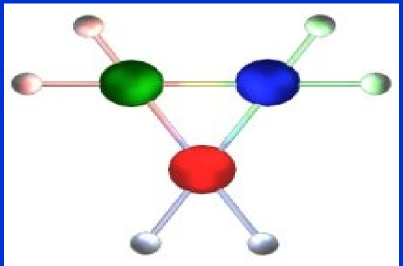
# *Computer intrusions and insider misuse*

***George B. Magklaras BSc (Hons)***

The Network Research Group (NRG)

University of Plymouth

***email: semaphore@jack.see.plym.ac.uk***



# An overview of the main topics:

- Introduction to the concept of IT system intrusions.
- The concept of insider misuse.
- How do we tackle insider misuse?
  - The derivation of an insider misuse taxonomy
  - Complementary techniques
  - The Insider Threat Prediction Tool (ITPT)
- Question time

# A look at the magnitude of the problem:

‘Which of the following types of electronic attack or misuse has your organization detected within the last 12 months?’

- 11% detected financial fraud
- 17% detected sabotage of data and/or networks
- 20% detected theft of proprietary information
- **25% detected system penetration from the outside**
- 27% detected a DoS attack
- **71% detected unauthorised access by insiders**.
- **79% detected employee abuse of Internet access privileges**
- **85% detected viruses**

***Source: 2000 CSI/FBI Computer Crime and Security Survey***

# Financial implications of IT intrusions:

| Type of intrusion: | 1999 | 2000 |
|---|---|---|
| •Theft of proprietary information | $1.8M | $1.1M |
| •*System penetration by outsider* | *$103K* | *$172K* |
| •*Unauthorized insider access* | *$142K* | *$1.0M* |
| •Computer viruses | $1.0M | $10M |
| •Denial of service | $116K | $108K |
| •Laptop theft | $86K | $6K |
| •Insider abuse of Internet access | $93K | $165K |

***Source: 2000 CSI/FBI Computer Crime and Security Survey***

# The concept and the classification of intrusions:

"In an IT context, an intrusion is considered as a sequence of related actions by a ***malicious*** adversary that results in the occurrence of **unauthorized security threats** to a target ***computing*** or ***networking*** domain".

**- Edward Amoroso - AT&T Labs**

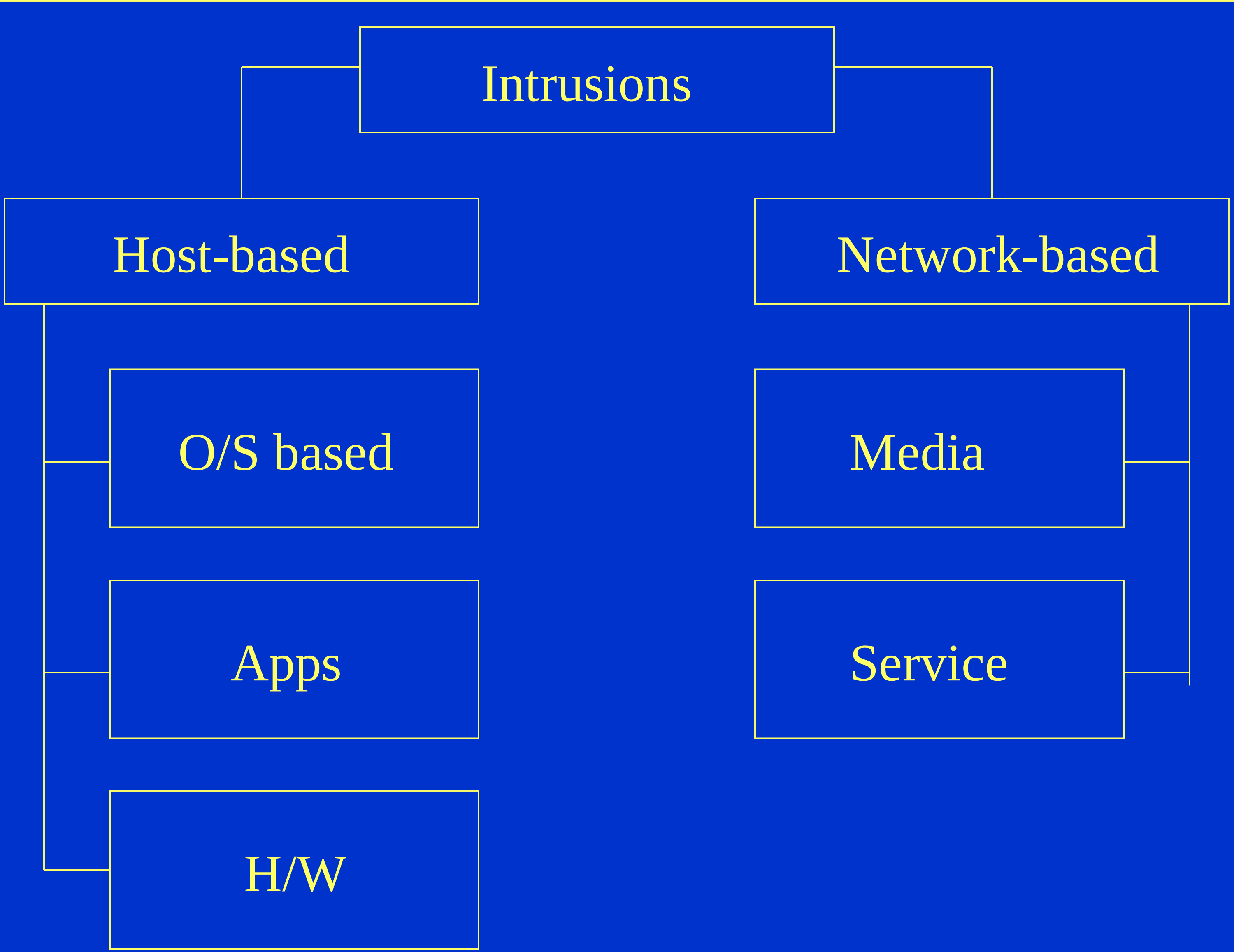
- Intrusion Taxonomies and computer security research community.

# Existing Intrusion Taxonomies:

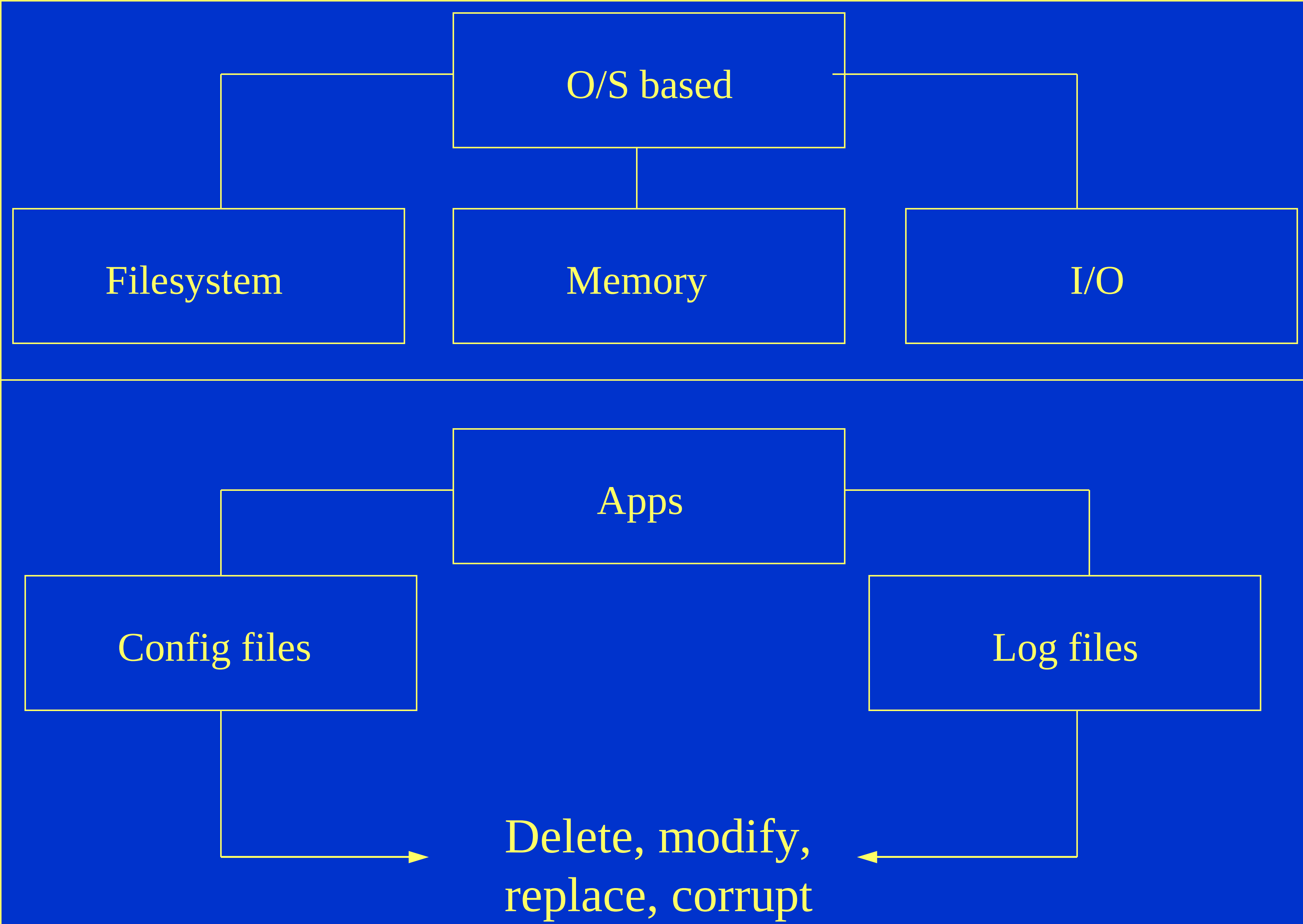
- **SRI Neumann-Parker Taxonomy**
- **Lindqvist and Jonssen's intrusion taxonomy**
- **John Howard's security incident analysis**

All of these taxonomies are not tailored for improving the research and development (R&D)of Intrusion Detection Systems. R&D issues may include:

- Investigation of IDS algorithms
- IDS integrity
- **Intrusion Specification Language**



**NRG proposed intrusion taxonomy (levels 1 and 2)**



O/S based

Filesystem

Memory

I/O

Apps

Config files

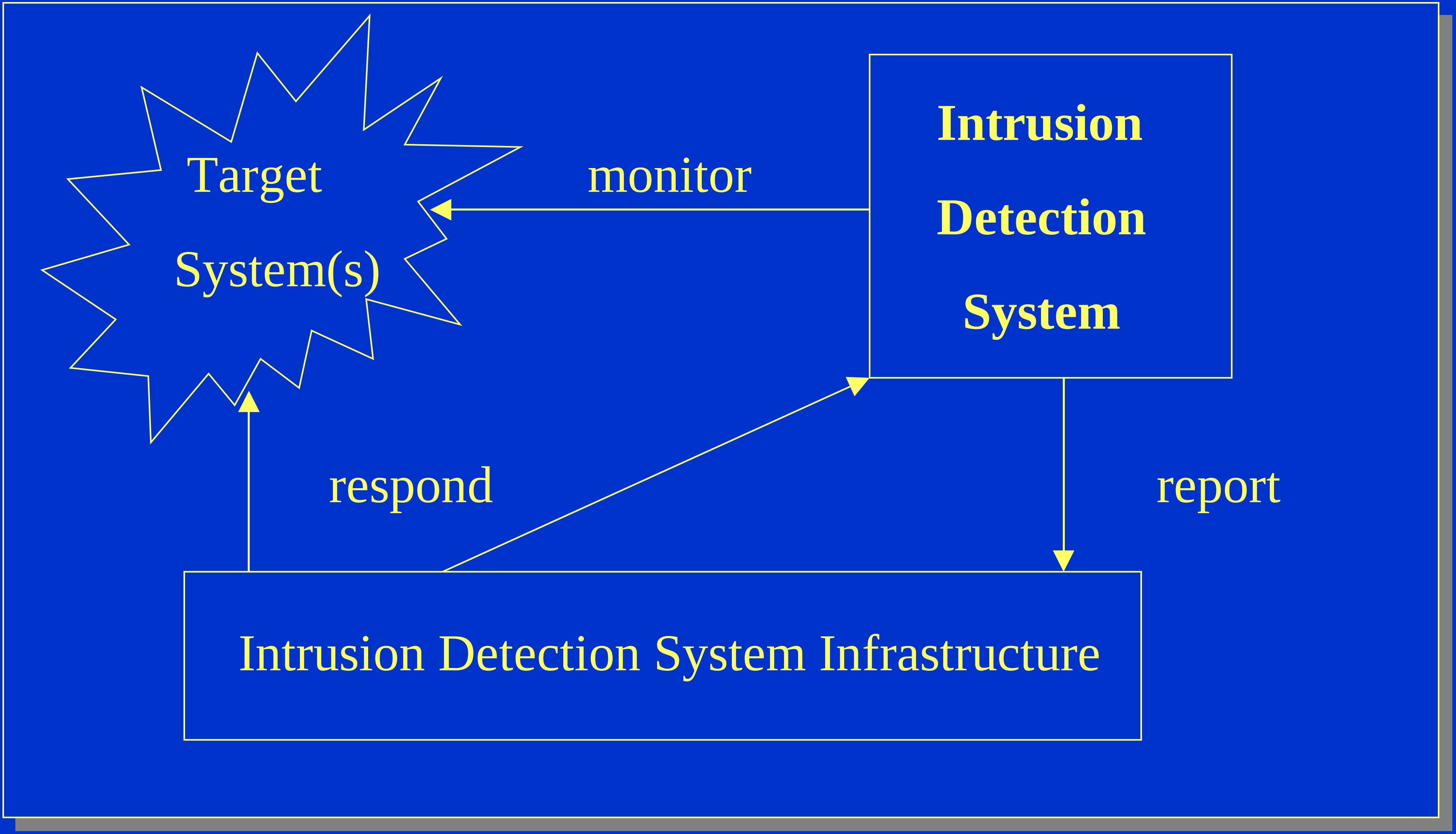
Log files

Delete, modify, replace, corrupt

# How do we combat IT intrusions?

- Traditional system maintenance tasks: upgrading and fixing software and hardware faults (operating system patching, application and hardware upgrades).
- Employment and update of anti-virus packages
- Use of data encryption technologies
- Use of firewalls to filter network traffic
- **Employment of Intrusion Detection Systems (IDS):**These tools monitor the events occurring in a computer system or network and search for indications of security-related problems.
- **Ideally, an organisation should employ all of the previously mentioned methods**.

# Simple Depiction of an Intrusion Detection System:


Target System(s)
monitor
Intrusion Detection System
respond
report
Intrusion Detection System Infrastructure

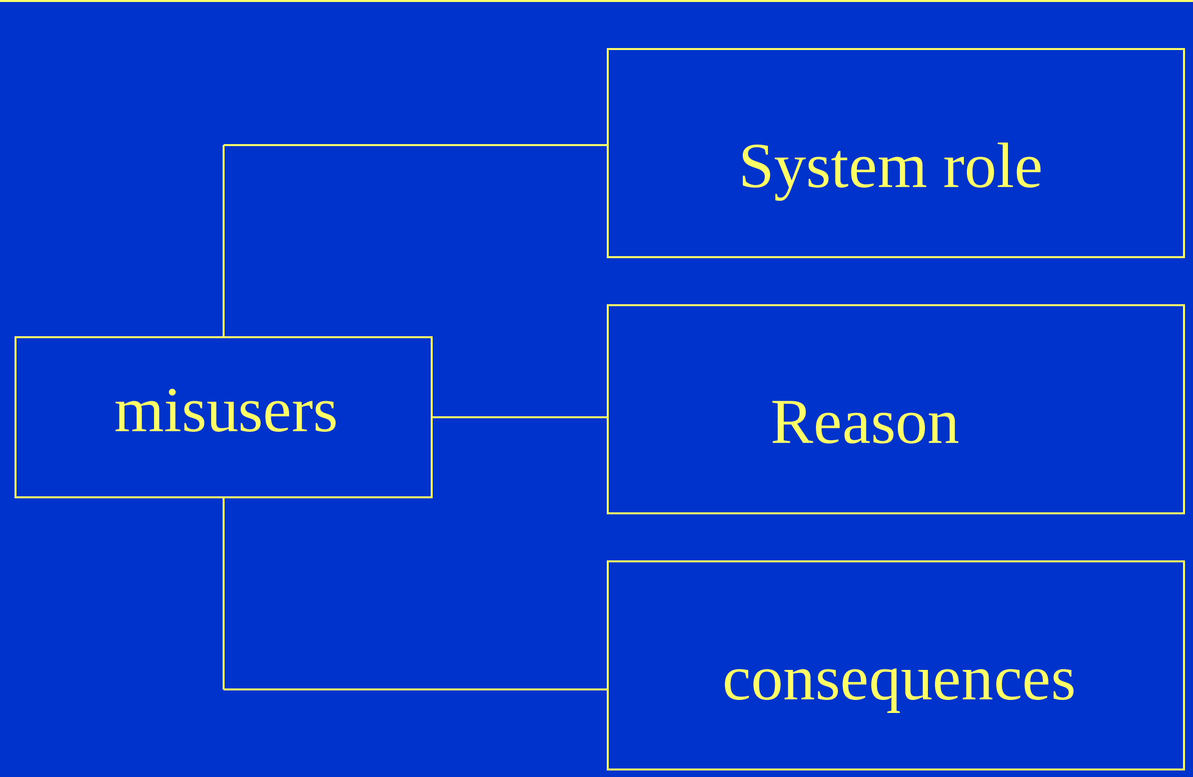
# *Are Intrusion Detection Systems a panacea?*

- An IDS may not recognise a new type of intrusion.
- They might give a large number of false positive alarms.
- Some IDS algorithms require extensive CPU resources:
  - Scalability is a problem.
  - Automated response to intrusive activities is limited.
- They do not address extensively insider threats

# The nature of the insider IT misuse:

- It is the fastest growing problem in the field of IT security.
- **Insider :** a user that has legitimate access to IT system resources and belongs to a particular organisation.
- **Misuse:** to use (something) in a wrong way or for a wrong purpose - Longman Dictionary of Contemporary English
- **Insider misuse:** A vague term: The act of causing harm to the system by abusing your legitimate privileges….
- The role of the information security policy:A *set of laws, rules, practices, norms and fashions that regulate how an organisation manages, protects, and distributes the sensitive information whilst regulating how an organisation protects system services*.

# The NRG insider misuse taxonomy:


misusers

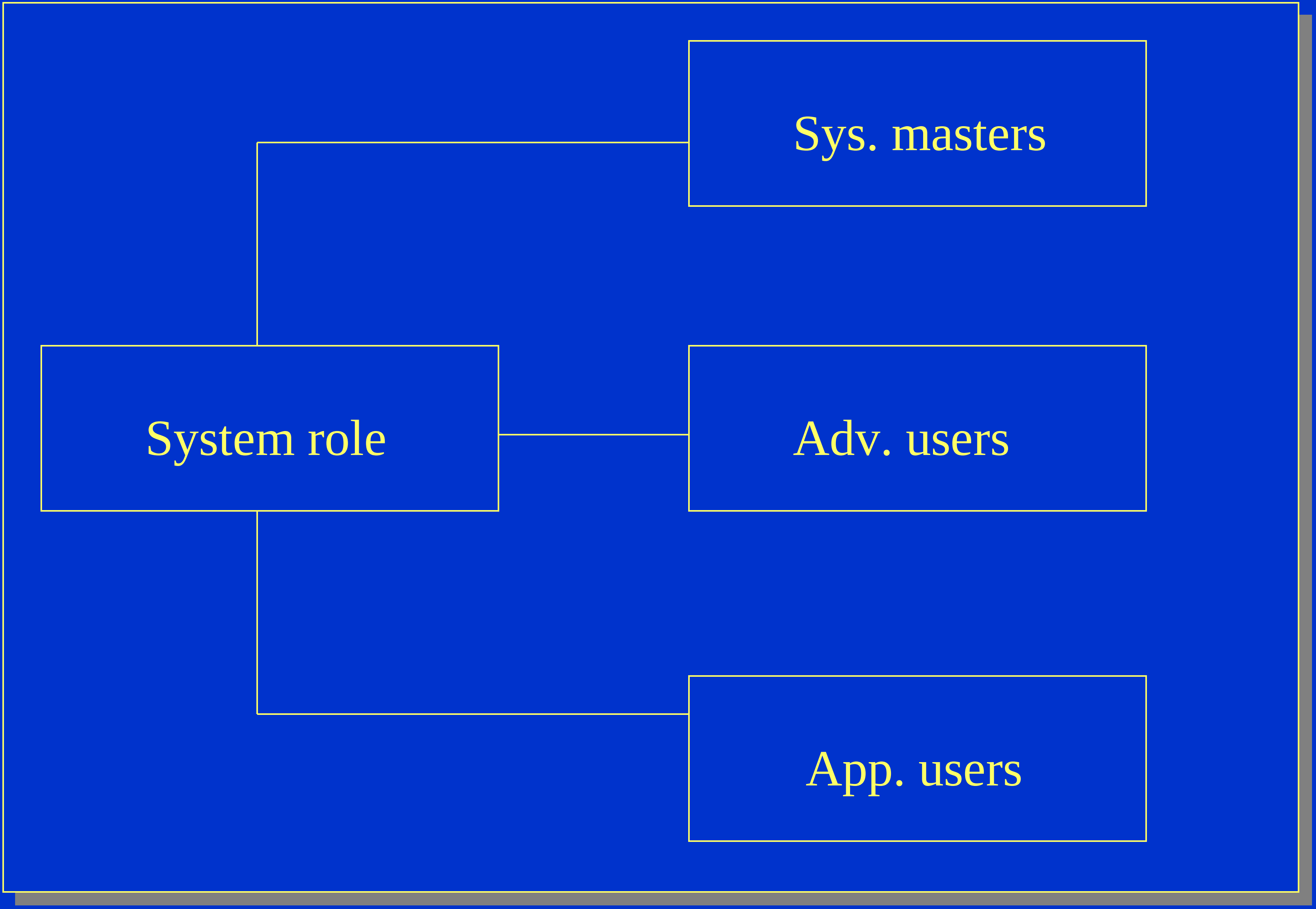
System role

Reason

consequences

NRG insider misuse taxonomy level 1

# Insider classification by system role:



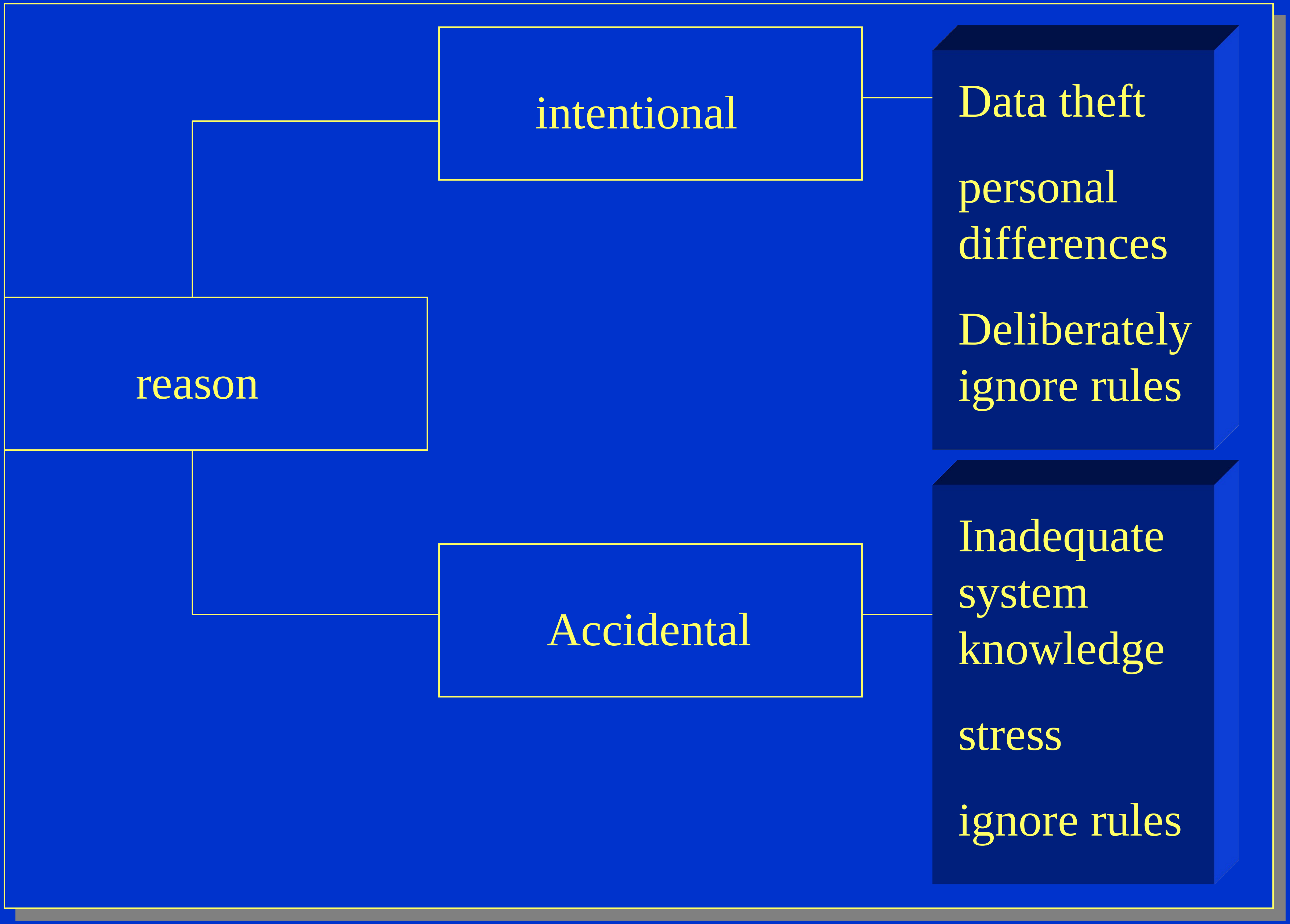
System role

Sys. masters

Adv. users

App. users

# Insider misuse classification by reason of misuse:



reason

intentional

Data theft

personal differences

Deliberately ignore rules

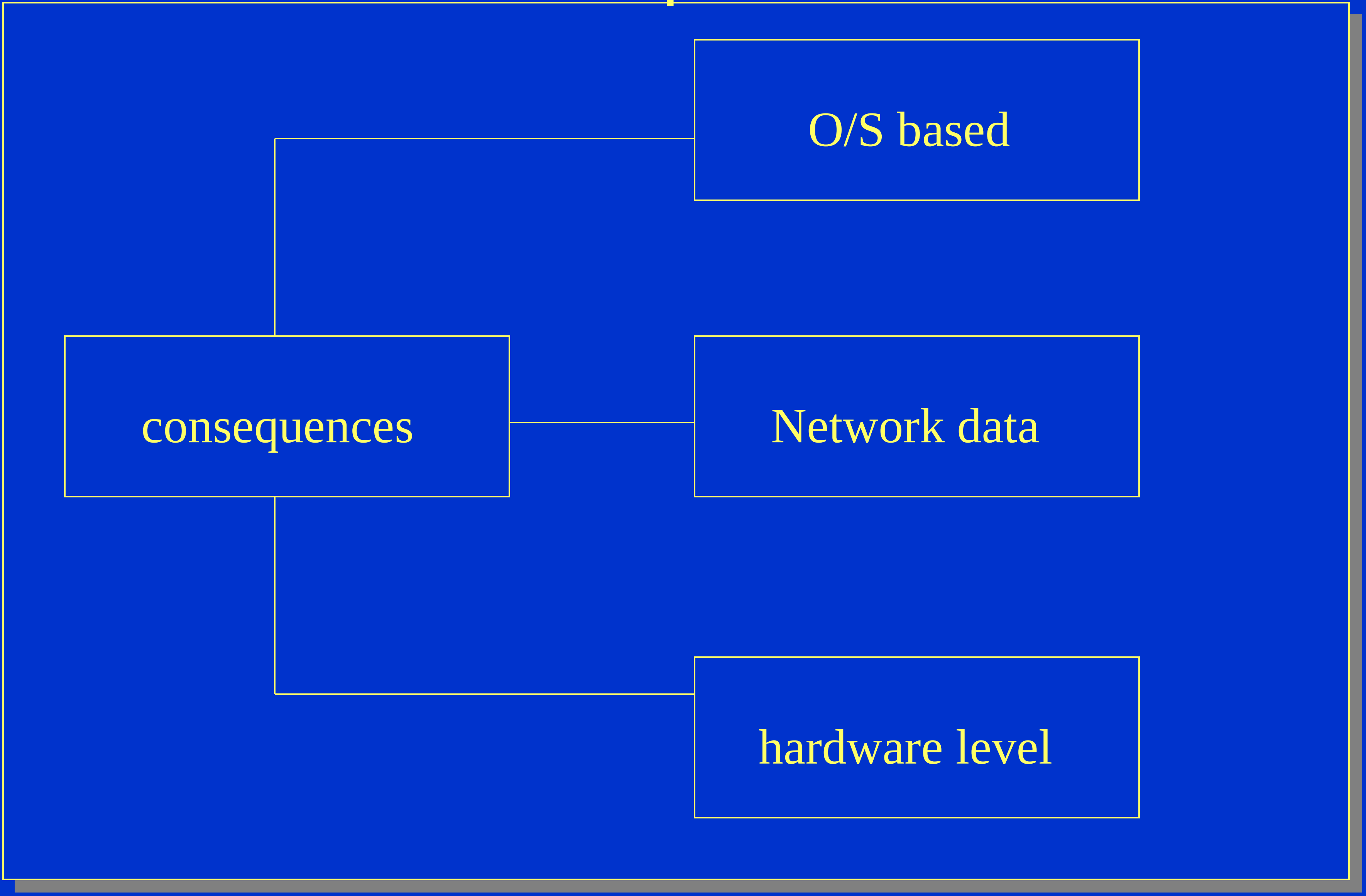
Accidental

Inadequate system knowledge

stress

ignore rules

# Insider misuse classification by system consequences:



# How do we tackle the problem of insiders?

- **Non system based approaches**:

  - Pre- employment screening procedures.

  - Employment of behavioral profiling psychologists.

  - Social engineering (error prone but sometimes useful)

  - Make sure that your information security policy is presented to your employees in a frequent and friendly manner.

- **System-based approaches**:

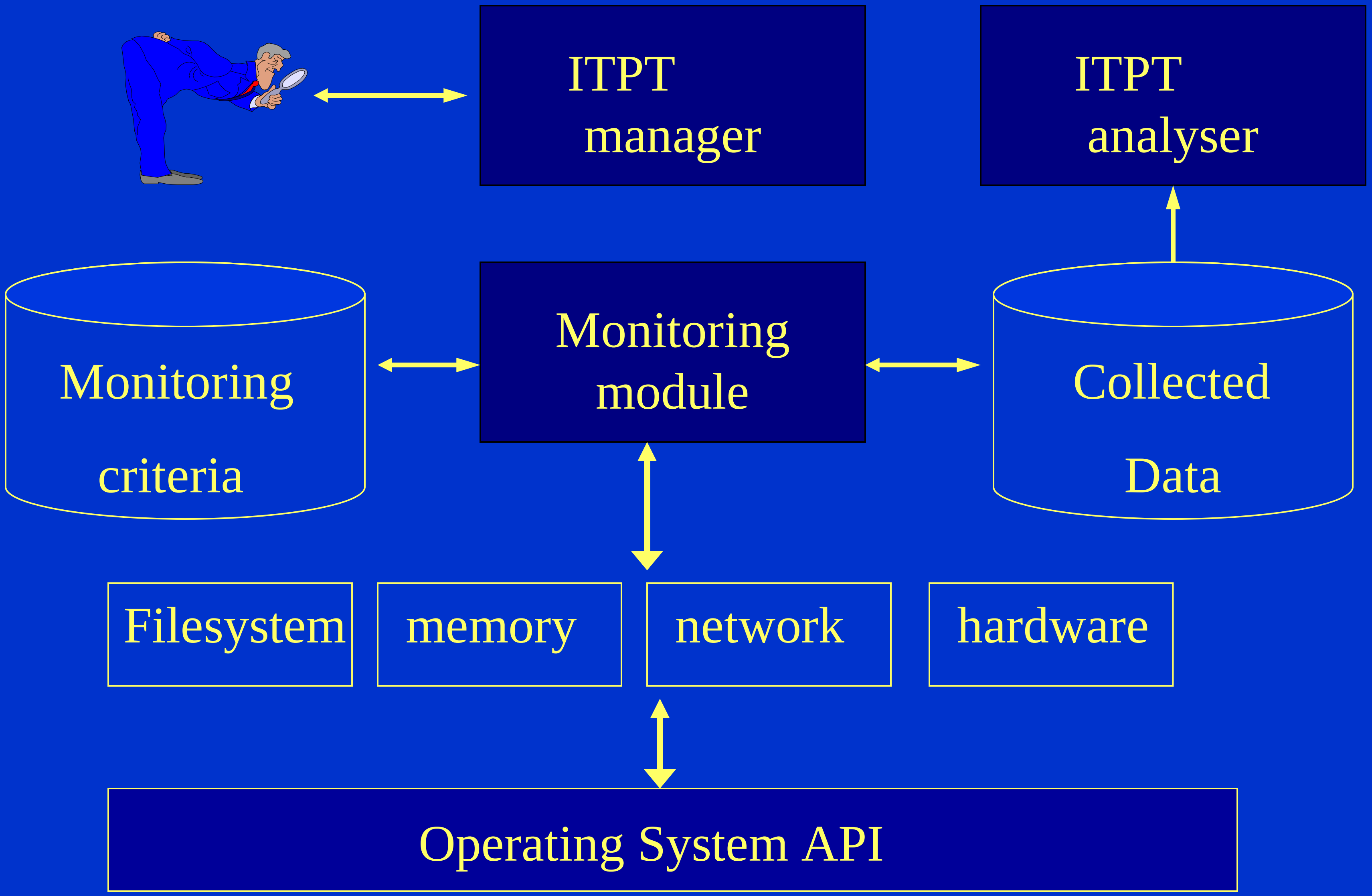
  - Investigate what features of your existing IDS, firewall and other security tools can be used to monitor or profile legitimate users.

  - Make sure that the monitoring techniques you use are compliant with existing legislation. Let users know they are being monitored.

# The Insider Threat Prediction Tool (ITPT):

- Most security tools are designed to address ‘threats’.
- Traditional security tools address threats at the moment of their occurrence.
- Attack estimation might be better than attack detection for detecting IT misuse.
- Thus, a system that relates legitimate user actions to the probability of performing a particular type of attack might be desirable.

# ITPT high-level module architecture:



ITPT manager

ITPT analyser

Monitoring criteria

Monitoring module

Collected Data

Filesystem

memory

network

hardware

Operating System API