# Computer Security: Intro

B. Jacobs and J. Daemen
B.Jacobs@cs.ru.nl
Version: fall 2016



iCIS | Digital Security
Radboud University

# Outline







# About this course I

## Lectures

- Weekly, 2 hours, Thursday morning (10h45)
- Lectures are based on own slides
  - Updated version, slightly different from previous years
- Lots of background information available on the web (esp. wikipedia)
  - Do use such additional sources!
  - Certainly if you do not fully understand things
- Up-to-date info (bookmark; accessible via my webpage) at: ru.nl/ds/education/courses/security-2016/
  - Slides and exercises will appear there

# About this course II

## Attitude

- Presence at the lectures is not compulsory . . .
  - but active attitude expected, when present
  - Phones/laptops shut down
- Politeness is highly appreciated!
- Asking questions:
  - about the exercises: talk to your course assistant
  - about the course: best to see me during the break
  - think/check before you send me email!
- The audience is large; chatting is annoying to everyone else
  - Exception: jokes are OK, but only if they are extremely funny

# About this course III

## Exercises

- Compulsory, make up ten percent of final mark
- Also weekly exercise meetings, on Fridays (at first 13:45, later 15:45)
  - Answers, for old exercises
  - Questions, for new ones
- 2 staff members: *Joost Rijneveld, Hans Harmannij*, and 3 students
- You may work in (stable) pairs, and also alone
  - if this is not the first time you do this course, you have to work alone!
  - it will be sent by email in which group you are

# About this course IV

## Exercises

- Schedule:
  - New exercise on the web on Friday morning, say in week $n$
  - You can try them yourself immediately and ask advice on Friday afternoon in week $n$
  - You can ask final questions, again on Friday in week $n+1$
  - You have to hand-in, via Blackboard, before Monday 9h00 AM sharp, in week $n+2$; late submissions will not be accepted
- Exercises URL on lectures page, with further instructions
- The first set of exercises appears Friday 9 sept.
  - first exercise course is on that same day

# About this course V

## Examination

- Final mark is weighted sum of:
  - average of markings of exercises
  - written exam (January)
  - (there is no mid-term exam for security)
- **Formula**: final = 0.9 * exam + 0.1 * exercises
- Re-exam of written exam in spring
  - only written exam can be done once again: mark for exercises remains
- If you fail again, you must start all over next year
  (including re-doing new exercises)

# About this course VI

## Some special points

- You can fail for this course!
  (I know, it's extremely unfair)
- 6ec means $6 \times 28 = 168$ hours in total
  - Let's say 18 hours for exam
  - 150 hours for 15 weeks means: 10 hours per week!
- Large, mixed audience: computer science, information science, pre-master, artificial intelligence, mathematics, . . . . . .
- Requires some flexibility
  - but computer security is inherently multidisciplinary

# About this course VII

## How to pass this course . . .

- Practice, practice, practice . . .
  Only in this way the course material can be internalised
- You don't learn to do it by just staring at the slides
  - or by letting your exercise partner do the work
- Exam questions will be in line with (compulsory) exercises

# About this course VIII

Experiences from earlier (mathematics) course, with similar marking (average of homework and exam):

| Study | # students | Homework | Exam | Final |
|---|---|---|---|---|
| KI | 16 | 8.1 | 6.5 | 7.1 |
| IC | 11 | 7.5 | 7.6 | 7.5 |
| IK | 5 | 6.9 | 7.1 | 6.8 |

Why were KI students doing so much worse at the exam?

- They exchanged answers in a *Facebook* group
- Who were they fooling?

# About this course IX

## Here is the deal:

- *We* provide: careful explanations & examples, and individual feedback
- *You* work for this course: regularly and diligently!
  - The topic is not really difficult, but you may have to get used to it, and work on each exercise yourself
  - everyone here should be able to pass.

## If you don't go for the deal ...

- You create problems that you will have to solve yourself
- Don't forget about the *bindend studie advies* (BSA): in the first year you need to collect at least 42 (or 45) ec out of 60!
- In 2015/2016 about 71% in IC got a positive BSA!

# About this course X: gender issues

(Source: Vox 6-10, nov. 2009)

# About this course XI: intellectual attitude

The right intellectual attitude involves both:

- intrinsic motivation/drive to understand how things work
- assertivity to be able to say: *I don't understand this!*

# About this course XII

## Sensitivity of the topic

- Not everything is publicly known (like e.g. in algebra)
- Some things are simply illegal: don't try this at home!
  - Moral compass/fibre/backbone required in this field
- Lectures are deliberately not recorded!
  - some inside stories & anecdotes will be told
  - they can be misinterpreted, out of context
- Following the daily news is strongly recommended: security is a highly political topic.

# About this course XIII

## Topics

- Basic notions: confidentiality, integrity, availability
  (jointly known as: CIA of information security)
- Basic techniques: symmetric cryptography: encryption, message authentication codes, . . . asymmetric cryptography: key establishment, electronic signatures, . . .
- Basic protocols for achieving security goals
- Basic technologies (PGP, SSL, certificates, etc)
- Underlying mathematics (cryptography) is used as tool box, not topic of study in itself
  - But very basics are included (substitution, transposition, RSA, El Gamal)
- Several practical examples: e-passport, voting, Bitcoins, . . .

# Beyond this course

## More about computer security

- There is a lot of interesting reading
  - Historical
  - Military/intelligence
  - Societal (eg. about privacy)
  - and technical, of course
- Reading a bit more is strongly encouraged
- Many connections with legal issues
  - You can find out about a *Minor* in law
  - Or follow the (master)course *Law in Cyberspace*

# Computer security @Nijmegen

## Research

- Security important research topic at Nijmegen
- Much theoretical research, eg. on crypto & protocol correctness
- Also many societal issues: involvement with
  - e-voting
  - e-passports and identity cards
  - bankcards (eg. EMV issues)
  - e-ticketing
  - smart (electricity) metering
  - road pricing
  - electronic patient records
  - cyber security

## Teaching

- A special *TRUE Security* master programme,
  - Jointly with Eindhoven
  - Also open to Math. & AI students

# Financial crime in NL in M€ (Source: Betaalvereniging)

| Activity | '92 | '10 | '11 | '12 | '13 | '14 | '15 |
|---|---|---|---|---|---|---|---|
| **bank robbery** | 570 | 26 | 7 | 4 | ? | ? | ? |
| **internet banking** | — | 10 | 35 | 38 | 9.6 | 4.7 | 3.7 |
| **bankcard skimming** | — | 20 | 40 | 29 | 6.8 | 1.3 | ±0 |

**Remarks**:

- You're an old-school loser if you're still planning a career as bank robber
- *Bad guys have gone digital*, in fraud, blackmail, sabotage, espionage
- New forms of financial fraud constantly appear, like: asking to send in your bank card: total fraud is a bit higher in 2015 than 2014

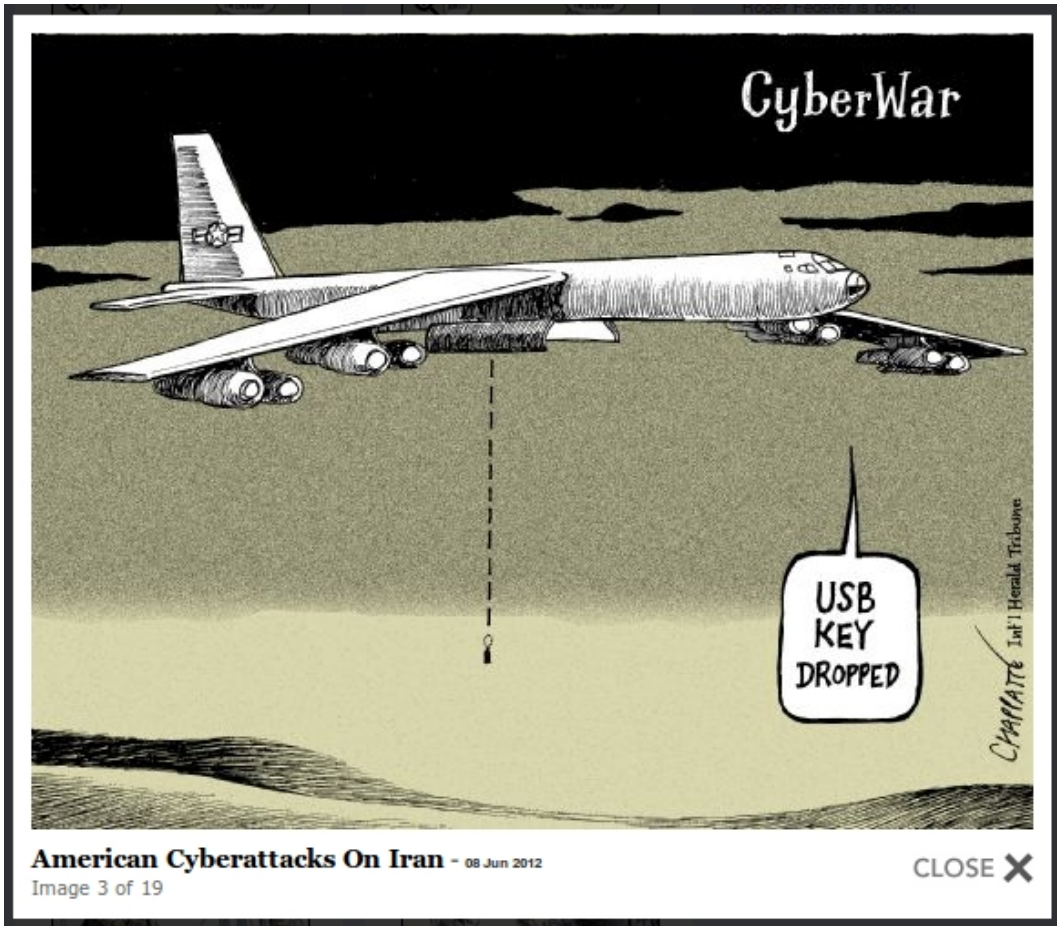
# “Over vijf jaar helft misdaad door cybercriminelen”

PG Gerrit Verburg, Nieuwsuur 15 juni 2016





# Warfare is going digital




(© Herald Tribune)

# Wars and Sciences

- **WWI** was the chemists' war, with the use of poisonous gases

- **WWII** was the phycists' war, with the atomic bomb

- **WWIII**, if ever, will be the computer scientists' war

# What is *computer security* about?

## Computer Security is about regulating access to (digital) assets

**Key issues**

- assets: the valuables that need protection
  - Eg. company secrets, or personal data (privacy)
- regulating access: involves
  - identification: who are you? / what are your attributes?
  - authentication: how do you prove this?
  - authorisation: what are you allowed to do
- Implicit there is a malicious attacker that is trying to get unintended access
  - Attacker model: what can the bad guys do?

# Attacker example

KPMG Amsterdam has a good computer security group

Some time ago, KPMG was approached by a large firm that had its own secure facilty, with sensitive and strategic data. It had:

- strong physical & electronic security measures
- strict operational security guidelines
- well-trained staff

KPMG was asked/challenged to try and obtain access, either physically or electronically ("red teaming")

They managed to get in as Santa Claus

(an attack known as: *Trojaanse Schimmel*)

# Yes, indeed . . .

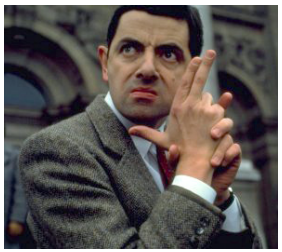
**Computer security is the nicest part of computer science!**





# Security management summary

Assets



Threats

Controls

# Important change

For many organisations, internet access has changed

- from an opportunity
- to a liability

# Threats from attackers

(1) How do you protect against a deliberate, well-motivated, malicious, resourceful, technically competent, intelligent, creative, socially skilful, patient attacker?

(2) Assume you think you have such protection, how do you test / verify it?

- How do you formalise the attacker?
- How to incorporate *out-of-the-box thinking* and *geeky sick minds* into your validation methods


(3) Formalisation only makes your assumptions explicit
- There is no reason an attacker will do what is assumed

# Controls: security requires a mix

## Protection of digital assets requires a mix of:

- Technical measures
  - Cryptography, as mathematical basis
  - Computers, to run cryptographic algorithms (and to break them)
  - Physical security, like tamper-resistant/proof hardware or ordinary locks
- Organisational measures
  - Examples: chipknip, banking, rocket launch (eg. from submarine)
  - *three B's*: burglary, blackmail, bribery
- Legal measures
  - Criminal law: esp. computer criminality laws
  - Civil law: eg. in user agreements (like for bank/travel cards)

# Example: civil vs. criminal law

- Imagine you are asked to test the security of a company's webpage, by trying to hack into it
- You sign a contract first, in which you exclude that the company can take you to court for hacking into its website
  - hence you exclude civil liabilities
  - that is: court procedures between you and the company
- But criminal liabilities remain
  - your hacking activity is simply illegal
  - theoretically, you run the risk of prosecution
  - that is: court procedures between you and the state
  - in practice however, this will not happen

# Legal relevance

## Important distinction

- Computer science for law (*rechtsinformatica*)
  - Eg. knowledge representation, formal reasoning
  - Strong AI flavour

- Law for computer science (*informaticarecht*)
  - The laws governing the use of computers
  - European origins
  - Strongly related to cyber crime
  - Part of penal law (*wetboek van strafrecht, Sr*)
  - Most relevant here
  - Topic of much debate, eg. proposal for hacking by police in CCIII

# Computer crime laws, in Dutch

- art. 138a, Sr: *computervredebreuk*
  No computer intrusion
- art. 139a, Sr: *afluisteren*
  No eavesdropping (for confidentiality)
- art. 161sexies, Sr: *stoornis*
  No computer disruption (for hardware and software integrity & availability)
- art. 350a, Sr: *wijzigen of vernietigen van opgeslagen gegevens*
  No data corruption (for data integrity).

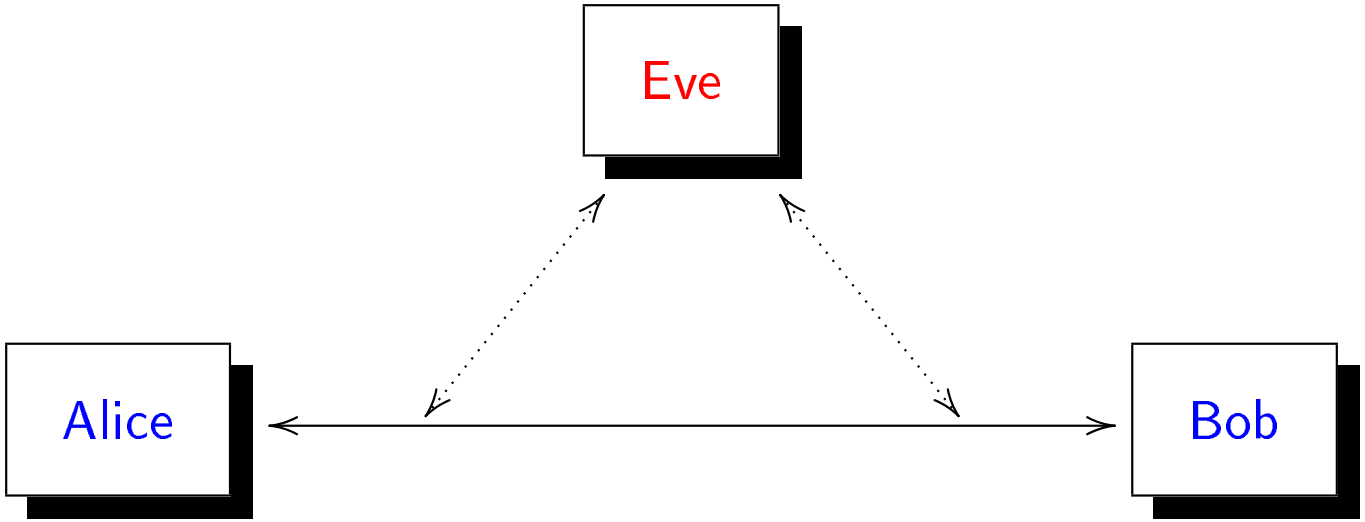
# Example legal text snippet

No eavesdropping:

> *Hij die door middel van een openbaar telecommunicatienetwerk, of door middel van daarop aangesloten randapparatuur overgedragen gegevens die niet voor hem, mede voor hem of voor degeen in wiens opdracht hij handelt, zijn bestemd, opzettelijk met een technisch hulpmiddel aftapt of opneemt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.*

# Intrusion schematics

Generally: Alice & Bob are good guys, who stick to the protocol;
Eve is evil




(Check out: http://downlode.org/Etext/alicebob.html )

# Aspects of intrusion

The intrusion of Eve may involve various aspects:

- Passive eavesdropping: read and/or store data, whether encrypted or not, possibly for future use
- Active intervention: delete and/or insert data

Also relevant:

- The nature of the connection between Alice and Bob (copper, fibre, electromagnetic) influences the possibilities and the effort that is required.
- Alice may emit unknowingly, eg. via
  - tempest: emmission security is a big thing in the military
    (but also killed voting machines in NL)
  - covert channels, eg. power consumption of smart cards, or deliberate leaking via malicious software.
    (or: increase of pizza deliveries to the Pentagon reveals upcoming military action)

# Traffic analysis

- In many situations it is already of great interest who is communicating with whom, without knowing the content
  - Eg. who does the prime minister call in a political crisis?
  - Who is in contact with a known terrorist?
- Recording/exploting such connection-info is traffic analysis
  - in the NSA surveillance discussion one speaks of *recording meta data*
- The European data retention directive (2006) forces communication providers to store phone & internet meta data of *all Europeans* for 6-24 months, and let authorities access it.
  - no longer valid, since CJEU-ruling of 8 april'14
- Meta data are already very privacy sensitive:
  - they show if you have communicated with an abortion clinic
  - they include your location, when you use a mobile phone
  - see *Correspondent* article on Ton Siedsma's meta data

# Relevance of meta data

"It's just meta data!"

"We kill based on meta data"
(former CIA & NSA chief Hayden)

# Main security goals (important slide!)

- **Confidentiality:** Eve cannot read the content of what Alice and Bob are communicating.
- **Integrity:** Eve cannot alter the content of the communication.
- **Authenticity** (or **"entity authentication"**): 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:** (*onloochenbaarheid*) 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)

(A bit confusingly "integrity" is sometimes called "message authentication")

# Security and safety

- Important conceptual distincition. In Dutch more subtle
  - *beveiliging* (German: *Schutz*, French: *sécurité*)
  - *veiligheid* (German: *Sicherheit*, French: *sûreté*)
- 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



iCIS | Digital Security
Radboud University

# Security and privacy

Two relations:

(1) Privacy can be seen as part of of computer security, dealing with protection of personal data

(2) Privacy is also important for personal security
- telling on your *Facebook* what your home address is and when you are away on holidays is asking for trouble
- think of mistreated women in women's shelters
- identity fraud is (becoming) a really serious problem.

# Security and autonomy

**Information is power**

- Who has access to which information determines the power relations in the world
  - Not: *follow the money*, but *follow the data*
  - Computer security is all about regulating this access
- Eg. are people still free/autonomous if *Google*/... determines what they get to see?
- You want to read more? Look eg. at:
  - Pariser, "The filter bubble" (2011)
  - Morozov, "The Net Delusion" (2011), "To Save Everything, Click Here" (2013)

  (for an introduction, watch them at ted.com)



iCIS | Digital Security
Radboud University

# Hero or traitor?

# Intelligence gathering 1.0 and 2.0


(Source: own TEDx talk, 2013)

# Importance/relevance of computer security

- When you read about computers in the press, probably more than 80% of the reporting is security related
- Security issues can make or break large public ICT-projects:
  - E-ticketing (Mifare problems, in OV-chip, Oyster, etc)
  - Electronic Health care files (EPD, in Dutch)
  - Road pricing
  - E-voting
  - etc.
- Relevance for companies:
  - Protection of their assets (intellectual property, stock-related info, strategy, . . . )
  - Protection of e-commerce transactions
  - Privacy & data protection regulation
  - Profiling customers & behavioural targeting ("CRM")

# Interdisciplinary character of Security

## Core disciplines

- Mathematics, esp. cryptography
- Computer science, esp. security protocols, operating systems, networking, formal methods, ...

## Some related/overlapping disciplines

- Law esp. wrt. cyber crime
- Management / organisation
- Security economics: what kind of economic stimulus improves security?
- Psychology of security: what triggers people to behave (in)securely: social engineering / pretexting

# Main security stakeholders (or: future employers!)

- Banks / financial institutions
  - Main concern: not confidentiality, but integrity of transactions
  - Also: non-repudiation of orders (esp. in e-banking)
- Telecom / internet operators
  - Concerns . . . ??
- Health care sector
  - Much focus on confidentiality / privacy
  - But also integrity & availability of electronic patient files
  - Note: integrity breach can be repaired, in principle, but confidentiality breach not
- Citizens, for protecting their own data against disclosure or capture (ransomware), and for privacy protection
- Intelligence / Military / Diplomats

# Intelligence services

## Double task

- Defensive: protecting own assets / communication
- Aggressive: uncovering secrets of others

## Common distinction

- Humint: intelligence from human sources
  (slow, rather unreliable, small volumes, local)
- Sigint: signals intelligence (including Elint & Comint)
  (non of the above; often crucial in world history, like in Enigma, Zimmermann Telegram, etc.)

# Some organisations

- USA
  - Internal: FBI, can also make arrests!
  - External: CIA, mostly humint
  - Sigint: NSA $\geq$ FBI + CIA
- UK
  - Internal: MI5
  - External: MI6 (aka. SIS), mostly humit
  - Sigint: GCHQ $\geq$ MI5 + MI6
- NL
  - General: AIVD
    (includes NBV = *Nationaal Bureau voor Verbindingsbeveiliging*)
  - Military: MIVD
  - Sigint: JSCU = Joint Sigint Cyber Unit (of both AIVD & MIVD)

All these organisations work in secrecy — and secrecy carries the risk to be a cover-up for failure and incompetence. But they are under independent oversight (like CTIVD in NL)

# Intelligence services & computer security

- High-tech users, often with their own research departments
  - NSA is biggest employer of mathematicians, worldwide
  - At GCHQ public key crypto was first invented (but not published)
- Setting / pushing / undermining of security standards
  (Green book, common criteria, etc.)
- Strong operational security culture
  (including clearances/background checks)
- Active player in cyber security area
- Slowly getting more open, relying on COTS, open source etc.

# Simple protocol examples: electronic car keys

The aim is to give an idea of what security protocols are all about. In each case, ask yourself: is this secure? What is a possible attack?

**C** = Car, **CK** = Car Key, $K\{M\} = M$ encrypted with key $K$, in:

| **(1) Identification number** | **(2) Encrypted version of (1)** |
|---|---|
| $\mathsf{CK} \longrightarrow \mathsf{C} \ : \ \mathsf{IdNr}$ | $\mathsf{CK} \longrightarrow \mathsf{C} \ : \ K\{\mathsf{IdNr}\}$<br>($K$ is shared crypto key) |
| **(3) Sequence number** | **(4) Challenge-response** |
| $\mathsf{CK} \longrightarrow \mathsf{C} \ : \ K\{N+1\}$<br>($N$ is last used number) | $\mathsf{CK} \longrightarrow \mathsf{C} \ :$ "open"<br>$\mathsf{C} \longrightarrow \mathsf{CK} \ : \ K\{N\}$<br>$\mathsf{CK} \longrightarrow \mathsf{C} \ : \ K\{N+1\}$ |

(Look for Keeloq for more information on actual attacks)

# What you need to learn in this course

**Paranoia!**

- *Professional* paranoia, not *personal*
- A *security mindset*
- For instance, when you receive an email ask yourself:
  - Do I know for sure from whom the email comes (authenticity)?
  - Who may have seen this email (confidentiality)?
  - Is this the version that the author sent (integrity)?
  - Is this message "fresh", or a replay of an old one?
  - Is the sender bound by this message (non-repudiaton)?