Cyber Security and Warfare

Isodarco, Aug. 7, 2025

Bart Jacobs — Radboud University Nijmegen, NL
bart@cs.ru.nl

Overview

Cyber Security and Warfare

Where we are, so far

Who is this guy?

- Professor at Nijmegen (NL), in computer security & privacy
  - studied mathematics & philosophy, ended up in computer science
  - also (formal) appointments in Law & Philosophy
  - member of Royal Academic Society (KNAW) and Stevin-winner
- Doing a mix of theoretical, practical, societal work
  - in security & privacy a shift towards usability
  - with more focus on sovereignty and digital commons
- Regular role in media on security/privacy/intelligence issues, and occasionally in parliamentary expert meetings
- Former member of NL Cyber Security Council (2011 - 2023), and of intelligence evaluation committee (2020)
- One of the founders of iHub Nijmegen's inderdisciplinary Hub for digitalisation and society, see ihub.ru.nl

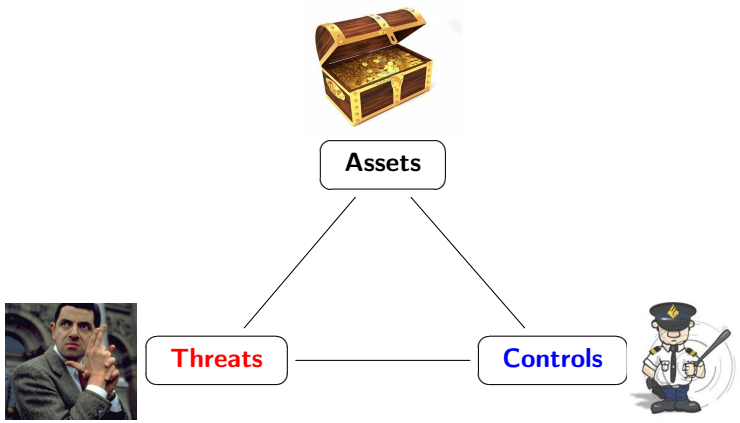
What is computer security about?

Computer Security is about regulating access to (digital) assets

Key issues

- Assets: the valuables that need protection
  - Eg. company/government secrets, or personal data (privacy)
- Regulating access: involves making sure that the **good guys** can get to the assets, but not the **bad guys**
  - who are we dealing with? who is on the other end of the line?
  - identity is very much part of the area
- Implicitly there is a malicious attacker that is trying to get unintended access
- Keep the good bits in and the bad bits out

Security management summary



Computer security is hot topic

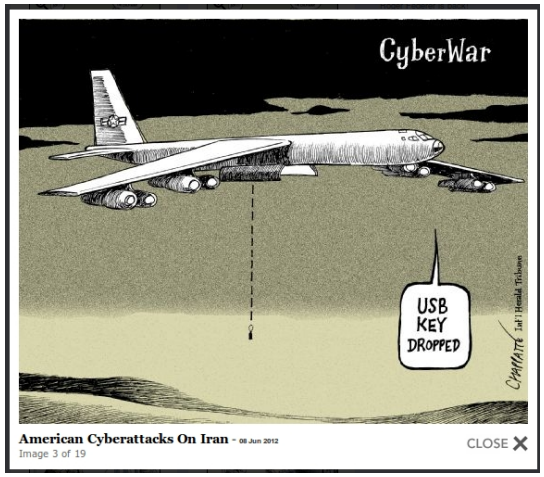
- Modern societies are highly dependent on digital technology
  - it offers great benefits, convenience, connectivity, etc.
- But this also makes us vulnerable
  - via unintented and intended (malicious) failures
  - clearly, the bad guys have gone digital
  - e.g. via *cyber* crime / espionage / warfare
  - but also via commerical and/or political manipulation
  - digital sovereignty has become urgent — finally
- Defence is typically more difficult than attack
  - esp. if the main focus is on functionality, not on security
  - see the Internet of Things, with all sorts of devices connected, monitoring, poorly designed, and not being maintained

Big question today: can we protect what we build?

Security and safety

- Important conceptual distincition, also in other languages
  - *Schutz* / *sécurité* / *sicurezza*
  - *Sicherheit* / *sûreté* / *incolumitá*
- Security is about protection against an active, malicious attacker that deliberately wants to undermine a (computer) system
- Safety is about protection against unintended accidents or errors
- Think about the difference between eg.
  - Nuclear safety / security
  - Food safety / security

Warfare is going digital



(© Herald Tribune, 2012)

Wars and Sciences: broad brush

- **WWI** was the chemists' war, with the use of poisonous gases
- **WWII** was the physicists' war, with the atomic bomb
- **WWIII**, if ever, will be the computer scientists' war

Broader, societal perspective

Follow what?

- Traditionally, one should "follow the money" in order to understand power relations in society.

From: All president's men (1976)

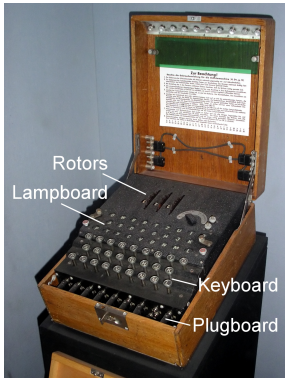
- Nowadays one needs to follow the data

- Big IT-companies have understood this like no other
- Note: computer security is about regulating access to assets
- There are many laws and rules to regulate and monitor financial flows. Regulation of data flows is still in its infancy

Where we are, so far

Old cryptographic systems

Scytala from Sparta



German Enigma from WWII

Check out `http://cryptomuseum.com/` for a large collection of devices & explanations

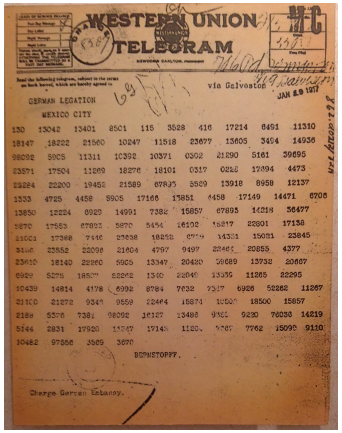
Cryptanalysis that changed the course of history

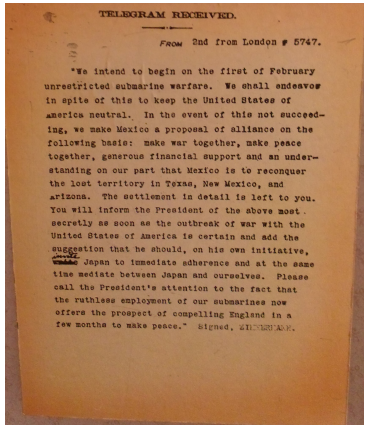
- The Zimmermann telegram in WWI, sent by Germany to incite war between Mexico & US, intercepted by the British and passed on the US; it brought the US into the war — see next page
- The breaking of the German Enigma in WWII by the British, shortening the war by probably at least a year.
- The breaking of the Japanese JN25 code in WWII by the US
  - it provided crucial intelligence in the Midway battle (1942)
  - and for ambushing the plane of Marshal Yamamoto (1943)

In 2020 operation Rubicon became known (a.o. via Peter Müller):

- the Swiss manufacturer of cryptographic equipment Crypto AG was secretly bought by BND and CIA (late 1960s)
- deliberately weak crypto was sold to about 100 countries, including Argentina, Egypt, Indonesia, but also to Italy, Spain

Zimmermann telegram, ciphertext and cleartext





(pictures from National Cryptologic Museum)

Modern encryption example

Example

The message:

Dit wil ik versleutelen!

becomes (with PGP-encrypt, in hexadecimals):

30a4 efde f665 d409 4946 c8b0 d82b 7620
312c bf1b 7f3a 8781 086d 069b b6e0 60a2
94c2 9b27 440c affd 5343 ca47 d0b4 afce 5719

Modern, software-based crypto systems are virtually unbreakable, when:

- well-designed and openly evaluated
- properly used

Main security goals

Alice & Bob are the "good guys", Eve is "bad", undermining them

- **Confidentiality:** Eve cannot read the content of what Alice and Bob are communicating.
- **Integrity:** Eve cannot alter the content of the communication.
- **Authenticity:** Alice and Bob are certain about each other's identities. In particular, Alice (say) is not talking to Eve, while she thinks she is talking to Bob.
- **Availability:** Eve cannot prevent the communication between Alice and Bob.
- **Non-repudiation:** (*undeniability*) Alice and Bob can not deny what they have communicated at a particular stage.
- **Accountability:** There is a reliable log of the communication history (of Alice, Bob, Eve, et al)

Realisation of security goals: confidentiality

Confidentiality is achieved via encryption

- Encryption requires (cryptographic) keys
  - in practice they are long numbers, far too long to remember
  - they must be bound to a person or organisation
- There are key management challenges:
  - keys must be stored securely, but readily available (e.g. via smartcard)
  - they must be bound to the right person / organisation
  - a secure backup of keys may be required; with whom?
- **Note:** encryption does not provide integrity
  - e.g. Eve may swap encrypted messages

Realisation of security goals: integrity

Integrity is achieved via hashes / fingerprints

- A hash of a message is a short garbled summary, that matches only to its original message.
- If Alice sends Bob the hash separately from the message, Bob can check if it still matches, and thus that the message is unchanged.
  - alternatively, a signed hash can be sent with the message
- Hashing does not guarantee confidentiality
- What do banks care more about, confidentiality or integrity?
  - and what about the military?

Realisation of security goals: authenticity

Integrity is achieved via challenge-response

- Suppose I wish to check for sure I'm talking to you
  - the idea is to ask you to do something that only you can do
- For instance:
  - I can send you a random encrypted message and ask you to decrypt it — assuming we know each other's keys
  - I can send you a random (unencrypted) message and ask you to digitally sign it
- **Question**: why should these messages be random?

Realisation of security goals: availablity

Availability is achieved via robustness

- robustness against attacks, typically denial-of-service (DOS)
- duplication and fallback of infrastructure
- restriction of usage, via authentication
- . . . (difficult in practice)

Realisation of security goals: non-repudiation

Non-repudiation is achieved via digital signatures

- An ordinary ("wet") signature binds the signer to a document
  - the signer is committed to the content
  - others can recognise the signer and keep him/her responsible
- A digital signature does this more effectively
  - the signer needs a personal "private" key to sign
  - everyone else can check via the corresponding "public" key
  - including the identity of the signer
  - if only one bit is changed in the document, the signature check fails
- Digital signatures are still not widely used
  - this may change with emerging ID-wallets (in the EU)

Realisation of security goals: accountability

Accountability is achieved by keeping logs

- Computer systems automatically keep logs of what happened
  - for specific purposes, one has to program one's own logging
  - with relevant info: identities, transactions, time-stamps, etc.
- Logs must be securely stored, separately, outside reach of an attacker
  - ideally they are also digitally signed, for authenticity
- They must also be inspected regularly
  - this is boring work that often does not happen
  - AI may help, to recognise anomalies

Where we are, so far

Cyber attacks/warfare, some general points

- **Activities**: digital attacks on the opponent, in order to disrupt / damage / gain access / compromise / confuse / misinform
- **Actors**: military / intelligence organisations, state-sponsored hackers, criminal gangs, self-organised civilians
- **Aims**: strategic, political, or military
- **Techniques**: mostly hacking (or DOS), sometimes well in advance, to build up a hidden position for disruption
- **Targets**: government agencies, military systems, critical infrastructure (communication, power), financial institutions, private corporations, the press, ...
- **Impact**: military, economic, psychological

Cyber attacks/warfare, some characteristics

(1) Attribution is difficult, providing plausible deniability
(2) Cyber attacks can weaken the opponent, below the radar
(3) They may involve preparatory positions, in the software infrastructure of the opponent, for later actual use and for threats
(4) They are cheap, empowering militarily weaker parties (asymmetric)
(5) Cyber warfare is volatile, difficult to count on (since access/positions may be lost), not "push button"

Cyber attacks work well in the grey zone, inbetween peace and war, like now between Europe and Russia

Ukraine: some first observations

(1) Cyberwar component is clearly present, but traditional kinetic warfare dominates — although drones are gamechanger
  - Ru hacked Ukr power grid, telecom, government websites
  - Ukr (recently) hacked Gazprom, Aeroflot
  - much electronic warfare, against drones and GPS
  - Big Tech essential for access (via Starlink) and cloud

(2) It is a whole-of-society networked conflict
  - notably in flexible drone production, training, deployment
  - effectively supported by Ukr's Diia app
  - two-way authenticated, secure communication between government and citizens, for continuity and engagement

Diaa services

- Digital Documents: passports, driver's, certificates, student IDs
- Government/public/health: tax, military, benefits, fines
- Banking and finance: also for payments, via linked back accounts
- Education: students can access their academic records, apply for scholarships, and manage other education-related services.
- Notifications and (emergency) alerts
- Digital signatures, for authenticity and non-repudiation
- Public transport info
- e-Enemy feature, for reporting Ru militairy activities, also via video

Atlantic Council (May 30, 2023): "Ukraine's Diia platform sets the global gold standard for e-government". It withstood Ru attack, so far.

Diia is far ahead of current EU digital ID-wallet plans. It is essential for whole-of-society warfare.

Question, for the discussion

Are cyber warfare activities more suited for the grey zone than for all out war?

Where we are, so far

iCIS | Digital Security
Radboud University

The authenticity crisis

- Concerns exist today about artificially generated content and dis-/mis-information — and their societally destabilising effect
- Veracity of information is unsolvable, esp. in political matters
  - fact checking provides limited help to citizens
- Authenticity is a more helpful concept
  - it involves certainty about source and integrity of messages
  - it can be guaranteed technically, via digital signatures
- Digital signatures are useful tools for people to make their own credibility and veracity judgements
  - signatures can strengthen institutions online — when they start signing

See BJ, *The Authenticity Crisis*, Computer Law & Security Review 53, 2024, doi.org/10.1016/j.clsr.2024.105962

iCIS | Digital Security
Radboud University

Benefits of systematic signing I

- Assume a video appears online in which the Dutch PM is extremely negative about Muslims or Jews
  - risk of societal uproar and international repercussions
- Would an AI-analysis of the video be helpful?
  - outcome would be probabilistic, say 80% certain that it's fake
  - this leads to AI-AI battles
- If the Dutch government would digitally sign all its messages it could publicly ask: *is the video signed?*
  - No? Then it is not authentic, since we sign everything!
  - Outcome is immediate, and unambiguous
- In this way "institutions" can strengthen their online position
  - their messages are recognsiably theirs

iCIS | Digital Security
Radboud University

Benefits of systematic signing II

- Government fact-checking does not work: the authorities telling citizens what is true and false
- More sensible: providing (signing) tools for authenticity empowers citizens, to make their own judgements
- Democracy is based on well-informed, open debates
- There is a deliberate anti-democratic, authoritarian strategy:
  - Steve Bannon: "flooding the zone with bullshit"
  - aim is: reality fatigue among the population
  - so that people react to another warcrime: "they say so much"
- Signing is helpful, but not a complete fake news solution
  - signatures will not help against confirmation bias

Own "hardening" work on PubHubs and Yivi

- New community platform PubHubs.net based on public values
  - aim is combination of privacy and accountability
  - via flexiile digital identities (with own eID wallet Yivi)
  - including digital signatures
  - for respectful, decent contact with (and in) rank and file of organisations
  - at this stage running pilots, broader launch later this year
- Such independent, locally-hosted platforms are important for:
  - digital sovereignty, continuity of business
  - whole-of-society approaches in crisis situations
- Also relevant for discussions about minors and "social" media
  - when there are decent alternatives, restricting access to dubious platforms is less dramatic

Fragility of current arrangements

- Ties with the US may be cut suddenly, e.g. because
  - red button of Trump, see International Criminal Court (ICC)
  - Putin cutting transatlantic cables
  - Court of Justice of the European Union (CJEU) likely to soon forbid data sharing with US — "privacy shield" under constant pressure of privacy activist/lawyer Max Schremms

Global platforms

VS	Europe	China

Google, Amazon, Uber, Apple, airbnb, NETFLIX, Spotify, Baidu 百度, Alibaba.com 阿里巴巴, Tencent 腾讯

etc

EU situation

We run American software on Chinese hardware

(and increasingly, Chinese software too)

Where did we go wrong?

Where we are, so far

iCIS | Digital Security
Radboud University

Concluding remarks

- The bad guys have gone digital, in cybercrime and cyberwarfare
- Power relations, also geopolitically, are determined by access to information flows
- Computer security techniques regulate such access
  - this makes it a socio-political topic
  - basic knowledge of their nature is required to understand the current world
- All out cyber conflict has not happened yet
  - but much is happening under the radar, in the grey zone
  - is that where the cyber conflict will stay?

iCIS | Digital Security
Radboud University