Intrusion Detection Systems & Honeypots

Jimmy McGibney <jmcgibney@tssg.org>
TSSG, Waterford Institute of Technology, Ireland
INET/IGC 2004, Barcelona, 10 May 2004

Security for the pervasive computing world

Outline

- **Intrusion Detection Systems (IDS)**
  - The Need for IDS
  - Types of Intruder
  - Host-based & Network-based IDS
  - Misuse detection vs Anomaly Detection
  - Effectiveness
  - Interoperability, Performance & Scalability
  - Products
- **Honeypots**
  - Definition & purpose of Honeypot
  - Deployment
  - Level of Interaction
  - Examples
  - Honeynets
- **New approaches & bringing them together**

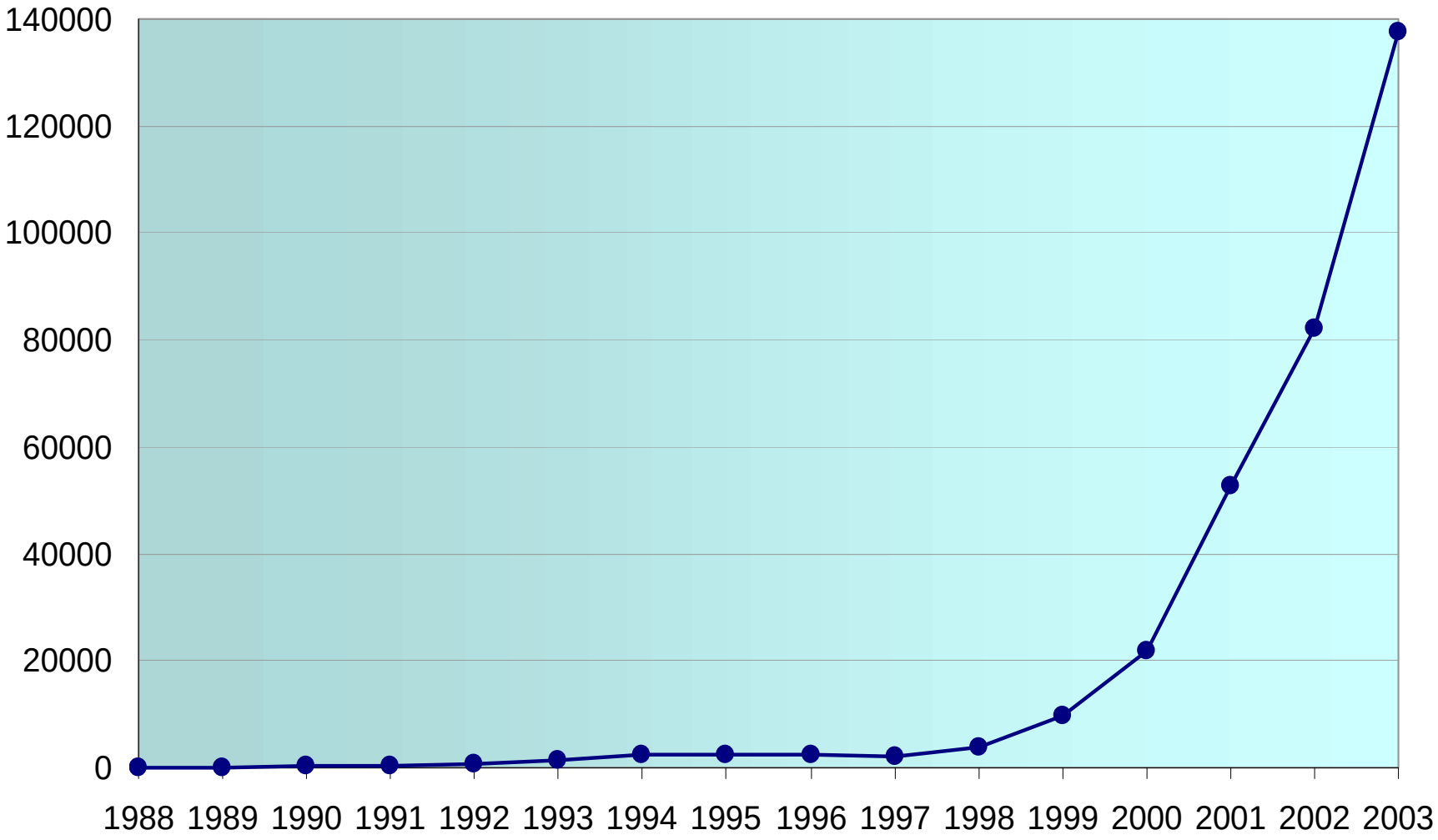
SEINIT

Intrusion Detection Systems

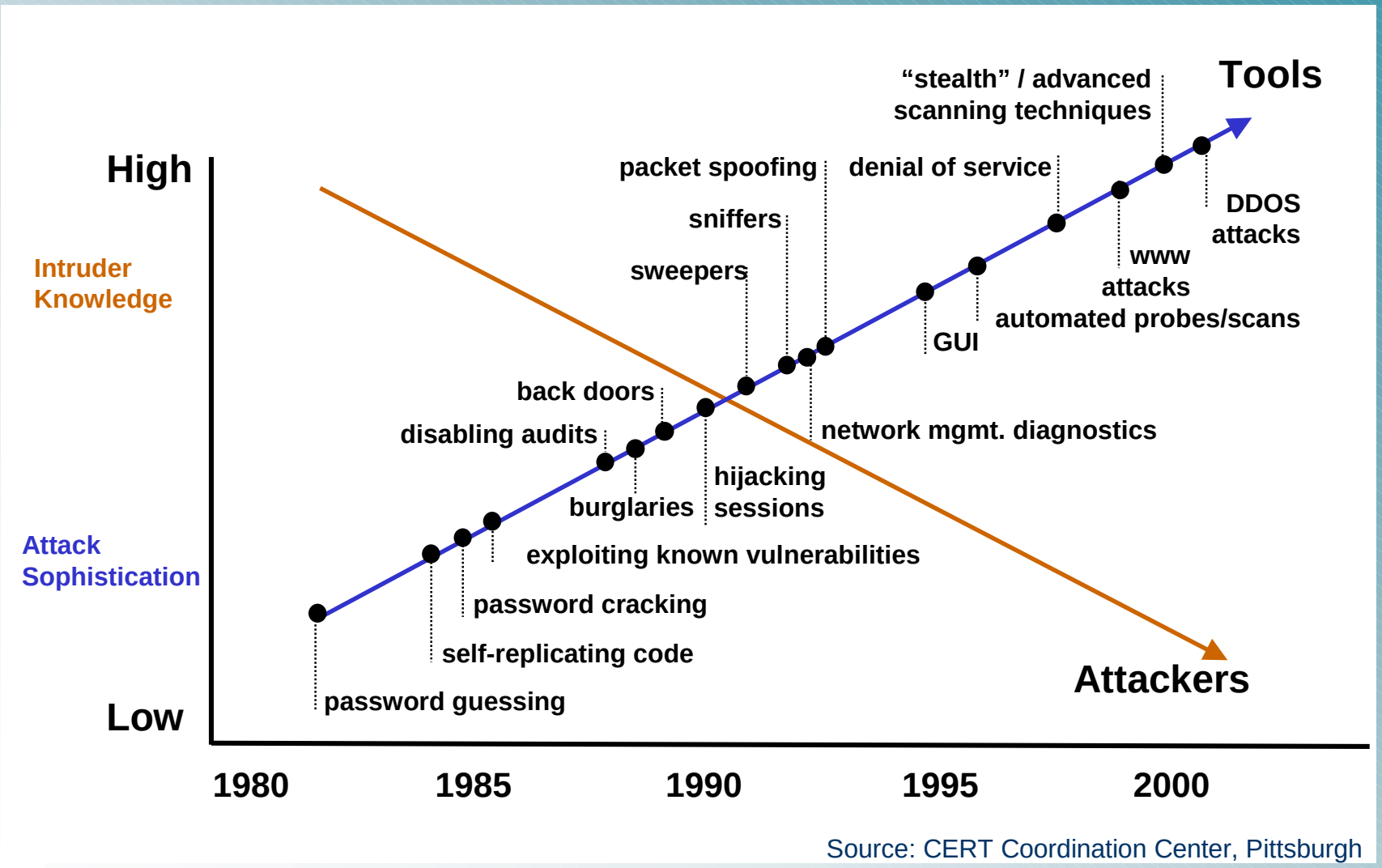
Intruders have all the aces…

- Internet access is easy and cheap
- Hard to analyse all traffic on gigabit (and faster) networks.
- Domination by a small number of OSs (mainly Windows)
  - Find an exploit and you have millions of sitting targets.
- User mobility
  - Traditional perimeter security of limited use
  - The death of firewalls? [see *Life without* firewalls, A. Singer, USENIX *;login:* Dec '03]
- Rapid dissemination of exploits among hacker community
- New technology weaknesses (e.g. WEP)

Incidents Reported to CERT/CC



Attack Sophistication vs. Intruder Technical Knowledge

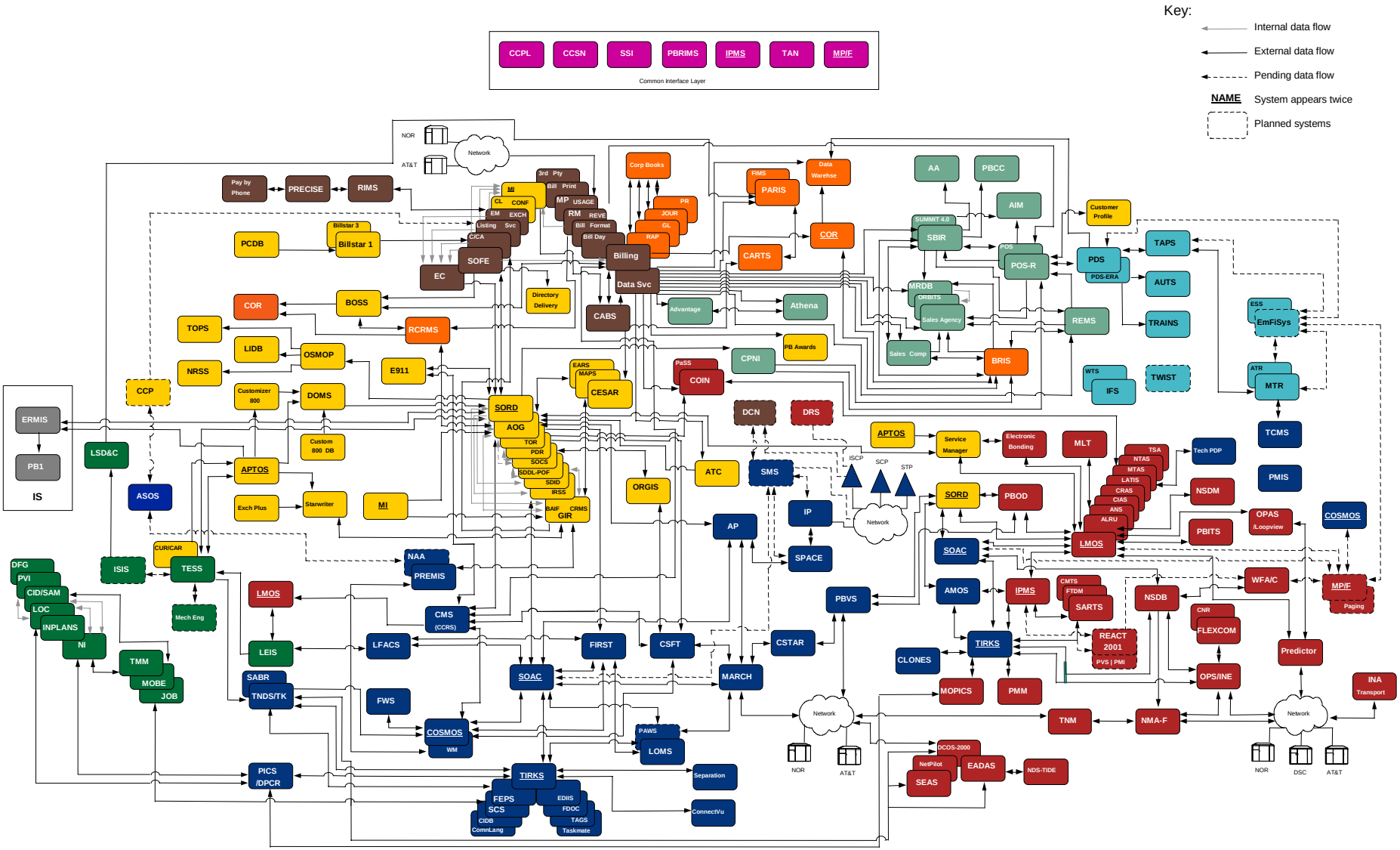


Source: CERT Coordination Center, Pittsburgh

"Head-spinning" Complexity

- Systems are getting more complex
  - How many lines of code in Windows these days? How long did it take to patch ASN.1 bug?
  - Technologies increasingly diverse, powerful, flexible, mobile
  - Mobile code
- User behaviour is getting more complex
  - People want pervasive presence
  - Business need for constant change and flexibility
  - Harder to profile "typical" behaviour

Real Example: Telecoms industry OSS



Types of Intruder

- **External penetrator**
  - Access to system by user who is not legitimate
- **Masquerader**
  - Exploitation of legitimate user's account to gain access. As far as system is concerned, masquerader is legitimate user.
- **Misfeasor**
  - Misuse of *authorised* access
- **Clandestine User**
  - Operation below the level at which audit trail data is collected
  - For example, gaining root access and suppressing logging to cover tracks

Host-based intrusion detection

- Collect & analyse data on usage of computer that hosts a service
- Normally based on logs from:
  - OS – e.g. UNIX syslog, Windows Event Logs
  - Applications (web servers, mail servers, etc)
- Advantages:
  - Good for insider attacks
  - Can detect unauthorised file modifications
- Problem of scalability:
  - As # hosts grows, difficult to deploy and manage IDS on each

Network-based intrusion detection

- Scrutinises packets that travel over the network
  - e.g. by setting IDS device NIC to promiscuous mode
- Advantages:
  - Can detect attack on host **before** host is compromised
- Disadvantages:
  - Limited where host encrypts packets (IPsec or higher layer)
  - Hard to do much per-packet processing if dealing with gigabit interfaces

Misuse Detection vs. Anomaly Detection

- Misuse Detection
  - Pattern matching approach
  - Collected data compared with *signatures* of known attacks
  - Positive match => intrusion
- Anomaly Detection
  - Statistical tests used to determine abnormal activity
  - Model “normal” behaviour and observe deviations from this
  - Assumes attack behaviour differs from legitimate activity
  - Data collected on behaviour of legitimate users over time

Misuse vs. Anomaly Detection

Misuse Detection	Anomaly Detection
Fewer false alarms	Large number of false alarms
IDS vendors maintain and issue signatures of known attacks	More adaptive – can detect previously unknown attacks
Fast processing (non-fuzzy matching)	Can require more processing power
No training required	Difficult to train in highly dynamic environments
Rule maintenance difficult (due to sheer number required)	Fewer rules

Some Misuse Detection Techniques

- Expression matching
  - Using regular expressions to match behaviour with profile signatures
- State transition modelling
  - Apply every event collected to instance of finite state machine.
  - State transitions occur on certain events.
  - Certain states defined as indicating intrusion.

Some Anomaly Detection Techniques

- Statistical models
  - Thresholds
  - Mean and standard deviation
  - Markov process model defining state transition probabilities. Alert raised if unlikely state transition occurs.
- System call traces
  - Model sequences of system calls for normal application usage & compare monitored sys call traces
- Protocol verification
  - Check for unusual or illegal use of protocol
- File checking using digest/checksum

IDS Effectiveness

- Objective: High detection rate while minimising false alarms
  - low detection rate => ineffective
  - too many false alarms => tendency to ignore
- Difficult to achieve this due to *base rate fallacy*

Example:

- 99.9% test accuracy [99.9% detection rate, 99.9% of normal usage yields negative]
- 1 in 100,000 of all events relate to intrusions

Then

Prob.(FalseAlarm) = *Prob.(NotIntrusion | PositiveResult)*

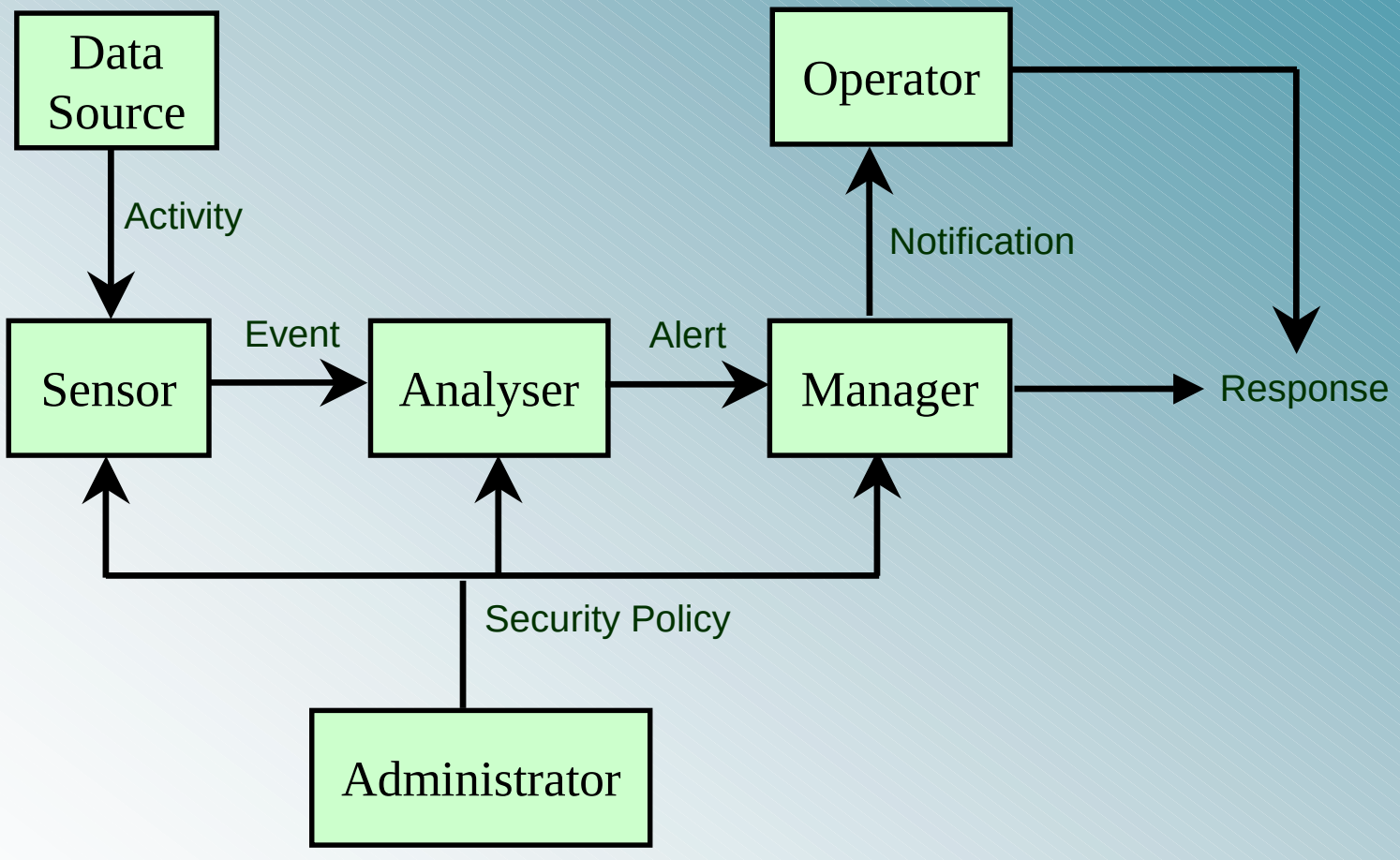
> 99% by Bayes' Theorem

Interoperability

- Some embryonic work on defining standards
- **Common Intrusion Detection Framework**
  - U.S. DARPA project, late 1990s, now dormant
- **IETF Intrusion Detection Working Group (idwg)**
  - Objective:
    - *"to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to management systems which may need to interact with them"*
  - 3 Internet-Drafts:
    - Intrusion Detection Message Exchange Requirements (expired)
    - Intrusion Detection Message Exchange Format
    - The Intrusion Detection Exchange Protocol (expired)

Interoperability

- **IDWG draft architecture:**



Performance

- Distributed Intrusion Detection
  - Carry out processing close to sensors
  - Need to correlate between events observed at the various components
- Multiple IDS instances, with slicing of event stream into several smaller streams
- Whitelisting
  - Rather than characterise attacks, define profile of *good* traffic. Pre-filter good traffic and send remainder to IDS

IDS Products

- Leading products are misuse-based
  - False positive rates too high with anomaly detection
  - Can get some benefits of anomaly detection by clever writing of rules
- A selection of leading products
  - Snort (open source)
  - RealSecure & BlackICE (Internet Security Systems)
  - Cisco IDS (Cisco)
  - eTrust (Computer Associates)
  - Entercept (McAfee)

Honeypots

Honeypots

- Definition:
  - *"A resource whose value lies in being probed, attacked or compromised"*
- System or component with no real-world value, set up to lure attackers
- By definition, all activity on a honeypot is highly suspect

Value of Honeypots

- **Advantages**
  - Collect small data sets of high value
  - Reduce false positives
  - Catch new attacks, false negatives
  - Work in encrypted or IPv6 environments
  - Simple concept requiring minimal resources
- **Disadvantages**
  - Limited field of view
  - Fingerprinting allows attackers to spot honeypots
  - May introduce risk

Deployment

- **Production Honeypot**
  - Designed to protect an organisation
  - Aid incident prevention, detection, response
- **Research Honeypot**
  - Designed to better understand attacker, develop statistical models, etc
  - Capture automated threats
  - Early warning about new attacks

Level of interaction

- **Low-interaction**
  - e.g. telnet prompt but no real OS behind it
  - Easy to manage; low risk
  - Gathers limited data (IP addrs, port no, time & date)
- **Medium-interaction**
  - e.g. give attacker virtual OS or imitated service
  - More work to set up; more valuable data; more risk
- **High-interaction**
  - e.g. allow attacker access real OS with real services
  - Can learn a lot: new tools, detailed attack patterns, etc
  - Harder to manage; most risk

Honeypot examples

- honeyd
  - monitors network of IP addresses; open source; low-interaction
- BackOfficer Friendly
  - free Windows honeypot; like burglar alarm, monitoring ports
- ManTrap
  - high-interaction commercial honeypot
  - virtual OS on which you can install production apps
- “home-grown”
  - Any system can be deployed as a honeypot if it has no real users or services - just set it up and see what happens!
  - Warning: Compromised systems can be used to launch attacks so be careful (e.g. block *outgoing* traffic)

Honeynets

- Very high-interaction honeypot
- Mimics a real-world organisation
- Often a network of typical systems, placed behind a firewall
- Honeynet Project: large-scale collaboration with objective to learn more about attacker activities

Wrapping up…

Some new IDS ideas & developments

- Artificial creation of diversity in systems to limit power of automated attack tools (lessons from biology)
- Information theory approach
  - Attack events tend to be more complex than normal events
  - Can analyse min #bits to which fixed-size event string can be compressed (Kolmogorov Complexity)
- Models based on biological immune systems

SEINIT approach (early stages)

- Use of honeypot to update IDS & policy
  - Idea of “virtual ring” encompassing protected resources.
  - Honeypot placed in ring to enhance intrusion detection capabilities
  - e.g. activity on honeypot indicates something abnormal happening within ring => update policy / IDS rules
  - Objective is an IDS that is **adaptive** and has **low false positive rate**
- Distributed and p2p IDS
- Wireless IDS sensors & honeypots
- IPv6 honeypot

Summary of Main Challenges

Ideal is a system that:

- Does not rely on predetermined definitions such as signatures
- Can keep running in the event of an attack
- Can learn to adapt to changing attack scenarios
- Generates few false alerts

For more information

Vulnerabilities & Incidents

- http://www.cert.org/

IDS

- Northcutt & Novak, Network Intrusion Detection, Que, '02
- Spafford et al, Practical UNIX & Internet Security, O'Reilly, '03
- Cox, Managing Security with Snort & IDS Tools, O'Reilly, '04
- http://www.ietf.org/html.charters/idwg-charter.html - IETF idwg
- http://www.sans.org/resources/idfaq - SANS FAQ:
- http://www.securityfocus.com/ids - articles, mailing lists, etc

Honeypots & Honeynets

- Spitzner, *Honeypots: Tracking Hackers,* Addison-Wesley, '03
- Honeynet Project, *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community*, Addison-Wesley, '01
- http://www.tracking-hackers.com/misc/faq.html - Honeypot FAQ
- http://www.honeynet.org/ - The Honeynet Project

Thanks!

- **Contact:** jmcgibney@tssg.org
- **Questions:**