Computer Security

HUMAN and ORGANISATIONAL FACTORS

Erland Jonsson

Department of Computer Science and Engineering

Chalmers University of Technology

The greatest threat: the Human Being

Why is the Human Being the greatest threat?:

- The Human Being is an integrated part of the system (on several levels, in all phases)
- The adaptation between the Human Being and the system is incomplete and error-prone
- The Human Being is human! (e.g. forgetful unsuspecting, negligent, egoistic, open to bribery, …)

Why is the Human Being the greatest threat? (cont'd)

- We do not really realize this (and in any case we do not act accordingly.)
- We are prejudiced
- We believe that we can solve the problem in a technical way -
  - but in reality we can only improve the odds!

- Example to follow: The use of passwords (remembering/aging/etc)

- We are prejudiced:

  What does hackers look like?
  Maybe like this:

But mostly like this:

Example: Use of passwords

- Intrusion method:
  Guess passwords/Exhaustive search
  (e.g. using the Crack software)

- Where is the vulnerability/Who is to blame?
  - system designer: who constructs the system?
    (password length insufficient, password file readable)
  - customer: who bought insecure software?
  - users:
    - who are choosing bad passwords?
    - who write them down/who give them away?
  - system administrator: for not checking the passwords?
  - the boss: who does not inform/educate his employees?

Example: Use of passwords
How to fix the problem - 1?

- Possible countermeasure 1:
  Generate passwords that could be pronounced and that are easy to memorize! But still being “random”:

  => Result: The sample space was significantly reduced, so it became much easier to guess the password with Crack!!
  (Human deficient conclusions)

Example: Use of passwords
How to fix the problem - 2?

- Possible countermeasure 2:

  Password aging: The system enforces a change after a certain predefined time:

  => RESULT: Users change between two different passwords all the time or “change/change back” immediately.

- Thus: The system “remembers” old passwords and does not accept re-use of a password that has already been in use (the last n times).

  => RESULT: Users change passwords n+1 times each time a password change is enforced!

  (Human laziness/inability to adhere to rules)

ATM PHANTOM WITHDRAWALS

Most fraud and security problems were caused by implementation errors and management failures (Rather than technical attacks and cryptanalysis.)

- No public feedback on how cryptographic system fail!
- Out several hundred problems reported only two were due to “bad” encryption, even though the cryptographic metods used were insufficient.

(Ref: Ross Andersson: “Why cryptosystems fail”, Communications of the ACM,Vol. 37, No. 11, 1994.)

ATM PHANTOM WITHDRAWALS

- "Phantom withdrawals" were mainly due to:
- software errors
  (1 transaction out of 10 000 goes wrong)
- postal interception: accounts for ab. 30% of card losses
- (former) employee fraud
  (1% of GB bank employees are dismissed each year for disciplinary reasons)

ATM PHANTOM WITHDRAWALS

Examples of specific security problems:

- The bank did not check address changes, so a bank clerk could have an extra card (+ PIN code) of a client's account issued to himself. It was also possible to prevent the "false" withdrawals to show up on the account statement.

- One bank had only three different PIN codes. (secret!)

ATM PHANTOM WITHDRAWALS

Examples of specific security problems (con't):

- Two men were "shoulder surfing" in the ATM queue to acquire PIN codes plus taking care of discarded ATM tickets (with the account number!) The system permitted manual entry of account number. (The problem was known and reported several years before.)

- Insertion of telephone card =
  = identical to last card inserted!
- A specific 14-digit sequence (introduced for testing purposes) would output ten banknotes!

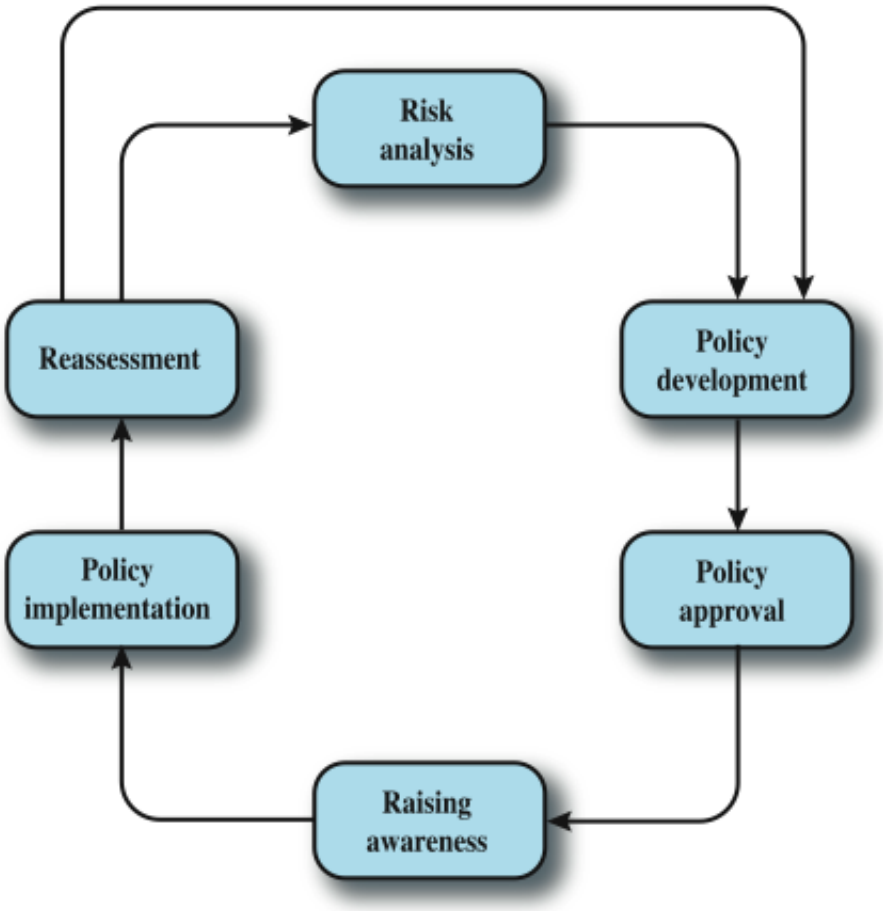
Organizational Security Policy

- "formal statement of rules by which people given access to organization's technology and information assets must abide"
- The term is also used in other contexts

Organizational Security Policy

- need written security policy document
- to define acceptable behavior, expected practices, and responsibilities
  - makes clear what is protected and why
  - articulates security procedures / controls
  - states responsibility for protection
  - provides basis to resolve conflicts
- must reflect executive security decisions
  - protect info, comply with law, meet org goals

Security Policy Lifecycle



Policy Document Responsibility

- security policy needs broad support
- especially from top management
- should be developed by a team including:
  - site security administrator, IT technical staff, user groups administrators, security incident response team, user groups representatives, responsible management, legal counsel

Document Contents - questions

- what is the reason for the policy?
- who developed the policy?
- who approved the policy?
- whose authority sustains the policy?
- which laws / regulations is it based on?
- who will enforce the policy?
- how will the policy be enforced?
- whom does the policy affect?
- what information assets must be protected?
- what are users actually required to do?
- how should security breaches be reported?
- what is the effective date / expiration date of it?

Security Policy Topics

- principles
- organizational reporting structure
- physical security
- hiring, management, and firing
- data protection
- communications security
- hardware
- software
- operating systems

Security Policy Topics cont'd

- technical support
- privacy
- access
- accountability
- authentication
- availability
- maintenance
- violations reporting
- business continuity
- supporting information

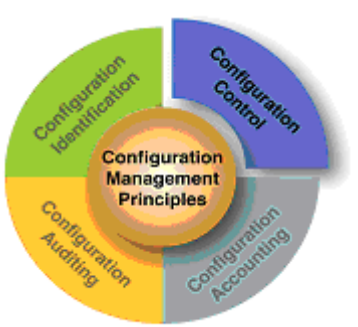
IT Security Plan

- provides details of
  - what will be done
  - what resources are needed
  - who is responsible
- should include
  - risks, recommended controls, action priority
  - selected controls, resources needed
  - responsible personnel, implementation dates

Implementation Plan

Risk (Asset/Threat)	Level of Risk	Recommended Controls	Priority	Selected Controls	Required Resources	Responsible Persons	Start – End Date	Other Comments
Hacker attack on Internet Router	High	1. disable external telnet access 2. use detailed auditing of privileged command use 3. set policy for strong admin passwords 4. set backup strategy for router config file 5. set change control policy for the router configuration	1	1. 2. 3. 4. 5.	1. 3 days IT net admin time to change & verify router config, write policies; 2. 1 day of training for net admin staff	John Doe, Lead Network Sys Admin, Corporate IT Support Team	1-Feb-2006 to 4-Feb-2006	1. need periodic test & review of config & policy use

Change and Configuration Management



- change management is the process to review proposed changes to systems
  - evaluate security and wider impact of changes
  - part of general systems administration process
- configuration management is keeping track of configuration and changes to each system
  - to help restoring systems following a failure
  - to know what patches or upgrades might be relevant
  - also part of general systems administration process

Incident Handling

- need procedures specifying how to respond to a security incident
- reflect range of consequences on the organisation
- codify action to avoid panic

- detect potential incidents
- help personnel to recover quickly
- document breaches for future reference
- use information gathered during incident handling to better prepare for future incidents

Personnel Security: Security in Hiring Process

- objective:
  - "to ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities"
- need appropriate background checks, screening, and employment agreements

Personnel Security: Employment Agreements

- employees should agree to and sign the terms and conditions of their employment contract, which should include:
  - information on their and the organization's security responsibilities
  - confidentiality and non-disclosure agreement
  - agreement to follow organization's security policy

Personnel Security: During Employment

- current employee security objectives:
  - ensure employees, contractors, third party users are aware of info security threats and concerns
  - know their responsibilities and liabilities
  - are equipped to support organizational security policy in their work, and reduce human error risks
- need for security policy and security training
- security principles:
  - principle of least privilege
  - separation of duties
  - limited reliance on key personnel

Personnel Security: Termination of Employment

- termination security objectives:
  - ensure employees, contractors, third party users exit organization or change employment in an orderly manner
  - return of all equipment
  - **removal of all access rights**
- critical actions:
  - remove name from authorized access list
  - inform guards that general access not allowed
  - remove personal access codes, change lock combinations, reprogram access card systems, etc
  - recover all assets

Standards

The ISO/IEC 27000-series is a collection of security standards:

- ISO/IEC 27001 Information Security Management System – Requirements
- ISO/IEC 17799 (= ISO/IEC 27002) Code of Practice for Information Security Management
- ISO/IEC 27003 Information Security Management System implementation guidance
- ISO/IEC 27004 Information Security Management Measurement
- ISO/IEC 27005 Information Security Risk Management

Summary

- introduced some important topics relating to human factors
- organizational security policy
- security plan
- change management
- configuration management
- personnel security