Computer Security: Intro

Bart Jacobs

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

Version: fall 2011

Outline

About this course I

Lectures

- Weekly, 2 hours, monday early morning
- Presence not compulsory . . .
  - but active attitude expected, when present
- Lectures based on own slides
  - Updated version, slightly different from slides used last year
- 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: `www.ru.nl/ds/education/courses/security-2011/`
  - Slides will appear there

About this course II

Exercises

- Compulsory, make up half of final mark
- Also weekly meetings, on thursday mornings
  - Answers, for old exercises
  - Questions, for new ones
- Assistants: Flavio Garcia & Pim Vullers
- You may work in (stable) pairs
- Schedule:
  - New exercise on the web on monday
  - Next thursday for questions
  - Next monday: hand-in, by email
- Exercises URL on lectures page.

About this course III

Examination

- Final mark is average (each 50%) of:
  - Average of markings of exercises
  - Final, written exam (January)
- Mark of written exam must be at least 5.
- Re-exam of written exam in spring
- If you fail again, you must start all over next year (including re-doing new exercises)

About this course IV

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, "*schakelaars*", artificial intelligence, mathematics, . . .
- Requires some flexibility
  - but computer security is inherently multidisciplinary

About this course V

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 will be told
  - they can be misinterpreted, out of context

About this course VI

Topics

- Basic notions: confidentiality, integrity, availability (jointly known as: CIA of information security)
- Basic techniques: encryption, both symmetric (shared secret key) and asymmetric (public key)
- 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)

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 conncections with legal issues
  - Esp. information science students are encouraged to follow the "computer law" course in the Law Faculty

Computer security @Nijmegen

Research

- Security important research topic at Nijmegen
- Focus on smart cards, in various forms
- Much theoretical research, eg. on 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 *Kerckhoffs* master programme
  - Jointly between Nijmegen, Twente and Eindhoven
  - Also open to Math. & AI students

What is *computer Security* about?

Computer Security is about regulating access to (digital) assets

Key issues

- assets: the valuables that need protection
- 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 an 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!

Serious, difficult questions

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. Formalization only makes your assumptions explicit
   - There is no reason an attacker will do what is assumed

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)
  - Tamper-resistant/proof hardware
- Organisational measures
  - Examples: chipknip, banking, rocket launch (eg. from submarine)
  - *three B's*: burglary, blackmail, bribery
- Legal measures
  - Penal law: computer criminality laws
  - Civil law: user agreements (eg. for bank/travel cards)

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

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).

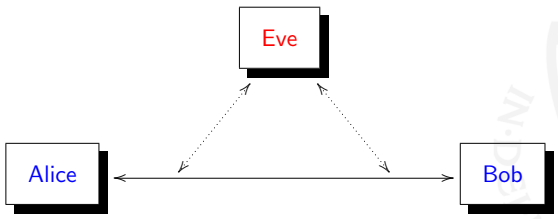
Example legal text snippet

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.

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:** Alice and Bob are certain about each other's identies. In particular, Alice (say) is not talking to Eve, while she thinks she is taking 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.
- **Accountability:** There is a reliable log of the communication history (of Alice, Bob, Eve, et al)

Security & safety

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

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 discplines

- 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
- 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
  (non of the above; often crucial in world history, like in Enigma, Zimmerman 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: NSO

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.

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 of security standards
  (Green book, common criteria, etc.)
- Strong operational security culture
  (including clearances/background checks)
- Slowly getting more open, relying on COTS, open source etc.

Towards proper protection in five steps

1. Make a list of your assets that need protection
   - include the relevant security goals (like CIA)
   - possibly with an informal ranking of required protection levels (like *high*, *medium*, *low*)
2. Make a threat analysis
   - who may wish try to do undermine which security goal? (*attack trees* may be useful tool)
   - what attack resources are assumed? (eg. funding, strength)
   - what are the risks? (eg. risk = probability * impact)
   - non-technical approach, so far
3. Design a security architecture, describing how to counter the identified threats
   - Still at a high level of abstraction
   - Eg. use strong authentication for employees

Towards proper protection in five steps

5. Get your architecture implemented
   - At this stage the technicalities really matter
   - Software correctness/security often more critical than cryptography
   - Modular approach to be preferred (for easy updates and avoiding lock-ins)
   - Distrust closed/proprietary solutions
6. Assessment of all of the above points 1-4
   - by an independent party
   - repeated regularly: "security is like fruit: it goes off quickly"
   - what guarantees can you reasonably expect?

Security is not a static state of affaires, but is dynamic

(More on this in master course "security in organisations")

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)**
$\mathsf{CK} \longrightarrow \mathsf{C} : \mathsf{IdNr}$	$\mathsf{CK} \longrightarrow \mathsf{C} : K\{\mathsf{IdNr}\}$ (K is shared crypto key)
(3) Sequence number	**(4) Challenge-response**
$\mathsf{CK} \longrightarrow \mathsf{C} : K\{N+1\}$ (N is last used number)	$\mathsf{CK} \longrightarrow \mathsf{C} :$ "open" $\mathsf{C} \longrightarrow \mathsf{CK} : K\{N\}$ $\mathsf{CK} \longrightarrow \mathsf{C} : K\{N+1\}$

(Look for Keeloq for more information on actual attacks)

What you need to learn in this course

Paranoia!

- *Professional* paranoia, not *personal*
- For instance, when you receive an email ask yourself:
  - Do I know for sure who it comes from (authenticity)?
  - Who may have seen this email (confidentiality)?
  - Is this the version that the author sent (integrity)?
  - Is the sender bound by this message (non-repudiaton)?

Further introductory material

- Read yourself: Ross Anderson's 2^{nd} edition: Chapter 2: Usability and Psychology
  - www.cl.cam.ac.uk/~rja14/Papers/SEv2-c02.pdf
  - Part of the first assignment is to read this chapter!
- And watch Bruce Schneier at TED:
  - http://www.ted.com/talks/bruce_schneier.html