DEFENDING THE EXPOSED FLANK
DIGITAL SUPPLY CHAIN SECURITY
FIRST 2017
Hi
I’m Martin McKeay
I have been in security for almost two decades
I have the scars to prove it
ACME AMERICAN WROUGHT ANVILS

THEY RING LIKE A BELL. No anvil made, English or American, surpasses our Acme in shape, material or finish. It is solid forged of two pieces of best wrought iron, welded at waist; face is made of one piece of tool steel, electrically welded to the body and warranted not to come loose. Base has sufficient spread to insure stability and prevent tipping; has long perfectly shaped horn and heel; face is trued and shaped by a special machine so that there are no hollow or uneven places; edges are perfectly tempered and will not chip. Hardie holes are straight and true, so you will have no trouble on account of anvil tools sticking or not setting level.

WE HAVE THE EXCLUSIVE SALE OF THE ACME. We take the entire output of the factory that makes them, and get them so cheap we are enabled to sell them at a lower price than others pay for anvils not as good. We sell more anvils than any concern in the United States. We could not sell so many unless they were everything we claim for them.

ONLY 9 1/2 CENTS POUND.

You Save More Money

The low prices on hardware in our last catalogue are lower still in this book. Over 3,000 hardware items reduced.
I am the Sr. Editor of the State of the Internet/Security report.
Now, I work for Akamai
This isn’t a vendor pitch
Honest
I’m here to talk about the exposed flank
Digital Supply Chain Security
ACT 1

MEANING
PHYSICAL SUPPLY CHAIN
DIGITAL SUPPLY CHAIN
WHAT DO I MEAN?

- Supply chain in this perspective is the managing of the internal components of an organization.
- The security to ensure the integrity of the information technology systems.
- Addressing security at all points in the workflow so that attackers may not openly compromise systems.
- Attackers might have been focused on stealing trucks historically, now they’re after your code.
WHO ELSE IS TALKING ABOUT THIS?
EXAMPLE OF A DIGITAL PICTURE FRAME OR USB DRIVE

HOW DID MY WIDGET GET HERE?
Supply chain issues with regard to Information Technology began to show themselves early on.
OR WORSE...

POOR SECURITY IN CODE

```c
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);  // root  xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);      // root  vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);      // root  admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);  // admin admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);  // root  888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);  // root  xmhdipc
add_auth_entry("\x46\x47\x44\x43\x57\x4E\x56", 5);                  // root  default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root  juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);   // root  123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);      // root  54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support support
add_auth_entry("\x50\x4D\x4D\x56", ",", 4);                          // root  (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x55\x4D\x50\x46", 4); // admin password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);        // root  root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);    // root  12345
add_auth_entry("\x57\x51\x47\x50", ",", 3);                        // user  user
add_auth_entry("\x43\x46\x4F\x4B\x4C", ",", 3);                    // admin (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);        // root  pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", ",", 3);                    // admin (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3); // admin admin1234
```
The focus in supply chain security has historically been towards enhancing the physical security of the supply chain logistics.

- Lack of concentration on the information technology/security

- Greater move to decentralized information technology solutions with global scale

- Information technology and the supply chain
WHO CARES?

• Who is taking the time to work on the problem?

• Organization that on supply chain include:

  • World Customs Organization (WCO), Customs Trade Partnership against Terrorism (C-TPAT), Container Security Initiative (CSI) from the US Customs and Border Protection and the Global Security Initiative from DHS.

  • ISO/PAS 28000 “Specification for security management systems for the supply chain”
MAGINOT LINE

• There is a concerted effort to secure physical side of logistics.

• IT solutions as they relate to supply chain have typically lacked the same focus.

• So why should this be of concern?

• Well...
CASE IN POINT...

An Iranian Oil Tanker Hacked Its Own Tracking System To Avoid Detection

ADAM CLARK ESTES  31 OCTOBER 2013 3:30 PM
WHAT COULD GO WRONG?
Pirates hacked shipping company to steal info for efficient hijackings
WAR STORIES AND SUCH

ACT II
GLOBAL, LEGAL, COMPLEXITY, HUMAN...

CHALLENGES & COMPLICATIONS
As we have more and more products delivered to us faster and cheaper, the scale of operations has gone global.

What are some impacts of this move?

- Outsourced help desk
- Offshore development centres
- Partner networks
GEOPOLITICAL
LEGAL ISSUES

• Legal issues are now global ones as supply chain expands across the globe.

• How do laws affect the production supply chain?

• Is there a lack of enforcement of said laws?

• Are you even legally able to be operating in the country?

• Ignorance of the law is no defense.
ATM, FAVORITE OF NE’ER DO WELLS
In Hours, Thieves Took $45 Million in A.T.M. Scheme

By MARC SANTORA
Published: May 9, 2013

It was a brazen bank heist, but a 21st-century version in which the criminals never wore ski masks, threatened a teller or set foot in a vault.

In two precision operations that involved people in more than two dozen countries acting in close coordination and with surgical precision, thieves stole $45 million from thousands of A.T.M.'s in a matter of hours.

In New York City alone, the thieves responsible for A.T.M. withdrawals struck 2,904 machines over 10 hours starting on Feb. 19, withdrawing $2.4 million.

The operation included sophisticated computer experts operating in the shadowy world of Internet hacking, manipulating financial information with the stroke of a few keys, as well as common street criminals, who used that information to loot the automated teller machines.
WHAT WENT WRONG?

- Vulnerable financial institutions
- Credit card processor was breached on two occasions
- Withdrawal limits removed on prepaid debit cards
- Cashing teams: 36,000 transactions and withdrew about $40 million from machines in the various countries in about 10 hours
We have all read about the APT problems.

Concerted efforts to purloin Intellectual Property. (Source Code, Process, Secret Sauce)

Using tools like Perforce and Git (as examples) partners often want access to source code.

Too often they get this access as a “business decision” which is your organization’s secret sauce.
Security Advisories Relating to Symantec Products - Symantec Reporting Server Improper URL Handling Exposure
SYM09-008

April 28, 2009

Revision History
None

Risk Impact
Low

| Remote Access | No |
| Local Access | Yes |
| Authentication Required | No |
| Exploit available | No |

Overview
The login web page in some versions of Symantec Reporting Server contains a URL handling error which could potentially allow an attacker to launch a phishing attack.

Affected Products

<table>
<thead>
<tr>
<th>Product</th>
<th>Affected Version</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec AntiVirus</td>
<td>10.1 MR7 and earlier</td>
<td>Update to 10.1 MR8 or later</td>
</tr>
<tr>
<td>Corporate Edition</td>
<td>10.2 MR1 and earlier</td>
<td>Update to 10.2 MR2 or later</td>
</tr>
<tr>
<td>Symantec Client Security</td>
<td>3.1 MR7 and earlier</td>
<td>Update to 3.1 MR8 or later</td>
</tr>
<tr>
<td>Symantec Endpoint Protection</td>
<td>11.0 MR1 and earlier</td>
<td>Update to 11.0 MR2 or later</td>
</tr>
</tbody>
</table>

Unaffected Products

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
Bitly discloses account compromise, urges users to change passwords
PARTNER NETWORKS

• Many manufacturing companies build and maintain interconnected networks

• The “I have a firewall so I’m OK” mentality should be shelved.

• Do you check your third party connections?

• Trust But (Test and) Verify
Security researchers create undetectable hardware trojans

Method can be used to weaken hardware random number generators used for encryption

By Jaikumar Vijayan
September 17, 2013 04:15 PM ET  7 Comments

A team of security researchers from the U.S. and Europe has released a paper showing how integrated circuits used in computers, military equipment and other critical systems can be maliciously compromised during the manufacturing process through virtually undetectable changes at the transistor level.

As proof of the effectiveness of the approach, the paper describes how the researchers created a backdoor into a well-known random number generator used in Intel's processors.
MORE RECENTLY...
U.S. military may have 10 robots per soldier by 2023

Military expects to soon be using autonomous robots to carry soldiers' gear and scan for enemy combatants

By Sharon Gaudin
November 14, 2013 05:32 PM ET   4 Comments

Computerworld - American soldiers patrolling dangerous streets will soon be accompanied by autonomous robots programmed to scan the area with thermal imaging and send live images back to the command center.

Likewise, squads of infantrymen hiking through mountains will be helped by autonomous robots.
YIPES!
DOD officials say autonomous killing machines deserve a look

While military requires person in loop, robots might decide when to shoot in future.

by Sean Gallagher - Mar 4, 2016 7:14pm CET
A Google self-driving car has finally caused an accident

Updated by Timothy B. Lee on February 29, 2016, 6:20 p.m. ET  tim@ vox.com
WHERE TO FROM HERE?

ACT III
• Compliance regimes are to address the BARE MINIMUM
OFF SHORE DEVELOPMENT

• Greater diligence is required when signing a contract

• The lowest bid is not always the best choice

• Ensure that you’re development partner adheres to your security requirements

• Make sure that they do not have offices in restricted countries

• Software liability?
HAMSTER WHEEL OF PAIN

- How do we get off this wheel of security issues?
- We need to be able to reproduce good results
DEFINED REPEATABLE PROCESSES

• There needs to be a concentration on defined repeatable processes

• Too often companies treat third party connections as one offs. (not for all of course)

• Not having a defined onboarding process for partners can result in unintended consequences.
The hardest battle I have ever fought has been for budget.

You need to make a strong case that articulates the risks to the business in terms that the business can understand.

Avoid the fear, uncertainty and doubt if at all possible.
INTERNAL APPLICATIONS

• Conduct code reviews. Go beyond unit tests.
• Hire third party companies to review code.
• Keep documentation current
INFRASTRUCTURE, DNS & WEB APPLICATIONS

- You have limited resources
- Concentrate on the items that are important in your supply chain
- Have a trusted partner
BUILD TO FAIL

- As with any IT implementation failure will come
- Make your applications/infrastructure resilient
- Don’t build for five nines
- Build to fail
BAMBOO ANALOGY

• Supply chain has many points that can be exploited along the way

• It is important to have a supply chain that can adapt
Thank you for taking the time to listen to me!
Questions?

Thanks

Martin McKeay
@mckeay

mmcckeay@akamai.com