IUMI 2004 · SINGAPORE · CONFERENCE · 12 – 15 SEPTEMBER

Cyber Terrorism

Shawn Carpenter
Computer Security Analyst
Sandia National Laboratories

Supported by the International Borders
and Maritime Security Program,
Charles Massey, Manager
cdmasse@sandia.gov

Sandia National Laboratories

What is Cyber Terrorism?

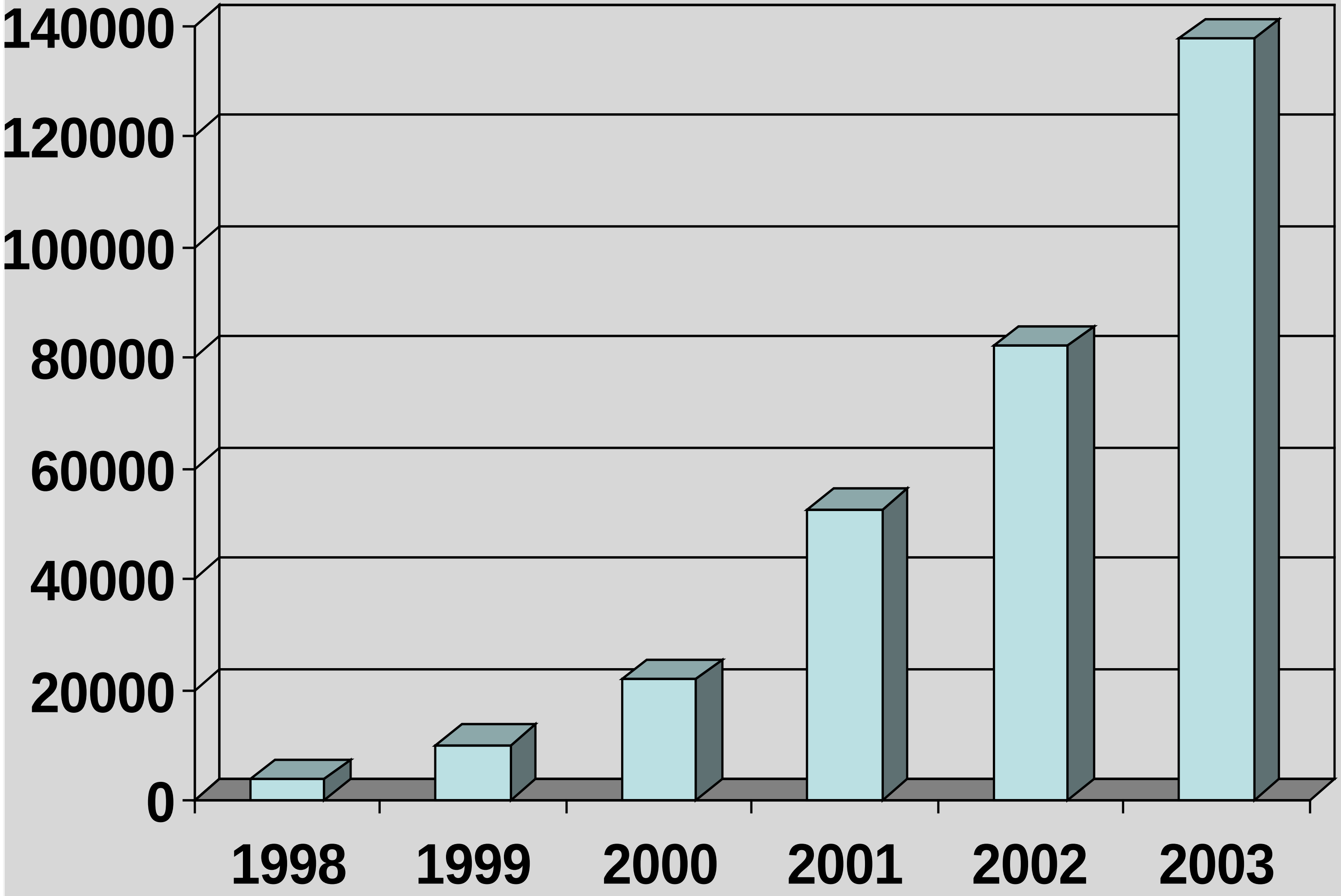
- Premeditated, politically motivated attack
- Targets information systems
- Results in violence against noncombatant targets or substantial economic harm

Is the Threat Real?

- Port of Houston – 2001
- Queensland, Australia sewage treatment system – 2000
- Arizona’s Roosevelt Dam – 1998

Computer Security Incidents

From (US CERT) Computer Emergency Response Team statistics



•IUMI 2004•
SINGAPORE CONFERENCE
•12 – 15 SEPTEMBER•

Sandia National Laboratories

Anatomy of an Attack

- Vulnerabilities in software / unprotected network access points
- No vulnerability assessment
- Poor awareness of security issues

  Queensland, Australia case

  - Unsecured wireless access points
  - Accessed using ordinary Commercial Off The Shelf (COTS) software and hardware
- Poor access control and monitoring
- Result:
  - Unauthorized control of wastewater/freshwater pumping stations
  - Environmental and economic damage

• IUMI 2004 • Singapore Conference • 12 – 15 September •

Sandia National Laboratories

Large Ports Are Attractive Targets

- Potentially high economic impact

  Significant impact on ship/port/facility

  Possible world trade disruption

  Port of Houston impact
- High visibility
- Low cost
- Low risk
- Numerous attack options

Marine Industry

Could this affect your organization?

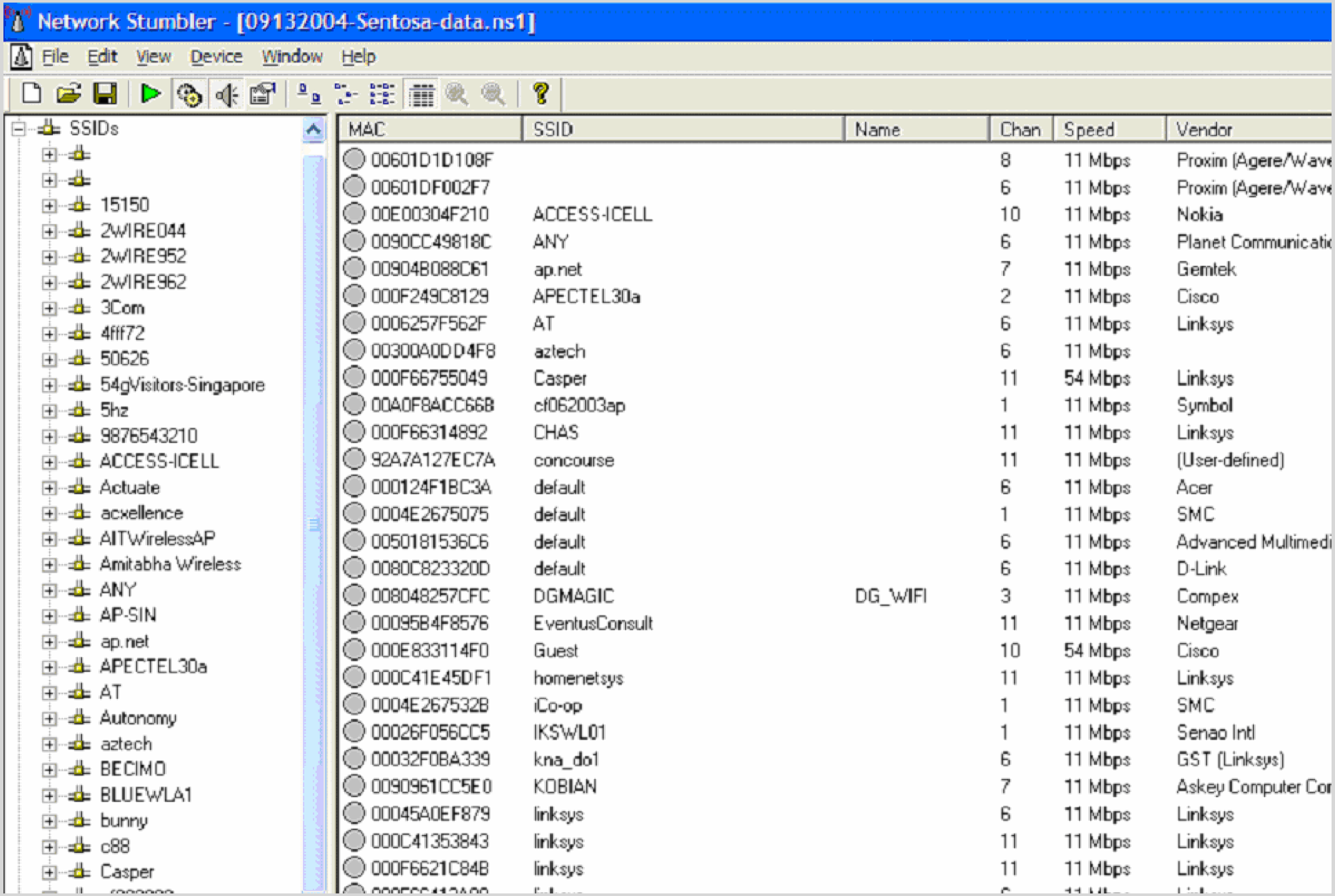
- Supervisory Control And Data Acquisition (SCADA)
- Port logistical software applications
- Internet / Communications

  Email

  Antivirus software (Trojans, viruses, worms)

  Ohio’s Davis-Besse Nuclear Power Plant – 2003
- Wireless communications (war driving)
- Modems (war dialing)
- Insiders / disgruntled employees

Sampling of 120 Unprotected Wireless Access Points Discovered in a Ten Minute Taxi Ride


Network Stumbler - [09132004-Sentosa-data.ns1]
File Edit View Device Window Help

SSIDs
- (blank)
- (blank)
- 15150
- 2WIRE044
- 2WIRE952
- 2WIRE962
- 3Com
- 4fff72
- 50626
- 54gVisitors-Singapore
- 5hz
- 9876543210
- ACCESS-ICELL
- Actuate
- acxellence
- AITWirelessAP
- Amitabha Wireless
- ANY
- AP-SIN
- ap.net
- APECTEL30a
- AT
- Autonomy
- aztech
- BECIMO
- BLUEWLA1
- bunny
- c88
- Casper

MAC	SSID	Name	Chan	Speed	Vendor
00601D1D108F			8	11 Mbps	Proxim (Agere/Wave
00601DF002F7			6	11 Mbps	Proxim (Agere/Wave
00E00304F210	ACCESS-ICELL		10	11 Mbps	Nokia
0090CC49818C	ANY		6	11 Mbps	Planet Communicatio
00904B088C61	ap.net		7	11 Mbps	Gemtek
000F249C8129	APECTEL30a		2	11 Mbps	Cisco
0006257F562F	AT		6	11 Mbps	Linksys
00300A0DD4F8	aztech		6	11 Mbps	
000F66755049	Casper		11	54 Mbps	Linksys
00A0F8ACC66B	cf062003ap		1	11 Mbps	Symbol
000F66314892	CHAS		11	11 Mbps	Linksys
92A7A127EC7A	concourse		11	11 Mbps	(User-defined)
000124F1BC3A	default		6	11 Mbps	Acer
0004E2675075	default		1	11 Mbps	SMC
0050181536C6	default		6	11 Mbps	Advanced Multimedi
0080C823320D	default		6	11 Mbps	D-Link
008048257CFC	DGMAGIC	DG_WIFI	3	11 Mbps	Compex
00095B4F8576	EventusConsult		11	11 Mbps	Netgear
000E833114F0	Guest		10	54 Mbps	Cisco
000C41E45DF1	homenetsys		11	11 Mbps	Linksys
0004E267532B	iCo-op		1	11 Mbps	SMC
00026F056CC5	IKSWL01		1	11 Mbps	Senao Intl
00032F0BA339	kna_do1		6	11 Mbps	GST (Linksys)
0090961CC5E0	KOBIAN		7	11 Mbps	Askey Computer Cor
00045A0EF879	linksys		6	11 Mbps	Linksys
000C41353843	linksys		11	11 Mbps	Linksys
000F6621C84B	linksys		11	11 Mbps	Linksys

Consequences

- Electronic intelligence loss
  - Aid physical attacks
  - Forge credentials
  - Emergency response plans
- Loss of data integrity
  - Change manifests
  - Redirect shipments / ships
  - Affect shipyard logistics
  - Cause delays
  - Impact inspections status

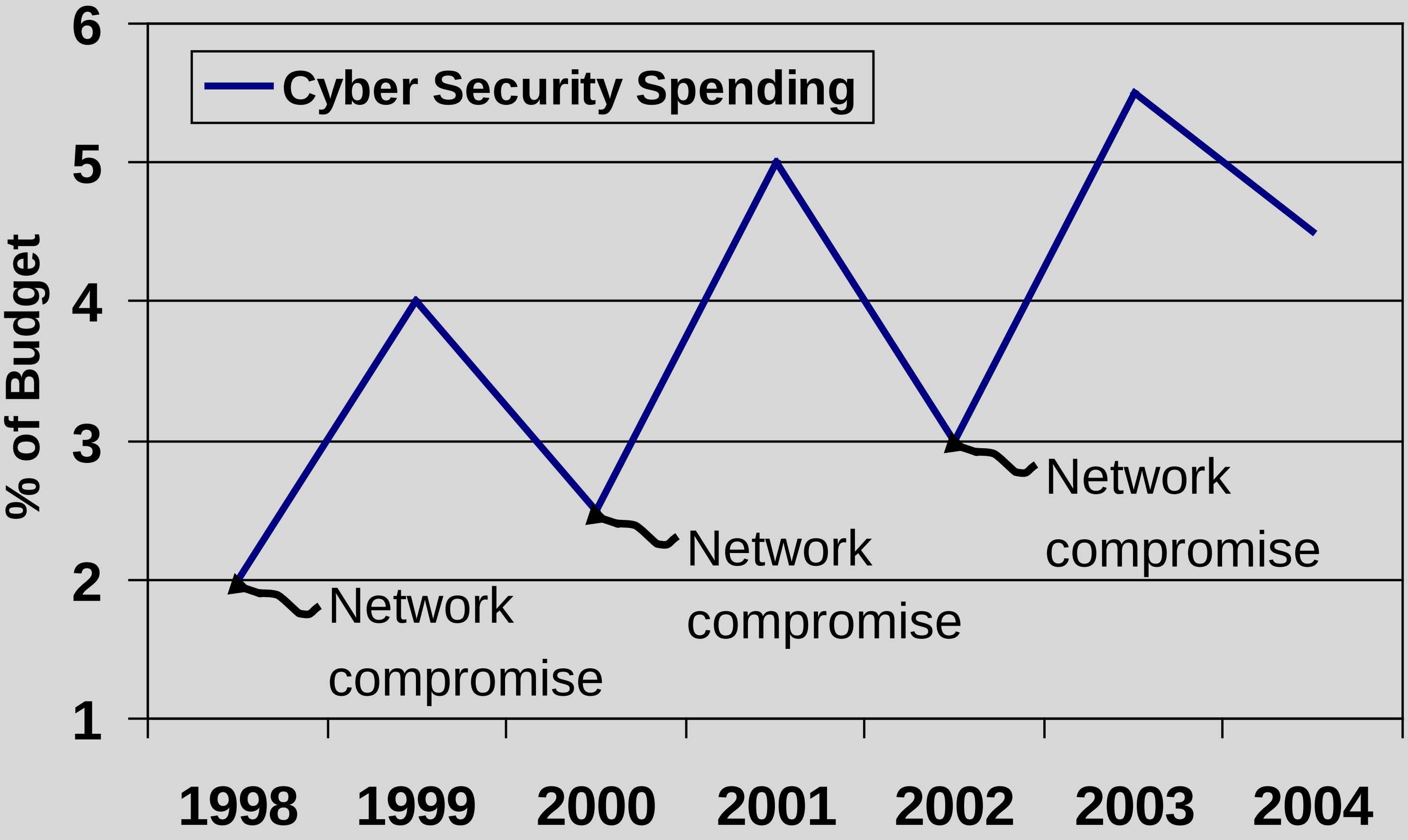
Port Cactus Scenario

- Target - Port Cactus, New Mexico
- Reconnaissance

  research target – Internet

  probe network for vulnerabilities
- Deliver Trojan via email
- Compromise other systems via trojaned system(s), stealthily install backdoors
- Capture logon credentials for port logistics application
- Change manifests, inspection records, etc. as necessary

The Reactionary Approach



The Proactive Approach

- There is no silver bullet

  Constant vigilance – dedicated personnel

  Network Intrusion Detection

  Effective process to quickly patch vulnerabilities

  Configuration management / firewalls / antivirus

  Integrated cyber incident response
- Backup systems / data recovery – no single point of failure
- Regular cyber security policy audits
- Formal network vulnerability assessments and corrective actions – Red Teaming
- Robust cyber security program with high-level support
- Employee education / awareness

IUMI 2004 SINGAPORE CONFERENCE 12 – 15 SEPTEMBER

Sandia National Laboratories

Questions?

Shawn Carpenter
Computer Security Analyst
Sandia National Laboratories
Albuquerque, NM
1-505-228-3762
1-505-845-7413
scarpe@sandia.gov