hp®

invent

LSE

K2
DEFENDER

Intrusion Detection Systems

Simon Bennett

K2 Defender

- Why IDS?
- Generations of IDS
- Is Near Enough Good Enough?
- Monitoring & Auditing – beyond traditional IDS

Why Intrusion Detection?

What is an IDS?

- A “Burglar Alarm” with CCTV
  - Door and window sensors
  - Motion Sensors
  - Temperature sensors
- Alerts on breaches in your electronic security policy

What types of things does an IDS do?

- Detects Attacks
- Detects Intrusion
- Remains Passive
- Retains traffic in its original state

Why Intrusion Detection?

- Defence in Depth – don’t expose yourself to a single point of failure
- Firewalls and Anti-virus don’t give 100% cover
- Collecting evidence for prosecution
  - Chain of custody
- Detecting “bad behaviour using good protocols”
- Internal Policy Breaches
  - Fraud
  - Breach of Chinese Walls

Generations of Intrusion Detection

The Formative Years

IDS Generations:

1) Host Based

2) Network Based

3) Hybrid Aggregated Sensor Systems

Generation 1: Host Based Intrusion Detection

- Securing the host in a pre-networked world

  - standard OS features
- Orange Book Standard
- 3rd party tools – Swatch & Tripwire
- Still Relevant today
  - A philosophical alternative
  - As part of an overall system
  - Independent computers

Generation 2: Network Intrusion Detection

- Sense on the network rather than on individual hosts
- A Packet Sniffer that can perform analysis
- Origins: NID/NSM, Shadow

Generation 2: Network Intrusion Detection

- Today: Snort, NFR, RealSecure, Dragon, Cisco
- Technology
  - Majority are Signature Based
  - Some Protocol Based
  - Merging technologies
  - Statistical Based
  - Limited by original architecture

Are Generation 2 systems “Good Enough”?

No

NIDS have not kept up with increasingly sophisticated hacker techniques or the advancing complexity of networks and organisational needs

Are Generation 2 systems "Good Enough"?

NIDS have not completely kept up with the advancing complexity of networks and number of attacks

1) Switched Networks
2) Increasing numbers of attacks
3) False Positives
   - Pager alerts
4) False Negatives
5) Part of the problem
6) Slow scans & other stealth techniques
7) What does it all mean anyway?

Near Enough?

- Human factor ignored
- Too much data, too little information
- Point solutions: no system-wide overview
- No historical correlation
- Difficult to manage & maintain
- Poor balance between flexibility and ease of use

Generations of Intrusion Detection

3rd Generation IDS

The Solution:

Hybrid Aggregated Sensor Systems

1) Full “posture” coverage
2) Centralised Management & Control
3) Hybrid Detection Engine
4) Environmentally Aware
5) Statistical Detection Features
6) K2, Man Hunt & Silent Runner
7) Database Centric

Hitting the Mark. 3rd Generation IDS:

- Reduce False Positives
- Keep up with the pace
  - True Gigabit monitoring
  - Dealing with the Human Factor
- Eliminate False Negatives
- Detect Slow scans
- Explain what it means
- Are not part of the problem

Monitoring & Auditing

Beyond Traditional Intrusion Detection

Beyond Traditional Intrusion Detection:

1) Differential Firewall Analysis

2) Monitoring Policy

3) Zero Day Analysis

Differential Firewall Analysis

- What was that again?
- “Watching the watchers”
- Double checking the rules
  - both directions
- “Clean room” audit of firewall rules

Differential Firewall Analysis: Why?

- Reduce risk, and protect against failure
- Firewalls are increasingly the target of attacks themselves
- Multiple vendor firewall roll-outs
  - are all your ACL’s *really* the same?
- Self checking vulnerability patching
- The Increased Complexity of firewalls has resulted in an increased risk of a *failure of the rules engine itself.*

Monitoring Policy

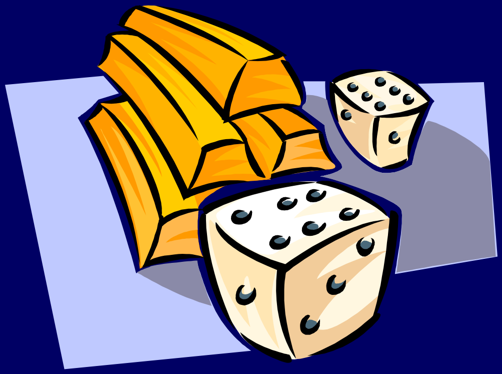
Security Monitoring on the Internal Network

- IDS tends to be externally focussed
- Employees can use *your* resources to launch attacks!
- Although rarely discussed, internal fraud and IT misuse is often an organisation's biggest IT security problem
- IDS can help!

So what?

It is not a problem – until it happens to you….

- CBI survey:
  - 2/3 of British companies hit in last 12 months
  - Organised crime: 13% of incidents
  - Internal fraud: 11% of incidents
- Internal Fraud typically understated
- Market does not treat admission of weakness kindly



Security Monitoring

Security policy

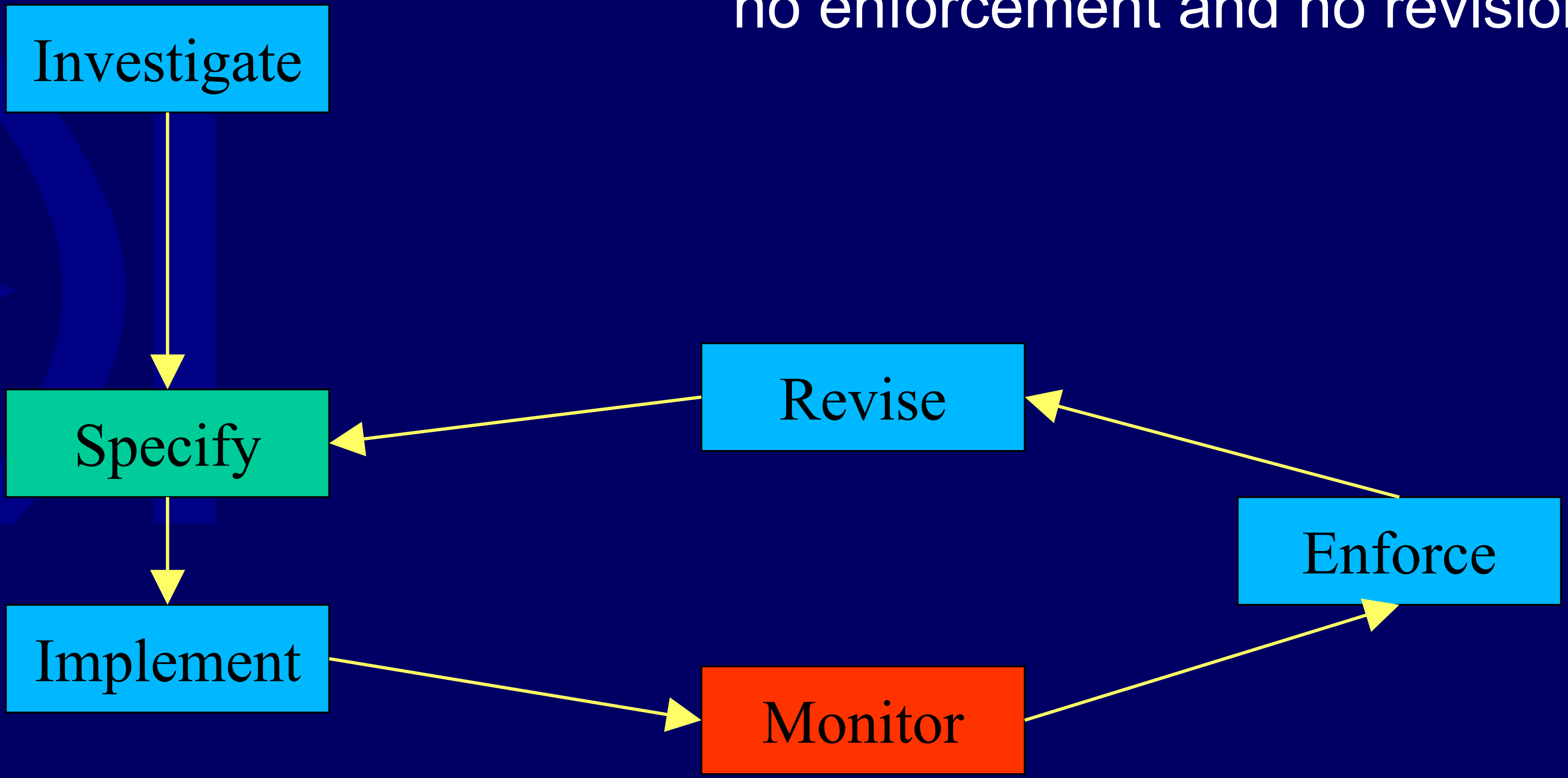
- Investigation
  - Understand your security requirements
- Specification
  - Describe your security needs
- Implementation
  - Implement the policy

Security policy (cont.)

- Monitoring
  - Check that organisation abides by the security policy
- Enforcement
  - Enforce the security policy
- Revision
  - Update your security policy as it changes

Monitoring is essential

No monitoring →
no enforcement and no revision



Zero Day Analysis

1) Analysis – beyond detection
2) When you have to know
3) Leveraging on white listing
4) The power of database
5) Ready, Aim…

In Conclusion

- Intrusion Detection Vendors have good intentions
- Most current implementations however, fall short of the mark
- Even so, most IDS systems are *under* utilised
- A paradigm shift is required if true security is to be realised

Turning network data into security knowledge

K2

DEFENDER

hp
®
invent

LSE