



National Electric Sector
Cybersecurity Organization

Threats, Vulnerabilities and Impacts: Energy Security in the Digital Age

Energy Assurance Summit

January 24 2012

University of Louisville, Shelby Campus

Louisville, KY

Advantage: Adversaries



Motivated, adaptive adversaries exist, and they don't follow the rules or regulatory checklists



Advantage: Adversaries



SONY

citibank



Bank of America



Morgan Stanley

The Washington Post



**Pacific Northwest
NATIONAL
LABORATORY**



HB Gary

YOUR NAME HERE...

Technology Landscape



- Emergent intelligence
- A new digital world order
- Widespread connectivity
- Size matters & doesn't
- Hyper-embeddedness
- Lingering legacy

Regulatory Landscape



- Smart Grid interoperability
- Compliance vs. Security
- White House movement
- Data breach disclosure
- Vendor, utility responsibility
- Intelligent islanding

Cybersecurity Landscape



- Research, espionage, organized crime, warfare
- Nation state quality defense is the new norm
- Isolation is extremely difficult
- Bolt-ons are complex
- Cyber-kinetic impacts



Cybersecurity Landscape



- Stuxnet
 - 5.74M Google hits
 - “Most sophisticated malware...”
 - “Game changer...”
- Duqu
 - 2.61M Google hits
 - Industrial equipment target



Threat Landscape



Google search opens SCADA systems to doomsday scenarios

By Joseph Volpe posted Aug 4th 2011 5:26AM



Google, the service so great
The search site played inad
(SCADA) systems in a Black
CTO walked attendees thro

twitter Login Join Twitter

Securing critical infrastructure at a snail's pace <http://bit.ly/gHgn3d> Why bother with kinetic attacks at all? #cyberwar #infosec #security

about 22 hours ago via web
Retweeted by 2 people

 **ArtKingston**
Arthur Kingston

Researcher demos attacks on Siemens industrial control systems - CNET



CNET

Researcher demos attacks on Siemens industrial control systems CNET

The protocol was intended to be open and packets are sent in plain text, he said, echoing concerns voiced by Jonathan Pollet, founder of Red Tiger Security, and Tom Parker, chief technology officer of FusionX, in their SCADA security workshop earlier ...
[How easily can a power plant be hacked? Verymsnbc.com](http://www.verymsnbc.com)

Threat Landscape



THE WALL STREET JOURNAL | TECHNOLOGY

U.S. Edition Home - Today's Paper - Video - Blogs - Journal Community

World - U.S. - New York - Business - Markets - Tech - Personal Finance - Life

Small Business -

Digital Personal Technology What They Know

TECHNOLOGY | JANUARY 23, 2012

Hackers-for-Hire Are Easy to Find

Article Comments

Email Print Save Tweet 400

By CASSELL BRYAN-LOW

Sitting in his Los Angeles home, Kuwaiti billionaire Bassam Alghanim received an alarming call from a business associate: Hundreds of his personal emails were posted online for anyone to see.

Mr. Alghanim checked and found it to be true, according to a person familiar with the matter. The emails included information on his personal finances, legal affairs, even his pharmacy bills, this person said.

*“Mr. Alghanim's lawyers allege in court filings that his brother hired investigators to illegally access his email with the help of Chinese hackers. **Cost to hire the hackers: about \$400.**”*


Vulnerability Landscape



twitter Login Join Twitter!

Nice attack scenario shown by Andrei Costin at #t2infosec - you could hack a laser printer so it stops the paper in the fuser, igniting it.

about 12 hours ago via Mobile Web
Retweeted by 21 people

 **mikkohypponen**
Mikko H. Hypponen

 **27 Bruce Barnett** @grymoire Close

SHODAN & SCADA results w/geoIP from C4: "Quantitatively Assessing and Visualising Industrial System Attack Surfaces" cl.cam.ac.uk/~fms27/papers/...

8:15 AM - 23 Jan 12 via web · Details

← Reply ↻ Retweet ★ Favorite

 **@reversemode**
Rubén Santamarta

Regarding missile failures, insecure BAS may pose risks <http://yfrog.com/6ggvpp> reporting to the ics-cert...

2 minutes ago via TweetDeck ☆ Favorite 🔄 Retweet ↻ Reply

Utah National Guard Armory's

ID= [redacted]

Username:

Password:

 **@krypt3ia**
krypt3ia October 7, 2011 Tweet 0

Rotate photo View full size

Authentication Required

A username and password are being requested by <http://98.198.97.45>. The site says: "Wadear test site"

User Name:

Password:

Cancel OK

Uhhhh... #shodan

Vulnerability Landscape

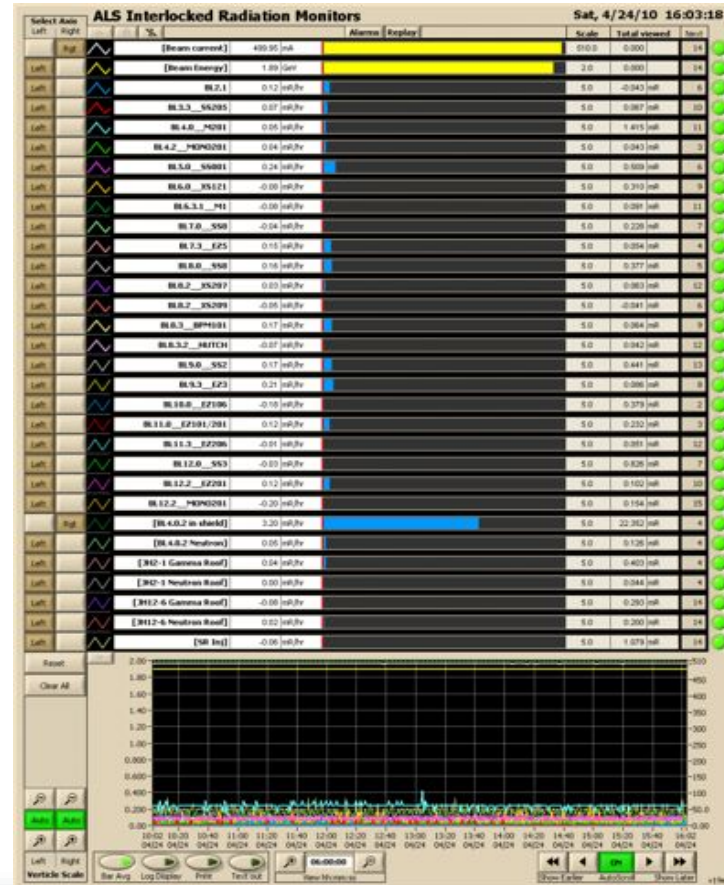


krypt0la @krypt0la

From the latest SCADA list dump via SHODAN from Lutz/AntiSec/Someone It's a SCADA but its a DEMO. cc @ArtyAlida
[twitpic.com/Bat93v](https://twitter.com/Bat93v)
[Hide photo](#)

TwitPic [Flag this media](#)

8:16 AM - 23 Jan 12 via Twitpic · Details
[Reply](#) [Favorite](#)



Vulnerability Landscape



46 “zero-day” SCADA vulnerabilities issued a two-week span

SCADA TROJANS

ATTACKING THE GRID
RUBEN SANTAMARTA
/Rooted^o CON 2011
3-4-5 Marzo 2011
Madrid

Luigi Auriemma
luigi@autistici.org

ADVISORIES

The complete archive of my advisories about [software security vulnerabilities](#) found by me

News
Advisories
Proof-of-concepts
Research
Fake_players_bug
MyToolz
Password_recovery
Patches
MyMusic
TestingToolz
About...
RSS_feeds
Amiga_ADF
Forum

search

luigi.org
backup.luigi.org
mmor.luigi.org

Stack overflow in Microsoft HTML Help 6.1 (CHM files)
12 Apr 2011: [adv - PoC - chm_1](#)

Vulnerabilities in Microsoft Reader 2.1.1.3143 / 2.6.1.7169
11 Apr 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - msreader_1/5](#)

DoS vulnerabilities in Microsoft Host Integration Server 2010 8.5.4224.0
11 Apr 2011: [adv - snabase_1](#)

Vulnerabilities in Siemens Tecnomatix FactoryLink 8.0.1.1473(SCADA)
21 Mar 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - factorylink_1/6](#)

Vulnerabilities in Iconics GENESIS32 9.21 and GENESIS64 10.51(SCADA)
21 Mar 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - adv8 - adv9 - adv10 - adv11 - adv12 - adv13 - genesis_1/13](#)

Vulnerabilities in 7-Technologies IGSS 9.00.00.11059(SCADA)
21 Mar 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - adv8 - igss_1/8](#)

Vulnerabilities in DATAC RealWin 2.1 (Build 6.1.10.10)(SCADA)
21 Mar 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - realwin_2/8](#)

Vulnerability Landscape



Project Basecamp "Vigilante" Hopes

Dale G Peterson

Like

+1 0

Tweet 2



the default.

While Kim Zetter's *Wired* article had a sensational "Vigilante" teaser headline, it was a fair accounting of the presentation at S4. And I was very pleased that she captured a couple of key quotes on the "why" of Project Basecamp and our goal of making it a Firesheep moment for PLC's.

Eric Butler's *Firesheep* plugin for the Firefox browser made it simple for anyone who could operate a browser to hijack Twitter, Facebook and Hotmail http sessions in a coffee shop's wifi. This security problem related to cleartext cookies that had not been addressed 2+ years after researchers disclosed it. After *Firesheep* the outcry from the users was so widespread that https quickly became a configurable option and in a few more months

Firmware					
Ladder Logic					
Backdoors					
Fuzzing					
Web			N/A	N/A	
Basic Config					
Exhaustion					
Undoc Features					

Vulnerability Landscape



The image shows two overlapping website screenshots. The background screenshot is for SHODAN, a search engine for Internet of Things (IoT) devices. It features a dark theme with a search bar and navigation links like 'Home', 'Search Directory', 'Data Analytics/ Exports', 'Developer Center', and 'Labs'. A prominent banner reads 'EXPOSE ONLINE DEVICES.' followed by a list of device types: 'WEBCAMS. ROUTERS. POWER PLANTS. IPHONES. WIND TURBINES. REFRIGERATORS. VOIP PHONES.' Below this is a 'TAKE A TOUR' button. The foreground screenshot is for ERIPP (Every Routable IP Project), which has a blue header. It includes a navigation menu with 'Home', 'FAQ', 'IP Database', 'Stats', and 'Contact', along with a 'Connect' button. A 'stats' section displays the following data:

Workers	0
Running:	34,188,425
Active	hosts223.255.12.248
found:	5888.5MB
Next IP group:	

Below the stats is a 'What's This?' section explaining the project's goal: 'This project will attempt to connect to every IP address on the internet. More specifically, we'll be connecting to port 80 (the port your browser uses to view webpages by default). This will tell us if the address we're connecting to is acting as a webserver.' A 'Why do this?' section is also visible.

There's An App For That



- “Get mobile access to your control system via an iPhone, iPad, Android and other smartphones and tablet devices. The Ignition Mobile Module gives you instant access to any HMI / SCADA project created with the Ignition Vision Module.”



To The Cloud!



“Use any standard browser on any device to access HMI. No downloads, no tedious installs, no plug-ins. Login and you have the HMI in your hands wherever you are: factory cafeteria, or parking lot, or on the beach, or even the golf course!”

“GoToMyHMI provides Secure, Easy and Fast access from any Browser to InstantHMI 6.0, ready to serve you on the cloud today. Remotely Monitor, ACK Alarms and Control your HMI for one low flat fee.”

Public Domain?



THE VERGE PRODUCTS · REVIEWS · FEATURES · SHOW · PODCAST · ABOUT · TIP US · FORUMS · Search articles & p

PREVIOUS STORY
Intel Android smartphone and tablet prototypes tested by MIT, look promising

NEXT STORY
SpnKIX are the motorized skate shoes Kickstarter generation

ANDROID · APPS & SOFTWARE

Lingering Android security flaw lets apps do things without permission

By Sean Hollister on December 28, 2012 04:00 AM

PCWorld » Blogs » Today @ PCWorld

Recommend: Like 74 | 113 | +7 4 | 714 | Email | 2 Comments | Print

TODAY @ PCWORLD

iPhone Security Flaw Shows Potential for App Store Malware

By Jared Newman, PCWorld Nov 8, 2011 1:20 PM



The iPhone App Store has a reputation for rock-solid security, but that rep took a hit this week when an app that could run unauthorized code and control phones remotely was released to the public.

Luckily, this bad app was released for research purposes—not malicious ones.

Security researcher and famous Mac hacker Charlie Miller demonstrated an iPhone security flaw using a dummy stock ticker app that Apple unwittingly accepted into the App Store. The app was able to call a remote computer, which could then download unsigned code to

From Obscurity To Novelty



- PLC, Smart Meter, comm device hacking
- Hacking cookbooks, fuzzers, sniffers
- Metasploit, Core Impact, etc
- Supply chain attacks
- Manuals available in all languages on Internet

Shiny Object



- Headline presentations at S4, BlackHat/DefCon, DerbyCon, RootedCon, BSides ...
- Wall Street Journal, National Journal, CNN
- Too many IT trade publications to name
- Blockbuster films, prime time TV shows
- Person-on-the-street, Congress, White House

National Electric Sector Cybersecurity Organization



- EnergySec awarded partial DOE funding to establish and maintain the National Electric Sector Cybersecurity Organization (NESCO)
- NESCO Mission:
 - Lead an independent, broad-based, public-private partnership to improve electric sector energy systems cyber security
 - Become the security voice of the electric sector

Engage Equip Empower



- Sharing requires trust
- Trust is built on relationships
- Our approach...
 - Bringing people together
 - Flexible technology options and solutions to extend and enhance relationships
 - Organic growth; birds of a feather

Summary



- Sufficient MMO exist for potential impacts to Energy infrastructure elements
- Adversaries will easily outpace regulation, procurement and implementation cycles
- Focus on your people first, technology second
- Balance prevention, detection and response
- *You are not alone*



Questions...

Patrick C Miller

President & CEO, EnergySec

Principal Investigator, National Electric Sector Cybersecurity Organization

patrick.miller@energysec.org

503.446.1212 (desk)

@patrickcmiller (twitter)

www.energysec.org