Setting the Standard for Automation™

Wireless Ethernet: Technologies and Security for the Water Industries

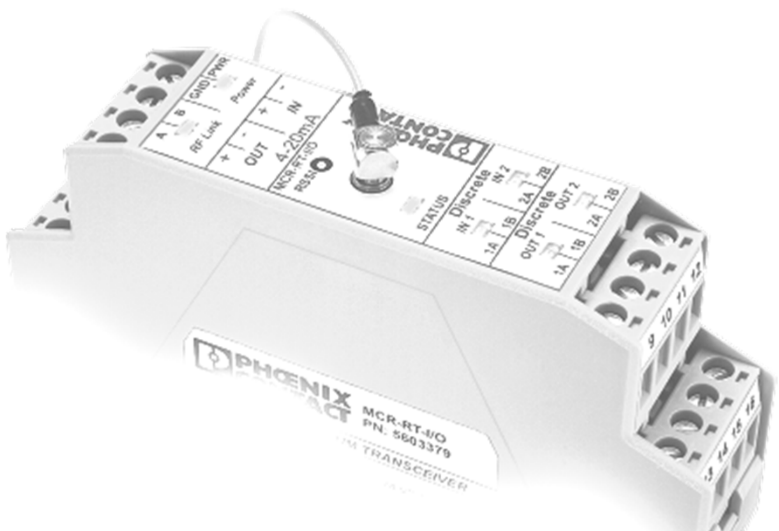
John Lavoie, Mike Nager
Phoenix Contact, Inc.

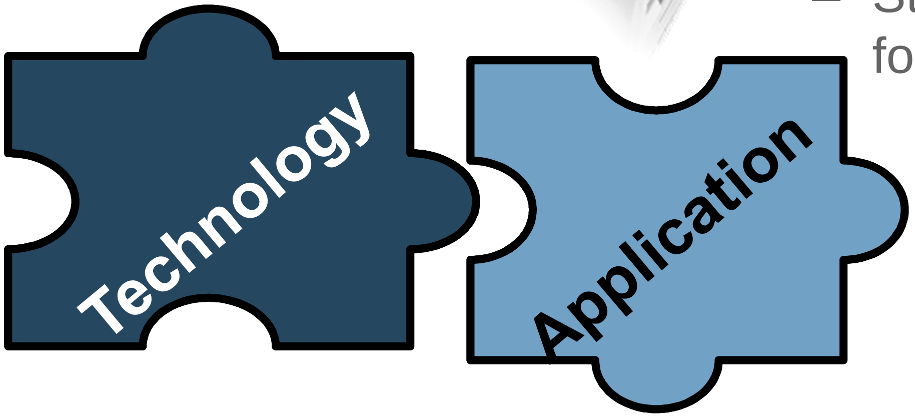
5th ISA Water/Wastewater Automatic Controls Division Symposium (WWAC)
3-5, Orlando, Florida

Agenda

- Why Wireless
- Wireless Ethernet Technologies
  - Differences and how to chose
- Securing Wired/Wireless Communications
- Applications

Using Wireless in Industrial Applications





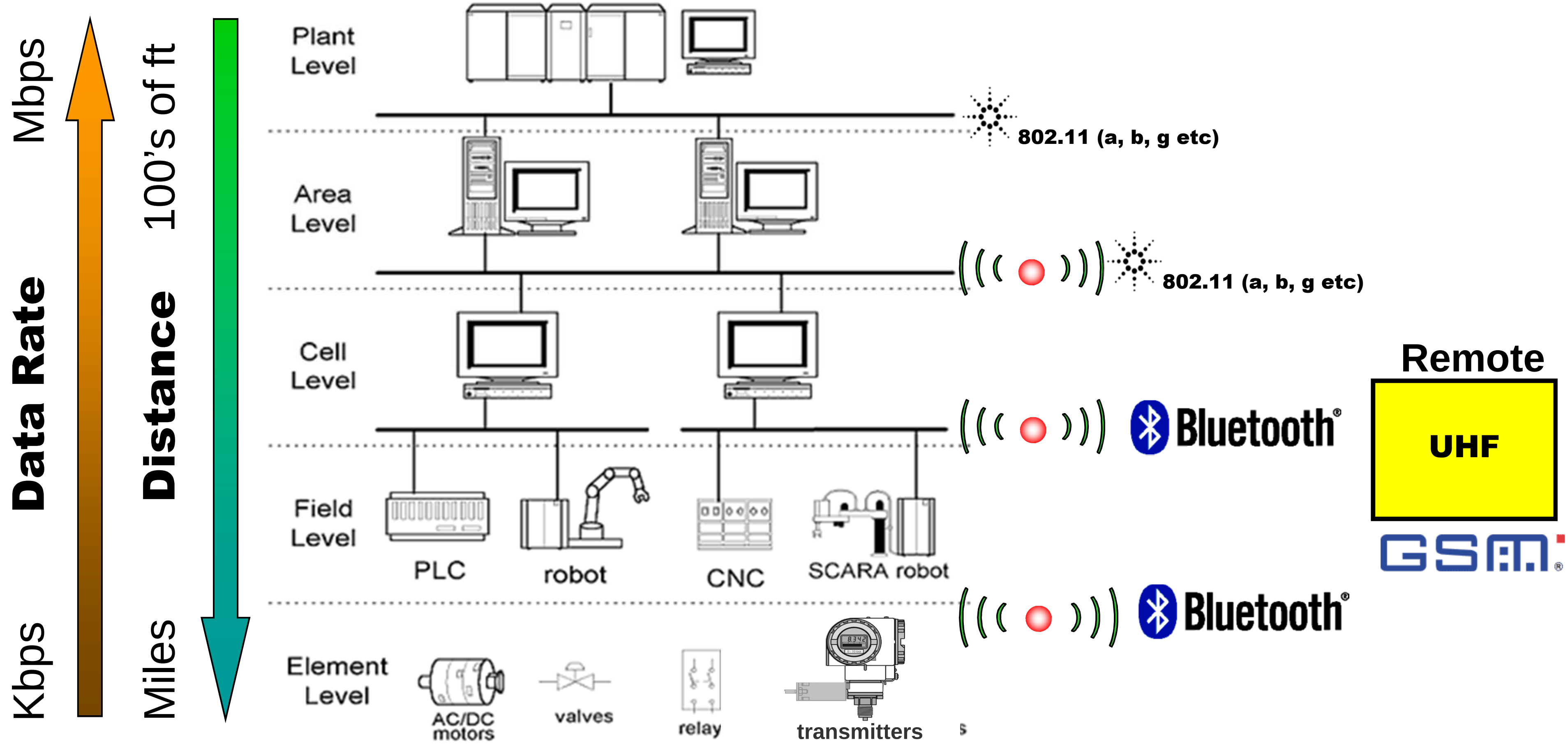
- Wireless has become a standard in everyday life
  - Commercially, for convenience
  - Industrially, to solve problems
- Developments in industrial wireless are accelerating very rapidly
  - New technologies are in development
  - Standards are being created specifically for industry

Benefits of Wireless in Industrial Applications

- Lower installation costs (than wired solutions)
  - Labor savings
  - Permits and delays
  - Material cost
- Faster installation vs. traditional cabling
- More application flexibility
- Offer an alternative to wiring harnesses and slip rings that could wear out on moving devices
- Provide monitoring and control of “stranded” devices in remote locations

Phoenix Contact Industrial Wireless Communication Solutions

(Application Space Matrix)



Proprietary wireless

Bluetooth

Wi-Fi standards 802.11 (a, b, g etc)

UHF — UHF Wireless

GSM

Wireless Ethernet Technologies

Bluetooth

- **Short** distances (Typical <300')
- Fastest update times
- Data rates up to 3Mbps
- Ethernet, Serial, or Wire-in Wire-Out I/O

WLAN (Wi-fi / 802.11)

- **Medium** distances (Typical 1000-3000')
- Fast update times
- Data rates up to 54Mbps
- Ethernet, Serial, or I/O

Wireless Ethernet Technologies

MOTR-9™

Proprietary Wireless (Trusted Wireless)

- **Long** distances (Typical 1-3 Miles)
- Slower update times
- Data rates up to 500Kbps
- Ethernet, Serial, or I/O

GSM®

Cellular (GSM/CDMA/2G/3G)

- **Very Long** distances (Around the world)
- Slowest update times
- Data rates up to 14.4Mbps
- Ethernet, Serial, or I/O

Different Layers of Wireless Security

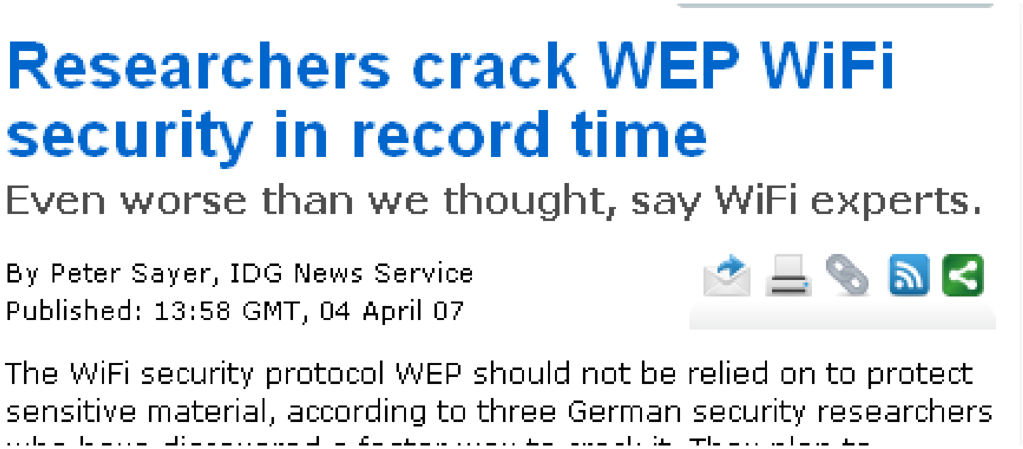
- **Encryption** takes “plane” text and makes it unreadable while flowing over a network

- **Authentication** ensures the devices on a network are suppose to be there

- Attacks can be preformed at various levels of a network. To combat attacks a network must contain high levels of both encryption and authentication

Wi-Fi (802.11a/b/g/n) Security Encryption

- WEP (Wired Equivalent Privacy)
  - Publicly known to be unsecured and hackable.
  - Not a suitable form of Encryption
  - Hack time 1-2 minutes (or less)



Researchers crack WEP WiFi security in record time

Even worse than we thought, say WiFi experts.

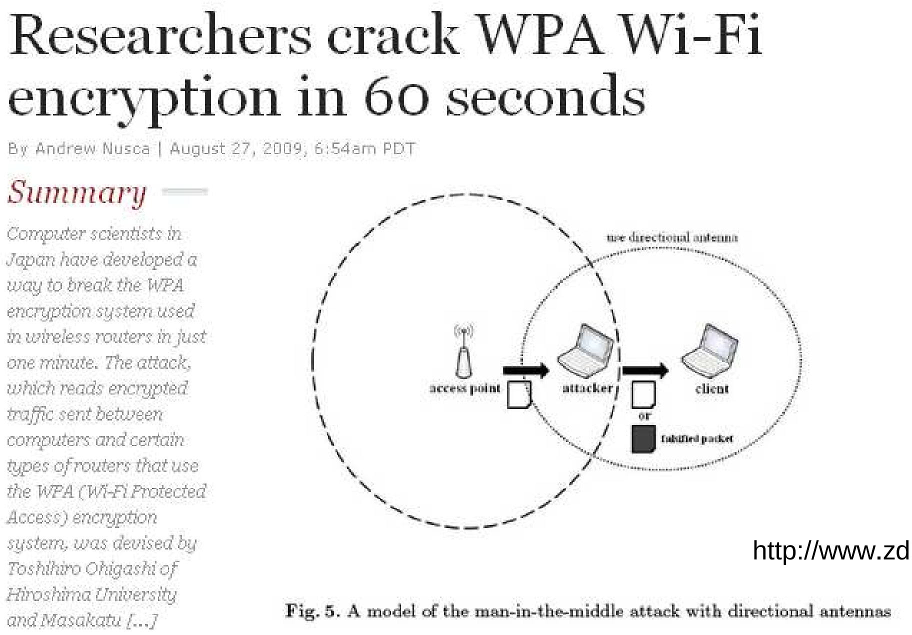
By Peter Sayer, IDG News Service
Published: 13:58 GMT, 04 April 07

The WiFi security protocol WEP should not be relied on to protect sensitive material, according to three German security researchers who have discovered a faster way to crack it. They plan to

http://news.techworld.com/security/8456/researchers-crack-wep-wifi-security-in-record-time/

Wi-Fi (802.11a/b/g/n) Security Encryption

- WPA (Wi-Fi Protected Access)
  - PSK (Pre-Shared Key) with TKIP
    - Susceptible to attack
  - PSK (Pre-Shared Key) with AES
    - Considered fairly secure



Researchers crack WPA Wi-Fi encryption in 60 seconds

By Andrew Nusca | August 27, 2009, 6:54am PDT

Summary

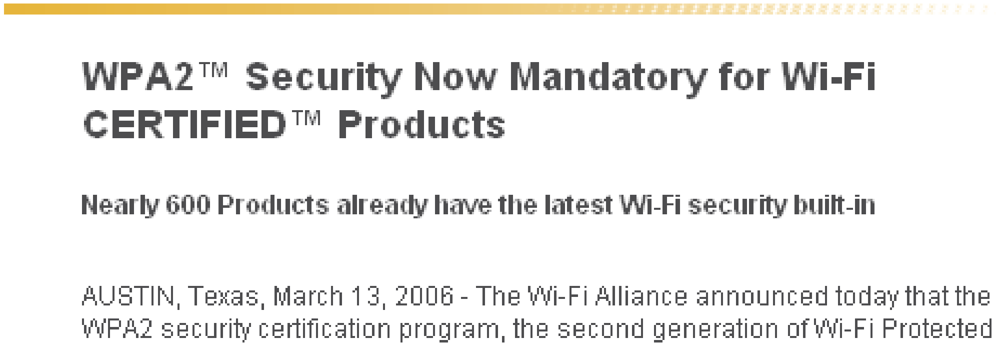
Computer scientists in Japan have developed a way to break the WPA encryption system used in wireless routers in just one minute. The attack, which reads encrypted traffic sent between computers and certain types of routers that use the WPA (Wi-Fi Protected Access) encryption system, was devised by Toshihiro Ohigashi of Hiroshima University and Masakatu [...]

Fig. 5. A model of the man-in-the-middle attack with directional antennas

http://www.zdnet.com/blog/btl/researchers-crack-wpa-wi-fi-encryption-in-60-seconds/23384

Wi-Fi (802.11a/b/g/n) Security

- WPA2 (Wi-Fi Protected Access 2)
  - PSK (Pre-Shared Key) with AES
    - Considered secure
  - Enterprise mode offers the greatest level of security although this requires additional hardware
  - Now required for a device to be considered Wi-Fi Certified



WPA2™ Security Now Mandatory for Wi-Fi CERTIFIED™ Products

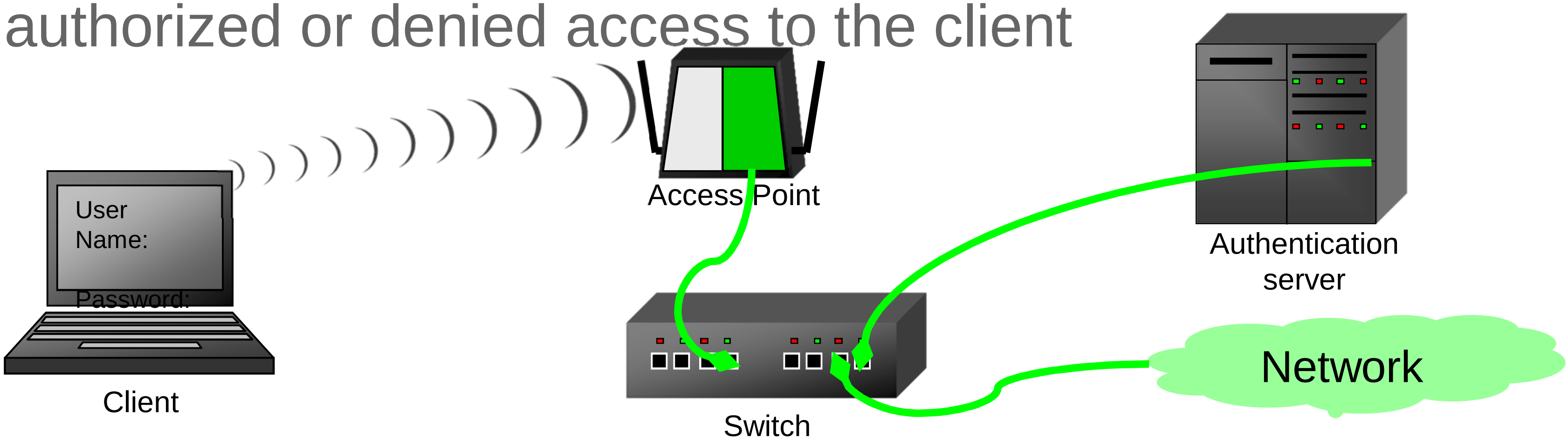
Nearly 600 Products already have the latest Wi-Fi security built-in

AUSTIN, Texas, March 13, 2006 - The Wi-Fi Alliance announced today that the WPA2 security certification program, the second generation of Wi-Fi Protected

http://www.wi-fi.org/news_articles.php?f=media_news&news_id=16

Wi-Fi (802.11a/b/g/n) Security Enterprise Level

- Client tries to join the network
- Using specific port defined by 802.1x the EAP is used to talk to the Authentication Server
  - Because of the 802.1x port protocol nothing can see the authentication process and the client can see nothing on the network
- Handshaking occurs and the Authentication server either authorized or denied access to the client



Wireless Security is only half the battle

- Wireless security is important however the same principles used for a physical networks should also be applied to wireless networks. This will further enhance the security of the overall network.

Why Networks Need Security

Threats

- Network overload by technical defects, broadcast storms
  - Automation gear is optimized to handle certain traffic
  - Easily disrupted by floods or other attacks
- Unauthorized or accidental access or equipment
  - Engineer connects to wrong PLC IP address.
- Malware (Worms)
  - Unintended introduction and dissemination of malware
  - Intended, targeted attacks from inside and outside: sabotage, espionage, white-collar crime, cyber terrorism

Why Networks Need Security - Risks

Potential Damages (Risks)

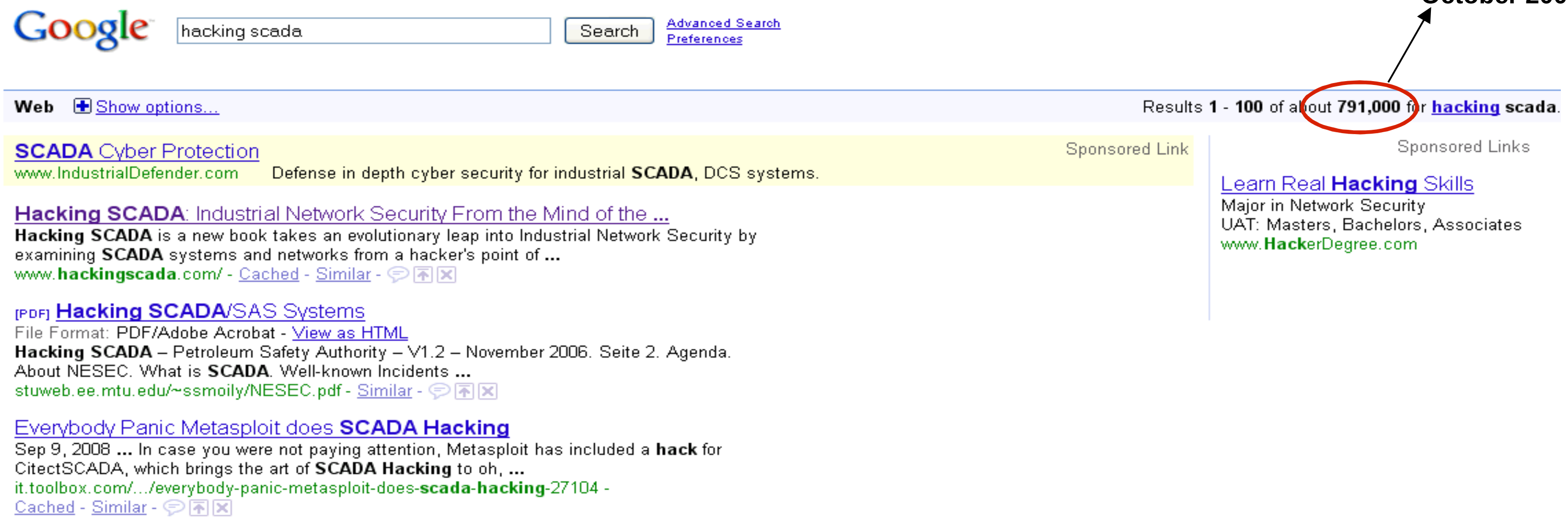
- Loss of production – Time and $$$
- Damage caused to health and environment
- Loss of intellectual property (process knowledge and data)
- Loss of compliance
  - NERC
  - FDA
  - Water/WasteWater coming soon
- Damage to corporate image

The Need for Security – Control Network

- Not nearly the visibility or urgency as in IT world
- 3 main reasons
  - Many “plant folk” consider their equipment impervious to attacks or an **unlikely target** for a hacker or that hacking their stuff is **difficult to do**.
  - Many neglect the fact they are now connected to other networks
  - Many rely on IT “to handle that sort of thing”
- Many challenges in securing control networks vs IT network
  - E.g. longer life-cycles, harsh environmental requirements
  - NTARS – “Never Touch A Running System”
- Tools and know-how to hack control systems becoming easier to obtain ☹

Cyber Security problem is growing

- Hacks, attacks, broadcast storms, etc. happen every day.
- Not just an IT problem anymore
- Inter-connectedness has a lot of plusses, but security must be addressed.
- Sophistication of attacks are rising while Expertise needed to pull of an attack is dropping



October 2009

Results **1** - **100** of about **791,000** for **hacking scada**.

SCADA Cyber Protection
www.IndustrialDefender.com Defense in depth cyber security for industrial **SCADA**, DCS systems.
Sponsored Link

Hacking SCADA: Industrial Network Security From the Mind of the ...
Hacking SCADA is a new book takes an evolutionary leap into Industrial Network Security by examining **SCADA** systems and networks from a hacker's point of ...
www.**hackingscada**.com/ - Cached - Similar -

[PDF] **Hacking SCADA**/SAS Systems
File Format: PDF/Adobe Acrobat - View as HTML
Hacking SCADA – Petroleum Safety Authority – V1.2 – November 2006. Seite 2. Agenda. About NESEC. What is **SCADA**. Well-known Incidents ...
stuweb.ee.mtu.edu/~ssmoily/NESEC.pdf - Similar -

Everybody Panic Metasploit does **SCADA Hacking**
Sep 9, 2008 ... In case you were not paying attention, Metasploit has included a **hack** for CitectSCADA, which brings the art of **SCADA Hacking** to oh, ...
it.toolbox.com/.../everybody-panic-metasploit-does-**scada-hacking**-27104 -
Cached - Similar -

Sponsored Links

Learn Real **Hacking** Skills
Major in Network Security
UAT: Masters, Bachelors, Associates
www.**Hacker**Degree.com

Attacks are happening – including in W/WW Industry

- Disgruntled employee and Dirty water
- Recently fired employee at an Australian Waste Water facility connects into *unsecured* Access Point
- Using knowledge of the SCADA system he helped design, releases 264,000 gallons of sewage into rivers
- Does this over 3 weeks. First 2.5 weeks, nobody knew ☹
- Took advantage of poor security (Wireless Access point) and his knowledge of the application to Gain System Control
- BTW 264,000 gallons is more than 35000 cubic feet, i.e. a football field covered in 9 inches

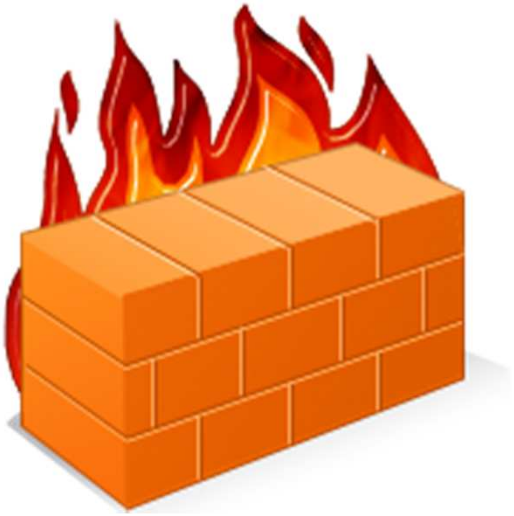
http://www.gao.gov/new.items/d04140t.pdf

So what can you do???

- **Take control of the situation**
  - Yes – It is IT's job to protect "the network" but…
  - Everyone has a role to play
  - Anyone can do their part
  - Somebody needs to take the initiative
  - Or Nobody will be able to work?
  - In many situations IT has a *bad* relationship with "the plant guys"
    - Don't cut off your nose to spite your face

So what can you do???

- **Defend your network:**
  - Firewall to limit traffic both into and out of your network
  - Segment your control network from IT networks and other control networks
  - Protect against common attacks such as Broadcast Storms, Spoofing and Denial of Service
  - If customer still insists “IT takes care of this” ask when was the last audit?
  - Make sure “Remote Access” is “Secure Access”



So what can you do???

- **Control Who Has Access**
  - Technicians, vendors, etc. may have a valid need for access to some equipment
  - That access should not be eternal and all powerful!
  - When they leave (voluntary or otherwise) revoke their accounts
  - Change shared passwords they may know
- **Use common sense:**
  - Change passwords from default values
  - Be cautious what you download from the Net (and on what PC you download it)

So what can you do???

- **Defense in Depth**
  - Multiple diverse layers of protection are better than a single monolithic one.
  - Easier to be granular and specific when in control over your own access rules
  - This means one big firewall isn't good enough!
  - "Great Wall of China" model doesn't work for network security. One breach destroys a dynasty.