Mobile Security

Information Security

Hans Georg Schaathun

University of Surrey

Autumn 2011 – Week 10

Outline

Session objectives

- Have the necessary overview to do a risk analysis for mobile computing platforms

Mobile Equipment

- Portable computers
- Smartphones
- USB sticks

1. Why is mobile equipment used?
2. What are the risks?

Outline

User controlled

- Typically, the user administrates laptops and smartphones
- Lacking competence, constency, and policy awareness
  - contrary to dedicated IT support staff
- Possibly mixing private and organisation data

Easy to lose

- Equipment left behind in Oslo cabs during six months period
  - 400 PDA-s
  - 1700 mobile phnes
  - 110 portable PC-s
- according to Pointsec Mobile Technologies
- USB sticks are even easier to mislay

The risk of theft is on top of that ...

Difficult to control

- A dozen USB sticks
  - used *ad hoc* to transfer data
  - stored in different pockets and drawers
- How do you remember what is stored on which stick?
  - Where are all your sticks?
  - Have you lost one?
- Even as a private user this is difficult
  - how do you deal with 1000 staff each with a dozen sticks?

More exposed

Mobile means leaving the safety of company perimeters ...

- Outside network security perimeter
  - Using public networks
- Outside physical security perimeters

Outline

Sensitive Data on Mobile Units

- Consider sensitive data, e.g.
  - trade secrets
  - personal information
- Some sensitive data (especially trade secrets) are necessary
  - staff need to do research and development on portable units

How do you design a system with controls to protect sensitive information on portable units?

Example 1: Encrypted Hard Drive

- Hard Drive Encryption makes it impossible to read from disk without a secret key
- *What residiual risk remains?*

Residual Risk

Encrypted Hard Drive

An attacker who steals an encrypted hard drive cannot read it.

- What about an encrypted hard drive in a laptop?
- Is the box running with the drive mounted?
- Is the secret key protected by a strong password?
- Is the password cached in memory or swap space?
- Is it possible for to spy out the password or key?

Supplemental Controls

Encrypted Hard Drive

- When the box is suspended or left unattended for even an instant
  - it must be screenlocked
- Furthermore,
  - wipe memory and swap files containing passwords and keys
- Preferably, wipe decrypted data

Note that data may be retrieved from memory by turning off the computer and quickly taking the memory into another device to read. It is not wiped immediately.

Control Example 2

Need to know (need to have)

- Limit available data.
- Only data needed for the work should be stored.
  - Delete data no longer needed
- On a laptop, this may mean
  - only data needed for the next two days/week/month
  - depending on risk analysis
- This requires
  - good policies (what to have and what to delete)
  - awareness and training (remember to delete)

Control Example 3

System Separation

A work computer is for work only.

- Not necessarily efficient
  - easier to work with one system
- But high-risk activities require high-risk awareness
  - and who can keep up that awareness during private surfing?

Control Example 4

Policy, Awareness, and Training

- Due care from the user's side is critical
- Many technical controls require co-operation from user
- Issues include
  - backup
  - upgrades and patches
  - sensible and careful use
  - avoid people peaking during work

Summary of the Case

Note. Ignoring controls which do not specifically adress sensitive information.

1. Encrypted Hard Drives is useful
   - but not sufficient
   - supplemental controls to avoid vulnerabilities
2. Limit the risk by strictly limiting assets on the mobile unit
3. Dedicated system for work reduces risk
4. Many vulnerabilities can be reduced by user awareness training

Outline

Question — Availability

- We have discussed controls to limit sensitivity-related loss
- Now consider loss of availability of data
    - as a result of a lost box
- *What controls would you propose?*

Control 1

Backup

Backup is the most obvious control.

- What challenges are particular for a laptop?
- Not always connected
  - automated, periodical backup impossible
- User cooperation is essential
  - run backup manually
  - or at least connect (if backup system detects connection)
- A professional backup system should sti
  - easy to use
  - as automatic as possible

Control 1

Backup

Backup is the most obvious control.

- What challenges are particular for a laptop?
- Not always connected
  - automated, periodical backup impossible
- User cooperation is essential
  - run backup manually
  - or at least connect (if backup system detects connection)
- A professional backup system should sti
  - easy to use
  - as automatic as possible

Control 2

Markings

- Marking the box with company contact details
  - cheap and simple control
  - will return most boxen left behind
- Special secure markings exist
  - detectible by police

Control 3

Due care

Mobile units are popular objects of theft.

- Don’t be an easy target
- Don’t leave it unattended
- Don’t leave it visible (e.g. in a locked car)

This is – of course – standard advice.

Outline

Mobile and Connected

A mobile unit is insufficient. It must connect to.

- What risks are associated with connecting a mobile unit?
- Use untrusted networks
  - local WiFi for connection
  - global Internet for transfer
- End-to-end encryption is required for most or all services
- Blanket access

Mobile and Connected

A mobile unit is insufficient. It must connect to.

- What risks are associated with connecting a mobile unit?
- Use untrusted networks
    - local WiFi for connection
    - global Internet for transfer
- End-to-end encryption is required for most or all services
- Blanket access

Use of Inhouse Network Services

Every network service exposed to outside (mobile) users pose a risk.

- Don't expose services unnecessarily
- Take care with the access control mechanisms
    - both client and server side
- Encrypted link
- Two-way identification and authentication

Use of External Network Services

All use of external services pose a risk.

- Mobile units do not benefit from
  - corporate firewalls
  - trusted inhouse DNS servers
  - trafic monitoring
  - intrusion detection
- Requires local protection
- Prudent use becomes (even) more critical

Software and OS vulnerabilities

- Laptops may be more vulnerable to software and OS bugs
  - why?
- Can easily miss routine updates from IT support
  - by being off-line
- The user must take some responsibility
- IT support needs a procedure to handle laptops
  - compatible with user work schedule

Software and OS vulnerabilities

- Laptops may be more vulnerable to software and OS bugs
  - why?
- Can easily miss routine updates from IT support
  - by being off-line
- The user must take some responsibility
- IT support needs a procedure to handle laptops
  - compatible with user work schedule

Support Dilemma

for discussion

Should the user have system privileges on his laptop?

Risk 1 The user forgets or are unaware of the latest security patch.

Risk 2 The user misconfigures the system, leaving critical vulnerabiities.

Risk 3 The user is unable to install necessary software that he needs in the field.

Risk 4 The user is unable to reconfigure the network/firewall/etc. to get connected at a client network.

Support Dilemma

for discussion

Should the user have system privileges on his laptop?

Risk 1 The user forgets or are unaware of the latest security patch.

Risk 2 The user misconfigures the system, leaving critical vulnerabiities.

Risk 3 The user is unable to install necessary software that he needs in the field.

Risk 4 The user is unable to reconfigure the network/firewall/etc. to get connected at a client network.

Outline

Summary

- Mobile computing platforms face extra risks
  - loss and theft
  - untrusted networks
  - less reliable IT support
- All of this must be adressed in a risk analysis
- Several controls must be considered
  - awareness and training
  - limited use
  - technical controls, incl. encryption