

SCADA/ICS Security in an Insecure Domain

RobertMichael.Lee@Gmail.com

Twitter: @RobertMLee

Introduction



CYA

“The opinions held and expressed by Robert M. Lee do not constitute or represent an opinion or position held by the United State’s government, Department of Defense, or US Air Force.”

What this Presentation is Not...

HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)



Source: [HTTP://IMGS.XKCD.COM/COMICS/STANDARDS.PNG](http://imgs.xkcd.com/comics/standards.png)

What this Presentation Is... (Takeaways)

- Education on “hackers”
- Understanding of a hacker’s methodology
- Education on some SCADA/ICS Threats
- Thinking like a hacker in your own research

What is a Hacker?

- The bad guy?
- A researcher?
- A subculture?
- A buzz term for the news media?

Hacker definition controversy



This section **needs additional citations for verification**. Please help [improve this article](#) by adding citations to reliable sources.

Currently, "*hacker*" is used in two main conflicting ways

1. as someone who is able to subvert computer security, if doing so for malicious purposes it can also be called a *cracker*.
2. a member of the [Unix](#) or the [free and open source software](#) programming subcultures or one who uses such a style of software or hardware development.

Hacker Origins

- MIT 1960's – Made computers work in ways they weren't designed; a positive term
- John Draper “phreaked” phones for free long-distance calls in the 1970's
- Kernel Memory corruption exploit by US Air Force member James P. Anderson - 1972
- Chaos Computer Club, Germany – 1980's
- William Gibson termed the term “cyberspace” in the science fiction novel *Neuromancer* in 1984

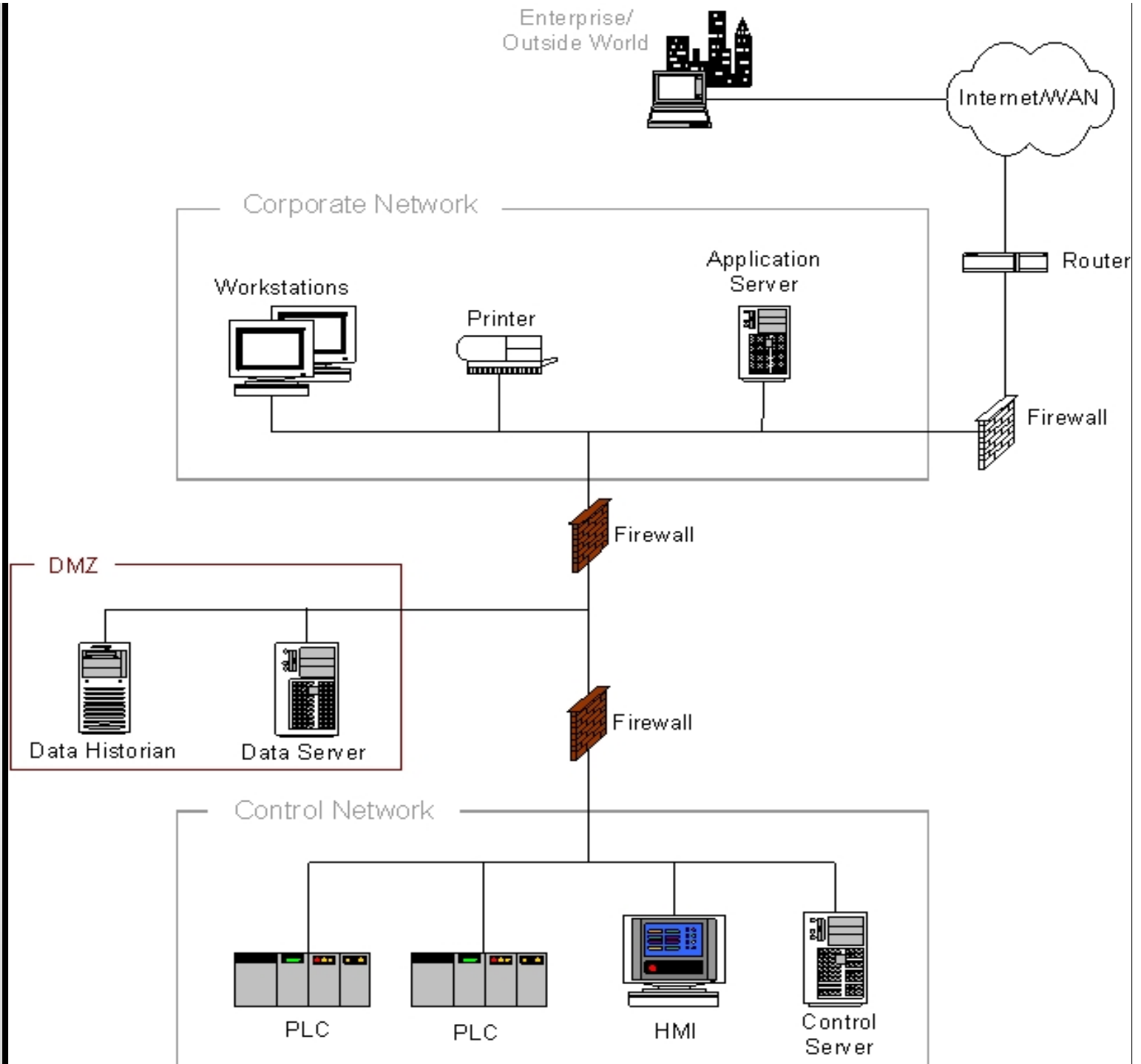
What is a Hacker?

- Someone who makes something work in a way it was not intended
- Computer Hacker – Making information systems, programs, etc. do things they were not designed to do for purposes such as offense, defense, intelligence gathering, or forensics
- PhD Hacker – Have people actually read your thesis

What is SCADA/ICS?

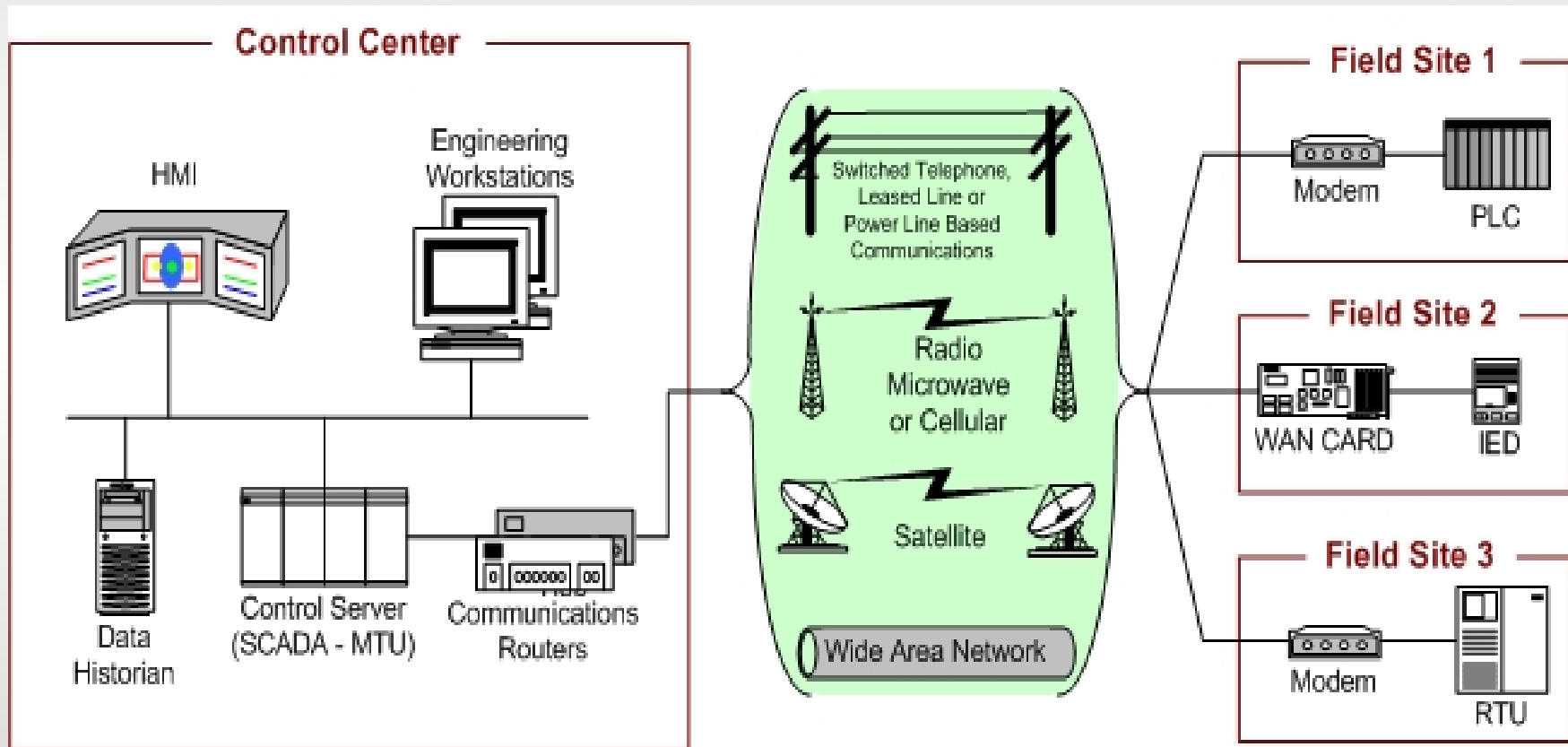
- Supervisory Control and Data Acquisition
 - Monitors large scale and often distributed control systems
- Industrial Control Systems
 - Manufacturing, Oil Refineries, Telecommunications, Satellites, etc.
- Control systems play a role in almost every aspect of daily life

Typical ICS Network



Source:
NIST 800-82

Typical SCADA Network



Source:
NIST 800-82

What is Cyberspace?

- Not just a term for getting grant money...
- A thin veil laid over all the other domains
- Interacts with almost every aspect of daily life
- Considered the fifth domain of warfare
 - (Air, Land, Sea, Space, and now Cyberspace)

What are SCADA/ICS Cyber Based Threats?

- Accidental Infections
 - Inability to patch
 - Poor security policies
- Advanced Targeted Attacks
- Common hacking tools
- Normal “hacker” methods
- Lack of security built in

Panetta: Cyber warfare could paralyze U.S.

By Scott Pelley

28

comments

47

Like

“The reality is that there is the cyber capability to basically bring down our power grid to create...to paralyze our financial system in this country to virtually paralyze our country.”

- Former U.S. Secretary of Defense
Leon Panetta



PLAY CBS NEWS VIDEO

← In 2009, the Pentagon established cyber command to wage war and defend America's cyber systems. It's a top priority for Secretary of Defense Leon Panetta. In an interview for "60 Minutes" CBS Evening News anchor Scott Pelley spoke with Panetta while he was touring the command post that's rigged to conduct nuclear war if need be. The Secretary told CBS News cyber war is one of his biggest worries.

Panetta: The reality is that there is the cyber capability to basically bring down our power grid to create ... to paralyze our financial system in this country to virtually paralyze our country. And I think we have to be prepared not only to defend against that kind of attack but if necessary we are going to have to be prepared to be able to be aggressive when it comes to cyber efforts as well. We've got to develop the technology, the capability, we've got to be able to defend this country.

[Panetta to Pelley: Iran will not be allowed nukes](#)
[60 Minutes: Cyber War, sabotaging the System](#)
[Pentagon: Cyber warfare skills inadequate](#)
[North Korea waging cyber warfare?](#)

Pelley: Is it fair to characterize your cyber command as currently engaged in battle every day?

Panetta: That's one of the interesting questions. What constitutes an act of war when it comes to cyber warfare? Countries use cyber as a way to exploit information. I think the Chinese use it as a way to gain information in the business arena. But if a cyber effort were made that, in fact, crippled this country or paralyzed this country or hit a major grid system then you have to ask the question does this constitute an act of war?

Stuxnet

- History Recap
- Not made by your traditional “hackers”
- Two portions:
 - Weapon System – “Computer hackers”
 - Payload – Exceptional engineers/scientists



Weapon System:

- 5 Vulnerabilities (4 0-Days)
 - Targeted Multiple OS
 - Spread on LAN
 - Injected via USB

Payload:

- Extremely Targeted Code
 - 1 Target 1 Kill
 - Module Based
- HMI/Safety Bypass Loop

Stuxnet

Encrypted Library

Configuration File

Encrypted Block

DB 8063

FC 6075

FC 6064

FC 6065

Stores input processes which relates to the number of centrifuges in each cascade. (6 is significant)

Initiation code to assign values for the centrifuges. (Values placed in groups 1-15 to match sections of Natanz cascade)

Attack configuration block; checks conditions to make sure the time is "right" for the attack.

Sets pointers in the code to each individual centrifuge; continues to check for proper attack conditions.

Information Gathering Tools

- Shodan
 - Ability to search for Internet connected control systems and facilities
 - Popular searches pre-saved for users who do not know what they are looking for
- Displayed Information
 - Company info, Social Media profiles, etc.

SHODAN - Computer Search Engine - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.shodanhq.com/ Google
Most Visited The Ethical Hacker Net... Hack Forums
SHODAN - Computer Search... Loading...
Main Exploits Research Videos Settings Logout Buy

SHODAN Search


Home Search Directory Data Analytics/ Exports Developer Center Labs


EXPOSE ONLINE DEVICES.


WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

[TAKE A TOUR](#) [FREE SIGN UP](#)


Popular Search Queries: Snom VOIP phones with no authentication - A list of Snom phone management interface without authentication

 **DEVELOPER API**
Find out how to access the Shodan database with Python, Perl or Ruby.

 **LEARN MORE**
Get more out of your searches and find the information you need.

 **FOLLOW ME**
Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS

<i>Shodan pinpoints shoddy industrial controls.</i> 	<i>It greatly lowers the technical bar needed to canvas the Internet...</i>	<i>'Shodan for Penetration Testers' presented at DEF CON 18</i>	<i>It's a reminder to many to know what's on your network...</i>
<i>Shodan is the Google for hackers.</i>	<i>Shodan vereinfacht die Suche nach SCADA-Systeme erheblich...</i>	<i>Firmen öffnen Stuxnet und Co. selbst die Tür.</i>	<i>Computerangriffe werden einfacher. Zumindest für die Nutzer von Shodan.</i>

Privacy Policy | Terms of Service © SHODAN

Waiting for www.shodanhq.com... Tor Enabled
8:42 PM 10/4/2011

Browse All Searches

Tag: **scada**

- 30 NOV 10 **scada**
US search

4 NOV 10 **SCADA**
SCADA systems search

26 JUL 10 **SAPHIR**
Siemens SAPHIR HVAC system with integrated web server enabled

17 AUG 11 **Delta Entelitouch**
Delta Controls Entelitouch

5 AUG 11 **Simatic**
Telnet Login without passwd to HMI, XP277

6 NOV 10 **Allen Bradley SLC5** UPVOTE
Allen Bradley SLC5 PLC

8 MAR 11 **Electro Industries GaugeTech**
Electro Industries GaugeTech SCADA - Homepage: <http://www.electroind.com/>

4 NOV 10 **Simatic S7 SCADA**
This right here would be the SCADA systems that Stuxnet targeted. Enjoy.

5 NOV 10 **Simatic HMI**
Human Machine Interface for Simatic systems. I've removed the S7 from this search because I posted it yesterday, so this should be revealing new results for all.

TAC/XENTA 913
I thought I was being a little unfair on the BACnet protocol, so I searched out the TAC/XENTA-913 gateway, which is, I believe (though I'm not certain) very LonWorks oriented.

Order By

- » Popularity
- » Recently Added

Popular Tags

http	24
scada	12
cisco	12
voip	9
ftp	9
sip	7
router	7
webcam	6
iis	6
anonymous	6
plc	5
ipcam	5
apache	5
default	5
bacnet	4
simatic	4
gateway	4
dreambox	4
remote	4
admin	4
access	4
password	4
ios	4
s7	3
server	3

[lonworks](#) [tac](#) [xenta](#) [bacnet](#) [scada](#) [plc](#)

Hacking Tools

- Exploit packs
- BackTrack
- Common tools like Nmap
- Metasploit
 - Various modules constantly developed
 - Many controllers NEVER get patches



[contact us](#) | [support](#)

[Home](#) | [Products](#) | [Services](#) | [Partners](#) | [About](#)



[Home](#) > [Products](#)

> [Agora Pack](#)

> [SCADA+ Pack](#)

> [Immunity's Canvas + 3rd party packs](#)

> [How to buy](#)

SCADA+ Pack

This is an attempt to collect ALL publicly available SCADA vulnerabilities in one exploit Pack.

SCADA and related vulnerabilities are very special due to their sensitive nature and possible huge impact involved to successful exploitation.
SCADA Systems are also "hard to patch", so even old vulnerabilities are actual.

The SCADA+ Pack features:

- Growing value
Due to low real systems patch rank
- We try to cover most of the public SCADA vulns!
Including old and newly discovered bugs
- 0 Days for SCADA
We conduct our own in depth research
- Focused on Industrial software & hardware environment
Not only SCADA, but also Industrial PCs, smart chips and industrial protocols are reviewed.
- Weak points analyses
Many industrial things suffer from weaknesses like hardcoded password and etc.

Metasploit Modules for SCADA-related Vulnerabilities

Metasploit Modules (via MSFUpdate / SVN)

Vendor	System / Component	SCADAhacker Reference	Metasploit Reference	Disclosure Date	Initial MSF Release Date
7-Technologies	IGSS	ICS-11-080-03	exploit/windows/scada/igss9_igssdataserver_listall.rb	Mar. 24, 2011	May 16, 2011
		ICSA-11-132-01A	exploit/windows/scada/igss9_igssdataserver_rename.rb	Mar. 24, 2011	Jun. 9, 2011
			exploit/windows/scada/igss9_misc.rb	Mar. 24, 2011	May 30, 2011
			auxiliary/admin/scada/igss_exec_17.rb	Mar. 21, 2011	Mar. 22, 2011
AzeoTech	DAQ Factory	Click Here	exploit/windows/scada/daq_factory_bof.rb	Sep. 13, 2011	Sep. 17, 2011
3S	CoDeSys	Click Here	exploit/windows/scada/codesys_web_server.rb	Dec. 2, 2011	Dec 13, 2011
BACnet	OPC Client	ICSA-10-264-01	exploit/windows/fileformat/bacnet_csv.rb	Sep. 16, 2010	Nov. 11, 2010
	Operator Workstation	n/a	exploit/windows/browser/teechart_pro.rb	Aug. 11, 2011	Aug. 11, 2011
Beckhoff	TwinCat	Click Here	auxiliary/dos/scada/beckhoff_twincat.rb	Sep. 13, 2011	Oct. 10, 2011
General Electric	D20 PLC	Press Release	auxiliary/gather/d20pass.rb	Jan. 19, 2012	Jan. 19, 2012
		DigitalBond S4	unstable-modules/auxiliary/d20tftpbdb.rb	Jan. 19, 2012	Jan. 19, 2012
Iconics	Genesis32	ICS-11-080-02	exploit/windows/scada/iconics_genbroker.rb	Mar. 21, 2011	Jul. 17, 2011
			exploit/windows/scada/iconics_webhmi_setactivexguid.rb	May 5, 2011	May 11, 2011
Measuresoft	ScadaPro	Click Here	exploit/windows/scada/scadapro_cmdexe.rb	Sep. 16, 2011	Sep. 16, 2011
Moxa	Device Manager	ICS-10-293-02 ICSA-10-301-01	exploit/windows/scada/moxa_mdmtool.rb	Oct. 20, 2010	Nov. 6, 2010
RealFlex	RealWin SCADA		exploit/windows/scada/realwin.rb	Sep. 26, 2008	Sep. 30, 2008
		ICS-11-305-01	exploit/windows/scada/realwin_scpc_initialize.rb	Oct. 15, 2010	Oct. 18, 2010
		ICSA-11-313-01	exploit/windows/scada/realwin_scpc_initialize_rf.rb	Oct. 15, 2010	Oct. 18, 2010
			exploit/windows/scada/realwin_scpc_txtevent.rb	Nov. 18, 2010	Nov. 24, 2010
		ICS-11-080-04 ICSA-11-110-01	exploit/windows/scada/realwin_on_fc_binfile_a.rb exploit/windows/scada/realwin_on_fcs_login.rb	Mar. 21, 2011 Mar. 21, 2011	Jun. 19, 2011 Jun. 22, 2011
Scadatec	Procyon	Click Here	exploit/windows/scada/procyon_core_server.rb	Sep. 8, 2011	Sep. 12, 2011
ScadaTEC	ModbusTagServer ScadaPhone	Click Here	exploit/windows/fileformat/scadaphone_zip.rb	Sep. 12, 2011	Sep. 13, 2011
Schneider Electric	CitectSCADA CitectFacilities		exploit/windows/scada/citect_scada_odbc.rb	Jun. 11, 2008	Nov. 8, 2010
Sielco Sistemi	Winlog	ICSA-11-017-02	exploit/windows/scada/winlog_runtime.rb	Jan. 13, 2011	Jun. 21, 2011
Siemens Technomatix	FactoryLink	ICS-11-080-01	exploit/windows/scada/factorylink_cssservice.rb	Mar. 25, 2011	Jun. 24, 2011
		ICSA-11-091-01	exploit/windows/scada/factorylink_vm_09.rb	Mar. 21, 2011	Jun. 21, 2011
Unitronics	OPC Server	n/a	exploit/exploits/windows/browser/teechart_pro.rb	Aug. 11, 2011	Aug. 11, 2011

```
root@bt: -
File Edit View Terminal Help

o o o
o o
o
PAYLOAD
| @ ) ( @ ) * * * * * | @ ) ( @ ) * * * * * | @ )
=====

LOOT
4D

= [ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ --- = [ 960 exploits - 509 auxiliary - 153 post
- --- = [ 257 payloads - 28 encoders - 8 nops
= [ svn r15903 updated today (2012.09.27)

RHOST => 172.16.1.30
[*] Got session id: 0x896978a7
[*] Got connection id: 0xac476989
[*] Auxiliary module execution completed

root@bt:~# msfcli auxiliary/micrologix_fault RHOST=172.16.1.30 e
```

Copyright 2011-2012 - CYBATI/cybatl.org

Source: Matt Luallen at CYBATI (has an excellent ICS Security Course)

Controller Exploits Require Access

- Hacking controllers require access to the controller which can be very difficult
- Must identify facilities
- Must break past security

Target the Users

- Advanced Persistent Threat...or BPT
- Spearphishing or USB/portable drives
- Supply chain hacks and user created links
- Most intrusions can be attributed to Layer 8



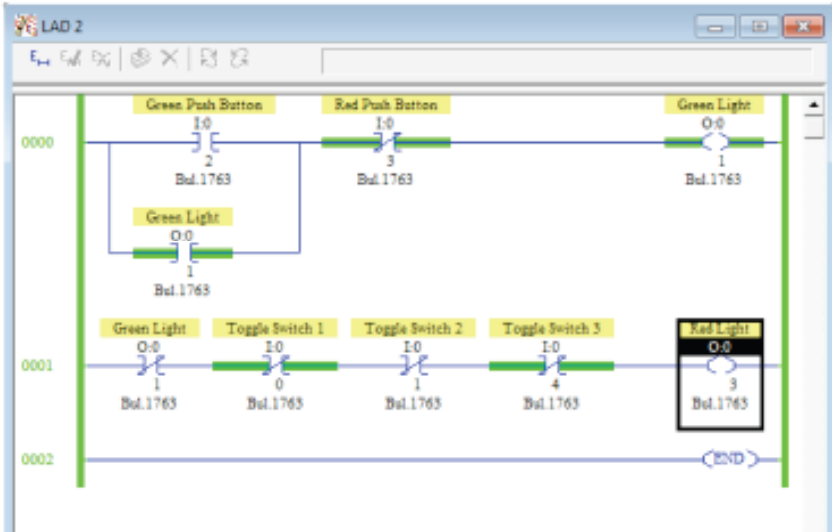


Because if you can't secure it surely someone else can...right?

Lack of Security in Devices/Protocols

- U.S. PDD-63 was in 1998
- Still poor (i.e. none) security on controllers
- FUD sellers advocating security “solutions”
 - It’s a process not a tool
- Unauthenticated protocols and traffic

Ladder Logic Programming



Data File II (bin) -- INPUT

Offset	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
I:0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
I:0.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
I:0.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
I:0.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
I:0.4	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1

I:0/0 Radix: Binary
 Symbol: Columns: 16
 Desc: Toggle Switch 1

Data File O0 (bin) -- OUTPUT

Offset	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
O:0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
O:0.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
O:0.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
O:0.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

O:0/0 Radix: Binary
 Symbol: Columns: 16
 Desc:

Source: Matt Luallen and his CYBATI course again

Advanced vs. Persistent

- Why create Stuxnet? How advanced was it?
- No longer mindset of “focus on large targets you get one shot”
- No logistic lines like in land warfare, defenses up front



Cyber Conflict and ICS

- Threat to Civilian Infrastructure
 - Target infrastructure as military target
 - Corporate secrets and competitive advantage
 - Labs research



Loss of Human Life



Offensive Approach

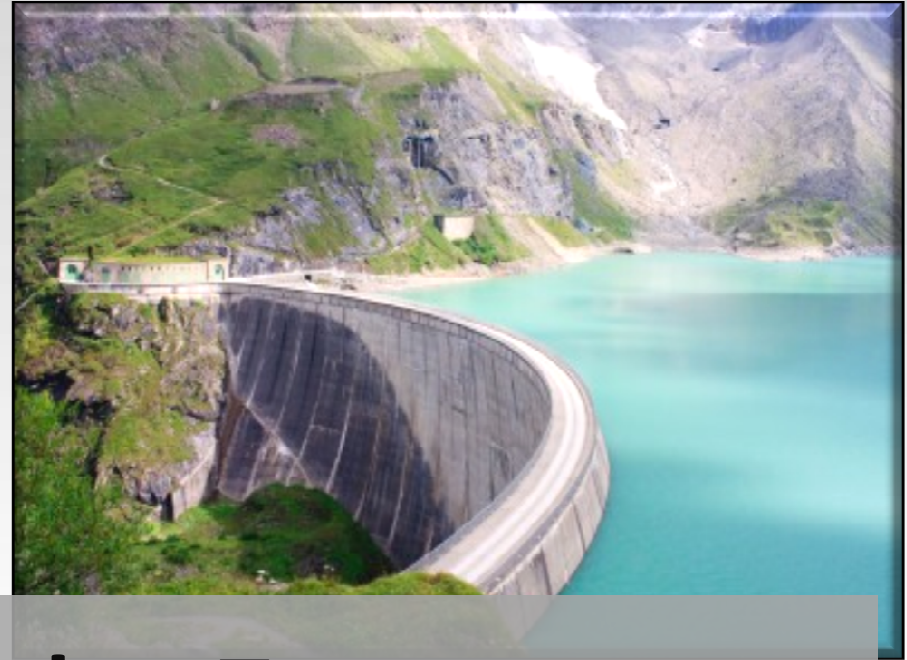
Computer Hacker Methodology

- Reconnaissance/Information Gathering
- Active Scanning/Enumeration
- Exploitation
- Privilege Escalation
- Persistent Access
- Cover Tracks

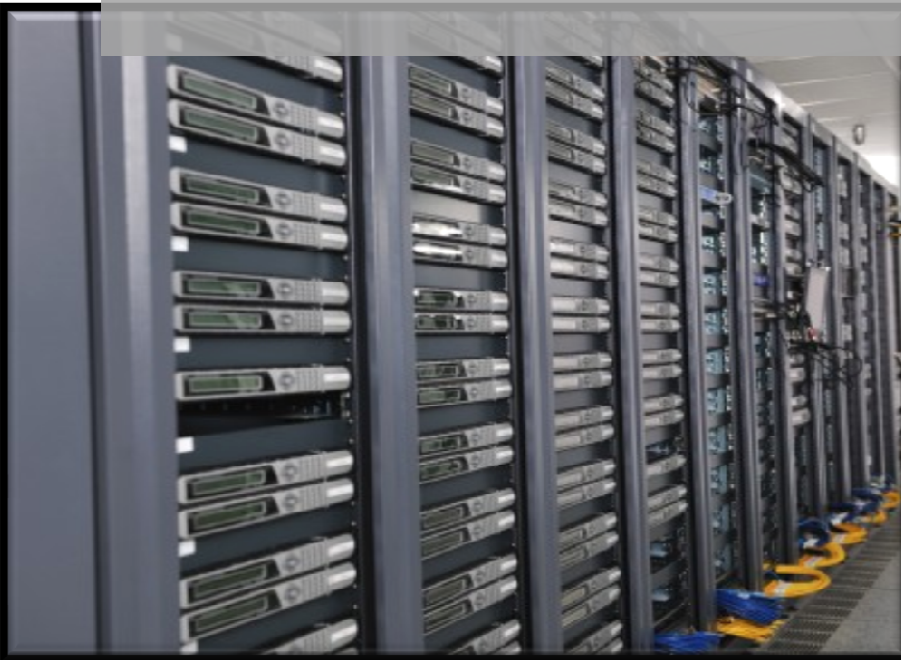


What is SCADA/ICS?

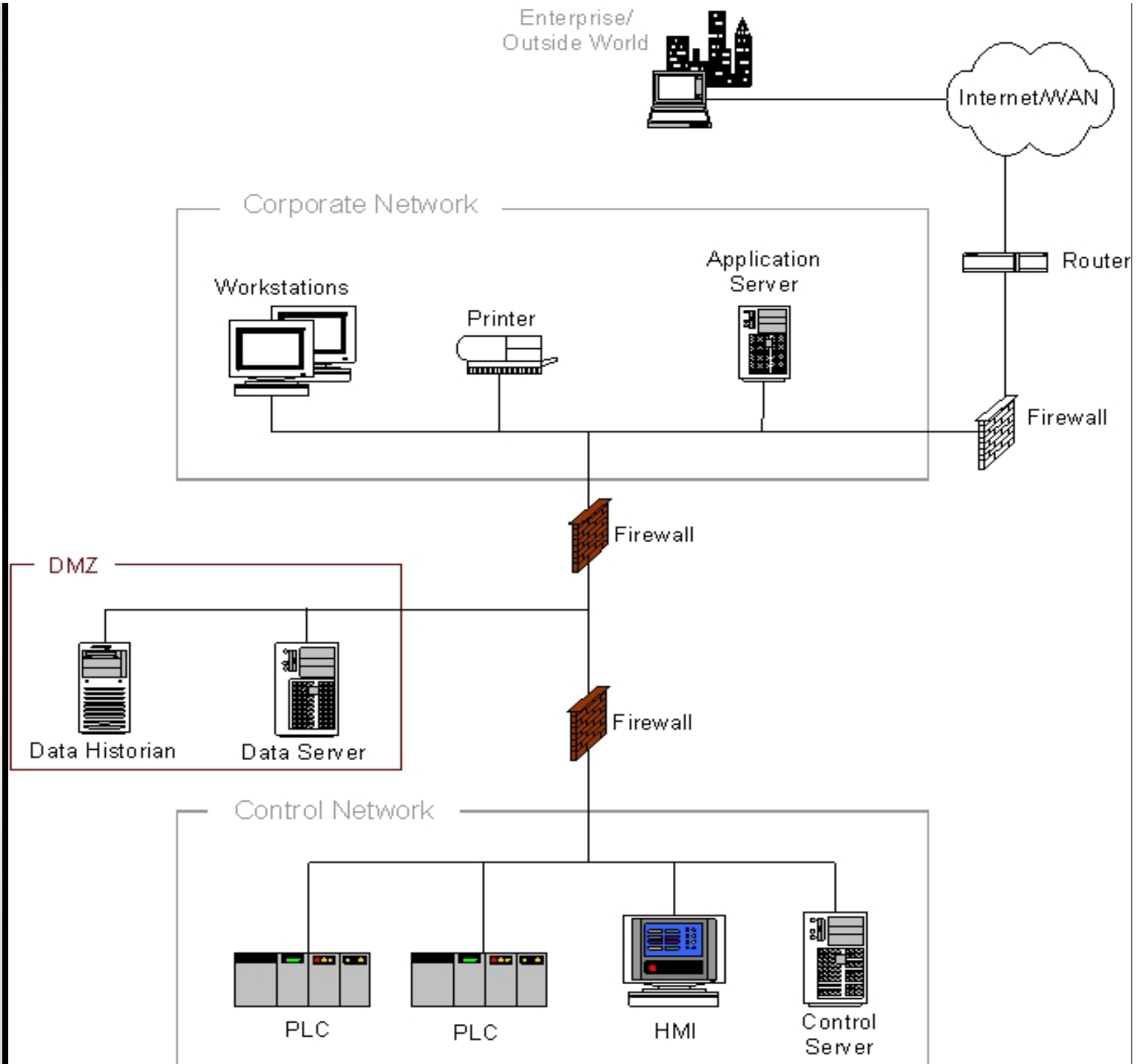
- Same slides as early...
- But now think like a hacker...
- Think like an attacker...



SCADA as Cyber Targets

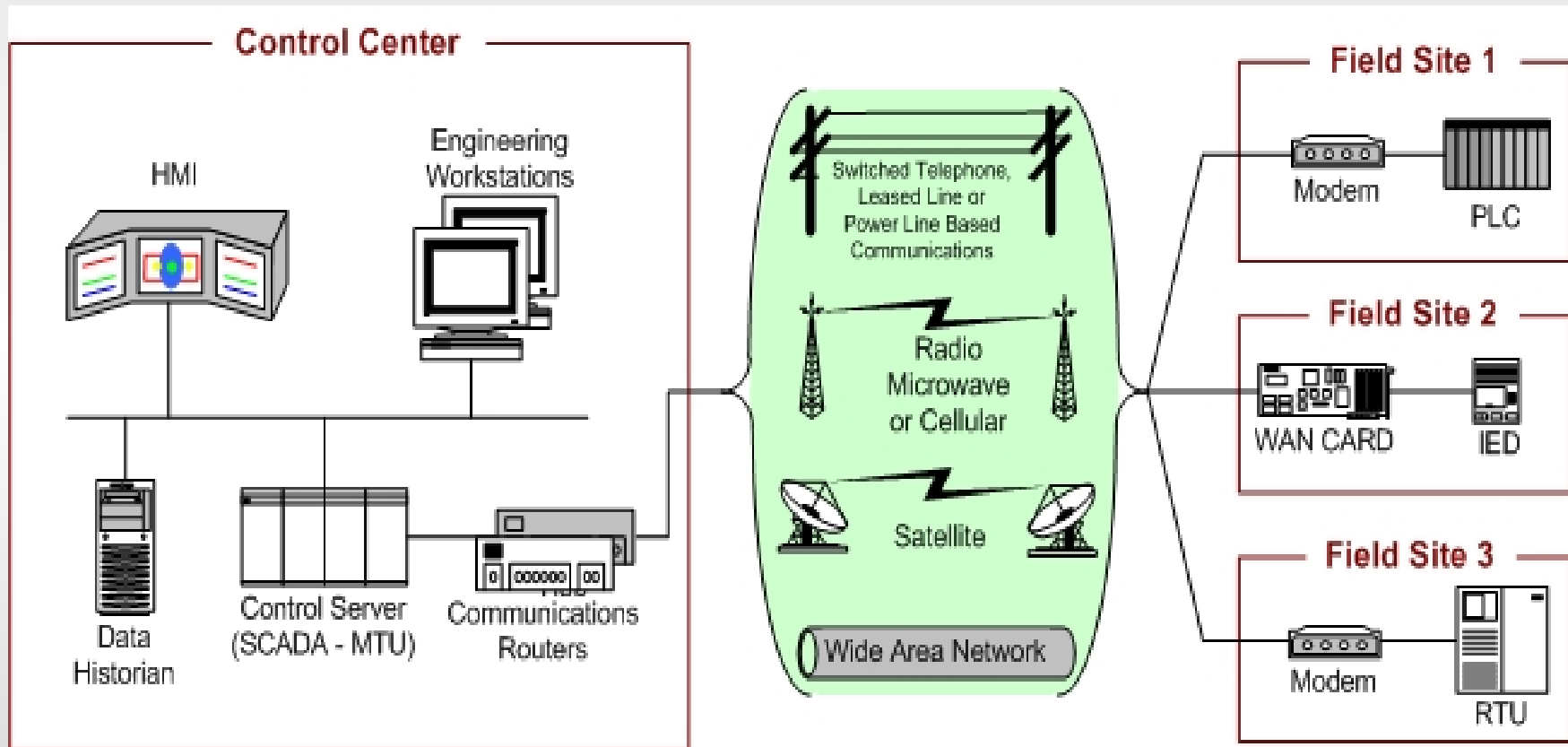


Typical ICS Network



Source:
NIST 800-82

Typical SCADA Network



Source:
NIST 800-82

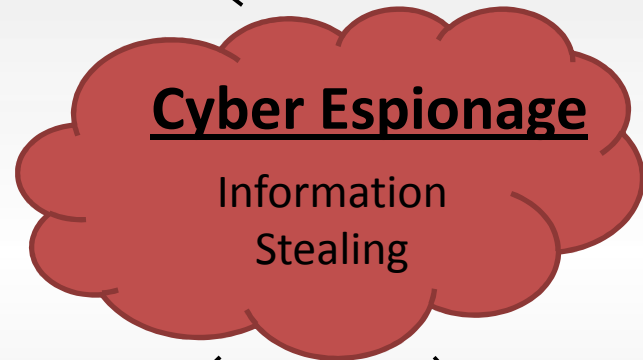
Hypothetical Attack Scenario



Industrial Control Systems



Certificate Authorities



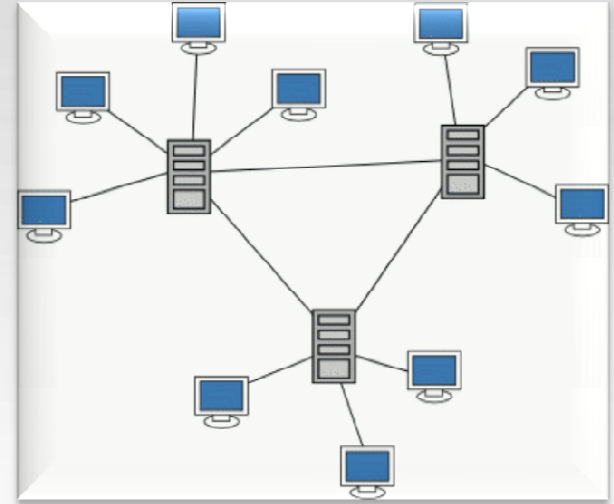
Industrial Factory



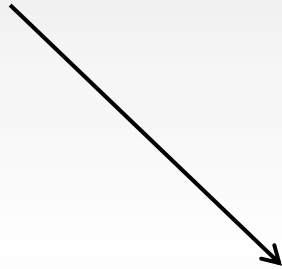
University/Corporate Research Laboratories/AV Companies

Cyber Attack

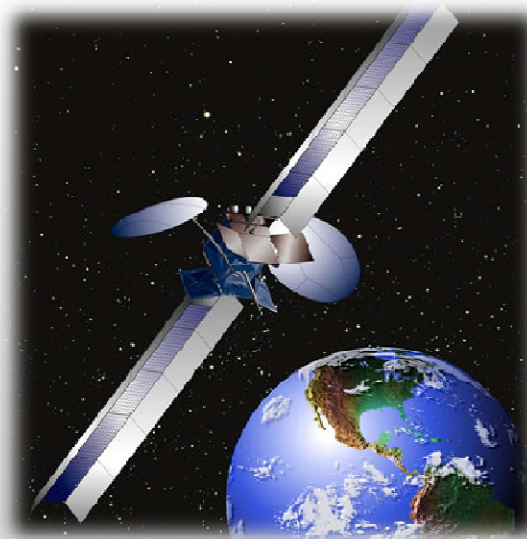
Disruption of
Communication



Key Internet Nodes/ISPs



Key Electrical Power Grids



Satellite Communication Network



Military Conflict
Nation vs. Nation
Non Nation vs Nation

Missile Radar/SAM
Sites/Warning Systems

Mobile C2 and
Attack/Defense A/C



Coastal Defenses

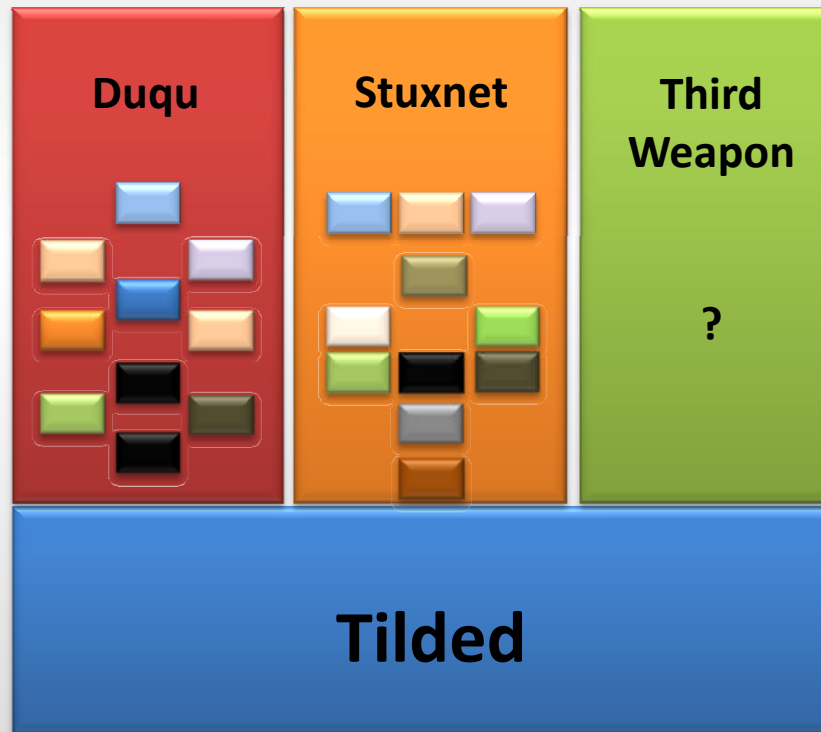
How Difficult is That?

- Very difficult and no need to exaggerate
 - However, it's something that is possible
- In fact we've already seen an approach to doing multiple approaches in one platform

Tilded

- History of Tilded
- Style
 - Framework for Stuxnet/Duqu
- Features
 - Module based code writing, similar drivers between August 2011 Duqu infection to Stuxnet, updatable framework
- Stuxnet and Duqu spawn
 - The reason Stuxnet/Duqu look as they do
 - Design driven by purpose and needs

Tilded



FUD vs. Real Threats

The Coming Cyber Attack That Could Ruin Your Life

www.thefiscaltimes.com/Articles/2013/03/11/The-Coming-Cyber-Attack-that-Could-Ruin-Your-Life.aspx#page1

With cyber attacks on the rise, is your company's data secure?

www.guardian.co.uk/media-network/media-network-blog/2013/feb/11/cyber-attack-security-data

The Next Cyber War Is Already in Progress: Security Expert

www.cnbc.com/id/100501836

8132-1869-2304-9579-8415

Cyber Attacks Becoming Top Terror Threat, FBI Says

www.informationweek.com/government/security/cyber-attacks-becoming-top-terror-threat/232600046

German firms see rising Chinese cyber attacks

www.thelocal.de/sci-tech/20130224-48165.html#.UT8e2xz-img

China leveled 'time-bomb' cyber attack on Japanese, researchers say

www.infosecurity-magazine.com/view/31131/china-leveled-timebomb-cyber-attack-on-japanese-researchers-say/

What Now?

- The current security regarding SCADA/ICS is horrible but not as bad as the news says
- What was amazing technology years ago is not now though; what was difficult research is now taken for granted
 - Accomplishing a difficult attack now will not be so difficult in the future as the tech/experience advances

Is Defense Doable?

- Yes!
- Approach security as a process
- Defense is actually easier when done right
 - Know your network and keep learning
- Provide accessible education to users
- Incorporate security mindset into research for the next generation of protocols/tech

“I’m Not the Security Guy”

- Who is this mythical “security guy?”
- It all starts with the research
 - If you do not incorporate it no one else will
- Approach your research from all angles
 - You think of how someone would attack your thesis, think of how someone would actually attack it
- Make your expertise work in new ways
- Security is part of the process

Conclusion

- Attacking SCADA/ICS is NOT easy
 - But it's doable and getting easier
- Security starts with the researcher
- If you do not research, examine, critique, analyze, theorize, propose, etc. the WHOLE process no one else will
- Think like an attacker with your systems, think of how you'd break them, and think outside the box...be a hacker...it impacts us all



HACKER

You keep using that word... I do not think it means what you think it means.

Questions?

RobertMichael.Lee@Gmail.com

Twitter: @RobertMLee