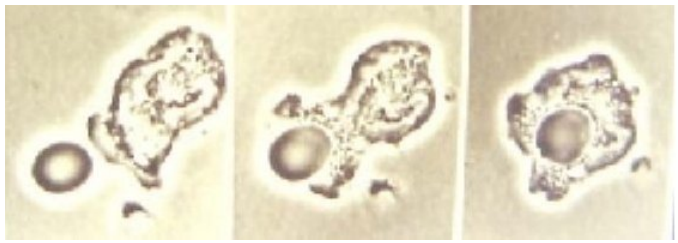
Intrusion Detection *vs* Virology

Benjamin Morin
benjamin.morin@supelec.fr
http://www.rennes.supelec.fr/ren/perso/bmorin/

Supélec, Rennes, France

May 4, 2006



Supélec

Introduction

Context

- I have been working in intrusion detection for the past five years
- But I don't know much about viruses (if not anything)
- I believe I am not the only one in this case
- However it seems we are basically talking about similar things

Objective of this talk

- Give a big picture of intrusion detection
- Position virology in the intrusion detection field

Outline

Outline

Outline

Outline

Plan

What is Intrusion Detection ?

What kind of definition ?

An Anderson-like definition ?

- Anderson gave the fundations of intrusion detection in the 80's
- Genuine definition

An IDS-like definition ?

- IDS stands for *Intrusion Detection Systems*
- What do IDSes *actually* do ?

A RAID scope-like definition ?

- RAID stands for *Recent Advances in Intrusion Detection*
- Main conference in the field
- `http://www.raid-symposium.org`

What is Intrusion Detection ?

What kind of definition ?

An Anderson-like definition ?

- Anderson gave the fundations of intrusion detection in the 80's
- Genuine definition

An IDS-like definition ?

- IDS stands for *Intrusion Detection Systems*
- What do IDSes *actually* do ?

A RAID scope-like definition ?

- RAID stands for *Recent Advances in Intrusion Detection*
- Main conference in the field
- `http://www.raid-symposium.org`

What is Intrusion Detection ?

What kind of definition ?

An Anderson-like definition ?

- Anderson gave the fundations of intrusion detection in the 80's
- Genuine definition

An IDS-like definition ?

- IDS stands for *Intrusion Detection Systems*
- What do IDSes *actually* do ?

A RAID scope-like definition ?

- RAID stands for *Recent Advances in Intrusion Detection*
- Main conference in the field
- `http://www.raid-symposium.org`

What is Intrusion Detection ?

What kind of definition ?

An Anderson-like definition ?

- Anderson gave the fundations of intrusion detection in the 80's
- Genuine definition

An IDS-like definition ?

- IDS stands for *Intrusion Detection Systems*
- What do IDSes *actually* do ?

A RAID scope-like definition ?

- RAID stands for *Recent Advances in Intrusion Detection*
- Main conference in the field
- `http://www.raid-symposium.org`

Genuine definition of intrusion detection

The goal of intrusion detection is to detect violations of a security policy, *i.e.*, violations of confidentiality, integrity, availability.

Problems & Questions

- Security policies are not always formally defined
  - Policy rules are generally implicit or fall within good sense
- Suspicious activities are not necessarily security policies violations *per se*
  - Shall only *successful* violations be reported ?

Intrusion Detection technologies have moved progressively to bypass these ambiguities

Genuine definition of intrusion detection

The goal of intrusion detection is to detect violations of a security policy, *i.e.*, violations of confidentiality, integrity, availability.

Problems & Questions

- Security policies are not always formally defined
  - Policy rules are generally implicit or fall within good sense
- Suspicious activities are not necessarily security policies violations *per se*
  - Shall only *successful* violations be reported ?

Intrusion Detection technologies have moved progressively to bypass these ambiguities

Genuine definition of intrusion detection

The goal of intrusion detection is to detect violations of a security policy, *i.e.*, violations of confidentiality, integrity, availability.

Problems & Questions

- Security policies are not always formally defined
  - Policy rules are generally implicit or fall within good sense
- Suspicious activities are not necessarily security policies violations *per se*
  - Shall only *successful* violations be reported ?

Intrusion Detection technologies have moved progressively to bypass these ambiguities

What do [most of currently deployed] IDSes detect ?

Do IDSes *only* detect ...

- ... intrusions (*i.e.*, successful attacks) ?
  - Alerts generally do not assess the success or failure of attacks
- ... attacks (*i.e.*, actual vulnerabilities exploits) ?
  - Many alerts refer to *legal* activities which are sometimes attacks
- ... potentially malicious activities ?
  - which include attacks and intrusions.

Do IDSes detect *all*...

- ... malicious activities ?
  - IDSes still miss attacks

What do [most of currently deployed] IDSes detect ?

Do IDSes *only* detect ...

- ~~... intrusions (*i.e.*, successful attacks) ?~~
  - Alerts generally do not assess the success or failure of attacks
- ... attacks (*i.e.*, actual vulnerabilities exploits) ?
  - Many alerts refer to *legal* activities which are sometimes attacks
- ... potentially malicious activities ?
  - which include attacks and intrusions.

Do IDSes detect *all*...

- ... malicious activities ?
  - IDSes still miss attacks

What do [most of currently deployed] IDSes detect ?

Do IDSes *only* detect ...

- ~~... intrusions (*i.e.*, successful attacks) ?~~
  - Alerts generally do not assess the success or failure of attacks
- ~~... attacks (*i.e.*, actual vulnerabilities exploits) ?~~
  - Many alerts refer to *legal* activities which are sometimes attacks
- ... potentially malicious activities ?
  - which include attacks and intrusions.

Do IDSes detect *all*...

- ... malicious activities ?
  - IDSes still miss attacks

What do [most of currently deployed] IDSes detect ?

Do IDSes *only* detect ...

- ~~... intrusions (*i.e.*, successful attacks) ?~~
  - Alerts generally do not assess the success or failure of attacks
- ~~... attacks (*i.e.*, actual vulnerabilities exploits) ?~~
  - Many alerts refer to *legal* activities which are sometimes attacks
- ... potentially malicious activities ?
  - which include attacks and intrusions.

Do IDSes detect *all*...

- ... malicious activities ?
  - IDSes still miss attacks

What do [most of currently deployed] IDSes detect ?

Do IDSes *only* detect ...

- ~~... intrusions (*i.e.*, successful attacks) ?~~
  - Alerts generally do not assess the success or failure of attacks
- ~~... attacks (*i.e.*, actual vulnerabilities exploits) ?~~
  - Many alerts refer to *legal* activities which are sometimes attacks
- ... potentially malicious activities ?
  - which include attacks and intrusions.

Do IDSes detect *all*...

- ~~... malicious activities ?~~
  - IDSes still miss attacks

Scope of RAID (wide)

Springer Keywords

intrusion detection network security secure communications	intrusion prevention IDS security	network intrusion anomaly detection
worm detection	distributed intrusion	
spoof detection mimicry attacks	portscan detection	deception systems
log-data analysis execution data mining	pattern analysis	data mining
access control risk management	audit control	logging
authentication ~~cryptographic attacks~~	privacy ~~cryptanalysis~~	

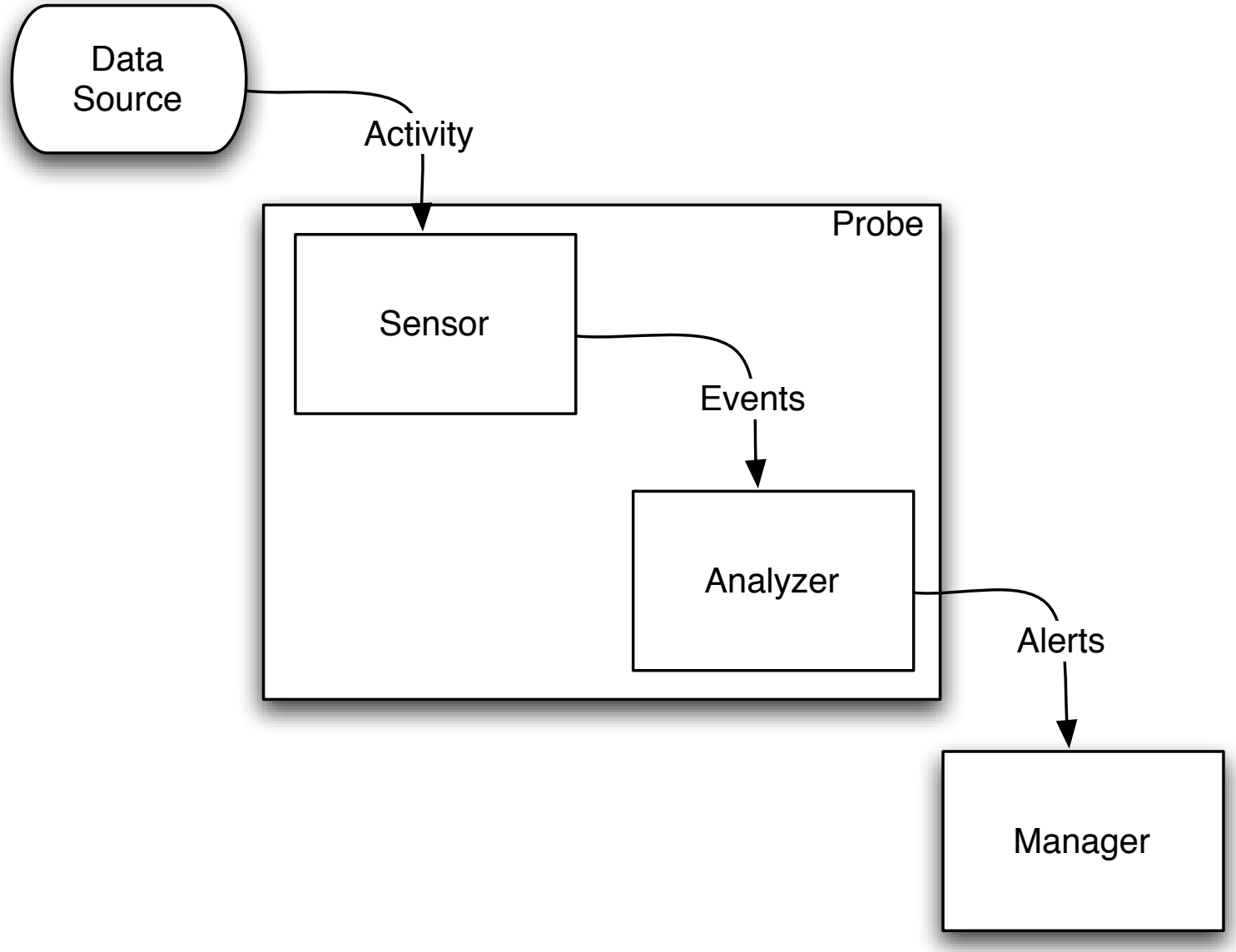
Scope of RAID (wide)

Session titles

Intrusion Prevention and Response	Intrusion Tolerance
System Call-Based Intr. Det.	Network-Based Intr. Det.
Anomaly Detection	Modelling process behaviour
Vulnerability Definitions	Modeling Attacks
Specification-Based IDS	Adaptive IDS
Worm Detection and Containment	Detecting Worms and Viruses
Attack and Alert Analysis	Correlation
IDS Cooperation	IDS Sensors
Modeling and Specification	Formal Analysis for Intrusion Detection
Network Infrastructure	Mobile and Wireless Networks
Data Mining	Handling intrusion-detection data
Stepping Stone Detection	
Intrusion Detection Analysis	Logging and IDS Integration
Legal Aspects	Assessment of IDS

Plan

Architecture of an IDS



Data sources

Network-based IDS (NIDS, *a.k.a* IPreventionS)

- Gather network packets through a dedicated network interface (promiscuous mode)
- Analysis of the content of headers and payloads
- Session reconstruction and application-level protocol reassembly

Host-based IDS (HIDS)

- System calls executed by operating systems for applications
- Audit system log files (*e.g.*, logins, user commands)

Applicative

- Applicative audit log files (*e.g.*, web server, databases, ...)

Data sources

Network-based IDS (NIDS, *a.k.a* IPreventionS)

- Gather network packets through a dedicated network interface (promiscuous mode)
- Analysis of the content of headers and payloads
- Session reconstruction and application-level protocol reassembly

Host-based IDS (HIDS)

- System calls executed by operating systems for applications
- Audit system log files (*e.g.*, logins, user commands)

Applicative

- Applicative audit log files (*e.g.*, web server, databases, ...)

Data sources

Network-based IDS (NIDS, *a.k.a* IPreventionS)

- Gather network packets through a dedicated network interface (promiscuous mode)
- Analysis of the content of headers and payloads
- Session reconstruction and application-level protocol reassembly

Host-based IDS (HIDS)

- System calls executed by operating systems for applications
- Audit system log files (*e.g.*, logins, user commands)

Applicative

- Applicative audit log files (*e.g.*, web server, databases, ...)

Type of analysis

Anomaly detection

- Attacks are detected by measuring a significant deviation of the behaviour of the monitored system with regard to a reference behaviour, supposed safe.
- Requires the building of the *normal* behavior model, generally through learning techniques
- All that is not allowed is forbidden.

Misuse detection

- Attacks are detected by the occurence of an attack pattern (*i.e.*, a signature) within a data source.
- Requires a database of known attack patterns.
- All that is not forbidden is allowed.

Type of analysis

Anomaly detection

- Attacks are detected by measuring a significant deviation of the behaviour of the monitored system with regard to a reference behaviour, supposed safe.
- Requires the building of the *normal* behavior model, generally through learning techniques
- All that is not allowed is forbidden.

Misuse detection

- Attacks are detected by the occurence of an attack pattern (*i.e.*, a signature) within a data source.
- Requires a database of known attack patterns.
- All that is not forbidden is allowed.

Qualifying IDSes

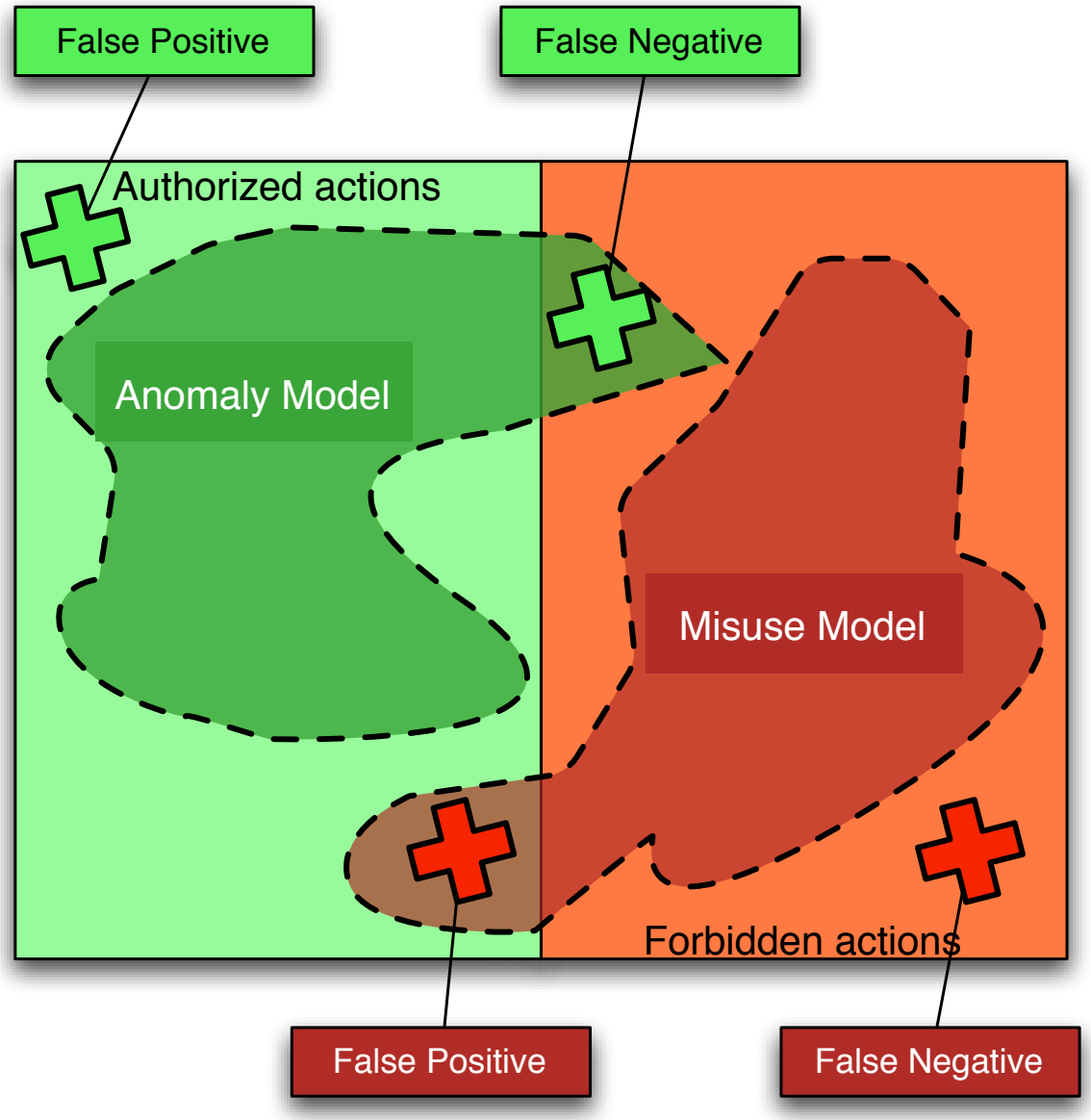
Accuracy

- Ability of an IDS to detect *only* attacks
- Measured with the false positive rate (alert in the absence of an attack)

Completeness

- Ability of an IDS to detect *all* attacks
- Measured with the false negative rate (attack in the absence of an alert)

False positives and false negatives



Classical Models : Pros and Cons

Misuse Detection

+ Generally accurate (low false positive rate) ...
- ... but using too generic signatures for efficiency reasons leads to decrease the accuracy (increase false positives)
- A signature database to be maintained : if not, decrease the completeness (increase false negatives)

Anomaly Detection

+ Generally complete (low false negative rate)
+ Ability to detect unknown attacks
+ Better maintainability
- Low accuracy (many false positives)
- No diagnosis

Classical Models : Pros and Cons

Misuse Detection

+ Generally accurate (low false positive rate) ...
- ... but using too generic signatures for efficiency reasons leads to decrease the accuracy (increase false positives)
- A signature database to be maintained : if not, decrease the completeness (increase false negatives)

Anomaly Detection

+ Generally complete (low false negative rate)
+ Ability to detect unknown attacks
+ Better maintainability
- Low accuracy (many false positives)
- No diagnosis

Two opposite examples : Forrest *vs* Roesch

Roesch approach (Snort)

- Misuse NIDS whose signatures are regular expressions
- Very simple, most popular IDS

Forrest approach

- Anomaly HIDS, also knows as immunological approach
- Model of the applications behavior composed of fixed-length system call sequences obtained by learning techniques
- Several variants proposed (variable length sequences, with system call parameters)

Which IDSes are currently used ?

NIDS

+ Ease of use and deployment
- Increasing network load
- Ciphered communications

Misuse analysis

+ Ease of maintenance
+ (Supposedly) few false positives
- Fail to detect unknown attacks

Where to go from here ?

Make Misuse and Anomaly Detectors Cooperate

- Parallel combination
- Serial combination
- Alert correlation

Improve the Quality of the Probes

- Multi-events pattern matching (misuse detection)
- Better learning process (anomaly detection)
- Alternative anomaly-based approaches :
  - Specification-based detection
  - Policy-based detection

Where to go from here ?

Make Misuse and Anomaly Detectors Cooperate

- Parallel combination
- Serial combination
- Alert correlation

Improve the Quality of the Probes

- Multi-events pattern matching (misuse detection)
- Better learning process (anomaly detection)
- Alternative anomaly-based approaches :
  - Specification-based detection
  - Policy-based detection

Plan

Toward a complete and accurate IDS ?

A *specification-based* approach

- Subfield of anomaly detection
- The *accepted* behaviour is obtained
  - through explicit specification
  - not by learning techniques

A *policy-based* approach

- Assumes a security policy is defined (*e.g.*, DAC, Bell-LaPaluda, Chinese Wall)
- Policy properties express *confidentiality* and *integrity* constraints
- These rules define the accepted behaviour of the monitored system
- Allows to detect attacks that lead to confidentiality and integrity violations

Toward a complete and accurate IDS ?

A *specification-based* approach

- Subfield of anomaly detection
- The *accepted* behaviour is obtained
  - through explicit specification
  - not by learning techniques

A *policy-based* approach

- Assumes a security policy is defined (*e.g.*, DAC, Bell-LaPaluda, Chinese Wall)
- Policy properties express *confidentiality* and *integrity* constraints
- These rules define the accepted behaviour of the monitored system
- Allows to detect attacks that lead to confidentiality and integrity violations

So, what's the difference with Access Control ?

Classical Access Control

- Check for the legality of individual operations
- Do not assume the presence of software flaws in the monitored system that enable privilege escalation
- A sequence of operations can be legal wrt the policy...
- ... but result in an illegal state.

Our approach

- Tracks [operating] system state evolution through *information flows*
- An information flow is an executed operation (*i.e.*, a system call) which accesses and modifies objects (*i.e.*, files, sockets, memory pages)
- Detects illegal information flows *wrt* the policy

So, what's the difference with Access Control ?

Classical Access Control

- Check for the legality of individual operations
- Do not assume the presence of software flaws in the monitored system that enable privilege escalation
- A sequence of operations can be legal wrt the policy...
- ... but result in an illegal state.

Our approach

- Tracks [operating] system state evolution through *information flows*
- An information flow is an executed operation (*i.e.*, a system call) which accesses and modifies objects (*i.e.*, files, sockets, memory pages)
- Detects illegal information flows *wrt* the policy

Intrusion Detection theorem (in brief)

Intrusion detection model

Establishes an equivalence relationship between the legality of a trace and the system state evolution :

$$islegal(\sigma, s_n) \Leftrightarrow \text{state changed and allowed by security policy}$$

Completeness of the detection

If an attack occurs (security violation), then an alert is raised (*islegal* is false)

$$islegal(\sigma, s_n) \Leftarrow \text{state changed and allowed by security policy}$$

Accuracy of the detection

If an alert is raised, then an attack occurred

$$islegal(\sigma, s_n) \Rightarrow \text{state changed and allowed by security policy}$$

Coming back to virology...

Would our IDS model detect any virus ?

- Yes, provided that the virus involves a security policy violation...
- ... which is generally not the case (?)

Why ?

- Intrusion detection often (but not always) aims at detecting attacks which exploit a software vulnerability exploitation leading to a security violation
- Viruses often exploit *human* flaws rather than *software* flaws (which is not the case for worms)
  - users inadvertently inoculate the virus in their machine by executing a program.
  - depending on the virus' objective, there is no policy violation *stricto sensu*, since the virus is executed with the user's privileges.

Plan

Conclusion : join us ! :-)

Virology ∩ Intrusion Detection = ∅ ?

- Intrusion detection does not study the viruses internal mechanisms (code)
- Rather, studies the viruses' side effects on the monitored system in order to *detect* them.

Virology ∩ Intrusion Detection ≠ ∅ ?

Worms have been studied in depth

- by the intrusion detection community
- by the virology community

Virology ⊂ Intrusion Detection ?

- The scope of the intrusion detection domain is broad
- Rather call it *operational security*

Conclusion : join us ! :-)

Virology ∩ Intrusion Detection = ∅ ?

- Intrusion detection does not study the viruses internal mechanisms (code)
- Rather, studies the viruses' side effects on the monitored system in order to *detect* them.

Virology ∩ Intrusion Detection ≠ ∅ ?

Worms have been studied in depth

- by the intrusion detection community
- by the virology community

Virology ⊂ Intrusion Detection ?

- The scope of the intrusion detection domain is broad
- Rather call it *operational security*

Conclusion : join us ! :-)

Virology ∩ Intrusion Detection = ∅ ?

- Intrusion detection does not study the viruses internal mechanisms (code)
- Rather, studies the viruses' side effects on the monitored system in order to *detect* them.

Virology ∩ Intrusion Detection ≠ ∅ ?

Worms have been studied in depth

- by the intrusion detection community
- by the virology community

Virology ⊂ Intrusion Detection ?

- The scope of the intrusion detection domain is broad
- Rather call it *operational security*

Thank you !

Questions ?