BlackHat Federal 2006 The Era of a Zero-Day Nation State

Characterising the threats to our nations information systems

Tom Parker <tom at rooted dot net>

Matt Devost <devost at terrorism dot com>

‘Who’ before ‘How’

- Introduction to Cyber A/C Theory
- Threat Vector Analysis
- Attack Capability Analysis
- Attack Motivation Analysis

Background

- RAND 1999-2000
- Private research
- Various workshops
- Auditing the Hacker Mind (Syngress/2004)
  - Parker, Devost, Sachs, Shaw, Stroz

Outlining the need

- Improved threat profiling capabilities
- Informed business decisions
  - Budgetary considerations
    - New firewall, or new application proxy?
  - Targeted penetration tests
  - More realistic red team & I/R exercises
- Improved attribution capabilities
- Improved event correlation
- Changing the way people ‘think’ about the cyber threat

Postulative Characterizations

- Why postulative / theoretical?
- Objectives of theoretical characterizations
- Applications
- Dissection of the Adversary Model

Key Objectives

- To make determinations of probable:
  - Adversarial motivations
  - Adversarial capabilities

Example Applications

- Theoretical Characterizations of:
  - Adversary to given information system
  - Adversary to given origination
  - Adversary to given country

Dissection of adversary model

- Components
  - Model ‘Properties’
  - Model Property ‘Objects’

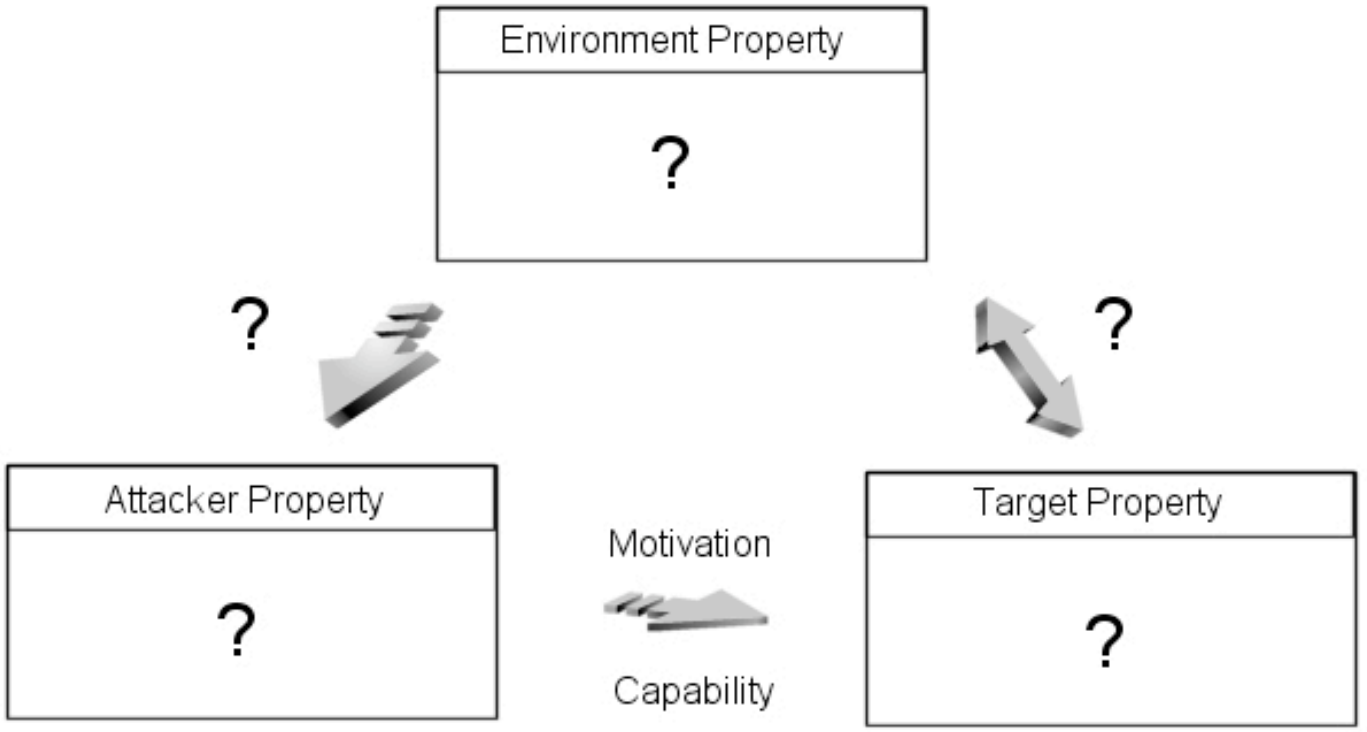
Model Operators

Type	Op	Meaning
Operator	/	Given
Operator	:	Relative to
Abbreviation	I	Impact
Abbreviation	S	Success
Abbreviation	p	Probability
Abbreviation	d	Detection
Abbreviation	A	Attempt
Abbreviation	P	Attack Parameters
Abbreviation	U	Uncertainty
Abbreviation	C	Consequence(s)

Adversary model (continued)

- Model constitution:
  - Environment property
  - Attacker property
  - Asset property
- Three observable property relationships / interactions

Adversary model outlined



Adversary model (continued)

- Environment Property
  - Can impact on multiple / groups of adversaries
- Attacker Property
  - Specific to individual adversaries

Environment Property

- World Events
- Political and cultural Environment
  - Significant events
    - EP-3E Spy Plane case study
    - Resultant China / US ‘hacker war’
  - Patriotism
  - Cultural: ‘Right’ to hack
  - Safety behind the monitor

Associations

- Intelligence Sources
- Technological Resources
- Financial Resources
- Others..

Activity Groups in Environment

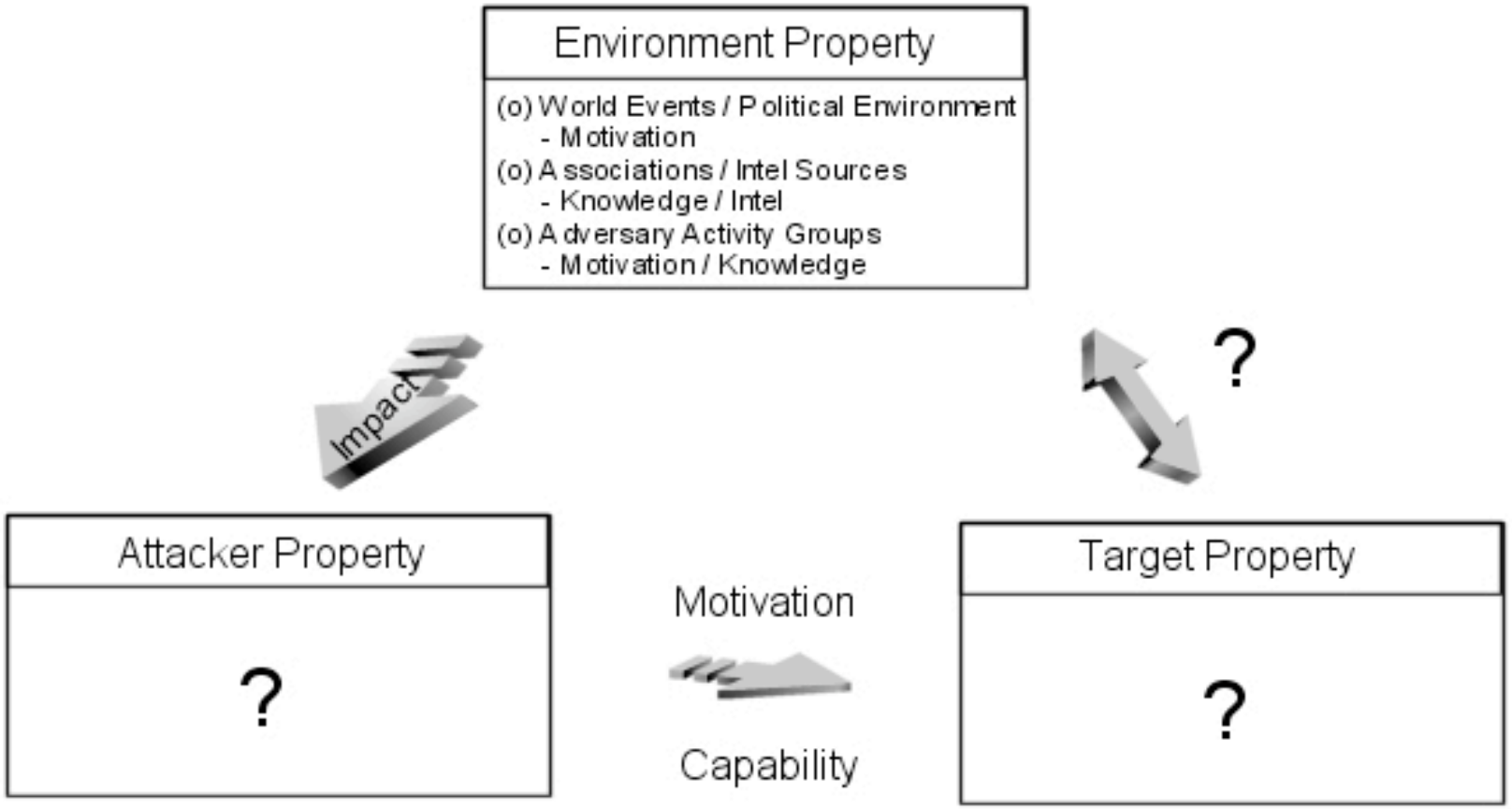
- Also called ‘Hacktavist’ groups
- Such groups primarily impact on attack motivators:
  - Need to impress peers
  - Increased level of self-confidence

Group Impacts

- **Attack objective**
  - May be that of the group, as opposed to the individual
- **Knowledge/skills**
  - Increased knowledge base
- **Finance**
  - If required, may be impacted upon

Group Impacts

- **Time**
  - Exponentially increased
- **Initial access**
  - Initial level of access may be elevated
- **Attitude to attributes of attack**
  - ‘Shared’ risk


Environment Property
(o) World Events / Political Environment
- Motivation
(o) Associations / Intel Sources
- Knowledge / Intel
(o) Adversary Activity Groups
- Motivation / Knowledge
Impact
?
Attacker Property
?
Motivation
Capability
Target Property
?

Attacker Property

- Resources Object
  - Attacker resources for given attack
- Inhibitor Object
  - Attitude to attack
- Driver / Motivator Object

Resources Object

- Time
- Skills
- Finance / Other
- Initial access

Attack Inhibitors

- Payoff/Impact Given Success (I/S)
- Perceived Probability of Success Given an Attempt (p(S)/A)
- Perceived Probability of Detection Given an Attempt (p(d)/A)
- Perceived Probability of Attribution (of Adversary) Given Detection (p(A)/d)
- Perceived Consequences to Adversary Given Detection and Attribution (C/(d)
- Adversary Uncertainty Given the Attack Parameters (U/{P})

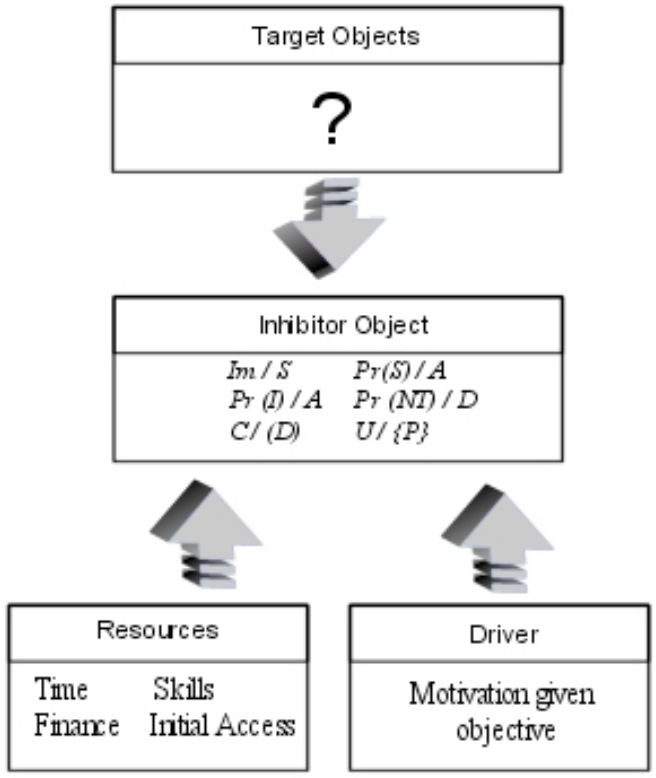
Attack Drivers

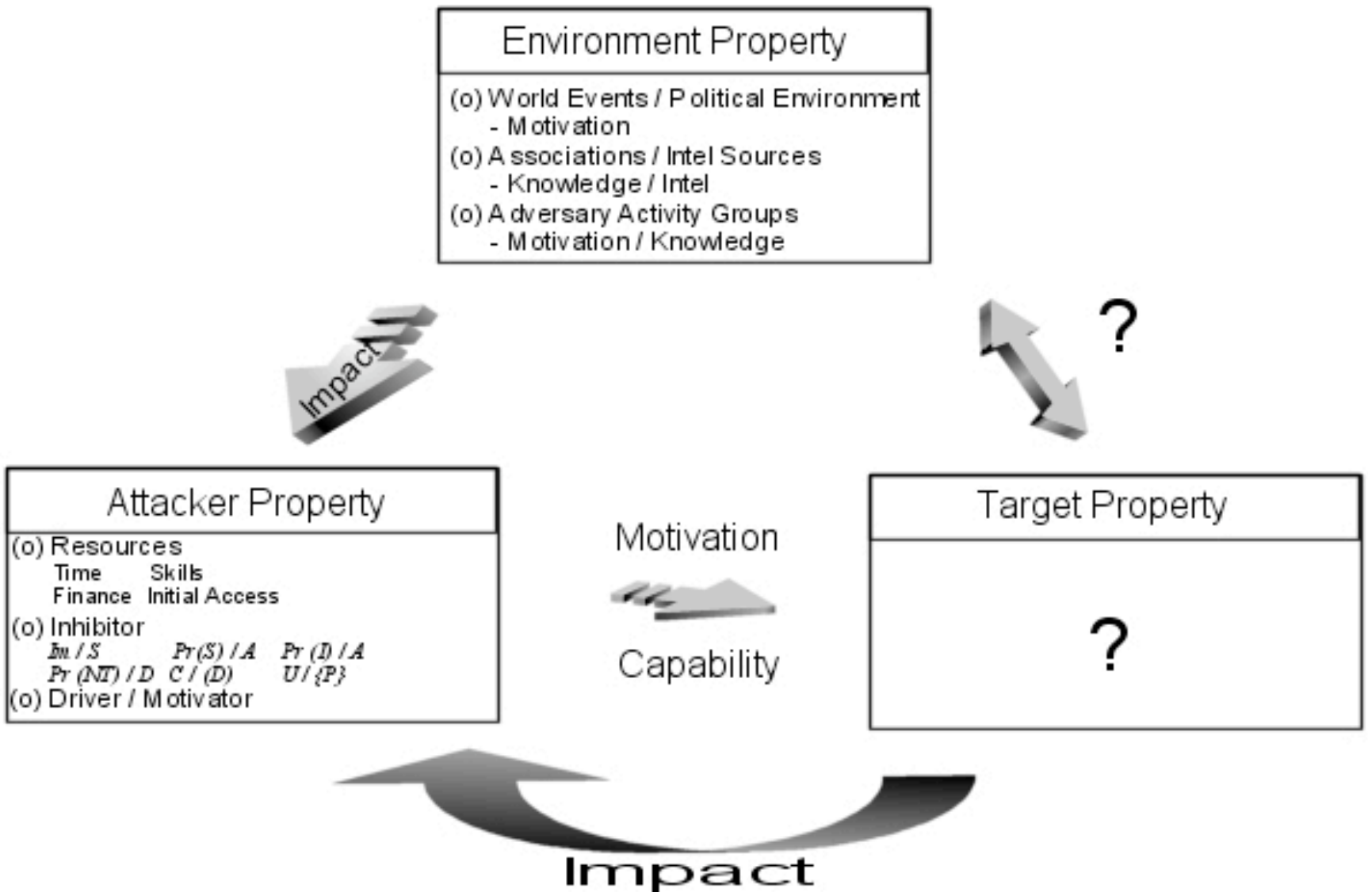
- Payoff/Impact Given Success (I/S)
- Perceived Probability of Success Given an Attempt (p(S)/A)
- Perceived consequences of failure

Inhibitor Offsetting

- Resources may be ‘spent’ to counter adverse conditions; such as:
- Adverse probability of detection
- Adverse probability of attribution
- Adverse probability of success

Inhibitor / Resource Offsetting

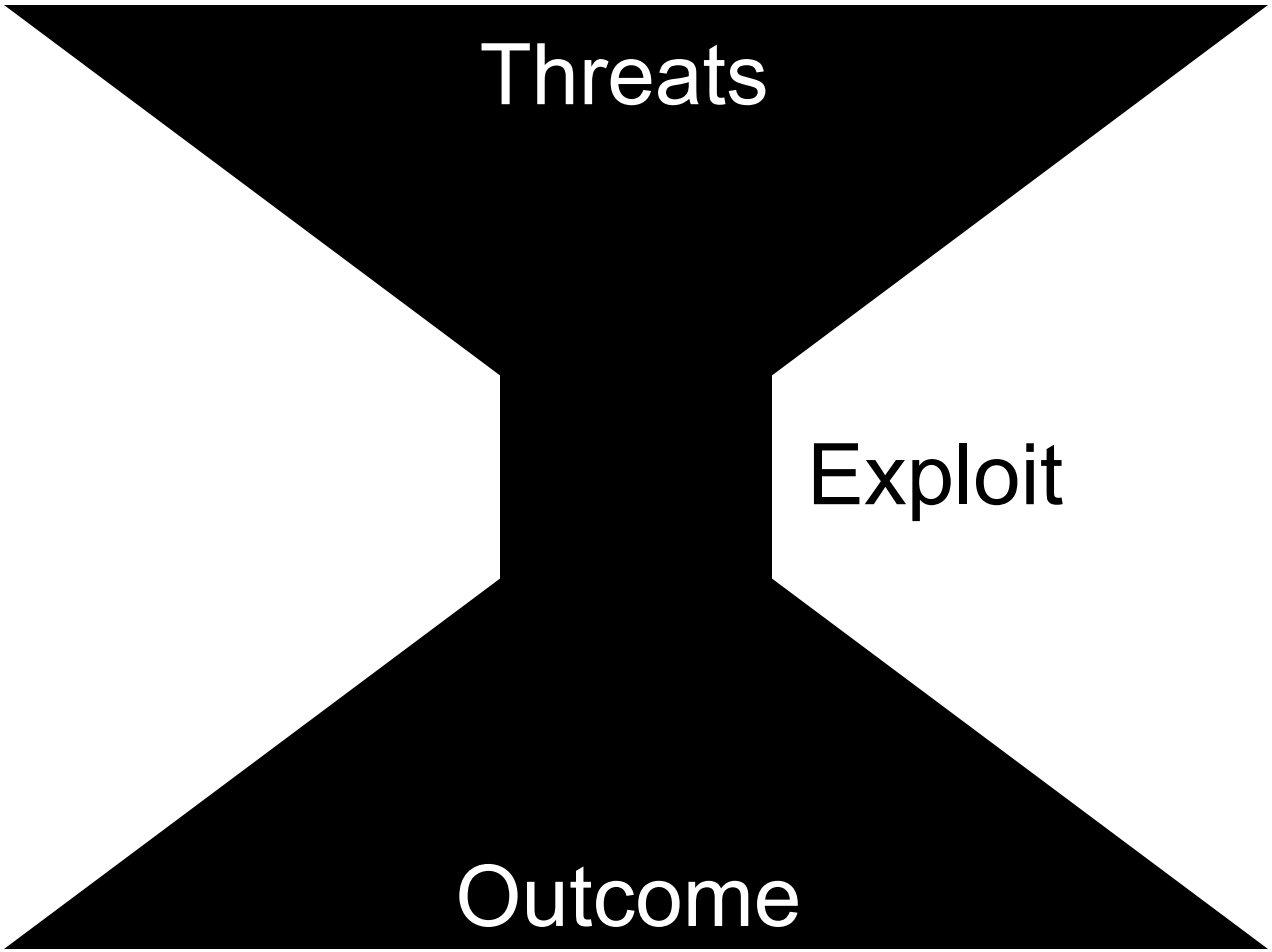



Environment Property
(o) World Events / Political Environment
- Motivation
(o) Associations / Intel Sources
- Knowledge / Intel
(o) Adversary Activity Groups
- Motivation / Knowledge
Impact
?
Attacker Property
(o) Resources
Time
Skills
Finance
Initial Access
(o) Inhibitor
Im / S
Pr (S) / A
Pr (I) / A
Pr (NI) / D
C / (D)
U / {P}
(o) Driver / Motivator
Motivation
Capability
Target Property
?
Impact

Nation State IW

Attack Capability Analysis

Threat Vector Analysis



Attack Capability Analysis

- ‘Natural’ Nation State Resources
  - Finance
  - SIGINT Capabilities (exploit and mapping)
  - Other pre-existing intel capabilities
- Nation States
  - N.Korea / China (for example)

Attack Motivation Analysis

- Nation State Coercion
  - Voluntary
    - Inspire attacks via nationalism
    - Turn a blind eye towards activity
    - Refuse to cooperate with international investigations
  - Mandatory
    - Issue “orders” to attack

Threat Spectrum

- So how urgent is the threat?
  - Terrorist broadcasting of intentions
    - “In a matter of time you will see attacks on the stock market/I would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies.” - Sheikh Omar Bakri Muhammad
  - Cultural conceptions in time
    - Acknowledgement of the potential capability does not mean an attack will occur in the near-term

Resource Acquisition

- Citizen participation / coercion
- Organized crime/state/terrorist convergence
- IW to support secondary attacks
  - To increase or augment impact
  - To raise money for kinetic attacks (e.g. selling secrets instead of cigarettes)

Nation State IW

What might such an attack ‘look like’

Augmenting the kinetic attack

- Increase or augment the impact of physical attack
- Attack supporting infrastructures (telecom, medical, transportation, power, etc.)
- Attack complimentary infrastructures (finance, national airspace systems)

A human element

- Adversary is not a 1 or a 0
  - Moving beyond the technical is the key challenge to adversary characterization
- “Insider placement” versus traditional “Insider” attacks
- Casing as a predictor

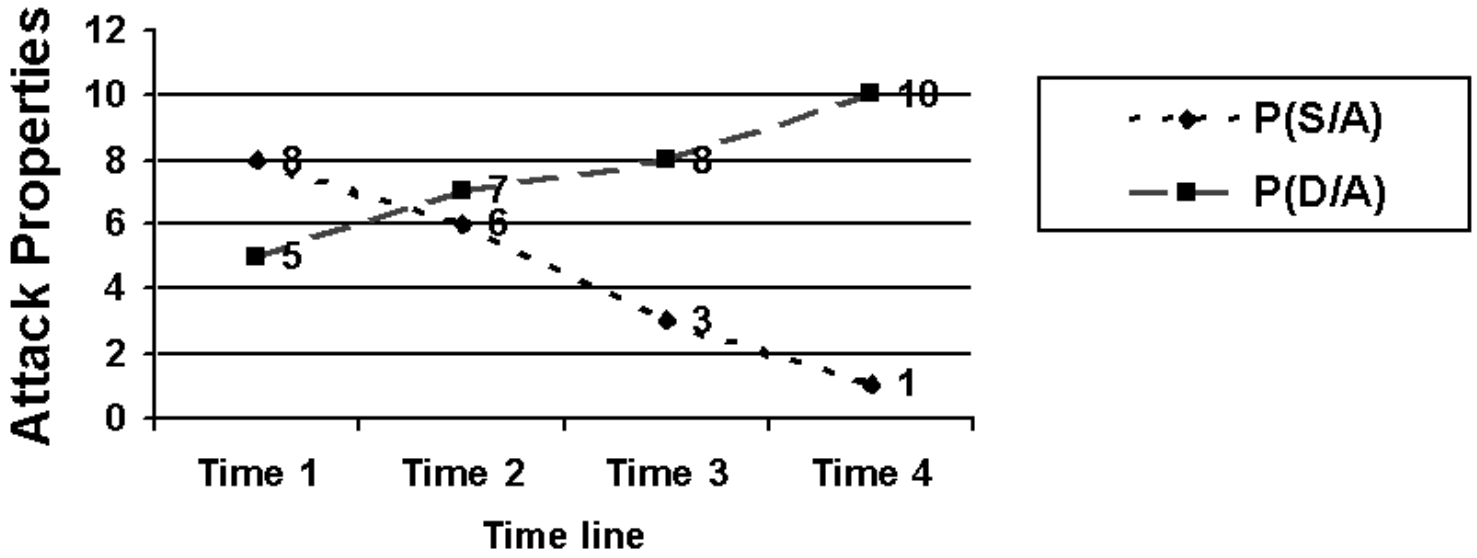
Early attack reconnaissance

- Reconnaissance may take several years
  - Signal to noise ratio
  - “Insider placement” as an indicator
- Need to be aware of potential for capability testing (anomalies in attack events)

Nation State I/W == 0day Attacks?

- Not necessarily
  - Low hanging fruit remain (SCADA?)
  - Resource Expenditure
  - Risk of engagement
  - However..

Disclosure impacts on inhibitors



Robust munitions / payloads

- Platform version interoperability
- Exploitation API's/Frameworks
  - CANVAS / METASPLOIT
- Precision / objective based payloads
  - Subtle data manipulation / flow control manipulation
  - Payload frameworks (MOSDEF)

Rootkit Technologies

- Advanced OS/Security Technology Subversion
  - Firewall technologies
  - Trusted computing technologies
  - Non-OS rootkits?
    - Network card firmware
    - BIOS
- Highly customized based on:
  - Target properties
  - Objective

Data exfiltration / comms

- Data egress technologies
  - Dremel worm
    - DNS Egress
- Stego
  - Publicly available
  - Growing interest in similar, but priorpetory (and harder to detect) technologies (which requires a capability!)
    - Deductions regarding those using traditional stego

Nation State IW

Detection and Remediation

Being Prepared

- Adversary Anticipation
  - Use of aforementioned characterization methods
  - Don’t get tricked into “blame bin Laden” mindset
  - Potential adversaries run the full spectrum of threats.

Impact Reduction

- Need holistic approach to risk management
- This requires:
  - More granularity of threat component
  - More granularity of capabilities (including zero day potentials)
  - Insight into potential impacts and safeguards

Information Warfare R&R

- IW Response and Reconstitution
  - Anomaly detection / early detection
  - Intel fusion with real world events
  - Pre-incident planning
  - Disaster recovery planning

Nation State IW

IW of the future?

Exploitation Technologies

- More advanced
  - Less accessible to Joe-public
    - In-house development
    - Increased coercion with pre-existing organized crime technology acquisition channels
  - Growth of established IW-capability industry
    - Increasing value placed in IW capabilities
    - W32 Remote: 2003 - $25,000; 2005 - $50,000
    - 2010?

Nation States

- China, N. Korea, Russia
  - Unrestricted Warfare
  - Titan Rain
  - Moonlight Maze

Terrorist Exploitation

- International terrorist groups
  - New venture, not a diversion of trusted tactics
  - Augment physical attacks
  - Spearhead economic attacks
- Displaced terrorist groups
  - Attract attention to a cause
  - Political bargaining

Terrorism / Organized Crime Convergence

- Tri-border region
  - Major convergence
    - Organized crime, terrorists, nations?
- Aum Shinrikyo
  - Engaged in both criminal and terrorist activity
  - Active software development capability
- Street gangs / Terrorists
  - Potential insiders?

Summing up

- Those with the capability, lack the intent
- Those with the intent, lack the capability

- Everything is subject to change…

Questions?