



Intrusion Management and ISMS

by Dr. David Brewer

Gamma Secure Systems Limited

Diamond House, 149 Frimley Road

Camberley, Surrey, GU15 2PS +44 1276 702500

dbrewer@gammassl.co.uk ■ www.gammassl.co.uk

Agenda

■ Intrusion Management

- *What is it?*
- *Any problems?*
- *Why all the interest?*
- *Some IT advice*

■ ISMS

- *What do the standards say?*
- *A case study*

■ Observations/Conclusions

Intrusion Management

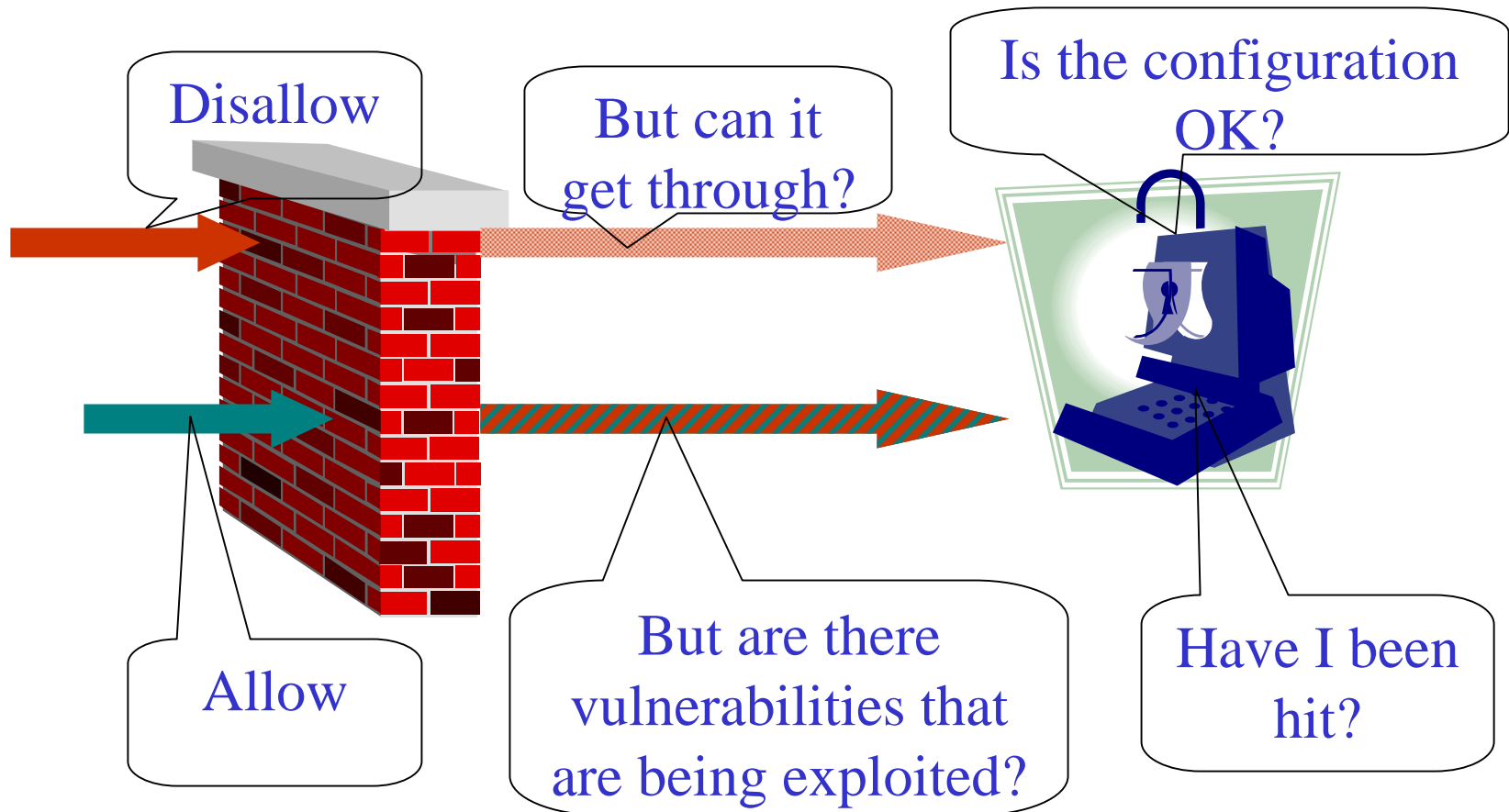
1 – What is it?

The Hypothesis

“... if I can't prevent it, can I detect that the event has occurred? ...”

See <http://www.gammasl.co.uk/topics/time/index.html>

Network Intrusion Detection



Is this Anything New?

■ NO

■ What about CCTV, PIRs etc

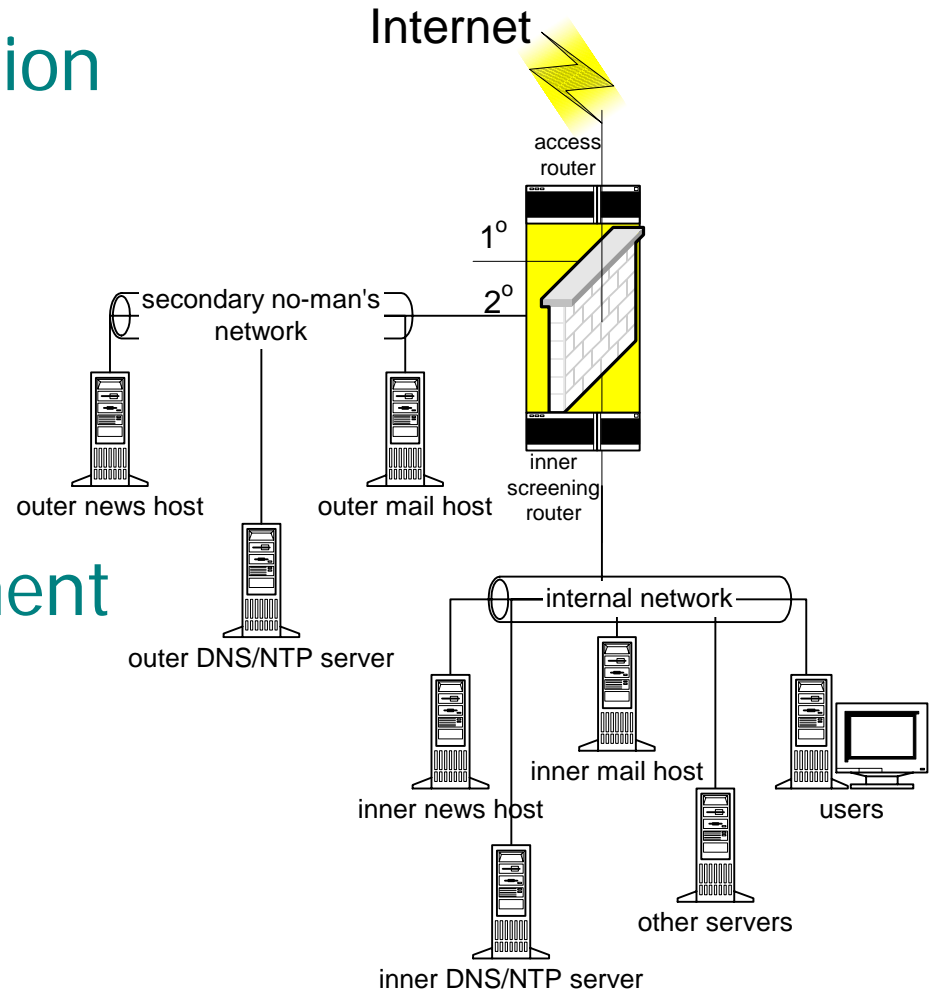
■ What's in common:

- *If a preventive control fails ...*
- *Can I detect the event/impact?*
- *Can I do that in good time?*

Types of IT Intrusion Detector

- Host Intrusion Detection Systems
- Network IDS
- Network Node IDS
- Vulnerability Assessment Scanners

- *Host scanners*
- *Network scanners*



Types of Physical IDS

- Alarm the jewels
- Watch the entrances and exits
- ... for the whole campus or just your company
- Have a security inspection



IT Alerts

- SNMP Trap
- E-mail
- Pager
- Session termination
- Firewall/router reconfiguration



Boss knows

Only a true fix silences alarm



Physical Alerts

- Bell
- Direct line to police/
security /you
- Mantraps (as in
Home Alone)



Boss knows

Only a true fix silences alarm



Just Physical and IT?

■ No

- Double entry book keeping was probably first!
- IC sensors on smart cards
- Application software, e.g. database table overflows
- Really anything

Intrusion Management

2 – Any problems?

Principal Problems

- None are fire and forget
- All rely on anomaly detection, even CCTV and PIR!
 - *Reliability of detecting anomalies*
 - *False positives*

How does IT IDS Work?

- Pattern matching packet contents v. database of known “signatures”
- Full protocol analysis on data stream
- Concentrate on everything “abnormal”

Getting the Best out of IT IDS

■ Careful planning:

- *What are you protecting, and from whom?*
- *What vulnerabilities/attacks concern you?*
- *Choice of NIDS versus NNIDS*

■ NIDS: dedicated server/performance limitations

■ False positives

RealSecure Network Sensor: RealSecure detects all occurrences of the string "GNUTELLA CONNECT" on any port. Although highly unlikely, a false positive is possible if this string occurs in network communications not associated with a Gnutella connection.

Extract from ISS Signature Reference Guide Version 6.0

An Aside (?)

■ Substantive (financial) audit techniques find anomalies:

- *Are the processing rules followed*
- *Are the results reasonable*
- *What data suggests misdeeds*

■ Examples:

- *1% interest on mortgage loan*
- *Same bank account on payroll and purchases*

Intrusion Management

3 – Why all the interest?

Why all the Interest

- Substantive financial audit techniques – well known and well understood
 - *but there are still troublesome areas such as derivatives .. Can you really detect errors?*
- Physical IDS - well known and well understood
 - *but still in the news...*
- IT IDS – not well known, less well understood
 - *Will standardisation help?*

Intrusion Management

4 – Some IT advice

The Management Cycle

- All ISMS components must adhere to a common security policy
- Scale responses to alarms
 - *Serious intrusions → immediate response*
 - *Mundane → regular examination of logs*
- Training
- Keep up-to-date

Network Security Policy

2.2 Access Router

Who is supposed to have what access to what?

O/S hardening?

What vulnerabilities do I have? What do I fix?

What do I monitor? Are they files, security parameters, packets or what?

How do I test it?

How do I keep it up-to-date?

Access Router Port	IP Datagram's Source Address	IP Datagram's Destination Address	Allowed Access
Inside	Inside	Outside	Yes
Outside	Outside	Inside	Yes
Inside	Inside	Inside	No
Outside	Outside	Outside	No
Inside	Outside	Any	No
Any	Loose Source-Routed	Any	No



The screenshot shows a web page titled "http://www.sans.org/infosecFAQ/win/harden_NT4.htm" with a "Confirm Password" dialog box. Below it is a network diagram showing various devices and connections. To the right, there is a list of security recommendations:

- L0phtCrack
- Copy of SAM created via RDISK /S
- Weak passwords
- Shared passwords

Destination	source	Internet	Phone.com	Test	WF4.com	DB	Service
Phone.com	E	✓	×	×	×	×	×
Test	E	✓	×	×	×	×	×
DB	E	×	×	×	×	×	×
Service*	E	×	×	×	×	×	×

Service*	MS WinNT-Trojan Horse potential with POSIX enabled	9.00	H	H	H	✓	/	✓	✓
Trojan Horse-MS Windows-BackOrifice 2000		9.00	H	H	H	✓	/	✓	✓

In Summary

- NIDS/NNIDS tells us if we are under attack
- HIDS tells us if we have been attacked
- VA tells us if we are/may-be vulnerable to attack
- There is overlap between the approaches, but also feedback
- But is it up-to-date?

ISMS

1 – What do the standards say?

What does ISO/IEC Say?

■ 9.7.2 Monitoring System Use

➤ *(c) unauthorised attempts such as*

...

➤ *(3) alerts from proprietary intrusion detection systems*

What does BS 7799-2 say?

■ Annex B (informative)

➤ *B.4 Check Phase ...*

➤ *EXAMPLE 1:*

The automatic actions of intrusion detection technology. A network intrusion detector checks whether the security of other components has been penetrated.

What else ...

- Annex B also talks about:
 - *Routine checks*
 - *Self-policing procedures*
 - *Learning from others*
 - *Internal ISMS audit*
 - *Management Review*
 - *Trend analysis*

ISMS

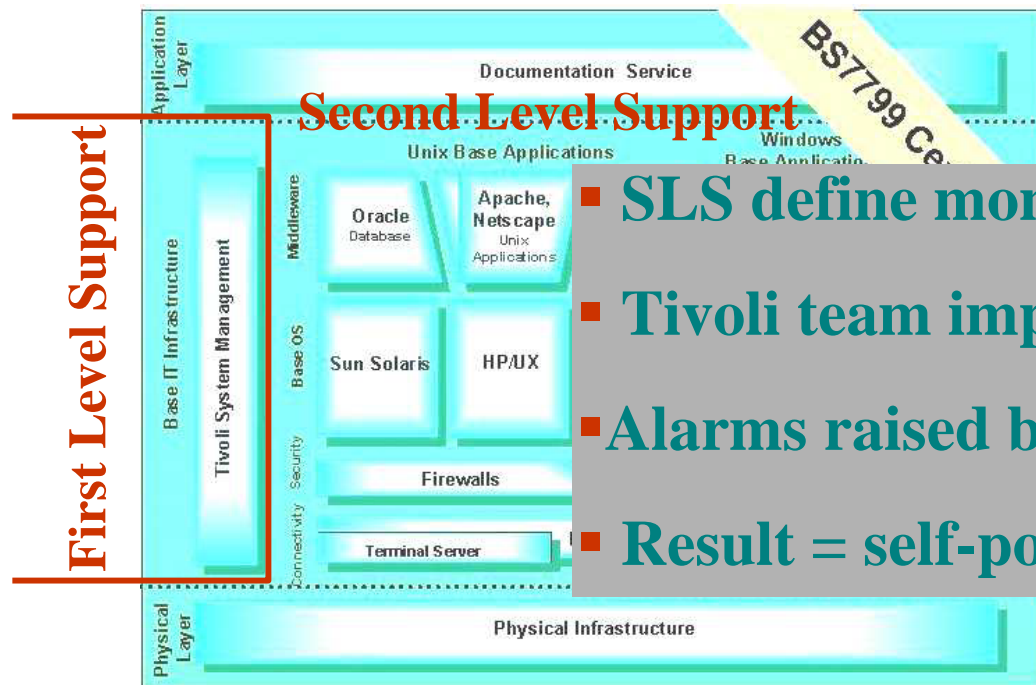
2 – A case study

Vodafone Information Systems



Management Structure

- Single team ↔ one team per “architectural” component



- SLS define monitoring requirements
- Tivoli team implement them
- Alarms raised by ARS
- Result = self-policing procedure

- Use for IDS



Use for CERT

- The implementation is automated and self-policing



```

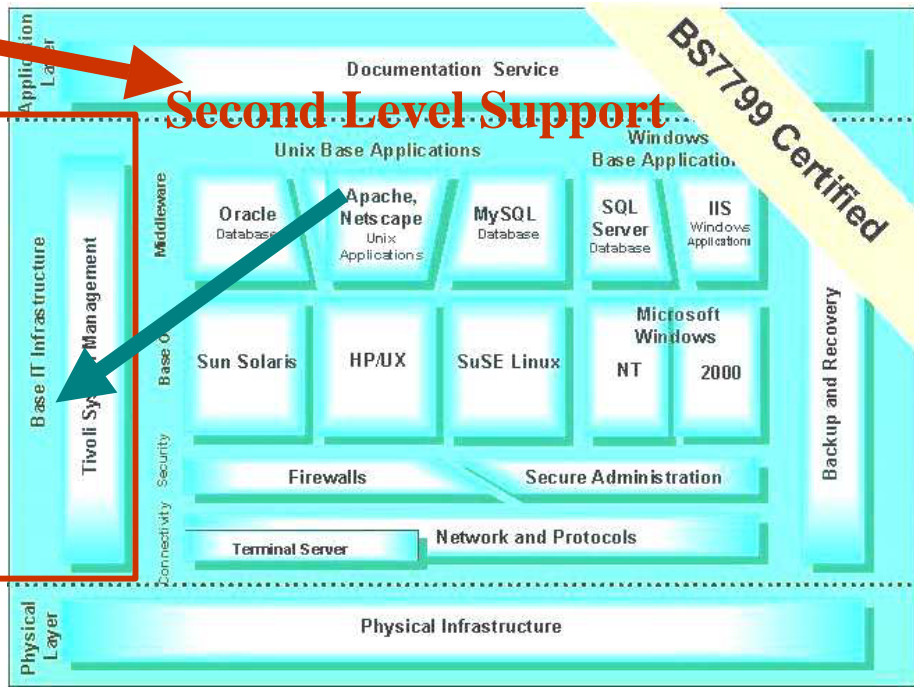
From: info@gamma.com
To: info@gamma.com
Subject: Info: your search results

This is an automated email to inform you of 'new' CVE entries since it
will show new entries are found, and only the profiles that you have
opted to the ISO profile management system. (Email about for you
Product: Executive Engineer)
New vulnerabilities:
CAN-2001-0444 on http://www.fbi.gov/ins/cfr/ins/can-2001-0444
CAN-2001-0445 on http://www.fbi.gov/ins/cfr/ins/can-2001-0445
CAN-2001-0446 on http://www.fbi.gov/ins/cfr/ins/can-2001-0446
CAN-2001-0447 on http://www.fbi.gov/ins/cfr/ins/can-2001-0447
CAN-2001-0448 on http://www.fbi.gov/ins/cfr/ins/can-2001-0448
  
```

Automatic process

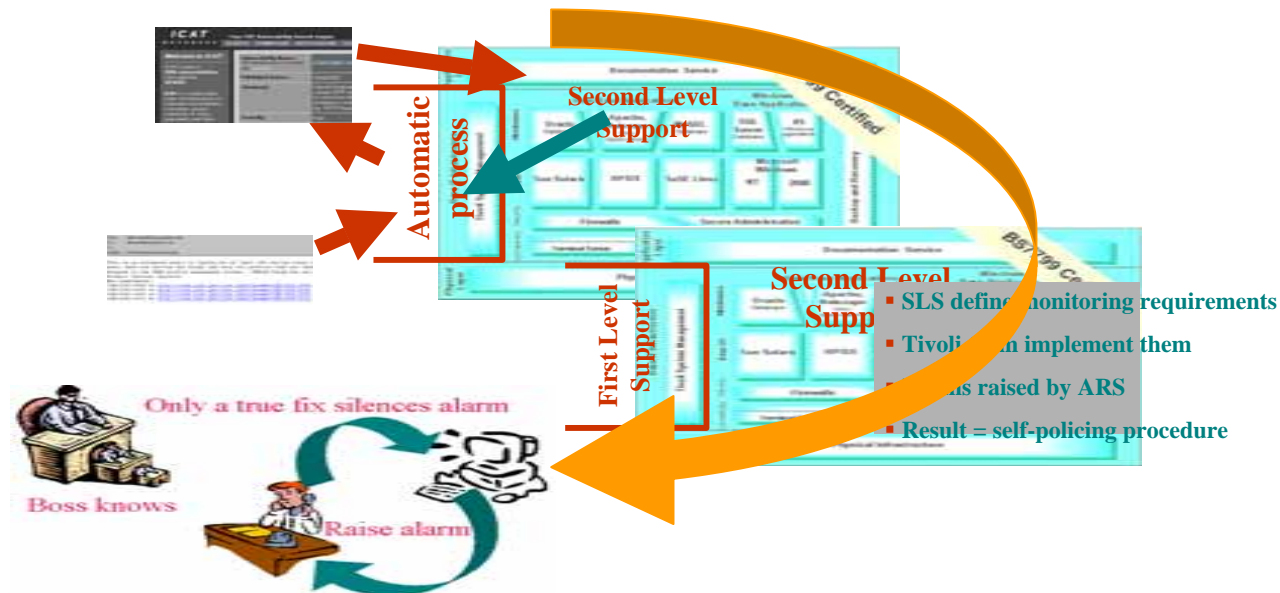
Second Level Support

BS7799 Certified



And everything Else

- Just an extension to trapping database problems..



- And what else....

Observations and Conclusions

Observations/Conclusions

- IDS is nothing new but very, very important
- It fits extremely well with BS 7799 – we designed it that way
- Major problem is new attacks and false positives
- At least with IT infrastructure there are methods to keep up to date



Thank you



I will take questions in the panel later

