Introduction to Communications Security

TkL Markus Peuhkuri

2006-03-13

Lecture topics

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

Course organisation

- Lectures on Tuesdays 8-12 at hall S3
  - slides in English*
  - lecture in Finnish
    ⇒ you are welcome to ask questions at lecture break and after

Avaintermit myös suomeksi.

- Optional, and maybe hands-on laboratory works
- Exam Tue 8th May 13-16 S3
  - is day ok?
  - probably five questions
  - focus on key concepts, not too many details (what is fifth bit from left in figure 4.2)
  - earlier exams are available

What information to follow

- Course web page `http://www.netlab.tkk.fi/opetus/s383153/` definitive source
- Changes 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

Who should take this course

- Anyone interested about communications security
  - vendor
  - network operator
  - organisation having ITC systems
  - end user

- Who should *not* take this course
  - if you have done T-110.4200 (or .4206)
  - you cannot have both on your degree
  - interest on personal course (1-2 cr) on networking security?

Course material

- Study book
  - Ross Anderson: Security Engineering — A Guide to Building Dependable Distributed Systems Some copies available from library, and also available as PDF
  - 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 a 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
  - information content mostly identical to 2005 slidesbut there are lot of small changes.
- 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 tkk.fi/hut.fi-domain).

Course material – 2

- 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 (except books) is available for self-service copying by course bulletin board at G2 wing
  - *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 measurement information and was one component for North-East US blackout in 2003
- Panix.com[1] 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, lost of other cases where a stolen laptop, lost USB key, CD-ROM, or tape has contained even hundreds of thousands personal details.
- A cracker had access to T-Mobile network for 7 months and had access to personal information, photos and FBI documents
- Computers on intensive care unit in Seattle hospital were part of botnet: as they attacked on other systems, they were themselves unusable resulting hospital to revert manual methods.
- Large networks (of thousand users) are shut down because of virus infections: use typewriters
- False security alers cause lots of expenses
- Doplhin Stadium (Super Bowl XLI) web site had malicious code

Computer security problems history

- The earliest computer-aided fraud: National City Bank of Minneapolis, 1966
- The earliest external intrusion: Federal Energy Administration, 1972
- The earliest large-scale identity theft breach: TRW Inc., June 1984
- "If you stand in front of a mirror and you don't like what you see, it does not help to fix the mirror" – Vint Cerf
  ⇒ Internet and computer (in)security is reflection of rest of society

Key terms

Security system * is designed to prevent unwanted events. This can be a preventive or one that has a deterrence effect.	turvajärjestelmä
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.	tahalliset teot
Defender * is the one protecting assets.	puolustaja
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.	hyökkääjä
Attacks * are ways to break security system.	hyökkäys
Assets * are the objects that Defender wants to secure.	kohteet, arvot
Countermeasures * are security mechanisms the Defender implements to protect assets.	vastatoimet

Information security areas

Confidentiality * is the concealment of information — luottamuksellisuus

- patient records can be read only by those giving treatment

Integrity * is trustworthiness of data — eheys

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

Availability * is the ability to use the information when desired — saatavuus, käytettävyys

- a stock broker must have access to trading system

Security is about tradeoffs

- Install a lock on a front door — have a risk forgetting the 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

Evaluation of security mechanism

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?[2]

Example: protecting an 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.

[1]Large ISP in NY

Enforcing that only each student answers only for himself

With online exam, implement an 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 an email with an authentication token to student's email address and accept only the 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 a fellow student who would not plan to participate to the course to register for course, and forward the 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[2]
  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.

How to estimate risks

- Common threats are easier evaluate
  - flooding, blackouts
  - email viruses
- Infrequent or low probability is difficult
  - half the time, one quarter of the time, one eighth of the time, almost never
  - one out of million is about the same as one out of billion
- Some events are easier to remember
  - are there more Finnish words with 'n' as first character than 'n' as third character?

[2]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.

Mistakes in risk estimation

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

Threat scenario may change

- Implementing a new security mechanism, a new threat may become a 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[3], 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 (0-day 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.

Four different targets

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

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

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

Target account on target system that has valuable assets.

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

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 deterring 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 the accounts are matched and evidence could be found from a surveillance camera, for example.

Why bad security?

- Security implemented as add-on to completed system
  - system is too complex to evaluate
  - security is not part of process
  - process does not exist
- Security seen as technical problem
- System purpose not one advertised
  - terrorist screening system helps for airline revenues
- Environment changes
  - a closed system interconnected to other systems
  - interaction of systems
  - the system gets new functionality and becomes enticing target
  - technological advances
  - an identifying token becomes an authentication token, for example
- Wrong threat model
  - is the fraud external or internal
- Security is not rewarded
  - a shop does hand out reward money from CC companies to cash keepers
    $\Rightarrow$ no motive to annoy by questioning 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[4]
  - Apache httpd 2.0: 50 KLOC
  - Mozilla 1.7: 1,600 KLOC
  - Linux 2.6: 5,700 KLOC[5]
  - Windows XP: 40,000 KLOC
- Most bugs will not harm during the normal course of operation

[4] errors / 1000 lines of code
[5] Based on a study 2005, the error rate was 0.17 bugs/KLOC

  - in most cases, when a buggy code is executed, the bug does not show up. For example, a bug may appear only when some very strange arguments are supplied to a function or if a input data is badly malformed. There may be some dead code that is newer executed under normal operation of program.
    $\Rightarrow$ the program will fail only with small probability $P \ll 1$

- Exploiting bugs: make the 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
  - for any non-trivial program, there is no possibility for exhaustive testing for all inputs and states

  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 the beginning

Security is about the weakest link

- It does not matter how many strong the other parts are
- Attacker can focus on the weakest link
- When removing the weakest link, one must make sure not to introduce another one
- Security is just one aspect of quality

authentication		firewall			
user	applications	OS	hardware	network	firewall application

Adding security measures

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 systems depending on it to fail.
2. Shirking problem:[6] 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 the latest patches on computers before we have time to test that they do not cause any problems for our applications.
4. Dedicated worker problem: if a security measure get in the way, it will be defeated

Summary

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

[6] 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.