Quick Overview

- Overview
- Network
  - IPTables
  - Snort
- Intrusion Detection
  - Tripwire
  - AIDE
  - Samhain
- Monitoring & Configuration
  - Beltaine
  - Lemon
  - Prelude
- Conclusions

Overview

- Why do this?
  - Changes to site firewall
  - Needs of new generation of software
  - Better to make decisions at a node or cluster level
- What do we want to do?
  - Layered security system for FIO machines
    - Network / firewall
    - Node
    - Cluster
  - Develop reusable components

Network Security

- What do we want to do?
  - Restrict external access to machines
    - Based on specific IP addresses and ports
    - Limit who can attack us and how
  - (Potentially) restrict out going connections to limit systems being used for DDoS attacks and unauthorized use
    - Check we’re not spoofing others
  - Easy way to block P2P / IRC / banned apps.

IPTables

- Kernel level packet filter
  - checks packets before they get to application

```
*filter
:INPUT DROP [0:0]
:OUTPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
-A INPUT --match state --state RELATED -j ACCEPT
-A INPUT --match state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp --dport ssh --match state --state NEW -j ACCEPT
COMMIT
```

Example configuration

IPTables cont.

- Currently deployed on 2 clusters
  - CASTORGRIDSC
  - FTS
- Based on NCM component from Joao Martins
  - We have expanded logging functions and chains
  - Have a (short) to do list for extra functions
- Simple to write rules for
- Limited in intelligence
  - Doesn’t spot port scans

IPTables cont.

- Can be used to block P2P, IRC, etc
  - Both to and from machine
  - Several ways to do this
    - Assuming static port number - block port
    - Limited outside connections – restrict IP addresses
    - Limited services – block all ports by default
- However ….
  - Does not make applications and services foolproof
  - Service vulnerabilities are still there!

Snort

- Similar to IPTables but for multiple nodes
  - Packet filter
  - Central monitoring system
- Can provide overview of attacks
  - Used it to create new rules before nodes get hit
- Network overhead ➔ performance issues
  - Do we want all this info? Who will use it?

Snort

- Advantages
- Can have sensors on both sides of the firewall
- Popular with many people
- Can be used before IPTables

- Disadvantages
- Not useful if we have firewalls on every machine
- Less useful on a cluster basis
- Not able to see rejected packets on IPTables output
- Possibly overkill for us
  - Site level better for DDoS attacks

Conclusions

- We can now deploy IPTables on nodes quickly and easily
- Need documentation on rules for services
  - This is ongoing
  - Developers need to document network connections more – this is a general issue
- Is this enough? Do people want more from the host based firewall?

Intrusion Detection

- Many types – network, file, kernel …
- Our interest: File integrity checkers
  - creates a database of hash values for system files and executables which existing file system can be checked against

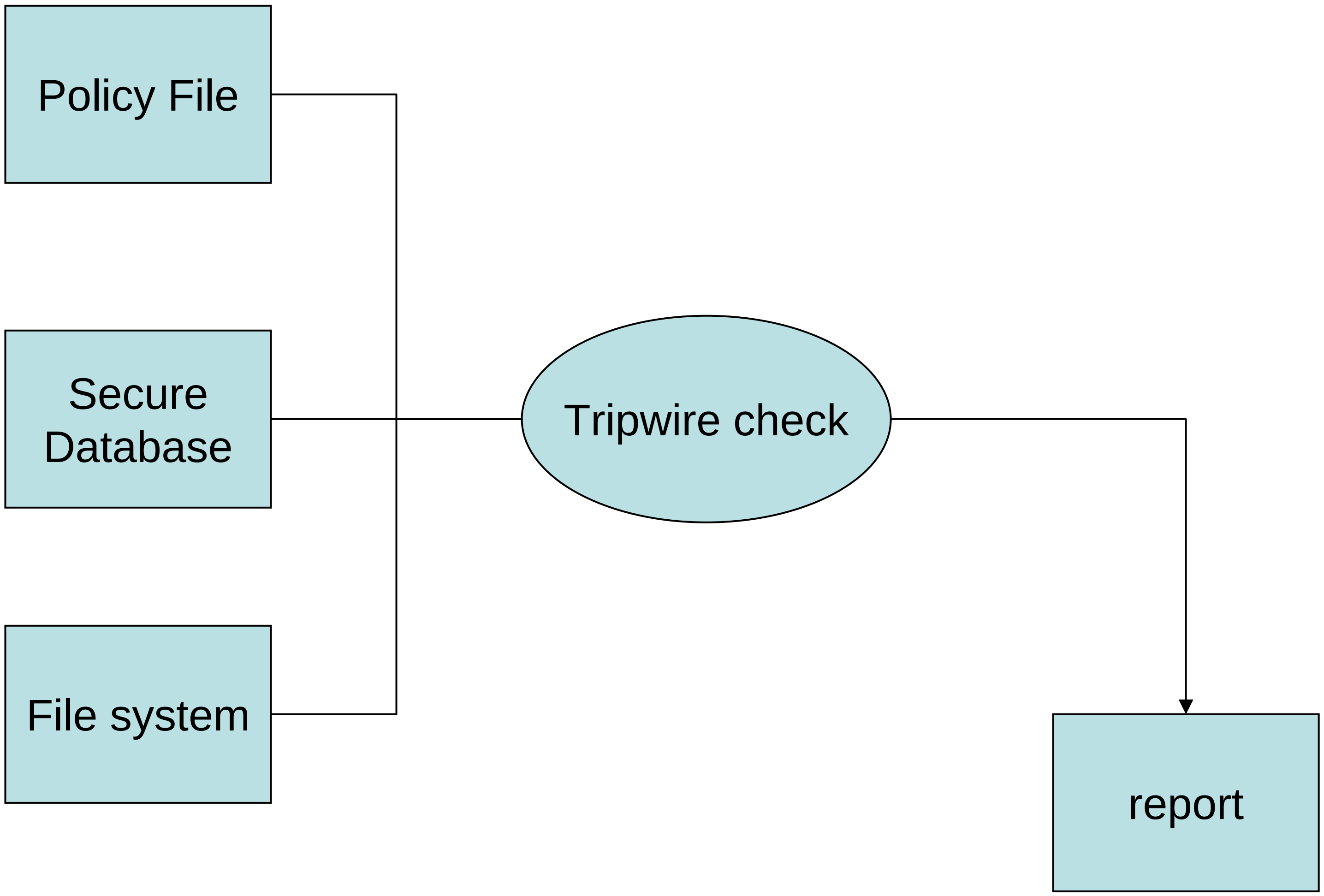
Tripwire - open source and commercial product

AIDE - open source alternative to Tripwire

Samhain - open source & designed for clusters

Tripwire

- Very mature IDS
- Widely used in academia and SoHo
  - CHEP 2004 paper by CIEMAT, Madrid
  - Update issues for us – what is we change ssh?
- Requires fine tuning to the system
  - Initially there are a large number of emails
- Has scalability issues
  - Software update issues


Policy File
Secure Database
File system
Tripwire check
report

Tripwire

- Policy File Example

```
(
  rulename = "Critical configuration files",
  severity = $(SIG_HI)
)
{
        /etc/crontab                    -> $(SEC_BIN) ;
}
# Rest of critical system binaries
(
  rulename = "OS executables and libraries",
  severity = $(SIG_HI)
)
{
     /bin                          -> $(SEC_BIN) ;
     /lib                         -> $(SEC_BIN) ;
}
```

Tripwire

- Advantages
- Fast to deploy
  - Install on system in 10 minutes by hand
  - Can be rpm deployed
    - Possible security issues
- In wide spread use
- Encrypted database
  - unlike AIDE
- Low network overhead
  - emails to root
- Can be run over ssh

- Disadvantages
- Single host solution
  - 1 database per node
  - Only profiles reused
- Limited development work – commercial version
- Security issues on install
- Password deployment
- Update deployment
- Message overhead
  - Big emails

AIDE

- Open source alternative to Tripwire

- Advantages
- More likely to be maintained than open source Tripwire

- Disadvantages
- Limited functionality
  - Not as mature as Tripwire
- Designed for single host not cluster
- Database not encrypted!
- Doesn’t scale for our needs

Samhain

- Mature IDS
- Seems to be overlooked in favour of Tripwire
- Similar functionality
  - Encrypted database
  - Profile language
- Better support for cluster and distributed environments

Samhain

- Advantages
- Open Source
- Very easy single system install – much like tripwire
- Clients can send reports to server
- Client can have central database & profile
- Allows central changes to database

- Disadvantages
- Includes numerous options
- Still have issue of initial database security
- Network overhead in client server mode
- Issues of central config changes – updates & multiple versions

Conclusions

- An IDS will be a useful component
  - Covers more files than a simple sensor can
  - More adaptable
    - e.g. notify only if log file size decreases
- Central monitoring useful in cluster environments
- Need to solve issue of upgrade changes
  - This can be a useful contribution to development

Monitoring

- What do we want?

- Information presentation
- Change management
  - Want to see what's happening
    - Has ssh been changed?
  - Filter alerts & good initial policy
    - not everything needs reporting
    - Reduce unnecessary messages
  - Deal with software upgrades
    - Don't want to run *n* db updates by hand

Suggestions & questions please!

What we looked at

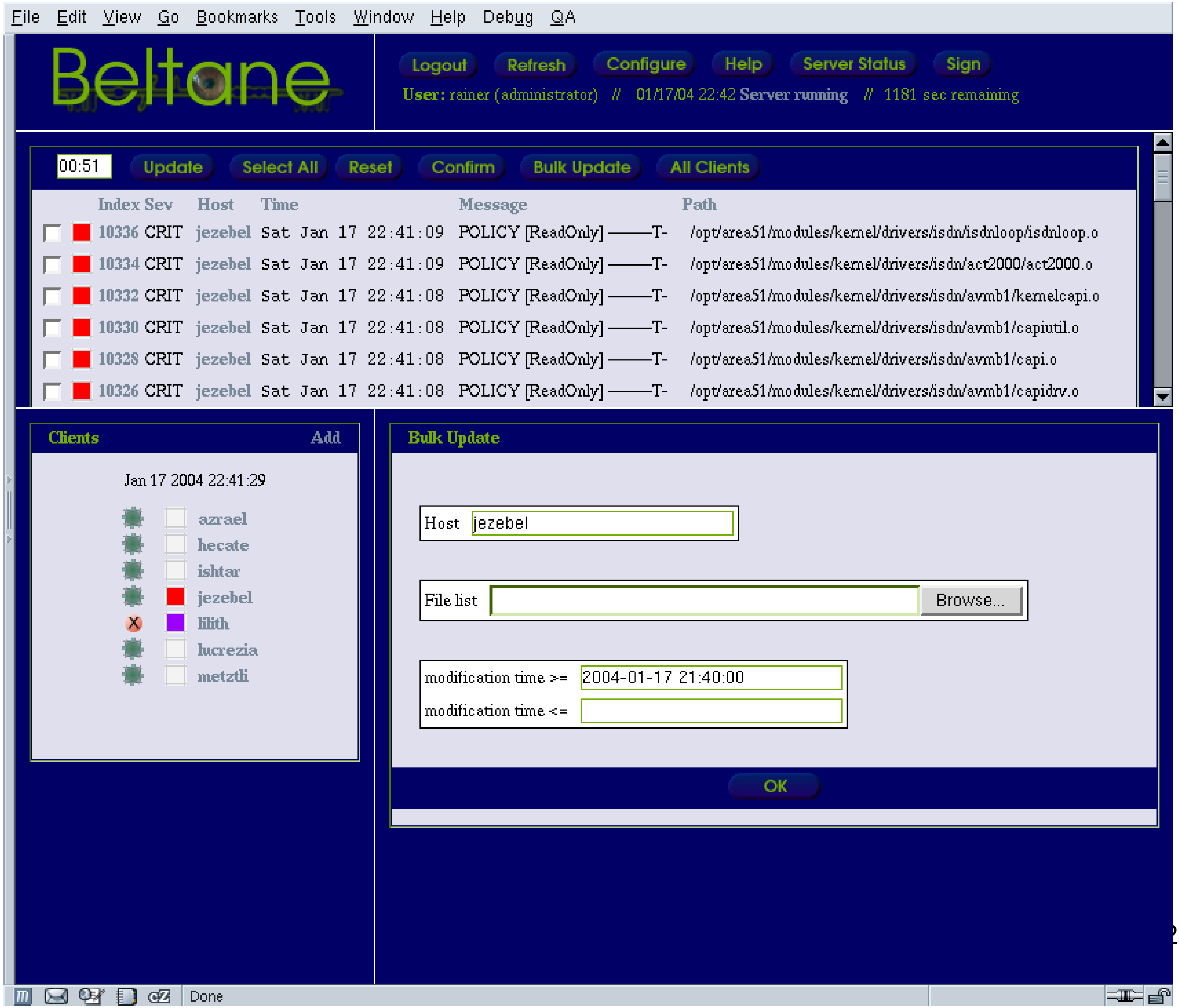
- Beltane - Samhain web interface
- Lemon - CERN monitoring system
- Prelude - security component presentation system

Beltane Monitor

- Web interface / console for Samhain
- Allows you to
  - browse client messages
  - acknowledge messages
  - modify the file signature database
- More advanced than Tripwire emails
  - Able to react immediately
  - Not (always) necessary to log into node to change database

Beltane Monitor

- Means installing software with web server
  - Developed for Apache – not sure about IIS
  - Beltane is specific to Samhain
    - Wont work for AIDE or Tripwire
  - May have scalability issues
    - Not tested with multiple clusters / >100 machines
    - Not sure if we can break down to cluster level
    - I'd like some Ganglia style features included …



User: rainer (administrator) // 01/17/04 22:42 Server running // 1181 sec remaining

00:51

		Index	Sev	Host	Time	Message	Path
□	🟥	10336	CRIT	jezebel	Sat Jan 17 22:41:09	POLICY [ReadOnly] ——T-	/opt/area51/modules/kernel/drivers/isdn/isdnloop/isdnloop.o
□	🟥	10334	CRIT	jezebel	Sat Jan 17 22:41:09	POLICY [ReadOnly] ——T-	/opt/area51/modules/kernel/drivers/isdn/act2000/act2000.o
□	🟥	10332	CRIT	jezebel	Sat Jan 17 22:41:08	POLICY [ReadOnly] ——T-	/opt/area51/modules/kernel/drivers/isdn/avmb1/kernelcapi.o
□	🟥	10330	CRIT	jezebel	Sat Jan 17 22:41:08	POLICY [ReadOnly] ——T-	/opt/area51/modules/kernel/drivers/isdn/avmb1/capiutil.o
□	🟥	10328	CRIT	jezebel	Sat Jan 17 22:41:08	POLICY [ReadOnly] ——T-	/opt/area51/modules/kernel/drivers/isdn/avmb1/capi.o
□	🟥	10326	CRIT	jezebel	Sat Jan 17 22:41:08	POLICY [ReadOnly] ——T-	/opt/area51/modules/kernel/drivers/isdn/avmb1/capidrv.o

Clients Add

Jan 17 2004 22:41:29

●	□	azrael
●	□	hecate
●	□	ishtar
●	🟥	jezebel
☒	🟪	lilith
●	□	lucrezia
●	□	metztli

Bulk Update

Host: jezebel

File list:

modification time >= 2004-01-17 21:40:00

modification time <=

Prelude

- Started as IDS – focused on the network
- Our interest is its monitoring system potential
  - Can receive reports from other IDSs
  - Standard message language - Intrusion Detection Message Exchange Format (IDMEF)
  - Uses MySQL or Postgres – no oracle support
- Web interface
- Central monitoring system for more / future security applications?
  Better choice than Beltane perhaps ….

Lemon

- Lemon – default monitor for our systems
- Looking for suggestions
  - Do we want to use lemon?
  - What do we want it to do?
    - Critical issue only or full report?
- We can see three scenarios …

Scenario 1

- Each node has a local db / log
- Lemon monitors this log and reports on a machine basis
- Advantages
  - No single point of failure
- Disadvantages
  - How do you deal with updates?

Scenario 2

- Nodes have a central log system
- Lemon gets data from central node
- Advantages
  - Only one sensor needed
  - Can use Tripwire or Samhain
- Disadvantages
  - Still have issue of updates

Scenario 3

- Nodes have client software but log, configuration and database centrally located
- Advantages
  - Only one sensor needed
  - Only one system for updates
- Disadvantages
  - Single point of failure
  - Only available with Samhain

Conclusions

- The monitoring / update system will important
- We need to make sure that we can monitor file changes in a sensible manner
- Don’t want to reinvent the wheel