Computer Security: Intro

Bart Jacobs

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

Version: fall 2010

Outline

About this course I

Lectures

- Weekly, 2 hours, on monday early evening
- Presence not compulsory . . .
  - but active attitude expected, when present
- 8 lectures planned:
  - In november: 8, 22, 29 Note: not on 15 nov!
  - In december: 6, 13
  - In january: 3, 10, 17
- Own slides as main course material
- Additional material on ad hoc basis (from the web)
- Up-to-date info (bookmark; accessible via my webpage) at: www.ru.nl/ds/education/courses/huygens-security-2010/

About this course II

Exercises

- Not compulsory, but extremely useful
- No exercise course foreseen; will be planned later
  - Answers, for old exercises
  - Questions, for new ones
- Assistant: Pim Vullers
- You may work in (stable) pairs
- Exercises URL on lectures page.

About this course III

Examination

- Written exam, fully determining your mark
- Date: 24 jan. 2011, 17:30-19:30
- Place: Hg00.307 (same as lectures)
- Re-exam of written exam in spring (??)

About this course IV

Some special points

- You can fail for this course!
  (I know, it's extremely unfair)
- 3ec means $3 \times 28 = 84$ hours in total
  - Let's say 14 hours for exam
  - 70 hours for 8 weeks means almost: 9 hours per week!
- Large, mixed audience, from whole faculty (except computer/information science) . . .
  - requires some flexibility
  - but computer security is inherently broad & multidisciplinary
- Not everything is publicly known (like e.g. in algebra)
- Some things are simply illegal: don't try this at home!
- The course will *not* be recorded on video

About this course V

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
- Underlying mathematics (cryptography) is used as tool box, not topic of study in itself
  - But very basics are included (substitution, transposition, RSA)

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. computer/cyber crime, but also copyright etc.
- A special *Kerckhoffs* master programme
  - Jointly between Nijmegen, Twente and Eindhoven
- Security, eg. smart cards, important research topic at Nijmegen

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?

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
  - Civial 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.*

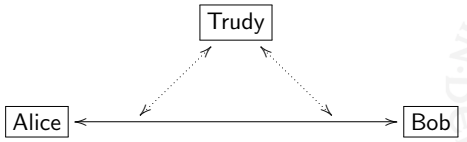
German constitutional court (*Bundesverfassungsgericht*)

Interesting verdict in 2008, explicating a new right from the German constitution:

> *Constitutional right to the confidenatiality and integrity of information technology systems.*

Intrusion schematics

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



Aspects of intrusion

The intrusion of Trudy 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

- Confidentiality: Trudy cannot read the content of what Alice and Bob are communicating.
- Integrity: Trudy 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 Trudy, while she thinks she is taking to Bob.
- Availability: Trudy 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, Trudy, et al)

Security & safety

- Important conceptual distincition. In Dutch more subtle
  - *beveiliging*
  - *veiligheid*
- 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 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

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

- 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
  - External: CIA
  - Sigint: NSA $\geq$ FBI + CIA
- UK
  - Internal: MI5
  - External: MI6 (aka. SIS)
  - 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.

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.

Security in other science disciplines

- **Chemistry**
  - Storage & protection of sensitive (poisonous/explosive) substances
  - ??
- **Biology**
  - viruses etc. for biological warfare (production/storage/...)
  - genetically modified plants/animals
  - ??
- **Physics**
  - Nuclear material
  - ??
- **Mathematics**
  - cryptographic algorithms
  - ??

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)

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`
  - The first assignment is to read this chapter!