Security Risk Analysis & Management
Security in System Development

- Risk Analysis & Management needs to be a part of system development, not tacked on afterwards
- Baskerville's three generations of methods
  1st Generation: Checklists
    Example: BS 7799 Part 1
  2nd Generation: Mechanistic engineering methods
    Example: this risk analysis method
  3rd Generation: Integrated design
    Not yet achieved

Introduction

Risk Analysis and Management Framework

- Assets
- Threats
- Vulnerabilities

Risks

Security Measures

Analysis

Management

Security Risk Analysis & Management
The meanings of terms in this area is not universally agreed. We will use the following:

- **Threat**: Harm that can happen to an asset
- **Impact**: A measure of the seriousness of a threat
- **Attack**: A threatening event
- **Attacker**: The agent causing an attack (not necessarily human)
- **Vulnerability**: A weakness in the system that makes an attack more likely to succeed
- **Risk**: A quantified measure of the likelihood of a threat being realised
**Definitions 2**

- **Risk Analysis** involves the identification and assessment of the levels of risk, calculated from the:
  - Values of assets
  - Threats to the assets
  - Their vulnerabilities and likelihood of exploitation

- **Risk Management** involves the identification, selection and adoption of security measures justified by:
  - The identified risks to assets
  - The reduction of these risks to acceptable levels
Goals of Risk Analysis

- All assets have been identified
- All threats have been identified
  - Their impact on assets has been valued
- All vulnerabilities have been identified and assessed
Problems of Measuring Risk

Businesses normally wish to measure in money, but

- Many of the entities do not allow this
  - Valuation of assets
    - Value of data and in-house software - no market value
    - Value of goodwill and customer confidence
  - Likelihood of threats
    - How relevant is past data to the calculation of future probabilities?
      - The nature of future attacks is unpredictable
      - The actions of future attackers are unpredictable
  - Measurement of benefit from security measures
    - Problems with the difference of two approximate quantities
      - How does an extra security measure affect a $\sim 10^{-5}$ probability of attack?
Risk Levels

- Precise monetary values give a false precision
- Better to use levels, e.g.
  - High, Medium, Low
    - High: major impact on the organisation
    - Medium: noticeable impact (“material” in auditing terms)
    - Low: can be absorbed without difficulty
  - 1 - 10
- Express money values in levels, e.g.
  - For a large University Department a possibility is
    - High
    - Medium
    - Low
Risk Analysis Steps

- Decide on scope of analysis
  - Set the system boundary
- Identification of assets & business processes
- Identification of threats and valuation of their impact on assets (*impact valuation*)
- Identification and assessment of vulnerabilities to threats
- Risk assessment
Risk Analysis – Defining the Scope

- Draw a context diagram
- Decide on the boundary
  - It will rarely be the computer!
- Make explicit assumptions about the security of neighbouring domains
  - Verify them!
Risk Analysis - Identification of Assets

- Types of asset
  - Hardware
  - Software: purchased or developed programs
  - Data
  - People: who run the system
  - Documentation: manuals, administrative procedures, etc
  - Supplies: paper forms, magnetic media, printer liquid, etc
  - Money
  - Intangibles
    - Goodwill
    - Organisation confidence
    - Organisation image
Identification and valuation of threats - for each group of assets

- Identify threats, e.g. for stored data
  - Loss of confidentiality
  - Loss of integrity
  - Loss of completeness
  - Loss of availability (Denial of Service)

- For many asset types the only threat is loss of availability

- Assess impact of threat
  - Assess in levels, e.g. H-M-L or 1 - 10
  - This gives the valuation of the asset in the face of the threat
Risk Analysis – Process Analysis

- Every company or organisation has some processes that are critical to its operation.
- The criticality of a process may increase the impact valuation of one or more assets identified.

So
- Identify critical processes.
- Review assets needed for critical processes.
- Revise impact valuation of these assets.
Risk Analysis – Vulnerabilities 1

- Identify vulnerabilities against a baseline system
  - For risk analysis of an existing system
    - Existing system with its known security measures and weaknesses
  - For development of a new system
    - Security facilities of the envisaged software, e.g. Windows NT
    - Standard good practice, e.g. BS 7799 recommendations of good practice
For each threat

- Identify vulnerabilities
  - How to exploit a threat successfully;

- Assess levels of likelihood - High, Medium, Low
  - Of attempt
    - Expensive attacks are less likely (e.g. brute-force attacks on encryption keys)
  - Successful exploitation of vulnerability;

- Combine them

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Low</th>
<th>Med</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Med</td>
</tr>
<tr>
<td>Med</td>
<td>Low</td>
<td>Med</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>Med</td>
<td>High</td>
</tr>
</tbody>
</table>
Assess risk

- If we had accurate probabilities and values, risk would be
  - Impact valuation x probability of threat x probability of exploitation
  - Plus a correction factor for risk aversion
- Since we haven't, we construct matrices such as

<table>
<thead>
<tr>
<th>Risk</th>
<th>Impact valuation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>
Responses to Risk

Responses to risk

- **Avoid** it completely by withdrawing from an activity
- **Accept** it and do nothing
- **Reduce** it with security measures
Security Measures

Possible security measures

- **Transfer the risk, e.g. insurance**
- **Reduce vulnerability**
  - Reduce likelihood of attempt
    - e.g. publicise security measures in order to deter attackers
    - e.g. competitive approach - the lion-hunter’s approach to security
  - Reduce likelihood of success by preventive measures
    - e.g. access control, encryption, firewall
- **Reduce impact, e.g. use fire extinguisher / firewall**
- **Recovery measures, e.g. restoration from backup**
Risk Management

- Identify possible security measures
- Decide which to choose
  - Ensure complete coverage with confidence that:
    - The selected security measures address all threats
    - The results are consistent
    - The expenditure and its benefits are commensurate with the risks
  - Consider doing less than the BS7799 recommendations?
Iterate

- Adding security measures changes the system
  - Vulnerabilities may have been introduced
- After deciding on security measures, revisit the risk analysis and management processes
  - e.g. introduction of encryption of stored files may remove the threat to Confidentiality but introduce a threat to Availability
    - What happens if the secret key is lost?
Conclusion: Problems of Risk Analysis and Management

- Lack of precision
- Volume of work and volume of output
- Integrating them into a "normal" development process
Current Risk Management Techniques
Commercial tools

- Mostly rely on check lists

- **CRAMM (CCTA Risk Assessment and Management Methodology)**:
  - UK Government approach
  - Supported by software

- **PROTEUS (BSI) software**:
  - Gap analysis to identify necessary actions and existing strengths
  - Comprehensive practical guidance and the text of BS 7799
  - Reporting, for easy monitoring and maintenance
  - Evidence to customers and auditors
Risk Management Techniques 2

Generic processes

- Threat trees (see below):
  - Threat analysis
  - Based on fault trees
  - Only addresses the threat identification stage

- Attack trees (see below)
  - Vulnerability analysis
AT&T Bell Laboratories

- Categorisation of threats
  - Disclosure / Integrity / Denial of service

- Categorisation of vulnerabilities by view
  - Personnel view
  - Physical view
  - Operational view
  - Communications view
  - Network view
  - Computing view
  - Information view

Threat Trees 2

- Model of system
- Calculate risks from
  - Impact
  - Vulnerability

Security Risk Analysis & Management
Attack Trees

● Tree Structure
  ● Goal is root node
  ● Ways of achieving goals are leaf nodes
  ● Costs can be associated with nodes

[Schneier, B, Secrets and Lies. 2000: John Wiley and Sons.]
Goal: Read a specific message …

1. Convince sender to reveal message (OR)
   1.1. Bribe user
   1.2. Blackmail user
   1.3. Threaten user
   1.4. Fool user

2. Read message when it is being entered into the computer (OR)
   2.1. Monitor electromagnetic emanations from computer screen (Countermeasure: use a TEMPEST computer)
   2.2. Visually monitor computer screen
   2.3. Monitor video memory
   2.4. Monitor video cables

3. Read message when it is being stored on sender's disk (Countermeasure: use SFS to encrypt hard drive) (AND)
   3.1. Get access to hard drive (Countermeasure: Put physical locks on all doors and windows)
   3.2. Read a file protected with SFS.

4. …..