

Cyber Adversary Characterization

Know thy enemy!

Brief History of Cyber Adversary Modeling

- Mostly Government Agencies. Some others internally.
- Workshops – DARPA 2000 Other Adversaries, RAND 1999-2000 Insider Threat, SRI 2002 Cyber Adversary Spectrum
- Bad Assumptions – Defender about attacker
 - Capability, Ability, Skills, Knowledge, Privilege, Access
- Decision Factors – Attacker (risk averse) Model
 - Resources, Complexity, Sophistication, Stealth
- Defenders assume attackers will attack system as they would. Assume they will use/abuse the system as it was designed to be. Assume systems works as designed.
- Defenders always behind attackers tools and methods
- Underestimate likelihood of attack. Threat profile
- Too busy chasing Top 10 lists (SANS/CERT, etc..)

No, REALLY know your enemy

- Sun Tzu “Art of War”– Beyond “Know your enemy” (understand the threat) mission impact, policy dictates security posture and dictates response, policy enforcement mechanisms in place to ensure policy is carried out.
- Cannot always assume most likely course of action
- Must take into account the unlikely events and be prepared
- Kinetic world ideas don’t always transition into cyber world
- Spectrum of adversaries – abilities, capabilities and goals
- Individual or group – resource aggregation
- Given the same tool different adversaries may have very different capability (may also modify it to evade IDS signature detection, etc...)
- Labeling is therefore dangerous – false sense of security
- Knowledge increase may exceed your expectation once exploit becomes more widely available.
- Be aware of the win-win situations – no apparent mission impact
- Information aggregation issue
- Only attacker knows when attack starts and ends

Portraying the CA

- Red Team must portray credible and consistent adversary to show effect on defenses
- Do many of the things that are being outlawed – vulnerability discovery, exploit creation
- Not just penetration testing
- Planned attack(s) with counter moves given responses expected or unexpected with high expectation of success.
- Artificial time constraints. Real world not as limited
- Have overall goals and sub goals per step
e.g. access confidential data and not leave traces of steps

Why characterize?

- Theoretical: To gain understanding of and an ability to anticipate an adversary in order to build improved threat models.
- Practice: Improved profiling of attackers at post attack and forensic levels.

Threat Assessment and Cyberterrorism

Matt Devost

Terrorism Research Center, Inc.

Devost@terrorism.com

“Your Adversary is not a 1 or 0!”*

- Differentiation of Adversaries is essential to security planning and incident response
- Threat Assessment/Adversary Characterization feeds into Risk Management process
- Without Threat analysis, you are not performing Risk Management
- Threat analysis allows for concept of “acceptable risk” - not all Threats can or should be countered

*Jason Healey

Calculating Risk Exposure

- Risks must be managed in context of:
 - What **threats/adversaries** exist?
 - What **tools/capabilities** can they use?
 - How attractive is the target (**goal/intent/likelihood**)?
 - What level of **access** can be obtained?
 - What **impact** would attack have?
 - What **safeguards** can be deployed to minimize exposure?

Threat Agents of Interest

- Unstructured Hacker
- Structured Hacker
- Organized Crime/Industrial Espionage
- Insider (user/supervisor/admin)
- Unfunded Terrorist Group/Hacktivist
- Funded Terrorist Group
- Nation State

Threat Techniques of Interest

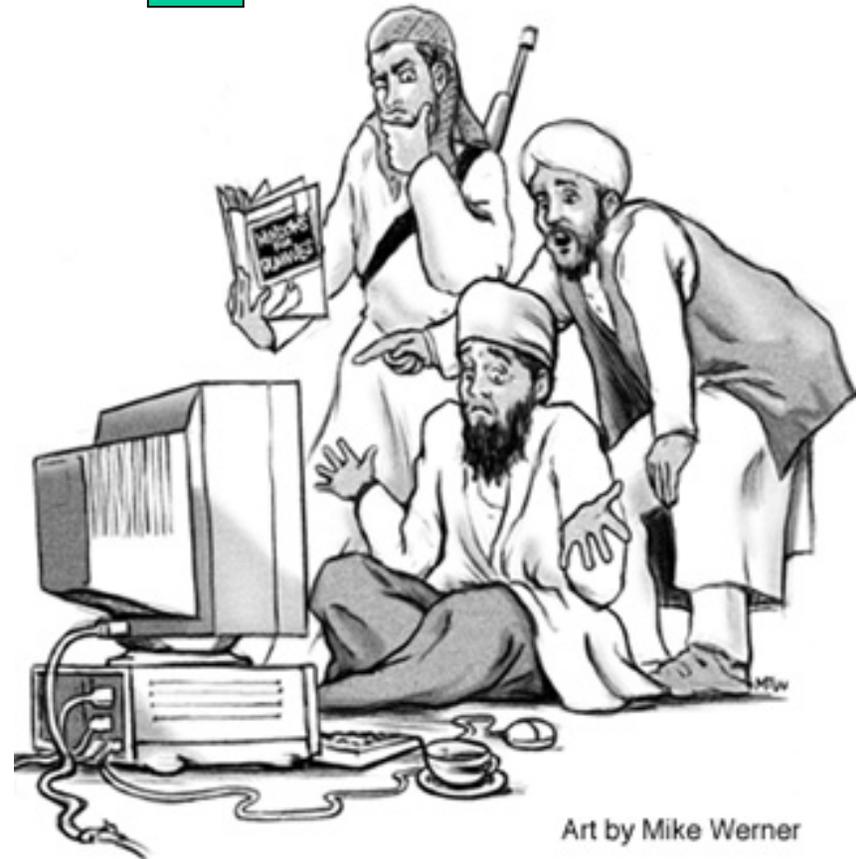
- Direct Penetration – Workstation
- Direct Penetration – Server
- Direct Penetration – Infrastructure Component
- InDirect Penetration – Workstation
- Indirect Penetration – Server
- Indirect Penetration – Infrastructure Component
- Customized Penetration Tool
- Insider Placement
- Insider Recruitment
- Malicious Code – Direct
- Malicious Code – Indirect
- Denial of Service
- Distributed Denial of Service
- Directed Energy
- Interception/Sniffing
- Spoofing/Masquerading
- Substitution/Modification
- Diversion

Implications for Cyberterrorism Analysis (Which one is correct?)

A



B



And how much are you willing to bet on it?

Characterizing Cyberterrorists

- Historical analysis won't work as we've never had a true incident of cyberterror
- “Imagine the threat”
- Red Team the threat
- Characterize capabilities and intent
- Assess and fix vulnerabilities
- Understand your current adversaries (e.g. what is happening now)

Adversary Characterization

Key Issues for Cyberterror

- Nature of terrorism has changed
 - International vs. Single Issue and Calculated Violence vs. Mass Casualty
 - Displaced groups may employ cyberterrorism as a differentiator
- Lessons are being learned by terrorists
 - What lessons can be drawn from cyberspace or critical infrastructure failures?
- Long-term planning cycle
 - 5 years of planning for Africa embassy attacks
- Targets, once identified, will be continually attacked until destroyed (absolute patience and dedication)
- Convergence
 - Will terrorists converge with Hackers ala Hactivism?
 - Can capability be acquired?

Likely Aspects of Cyberterrorism

- **In Parallel with a Physical or WMD Attack**
- **To Decrease Confidence in Critical Infrastructures/ Psychological operations**
- **To Cause Physical Damage and/or Loss of Human Life (most attractive/least probable)**
- **Nation state as sponsor or using as a tool of strategic influence (don't over-generalize your adversaries!)**

Point Scoring: Rating-the-Hacker

Toby Miller

toby_miller@adelphia.net

Point Scoring: Why?

- No “standard” system to help rate the attacker
- No system to help with the threat level
- Help management in the decision making process

Point Scoring: The Categories

- Passive Fingerprinting
- Intelligence
- The Attack
- The Exploit
- Backdoors | Cover up
- Other

Point Scoring: Past, Present, Future

- Originally posted on incidents.org
- Currently on rev2
- Soon to release rev 3
- www.ratingthehacker.net

Tool characterizations,
Disclosure Patterns and
Technique scoring.

Tom Parker – Pentest Limited (UK)

The Hacker Pie

- Representative of characterization metrics which build the final characterization.
- Available elements dependant upon scenario.
- Does not rely solely upon IDS/attack signature data.

Point Scoring Systems (Continued)

- Attempt to characterize an adversary based on attack information captured from the wild.
- Attempt to characterize adversary based upon “technique classification model”
- Attempt to characterize adversary based upon “tool classification model”

Tool classification model

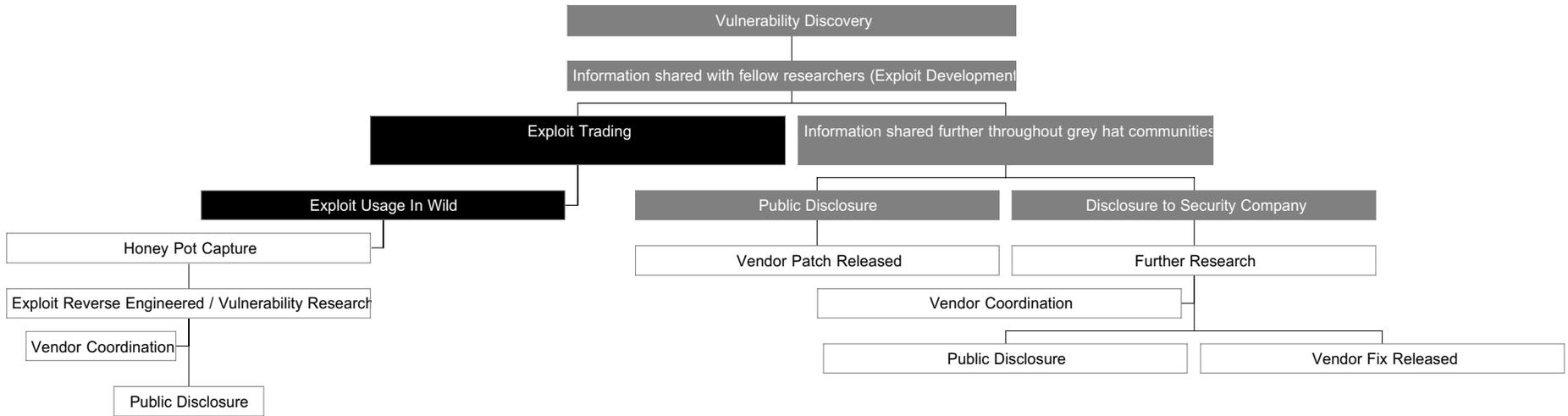
- Availability of application
- Origins of application
- Ease of use
 - Requires in-depth knowledge of vulnerability to execute?
 - Other mitigating factors

Disclosure Food Chain Characterization

- All tools have a story
- Often years before dissemination into public domain.
- Social demeanour often key to placing in disclosure disclosure chain.
- “Pyramid” metric.

The Disclosure “Food Chain”

Exploit Development



Marcus Sachs

National Cyber Security Division
US Department of Homeland
Security

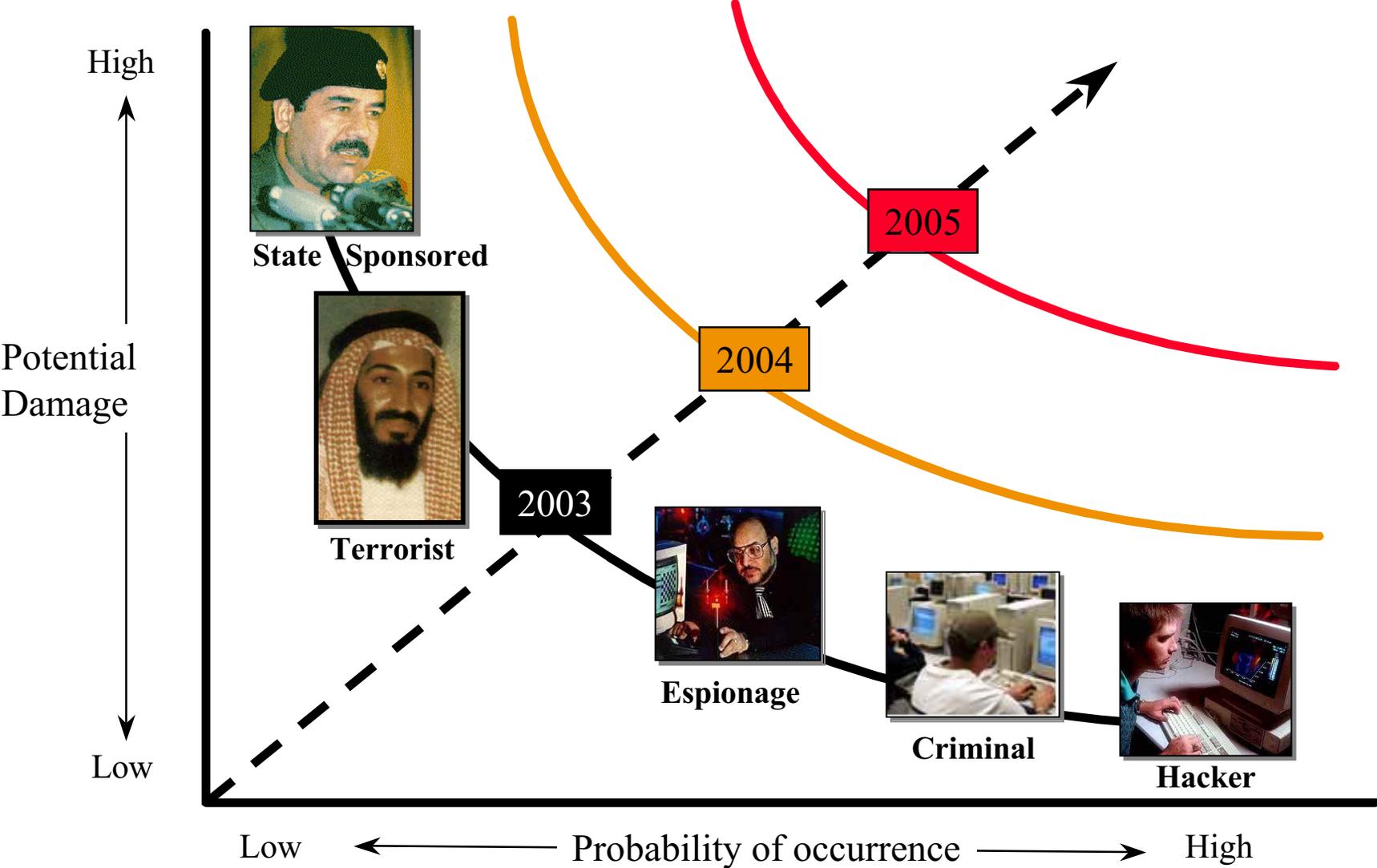
The Cyber Threat to the United States

- US national information networks have become more vulnerable—and therefore more attractive as a target
- Growing connectivity among secure and insecure networks creates new opportunities for unauthorized intrusions into sensitive or proprietary computer systems
- The complexity of computer networks is growing faster than the ability to understand and protect them
- The prospects for a cascade of failures across US infrastructures are largely unknown.

Cyber Threats to Critical Infrastructure

- Hacker/Script Kiddies/Hobbyist
- Disgruntled Employee
- Insider aiding others
- Hacktivist
- Industrial Espionage
- Foreign Espionage
- Terrorist
- State Sponsored Attack

The Threat is Increasing



Source: 1997 DSB Summer Study

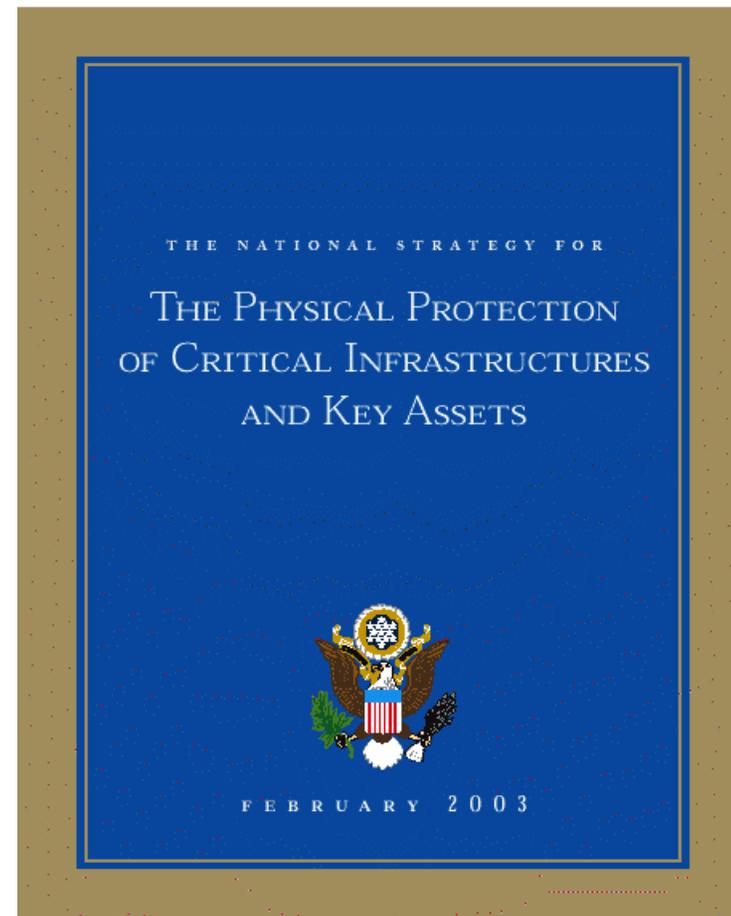
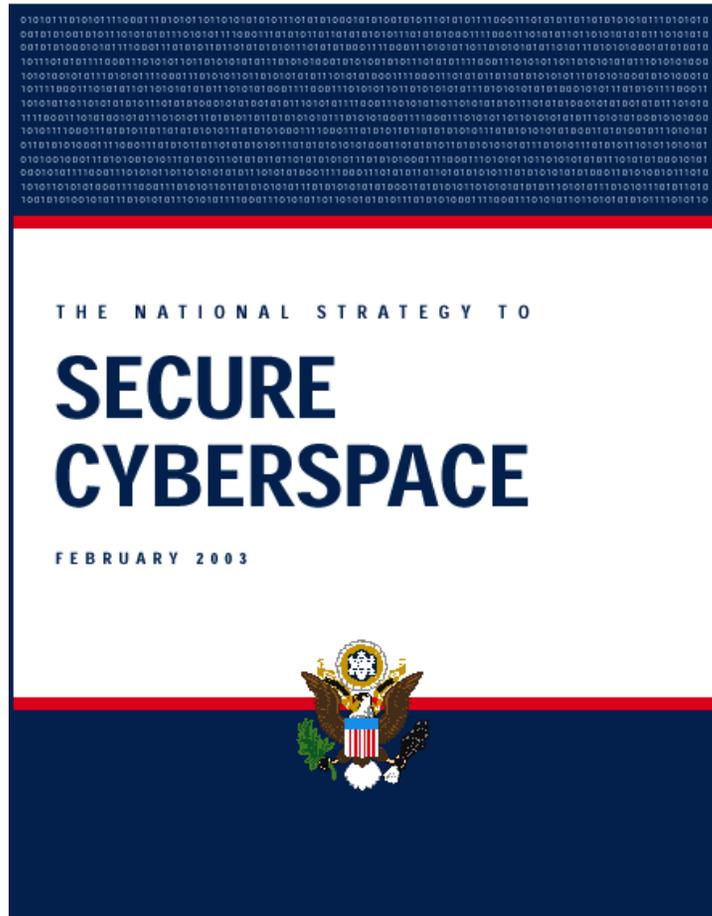
Why are we so Vulnerable?

- Internet was not built to be secure
- “Secure” (i.e., obscure) software being replaced by commercial products in infrastructures
- Software development focused on “Slick, Stable, Simple” (not “Secure”)
- System administrators lack training
- Leaders rarely see computer security as part of the “bottom line”
- User awareness is low

Why We're Concerned About Hackers

- **The real threat to Critical Infrastructure is not the hacker, but the structured state-sponsored organization**
- **However...**
 - **Sometimes it's hard to tell the difference - both use the same tools**
 - **Growing sophistication and availability of tools increases concern**
 - **We have to assume the worst until proven wrong**
- **So...**
 - **We take seriously all unauthorized activity**
 - **We will use all technical and law enforcement tools to respond ... and deter**
 - **We will seek legal prosecution where appropriate**

New Homeland Security Strategies



<http://www.whitehouse.gov/homeland/>

National Strategy to Secure Cyberspace

- Nation fully dependent on cyberspace
- *Range of threats: script kiddies to nation states*
- *Fix vulnerabilities, don't orient on threats*
- New vulnerabilities require constant vigilance
- Individual vs. national risk management
- Government alone cannot secure cyberspace

Priority II

A National Cyberspace Security Threat and Vulnerability Reduction Program

- Enhance law enforcement's capabilities for preemption, prevention, and prosecution
- Secure the mechanisms of the Internet including improving protocols and routing
- Foster trusted digital control systems/ supervisory control and data acquisition systems
- Reduce and remediate software vulnerabilities
- Improve physical security of cyber and telecommunications systems

Questions?

- Contact:

tom.parker@pentest.co.uk

marcus.sachs@dhs.gov

toby_miller@adelphia.net

devost@terrorism.com