

# "It Only Takes a Pinprick to Burst your Enterprise Security Bubble"

WWISA Presentation

Monday 28<sup>th</sup> November 2005

Andy Prow,

Managing Director of Aura Software



# The Message

“Think about security in EVERY IT project within your organisation”

“Make NO assumptions about which aspects of your IT are SAFE”

“PLAN for a security breach”

“Make information security a CEO and senior management team priority”

“Raise employee awareness of security issues within the whole organisation”

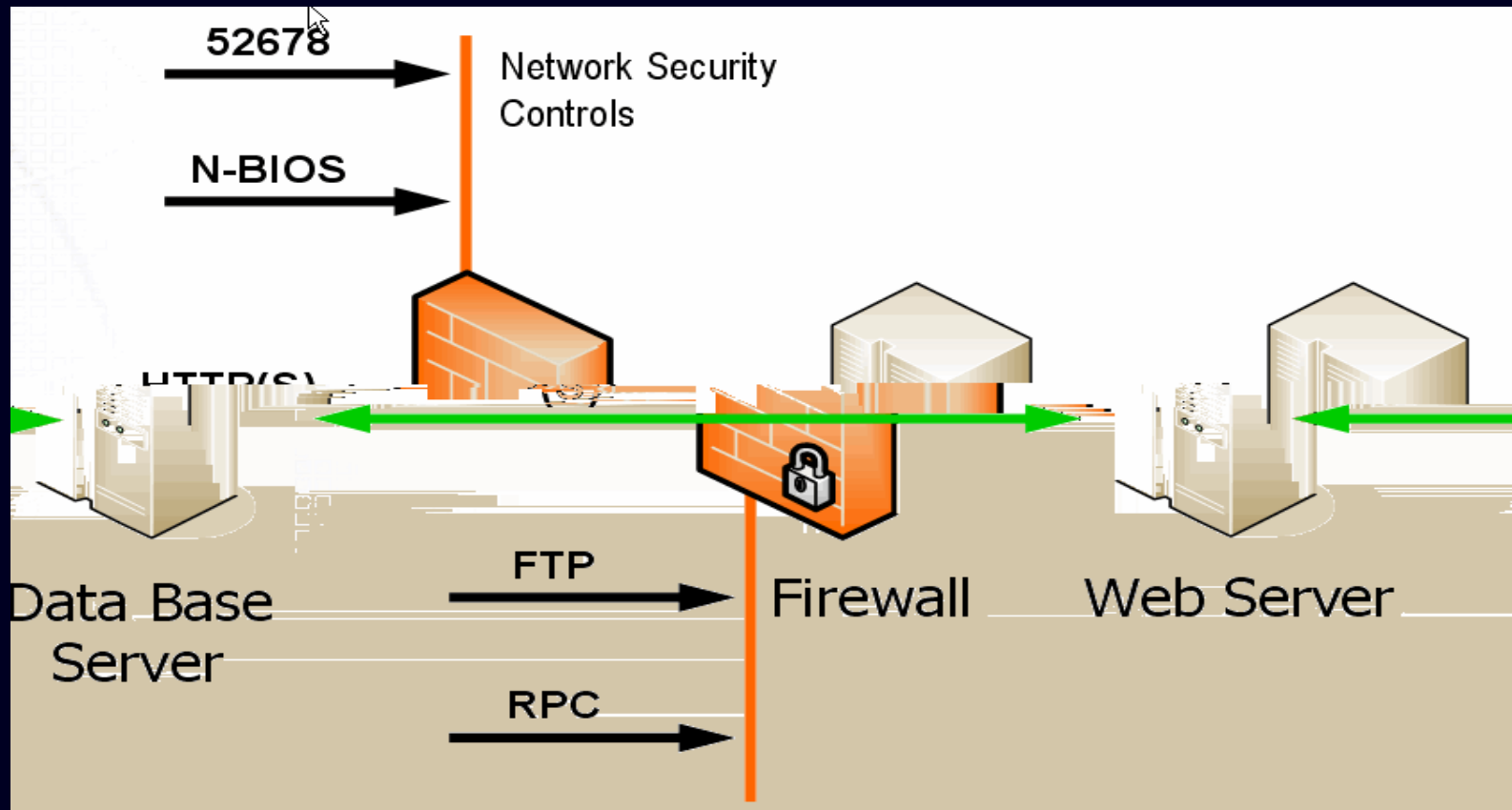
# Who are we?

- Andy Prow
  - Software development industry for 11 years
  - Lead development and development manager roles
  - Technical Architect and Solutions Architect
- Aura Software Architects (2001)
  - Software Architecture and Design
  - Specialist Development (Microsoft Technologies)
- Aura Software Security (2005)
  - Security Analysts and Consultants
  - Secure Software Development Experts

# Today's Talk?

- Common Vulnerabilities and Exploits
  - Things you will be facing and SHOULD know about
- Common Protection
  - Things you SHOULD have in place
- Unusual Vulnerabilities
  - Issues you can't plan for (real-world examples)
- What to do
  - How to protect against issues you can't plan for!

# Common Vulnerabilities: Web-interfaces



# Common Vulnerabilities: Web-interfaces

- Web

- Unpatched web-servers and database servers.

- Automated web-vulnerability scanners

- Acunetix, WebInspect

- Invalid file permissions

- Google searches e.g.

- filetype:mdb users.mdb

- intitle:index.of.etc passwd

- Custom

- Scripting / SQL Code Injection

- Cookie tampering – Achilles (web-proxy)

- Brute force attacks – Hydra, Brutus

- Man in the middle

- Sniffing web-traffic

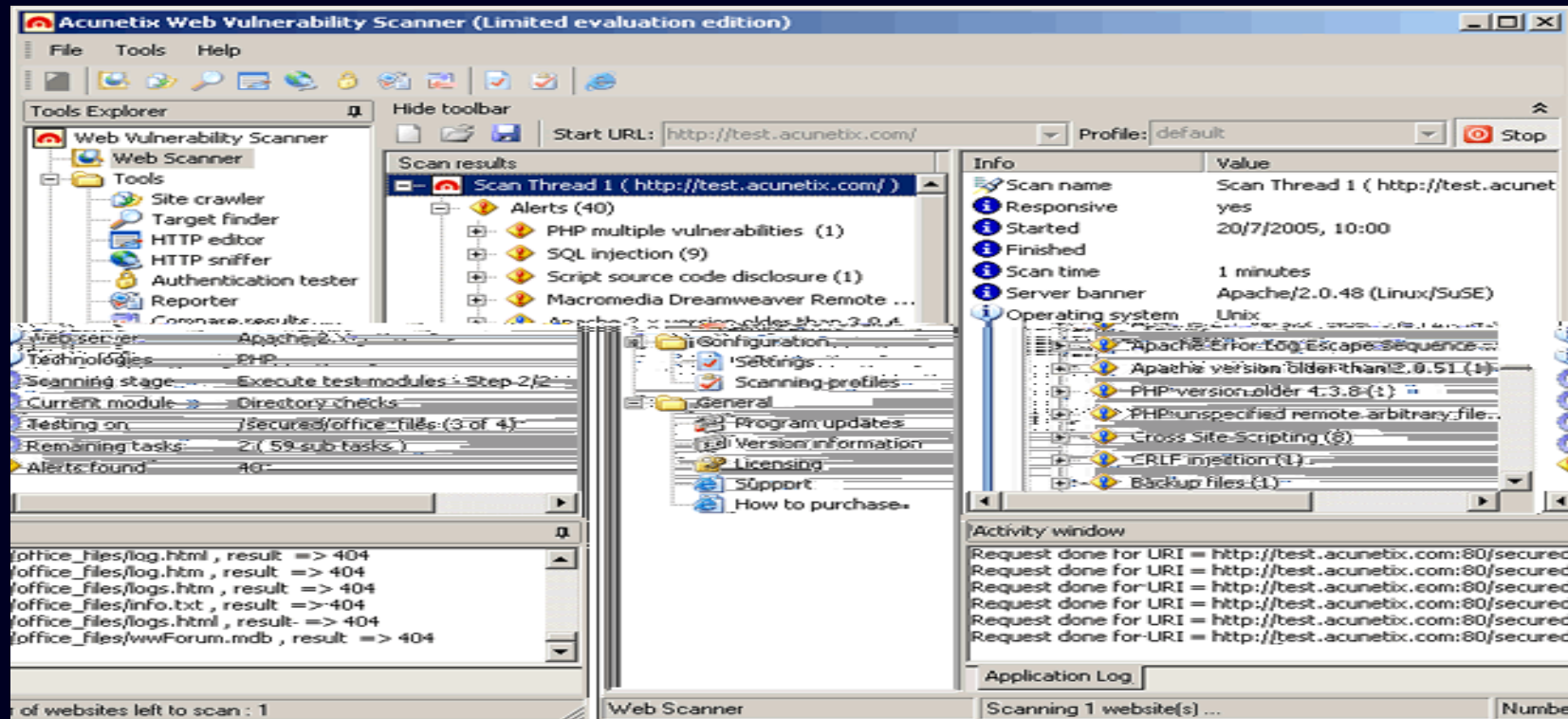
- Pharming (DNS cache poisoning)

- Proxies that spoof SSL

- Odysseus

# Common Vulnerabilities Web-interfaces

- Acunetix
  - Automated web-vulnerability scanner



# Common Vulnerabilities Wireless

- Wireless

- Wireless detection tools

- Network Stumbler, Kismet (KisMAC)
    - Hidden SSID identification, AP Model & Type, WEP/WPA, MAC address filtering...
    - “Wellington WarDrive” in June – 300+ scanned, 100+ OPEN (50 Corporate), and 100+ poorly secured (WEP and/or MAC address filtering only)

- MAC address sniffing

- MAC address spoofing

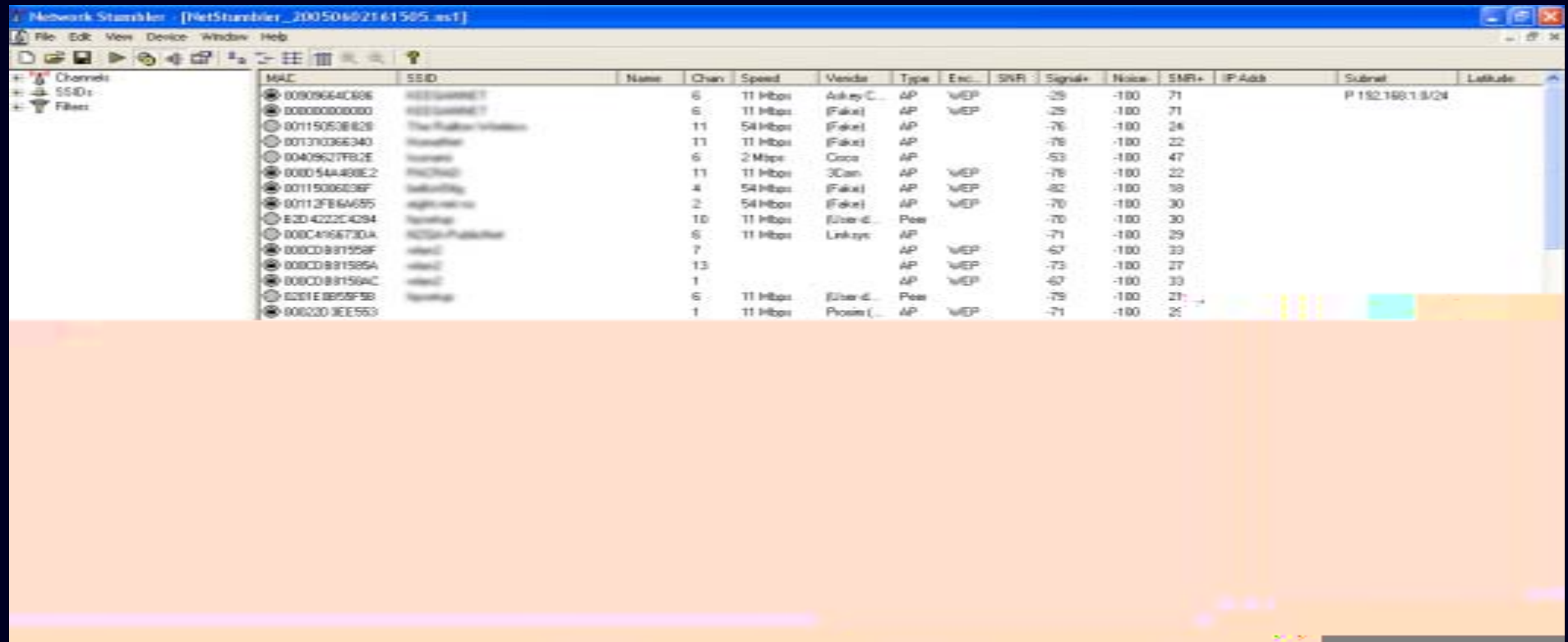
- WEP cracking

- WPA cracking

# Common Vulnerabilities Wireless

Network Stumbler

–Wireless Detection Tool



The screenshot shows the Network Stumbler application window. The main area displays a table of detected wireless networks with the following columns: MAC, SSID, Name, Chan, Speed, Vendor, Type, Enc, SNR, Signal, Noise, SMR, IP Addr, Subnet, and Latitude. The table contains 15 rows of data, including entries for '192.168.1.1', '192.168.1.24', and '192.168.1.33'.

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc	SNR	Signal	Noise	SMR	IP Addr	Subnet	Latitude
00909664C606	192.168.1.1		6	11 Mbit/s	Artek C...	AP	WEP	-29	-100	71			P 192.168.1.1/24	
000000000000	192.168.1.24	(Fake)	6	11 Mbit/s	(Fake)	AP	WEP	-29	-100	71				
001150538828	The Huber-W...		11	54 Mbit/s	(Fake)	AP		-76	-100	24				
00137036E340	Hotspot		11	11 Mbit/s	(Fake)	AP		-76	-100	22				
00409C27FB2E	Hotspot		6	2 Mbit/s	Cisco	AP		-53	-100	47				
000054A480E2	Hotspot		11	11 Mbit/s	3Com	AP	WEP	-76	-100	22				
00115006036F	Hotspot		4	54 Mbit/s	(Fake)	AP	WEP	-82	-100	38				
00112FB6A655	Hotspot		2	54 Mbit/s	(Fake)	AP	WEP	-70	-100	30				
E3D422C4294	Hotspot		10	11 Mbit/s	(Fake)	Pos		-70	-100	30				
00C416673DA	Hotspot		6	11 Mbit/s	Linksys	AP		-71	-100	29				
000CD881588F	Hotspot		7			AP	WEP	-67	-100	33				
000CD881585A	Hotspot		13			AP	WEP	-73	-100	27				
000CD881584C	Hotspot		1			AP	WEP	-67	-100	33				
0201E8855F98	Hotspot		6	11 Mbit/s	(Fake)	Pos		-75	-100	21				
000203CE553	Hotspot		1	11 Mbit/s	Proxim (...)	AP	WEP	-71	-100	26				

# Common Vulnerabilities Servers

- Known vulnerabilities and exploits
  - Specialist tools and websites to:
    - Identify version of server and services (such as telnet, web-server, FTP)
    - Map versions against known and new exploits
    - Provide exploitation tools, packets and payloads
  - Unpatched / slow to patch
    - “80% of exploits are available within the first 19 days of a critical vulnerability”
    - Poorly administered
      - “When the DoD did studies on the matter, they found these actual attacks accounted for only 30% of hacking. Attacks against configuration and essentially poor system hardening account for 70% of successful attacks.”
- Unauthorised administrator or physical access
  - Who are your administrators? Are they skilled?
  - Secure location
  - Hardware re-use

# Common Vulnerabilities Servers

ElseNot Project - [ElseNot.com](http://ElseNot.com)

–“Goal: Exploit for Every Microsoft Security Bulletin”

## ElseNot Project

Layne [at] Elsenot . com

Goal: Exploit for every Microsoft Security Bulletin

[133 Exploits](#) / [459 Bulletins](#)

[Info](#) - [Contact](#) - [References](#)

Date	Bulletin Description and Exploit	Affected Software Service Packs	Bulletin Rating
Nov 8, 2005	<b>MS05-053:</b> <a href="#">Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (896424)</a> <b>Exploit:</b> <a href="#">Please Submit</a>	Windows 2000 Service Pack 4, Windows XP Service Pack 1, Windows XP Service Pack 2, Windows Server 2003 Gold, Windows Server 2003 SP1	Critical
Oct 11, 2005	<b>MS05-052:</b> <a href="#">Cumulative Security Update for Internet Explorer (896688)</a> <b>Exploit:</b> <a href="#">Please Submit</a>	Internet Explorer 5.5 SP2, Internet Explorer 5.01 SP4, Internet Explorer 6.0 SP1, Windows Server 2003 Gold, Windows Server 2003 SP1, Windows XP Service Pack 2, Windows 2000 Service Pack 4, Windows XP Service Pack 1	Critical
Oct 11, 2005	<b>MS05-051:</b> <a href="#">Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)</a> <b>Exploit:</b> <a href="#">Please Submit</a>	Windows 2000 Service Pack 4, Windows XP Service Pack 1, Windows XP Service Pack 2, Windows Server 2003 Gold, Windows Server 2003 SP1	Critical

# Common Vulnerabilities Servers

MilW0rm – [www.milw0rm.com](http://www.milw0rm.com)

–Up to date source of exploits for all platforms and applications.



The screenshot shows the MilW0rm website interface. At the top, there are navigation links: [ home ] [ exploits ] [ platforms ] [ shellcode ] [ search ] [ cracker ] [ links ] [ rss ] [ archive ]. The main heading is "MILW0RM" in a large, stylized font, with "STREETXL.COM" underneath. Below the heading, there is a sub-heading "[ remote ]". The main content is a table of exploits with columns for #, DATE, DESCRIPTION, HITS, and AUTHOR. The table is partially obscured by a sidebar on the left and a search bar at the top.

#	DATE	DESCRIPTION	HITS	AUTHOR
	2005-11-22	Mambo <= 4.5.2 Globals Overwrite / Remote Command Exection Exploit	1429	R D rgod
	2005-11-20	MailEnable 1.54 Pro Universal IMAPD W3C Logging BoF Exploit	1005	R M D y0
	2005-11-20	Google Search Appliance proxystylesheet XSLT Java Code Execution	1330	R M D H D Moore
	2005-11-17	FluxBoard 1.0.3 (config.php) SQL Injection / Command Execution Exploit	1538	R D rgod
	2005-11-17	FreeFTP <= 1.0.8 (USER) Remote Buffer Overflow Exploit		
	2005-11-12	Veritas Storage Foundation 4.0 VCSI18N LANG Local Overflow Exploit		
	2005-11-09	Operator Shell (osh) 1.7-14 Local Root Exploit		
	2005-11-09	Sudo <= 1.6.8p9 (SHELLOPTS/PS4 ENV variables) Local Root Exploit		
	2005-11-09	FreeBSD (4.x , < 5.4) master.passwd Disclosure Exploit		
	2005-11-08	SuSE Linux <= 9.3, 10 (chfn) Local Root Privilege Escalation Exploit		

# Common Vulnerabilities Servers

## Nessus – Server Vulnerability Scanner

Report for scope: All checks (Task: scan localhost)

Subnet	Port	Severity
localhost	unknown (5432/tcp)	Security Warning
	www (80/tcp)	Security Note
	unknown (6000/tcp)	
	ntp (123/udp)	
	mysql (3306/tcp)	
	general/tcp	

The /doc directory is browsable.  
/doc shows the content of the /usr/doc directory and therefore it shows which programs are installed on the system.

Solution : Use access restrictions for the /doc directory.  
If you use Apache you might use this in your access.conf:

```
<Directory /usr/doc>
AllowOverride None
order deny,allow
deny from all
allow from localhost
</Directory>
```

Risk factor : High  
CVE : CVE-1999-0678  
BID : 318

Scan took place from Tue Feb 8 00:20:07 2005 to Tue Feb 8 00:20:49 2005

Message log  
Welcome to Nessus GTK Client, <http://www.nessus.org/>  
Copyright 1998-2004 by Renaud Deraison  
Authors: Renaud Deraison, Thomas Arendsen Hein, Jan-Oliver Wagner, Michel Arboi (SSL-Support), Bruce Verderaime (Pie/Charts)  
Info: This page is not available in the current context.

not connected

# Common Protection

- Normal steps taken
  - Patching servers
  - Firewalls, DMZ, VPNs
  - Website security, SSL
  - Antivirus and Anti-Spyware products
  - Mail filters
- Additional Steps
  - Dedicated IT Security Team
  - Network Monitoring Systems
  - Intrusion Detection Systems

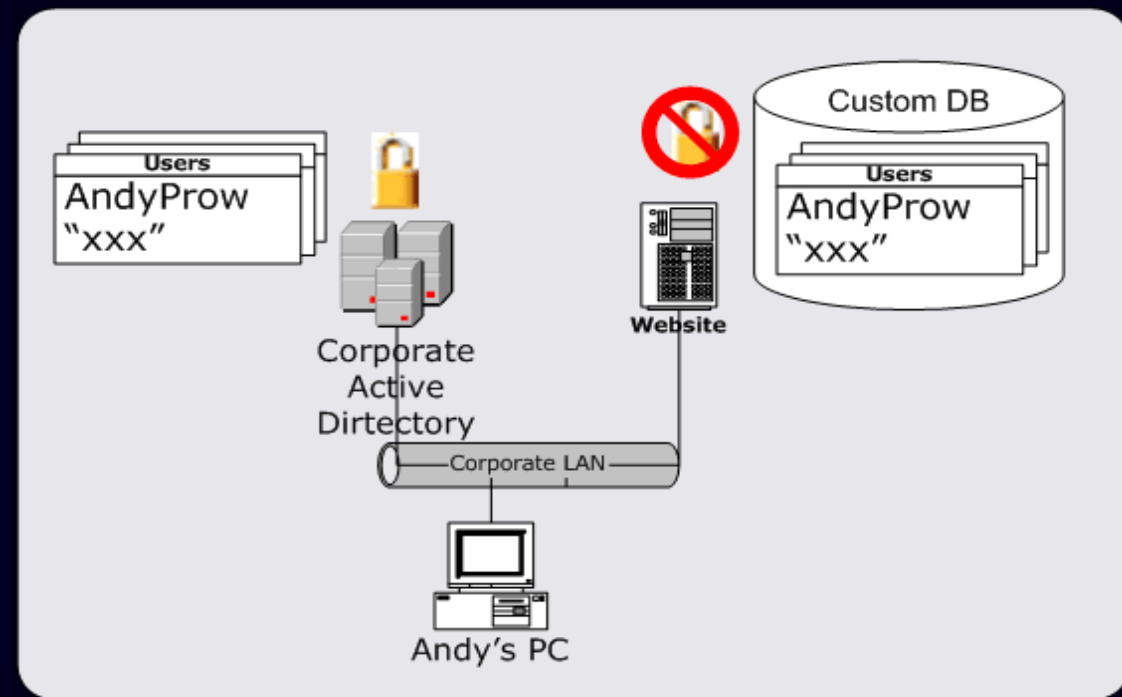
# Things that Pop your Bubble

- Wellington bank with 14 locked down wireless AP, but 1 wide-open AP
  - The issue:  
Pro-active, “can-do” manager buys a standard DSE Wireless AP to cater for new temporary staff. Simply installs and it works.
  - The impact:  
TOTALLY unsecured wireless access point, with default settings connected to corporate LAN!

# Things that Pop your Bubble

“Government agency with a custom application with unsecured NT User IDs and Passwords”

- AD is well secured
- Users self register with AD usernames and passwords
- Custom DB is NOT secured



# Things that Pop your Bubble

“Managing Director with default wireless AP at home”

## –The Issue

- MD connects to ADSL
- Purchases a common ADSL/Wireless router
- Plug-and-play settings with NO security

## –The Threat

- The MD's laptop is now vulnerable to a hack from their home

# Things that Pop your Bubble

## Latest Example: "Sony Rootkit"

### -The Issue

- New Sony CDs install a copy protection utility that sits beneath Windows XP, and stops multiple copies of a CD, or unprotected ripping of the CD.

### -The Threat

- The "copy protection utility" is based on a RootKit, which sits beneath the operating system. RootKits are a hacker's dream as they give escalated permissions to processes, can create files and processes invisible to the OS. Usually the hard-part for a hacker is "how to get a RootKit onto a remote machine?" – thanks Sony!

# What do you do?

- Threat Modelling

- Understand your adversary

- Who would breach your security?

- Understand your assets?

- What would they be after?

- Understand your IT security risks

- How could an attacker get in?

- Understand the impact to your business

- What could they do to impair your business?

- Mitigate the threats

- How do we prevent this from happening?

# What do you do?

- In-House-Hacker

- Performs pro-active security checks. E.g.

- Server vulnerability checks

- Wireless AP checking

- Armed with the latest hacker tools

- MUST be well trained

- MUST be well trusted

- Trusted Security Advisors (Aura)

- Constantly monitoring threats, exploits, patches and tools

- Trusted entity, who knows your internal IT infrastructure and configuration.

- Proactively participates in the hacker / security community e.g.

- OWASP – [www.OWASP.org](http://www.OWASP.org) - Open Web Application Security Project

# The Message

“Think about security in EVERY IT project within your organisation”

“Make NO assumptions about which aspects of your IT are SAFE”

“PLAN for a security breach”

“Make information security a CEO and senior management team priority”

“Raise employee awareness of security issues within the whole organisation”

# Do It Now...

- Make security part of your day-to-day business
  - Think security in every IT project
  - Think security in every IT system
- Make information security a CEO and senior management team priority
  - Actually DO Threat Modelling
  - Ensure you have security processes in place
- Raise employee awareness of security issues within the whole organisation.
  - Data classification
  - Danger of USB devices, iPods, Sony CDs, Home wireless...
  - Ongoing training in systems and controls

# "It Only Takes a Pinprick to Burst your Enterprise Security Bubble"

WWISA Presentation  
Monday 28<sup>th</sup> November 2005

Andy Prow,  
Managing Director of Aura Software  
Andy@AuraSoftware.co.nz

More info is available from

[www.AuraSoftwareSecurity.co.nz](http://www.AuraSoftwareSecurity.co.nz)

