Communications security basics

TkL Markus Peuhkuri

2008-03-18

Lecture topics

- Basic components of communications security
- Threats
- Policy and mechanisms
- How to build security and assurance
- Are there any limits in deploying security
- Social engineering — is a human the weakest link

After this lecture you should know basic conectpts and limitations of information security

Confidentiality

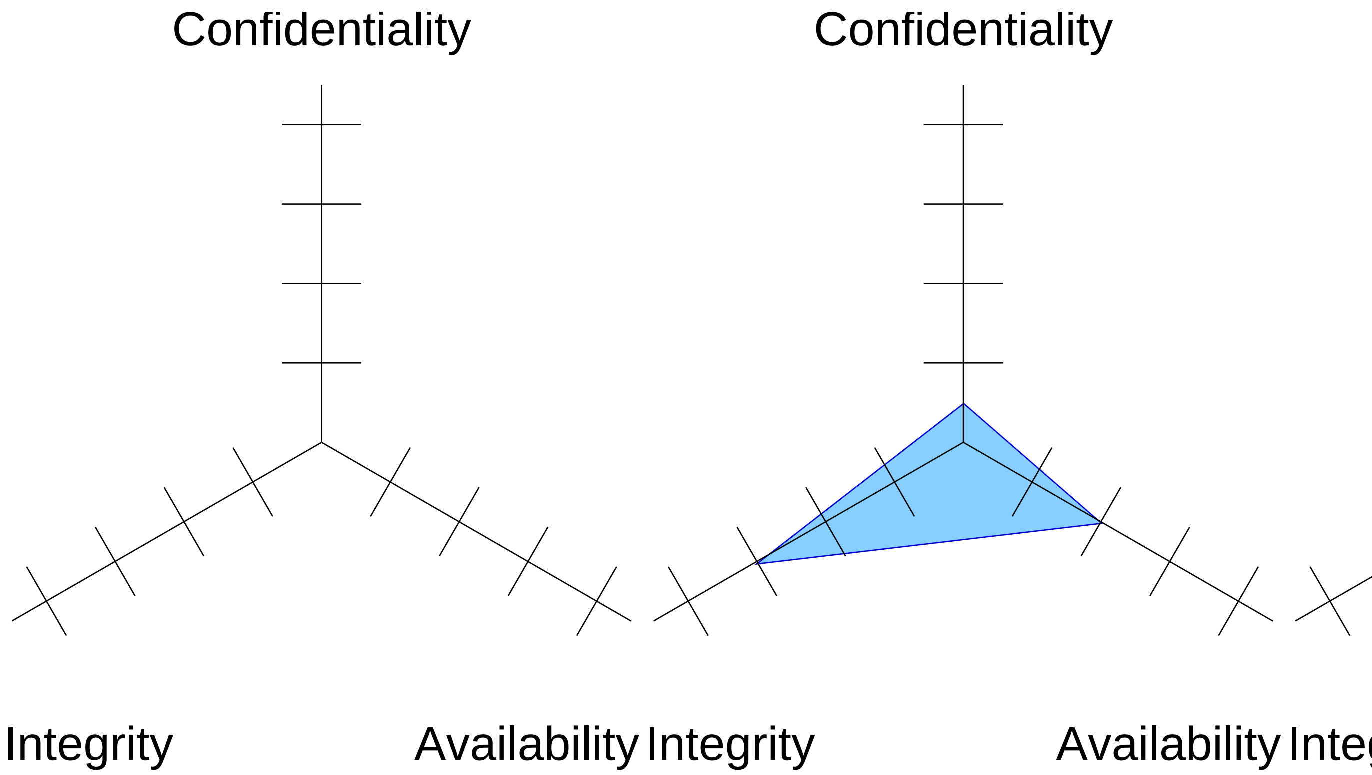
- Concealment of
  - information
  - resources
- Enforced by access control
  - cryptography
  - control mechanisms, such as on operating systems or physical locks
  - hiding
- Trust on underlying systems required
- Because of the nature of an information, only prevention
  - keys and certificates can be revoked

Integrity

- Trustworthiness of
  - information
  - resources
  - source
- Mechanisms

  prevention by disabling any unauthorised change on data, by using read-only media. For example rules for computerised bookkeeping in Finland require that data is written periodically on CD-R media.

  detection will tell if data is still trustworthy: in some cases it can be detected how information was modified while usually it is just an assertion.



Availability

- A system design principle
  - usually against hardware or software failures: for highly reliable systems there may be multiple independent software implementations running on different hardware that vote for the right action.
  - attacker would manipulate environment
- In many cases, the easy attack
- Can be used to facilitate other attack. A possible attack would be overloading the server for certificate revocation lists: users could not check for revoked certificates and would accept a compromised certificate.
- Unforeseen sequence of events. For example, many computing facilities had their backup generators started on Manhattan after 9/11. However, the air intakes were clogged-up with dust and fuel refills could not be delivered in time resulting power outage.

%	per year	per day
99	3d 15h 36m 0s	14m 24s
99,9	8h 45m 36s	1m 26s
99,99	52m 33s	8.6s
99,999	5m 15s	0.9s
99,9999	32s	0.1s

Solving CIA triangle

- Each area may have different weight
- Even same data on different times

Threats in communications

- Disclosure* — data is exposed paljastuminen

    - snooping
    - passive wiretapping
- Deception* — invalid data is accepted erehdyttäminen
    - modification of information
    - active wiretapping
    - masquerading* tekeytyminen
      ⇒ delegation is authorised masquerading
    - repudiation of origin
    - denial of receipt
- Disruption* — incorrect operation häirintä
    - delay, causing system to fail possibly more insecure system
    - denial of service
- Usurpation* — resource is used by other entity käyttöönotto, anastus

Policy and mechanism

Security policy * what is allowed and what is not — a statement turvapolitiikka

- may be modelled mathematically
- in most cases, after-the-fact interpretation is needed
- a composite policy, resulting from combining two or more entities (companies, universities, ISPs) security policies can be a very complex one. Various laws may complicate situation further, especially if multiple jurisdictions must be taken into account.

Security mechanism * a method, tool or procedure to enforce policy turvamekanismi

- technical
- non-technical

Prevent — Detect — Limit — Recover

Prevention * make an attack to fail estäminen

- if the threat is an attack from the Internet, disconnect the machine
- access control, secure design, encryption

Detecting * an attack or an attempt havaitseminen

- even if the attack fails, detecting provides information
- monitoring, log analysis, traffic analysis

Limiting * consequences of an attack rajaaminen

- e.g. shuting down infected systems to protect rest
- compartmenting systems makes this easier

Recovering * saves what is left or undoes the damage toipuminen

- stop attack, for example taking the system off-line. In some cases it is not possible to take system off-line because of risks of other damage.
- assess and repair any damage
- can be complicated if it is unsure when compromise took place
- reinstalling system from original install media, while truly paranoid does not trust even hardware anymore (BIOS, harddisk controller has malicious code?).

How we start building security?

- Policy has some *assumptions*
  - what kind of security is needed
  - what is the environment
- System has two kinds of states
  - secure
  - insecure
- Security mechanism disallow change to states of different type
- Assurance is the level of trust
  - specification of desired behaviour
  - analysis if specification is not violated
  - proofs or arguments that desired behaviour is implemented

Building assurance

- Specification is statement of the desired functionality
  - formal (mathematical, specification language) or informal
  - allowed and non-allowed states
- The design compiles into components
  - hardware
  - software
  - operating procedures
- Determine that the design and the specification match
  - mathematically, if designed so
  - using arguments; specifications often woolly
⇒ arguments unconvincing or with limited coverage
- Implementation realises a design that has the desired behaviour
  - proof of correctness is difficult
⇒ testing is the prevailing method to assure design
  - security testing hard: more on later lectures
  - system relies on other components: for example if our program implements the correct design but uses some library that does not work as specified, the specification is not properly implemented.
  - domain boundaries difficult: interactions with users, applications, operating systems, hardware, network, and protocols are potential weak points.

How good security one needs and can afford?

- Cost-benefit analysis
  - securing system should not cost more than value of the data or system protected
  - overlapping benefits
  - where security mechanisms are implemented
- Risk analysis
  - likely ⇔ unlikely

  - serious ⇔ nuisance
  - unacceptable ⇔ acceptable
  - environment: this includes such things if system is connected to the Internet, are system users trustworthy, who are the potential attackers, how valuable the system is as whole
  - prohibited but possible environment changes: for example, a company policy may disallow connecting laptop to home network but if user must transfer some files, he may do it to get his work done.

- Laws, regulation and public relations
  - crypto export and use controlled
  - some level of security mandated by laws. In California, for example, a company must notify customers if there is a reason to believe that their personal data is compromised. On later lectures Finnish laws are covered.
  - problems with multiple jurisdictions
  - publicly acceptable practises
  - loss of reputation ⇒loss of sales

Security in organisation

- How to implement security
- No direct financial rewards
- Security measures result often loss of productivity. If, for example, some operation takes 4 minutes if all security procedures are followed by the book and 3 minutes if some of security mechanisms are disabled, then security measures are not used in "common operations".
- Who is responsible for security?
  - undergraduate trainee
  - computer system administrator
  - CIO: chief information officer*
  - CEO: chief executive officer

  tietohallintopäällikk
  -johtaja

  responsibility without the power is futile
- Sufficient resources
  - knowledgeable system administration
  - employees are trained to understand and use security. There are limits, what user education can do, especially when security breach attempts are rare.
  - information systems security is just one area

Top management must be commited

- Without management support there cannot be real security
  - allocating resources
  - making priorities
  - showing example, that fails often: don't you know who I am?
- Security is just one attribute of quality
- Standards and best practices emphasise management commitment to information security

Implementing security with people

- “Our system is secure, if no-one uses it”
- Outsiders can be detected at the perimeter
- Insiders the difficult part: they
  - have *authority* to use the system
  - have *access* to the system
  - *know* details about the system
- Users must understand why each security measure exists
  - there are limits with user education
  - how to educate every Internet user?
- Well-defined processes and methods help a lot
  - information security is one aspect of quality
- Social engineering age-old con man method[1]

Social engineering*

tekeytyminen, urkinta

- Computers are inflexible, humans adapt[1]
- Some common exploited scenarios
  - tit-for-tat helping (building trust)
  - authority over other party
  - pity, team player
  - greed
  - asking small amount of information at time
- Viruses use also social engineering: many email viruses have a topical subject (celebrity pictures, messages from administration, crab news headlines) and trick users to open attachments
- Phishing[2] is an automated con man. “Phishing” refers to collecting trustworthy information by masquerading to a trusted party, such as bank, eBay or PayPal.

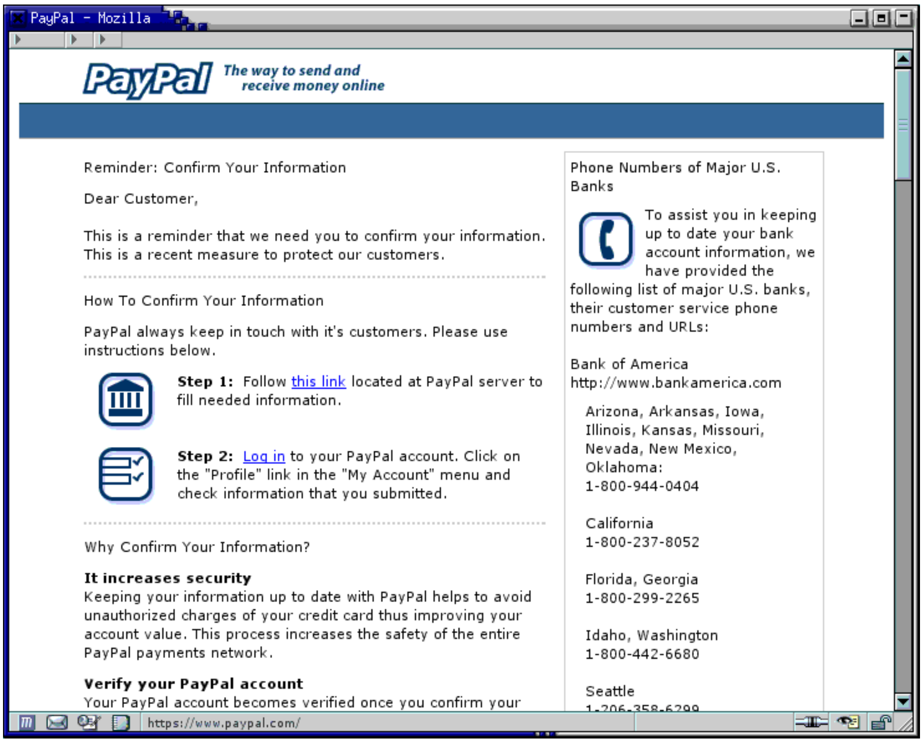
Phishing: fishing for valuable information

- Trick users to reveal valuable information: credit card details, bank or website passwords, personal information
- Spam email messages
- Possibly malicious payload
  - or trick user to download some spy-ware
- Ever larger problem: December 2004 ⇒2005 ⇒2006 ⇒2007 `http://www.antiphishing.org/`
  - 1707 ⇒7197 ⇒28531 ⇒25328 fake sites
  - 55 ⇒121 ⇒146 ⇒144 brands used (91,7 % financial institutions)
  - 180 ⇒340 ⇒269 key-logger crime-ware known
  - fake site on-line for 6 ⇒4 ⇒3 days on average (max 31 ⇒30 ⇒31)

[1] Note, that this is not just a bad thing. A human can make judgement and act on a situation that was not anticipated.

[2] Word “phishing” comes from “fishing” with hacker lingo f⇒ph.

Who's talking?



Reminder: Confirm Your Information

Dear Customer,

This is a reminder that we need you to confirm your information. This is a recent measure to protect our customers.

How To Confirm Your Information

PayPal always keep in touch with it's customers. Please use instructions below.

Step 1: Follow this link located at PayPal server to fill needed information.

Step 2: Log in to your PayPal account. Click on the "Profile" link in the "My Account" menu and check information that you submitted.

Why Confirm Your Information?

It increases security
Keeping your information up to date with PayPal helps to avoid unauthorized charges of your credit card thus improving your account value. This process increases the safety of the entire PayPal payments network.

Verify your PayPal account
Your PayPal account becomes verified once you confirm your

Phone Numbers of Major U.S. Banks

To assist you in keeping up to date your bank account information, we have provided the following list of major U.S. banks, their customer service phone numbers and URLs:

Bank of America
http://www.bankamerica.com

Arizona, Arkansas, Iowa, Illinois, Kansas, Missouri, Nevada, New Mexico, Oklahoma:
1-800-944-0404

California
1-800-237-8052

Florida, Georgia
1-800-299-2265

Idaho, Washington
1-800-442-6680

Seattle
1-206-358-6299

What is between lines (HTML)

- Status-field is updated every 25 ms

  ```
  var boodschap = 'https://www.paypal.com/'; function dgstatus() { window.status = boodschap; timerID= setTimeout("dgstatus()", 25); }
  ```

- Link has an IP address

  ```
  Follow <a href="http://210.78.22.113/verify.html">this link</a> located at PayPal server to fill needed information.
  ```

- PayPal is located in California

  ```
  Domain Name: PAYPAL.COM
  Administrative Contact, Technical Contact: Inc., PayPal (36270680P) hostmaster@PAYPAL.COM 1840 Embarcadero Rd. Palo Alto, CA 94303 US 408-376-7400 fax: 650.251.1101
  ```

- as is `www.paypal.com`

  ```
  www.paypal.com has address 64.4.241.32 OrgName: PayPal OrgID: PAYPAL Address: 303 Bryant Street City: Mountain View StateProv: CA PostalCode: 94041 Country: US
  NetRange: 64.4.240.0 - 64.4.255.255 CIDR: 64.4.240.0/20
  ```

- Information update server (`210.78.22.113`) outsourced to China?

  ```
  inetnum: 210.78.22.64 - 210.78.22.128 netname: SHJITONG-CN descr: JiTong Shanghai Communications Co.,Ltd address: Room 1001,Lekai Builing,Shangcheng Road, address: Pudong Xin district,Shanghai country: CN
  ```

Another phishing

- `From: ITviikko Digilehti <itviikko.digilehti@sanoma.fi>`
- A link to register

  ```
  Rekisteröidy Digilehden lukijaksi
  <A href="http://www.webstudio.fi/itviikko/esittely.html"
  target=_top>tästä</A>
  ```

  Not to `itviikko.fi`?

  ```
  domain:   webstudio.fi
  descr:    SOPRANO COMMUNICATIONS OY
  ```

- Email sender:

  ```
  Received: from mail pickup service by mail.swelcom.fi
     with Microsoft SMTPSVC; Thu, 20 Jan 2005 12:50:28 +0200
  ```

  Possibly compromised server, not **itviikko.fi**?

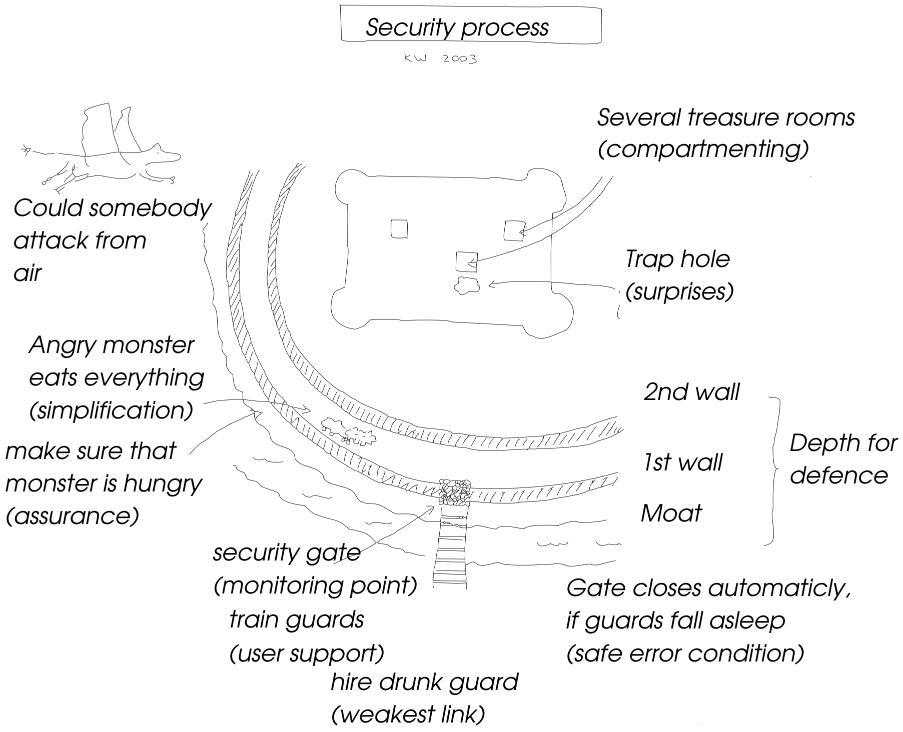
  ```
        domain:   swelcom.fi
        descr:    SWelcom Oy
  ```

Another phishing...

- Thus web address points to somewhere else and email sent by third party
  ⇒ Phishing attack?

I got confirmation that the email was genuine, even if it had all signs of a phishing attack. It is very difficult for an average user to identify which messages are righteous and which are not as technically there is no difference.

One view to security process



Summary

- Security builds with steps

  1. threats
  2. policy
  3. specification
  4. design
  5. implementation
  6. operation and maintenance

- Process is iterative

  1. plan
  2. do
  3. check
  4. act

References

[1] Kevin D. Mitnick, William L. Simon, and William Simon. *The Art of Deception: Controlling the Human Element of Security.* John Wiley & Sons, Inc., New York, NY, USA, 2002.