Introduction to Communications Security

Markus Peuhkuri

2005-01-18

Lecture topics

- How to complete course
- Basic topics on security
- Risk estimation
- What should be protected
- Why security fails

Course organisation

- Lectures on Tuesdays 10-12 at hall S2
  - slides in English[1]
  - lecture in Finnish
    ⇒ you are welcome to ask questions at lecture break and after
- Some questions available on net after lecture
  - true/false
  - if you have answered correctly (limit yet to define) within a week from lecture, you will get 1–2 points for exam
- Some hands-on exercises at second half
  - three or four groups on Wednesdays
  - unsure about personnel, subject to be cancelled
- Exam Wed 11th May 9-12 S1
  - probably five questions
  - focus on key concepts, not too many details
  - example questions will be provided by end of course
- Course web page `http://www.netlab.hut.fi/opetus/s38153/` definitive source
- Updates announced also on opinnto.sahko.s-38.tietoverkkotekniikka
- Urgent messages by email (make sure that you enrol with topi)
- Markus Peuhkuri
  - Markus.Peuhkuri@tkk.fi
  - reception after lecture

[1] Avaintermit myös suomeksi.

Course material

- Study book
  - Ross Anderson: Security Engineering — A Guide to Building Dependable Distributed Systems Some copies available from library.
  - Matt Bishop: Introduction to Computer Security
  - Matt Bishop: Computer Security — Art and Science Some copies available from Helsinki University.

  The book by Ross Anderson has more engineering approach and covers large set of practical security related aspects and examples. Matt Bishop has more focus on formalism (more computer science than networking).
- Lecture notes
  - batch(es) will be available by Edita
  - available from web page by Monday afternoon
- Additional material
  - provides updated material compared to books
  - batch(es) will be available by Edita
  - available as links from web page (Some may be available only from hut.fi-domain).
- Note that you are *not allowed to print with TKK printers*
  - available on web pages to benefit those who read on-screen or print with their own or friends printer
- All material (expect books) is available for self-service copying by course bulletin board
  - *only one set* will be provided!

Topics covered on course

- Generic introduction to security
- Fundamental concepts in information security
- Security in communications networks
  - fixed
  - mobile, wireless

Some headlines

- Davie-Besse nuclear reactor control network was disabled by Slammer worm in 2002
- Blaster worm delayed power grid measurment information and was one component for North-East US blackout in 2003
- Panix.com[2] lost control for its domain resulting all emails of its customers to directed to third party in January 2005
- 30,000 personal records stolen from George Mason University
- Group stole USD 1.5 million worth from Wal-Mart using fake bar-codes
- A cracker had access to T-Mobile network for 7 months and had access to personal information, photos and FBI documents
- UK woman cannot sleep because someone stole remote control for her brain implant, possibly surgery needed to replace device.

[2]Large ISP in NY

Key terms

Security system is designed to prevent unwanted events. This can be a preventive or one that has a deterrence effect.

Intentional actions are those that are of interest from security perspective. Unintentional actions are handled by safety systems. In some cases safety systems prevent also intentional attacks (and security systems some unintentional unanticipated events) but the evaluation principle is a different.

Defender is the one protecting assets.

Attacker performs intentional unwarranted actions. Note that this should not have any moral loading: for example the law enforcement may be the one that attacks on communications of organised crime.

Attacks are ways to break security system.

Assets are the objects that Defender wants to secure.

Countermeasures are security mechanisms the Defender implements to protect assets.

Components of information security

Confidentiality is the concealment of information[3]

- patient records can be read only by those giving treatment

Integrity is trustworthiness of data[4]

- data integrity
- origin integrity (authentication)
- a bank must have integrity over it account records

Availability is the ability to use the information when desired[5]

- a stock broker must have access to trading system

Security is about tradeoffs

- Install a lock on a front door — have a risk forgetting key
- Install a burglar alarm — annoy your neighbourhood
- Use passwords on computers — forget it after vacation
- Use encryption for you photos — loss them for ever if you forgot the key pass phrase
- Have a low limit on credit card — have to spend nights in budget hotels
- Use encryption for a web site — need a faster computer

Five-step evaluation of security mechanism[2]

1. What assets are you trying to protect?
2. What are the risks to these assets?
3. How well does the security solution mitigate those risks?
4. What other risks does the security solution cause?
5. What costs and trade-offs does the security solution impose?

[3] luottamuksellisuus
[4] eheys
[5] saatavuus

Example: protecting exam

Protecting exam questions by writing questions on lecturer's laptop on which no-one other has access

1. Exam questions.
2. If a student learns the five questions she won't learn whole area of course and gets a good grade without merit.
3. Provided that the computer security is solid and laptop is not stolen, no student has possibility to learn questions.
4. The exam questions will be lost if laptop is stolen, gets broken, or lecturer forgets it home on exam day. ⇒Students will get bad questions. The laptop is an interesting target for a student and thus other documents in laptop may lose their confidentiality.
5. The laptop cannot be borrowed. Lecturer must take extra care of it and must remember not to backup the exam to server.

Enforcing that only each student answers only for himself

With online exam, implement authentication mechanism so that a student can answer only for himself and the other student cannot answer for him. Or a student cannot learn right answers by using other students student id. Solution: send email with authentication token to student's email address and accept only right token.

1. The answering situation is fair for each student and the other student cannot answer on behalf of the other student.
2. One student could try to use dummy student id and learn answers or other student could share answers to other student.
3. For the first risk, using dummy student id, this works. For the other risk, this does not help: it would be possible to ask fellow student who would not plan to participate to the course to register for course, and forward authentication token that can be used to learn answers.
4. Some student may want to break in server to learn how key is calculated.
5. If there are problems with email, a student cannot answer to questions.

A Threat can be a Risk

Threat is a potential way to subvert security

Risk is probability of threat and serious of threat

- Different threats in case of break-in to home computer:
  1. using computer to send spam or taking part of DDOS
  2. extracting CC numbers and personal details[6]
  3. deleting all documents, including family photos
  4. distributing family photos around net
  5. publishing company-secret documents

  Depending on situation, the last item could be the most serious, however depending if backups are taken or types of pictures, third or fourth would be greatest risks while the most probable risk would be the first one.

[6] In US, identity thief is a large scale problem: it is estimated that about one million people are victims of some degree of identity thief annually and the trend is growing.

Some risk estimation

- Which animal is the most dangerous (based on number of deaths in US)
  - deer
  - dog
  - pig
  - shark
  - snake

  1. deer (135)
  2. dog (18)
  3. snake (15)
  4. pig (?)
  5. shark (0,6)

- The most probable cause of death 2000-2003 (in US)
  - air plane accident
  - diabetes
  - flood
  - hit by thunder
  - murder
  - road accident
  - terror attack
  - train accident

  1. diabetes (68 000)
  2. road accident (41 000)
  3. murder (15 600)
  4. terror attack (1 000)
  5. air plane accident (631)
  6. train accident (530)
  7. flood (139)
  8. hit by thunder (87)

- The most probable cause of death 2000-2002 (in Finland)
  - accidentals falls and stumbles
  - asthma
  - cancer in respiratory organ (lungs, throat)
  - diabetes
  - drowning
  - influenza
  - murder, manslaughter
  - pneumonia
  - poisoning accidents (excl. alcohol)
  - road accident
  - suicides
  - water transport accident

  1. pneumonia (41 / 100,000)
  2. cancer in respiratory organ (lungs, throat) (32)

3. suicide (21)
4. accidentals falls and stumbles (18)
5. diabetes (9.2)
6. road accidents (7.2)
7. poisoning accidents (excl. alcohol) (3,4)
8. drowning (2.7)
9. murder, manslaughter. (2.7)
10. asthma (1,8)
11. water transport accidents (1,2)
12. influenza (1,2)

Common pitfalls for risk estimation

- Underestimate risks that one takes often (and voluntary)
- Overestimate risks that one cannot have any impact on or that are rare, or spectacular
- Risks that are personified are perceived to be higher; J. Stalin: "*A single death is a tragedy, a million deaths is a statistic.*"
- Unusual events have news coverage and people think those as higher risks

Threat scenario may change

- Implementing a new security mechanism, a new threat may become significant risk
  - implementing mandatory stopper device reduced number of car thief, but increased number of carjackings
  - moving from analog mobile phones to GSM virtually ended phone cloning and increased use of stolen credit cards to get prepaid cards

Different assets

Money is traceable as long it is bits in computer systems; unmarked cash is anonymous

Information can be stolen[7], but most often it is just copied. Information that has leaked is impossible to get back with 100 % confidence.

Reputation of organisation is in many cases lost with defacement.

Uninterrupted operation of web site or network can be threatened by an extortionist, a competitor, or opposing group.

Four different attackers

Vandals are in large numbers. Should not be a problem for proper administration unless serious vulnerability emerges with ready-made exploit.

Ordinary criminals do not care what system they break in, as long it is useful (for SPAM, DDOS) or contains valuable data (CC numbers with details, SS numbers).

Advanced criminals target specific systems, based either on assignment or opportunistic. Quite often has significant part of social engineering.

Governments or terrorists are often well-funded and have possibility to deploy/blackmail insider.

[7] So that original owner does not have it anymore.

Four different targets

Any account on any system to be used as step-stone for further attacks or just one resource for file storage and communications.

Any account in one domain to change external attack inside attack, possibly inside firewall perimeter.

Any account in one system that has proper protection makes possible to get desired information or a step closer for privileged account.

Target account on target system that has valuable assets.

Steps on security

Prevent implement mechanisms to prevent

Detect have mechanism to identify security breach after-the-fact

Respond take corrective steps; try to remove any benefit from attack

Detecting and responding will have have a detering effect. Nothing prevents a bank clerk to put money in her pocket from the bank safe. However, this will be detected at some point when accounts are matched and evidence could be found from surveillance camera, for example.

Why bad security?

- Security implemented as add-on to completed system
  - system too complex to evaluate
- System purpose not one advertised
  - terrorist screening system helps for airline revenues
- Environment changes
  - closed system interconnected to other systems
  - system gets new functionality and becomes enticing target
  - technological advances
  - identifying token becomes authentication token, for example
- Wrong threat model
  - is fraud external or internal
- Security is not revarded
  - a shop does hand out revard money from CC companies to cash keepers
    $\Rightarrow$ no motive to risk question customer
- Designers or operators do not suffer on security failures
- Security system must be disabled to get work done

Why programs fail?

- Any large program has bugs: industry average 20-30 bugs/KLOC[8]
  - Apache httpd 2.0: 50 KLOC
  - Mozilla 1.7: 1,600 KLOC
  - Linux 2.6: 5,700 KLOC[9]

[8] bugs / 1000 lines of code
[9] Based on a study, error rate 0.17 bugs/KLOC

  - Windows XP: 40,000 KLOC

- Most bugs will not harm during normal course of operation
  - in most cases, when a buggy code is executed, the bug does not show up. For example, the bug may appear with only some very strange arguments to function or if the input is badly malformed. Or there is some dead code (code that is newer executed under normal operation of prgram).
    $\Rightarrow$ the program will fail only with small probability $P \ll 1$

- Exploiting bugs: make program fail every time $P = 1$
  - attacker can select suitable set of inputs to program that gives wanted result
  - in many cases attacker can test on ones own system until the attack succeeds and possibly goes undetected

  In normal course of testing, the program is tested against specification. This states what kind of inputs there are for program and what it should output. The test may fail to stress program with combination of inputs.

- It is hard to add security for a complex program
  $\Rightarrow$ security must be a design principle from start

Security is about the weakest link

- It dows not matter how many strong other parts are
- Attacker can focus on the weakest link
- When removing the weakest link, one must make sure not to introduce another one

authentication		firewall			
user	applications	OS	hardware	network	firewall application

Why adding more security measures may make systems less secure[1]

1. Common-mode problem: new items must be truly independent. If there is a common component, then a failure in it will result all dependet systems to fail.
2. Shirking problem:[10] someone or something other has checked it already. A strange email — but the antivirus software does not alert on it, so it must be safe to open.
3. Overcompensation problem: safer system enables more risks. Because we have firewall, we can decide not to deploy latest batches on computers before we have time to test that they do not cause any problems for our applications.
4. Dedicated worker problem: if security measure get in the way, they will be defeated

Summary

- You know how to complete course?
- Basic terminology for security
- Evaluating security risks
- Common failures

[10] Also known as "bystander apathy"

References

[1] Don Norman. Why adding more security measures may make systems less secure. *RISKS-LIST: Risks-Forum Digest*, 23(63), December 2004. URL:`http://catless.ncl.ac.uk/Risks/23.63.html`.

[2] Bruce Schneier. *Beyond Fear*. Copernicus Books, 2003.