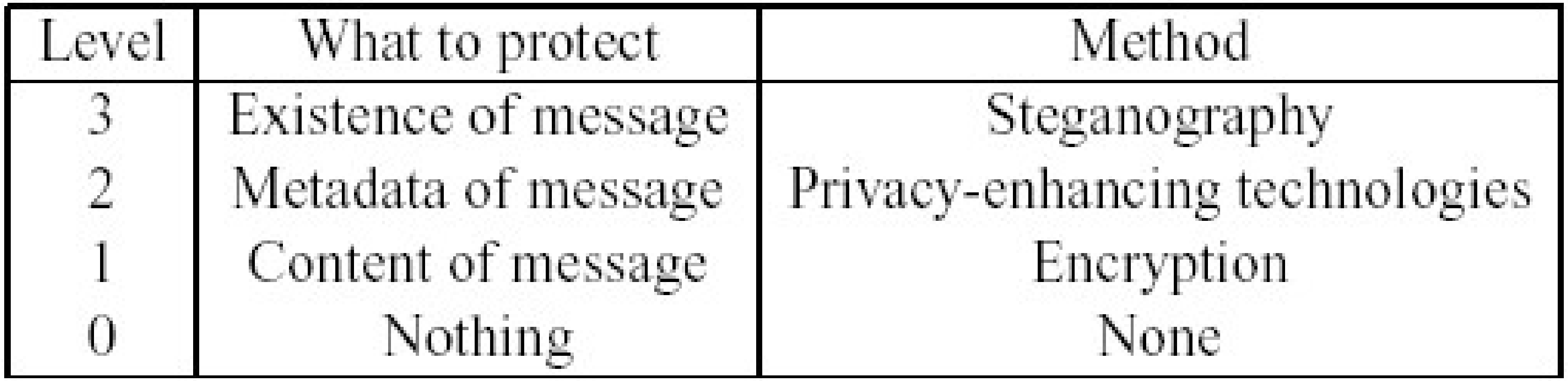
Monitoring
and intrusion detection

Information protection

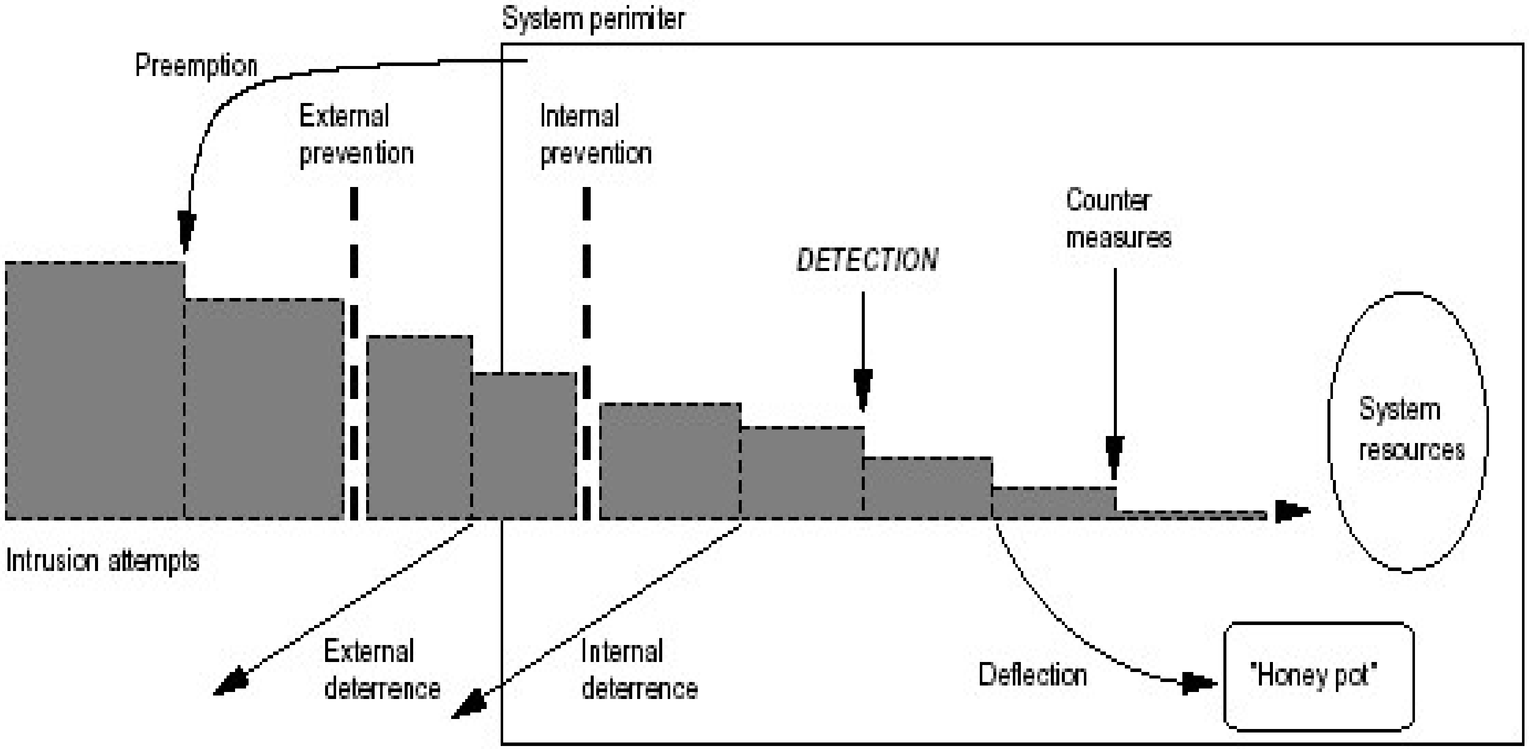


Level	What to protect	Method
3	Existence of message	Steganography
2	Metadata of message	Privacy-enhancing technologies
1	Content of message	Encryption
0	Nothing	None

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?

Defence lines: anti-intrusion methods



Picture by S.Axelsson

Taxonomy of anti-intrusion methods

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

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

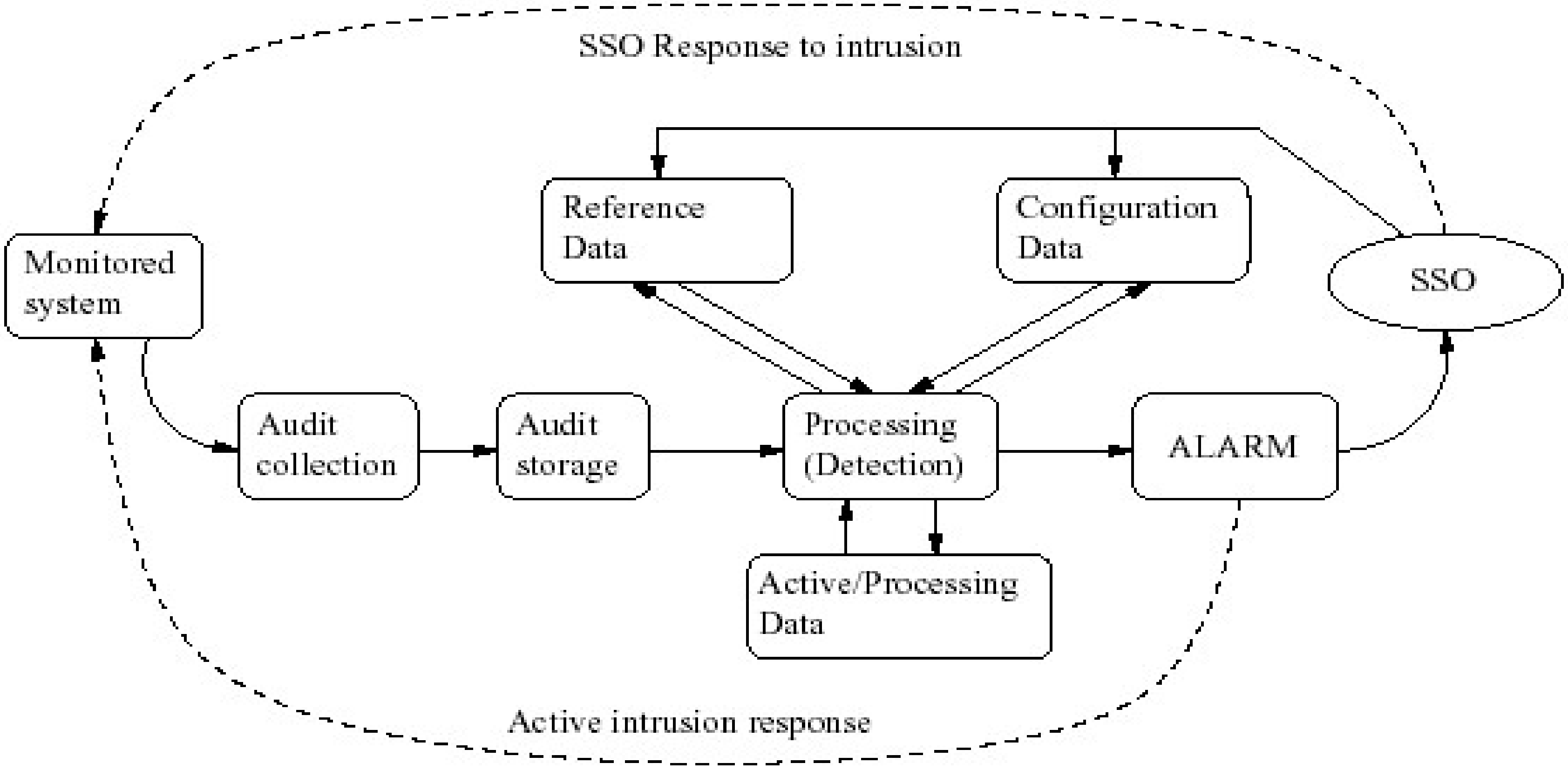
Anti-intrusion methods (cont.)

- **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

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;

Typical intrusion detection system (IDS)



Picture by S.Axelsson

Elements of typical 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

Elements of typical IDS (cont.)

- **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 IDS

- **Network-based IDS:**
  - monitor network backbones;
  - distributed among different nodes in the network;
  - usually passive => not easy to detect by an attacker;
  - may not be able analyse the traffic in large busy networks

- **Host-based IDS:**
  - Operate on hosts;
  - defend and monitor the operating and file systems for signs of intrusion;
  - Usually monitor activities with higher level of details

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;
- **Knowledge based detection** (policy based signature based, specification based): system tries to match the *explicit policies/signatures* with the data collected to find an evidence of the suspicious behaviour

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)