Network Security: The Principles of Threats, Attacks and Intrusions (Part 2)

APRICOT 2004
Tutorial, 24 February 2004
Kuala Lumpur

Ray Hunt, Associate Professor (Networks and Security), University of Canterbury, New Zealand

What is an Intrusion?

Sequence of related actions by a malicious adversary that results in occurrence of security threats to target computer or network

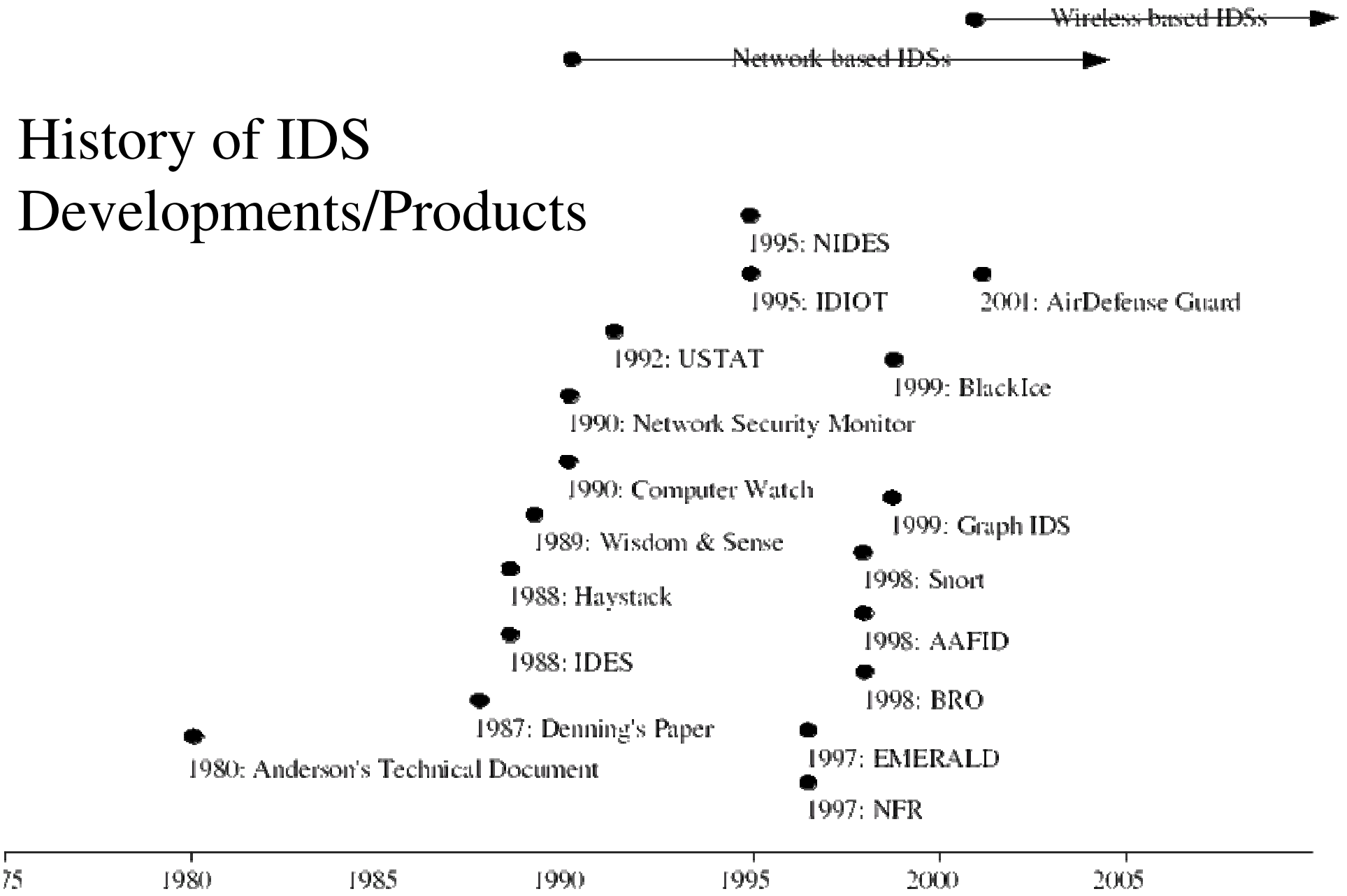
Indicators:

- Repetition of unusual behaviour
- Exploitation of known vulnerabilities
- Inconsistent packet sequences or routes
- Unexplained problems
- Suspicious traffic content

Major Reasons for Using Intrusion Detection Systems are..

- To detect intruders, attacks, abuse...
- To detect probes
- To provide active network security
- To provide a means of deterrent
- To collect data on system behavior so as to recover after intrusion
- To indirectly provide useful information

History of IDS Developments/Products

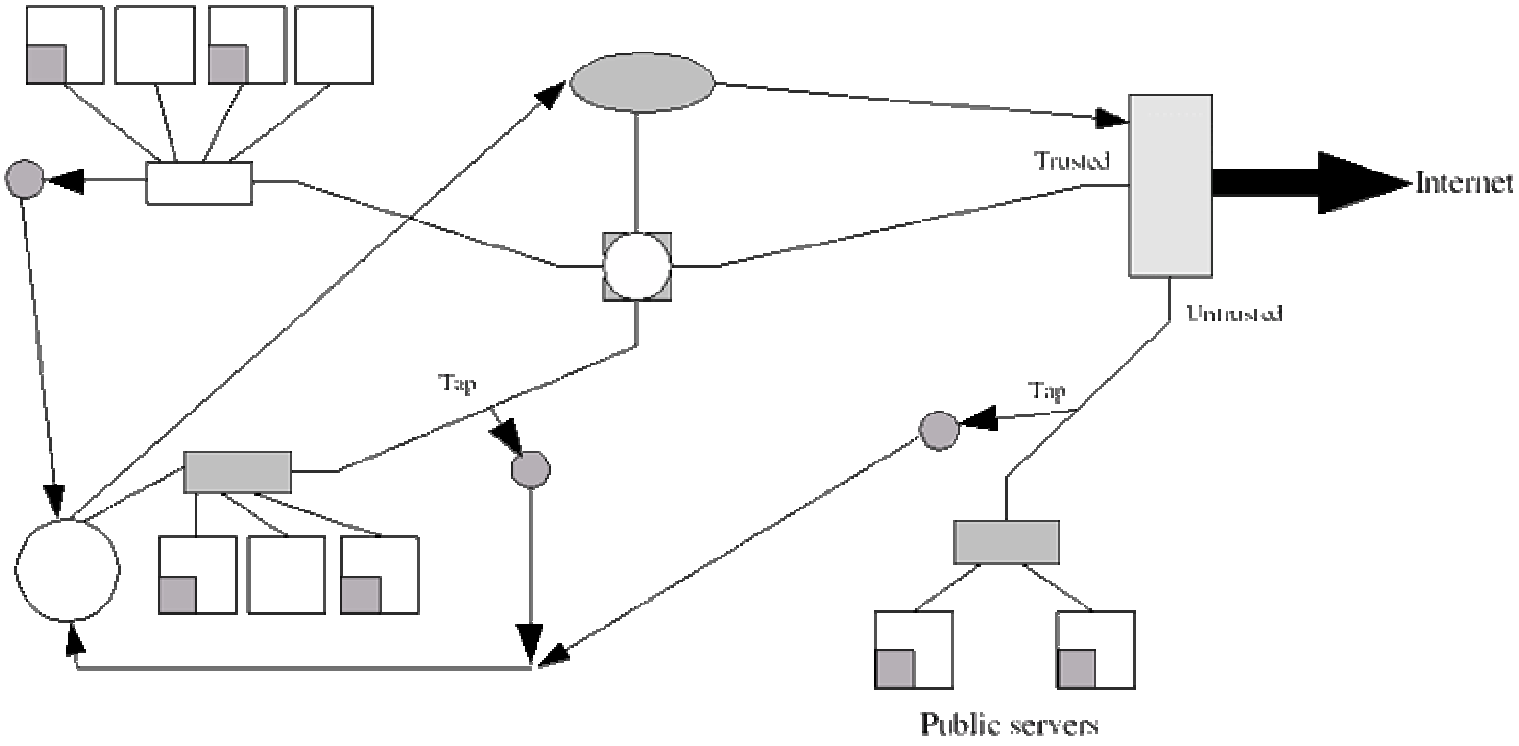


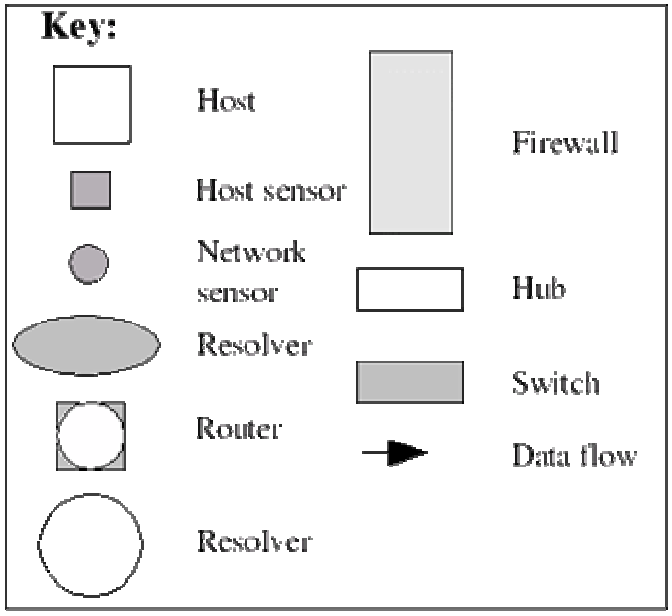
IDS Goals

- Differentiate normal from damaging actions
- Scalable
- Variety of network systems and architectures
- Adapts in response to new attacks
- Reports attacks in real-time
- Co-operates with other security mechanisms

IDS Goals

- Increase monitoring at suspicious points
- Protect against being attacked itself
- Function in face of network failure
- Minimal performance impact
- Generate audit information
- Reflect security policy of organisation





IDS Architecture

IDS Architecture Components

- Sensors - data gathering for the IDS
- Monitors - process the collected data
- Resolver - determines appropriate responses
- Controller - configuration of components in a distributed system

Modern IDS apply these components in a cascading fashion, ie - allowing higher level system overviews to be gained as a user ascends through the tree

IDS Techniques

- Misuse Detection (M-IDS) - attempts to match observed v expected behaviour (eg signature analysis, Petri nets, state transition diagrams, genetic algorithms)
- Anomaly Detection (A-IDS) - models expected behaviour (eg statistical, expert systems, neural networks)

IDS Techniques

- Location of Sensors - network-based (no processing overheads and difficult to attack) *or* host-based (performance impact but good data collection)
- Monitor Processing Patterns - real-time (cf. batch) detection of significant benefit (performance issues)
- Distributed Correlation - simple interfaces (eg Shadow) or hierarchical (eg GrIDS)

Capabilities of IDS

- Second level of defense if primary security fails
- Clear view and summary (eg Tripwire)
- Extracts information useful in tracking intrusions
- Identifies nature of abuse - (eg systems modifications for later backdoor use)
- IDS logs as evidence in legal cases

Capabilities of IDS

- IDS can assist in detecting mis-configurations
- Combined with network security scanners, security holes can be revealed - eg finding particular firewall is vulnerable to certain attacks
- IDS can determine which resources are targeted
- New attacks every month - simplifies detection
- IDS works well with security policy

Limitations of IDS

- Reporting tool - cannot stop ongoing intrusions
- Cannot trace intrusion with poor authentication
- Can only trace intrusion to point of entry to system
- Must be aware of security policy
- Attackers may attack IDS systems
- Depends upon seeing *all* traffic
- Models event - systems react in different ways
- Widely spread attacks may be ignored
- New attacks continually being discovered
- Scaling problems

Current Development in IDS

- Distributed and scalable IDS
- Use of AI and pattern matching
- Embedded IDS in network devices
- Use in other areas - telephone / credit card systems
- Adaptation to new technologies
- Automatic recognition of new attacks (adaptive AI)
- IDS which responds to attacks in progress
- IDS standards/groups (eg CIDF, IDWG, IDSC ….)

Intrusion Detection Systems and Products

- Manual Review Techniques
- Full-scale IDS may not always be appropriate:
  - connect dummy service to ports (eg IMAP (143), SMB (139), HTTP (80) - trigger script when attacked
  - use log files and audit info to build critical log
  - use simple monitors such as NetMon and FileMon

Types of IDS

- Host-based (HIDS)
  - searches for mis-configurations and dangerous settings, unusual privileges etc
- Network-based (NIDS)
  - checks host security policies, dangerous or unnecessary services
- Hybrid

Vary according to whether:

fixed/wireless

commercial/freeware

operating system

Host-Based IDS

- GFi LANgaurd SELM Windows *Commercial*
  http://www.gfi.com/lanselm/index.html
- EMERALD eXpert-BSM Solaris *Commercial*
  http://www.sdl.sri.com/projects/emerald/releases/eXpert-BSM/
- ISS BlackICE Windows *Commercial*
  http://blackice.iss.net
- Symantec Host IDS Windows/Solaris *Commercial*
  http://enterprisesecurity.symantec.com/products
- LIDS Linux *GPL* http://www.lids.org

Network-Based IDS

- AirDefense Guard *(Wireless IDS)* Hardware *Commercial*
  www.airdefense.net/products/airdefense_ids.shtm
- NetDetector Solution Hardware *Commercial*
  www.niksun.com/index.php?id=194
- Network Flight Recorder Security Hardware *Commercial*
- RealSecure Network Sensor
  Windows/Linux/Solaris/Nokia *Commercial*
- Symantec ManHunt Solaris/Linux *Commercial*
- Shoki *nix *GPL* http://shoki.sourceforge.net
- Snort *nix *GPL* http://www.snort.org
- Sourcefire Intrusion MS Hardware *Commercial*

Hybrid IDS

- Prelude *nix *GPL* http://www.prelude-ids.org
- RealSecure Network Sensor Windows/*nix *Commercial* www.iss.net/products_services

Example NIDS: SNORT

- Lightweight IDS system capable of performing real-time traffic analysis and packet logging
- Can perform protocol analysis, content searching/matching.
- Can be used to detect a variety of attacks and probes, eg:
  - buffer overflows
  - stealth port scans
  - CGI attacks
  - SMB probes
  - OS fingerprinting attempts

Example IDS: SNORT

- Snort has three primary uses. It can be used as:
  - a packet sniffer like tcpdump
  - a packet logger (useful for network traffic debugging, etc)
  - a full network intrusion detection system
- Snort/IDS operates from a script rule file applied to each packet monitored
- Provides specialised access to IP packets, eg fragmentation bit checks
- Example rule:

```
alert tcp any any -> 192.168.0.1/24 111 {content: "|00 01 86 A5|";
                                         msg: "mountd access";  }
```

Example IDS: BlackIce

Host-based IDS for Windows and carries out extensive port analysis

- Four levels: Paranoid, Nervous, Cautious, Trusting
- Provides back-trace of intruders via NetBios
- Uses signature files to detect known attacks
- Real time network usage graph
- Links to full protocol stack
- http://blackice.iss.net

Example IDS: ZoneAlarm

ZoneAlarm (= Firewall + IDS)

- www.zonelabs.com
- Personal firewall with security settings of High, Medium, Low for both LAN and Internet connections, and a mail attachment check setting
- Alerts occur when access to an unauthorised port is attempted. ZoneAlarm advises what likely cause is and how indicative of an attack it is
- Access is allowed/denied for programs on the host PC to connect to the Internet
- ZoneAlarm Pro $US50 for single user and $US1800 for 50 users
- ZoneAlarm - free for home users

Tools Supporting Active Security

- Mapping Tools
- System Scanning Tools
- System Integrity Checkers
- Honeytraps

IDS Support Tools - Mapping Tools

Network Mappers

- Commercial and free tools available - nmap and Cheops-NG
- Carry out - DNS zone transfers, address/port scanning, host requests, promiscuous monitoring
- nmap sends variety of packets with illegal flags, ICMP echos, fragmented packets etc to hosts and analysing responses
- eg recognise Linux with kernels older than 2.0.35 by using packet with SYN and illegal flags set

IDS Support Tools - Mapping Tools

- Cheops *nix *GPL (no longer supported)* www.marko.net/cheops/
- Cheops-NG *nix *GPL* http://cheops-ng.sourceforge.net/
- nmap *nix/Windows *GPL* http://www.insecure.org/nmap

IDS Support Tools - System Scanning Tools

- Tools used to detect and report on vulnerabilities in computer or network
- Uses database of known vulnerabilities and attempts matching to these records
- For an attacker these tools allow location of potential specific targets, eg
  - open HTTP port with a known vulnerability

IDS Support Tools - System Scanning Tools

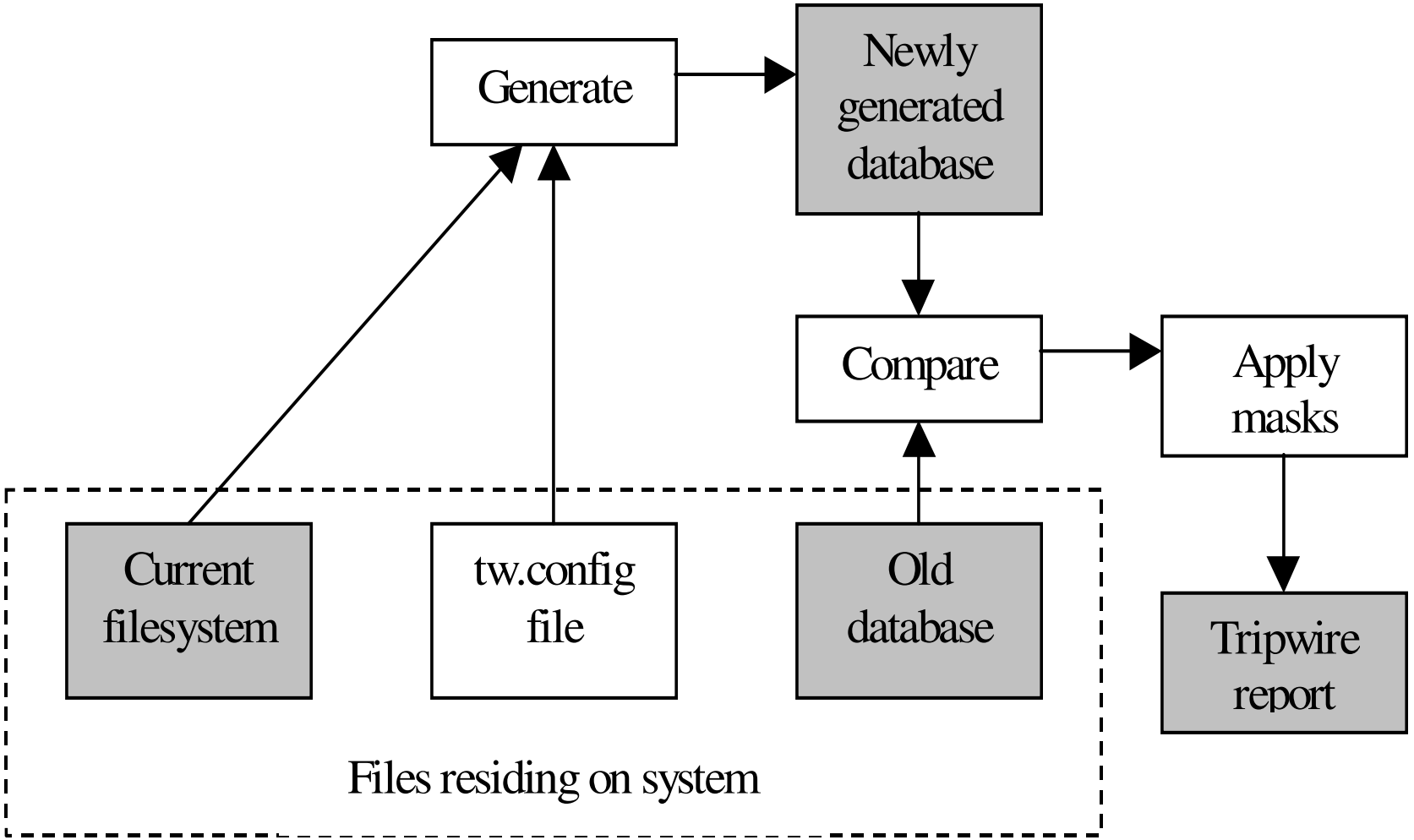
- Core Impact Windows *Commercial*
- GFi LANguard NSS Windows *Commercial/Freeware*
- ISS Internet Scanner *Commercial*
- Nessus *nix *GPL* www.nessus.org
- Rapid7 NeXpose Linux/Windows *Commercial*
- Retina Windows *Commercial*

IDS Support Tools - System Integrity Checkers

- Detect anomalies which may indicate that data on computer has been tampered with
- Cannot detect intruders until after intrusion and so are not real-time like IDSs
- Stores hashed snapshot of file systems and compares to current system state and reports discrepancies

IDS Support Tools - System Integrity Checkers

- Tripwire is best example
- Commonly support hashing algorithms, eg - MD4/5, SHA, ITU CRC-16 and -32 signatures
- Reference database based upon initial trusted system
- Only reports changes already present in system
- Last line of defence - system is already compromised!



Structure of the Tripwire system

IDS Support Tools - System Integrity Checkers

- Aide *nix *GPL*
- Chkrootkit *nix *Open Source*
- Integrit *nix *GPL*
- Ionx Data Sentinel Windows *Commercial*
- GFi LANguard SIM Windows *Commercial/Freeware*
- Osiris *nix *Open Source*
- Samhain *nix *GPL*
- Tripwire *nix/Windows *Commercial* and *Open Source*

IDS Support Tools - Honeytraps

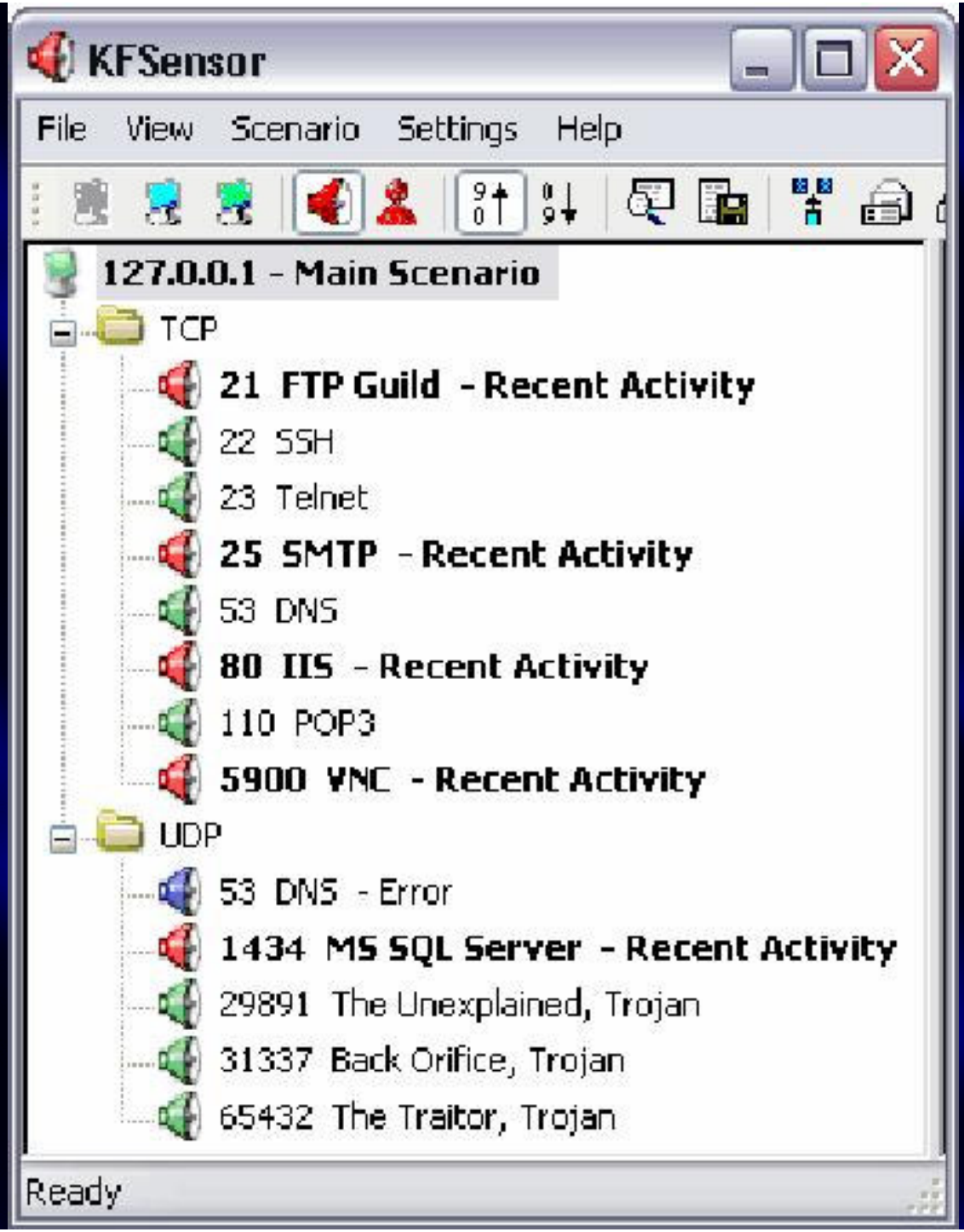
Current IDS methodologies have shortcomings:

- problem recognising novel attacks
- occurrence of false positives
- reporting of attacks of no interest

- Honeytrap system – simulated or real system that exists for sole purpose of being attacked!
- Looks and behaves like real system
- Must not be launching pad
- Must gather valuable information on attacker

IDS Support Tools - Honeytraps

- Bait and Switch *nix *BSD*
- KeyFocus Sensor Windows *Commercial*
- NetBait Enterprise i386-based *Commercial*
- Symantec Decoy Server Solaris *Commercial*
- Verizon NetFacade *nix *Commercial*



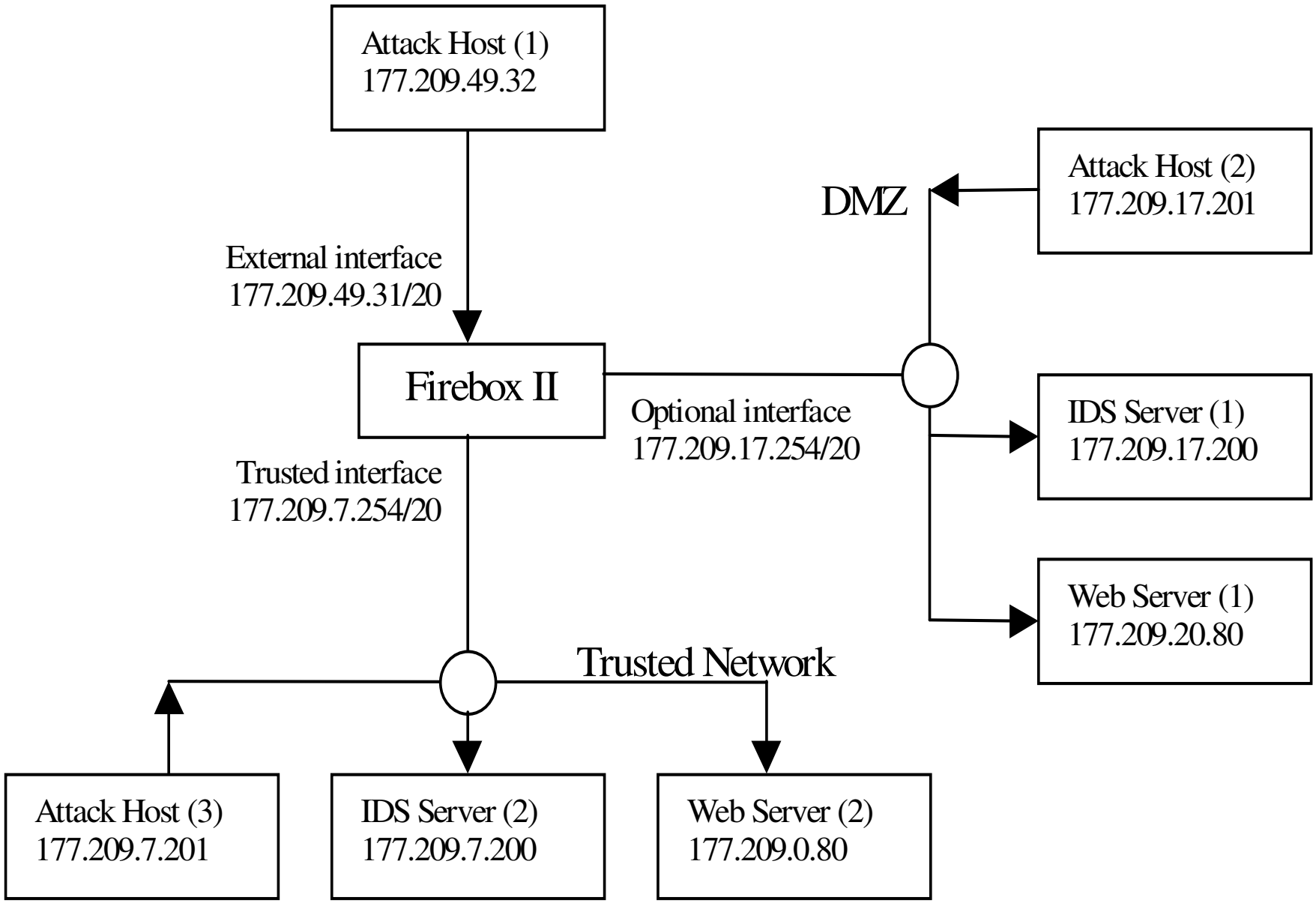
KFSensor Honeypot Output

IDS Standards

- Common Intrusion Detection Framework (CIDF)
  - Common protocols and interface standards (1999)
- Intrusion Detection Working Group (IDWG)
  - Produced 4 Internet Drafts (2002)
- Open Security Evaluation Criteria (OSEC)
  - Evaluation of and tests on products (2003)
- Intrusion Detection Systems Consortium (IDSC)
  - Vendor consortium promoting product adoption by defining common terminology, integrity, standards

Intrusion Detection Experiments

- Watchguard firewall used as testbed for Intrusion Detection Analysis
  - simulates small office network
  - single public server
  - limited set of machines on firewall's trusted network
  - unspecified number of machines on external network



Firewall testbed

Intrusion Detection Case Study

Sample Firewall policy might be ….

- Incoming FTP traffic allowed (via proxy) only if destined for 204.137.98.164 - public server located in optional network
- Outgoing FTP traffic allowed without restriction
- Incoming HTTP traffic allowed (via proxy) only if destined for 204.137.98.165
- Outgoing HTTP traffic allowed without restriction Incoming SMTP traffic was allowed only to 177.209.49.31 (external firewall interface)
- Outgoing SMTP traffic was allowed only from 177.209.0.25 (hypothetical SMTP server on trusted network)
- Configuration access to firewall allowed from internal networks
- IP Masquerading was disabled
- Port Autoblocking was disabled
- All other ports and services were blocked

Intrusion Detection Case Study

1. Scan Web server (2) and IDS server (2) from Attack host (3) (all machines on a common network segment)
2. Scan Web server (1) and IDS server (1) from Attack host (3) (attack on *optional from trusted network*)
3. Scan Web server (2) and IDS server (2) from Attack host (2) (attack on *trusted from optional network*)
4. Scan Web server (1) and IDS server (1) from Attack host (1) (*external* attack on *optional network*)
5. Scan Web server (2) and IDS-server (2) from Attack host (1) (*external* attack on *trusted network*)

Intrusion Detection Case Study

- Scan 1 gives baseline of what attacks IDS tools are capable of recognising, and corresponds to an internal attack on trusted network
- Scan 2 simulates internal attack against optional network
- Scan 3 simulates result if machine on optional network is compromised and then attacks internal machines
- Scan 4 -very common case - external attacker attempts to access machines on optional network
- Scan 5 is same situation for trusted network

Intrusion Detection Case Study

Conclusions

- IDS can highlight problems with Firewall configurations
- Out-of-box configurations may be dangerous
- Firewalls protect inaccessible machines well
- Firewalls do not protect against application-level attacks
- Firewalls are themselves vulnerable to attack
- IDS tools can recognise many attacks
- IDS tools have different detection sets
- Network IDS recognise attacks from their area of coverage
- Network scanning tools are susceptible to false readings
- Firewalls offer minimal detection capabilities