Transportation Cyber Security

Edward Fok
Federal Highway Administration – Resource Center
Operations Technical Service Team
What are we trying to protect

• Safe surface operation
• Efficient surface mobility
• Reliable and trusted information to the public
Why Surface Transportation?

• Hacker mentality: Naturally curious
• Hacker mentality = Mountain climber mentality
• Engineers build system to function
The Risk Curve

GROUP III
NATION STATES TERRORISTS

GROUP II
ORGANIZED CRIME HACKERS FOR HIRE INSIDERS COMPETITION

GROUP I
ANYONE

LIKELIHOOD

Smallest

Very

CONSEQUENCES

Largest

LESS

OPEN SOURCE COLLECTION / RECON
SYSTEM SCANNING / PROFILING
SYSTEM COMPROMISE
SYSTEM CONTROL
SPECIFIC ATTACK
TARGETED EXFILTRATION
DDoS
SOPHISTICATED INJECTION
SUPPLY CHAIN
CATASTROPHIC IMPACT
DEBILITATE RECOVERY
GET NAKED!
Welcome to myBART!

myBART sends out a free weekly email full of entertainment news, ticket giveaways and big discounts to events happening close to BART stations.

Become a myBART member to enter our contests for a chance to win some free tickets, or explore the site right now to see this week's discount offers and find something fun to do that you can ride BART to.

myBART. Providing weekly reasons to get off the couch.
“Sooner or later the people in this country gotta realize the government does not give a fuck about them. The government doesn’t care about you, or your children, or your rights, or your safety, it simply doesn’t give a fuck about you. It’s interested in its own power, that’s the only thing, keeping it and expanding it wherever possible.”

Dear Bay Area Rapid Transit, The People and All Government Agencies,

We are Anonymous, we are your citizens, we are the people, WE DO NOT TOLERATE EXPRESSION FROM ANY GOVERNMENT AGENCY.

BB&T has proved multiple times that they have no problem exploiting and abusing the people.

First they displayed this in the two recent killings by BART police. Under no circumstance, unless police are shot at, make police killings acceptable. Non-lethal weapons were available to use during both incidents, providing even if that was necessary, but instead they shot to kill. Next they violated the people’s right to assembly and prevented other bystanders from using emergency services by blocking cell phone signals in order to stop a protest against the BART police murders.

Lastly, they set up this website called mybart.gov and they added their numbers in with virtually no security.

The data was stored and easily obtainable via basic sql. Any 8 year old with an internet connection could have done what we did to find it. On top of that none of the info, including the passwords, was encrypted. In short, we have reduced the protection level to no protection, to the people.

The governments and government agencies of the world are becoming tyrannical and oppressive, and the people are responding and will not take your shit for much longer. The people will fight this oppression with protests, demonstrations, picketing, hacking, dudos, online attacks and by any other means.

We will not allow ourselves to be killed, employed, or get aquitted. From the streets of Chile, England, Portugal, San Francisco, Oakland, the people are rising up and we will support each other and stand in solidarity. Worldwide resistance is happening, we will participate in solidarity against oppression. SOLIDARITY IS OUR WEAPON.

Thus below we are releasing the User Info Database of MyBart.gov, to show that BART doesn’t give a shit about it’s customers and riders and that the people will not allow you to kill us and call us cowards. This is but the tip of the many services we will be releasing to any citizen that has his information published. We will not stop until you stop, provided you should go BART and shit then your info wasn’t secured with them. Also do not worry, probably the only information that will be shared from this database is that of BART employees.

Greet to TeamPoison, lulzsec, anti-sec, anarchists, anon, bay of rage. No Justice. No BART. WA in the bay, your soon name, anonymous irk.

World Wide Solidarity. “Join us to make 2011 the year of liaises and revolutions.”
Breaking: Two Explosions in the White House and Barack Obama is injured
INSTRUKCJA
Dla Kierujących
Pojazdami
Kombinacji Militarnej.
MPK Łódź
SP Z.O.O.

[Image of various keys, tools, and a manual on a wooden table]
SIRIT INTERNAL TRANSPONDER
P/N 9794480-0006
REV 2.0B

Antenna (RCV)
Battery
Demodulation circuit
TI MSP430
Buzzer
Antenna (XMIT)
Field Devices

• Attackers are not traffic engineers
• Examples:
  – “Smart” Parking Meter Implementation, Globalism, and You (2009)
  – How to hack a country’s transport network (2012)
Field Networks

• Wire Theft

• Wireless Systems
  – Leased
  – Owned (APCO P25, 4.9GHz)
Obama's Cellphone Account Breached by Verizon Employees
How do you hack into a tornado siren warning system and trigger the sirens from your home computer?

I'm totally just curious - I'm not planning on doing this.
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=2332, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=2951, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=2960, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=3983, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=3023, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=176, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=302, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=320, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=329, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=347, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=356, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=365, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=374, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=383, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=392, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=401, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=410, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=419, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=428, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=437, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=455, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Broadcast</td>
<td>IEEE Probe Request, SN=464, FN=0, Flags=............C, SSID=</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Sorry bro not tellin'**

...but there are default SSIDs :)
It exploits the following vulnerabilities in Microsoft Windows to spread copies of itself via networks and removable drives:

- MS08-067
- MS10-061
- MS10-046

It installs server and client components to vulnerable systems to execute certain backdoor functions to any client that it can connect to.

It connects to a remote server to test for internet connection and to send and receive commands from a remote malicious user.

It attempts to gain access to the back-end SQL database of WinCC SQL server using CVE-2010-2772 to allow an attacker to view project databases and information from vulnerable SCADA systems.
Humming along with technology, until it's not
Computer meltdown creates traffic-light chaos in Montgomery

By Ashley Halsey III
Washington Post Staff Writer
Thursday, November 5, 2009
A logic bomb allegedly planted by a former engineer at mortgage finance company Fannie Mae last fall would have decimated all 4,000 servers at the company, causing millions of dollars in damage and shutting down Fannie Mae for at least a week, prosecutors say.
These tables control torque limits acting on the motor over its speed range. The 100% Accel table controls maximum motoring, the 100% Brake table controls maximum generation, and the Creep table controls torques when "zero torque" is requested.

<table>
<thead>
<tr>
<th>RPM</th>
<th>0</th>
<th>300</th>
<th>600</th>
<th>900</th>
<th>1200</th>
<th>1500</th>
<th>1910</th>
<th>2100</th>
<th>2400</th>
<th>2700</th>
<th>3000</th>
<th>3300</th>
</tr>
</thead>
<tbody>
<tr>
<td>100% Accel Torque</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>191</td>
<td>173</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0kW</td>
<td>6kW</td>
<td>13kW</td>
<td>19kW</td>
<td>25kW</td>
<td>31kW</td>
<td>40kW</td>
<td>44kW</td>
<td>50kW</td>
<td>57kW</td>
<td>60kW</td>
<td>60kW</td>
</tr>
<tr>
<td>100% Brake Torque</td>
<td>-200</td>
<td>-200</td>
<td>-200</td>
<td>-200</td>
<td>-200</td>
<td>-200</td>
<td>-200</td>
<td>-200</td>
<td>-200</td>
<td>-191</td>
<td>-173</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
<td>-0kW</td>
</tr>
</tbody>
</table>

In situations where the motor speed goes over these speed limits, the system will reduce the motoring torque to prevent the motor from going faster.

| Speed Limit (RPM): | 3600 | -3600 |
| RPM Range for Torque Reduction: | 300 | 300 |

Torque Limiting over Range:
- Accelerator > Zero Torque
- Accelerator > Brake Torque

Hand Controller Settings

Note: Values in volts. Range: -0.5V - 5.5V

<table>
<thead>
<tr>
<th>Accelerator</th>
<th>Brake</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Error:</td>
<td>5.5</td>
</tr>
<tr>
<td>Maximum Allowed:</td>
<td>4.5</td>
</tr>
<tr>
<td>Minimum Allowed:</td>
<td>0.5</td>
</tr>
<tr>
<td>Minimum Error:</td>
<td>-0.1</td>
</tr>
</tbody>
</table>
The Risk Curve

GROUP III
NATION STATES
TERRORISTS

GROUP II
ORGANIZED CRIME
HACKERS FOR HIRE
INSIDERS
COMPETITION

GROUP I
ANYONE

OPEN SOURCE COLLECTION / RECON
SYSTEM SCANNING / PROFILING
SYSTEM COMPROMISE
SYSTEM CONTROL
SPECIFIC ATTACK
TARGETED EXFILTRATION
DDoS
SOPHISTICATED INJECTION
CATASTROPHIC IMPACT
SUPPLY CHAIN
DEBILITATE RECOVERY

LIKELIHOOD

LESS

VERY

CONSEQUENCES

SMALLEST

LARGEST
Where to Get HELP!

Multi-State Information Sharing & Analysis Center (MS-ISAC)
http://msisac.cisecurity.org

Computer Emergency Response Team (CERT)
• http://www.cert.org
• Document: Roadmap to Secure Control Systems in the Transportation Sector
• Very good source on Insider Threat and Prevention

Microsoft Technet

ISO/IEC 27000

Information Security Forum
“Standard of Good Practice”

Industrial Control System-CERT Self Assessment
http://ics-cert.us-cert.gov/Assessments

National Institute of Standards and Technology
http://csrc.nist.gov/index.html

SANS Institute
• http://www.sans.org
• http://ics.sans.org

National Vulnerability Database
http://nvd.nist.gov

AntiVirus
• http://av-comparatives.org/
• EICAR virus scanner tester