The Whitehat Advisories: An Introduction

Invenia mvia mautfacia m

“Why do I need IT security?”

- 2003 statistics show a total of 138000 incidents
- 2003 FBI survey showed a total annual loss of
  - $70.1 million (theft of proprietary data)
  - $65.6 million (denial of service)
  - $27.3 million (viruses)
- 2004 E-crime survey showed an annual loss of $660 million
- The same survey showed respondants averaged 136 incidents
- 2003 statistics show 70% of incidents occurred over the web port
- Gartner reports about 600 successful web compromises a day
- Gartner says 60% of incidents to be financially/politically motivated in 2005
- Radicati Group estimates spam at 52% of email messages in 2004

Inveniamviamautfaciam

“But what about … ?”

Myth 1: Perimeter security is paramount.
Reality: Firewalls are important but not, by themselves, adequate.

Myth 2: The network is configured securely.
Reality: All human systems are fallible.

Myth 3: We know the ins and outs of the system.
Reality: Not all of them.

Myth 4: Depend on software.
Reality: Even the best is flawed.

Myth 5: Relying on core vendors helps security.
Reality: On the contrary, heterogeneity may promote security.

Myth 6: Regulation will taper off.
Reality: No it won’t. it will get worse.

Myth 7: Identity controls keep the bad guys out.
Reality: Yes, but remember that good guys can turn bad.

Inveniamviamautfaciam

“Is it really that bad?”

- Microsoft had about 1 new security patch a week in 2003 (Total of 51)

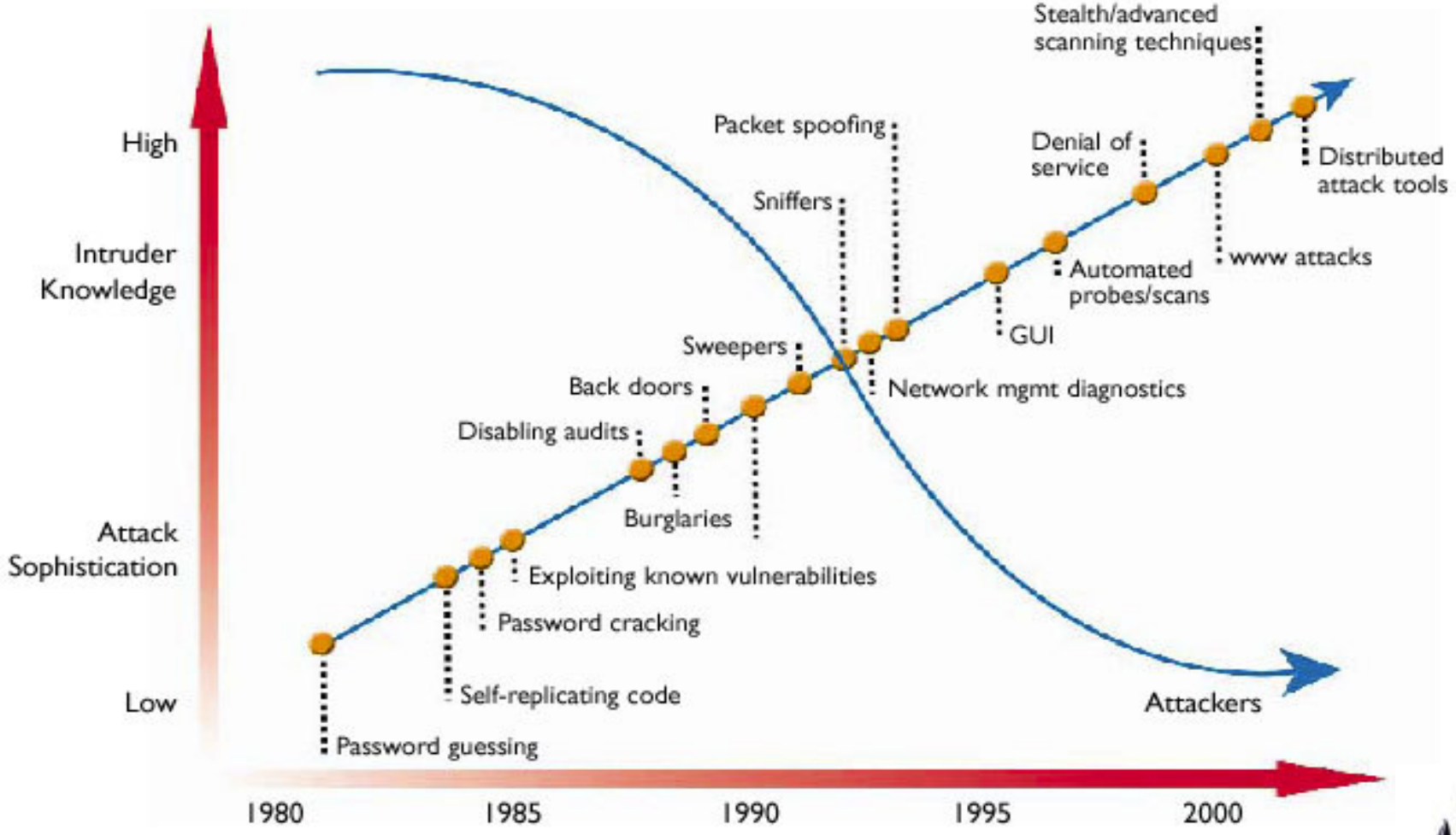
- HoneyNet project uses unprotected machines to measure attacks
  - Manually compromised, 15 minutes
  - Automated compromise, under 60 seconds
  - Life expectancies of vulnerable Win32 system is under three hours
  - Life expectancies of vulnerable Linux system is three months.

- USA Today conducted similar test from Sept. 10 to Sept. 25 2004
  - Intruders made 305,922 attempts to compromise six computers.
  - Windows XP using Service Pack 1, compromised nine times
  - First of the above compromises happened after 4 minutes

- According to the CERT centre, the yearly number of vulnerabilties;
  - 2000 – 1090 vulnerabilities
  - 2001 – 2437 vulnerabilities
  - 2002 – 4129 vulnerabilities
  - 2003 – 3784 vulnerabilities
  - 2004 – 3780 vulnerabilities

Inveniamviamautfaciam

“Is it really that bad?”



Attack sophistication vs. intruder technical knowledge

Source: Software Engineering Institute, Carnegie Mellon University

Invenia m via m au t fa c ia m

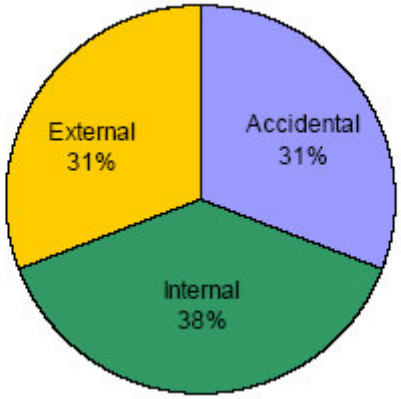
"So who does this stuff?"

- 2003 E-crimes survey, respondents reported
  - 71% of attacks came from outsiders
  - 29% of attacks came from insiders

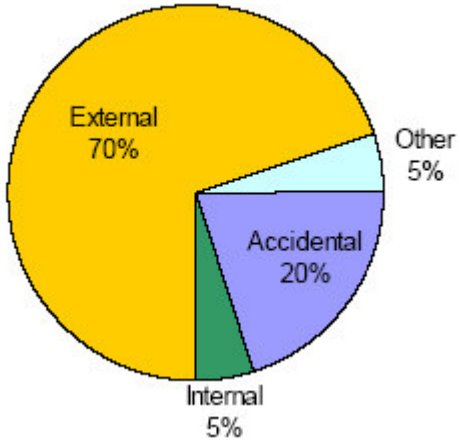
- Same survey's respondents had this to say about the source of security threats
  - 40% (hackers)
  - 31% (current or former employees)
  - other 29% (automated attacks, neglience, etc)

- 2003 Deloitte & Touche, 70% of security incidents originated externally

- The graphs from the above survey follow..



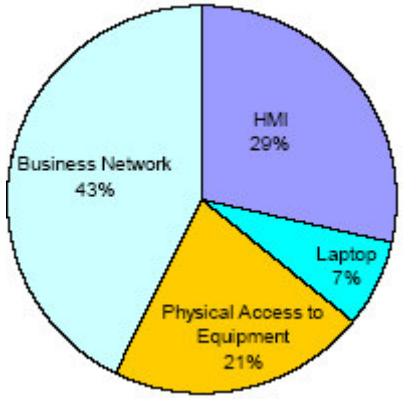
Security Incidents by Type 1982 -2000



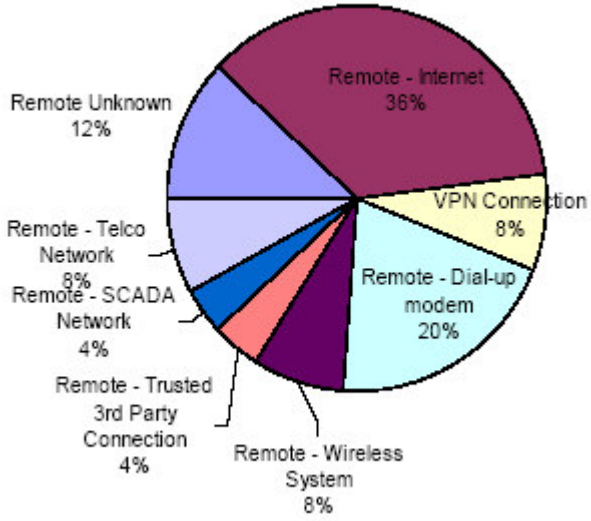
Security Incidents by Type 2001-2003

“How do they get in?”

- 2003 Deloitte & Touche split incidents into internal and external..



Internal Security Incidents by Entry Point



External Security Incidents by Entry Point

- Symantec fears blended threats which combine multiple attack vectors

Inveniamviamautfaciam

“What does this mean in SA?”

•IT Security in SA may not have publicity it does elsewhere, but …

•SA has the King Commision II, corporate governance report
  - •The entire board is responsible for IT security breaches
  - •Security measures and risk must be disclosed in annual report

• The ECT Act firmly lays out penalties for cyber-crime

• We have also had a share of sensationalism; Absa, Carte Blanche, etc

• The world is now also a very small place, truly a global village

• The point is: We are not exempt because we are in South Africa

“The Whitehat Advisories”

- We are people who believe we should share knowledge and help others to understand IT security
- We believe in raising the awareness level of all interested parties
- We want to show not only what the attackers do, but how to prevent it, as well as the best business practices around IT security. As only with all three can a proper and coherent IT security strategy be formed
- We believe this is important because only by properly understanding the problems can we address them
- The attacker community has always seemed to have better communication then normal business, we want to help address this

Invenia amvia amautfaciam

Thank you for your attention

References

-http://www.microsoft.com/smallbusiness/issues/technology/security/
-http://www.cert.org/stats/cert_stats.html
-http://www.cert.org/about/ecrime.html
-http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm
-http://isc.sans.org/survivalhistory.php
-http://www.honeynet.org

Inveniamviamautfaciam