An analytical framework for cyber security
An analytical framework for cyber security

Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.
An analytical framework for cyber security

November 2011

DARPA
What we hear.
Goal

- Demonstrate asymmetric ease of exploitation of DoD computer versus efforts to defend.

Result

- Multiple remote compromises of fully security compliant and patched HBSS\(^\dagger\) computer within days:
  - 2 remote accesses.
  - 25+ local privilege escalations.
  - Undetected by host defenses.

Total Effort: 2 people, 3 days, $18K

HBSS Costs: Millions of dollars a year for software and licenses alone (not including man hours)

\(^\dagger\) = Host Based Security System (HBSS)
Users are the weak link...

Finweb = Jane123
DTS = 123Jane
PKI = JaneA123
DiskCrypt = Jane123A
Gmail = Jane123A
The supply chain is potentially compromised...

Approximately 3500 ICs.
- 200 unique chip types.
- 208 field programmable gate arrays (FPGAs).
- 64 FPGA and 9 ASIC types across 12 subsystems.

78% of FPGAs and 66% of ASICs manufactured in China and Taiwan.

Approved for Public Release, Distribution Unlimited.
Our physical systems are vulnerable to cyber attacks...

U.S. plans to issue official protest to China over attack on Google

by Ellen Nakashima

The United States will issue an official protest to the Chinese government over a major espionage attack targeting Google's computer systems and rights activists' email accounts that the search-engine giant said originated in China.

"We will be issuing a formal declaration" and seek an explanation, he said. The move may signal a shift for an administration that has been reluctant, according to China experts, to press sensitive issues such as human rights, lest it offend a country whose cooperation it seeks in other areas.

On Tuesday, in a rare disclosure by a major firm, Google announced that its "corporate infrastructure" had been hacked and Google, were affected.

Google also said it will no longer filter Internet searches on its Chinese search engine, Google.cn. Although it did not directly accuse China, the Silicon Valley technology giant threatened to pull out of the country if the government does not allow it to operate uncensored.

Chinese officials said that their laws ban hacking and that China's Internet is open.

A highly sophisticated and targeted "attack" on Google corporate infrastructure (known as Aurora)

Small group of academics took control of a car using Bluetooth and OnStar. They were able to disable the brakes, control the accelerator, and turn on the interior microphone.¹

False speedometer reading
Note that the car is in park...

We are doing a lot, but we are losing ground...
Federal Cyber Incidents and Defensive Cyber Spending fiscal years 2006 - 2010

[2] INPUT reports 2006 - 2010

Cyber Incidents Reported to US-CERT [1] by Federal agencies

Federal Defensive Cyber Spending [2] ($B)

0.0 2.0 4.0 6.0 8.0 10.0

2006 2007 2008 2009 2010
Why?
We are divergent with the threat...

* Public sources of malware averaged over 9,000 samples (collection of exploits, worms, botnets, viruses, DoS tools)
User patterns are exploitable...

A recent Defcon contest challenged participants to crack 53,000 passwords. In 48 hours, the winning team had 38,000.

Profile for the winning team, Team Hashcat
October 2010 vulnerability watchlist

<table>
<thead>
<tr>
<th>Vulnerability Title</th>
<th>Fix Avail?</th>
<th>Date Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Privilege Escalation Vulnerability</td>
<td>No</td>
<td>8/25/2010</td>
</tr>
<tr>
<td>Denial of Service Vulnerability</td>
<td>Yes</td>
<td>8/24/2010</td>
</tr>
<tr>
<td>Buffer Overflow Vulnerability</td>
<td>No</td>
<td>8/20/2010</td>
</tr>
<tr>
<td>Sanitization Bypass Weakness</td>
<td>No</td>
<td>8/18/2010</td>
</tr>
<tr>
<td>Security Bypass Vulnerability</td>
<td>No</td>
<td>8/17/2010</td>
</tr>
<tr>
<td>Multiple Security Vulnerabilities</td>
<td>Yes</td>
<td>8/16/2010</td>
</tr>
<tr>
<td>Remote Code Execution Vulnerability</td>
<td>No</td>
<td>8/16/2010</td>
</tr>
<tr>
<td>Use-After-Free Memory Corruption Vulnerability</td>
<td>No</td>
<td>8/12/2010</td>
</tr>
<tr>
<td>Remote Code Execution Vulnerability</td>
<td>No</td>
<td>8/10/2010</td>
</tr>
<tr>
<td>Multiple Buffer Overflow Vulnerabilities</td>
<td>No</td>
<td>8/10/2010</td>
</tr>
<tr>
<td>Stack Buffer Overflow Vulnerability</td>
<td>Yes</td>
<td>8/09/2010</td>
</tr>
<tr>
<td>Security-Bypass Vulnerability</td>
<td>No</td>
<td>8/06/2010</td>
</tr>
<tr>
<td>Multiple Security Vulnerabilities</td>
<td>No</td>
<td>8/05/2010</td>
</tr>
<tr>
<td>Buffer Overflow Vulnerability</td>
<td>No</td>
<td>7/29/2010</td>
</tr>
<tr>
<td>Remote Privilege Escalation Vulnerability</td>
<td>No</td>
<td>7/28/2010</td>
</tr>
<tr>
<td>Cross Site Request Forgery Vulnerability</td>
<td>No</td>
<td>7/26/2010</td>
</tr>
<tr>
<td>Multiple Denial Of Service Vulnerabilities</td>
<td>No</td>
<td>7/22/2010</td>
</tr>
</tbody>
</table>

6 of the vulnerabilities are in security software.

Color Code Key:
- **Vendor Replied – Fix in development**
- **Awaiting Vendor Reply/Confirmation**
- **Awaiting CC/S/A use validation**

Approved for Public Release, Distribution Unlimited
These layers increase the attack surface...

Constant surface area available to attack

Regardless of the application size, the system loads the same number of support functions.

DLLs: run-time environment = more commonality

For every 1,000 lines of code, 1 to 5 bugs are introduced.

Application specific functions
We amplify the effect by mandating uniform architectures.
The US approach to cyber security is dominated by a strategy that layers security on to a uniform architecture.

We do this to create tactical breathing space, but it is not convergent with an evolving threat.
Technology is not the only culprit... nor the only answer.
There are multiple choices for addressing the supply chain vulnerability:

- Resort to manufacturing all chips in trusted foundries. This is not feasible or sustainable.
- Screen all chips in systems critical to National Security or our economic base. Despite recent advances in screening technology, this is not feasible, affordable, or sustainable at the scales required.

Economics matter…

<table>
<thead>
<tr>
<th>Process</th>
<th>Trusted Design and Untrusted FAB</th>
<th>Untrusted Design ASIC</th>
<th>Untrusted Design FPGA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Phase 1</td>
<td>Phase 2</td>
<td>Phase 3</td>
</tr>
<tr>
<td>$P_D$</td>
<td>90.0%</td>
<td>99.0%</td>
<td>99.9%</td>
</tr>
<tr>
<td>$P_{FA}$</td>
<td>$10^{-3}$</td>
<td>$10^{-5}$</td>
<td>$10^{-7}$</td>
</tr>
<tr>
<td># of Transistors Evaluated</td>
<td>$10^5$</td>
<td>$10^6$</td>
<td>$10^7$</td>
</tr>
<tr>
<td>Time to Evaluate*</td>
<td>480 H</td>
<td>240 H</td>
<td>120 H</td>
</tr>
</tbody>
</table>

Selective screening coupled with diplomatic sanctions may create new solutions that are both feasible and sustainable.

- 3,500 IC’s on the F-35
- Single FPGA = 400 million transistors
- Modern chips = 2.5 billion transistors
Business incentives matter...

Understanding them in the context of ‘game theory’ reveals the problem.

Bot Herder strategy example:

<table>
<thead>
<tr>
<th>Bot Herder Cost</th>
<th>Bot Herder Return</th>
<th>Antivirus Cost</th>
<th>Antivirus Return</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short</td>
<td>Long</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(High)</td>
<td>(High)</td>
</tr>
<tr>
<td>Small</td>
<td>High</td>
<td>0</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Low)</td>
</tr>
</tbody>
</table>

The security layering strategy and antitrust has created cross incentives that contribute to divergence.

‡ = “exclusive or” logical operation
* = Advanced Encryption Standard
Layering and uniformity have created unintended consequences... we are in need of new choices...

**Examples:**

<table>
<thead>
<tr>
<th>Belief</th>
<th>Approach</th>
<th>Example</th>
<th>Unintended consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense in depth</td>
<td>Uniform, layered network defense</td>
<td>Host Based Security System</td>
<td>Larger attack surface introduces more areas of exploitability for attackers...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Homogeneous targets that amplify effects...</td>
</tr>
<tr>
<td>Users are best line of defense</td>
<td>Operator hygiene</td>
<td>15 character password</td>
<td>Users take short cuts and become enemy assets...</td>
</tr>
<tr>
<td>The interplay of technology, policy, incentives will favor better security.</td>
<td>Antitrust law rulings, use of COTS</td>
<td>Competition and independence in security software and COTS</td>
<td>Cross incentives that undermine security</td>
</tr>
</tbody>
</table>

**We need new choices that create:**

Users as the best line of defense without impeding operations.
Layered defense without increasing surface area for attack.
Heterogeneous systems that are inherently manageable.
We missed it too...
..let’s fix it.