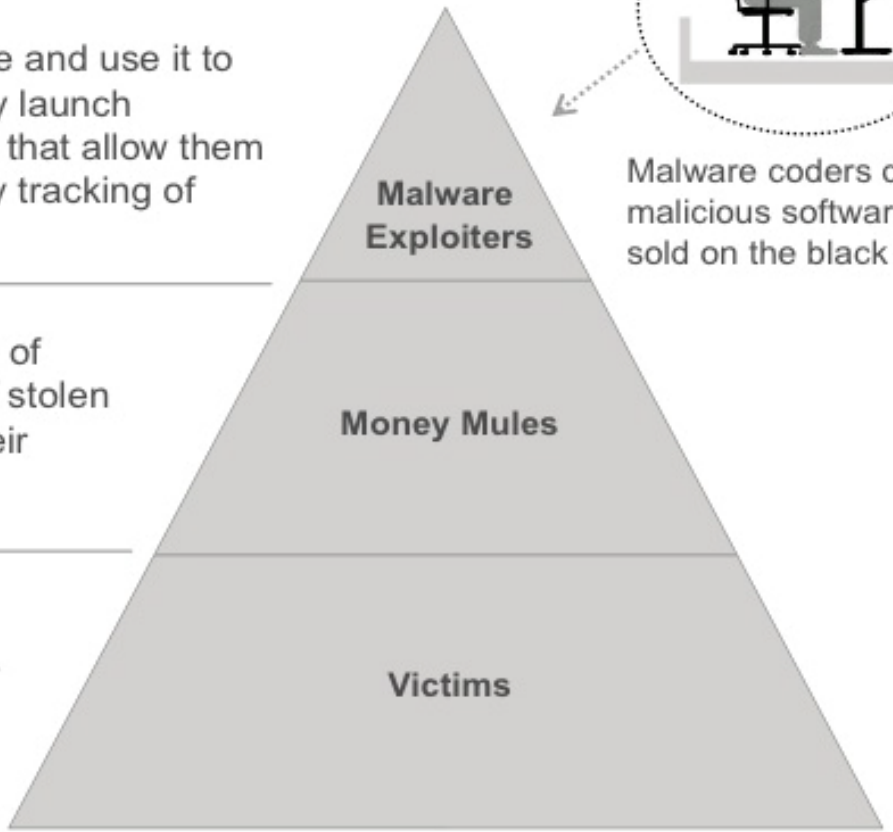
Cyber Theft Ring

Malware exploiters purchase malware and use it to steal victim banking credentials. They launch attacks from compromised machines that allow them to transfer stolen funds and deter any tracking of their activities.

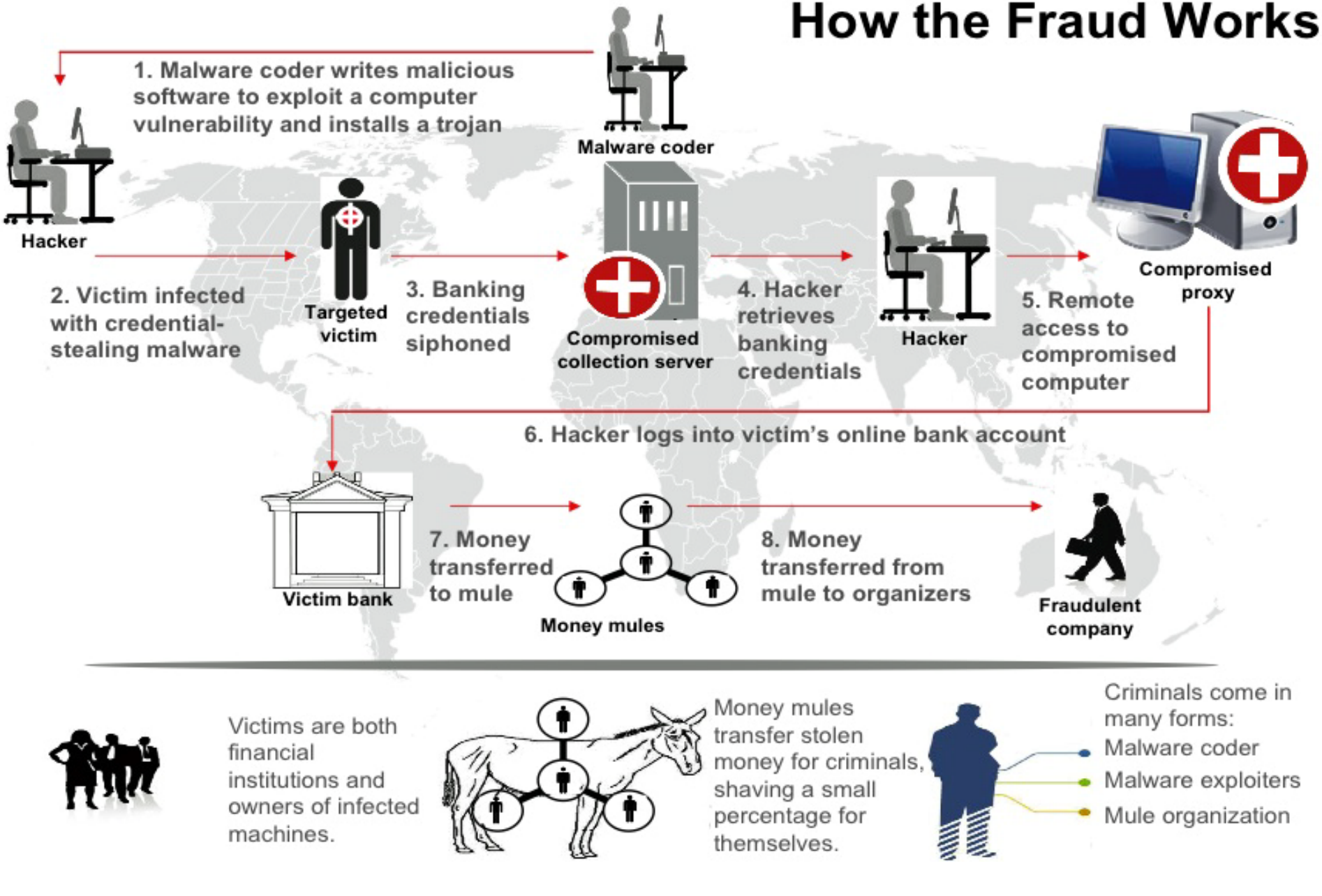


Money mule networks are comprised of individuals engaged in the transfer of stolen funds who retain a percentage for their services.

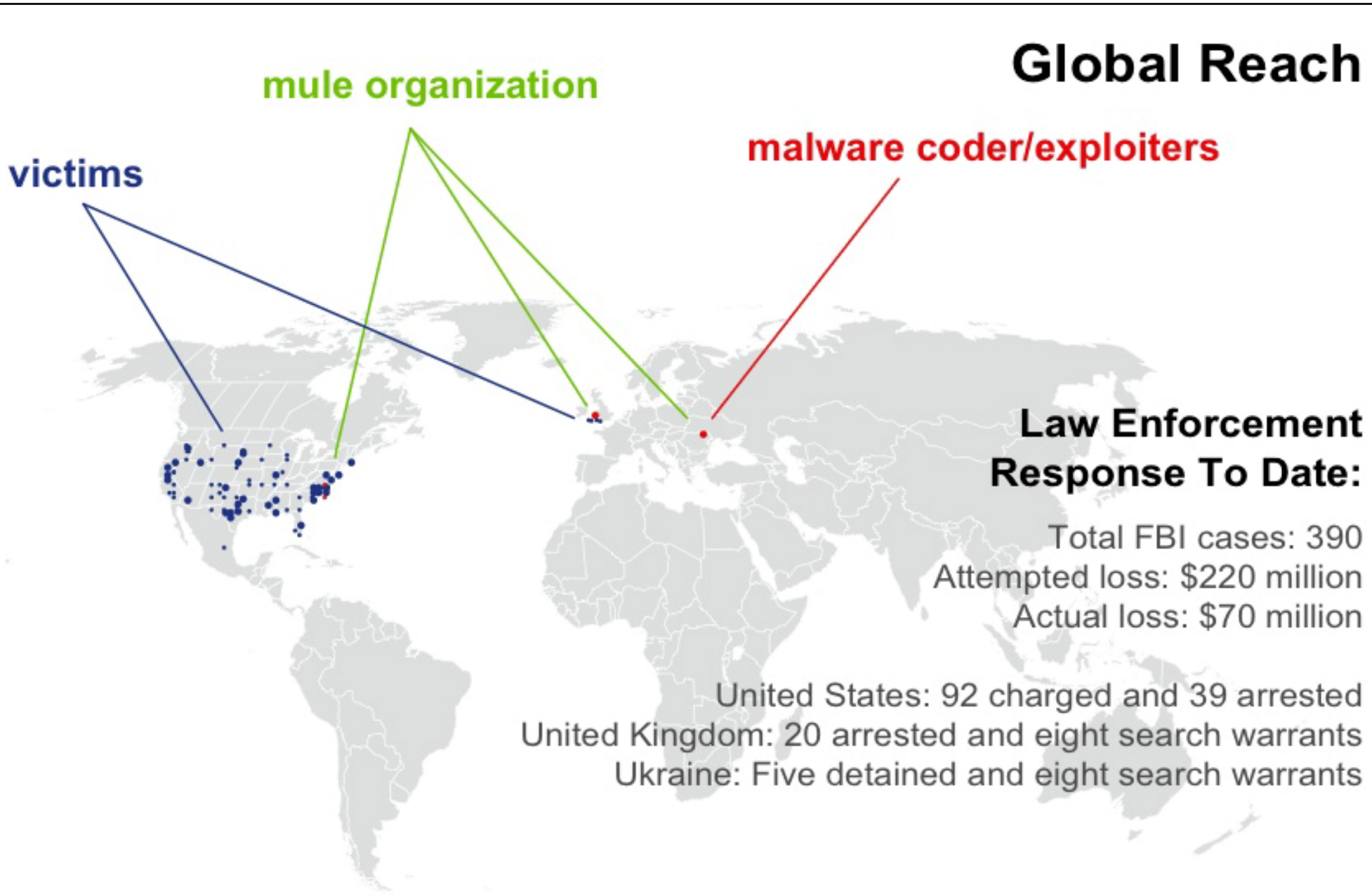
Victims include individuals, businesses, and financial institutions.



source: http://en.wikipedia.org/wiki/File:FBI_Fraud_Scheme_Zeus_Trojan.jpg



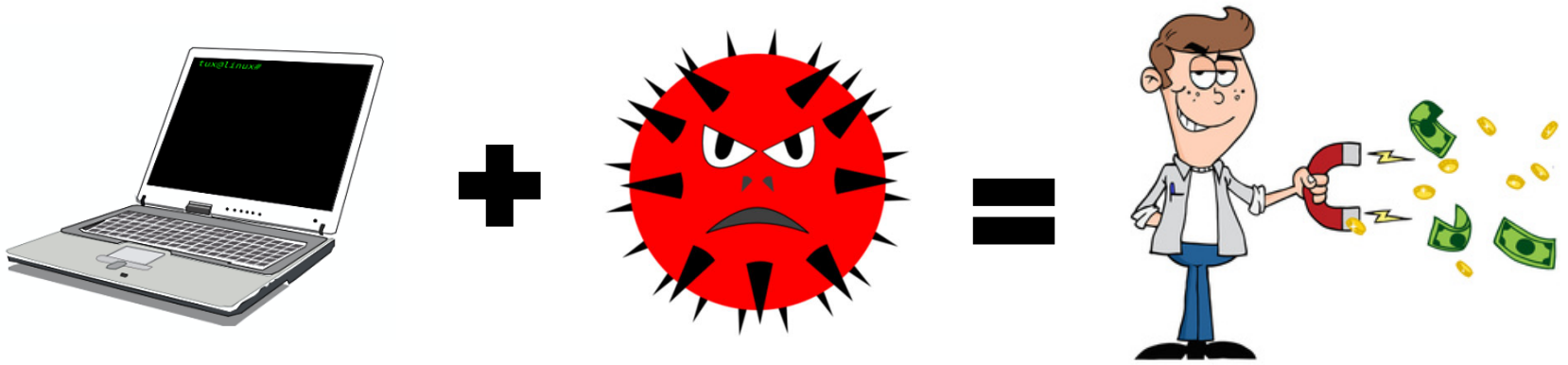
source: http://en.wikipedia.org/wiki/File:FBI_Fraud_Scheme_Zeus_Trojan.jpg



source: http://en.wikipedia.org/wiki/File:FBI_Fraud_Scheme_Zeus_Trojan.jpg

Ransomware

- **ransomware = malware oriented to get a ransom**
  - on desktop and laptop (disk content made unreadable) …
  - … but also for tablet and smartphone (made unusable)
  - unblocked (not always) after paying a certain amount of money



Ransomware-as-a-service

- **TOX malware (server in the TOR anonymous network)**
  - ask for the ransom and handles the payment (with a 20% service fee)
  - the "customer" has only the task to distribute it to the victims
  - fast growth (1000 customers/week, 100 infections/hour)

Ransomware: not only technology but also procedures and organization

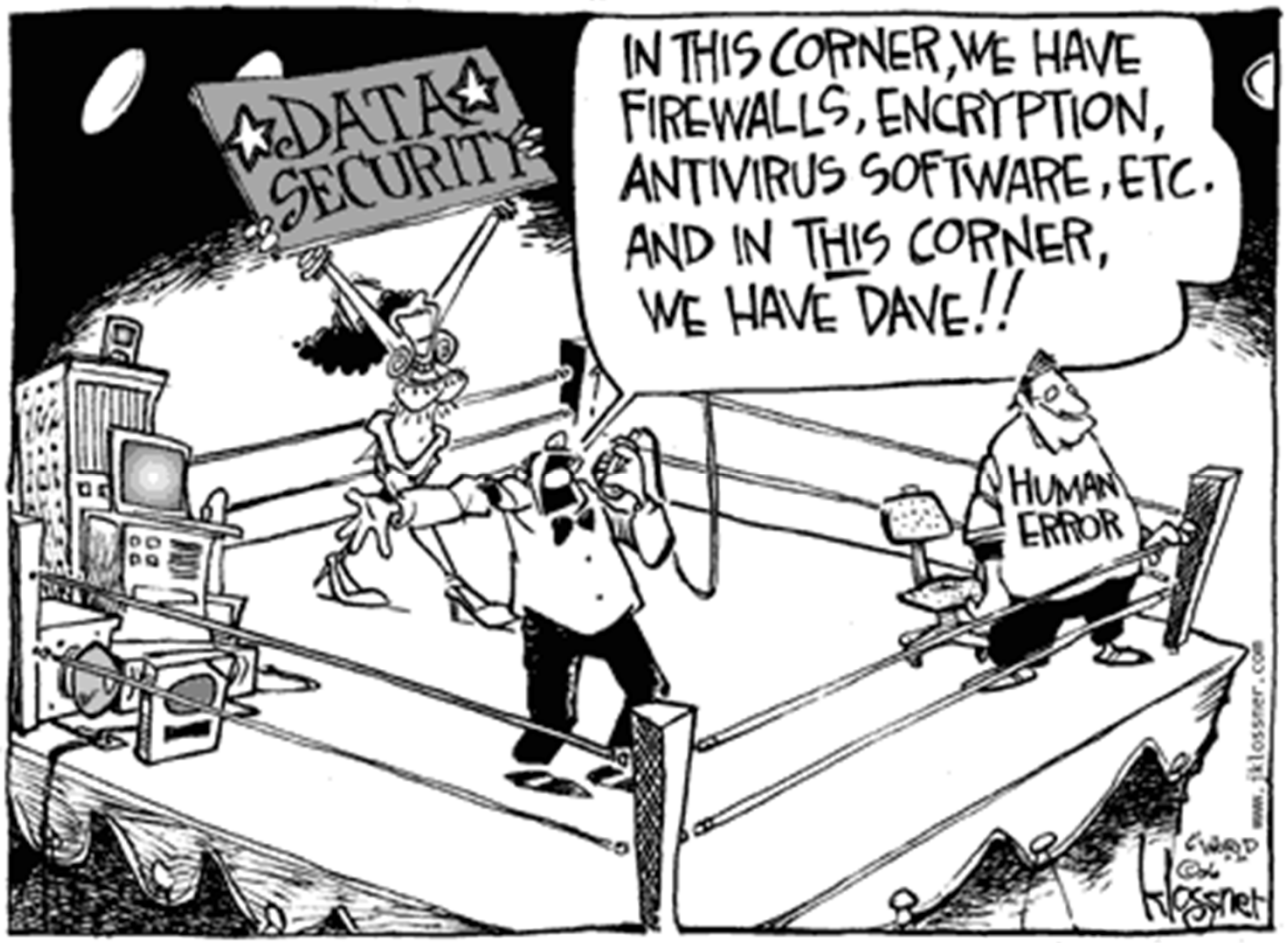
- **encrypted data?**
  - hakuna matata = don't worry, we have a backup!
- **how old is the backup?**
  - the silent ransomware …
- **off-line or network backup?**
  - the case of the digital dentist …
- **verified or "trusted" backup?**
  - the case of Swedish backup …
- **when was the attack?**
  - the case of the video archive …

State of ransomware 2021

- **survey 5,400 IT managers, mid-size companies, 30 countries**
  - 37% affected (51% in 2020)
  - data encryption for 54% of the attacked (73% in 2020)
  - financial impact for recovery 1.85M$ (761k$ in 2020)
- **companies that paid the ransom 32% (26% in 2020)**
  - … but only 8% got the whole data back
  - … and 29% recovered up to half of the data
  - 65% is the average amount of data recovered after payment
- **retail and education the most attacked sectors (44% each)**
- **local government most likely to have data encrypted (69%)**

source: sophos-state-of-ransomware-2021-wp.pdf

Technology and human beings



http://jklossner.com/computerworld/images/security26.gif

Basic problems (non technological)

- low problem understanding (awareness)
- mistakes of human beings (especially when overloaded, stressed, …)
- human beings have a natural tendency to trust
- complex interfaces / architectures can mislead the user and originate erroneous behaviours
- performance decrease due to the application of security measures
- …

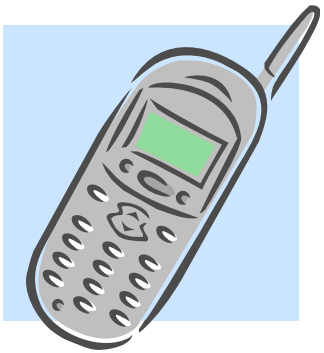
Social engineering techniques and strategies

- **ask for the (involuntary) user's participation to the attack**
- **usually naive users are targeted (e.g. "do change immediately your password with the following one, because your PC is under attack") ...**
- **… but experienced users are targeted too (e.g. by copying an authentic mail but changing its attachment or URL)**
- **via mail, phone, fax, or even paper**
- **psychological pressure:**
  - "help me, otherwise I'll be in troubles …"
  - "do it, or I'll report it to your boss …"
- **showing acquaintance with the company's procedures, habits and personnel helps in gaining trust and make the target lower his defences**

Phishing (~fishing)

Fake mail / IM

- **it's easy to create a fake mail**
  - … but it's difficult to use the right "tone"
  - … it's better to use an original mail with a different (malicious) attachment
- **… but we can also create a fake SMS or IM**
  - e.g. fake ATM withdrawal message
- **fake kidnapping alarm**



(Repubblica, 30/9/2017)

Mr. Confindustria in Brussels tricked by an hacker: 500,000 Euro lost. Fired.

"Transfer immediately half a million to this foreign bank account. But this mail was from an hacker. And the money has disappeared.
The fake order was (apparently) signed by director Panucci: "Please execute and don't call me because I'm out of office with the president".

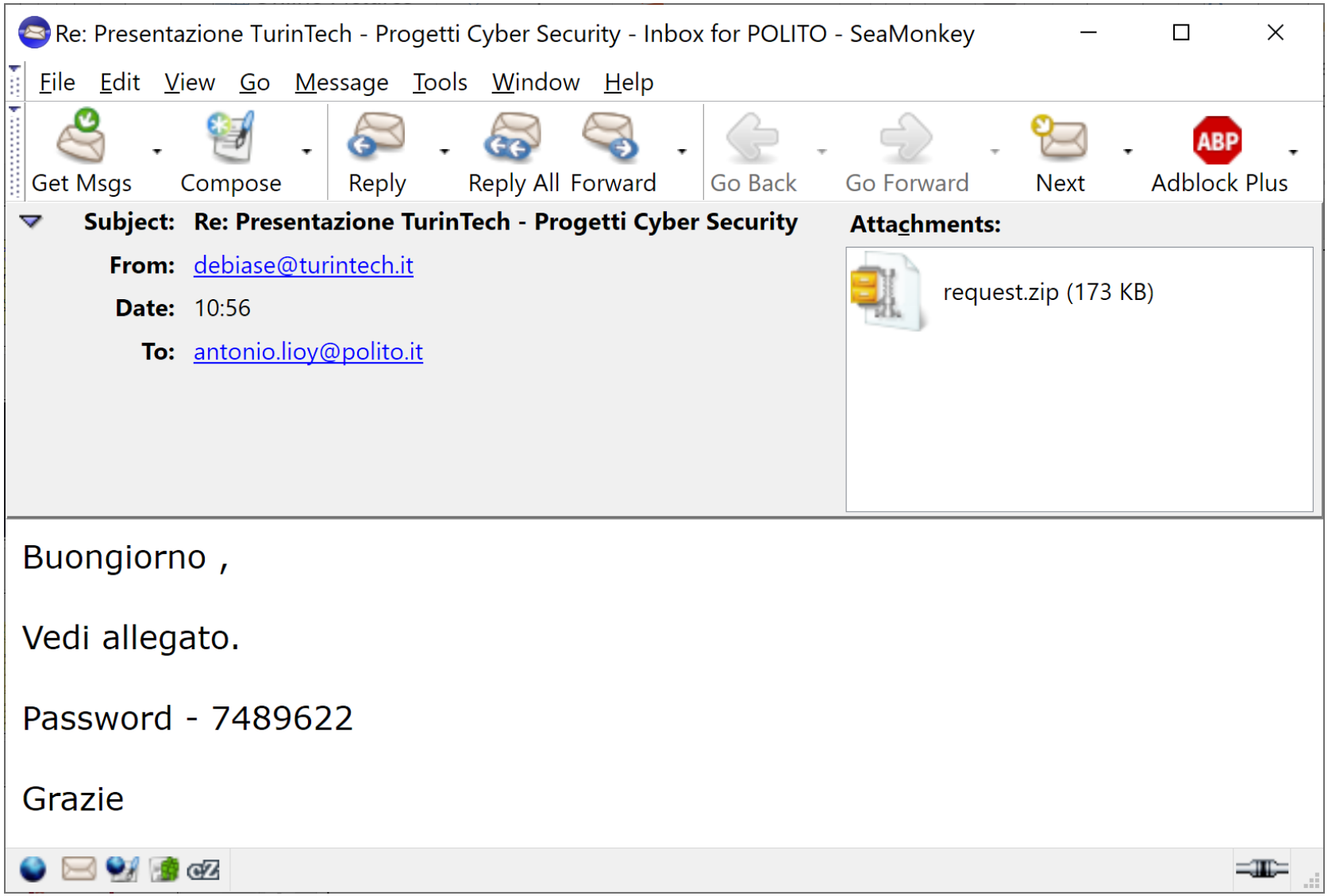
A mail from CIA …

```
From: Post@cia.gov
Date: Tue, 22 Nov 2005 17:51:14 UTC
X-Original-Message-ID: <1e3c8.15d13bbb95@cia.gov>
Subject: You_visit_illegal_websites

Dear Sir/Madam,
we have logged your IP-address on more than 30 illegal Websites.
Important: Please answer our questions!
The list of questions are attached.

Yours faithfully,
Steven Allison

++++ Central Intelligence Agency -CIA-
++++ Office of Public Affairs
++++ Washington, D.C. 20505
++++ phone: (703) 482-0623
++++ 7:00 a.m. to 5:00 p.m., US Eastern time
```

the attachment is the SOBER worm!

SMShing

A smart fake-mail



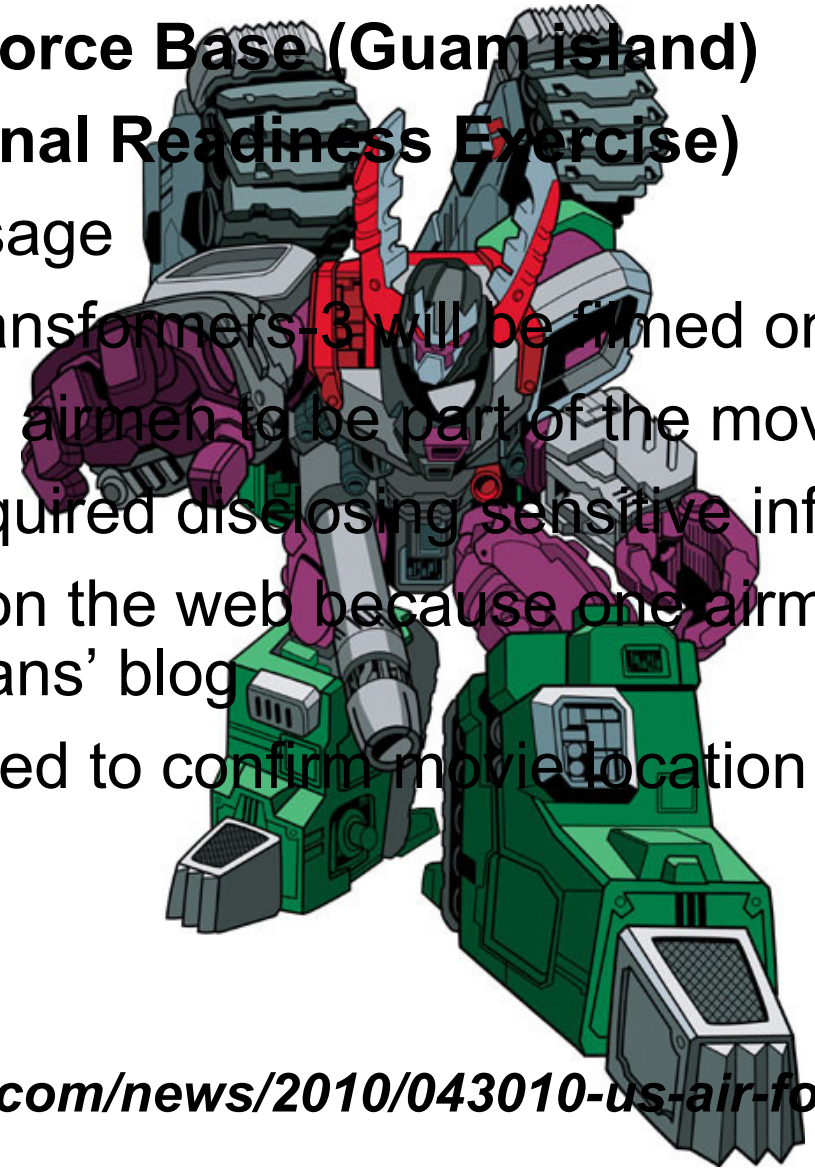
T.J.Maxx attack (2007)

- **45 M credit/debit card numbers stolen**
- **in a period of 18 months (up to January 2007)**
- **a 10 M USD legal class action started by 300 banks (e.g. Massachusetts Bankers Association, Maine and Connecticut Associated Banks)**
- **attack succeeded due to the use of WEP rather than WPA**
  - protection must be consistent with SOTA (State-Of-The-Art)
- **attack performed by 10 people (3 USA, 3 UKR, 2 CHN, 1 BEL, 1 EST + "Delpiero")**
- **one ex-cracker hired by the US secret service**

http://blog.wired.com/27bstroke6/2008/08/11-charged-in-m.html
http://www.wired.com/politics/law/news/2007/06/secret_service#

Phishing via Transformers3 (apr 2010)

- **Andersen Air Force Base (Guam island)**
- **ORE (Operational Readiness Exercise)**
  - phishing message
  - “the movie Transformers-3 will be filmed on Guam”
  - “looking for 20 airmen to be part of the movie”
  - application required disclosing sensitive information
  - event leaked on the web because one airman disclosed that on Transformer fans’ blog
  - journalists called to confirm movie location

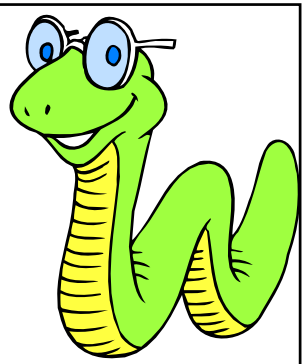


www.networkworld.com/news/2010/043010-us-air-force-phishing-test.html

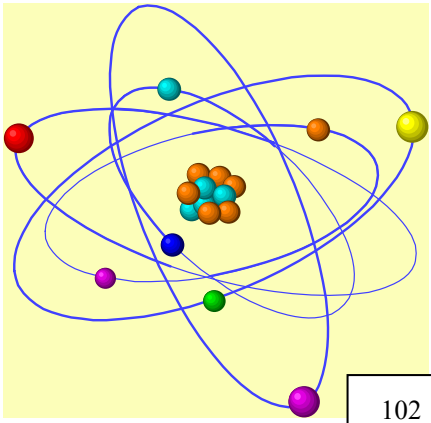
Some important recent attacks

- **Stuxnet**
  - cyber-physical systems
- **Black Energy**
  - critical infrastructure
- **Mirai, BlueBorne, BrickerBot**
  - Internet-of-Things, automotive, home

Stuxnet (2010)

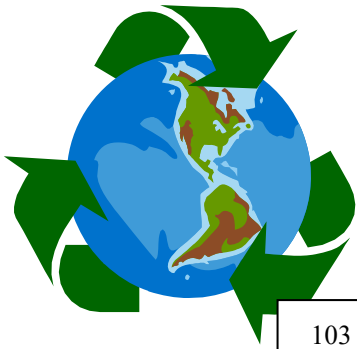


- **prototype of a new kind of attack**
- **worm + virus for Windows**
  - attempt to propagate to other systems
  - attempt to damage the SCADA systems (of a specific manufacturer) attached to the infected nodes
  - malware for cyberphysical systems
- **attack and propagation vectors:**
  - 1 known vulnerability (patch available)
  - 1 known vulnerability (no patch)
  - 2 “zero-day” vulnerabilities



Stuxnet: timing and location

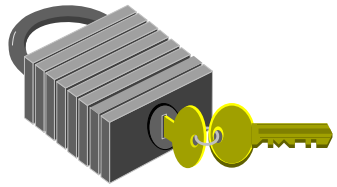
- 17/6/10 first detection
- 24/6/10 detected the use of a first signature certificate to appear as valid MS software !()
  - revoked on 17/7/10
  - … but the malware starts using a second signature certificate!
- 14-15-16/7/10 security bulletins by CERT and MS
- patches gradually released through October ’10
- self-stopped its propagation on 24/6/2012
- geographic distribution:
  - 52% Iran
  - 17% Indonesia, 11% India, …



Stuxnet: mechanisms

- **distribution and propagation:**
  - USB key as initial attack vector
  - shared disks (network share)
  - MS-RPC and MS-spool bugs
- **likely first infection via a USB key of a maintenance technician**
- **disguised as a driver**
  - with a digital signature validated by Microsoft!!!
  - uses two different certificates
- **access from the infected node to the back-end DB thanks to a shared default pwd (!!!) on every node**

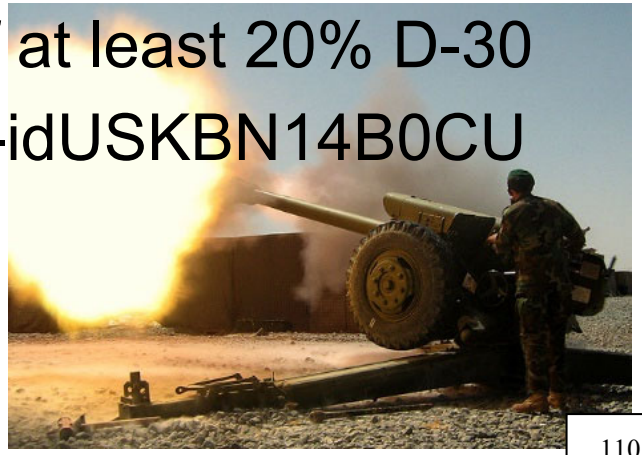
Stuxnet: lessons learnt



- **systems protected with physical separation (air gap) ... but without other standard protections:**
  - no anti-virus
  - no patch
  - no firewall
- **unnecessary services active:**
  - MS-RPC
  - shared network print queues
  - shared network disks
- **validation list for software to be installed**

Fancy Bear / APT 28

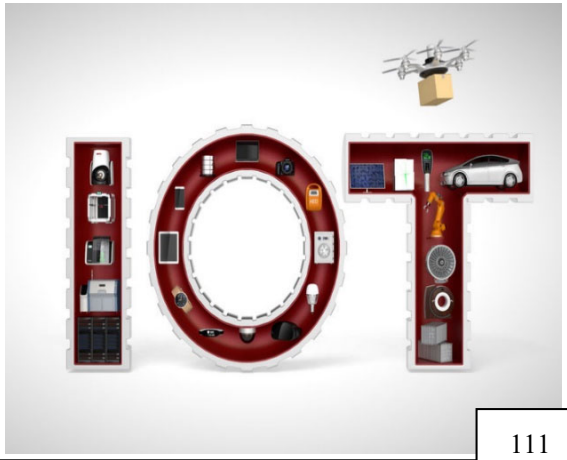
- **hacking group likely connected with the Russian military intelligence agency GRU**
- **cyber-attacks/espionage against German and Norwegian parliaments, French station TV5Monde, White House, NATO, U.S. Democratic National Committee, OSCE, the campaign of French presidential candidate Emmanuel Macron, …**
- **(2014-16) Android malware to target the Ukrainian Army's Rocket Forces and Artillery**
  - infected app to control targeting data for the D-30 howitzer
  - X-Agent spyware, permitted destruction of at least 20% D-30
  - www.reuters.com/article/us-cyber-ukraine-idUSKBN14B0CU



U.S. Army photo by Sgt. 1st Class David Trice - U.S. DoD
https://commons.wikimedia.org/w/index.php?curid=3668528

Exploiting IoT vulnerabilities: Mirai

- **cyberworm (Sep'16-Nov'16)**
- **victims are transformed in botnets for large-scale DDoS**
- **known disruptive attacks**
  - Krebs on Security → up to 620 Gbit/s
  - Ars Technica → up to 1Tbit/s
  - Dyn DNS provider → requests from tens of millions of IPs
- **botnets deployed into millions of IoT devices**
  - cameras, residential routers, baby monitors, …
  - almost no protection installed
  - Mirai easily spreads into home networks



Mirai (II)

- **a very complex malware**
  - almost no external dependencies (compiled w/ static libraries)
  - cross compiled to be executed on several platforms
  - released as open-source (!)
- **propagation scan phase to compromise additional targets**
- **observes the victim system before contacting the C&C**
  - anti-sandboxing strategy
    - connects to a fake C&C
    - IF no suspicious events recorded THEN go to the real C&C
- **performs different attacks**
  - driven by the C&C
  - TCP, UDP, GRE, also SYN flooding

The Wind-Infostrada case (fiber subscribers)

Bonny F.
un'ora fa

Hi guys.. Sorry for not speaking Italian. The Wind modems had telnetd running on port 8023 and a default password admin/admin which gave anyone root access to them. Unfortunately the modems got bricked by malware known as 'BrickerBot' which wrote random data over the partitions. When Wind eventually asks customers to return the devices for a replacement you'll want to be first in line..

- October 2017
- modem out of order > to be replaced
- was this for the good? (to avoid the creation of a botnet)
- similar (but worse) to the Deutsche Telekom case in 2016

The Wind-Infostrada case: lessons learnt

- use strong passwords (sigh!)
- change default password upon installation
- permit administrative access only from specific "trusted" networks
- apply timely all security patches to minimise the WOE

Real-time attack maps

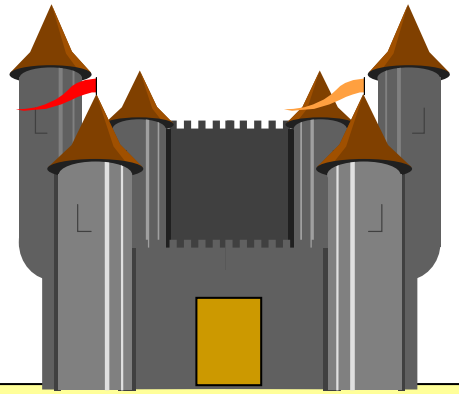
- **some resources:**
  - Norse = http://map.norsecorp.com/
  - Fireeye = https://www.fireeye.com/cyber-map/threat-map.html
  - Fortinet = http://threatmap.fortiguard.com/
  - Check Point = https://www.checkpoint.com/ThreatPortal/livemap.html
  - Kaspersky = https://cybermap.kaspersky.com/
  - Digital Attack Map (DDoS) = http://www.digitalattackmap.com/
  - Bitdefender = https://threatmap.bitdefender.com/
  - LookingGlass = https://map.lookingglasscyber.com/
  - IPew = https://www.vanimpe.eu/pewpew/index.html

Attack maps: sample data sources

- OAS = On-Access Scan
- ODS = On-Demand Scan
- MAV = Mail Anti-Virus
- WAV = Web Anti-Virus
- IDS = Intrusion Detection System
- VUL = VULnerability scan
- KAS = Kaspersky Anti-Spam
- BAD = Botnet Activity Detection

The three (four) pillars of security

0. Planning
(security policy, …)



1. Avoidance
(FW, VPN, PKI, …)

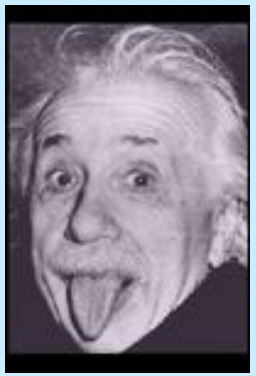
3. Investigation
(forensic analysis,
internal audit, …)

2. Detection
(IDS, monitor, …)

The NIST cybersecurity framework

https://www.nist.gov/cyberframework/online-learning/five-functions

Hacker & C.



hacker

cracker

script kiddie

wannabe lamer

Kevin Siers, NC, USA (cartoon from the Charlotte Observer)