Protection Profiles as a Governmental Tool

Anders Staaf
anders.staaf@combitech.se
Agenda

- Short presentation of Combitech
- New Swedish regulation
- Driving forces
- Developing methodology
- Impact on governmental organizations
- Summary
Combitech – Combining Engineering, Environment and Security!

- One of the biggest consulting companies in Sweden within information security
- Worked with Common Criteria for more than 15 years
- ITSEF since 2007

Securing Possibilities™
Sweden applying mandatory rules to use CC certified products!

- To protect critical information handled by
- Civil governmental infrastructure
Threats from mobile devices…

**Space Station Computers Catch Virus in Orbit**  
By Tariq Malik  
Senior Editor, www.space.com  
posted: 27 August 2008  
2:59 pm ET  
…

**Malware implicated in fatal Spanair plane crash**  
Computer monitoring system was infected with Trojan horse, authorities say  
By Leslie Meredith  
www.technewsdaily.com  
updated 8/20/2010 4:48:01 PM ET  
…

**Security Breach: Feds Lose Laptop Containing Sensitive Data -- Again**  
This time, a thief made off with a computer containing unencrypted details of about 2,500 participants in an NIH clinical trial  
By Larry Greenemeier,  
www.sciencemag.org  
…

**UK laptop containing sensitive information on patients stolen**  
by WHAS11 News  
WHAS11.com  
Posted on August 22, 2010 at 3:32 PM  
…
and cyberattacks…

2007 cyberattacks on Estonia

From Wikipedia, the free encyclopedia

Cyberattacks on Estonia (also known as the Estonian Cyberwar or Web War 1) refers to a series of cyber attacks that began April 27, 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters …

Some Russian PCs used to cyberattack Georgia

Updated 8/17/2008 9:27 PM
By Byron Acohido, USA TODAY

Thousands of Russian supporters are volunteering their PCs to be used in cyberattacks against websites supporting the rival state of Georgia. …
Driving forces

• Real threats:
  ▪ Organized attacks against governmental assets available at the Internet
  ▪ Classified information revealed from found or stolen mobile devices
  ▪ Malware spread by mobile devices
  ▪ …

• Better protection of IT infrastructure

• Leads to more certified products available

• Security awareness among the organisations
Critical Infrastructure

Areas in the society where IT infrastructure can be considered as critical:

- Computer and telephone networks
- Energy production, distribution
- Transportation
- Health care
- Police, fire brigades, etc.
- Payment services (used by banks, PTT)
- Civil governmental management (national, regional, local)
Development of the rules

• The Swedish governmental agency “MSB” responsible

• Close cooperation with the Swedish CB, FMV/CSEC, and other governmental organizations related to IT security
The Swedish Civil Contingencies Agency, MSB

- MSB is responsible for preparedness for and prevention of emergencies and crises
- MSB is the focal point for coordinating Swedish national information security
- MSB develops measures to improve Sweden’s ability to prevent and handle IT incidents
- MSB is the CCRA signatory for Sweden
Combitech’s Role

Combitech has supplied MSB with information related to IT security in general and Common Criteria in special in a number of reports

- Reported vulnerabilities in products
- Analysis of existing Protection Profiles
- International comparison of regulations
- ...

International references

- US regulations, NSTISSP 11 ("Policy 11") and DoD 8500
- Directives from EU
- Economical means of control, e.g. tax reduction
- Etc.
When do the rules apply?

Applies to IT product that is:

- Used by a governmental organization
- Handling critical information
- Of a category for which a governmental Protection Profile has been assigned
Organizations concerned

- Governmental authorities
- Civil area, defense not included
# Information Classification

<table>
<thead>
<tr>
<th>Aspects: Impact</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serious / Catastrophic</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Severe</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Significant</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Library of Protection Profiles

Divided into a number of categories:

- Anti-virus programs
- Authentication – Smart cards, biometry, other
- Firewalls
- Databases
- Intrusion detection - IDS/IPS
- Memory protection - Hard disks, USB-memories
- Multi function equipment – Printers, copiers, faxes
- Network equipment – Routers, switches
- Operative systems
- PKI, certificate management
- Wireless LAN
- Wireless WAN – Mobile internet, Smartphones/PDAs
- VPN
- Web server, application servers
- Web browsers
Development Strategies for the PP Library

1. Use existing, certified Protection Profiles
   - Most cost effective
   - May require cooperation with the authors for maintenance
   - Certified products may already be available

2. Develop new Protection Profiles in cooperation with other countries
   - Cost effective
   - May yield competence exchange
   - Bigger penetration potential than locally used PP

3. Internally develop Protection Profiles for local use
   - Less cost effective
   - Builds local competence
   - May be necessary to comply to local requirements, e.g. legislation
Prioritizing Protection Profiles

Aspects taken under consideration:

- Risk for future attacks mounted on the product type
- Number of actual attacks observed
- Number of units deployment within governmental organizations
- Costs for the organization to introduce a Protection Profile
- Local (Swedish) competence within the area
Prioritizing Protection Profiles

Resulting in a list consisting of (not very surprisingly):

1. Mobile devices
2. First level of defense for networks, e.g. firewalls
3. The rest
Impact on Governmental Organizations

• Cost impact on purchased product

• Routines for users

• Routines for administrators

• Education for the purchase department
Summary

• Sweden introduce new rules for using certified products in critical gov. infrastructure

• Building a Protection Profile library

• Starting with mobile devices and critical network products