Stranger in a Changed Land

International Conference on Cyber Warfare and Security
March 2022
The Long and Winding Road....

Cyber Security

Information Assurance

Information Security

Defensive Information Operations

Computer Network Defense

Software Assurance

Computer Security

Software Security

System Security

Communications Security

Universal Assurance?

What’s Next???

COSMIC Security??

Surety

Safety Engineering
Seismic Shifts

• Communications Security → “Cyber”

• Mathematics → CS, Networking, Analytics

• Technology → Information, Operations

• Government monopoly → user/market driven

• “Control Model” of security → open market

• National Security → economic/social Risk
A few lessons

• Knowing about flaws doesn’t get them fixed

• In Cyberspace, we all have more in common than different

• The Bad Guy doesn’t perform magic
  • and most attacks are repeats of a pattern

• There’s a large but limited number of defensive choices
  • and the 80/20 rule applies (The Pareto Principle)

• Cyber Defense is really Information Management
  • and when you see “share”, replace with “translate” and “execute”

• Cybersecurity is not an event, a tool, or training – it’s a machine
  • fueled by information
  • the optimal place to solve a security problem is .... *not* where you found it
The National Security Agency (NSA)

Never Say Anything?  Not Seen Anywhere?  Needs Scant Attention?

• Signals Intelligence (SIGINT)
• Cybersecurity (from COMSEC, INFOSEC, Information Assurance...)

Offense + Defense = ???
The National Security Agency (NSA)

Defense wins games,
Offense wins budgets!

- Resources
- Culture
- Recognition
- Leadership Attention
Offense + Defense =?

• Cross-training
• Access to resources (financial, technology, think-tanks...)
• Linkage to the ecosystem (Industry, Policy-Makers, Academia)
• World-wide insight
• Embedded in a highly complex infrastructure
A Cyberdefense OODA Loop

(“Patch Tuesday”)

**OBSERVE**
Track security bulletins, advisories

**ORIENT**
Assess applicability, operational issues, risk

**DECIDE**
Prioritize remediation

**ACT**
Rollout, Monitor, Manage “breakage”

**ACT**
Deploy

**DECREASE**
Weaponize
“Dueling OODAs”
(and the role of Threat Intelligence, Analytics)

• There are many loops, often connected
• “farther in space, earlier in time”
• The Bad Guy’s loop is an opportunity
How Much Should I Care?

Weakness

Flaw

Vulnerability

Exploit

Attack
<table>
<thead>
<tr>
<th>WHAT YOU SHOULD KNOW</th>
<th>WHAT DOES IT MEAN?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone in organized crime (or espionage) who is not in this (cyber) ought to be</td>
<td>The Bad Guys are highly motivated</td>
</tr>
<tr>
<td>sued for malpractice</td>
<td></td>
</tr>
<tr>
<td>Almost all attacks are repeats of a type or class; Bad Guys do not perform</td>
<td>Build a foundation before taking a “moonshot”; understand the types, classes, patterns of attackers</td>
</tr>
<tr>
<td>magic</td>
<td></td>
</tr>
<tr>
<td>Just pointing out problems doesn’t get them fixed</td>
<td>Solutions are part of a complex system of feedback, incentives, and verification</td>
</tr>
<tr>
<td>It’s hard to have a unique problem or an original thought</td>
<td>Point to existing standards, ideas, frameworks</td>
</tr>
<tr>
<td>No security snapshot will work; trust is dynamic</td>
<td>Encourage machinery, not reports; measurement, not a state (of security); good IT and Ops management</td>
</tr>
<tr>
<td>Threat Sharing is over-rated</td>
<td>Focus on translation, action, efficiency, info management</td>
</tr>
<tr>
<td>Not every problem can be solved in the cyber domain</td>
<td>Diplomacy, economics, policy, social norms</td>
</tr>
<tr>
<td>Everyone’s role is changing (industry, government, academia, non-profits, standards)</td>
<td>Less control, more about behavior; less central and top-down, more cooperative</td>
</tr>
<tr>
<td>We need better components</td>
<td>Software quality, architectures, services</td>
</tr>
</tbody>
</table>
• Website:  www.cisecurity.org
• Email:  Controlsinfo@cisecurity.org
• Twitter:  @CISecurity
• Facebook:  Center for Internet Security
• LinkedIn:  Center for Internet Security

Tony Sager, Center for Internet Security
www.sagercyber.org