Monitoring and intrusion detection

How to protect

- We have seen several approaches and techniques for the information protection (mainly at the levels 2,3);
- Techniques were mainly focusing on how to make a security/privacy attack difficult;
- Not all attacks may be prevented;
- How to deal with the attacks anyway?

Information protection

<table>
<thead>
<tr>
<th>Level</th>
<th>What to protect</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Existence of message</td>
<td>Steganography</td>
</tr>
<tr>
<td>2</td>
<td>Metadata of message</td>
<td>Privacy-enhancing technologies</td>
</tr>
<tr>
<td>1</td>
<td>Content of message</td>
<td>Encryption</td>
</tr>
<tr>
<td>0</td>
<td>Nothing</td>
<td>None</td>
</tr>
</tbody>
</table>

Defence lines: anti-intrusion methods

Picture by S.Axelsson
**Anti-intrusion methods**

- **Prevention**: to preclude, or seriously reduce likelihood of a particular attack;
  - It may be internal prevention, controlled by the system itself (system owner), or
  - It may be external, taking place in the environment of the system
- **Pre-emption**: to strike against the threat before it could strike against us;
- **Deterrence**: to persuade an attacker not to launch an attack, or to stop ongoing attack. Usually done by increasing the risk of negative consequences for the attacker

**Intrusion detection**

- Intrusion detection is the most important of anti-intrusion methods:
  - Prevention, pre-emption and deterrence are not absolute and attacks happen;
  - For countermeasures one has to detect an attack
- We consider general principles, structure and functionality of IDSs;

**Taxonomy of anti-intrusion methods**

- Prevention
- Pre-emption
- Deterrence
- Deflection
- Detection
- Countermeasures

**Anti-intrusion methods (cont.)**

- **Deflection**: to trick away an intruder from where he could do some damage ("honeypot" techniques);
- **Detection**: aims to find intrusion attempt and launch countermeasures;
- **Countermeasures**: to actively counter an intrusion
Typical intrusion detection system (IDS)

- **Audit collection**: collect data for intrusion detection, including keyboard input, data from various log files, data on network activities;
- **Audit storage**: stores the data for further processing, amount of data may be the problem;
- **Processing**: based on collected data, algorithm(s) are executed to find an evidence (with some degree of certainty) of the suspicious behaviour;
- **Configuration data**: specify the way IDS works, how to collect data, how to respond to detected attack, etc;
- **Reference data**: information about known intrusion signatures, information about bad/normal behaviour;
- **Active/Processing data**: intermediate results, which should be stored during processing;
- **Alarm**
Types of IDSs (cont)

• **Application-based IDS**: deal with the events appearing inside of a particular application, such as
  • Database management systems;
  • Content management;
  • Accounting system

Intrusion detection methods

Two main categories:

• **Anomaly based intrusion detection**: system reacts to abnormal behaviour. Behaviour profiles are used and system is able to learn what is a “normal” behaviour;
  • Policy based detection (signature based, specification based): system tries to match the *explicit policies* with the data collected to find an evidence of the suspicious behaviour:
    • Default permit policies;
    • Default deny policies.

Anomaly based detection

**Advantages:**
• possibility of detection of novel attacks as intrusions;
• less dependence of IDSs on operating environment;
• ability to detect abuse of user privileges.

**Disadvantages:**
• A substantial false alarm rate;
• User behaviors can vary with time, requiring a constant update of the normal behaviour profile database.

Signature based method

**Example of a signature**: alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"MISC large ICMP"; dsize: >800; reference:arachnids,246; classtype:bad-unknown; sid:499;)

Alarm will be raised if a ICMP packet incoming from the external network,m associated with any port and having a size more than 800 bytes

**Advantages:**
• very low false alarm rate;
• simple algorithms, easy implementation.

**Disadvantages:**
• difficulties in updating information on new types of attacks;
• Unable to detect unknown attacks (knowledge based)