Intrusion Detection Systems (IDS)

Presented by

Erland Jonsson

Department of
Computer Science and Engineering

Intruders & Attacks

- Cyber criminals
- Activists
- State-sponsored organizations Advanced Persistent Threat (APTs)
- Others
- Apprentice, Journeyman, Master

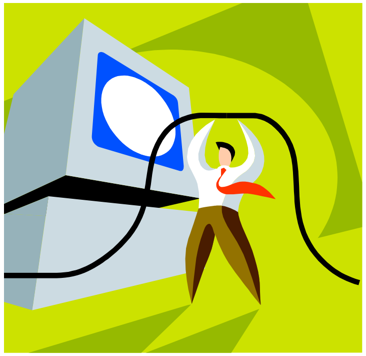
Intruder Behavior

- Target Acquisition and Information Gathering
- Initial Access
- Privilege Escalation
- Information Gathering or System Exploit
- Maintaining Access
- Covering Tracks

Contents

- Motivation and basics (Why and what?)
- IDS types and detection principles
- Key Data
- Problems with IDS systems
- Prospects for the Future

Why Intrusion Detection?



Intrusion Detection

- Intrusion Detection Systems (IDS) does not (a priori) protect your system
- It works as burglar alarm
- Intrusion Detection Systems constitute a powerful **complement** (to basic security)

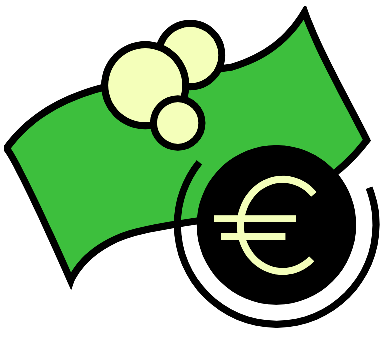
Motivation for Intrusion Detection

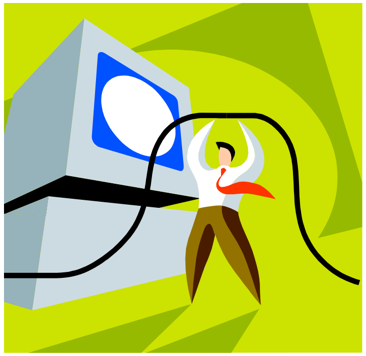
- Even it you do not succeed to stop the intrusion it is of value to know that an **intrusion** has indeed **occurred**, **how** it occurred and which **damage** that has been caused.

IDS's are used for:

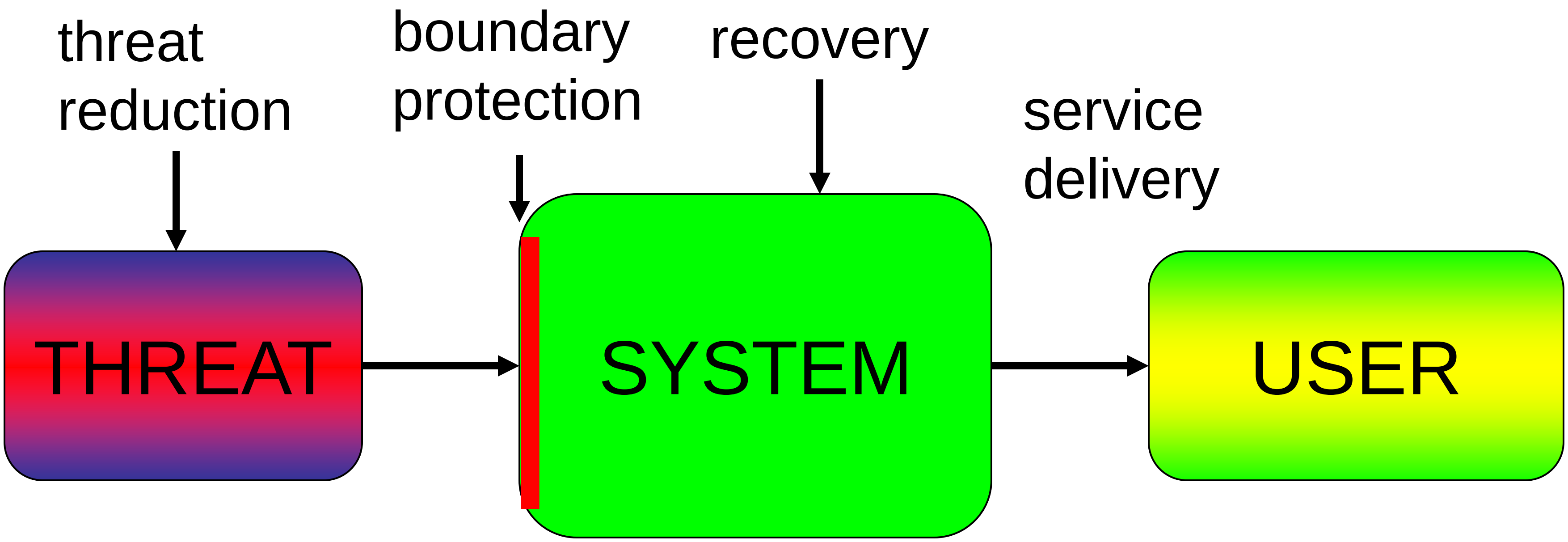
- detect intrusions and intrusion attempts
- give alarms
- stop on-going attacks (possibly)
- trace attackers
- investigate and assess the damage
- gather information for recovery actions

What is Intrusion Detection?





What is Security? - protection principles



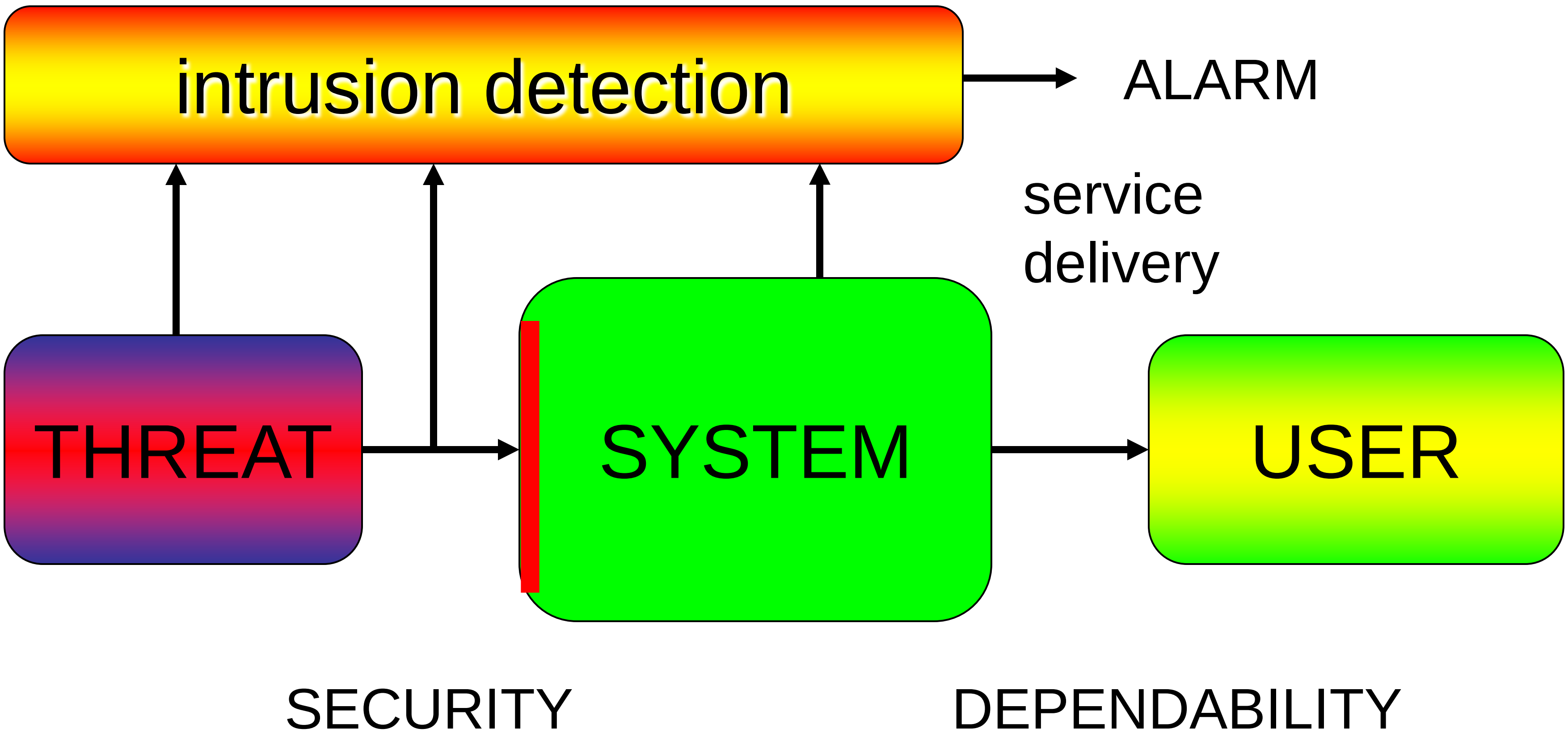
SECURITY

DEPENDABILITY

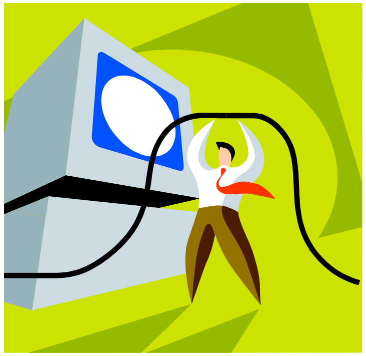
Security=Datasäkerhet

Safety=Katastrofsäkerhet

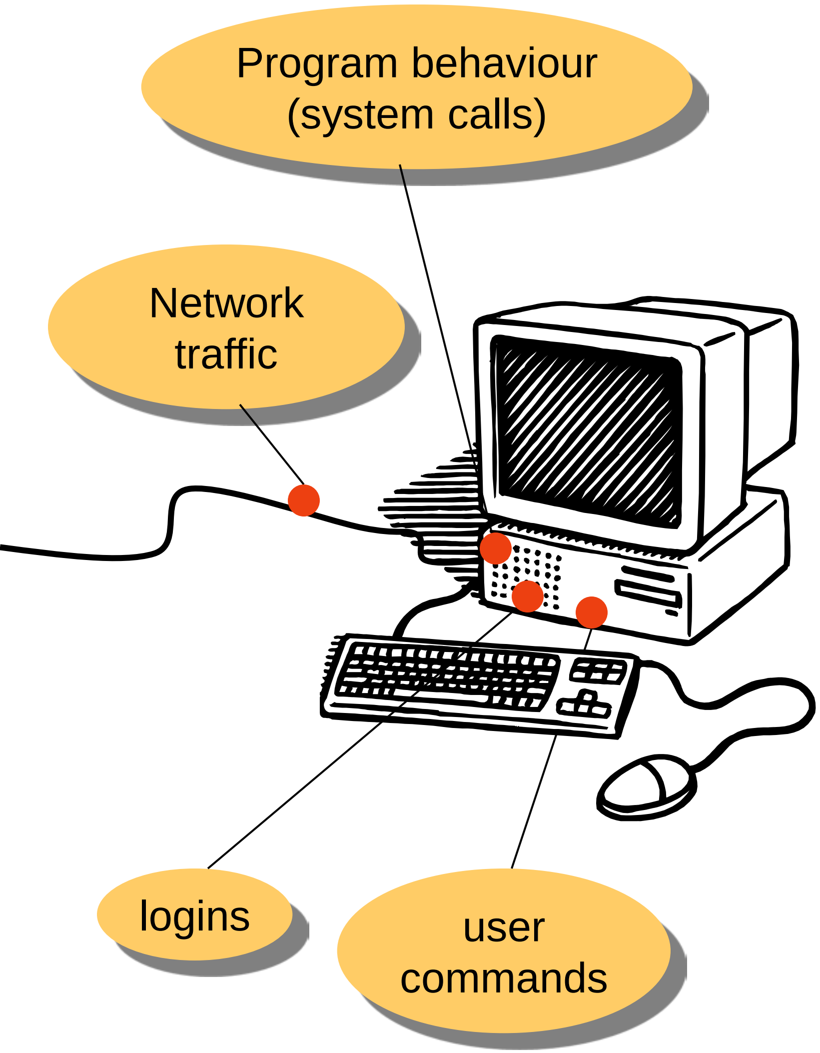
What is Security? - intrusion detection



How is detection accomplished?



Logging is the basis for ID – sensors for intrusion detection



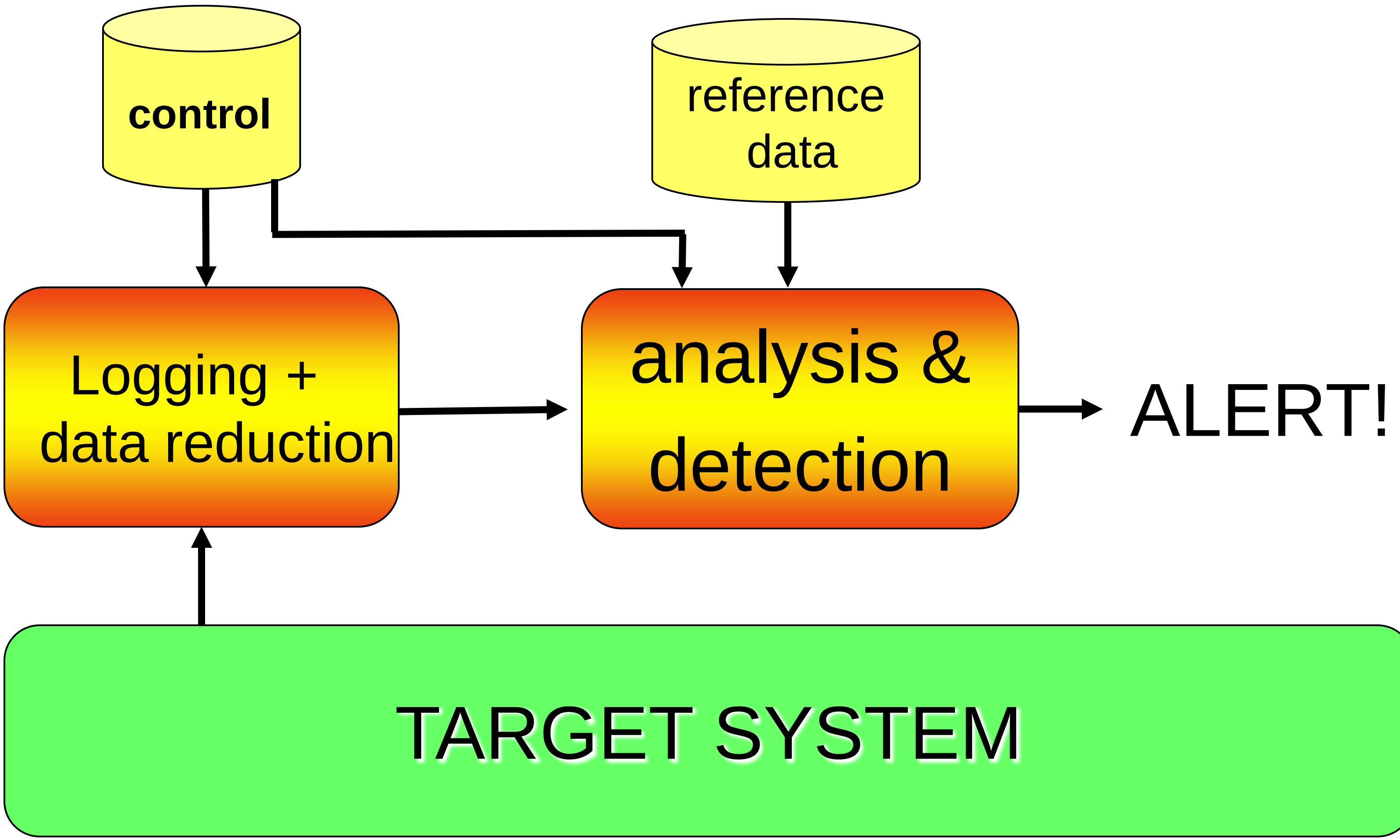
What do you log?

- Network traffic to detect ”network attacks”
- System calls to detect programs that behave suspiciously
- User commands to detect masquerading, i.e. when an attacker is using another user’s account
- Logins, in order to know who was active on the system when it was attacked

What do we want to detect

- ”Ordinary” intrusions
  - ”sniffing” of passwords
  - buffer overflow attacks
  - Availability attacks (DoS, denial-of-service) are common and hard to protect against
- Information gathering, i.e. ”attacks” aiming at open ports and weaknesses
    - vulnerability and port scanning:
      Satan, Nmap, Nessus, OpenVAS

Components in an Intrusion Detection System



Principles of Intrusion Detection

There are two main principles:

- **misuse detection** (missbruksdetektering)
  - define what is ***"wrong"*** and **give a*larms for that*** ("default permit")
- **anomaly detection** (avvikelsedetektering)
  - define what is ***"correct"*** and **give a*larms for everything else*** ("default deny")

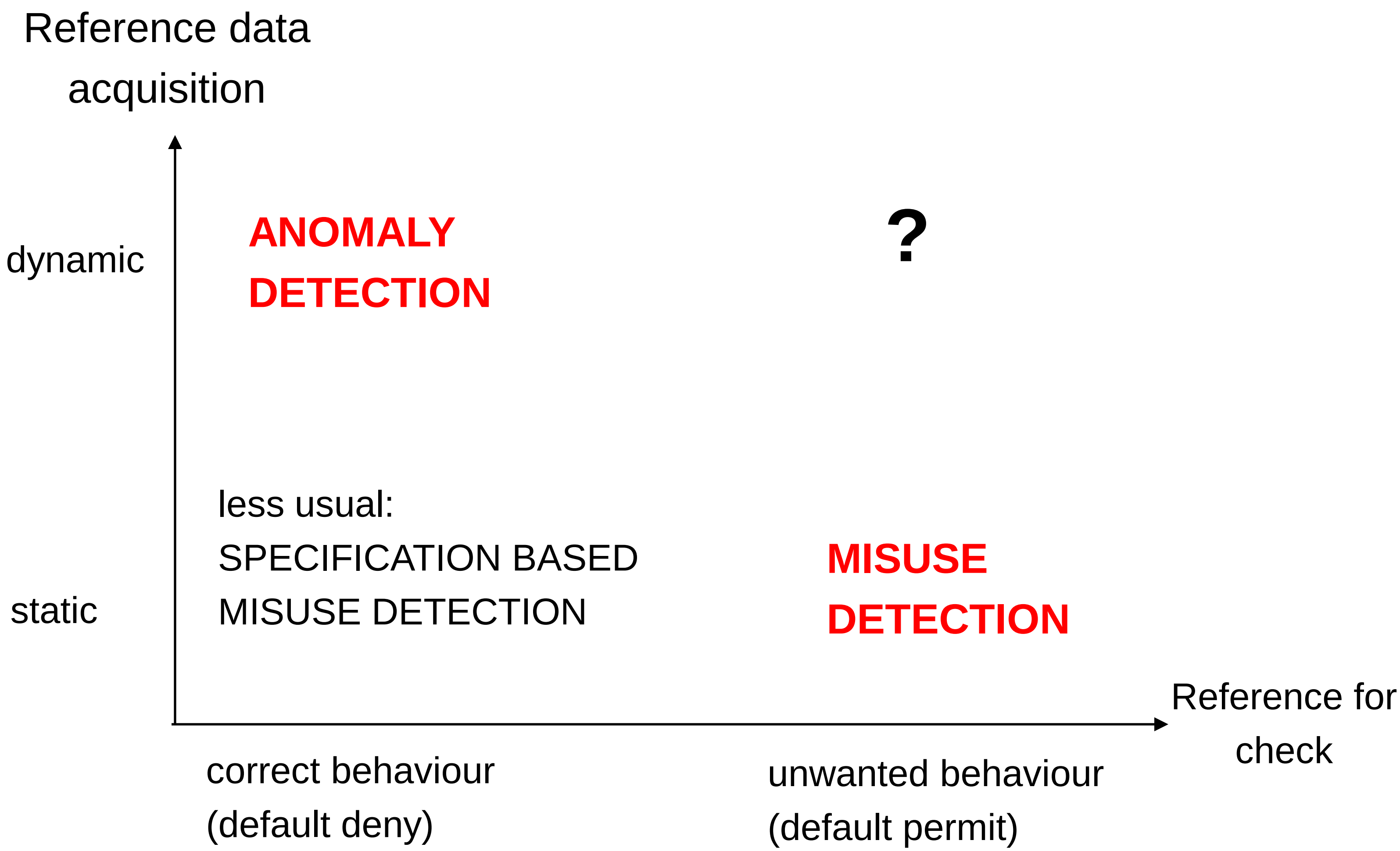
Principles of Intrusion Detection

The book uses another classification scheme:

- **anomaly detection**

- **signature detection**
  - rule-based anomaly detection,
    in which rules are based on historical anomalies
    (is really anomaly detection)
  - rule-based penetration identification,
    which largely is identical to **misuse detection**

IDS Systems - overview



Key Data for IDS Systems

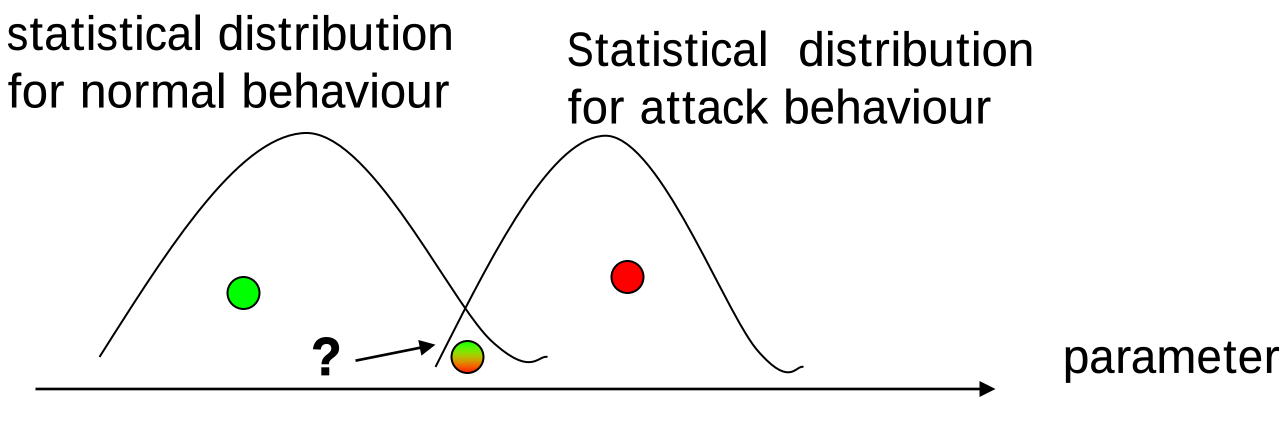
- **FIGURES-OF-MERIT** for IDS-systems
  Which attributes are interesting?
- no alarms should be given in the abscence of intrusions
- intrusion (attempts) must be detected
- probability of detection (“hit rate”) (upptäcktssannolikhet)
- rate of false positives (“false alarm rate”) (falskalarmrisk)
- rate of false negatives (“miss rate”) (misssannolikhet)

Key data for IDS Systems (cont'd)

	no alarm	alarm
intrusion	**MISS**	**OK**
no intrusion	**OK** normal state	**FALSE ALARM** problem area !?

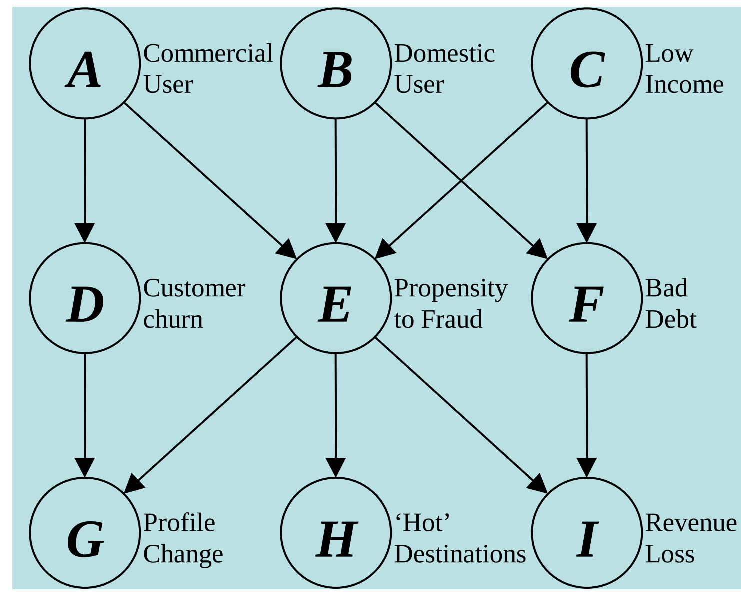
Detection problem

- Classification
  - the detection is a traditional clasification problem
  - Separate intrusion events from normal events
  - however, there is an overlap…..



Detection methods

- Rule based
- Pattern matching
- Expert systems
- Thresholds
- Statistical analysis
- Bayesian networks
- Neural networks
- Markov models
- etc

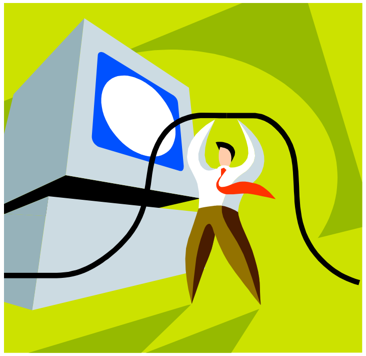


Pr{*A*}	= 0.76	Pr{*B*}	= 0.24	Pr{*C*}	= 0.74
Pr{*D*|¬*A*}	= 0.27	Pr{*D*|*A*}	= 0.73		
Pr{*E*|¬*A*,¬*B*,*x*}	= 0.01				
Pr{*E*|¬*A*,*B*,¬*C*}	= 0.02	Pr{*E*|¬*A*,*B*,*C*}	= 0.04	Pr{*E*|*A*,*x*,*x*}	= 0.03
Pr{*F*|¬*B*,*x*}	= 0.00	Pr{*F*|*B*,¬*C*}	= 0.01	Pr{*F*|*B*,*C*}	= 0.04
Pr{*G*|¬*D*,¬*E*}	= 0.03	Pr{*G*|¬*D*,*E*}	= 0.72		
Pr{*G*|¬*D*,*E*}	= 0.84	Pr{*G*|*D*,*E*}	= 0.96		
Pr{*H*|¬*E*}	= 0.58	Pr{*H*|*E*}	= 0.42		
Pr{*I*|¬*E*,¬*F*}	= 0.02	Pr{*I*|¬*E*,*F*}	= 0.98		
Pr{*I*|*E*,¬*F*}	= 1	Pr{*I*|*E*,*F*}	= 1		

Requirements on IDS Systems

- system response time (real-time behaviour?)
- fault tolerance (due to e.g. s/w, h/w, configuration, etc)
- ease of integration, usability and maintainability
- portability
- support for reference data updates (misuse systems) (cp virus programs)
- “excess” information (privacy aspects)
- the “cost” (CPU usage, memory, delays,...)
- host-based or network based?
- security of the IDS (protect the reference information) ?

Problems with IDS systems



A few practical problems

1. False alarms
2. Adaptivity/Portability
3. Scalability
4. Lack of test methods
5. Privacy concerns

Problem area 1

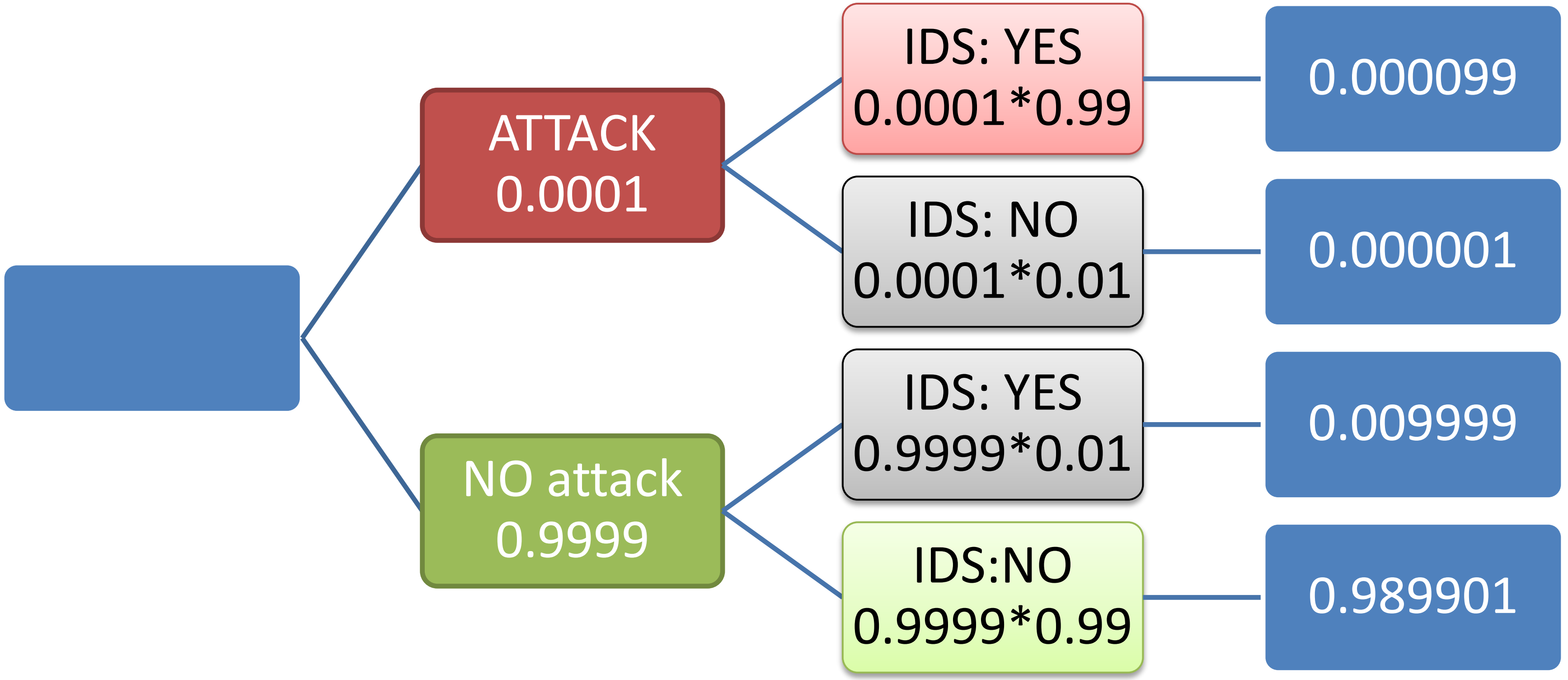
- False alarms
  - MANY alarms
  - If detection is 99% correct and the number of intrusions is 0.01% in the analysed information: 99% of all alarms will be false alarms!
  - There is a trade-off between covering all attacks and the number of false alarms
  - (False) alarm investigation is resource demanding

Base rate Fallacy

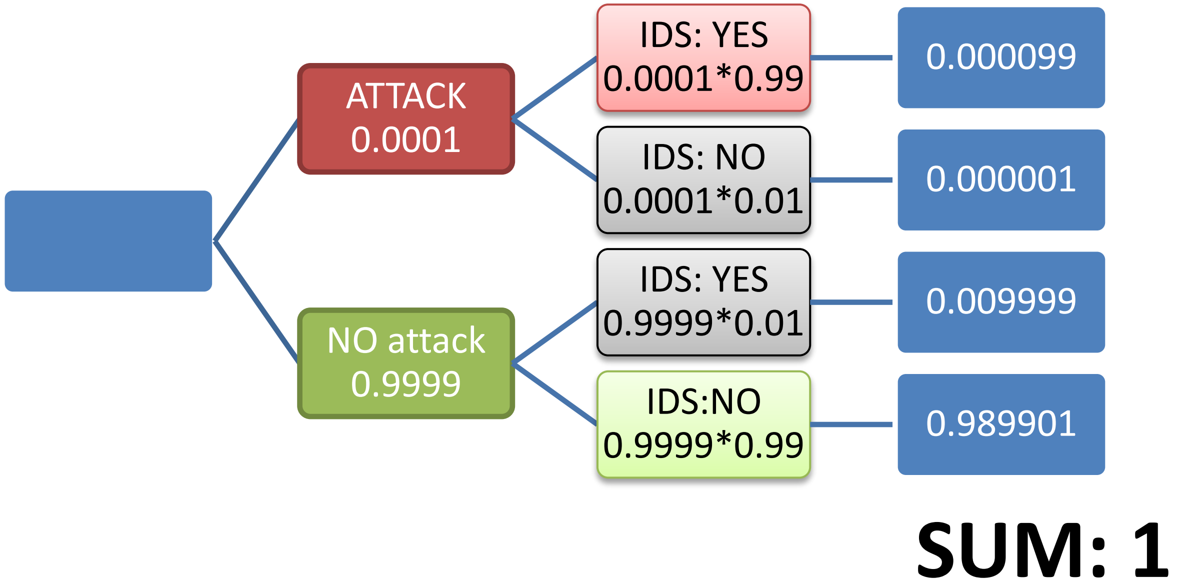
- Accuracy is 99%
- Number of attacks: 0.01% in analyzed data.

	attack	no attack
alarm	True Positive	False Positive
no alarm	False Negative	True Negative

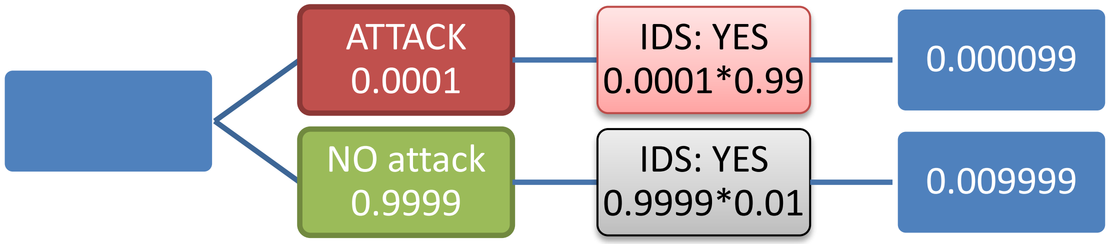
- Accuracy = TP + TN / all
- In this case: (TP+FN) / all = 0.0001
  ➔ (FP+TN) / all = 0.9999


ATTACK
0.0001
NO attack
0.9999
IDS: YES
0.0001*0.99
IDS: NO
0.0001*0.01
IDS: YES
0.9999*0.01
IDS:NO
0.9999*0.99
0.000099
0.000001
0.009999
0.989901

SUM: 1



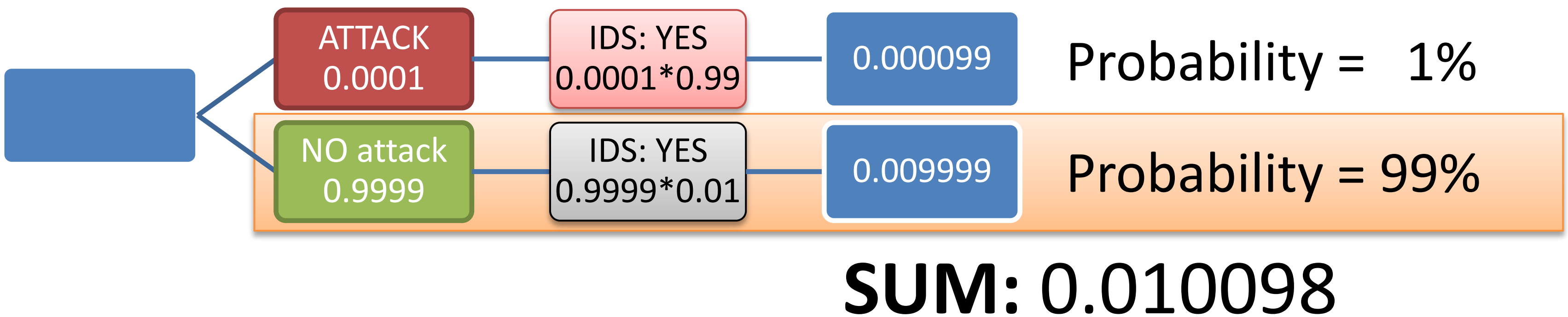
We got an alarm – is it true or false?



SUM: 0.010098

We got an alarm – is it true or false?

Remove all cases that no longer can be true.



We got an alarm – is it true or false?
Remove all cases that no longer can be true.

Problem area 1

- False alarms
  - MANY alarms
  - If detection is 99% correct and the number of intrusions is 0.01% in the analysed information: 99% of all alarms will be false alarms!
  - There is a trade-off between covering all attacks and the number of false alarms
  - (False) alarm investigation is resource demanding

Problem area 2

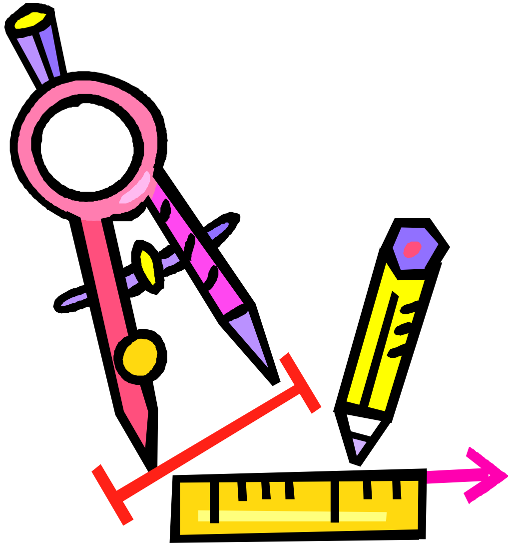
- Adaptation/Portability
  - You can not buy a detection system that is adapted to your computer system
  - The services provided are often unique
  - The user behaviour varies
  - The adaptation of a (simple) network based IDS may require two weeks of work

Problem area 3

- Scalability
  - Network-based IDS – network speeds
  - One sensor, many sensors (office network)
  - One sensor, many sensors (Internet of Things)

Problem area 4

- Test methods



  - there is normally no IDS specification that states what intrusions the system covers
  - Only (?) DARPA has made a comparative study, which has been much criticized (Lincoln Lab data 1999)

A few practical problems

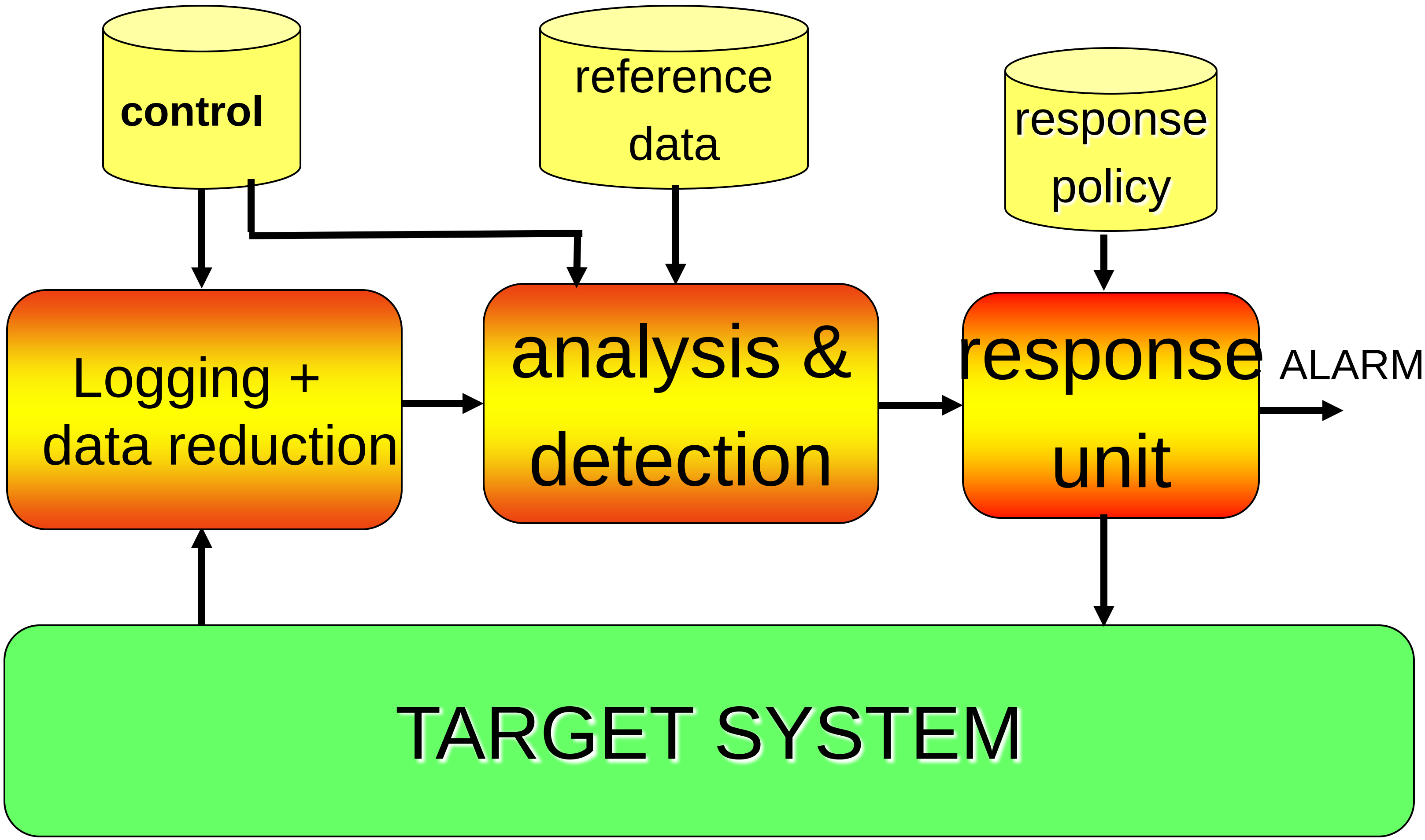
1. False alarms
2. Adaptivity/Portability
3. Scalability
4. Lack of test methods
5. Privacy concerns

The future

Intrusion prevention systems (IPS)

- Is ”hot” right now
- Gartner Group report: ”IDS is dead, long live IPS”
- The meaning of IPS is not well defined – it is rather a commercial term
- The ”best” interpretation is an IDS with some kind of response function, such as
  - reconfiguring a firewall
  - disrupt TCP connections
  - discontinue services
  - stop system calls (in runtime)

Components in an IDS with response function



The future

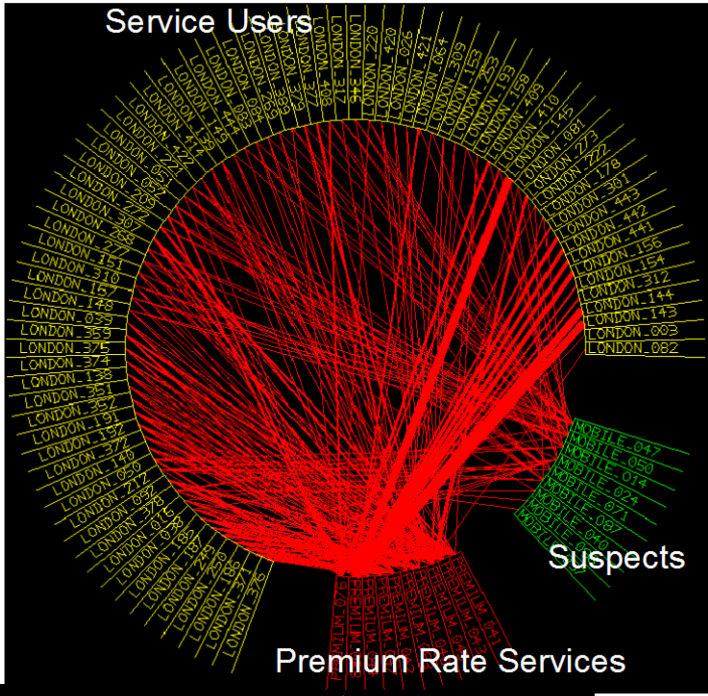
- “earlier” detection, detection of “unwanted behaviour”, i.e. potential intrusion attempts, pro-active data collection more intelligent systems
- diversion, deflection, “honey pots”
- active countermeasures
- “strike back” !?
  (not to be recommend!)
- truly distributed systems
  (alert correlation)
- fraud detection

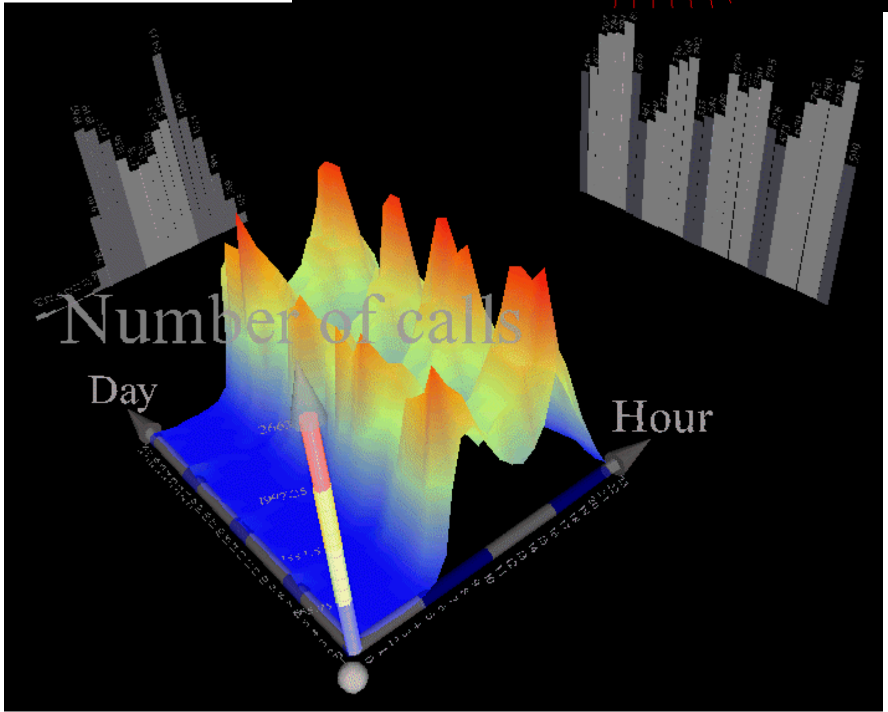
Future threats

- Threat 1: higher transmission rates make network data collection hard (or even impossible)
- Threat 2: increased use of encryption reduces the amount of useful data.

Future possibilities

- New detection methods
  - Visualization
    - Find patterns and anomolous behaviour
    - Use the qualities of the human brain!
- Combining methods
- Intrusion tolerance





Honeypots

A Honeypot is a decoy system, designed to lure a potential attacker. Thus, these systems are made to look like a real system, as far as possible, but they are completely faked.

The goals of a honeypot are:

- collecting information of attacker activity
- diverting attackers (from the real system)
- encourage the attacker to stay long enough on the system for the administrator to respond

The honeypot can be mounted:

in the internal or external network or in the DMZ

Honeypots (cont'd)

Honeypot are of two different types (at least):

- production honeypots
  - easy to use
  - gathers limited information
  - used by companies, etc
- research honeypots
  - complex to deploy and maintain
  - gathers extensive information, intended for research and long-term use
  - used by academia, military, governments, etc