Industrial Control Systems Cybersecurity Landscape

Patrick C Miller, President and CEO, EnergySec

July 19 2011

Annual Emerson Ovation/WDPF Users' Group Conference

What Is NESCO?

- Mission: Lead an independent, broad-based, public-private partnership to improve electric sector energy systems cyber security
- Goals:
  - Identify, disseminate common effective cyber security practices
  - Analyze, monitor and relay infrastructure threat information
  - Focus cybersecurity research and development priorities
  - Work with federal agencies to improve electric sector cyber security
  - Encourage key electric sector vendor support and interaction

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Advantage: Adversaries

- Security approaches favor new installations, legacy environments are still vulnerable
- Very difficult to replace/patch in-service devices
- Isolation has diminishing security value
- Security products vs. buying secure products
- Engineering (N-1) and Security are different
  - Nature may be sophisticated, but it isn't malicious
- Hackers don't use a compliance checklist
  - Following a compliance checklist won't make you secure

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Advantage: Attackers

- Intelligent, adaptive adversaries exist
- Cyberwar:
  - Stuxnet is a game changer, sets the new bar
- Espionage:
  - Project, market & customer data (e.g. NightDragon)
- Organized crime:
  - Same old tricks, new platform

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Advantage: Adversaries

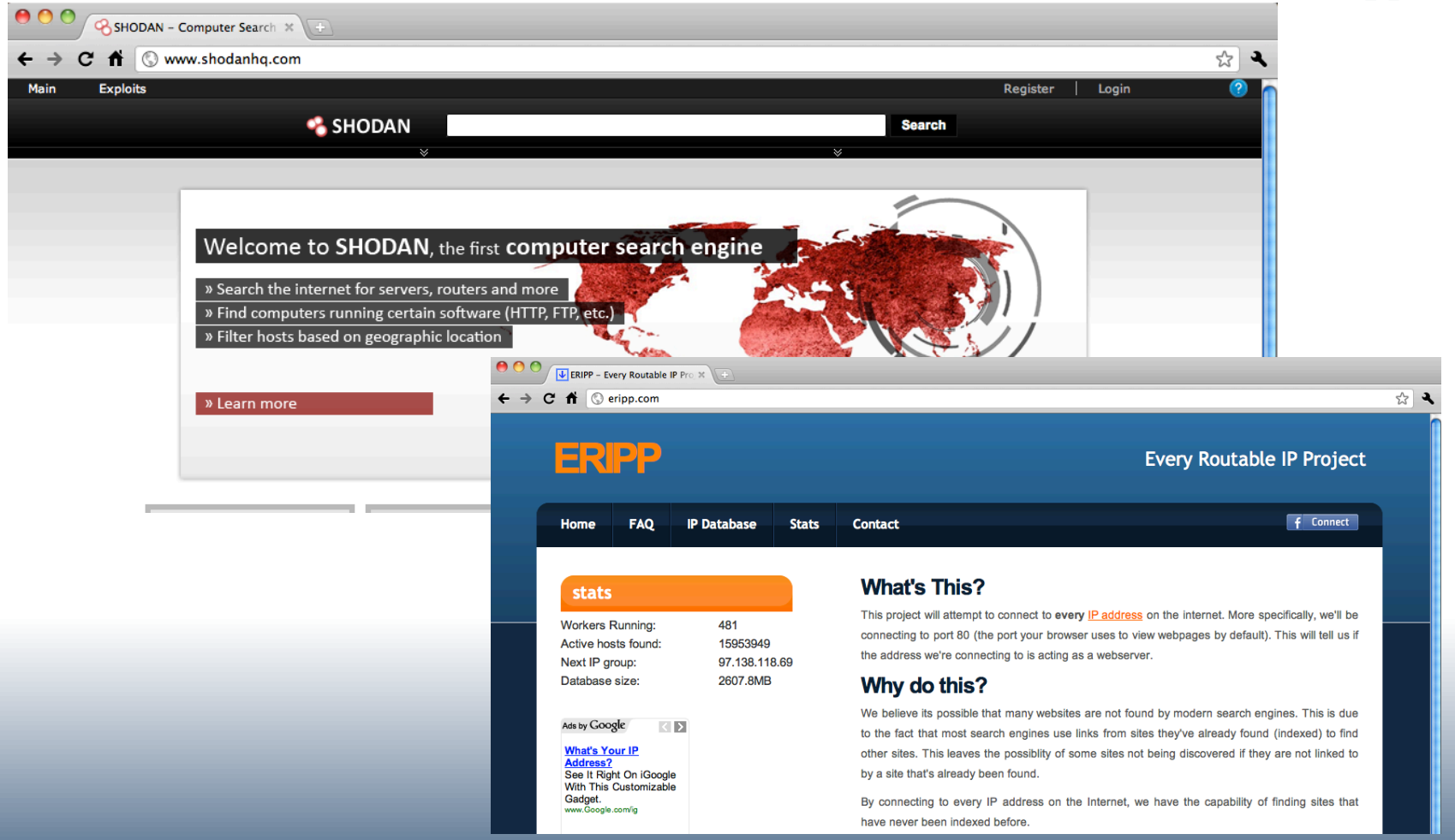
- Google search for "APT"
  - 34 hits in Jul 09
  - 169 hits in Jan 10
  - 1.2M+ hits June 11
- Google search for "cyberwar"
  - 416 hits Dec 09
  - 1.4M hits Feb 10
  - 3.4M+ hits June 11
- Welcome to the cyberarms race

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Advantage: Adversaries

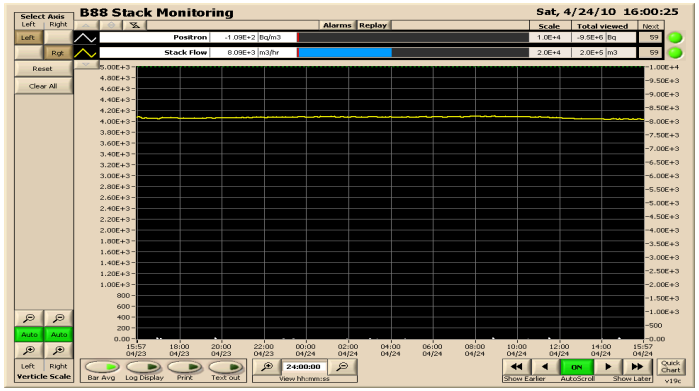
The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

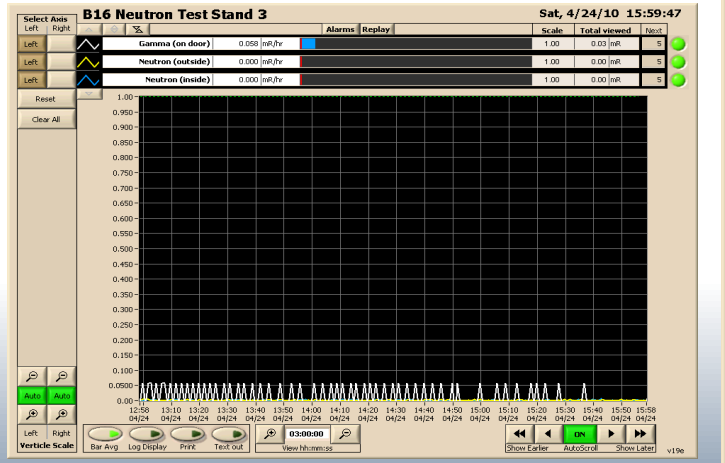
SHODAN, ERIPP, ETC

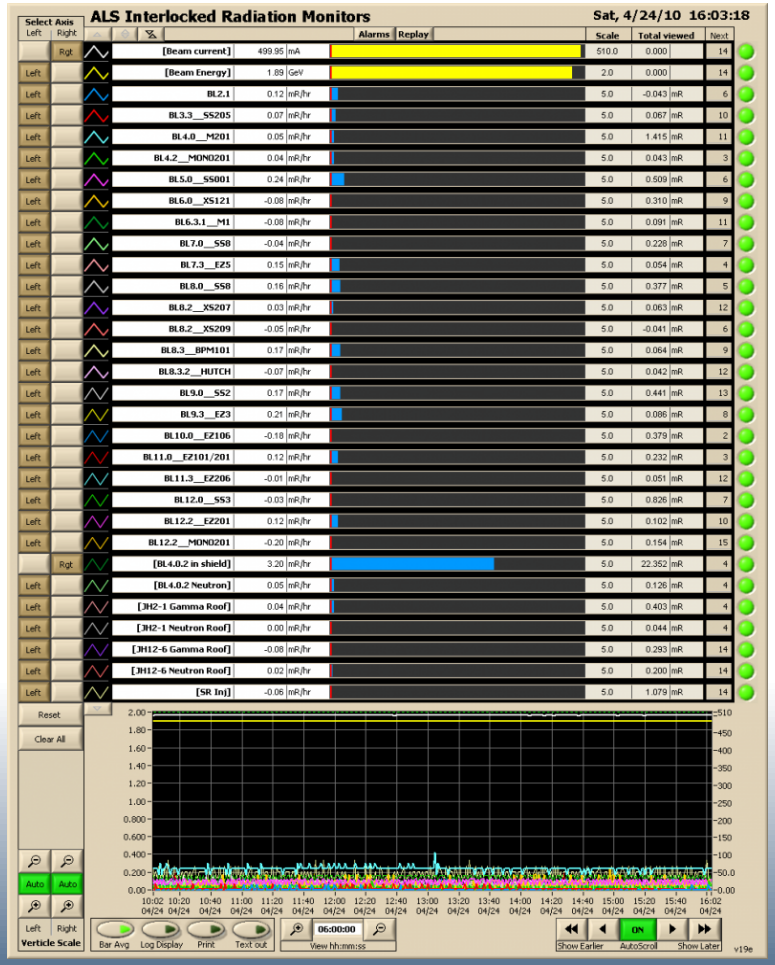


The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

SHODAN, ERIPP, ETC







Berkeley Cyclotron HMI images

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

The "Air-Gap" Myth

69.92.101.2
Added on 10.02.2011
69-92-101-2.cpe.cableone.net

HTTP/1.0 200 OK
Server: LV_HTTP/1.0
Date: Thu, 10 Feb 2011 0
Content-type: text/html
Last-modified: Wed, 25 J
Content-length: 704

96.11.251.66
Added on 13.08.2010
rrcs-96-11-251-66.central.biz.rr.com

HTTP/1.0 401 401 Authorization Required
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Server: Ubicom/1.1
Content-Length: 26
WWW-Authenticate: Basic realm="(Tenn-Plant)"
Connection: close

69.139.97.213
Added on 09.02.2011
c-69-139-97-213.hsd1.ms.comcast.net

HTTP/1.0 200 OK
Server: LV_HTTP/1.0
Date: Wed, 09 Feb 2011 1
Content-type: text/html
Last-modified: Wed, 25 J
Content-length: 704

64.7.227.38
Adtran NetVanta
Added on 25.05.2010

HTTP/1.0 401 401 Authorization Required
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Server: Ubicom/1.1
Content-Length: 26
WWW-Authenticate: Basic realm="(Wnsbro Water Plant)"
Connection: close

66.212.169.244
Added on 09.02.2011
dl.cashcode.com

HTTP/1.0 200 OK
Server: LV_HTTP/1.0
Date: Wed, 09 Feb 2011 (
Content-type: text/html
Last-modified: Tue, 05 A
Content-length: 1041

209.47.163.29
Adtran NetVanta
Added on 15.04.2010

HTTP/1.0 401 401 Authorization Required
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, max-age=0

139.6.18.127
Added on 01.02.2011
ntrt127.nt.FH-Koeln.DE

HTTP/1.0 200 OK
Server: LV_HTTP/1.0
Date: Tue, 01 Feb 2011 1
Content-type:
Content-length: 580

69.43.15.180
Added on 19.11.2009

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Application Notice — 0024
Compliance Application: CIP-002—CIP-009 Routable Protocols and Data Diodes

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

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."

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

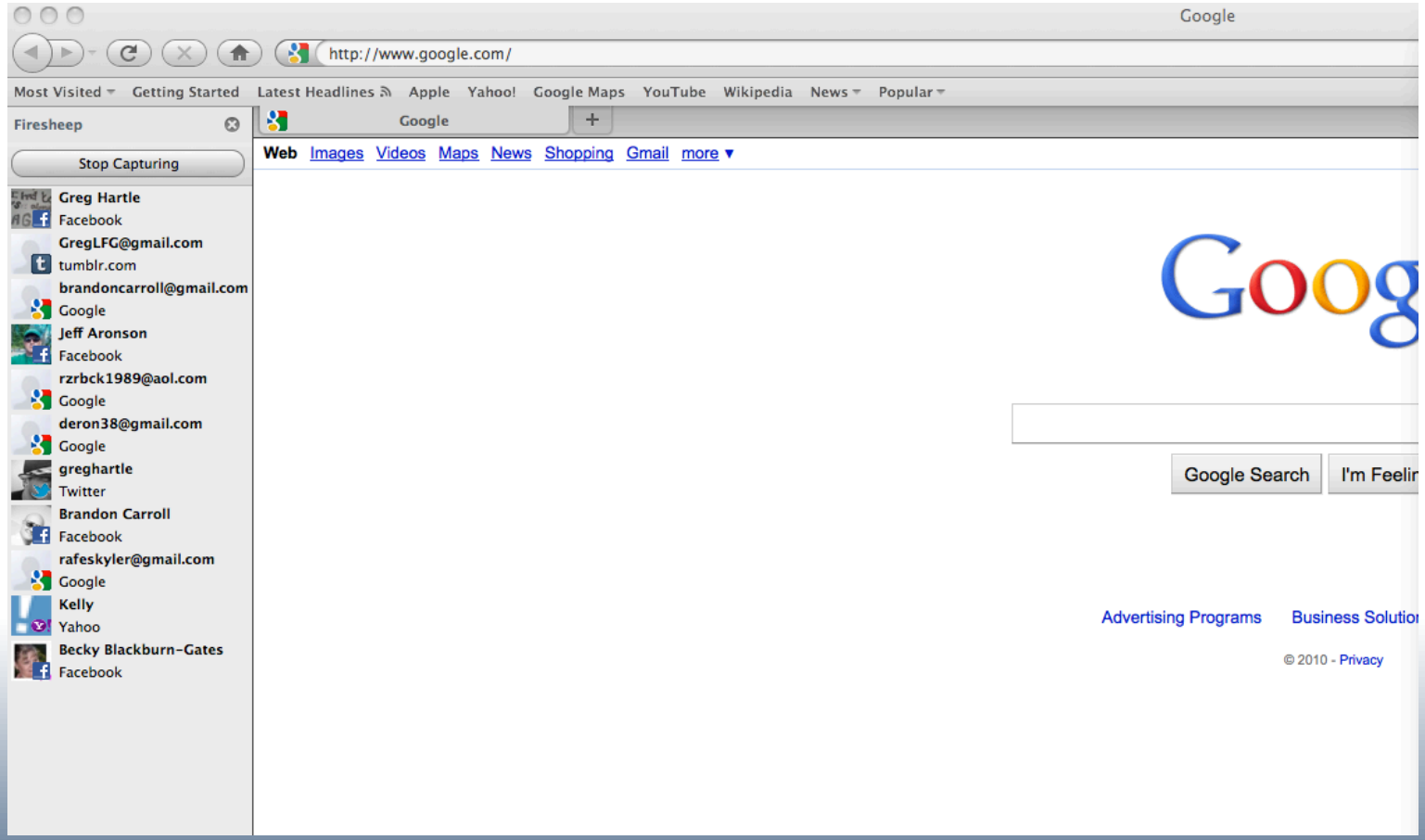
HMI In The Cloud

"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."

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Public Domain

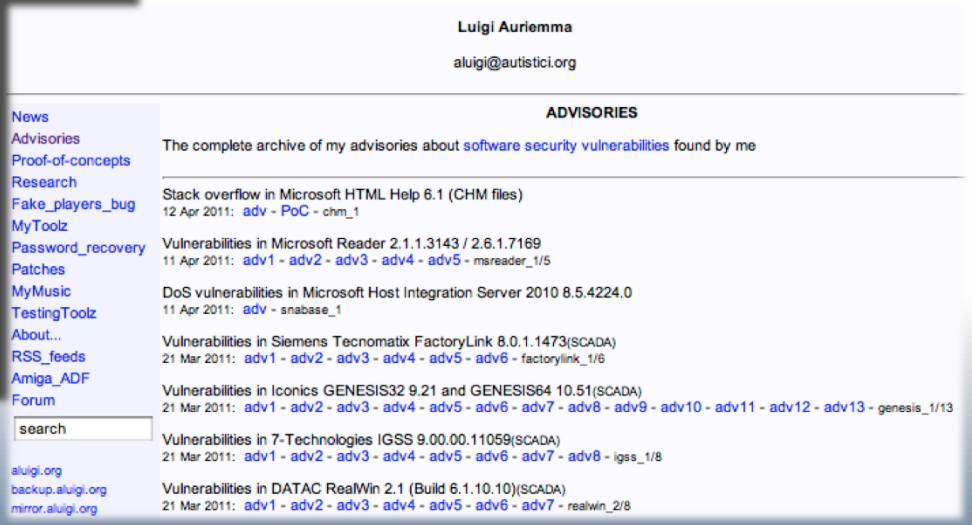


The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Research and Disclosure

EnergySec

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



The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

From Obscurity To Novelty

- Smart Meter hacking
- Hacking cookbooks
- Metasploit, Core Impact, etc
- Fuzzers
- Supply chain attacks
- Manuals available in all languages on Internet

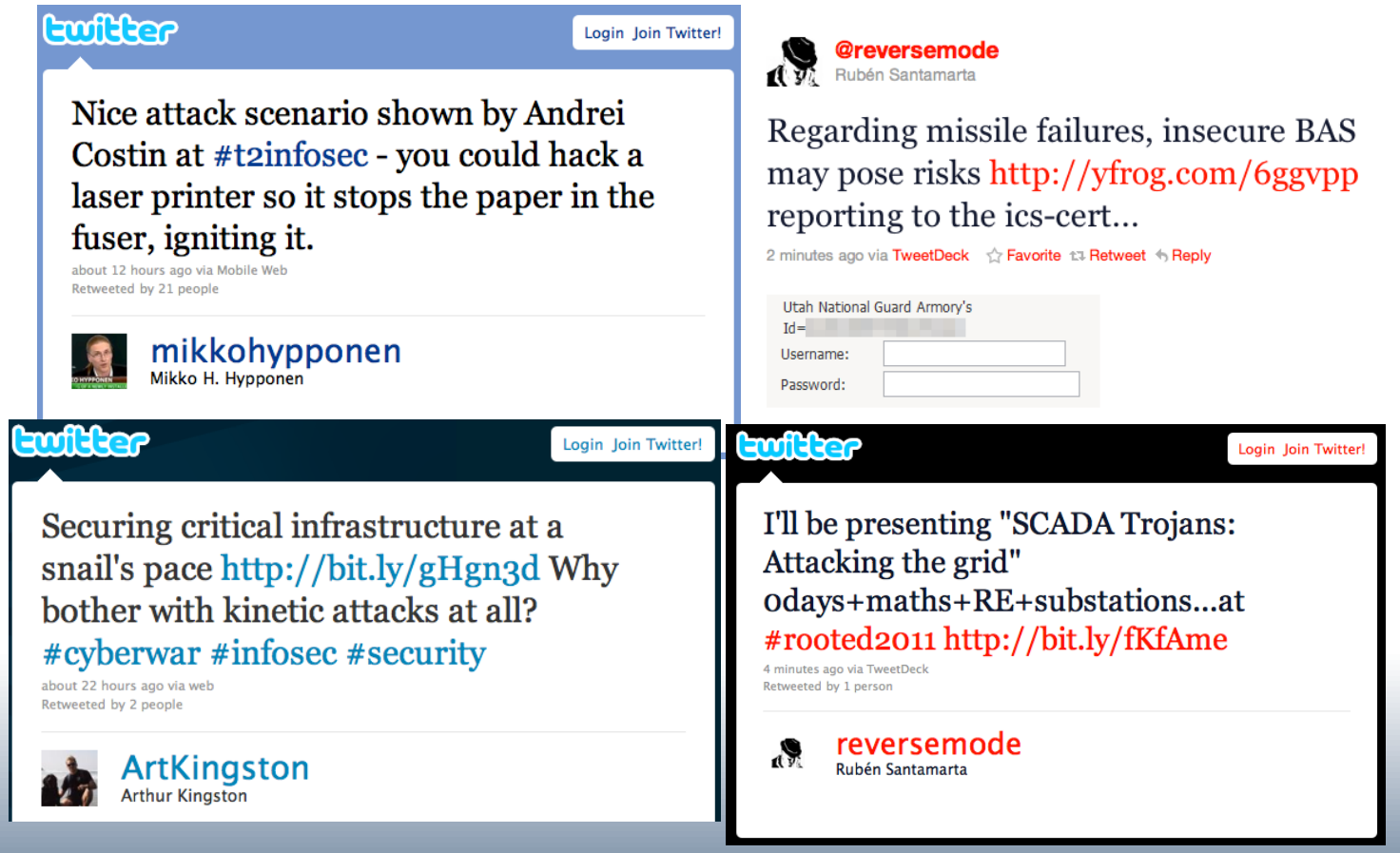
The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Shiny Object

- Shiny object for the mass media
- 60 minutes
- Wall Street Journal, National Journal, CNN
- Too many IT trade publications to name
- Blockbuster films
- Prime time television shows
- Social Media…

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

TwitBookBlogosphere



The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

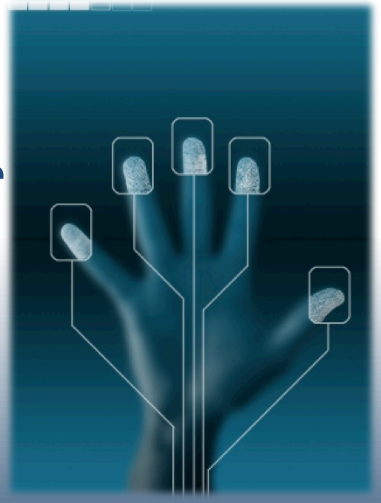
Economic Drivers

- Recession economy brings unique challenges
- Decreased participation working groups and conferences
- Static or shrinking headcount; increased workload
- Downsizing, pay freezes, etc increase insider threat
- Decreased spending on new equipment
- Older products extended beyond intended lifespan
- Security more expensive for customers and vendors

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

People Problem

- Humans are the **weakest** link in any security system
  - Passwords for candy; Social engineering
- Humans are also the **strongest** link
  - The Aware Person System (APS)
  - ICS culture shift is very slow, but powerful
- Danger: untrained operators of power tools can cause significant damage
  - Increasing complexity = training treadmill



The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Back In The Good Old Days

- Pneumatic, electromechanical, analog
- Telephone meant POTS or “bat phone” – no VoIP
- No Internet
- Less automation
- Less complexity
- Proprietary
- Long life span

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

ICS Gen-X

- Automation, more complexity
- Internet Protocol (TCP/UDP/etc)
- Data, more data and even more data
- Processing power, memory, bandwidth
- Interconnected business
- Migration from flat to segmented networks
- COTS software and hardware
- Increasingly shorter lifespans

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Millennium Systems

- Highly digital, highly complex
- Highly interconnected, highly layered
- Bitflocking, dynamic emergent behavior
- New protocols
- New interdependencies
- Homogenization
- Innovation treadmill; constant lifespan flux

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Current Landscape

- Regulatory compliance is stealing the show
- Mixing legacy and bleeding edge tech is difficult
- Logical distance between kinetic endpoint and HMI is exponentially increasing; "hyperembeddedness"
- No system is 100% isolated or 100% secure
- Researchers and hackers know all of this and more
- Nation-state quality defense is the new norm
- Sufficient motive, means and opportunity exist to take the threat seriously

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

Questions?

Non-profit. Independent. Trusted.

Patrick C Miller, President and CEO
patrick@energysec.org
503-446-1212
@PatrickCMiller

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy