SCADA and ICS for Security Experts: How to Avoid Cyberdouchery

James Arlen, CISA
SECTOR - Toronto - 2010
Disclaimer

I am employed in the Infosec industry, but not authorized to speak on behalf of my employer or clients.

Everything I say can be blamed on a disturbance in the force.
Credentials

- 15+ years information security specialist
- staff operations, consultant, auditor, researcher
- utilities vertical (grid operations, generation, distribution)
- financial vertical (banks, trust companies, trading)
- some hacker related stuff like game show host, etc.

...still not an expert at anything.
Before you ask...

- This is a talk about talking about SCADA.
- There is some technical material, but not much.
- Yes, I’m going to talk about Smart Grid.
- Yes, I’m going to talk about Siemens and Stuxnet.
- No, I’m not going to make you an expert today either.
1/ Stop Sounding Stupid
Scada

got

sexy
Follow the money
Who's an expert now?
One time at security camp
Gotta get me a piece of that
Gotta get me a piece of that
2/ Big Things and Little Things
Not all 'scada' is SCADA
Big things: power grid
Big things:
pipeline
Inter-connected sensors and controls under central management
Interconnected sensors and controls under central management
Supervisory control and data acquisition
Little Things:
chemical plant, power plant, manufacturing facility
Little Things: chemical plant, power plant, manufacturing facility
Little Things: chemical plant, power plant, manufacturing facility
Little Things: chemical plant, power plant, manufacturing facility
Little Things: chemical plant, power plant, manufacturing facility
Little Things:
chemical plant, power plant, manufacturing facility
Lots of individual capabilities with some orchestration
Programmable logic controllers
Programmable logic controllers
Programmable logic controllers
Industrial control systems/
Distributed control systems
3/ Part of a Bigger Picture
So if you break the computer, you break everything
What happens when Edna falls into the reactant vessel?
This is the data
<table>
<thead>
<tr>
<th>Address</th>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0030</td>
<td>3577 c1c2 040c 0117 ffff 0000 0100 0301</td>
<td>Sw..............</td>
</tr>
<tr>
<td>0x0040</td>
<td>6400 a0d6 0000 6400 0000 0000 5b</td>
<td>d................</td>
</tr>
<tr>
<td>0x0000</td>
<td>4500 004d 60c5 4000 4006 5892 c0a8 0001</td>
<td>E...M.@@X.....</td>
</tr>
<tr>
<td>0x0010</td>
<td>c0a8 0002 d188 4e20 dfbe bdal b218 bc0a</td>
<td>......N...........</td>
</tr>
<tr>
<td>0x0020</td>
<td>5018 16d0 b63d 0000 056a 1cc4 0a00 0100</td>
<td>P.............d....</td>
</tr>
<tr>
<td>0x0030</td>
<td>5377 c1c2 040c 0100 0000 ffff 0100 0301</td>
<td>Sw..............</td>
</tr>
<tr>
<td>0x0040</td>
<td>6400 c7b0 0000 6400 0000 0000 5b</td>
<td>d..{d.............</td>
</tr>
</tbody>
</table>

This is the data
This is the process
This is the process
This is the process
I know you can grok the protocol, can you break the controls?
I know you can grok the protocol, can you break the controls?
Oh, you forgot about safety
Oh, you forgot about safety
Oh, you forgot about testing
Oh, you forgot about testing
Oh, you forgot about people
Oh, you forgot about people
What if it really is SCADA?
Stuff breaks
All the &*$ing time
And it gets fixed
And it gets fixed
And you never noticed
And you never noticed
And you never noticed
And you never noticed
But wait a second here...
WAIT!!!!
You haven’t talked about...
- the aurora demonstration
- the aurora demonstration
- smart grid
- the aurora demonstration
- smart grid
- STUXNET!!!!!!!
What about the Aurora Explosion Demo Awesome Video??????
Oh yeah, and BTW...

Smart meters aren’t SCADA
Stuxnet...
Stuxnet...

what a cybermess.
Stuxnet renews power grid security concerns

First known SCADA malware program to target control systems prompts new questions about security of U.S. power grid

By Jaikumar Vijayan
July 26, 2010 02:31 PM ET

Computerworld - Last week’s disclosure of a sophisticated malware program targeting control system software from Siemens AG has renewed long-standing concerns about whether the U.S power grid can withstand targeted cyberattacks.

The malware program, called Stuxnet, is designed to exploit a Windows Zero Day flaw to find and steal industrial data from Supervisory Control And Data Acquisition (SCADA) systems running Siemens’ Simatic WinCC or
And frankly, no one is looking good here...
Siemens marketing / legal dep’t takes it the furthest...
4/ Practical Positive Things
You can understand this stuff
You can help
They need you
You need to suck it up
It's time to learn before teaching
It's time to learn before teaching
5/ You Wouldn't Believe Me If I Told You
The Organization is against you
Your prima donna attitude is against you
Your age is against you
It's time to start hacking
First you hack the org
Then you own their asses
Then you own their asses
6/ Movies Would Have You Believe
How to Hack a Computer in an Action Movie
It's a mad mad graphical awesome world
It's a mad mad graphical awesome world
It's a mad mad graphical awesome world
It's a mad mad graphical awesome world
It's a mad mad graphical awesome world
It's a mad mad graphical awesome world
It's a mad mad graphical awesome world
What an afternoon at the console really feels like
What an afternoon at the console really feels like
What an afternoon at the console really feels like
7. The Media Hypes It As If...
There's a hacker behind the bush.
There's a hacker behind the bush
There's a hacker behind the bush.
There's a hacker behind the bush
There's a hacker behind the bush.

Last fall, when a Department of Homeland Security video depicted a turbine exploding in a hacker attack, viewers may have been at the end.
A 14yo in Mom's basement
A 14yo in Mom's basement
A 14yo in Mom's basement
L337 cadre of soldiers
L337 cadre of supersoldiers
L337 cadre of genetically engineered supersoldiers
8/ Bad Shit That Actually Happened
Not necessarily public news.
9/ What Could Have Saved It
Superheroes
Superheroes, Ninjas
Superheroes, Ninjas and Pirates
Following Instructions
Or, not sucking at implementation
Or, doing what you're told
Or, stuff that has nothing at all to do with computers
10/ What You Can Do - Little Picture
Learn
Stop listening to "experts"
Modest changes, massive results
11/ What You Can Do - Big Picture
Stop feeding the trolls
Avoid being ‘that person’
Press for sane acquisitions
Study past success
Study past success
Q & A

twitter: @myrcurial
james.arlen@pushthestack.com
Byron Sonne
- Canadian security researcher
- arrested in the lead up to the G20 summit in Toronto
- being held without bail - trial in 2 years
- please support him
Credits, Links and Notices

Me:
http://myrcurial.com  http://cyberdouchery.com
http://securosis.com  http://liquidmatrix.org/blog

Thanks:
All of you, My Family, Friends, Jeff Moss (for demanding this talk) Brian Bourne, and the rest of the SECTOR Team.


Inspiration:
twitter, fast music, caffeine, my lovely wife and hackerish children, blinky lights, shiny things, modafinil & altruism.

http://creativecommons.org/licenses/by-nc-sa/2.5/ca/