

# Computer Security DD2395

<http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasakh10/>

Fall 2011

Sonja Buchegger

[buc@kth.se](mailto:buc@kth.se)

Lecture 10, Nov. 24, 2011  
Social Engineering

# Course Admin

- GPG Lab 1 bonus results in RAPP
- Master's students: ready for seminar? Many have not signed up yet!
- Lab 3 web attacks: optional sessions and showing your work

# How Social Engineers Work

The social engineer employs the same persuasive techniques the rest of us use every day. We take on roles. We try to build credibility. We call in reciprocal obligations. But the social engineer applies these techniques in a manipulative, deceptive, highly unethical manner, often to devastating effect.

--Brad Sagan, social psychologist

# Social Engineering

Examples taken from:  
The Art of Deception by Kevin Mitnick

# Example Scenarios

- Prepare to answer these questions:
- What is happening?
- How does the social engineer get information/access?
- How could this have been avoided?

# Techniques

# Phases

- Pretexting
- Get data
- Keep connections
- Combine data
- Use it

# What for?

- Industrial spying
- Access to resources
- Data theft
- Identity theft

# Techniques

- Trappings of role
- Credibility
- Forcing the target into a role
- Distracting from systematic thinking
- Momentum of compliance
- Bury questions
- Get pieces from different sources

# More Techniques

- Read victim's openness
- Test with personal information
- Back off, don't burn the source
- Create then fix a problem

# Exploits

- The desire to help
- Attribution
- Liking
- Fear
- Reactance

# Countermeasures

# Countermeasures

- Clear concise protocols that are enforced
- Awareness training
- Simple rules to define sensitive information
- Simple rule that ID required for restricted action
- Data classification policy
- Resistance training
- Testing by security assessment
- Politeness change, “NO” is OK

# Policies

- See Mitnick PDF

# Human Factors

important, broad area

consider a few key topics:

- security awareness, training, and education

- organizational security policy

- personnel security

- E-mail and Internet use policies

# Security Awareness, Training, and Education

prominent topic in various standards

provides benefits in:

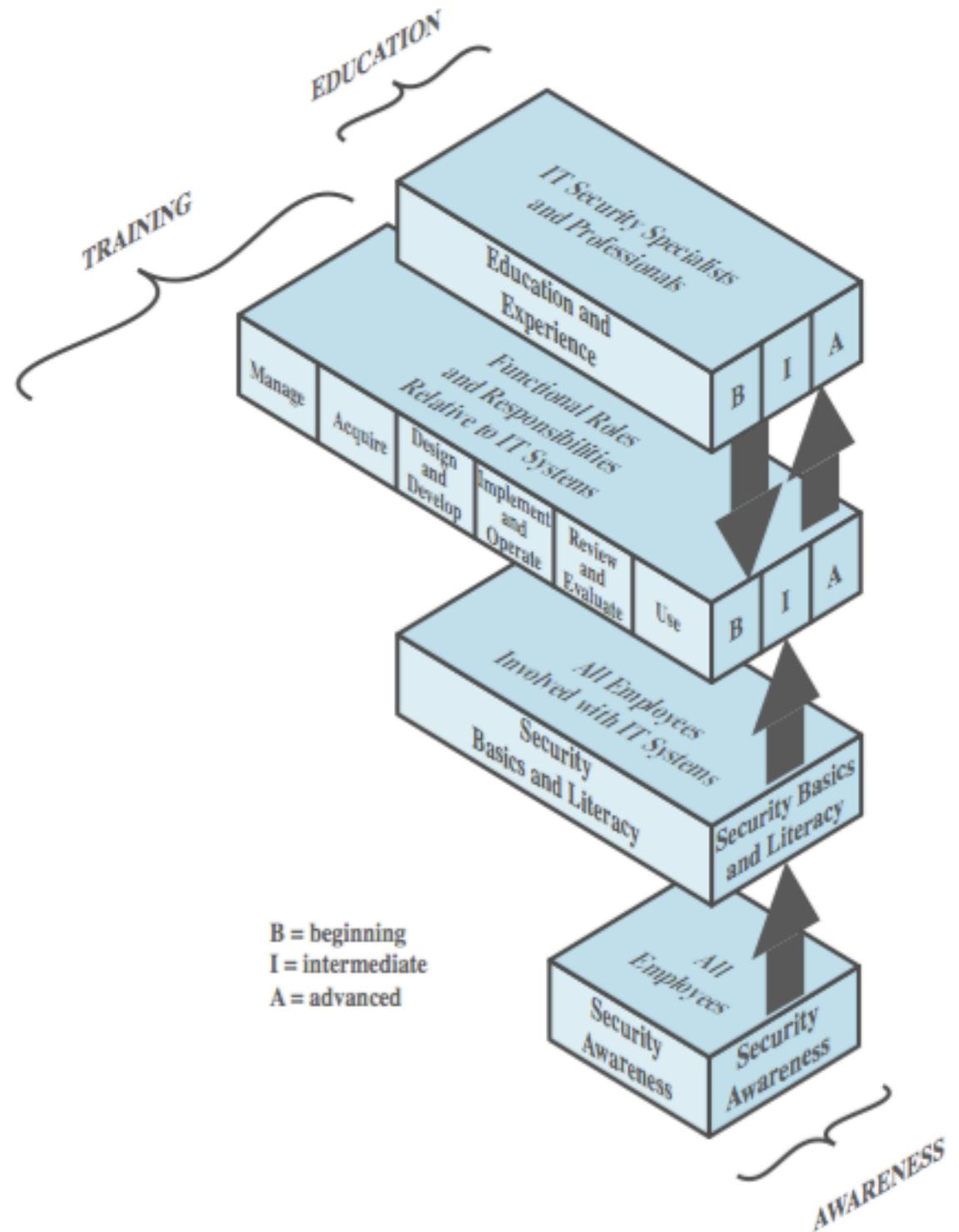
- improving employee behavior

- increasing employee accountability

- mitigating liability for employee behavior

- complying with regulations and contractual obligations

# Learning Continuum



# Awareness

seeks to inform and focus an employee's attention on security issues

threats, vulnerabilities, impacts, responsibility

must be tailored to organization's needs

using a variety of means

events, promo materials, briefings, policy doc

should have an employee security policy document

# Training

teaches what people should do and how they do it  
to securely perform IS tasks

encompasses a spectrum covering:

general users

good computer security practices

programmers, developers, maintainers

security mindset, secure code development

managers

tradeoffs involving security risks, costs, benefits

executives

risk management goals, measurement, leadership

# Education

most in depth

targeted at security professionals whose jobs  
require expertise in security

more employee career development

often provided by outside sources

- college courses

- specialized training programs

# Organizational Security Policy

“formal statement of rules by which people given access to organization's technology and information assets must abide”

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

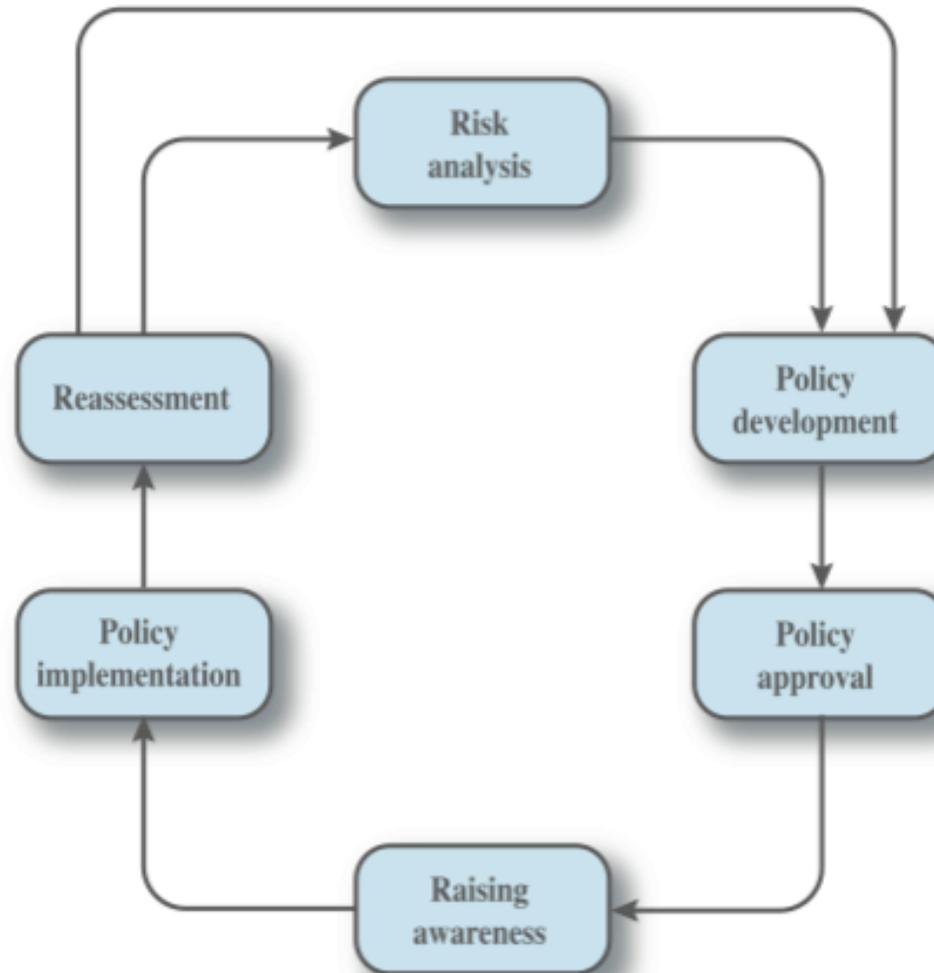
states responsibility for protection

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 admins, security incident response team, user groups representatives, responsible management, legal counsel

# Document Content

- 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.

technical support

privacy

access

accountability

authentication

availability

maintenance

violations reporting

business continuity

supporting information

# Resources

## ISO 17799

popular international standard

has a comprehensive set of controls

a convenient framework for policy authors

## COBIT

business-oriented set of standards

includes IT security and control practices

## Standard of Good Practice for Information Security

other orgs, e.g. CERT, CIO

# Personnel Security

hiring, training, monitoring behavior, and handling departure

employees security violations occur:

- unwittingly aiding commission of violation

- knowingly violating controls or procedures

threats include:

- gaining unauthorized access, altering data, deleting production and back up data, crashing systems, destroying systems, misusing systems, holding data hostage, stealing strategic or customer data for corporate espionage or fraud schemes

# 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

# Background Checks & Screening

issues:

- inflated resumes

- reticence of former employers to give good or bad references due to fear of lawsuits

employers do need to make significant effort to do background checks / screening

- get detailed employment / education history

- reasonable checks on accuracy of details

- have experienced staff members interview

for some sensitive positions, additional intensive investigation is warranted

# 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 abide by organization's security policy

# During Employment

## current employee security objectives:

- ensure employees, contractors, third party users are aware of info security threats & concerns

- know their responsibilities and liabilities

- are equipped to support organizational security policy in their work, and reduce human error risks

## need security policy and training

## security principles:

- least privilege

- separation of duties

- limited reliance on key personnel

# Termination of Employment

## termination security objectives:

ensure employees, contractors, third party users exit organization or change employment in an orderly manner that the return of all equipment and the removal of all access rights are completed

## 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

# Email & Internet Use Policies

E-mail & Internet access for employees is common in office and some factories

increasingly have e-mail and Internet use policies in organization's security policy

due to concerns regarding

- work time lost

- computer / comms resources consumed

- risk of importing malware

- possibility of harm, harassment, bad conduct

# Suggested Policies

business use only

policy scope

content ownership

privacy

standard of conduct

reasonable personal use

unlawful activity prohibited

security policy

company policy

company rights

disciplinary action

# Example Policy

## COMPANY SECURITY POLICY – INDEX

### Executive Summary

1. **Security Policy**
  - 1.1. Security Policy Documents
  - 1.2. Review and Evaluation
2. **Company Security**
  - 2.1. Information security infrastructure
  - 2.2. Security of third party access
  - 2.3. Outsourcing
  - 2.4. Partnerships, Joint ventures and Alliances
3. **Asset classification and control**
  - 3.1. Accountability for assets
  - 3.2. Fraud policy
  - 3.3. Information classification
  - 3.4. Asset Protection
4. **Personnel security**
  - 4.1. Security in job definition and resourcing
  - 4.2. User training
  - 4.3. Responding to security incidents and malfunctions
  - 4.4. Joiners, Leavers and Travellers
5. **Physical and Environmental security**
  - 5.1. Secure Areas
  - 5.2. Equipment Security
  - 5.3. General Controls
6. **Communications and operations management**
  - 6.1. Operational procedures and responsibilities
  - 6.2. System planning and acceptance
  - 6.3. Protection against malicious software
  - 6.4. Housekeeping
  - 6.5. Network management
  - 6.6. Media handling and security
  - 6.7. Exchanges of information and software
7. **Logical Access control**
  - 7.1. Business requirement for access control
  - 7.2. User access management
  - 7.3. User responsibilities
  - 7.4. Network access control
  - 7.5. Operating system access control
  - 7.6. Application access control
  - 7.7. Monitoring system access and use
  - 7.8. Mobile computing and Teleworking
  - 7.9. Internet/Intranet access

# Summary

introduced some important topics relating to  
human factors

security awareness, training & education

organizational security policy

personnel security

E-mail and Internet Use Policies

# Security Principles

- Least Privilege
- Fail-Safe Defaults
- Economy of Mechanism
- Complete Mediation
- Open Design
- Separation of Privilege/Duty
- Least Common Mechanism
- Psychological Acceptance