Communications security basics

Markus Peuhkuri

2005-01-25

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 human the weakest link

Confidentiality

- Concleament 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 nature of information, only prevention
  - keys and certificates can be revoked

Integrity

- Trustworthiness of
  - information
  - resources
  - source
- Mechanisms

  prevention by disabling any unauthorised change on data

  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 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 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

Threats in communications

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

Policy and mechanism

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

- may be modelled mathematically
- in most cases, after-the-fact interpretation needed
- composite policy, resulting from combining two or more entities (companies, universities, ISPs) security policies can be a very complex one

Security mechanism method, tool or procedure to enforce policy

- technical
- non-technical

Prevent — Detect — Recover

Prevention make attack to fail

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

Detecting an attack or an attempt

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

Recovering saves what is left or undoes damage

- stop attack, for example taking system off-line. In some cases it is not possible to take system off-line because of other risks.
- 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 different type state
- 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 desired functionality
  - formal (mathematical, specification language) or informal
  - allowed and non-allowed states
- Design compiles into components
  - hardware
  - software
  - operating procedures
- Determine that design and specification match
  - mathematically, if designed so
  - using arguments; specifications often woolly
    ⇒ arguments unconvincing or with limited coverage
- Implementation realises design that has desired behaviour

- proof of correctness difficult
  ⇒ testing prevailing method to assure design
- security testing hard: more on later lectures
- system relies to other components: for example if our program implements correct design but uses some library that does not work as specified, specification is not properly implemented.
- domain boundaries difficult: interactions with users, applications, operating systems, hardware, network, 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
  - at what point security is implemented
- Risk analysis
  - likely ⇔ unlikely
  - serious ⇔ nuisance
  - unacceptable ⇔ acceptable
  - environment: this includes such things if system is connected Internet, are system users trustworthy, who are potential attackers, how valuable system is as whole
  - prohibited but possible environment changes
- Laws, regulation and public relations
  - crypto export and use controlled
  - some level of security mandated by law. 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

Implementing security in organisation

- 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 security is disabled, those security measures are not used in "common operation".
- Who is responsible for security?
  - undergraduate trainee
  - computer system administrator
  - CIO: chief information officer[1]
  - CEO: chief executive officer

  responsibility without 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.

[1] tietohallintopäällikkö

Implementing security with people

- "Our system is secure, if no-one uses it"
- Outsiders can be detected at 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?
- Social engineering age-old con man method

Social engineering

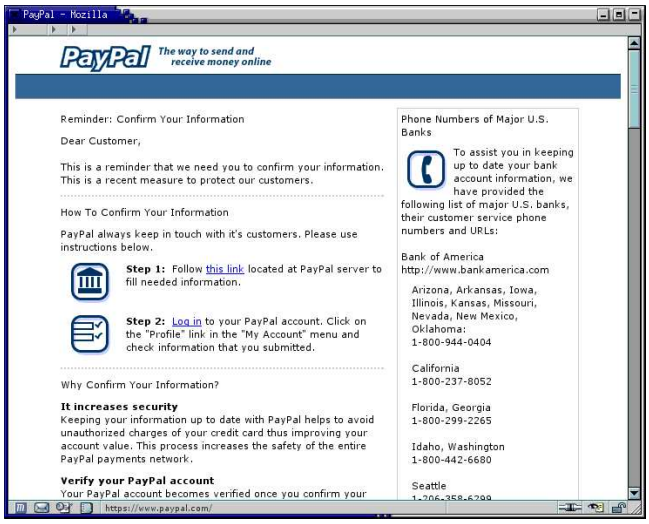
- Computers are inflexible, humans adapt[2]
- Some common exploited scenarios
  - tit-for-tat helping (building trust)
  - authority over other party
  - pity, team player
  - greed
  - asking small amount of information at time
- Viruses use also social engineering: many email viruses have topical subject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

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
  - 1707 fake sites (24 % growth in 6 months)
  - 55 brands used (86 % financial institutions)
  - fake site on-line for 6 days on average (max 30)

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

Who's talking?



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
```

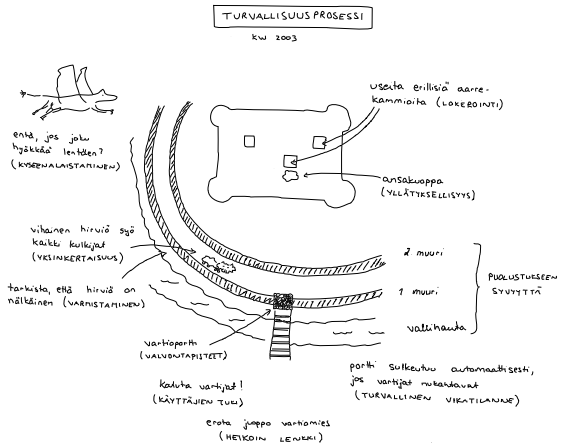
  Possibly compromised server, not **itviikko.fi**?

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

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

I've yet to receive a confirmation, but I think that that email was genuine, even if it had all signs of phishing attack. It is very difficult for an average user to identify which mails 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