

SCADA

Fear, Uncertainty, and the Digital Armageddon

Presented By Morgan Marquis-Boire

© 2008 Security-Assessment.com

- Hi, My Name is Morgan

© 2007 Security-Assessment.com

- Hi, My Name is Morgan
- I’m a security guy



© 2007 Security-Assessment.com

- Hi, My Name is Morgan
- I’m a security guy
- Security-Assessment.com



© 2007 Security-Assessment.com

- Security-Assessment.com
  - Independent security consultancy; no sales, no products, no fixing the things we break
  - NZ's largest & most experienced security team
  - Experienced with large, critical networks
    - Banks, airlines, government, telco and utility
  - Paid to think like hackers, and break things like hackers

© 2007 Security-Assessment.com

- So What's a SCADA and where can I get one?
  - What is it?
  - Why is it so hip right now?

© 2007 Security-Assessment.com

- SCADA - Supervisory Control and Data Acquisition
  - There is a tendency by the media to refer to all industrial control systems (ICS) as SCADA



© 2007 Security-Assessment.com

- SCADA - Supervisory Control and Data Acquisition
  - There is a tendency by the media to refer to all industrial control systems (ICS) as SCADA
  - SCADA systems support processes that manage water supply and treatment plants
  - Electrical power distribution and transmission
  - Operate chemical and nuclear plants
  - HVAC systems – Heating, Ventilation, Air Conditioning
  - Traffic Signals
  - Mass transit systems
  - Et al.



© 2007 Security-Assessment.com

- Real World Examples
  - Accident
  - Worm Outbreak
  - Sabotage
  - Disgruntled Ex-employee
- These sound familiar?

© 2007 Security-Assessment.com

- When Good SCADA Goes SERIOUSLY WRONG
  - “About 3:28 p.m., Pacific daylight time, on June 10, 1999, a 16-inch-diameter steel pipeline owned by Olympic Pipe Line Company ruptured and released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1.5 hours after the rupture, the gasoline ignited and burned approximately 1.5 miles along the creek. Two 10-year-old boys and an 18-year-old young man died as a result of the accident. Eight additional injuries were documented. A single-family residence and the city of Bellingham's water treatment plant were severely damaged. As of January 2002, Olympic estimated that total property damages were at least $45 million.”

© 2007 Security-Assessment.com



© 2007 Security-Assessment.com

I was promised some FUD

- This was an accident
  - “The Olympic Pipeline SCADA system consisted of Teledyne Brown Engineering SCADA Vector software, version 3.6.1., running on two Digital Equipment Corporation (DEC) VAX Model 4000-300 computers with VMS operating system Version 7.1. In addition to the two main SCADA computers (OLY01 and 02), a similarly configured DEC Alpha 300 computer running Alpha/VMS was used as a host for the separate Modisette Associates, Inc., pipeline leak detection system software package.”

© 2007 Security-Assessment.com



© 2007 Security-Assessment.com



© 2007 Security-Assessment.com

I was promised some FUD

- This was an accident
  - “The massive fireball sends a plume of smoke 30,000 feet into the air, visible from Anacortes to Vancouver, B.C., Canada.”

© 2007 Security-Assessment.com

- Digruntled Employee
  - Vitek Boden, in 2000, was arrested, convicted and jailed because he released millions of liters of untreated sewage using his wireless laptop. It happened in Maroochy Shire, Queensland, as revenge against his a former employer.
  - http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

© 2007 Security-Assessment.com

- Digruntled Employee
  - "Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency.

    The Maroochydore District Court heard that 49-year-old Vitek Boden had conducted a series of electronic attacks on the Maroochy Shire sewage control system after a job application he had made was rejected by the area's Council. At the time he was employed by the company that had installed the system. Boden made at least 46 attempts to take control of the sewage system during March and April 2000.

    On 23 April, the date of Boden's last hacking attempt, police who pulled over his car found radio and computer equipment.

    Later investigations found Boden's laptop had been used at the time of the attacks and his hard drive contained software for accessing and controlling the sewage management system.

© 2007 Security-Assessment.com

I was promised some FUD

- Worm Attack
  - "In August 2003 Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours."

    NIST, Guide to SCADA
  - Slammer worm crashed Ohio nuke plant network – Kevin Poulson

    http://www.securityfocus.com/news/6767

© 2007 Security-Assessment.com

- Worm Attack
  - “The Slammer worm entered the Davis-Besse plant through a circuitous route. It began by penetrating the unsecured network of an unnamed Davis-Besse contractor, then squirmed through a T1 line bridging that network and Davis-Besse's corporate network. The T1 line, investigators later found, was one of multiple ingresses into Davis-Besse's business network that completely bypassed the plant's firewall, which was programmed to block the port Slammer used to spread.”

© 2007 Security-Assessment.com

- Sabotage
  - Thomas C. Reed, Ronald Regan's Secretary, described in his book "At the abyss" how the U.S. arranged for the Soviets to receive intentionally flawed SCADA software to manage their natural gas pipelines. "The pipeline software that was to run the pumps, turbines, and values was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds." A 3 kiloton explosion was the result, in 1982 in Siberia.
- http://www.themoscowtimes.ru/stories/2004/03/18/014.html

© 2007 Security-Assessment.com

- Other incidents
  - In 1992, a former Chevron employee disabled it's emergency alert system in 22 states. This wasn't discovered until an emergency did not raise the appropriate alarms
  - In 1997, a teenager broke into NYNEX and cut off Worcester Airport in Massachusetts for 6 hours by affecting ground and air communications
  - In 2000 the Russian government announced that hackers had managed to control the world's largest natural gas pipeline (Gazprom)
  - In 2003, the east coast of America experienced a blackout. While the Blaster worm was not the cause, many related systems were found to be infected
  - Computers and manuals seized in Al Qaeda (allegedly) training camps were full of SCADA information related to dams and other such structures

© 2007 Security-Assessment.com

- Other incidents – real or otherwise
  - "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."

    ---CIA "Senior Analyst" Tom Donahue – Jan 2008

© 2007 Security-Assessment.com

- Other incidents – real or otherwise
  - "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."

    ---CIA "Senior Analyst" Tom Donahue – Jan 2008

© 2007 Security-Assessment.com

- Other incidents – real or otherwise
  - "Computer hackers in China, including those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of U.S. companies and government agencies, stolen proprietary information from American executives in advance of their business meetings in China, and, in a few cases, gained access to electric power plants in the United States, possibly triggering two recent and widespread blackouts in Florida and the Northeast, according to U.S. government officials and computer-security experts."

    ---National Journal Magazine – 31st May 2008

© 2007 Security-Assessment.com

- Other incidents – real or otherwise

  - "This is all so much nonsense I don't even know where to begin."

    ---Bruce Schneier – 2nd June 2008

© 2007 Security-Assessment.com

- Other incidents – real or otherwise
  - "This time, though, they've attached their tale to the most thoroughly investigated power incident in U.S. history." and "It traced the root cause of the outage to the utility company FirstEnergy's failure to trim back trees encroaching on high-voltage power lines in Ohio. When the power lines were ensnared by the trees, they tripped. [...]

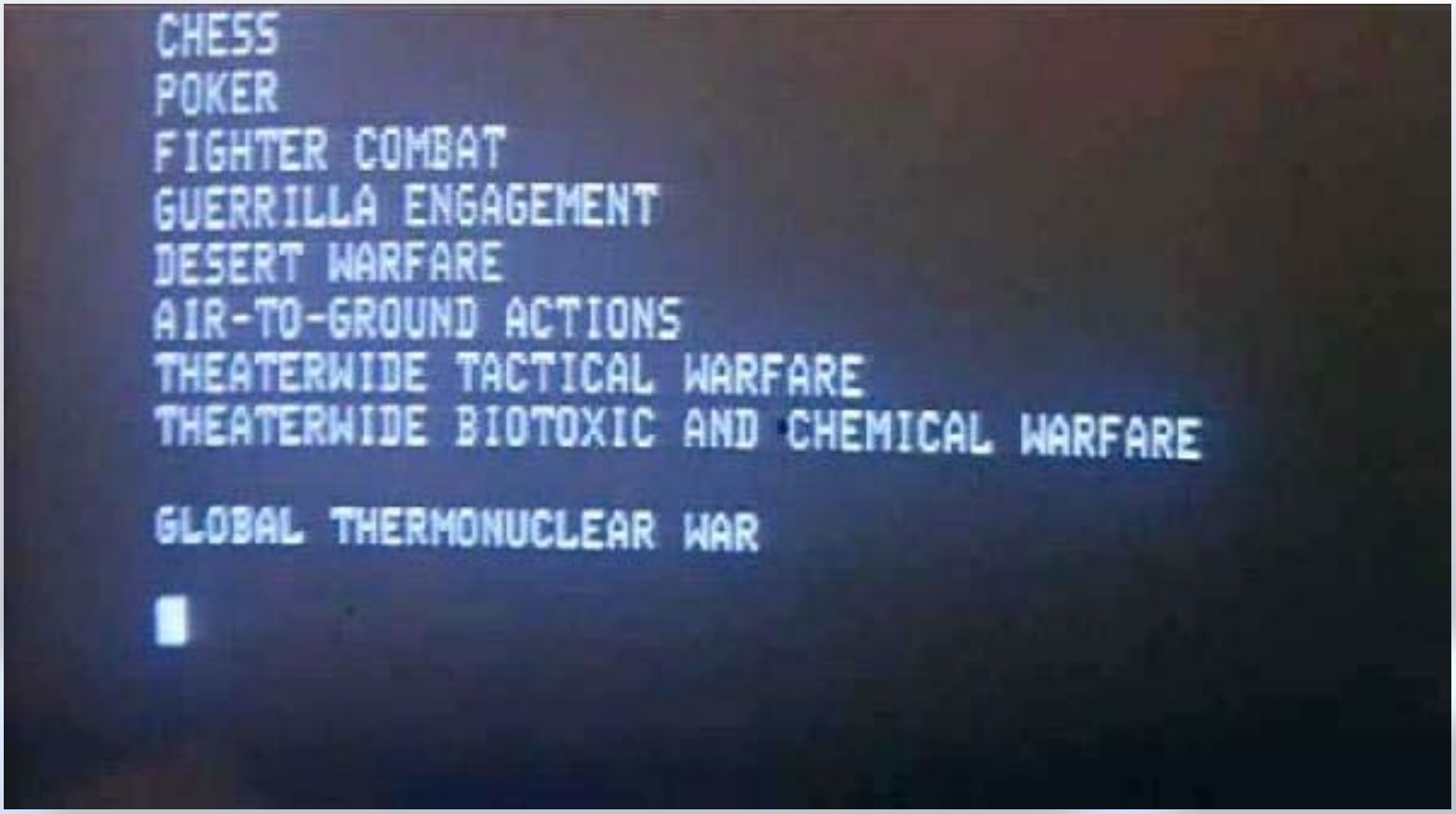
    So China...using the most devious malware ever devised, arranged for trees to grow up into exactly the right power lines at precisely the right time to trigger the cascade."

    --Wired 29th May 2008, Kevin Poulson

© 2007 Security-Assessment.com

- Security Risk defined largely by threat
  - Massive power blackout
  - Oil Refinery explosion
  - Waste mixed in with drinking water
  - Dam opens causing flooding
  - Traffic Chaos
  - Nuclear Explosion?

© 2007 Security-Assessment.com



© 2007 Security-Assessment.com

- Risk is worse these days because hacking is EASY!
  - Hacking used to involve skilled attackers performing simple attacks (password guessing, brute forcing etc)
  - Now with the rise of easily available hacking tools, complex attacks can be carried out by relatively unskilled attackers...

© 2007 Security-Assessment.com

- Risk is worse these days because hacking is EASY!
  - Hacking used to involve skilled attackers performing simple attacks (password guessing, brute forcing etc)
  - Now with the rise of easily available hacking tools, complex attacks can be carried out by relatively unskilled attackers...
- Bust out your aircrack, nmap, nessus, metasploit, wicrawl, buy yourself a Russian 0day pack and you're ready to be part of the problem...

© 2007 Security-Assessment.com

I was promised some FUD

- Where's my digital armageddon???
  - Let's watch a video then we'll have a couple of case studies

© 2007 Security-Assessment.com

O.K. too much FUD

- The digital Armageddon hasn't happened yet
  - Stories are obviously exaggerated to stir up outrage
    - Blaster did not cause the east coast power outage
    - Stories of "teenaged hackers" are frequently exaggerated
    - Chinese hackers get blamed for everything from missing beer to lost homework...
- Dire predictions have thus far been incorrect.
  - IDC named 2003 "the year of cyber-terrorism", predicting that a major cyber-terrorism event would bring the internet to its knees.

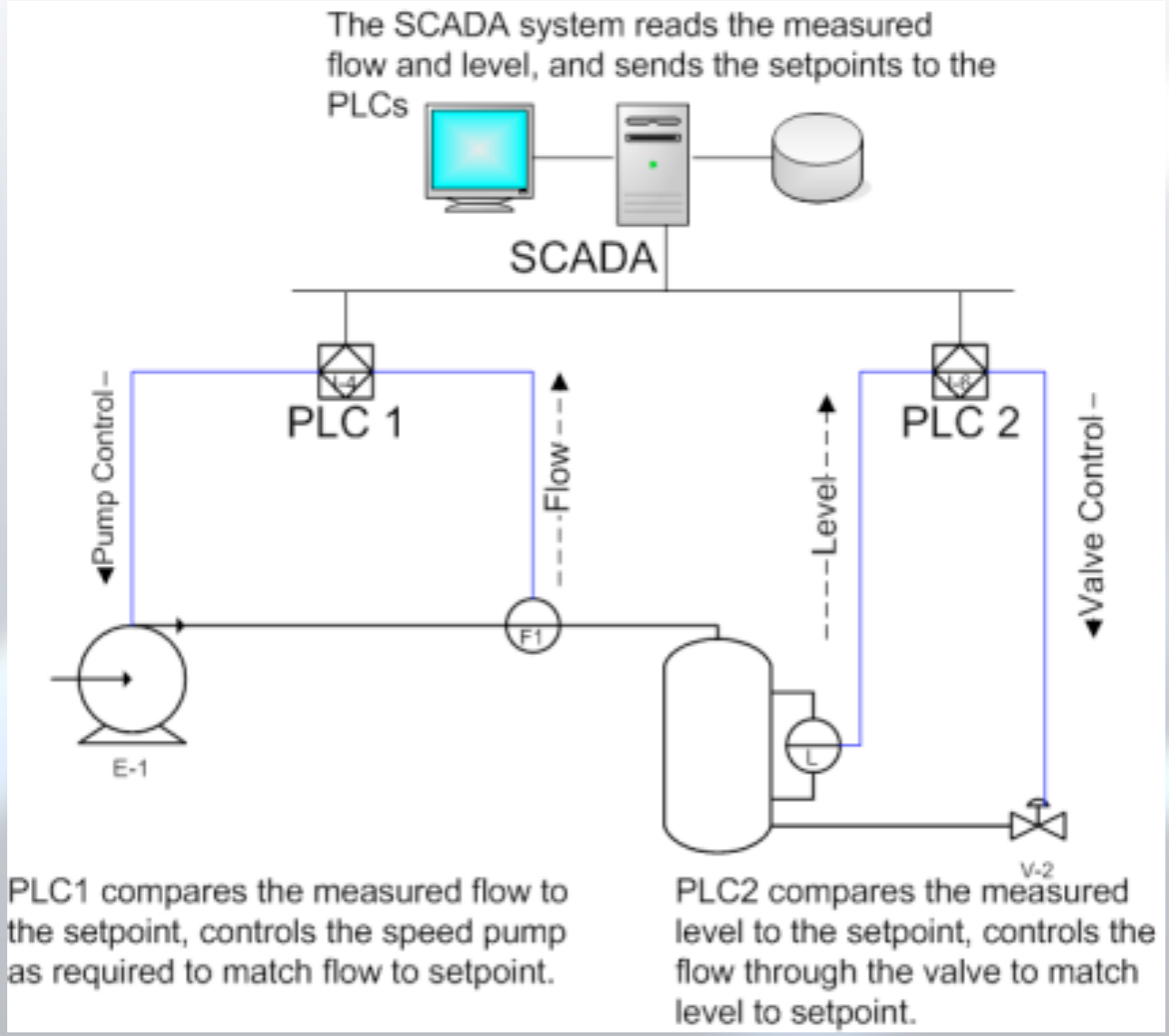
© 2007 Security-Assessment.com

- So what is it actually?
  - A SCADA system consists of central host that monitors and controls smaller Remote Terminal Units (RTUs) sprinkled throughout a plant, or in the field at key points in an electrical distribution network. The RTUs, in turn, directly monitor and control various pieces of equipment.

© 2007 Security-Assessment.com

- Components of a SCADA network – Edge Devices
  - RTU / PLC – Reads information on voltage, flow, the status of switches or valves. Controls pumps, switches, valves.
  - Most site control is performed by these devices automatically
  - Data acquisition begins at the RTU or PLC level and includes meter readings, equipment reports etc
  - Functionality is usually restricted to basic site overriding or supervisory level intervention
    - E.g. A PLC may control the flow of water through, but the SCADA system will allow an operator to set alarm conditions, change the set points for the flow etc etc

© 2007 Security-Assessment.com



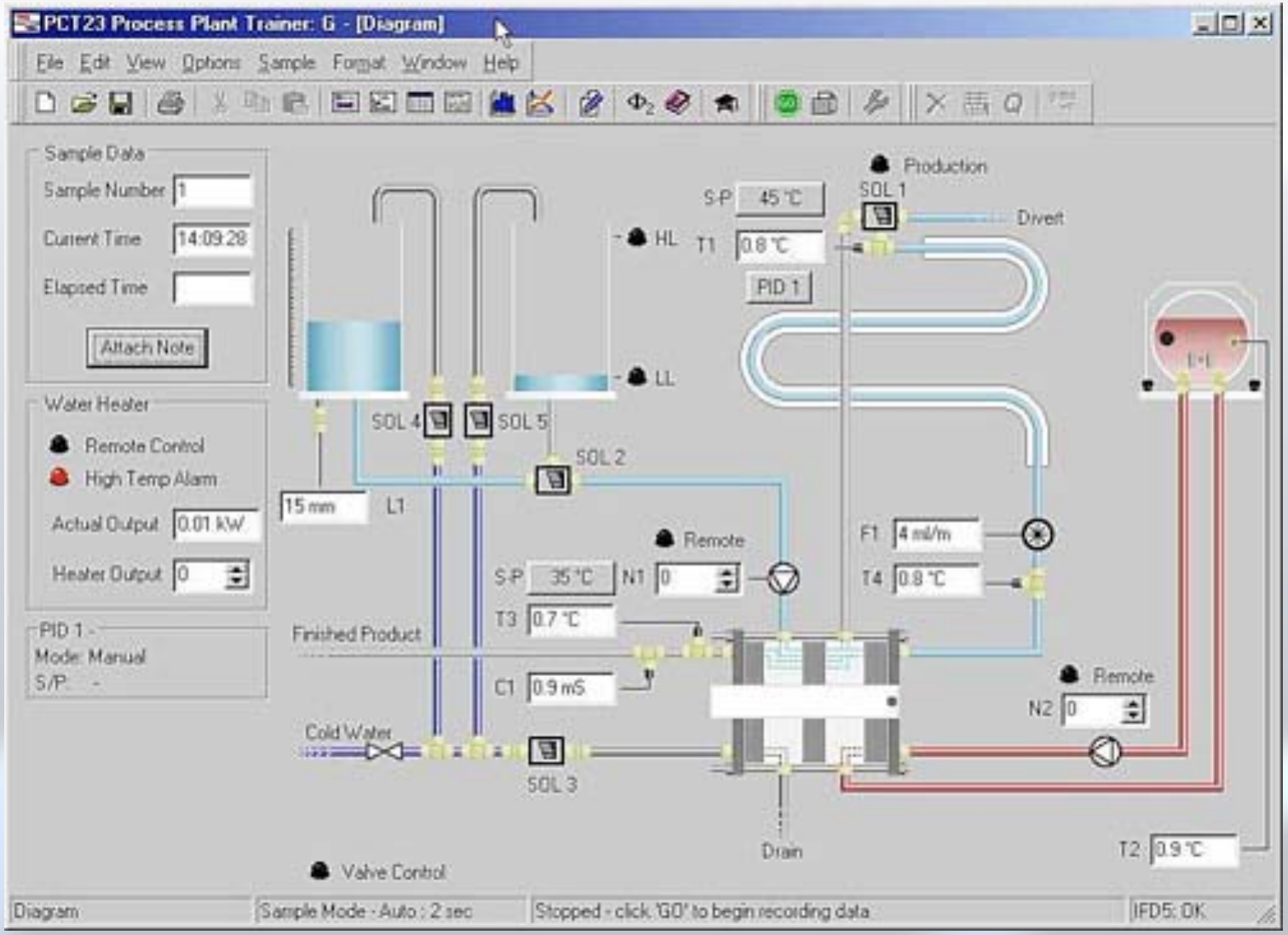
© 2007 Security-Assessment.com

- Components of A SCADA Network – Intermediate Layer
  - The “Master Station” is the servers and software responsible for communicating with the field equipment and then to the HMI software generally running on workstations
  - Data is sent from (RTU) PLCs to a Master Station where it is compiled in a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal RTU (PLC) controls
  - This may be a single computer in smaller installations or many servers in redundant clusters in larger installations
  - Today both Master Stations and HMIs are run on all major operating system platforms: UNIX, Windows, VMS etc

© 2007 Security-Assessment.com

- Components of A SCADA Network – Management Layer
  - A Human Machine Interface or HMI is the apparatus which presents process data to a human operator, and through which the human operator controls the process.
  - The HMI provides a standardized way to monitor and to control multiple remote controllers, PLCs and other control devices which would usually be distributed in a way which makes manual data gathering difficult
  - This usually takes the form of a mimic diagram. This is a schematic representation of the plant which is being controlled
  - For example, a picture of a pump connected to a pipe can show the operator that the pump is running and how much fluid it is pumping through the pipe at the moment. The operator can then switch the pump off

© 2007 Security-Assessment.com



http://www.armfield.co.uk – Industrial Food Technology

© 2007 Security-Assessment.com

- Components of a SCADA network – Communications Layer
  - This was traditionally a mix of radio and direct serial or modem connections
  - Equipment frequently communicated via proprietary protocols carried over something like RS-485 (multipoint serial connection)
  - This meant that those who invested in a particular hardware solution had a limited upgrade path
  - To avoid such issues open communications protocols such as DNP3.0 (over serial or IP) became increasingly popular
  - Open architecture SCADA systems allow a mix-and-match approach with different vendor's hardware
  - In the 2000s protocols such as Modbus/IP allow open interfacing

© 2007 Security-Assessment.com

- Raw Data Protocols – Modbus / DNP3
  - For serial radio links mainly, but you can run anything over anything these days, especially TCP/IP (for better or worse)
  - Reads data (measures voltage / fluid flow etc)
  - Sends commands (“flip switches!”, “starts pumps!”) / alerts (“it’s broken!”)
- High Level Data Protocols – ICCP / OCP
  - OLE for Process Control (OCP) used for intercommunication between heterogeneous hardware / software combinations allowing communication between devices originally not intended to be part of an industrial network
  - Designed to send data / commands between apps / databases
  - These protocols often bridge between office and control networks

© 2007 Security-Assessment.com

- Let’s not forget…

© 2007 Security-Assessment.com

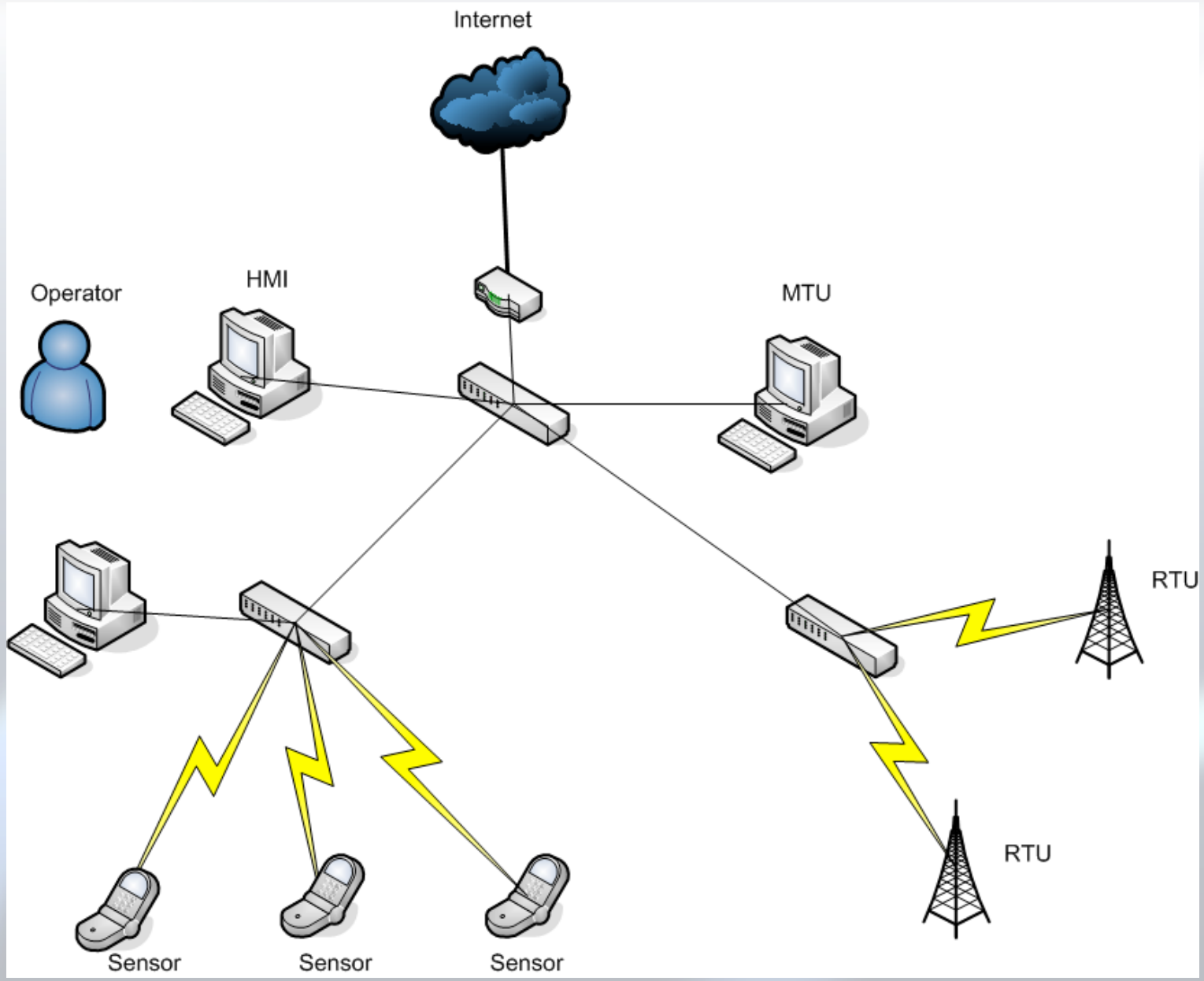
- Let’s not forget… The operator.

© 2007 Security-Assessment.com

In keeping with tradition



© 2007 Security-Assessment.com



© 2007 Security-Assessment.com

- SCADA Networks – Past and Present
  - These could be described as “primitive” when compared to most modern networks
  - Proprietary Hardware & Software (Past)
    - Manuals and procedures not widely available
    - Closed systems considered to be immune to outside threats
  - Interconnected Networks (Present)
    - Utility Networks, Corporate Networks, Internet
    - DNP3 over TCP/IP
- Modern stuff is susceptible to modern (or perhaps not so modern) attacks (SYN Flood, Ping of death)

© 2007 Security-Assessment.com

- Wonderware SuiteLink Denial of Service vulnerability

  - “One third of the world’s plants run Wonderware software solutions. Having sold more than 500,000 software licenses in over 100,000 plants worldwide...”
  - Wonderware SuiteLink Denial of Service vulnerability
  - “a malformed packet that causes a memory allocation operation (a call to new() operator) to fail returning a NULL pointer. Due to a lack of error-checking for the result of the memory allocation operation, the program later tries to use the pointer as a destination for memory copy operation, triggering an access violation error and terminating the service.”

© 2007 Security-Assessment.com

- Wonderware SuiteLink Denial of Service vulnerability
  - This was followed by a SERIOUSLY arduous process of notification and release
  - "**2008-03-03:** Core sends proof-of-concept code written in Python.
  - **2008-03-05:** Vendor asks for compiler tools required to use the PoC code.
  - **2008-03-05:** Core sends a link to http://www.python.org where a Python interpreter can be downloaded."

© 2007 Security-Assessment.com

- CitectSCADA ODBC service vulnerability
  - Citect is a fully owned subsidiary of Schneider Electric, has more than 150,000 licenses of its software sold to date.
  - Arbitrary code execution remote unauthed....!
  - “The ODBC Server component listens on port 20222/tcp by default to service requests from clients on TCP/IP networks. The application layer protocol used over TCP reads an initial packet of 4 bytes...”
  - “Due to a lack of a proper length checking of the read data, a memory copy operation that uses as destination a buffer of fixed size allocated in the stack “can be overflowed...”
  - Long filename, long parameter, malformed data. Another day, another vulnerability. Same bug. Different App.

© 2007 Security-Assessment.com

- Lots of Research Being Published
  - BlackHat Federal 2k6 – Maynor and Graham (ISS) – SCADA Security and Terrorism: We're not crying wolf.
  - Hack in the Box 2k7 – Raoul Chiesa and Mayhem – Hacking SCADA: How to 0wn Critical National Infrastructure
  - Defcon 2k7 – Ganesh Devarajan – Unraveling SCADA Protocols: Using Sulley Fuzzer
  - Petroleum Safety – Gresser – Hacking SCADA/SAS Systems
- Why is SCADA the hot topic of security?
  - The possible ramifications of a SCADA compromise are very tangible
  - Cyber-Enabled Terrorism is the new Chemical Warfare

© 2007 Security-Assessment.com

- SCADA is changing
  - From proprietary, obscure, and isolated systems
  - Towards standard, documented and connected ones

- “ It's not that these guys don't know what they are doing. Part of it is that these systems were engineered 20 years ago, and part of it is that the engineers designed these things assuming they would be isolated. But--wham!--they are not isolated anymore. ”
  - Alan Paller, director of research, SANS Institute

© 2007 Security-Assessment.com

- You can test the security of SCADA networks with what you know now
- The rest you can find on the internet
- You don't need custom tools:
  - Sulley Fuzzer, Modscan
  - Or even detailed knowledge of technologies like OPC, RTU, PLC, MODBUS
  - You will, however, need to know 802.11/a/b/g, VoIP, Windows, Unix, SMB, SQL, and various intelligence gathering techniques

© 2007 Security-Assessment.com

- You can test the security of SCADA networks with what you know now
- The rest you can find on the internet
- You don't need custom tools:
  - Sulley Fuzzer, Modscan
  - Or even detailed knowledge of technologies like OPC, RTU, PLC, MODBUS
  - You will, however, need to know 802.11/a/b/g, VoIP, Windows, Unix, SMB, SQL, and various intelligence gathering techniques
  - Old school is good school...

© 2007 Security-Assessment.com

- Radio Frequency Scanning
  - Scanners first became popular and widely available during CB Radio's heyday in the 1970s. The first scanners often had between four and ten channels and required a separate crystal for each frequency received.
  - Modern programmable scanners allow hundreds or thousands of frequencies to be entered via a keypad and stored in various 'memory banks' and can scan at a rapid rate due to modern microprocessors.
  - Scanners are often used to monitor police, fire and emergency medical services.
  - There are several free software packages which will decode various data protocols commonly sent over radio, ie POC32 for pager messages, Shipplotter for VHF maritime band

© 2007 Security-Assessment.com

- Radio Frequency Scanning
  - Many SCADA messages and alerts are sent over radio link
  - SCADA monitoring and alarm systems can generally use many different communication mechanisms
  - The pager network is a common communication mechanism due to the high availability of the pager network
  - The problem with this is that they leak too much info in clear text which is available to anyone with...

© 2007 Security-Assessment.com

- Radio Frequency Scanning
  - This cost $250NZD at Dick Smith Electronics across the road from our office – Uniden Bearcat92XLT



© 2007 Security-Assessment.com

- Radio Frequency Scanning
  - Many SCADA messages and alerts are sent over radio link
  - SCADA monitoring and alarm systems can generally use many different communication mechanisms
  - The pager network is a common communication mechanism due to the high availability of the pager network
  - The problem with this is that they leak too much info in clear text which is available to anyone with...
  - So what can information can be gathered?

© 2007 Security-Assessment.com

State of the System

```
1097727 19:58:10 14-03-08 POCSAG-4  1200  Hello, Bob, Moa SCADAlarm is active.
1097727 11:58:17 26-03-08 POCSAG-4  1200  Hello, Bob, WTP SCADAlarm Test Signal.
1066030 16:19:56 12-05-08 POCSAG-4  1200   FoxSCADA Alarm
1060526 11:08:29 18-04-08 POCSAG-4  1200  ALM 18/4/08 10:?8 Tokonui Sewer Well Pump No 1 Ph-Fail -
                                          Dial 03        6  ID= 4663
1097725 18:26:40 17-03-08 POCSAG-4  1200  ...1640950; Der Meel;3834993;South Coast;Strong smell of open sewer.;
1097725 12:01:40 18-03-08 POCSAG-4  1200  3880054 IPS Inlet Pumps One Or More Faulty Alarm
1069115 12:01:46 17-03-08 POCSAG-4  1200  Eastbourne St Water Fluoride Disabled 17 12:01:02 Ref=0004
1069115 15:26:40 17-03-08 POCSAG-4  1200  Whi / Esk Source Whi Pmp Lockout (Sw 17 15:25:41 Ref=0003
1069115 11:21:46 17-03-08 POCSAG-4  1200  Eastbourne St Water Dosing No 3 Fault On 17 11:21:02 Ref=0004
1112455 14:06:26 06-05-08 POCSAG-4  1200  ALM 6/5/08 14:01 Dovedale Rural Dovedale Booster
                                          Chlorine Injector Pump Not in Auto, dial 54     8 Alarm ID = 187712
1069115 09:12:40 26-03-08 POCSAG-4  1200  Esk Ridge Pumps Modbus Offline 26 08:52:12 Ref=0006
```

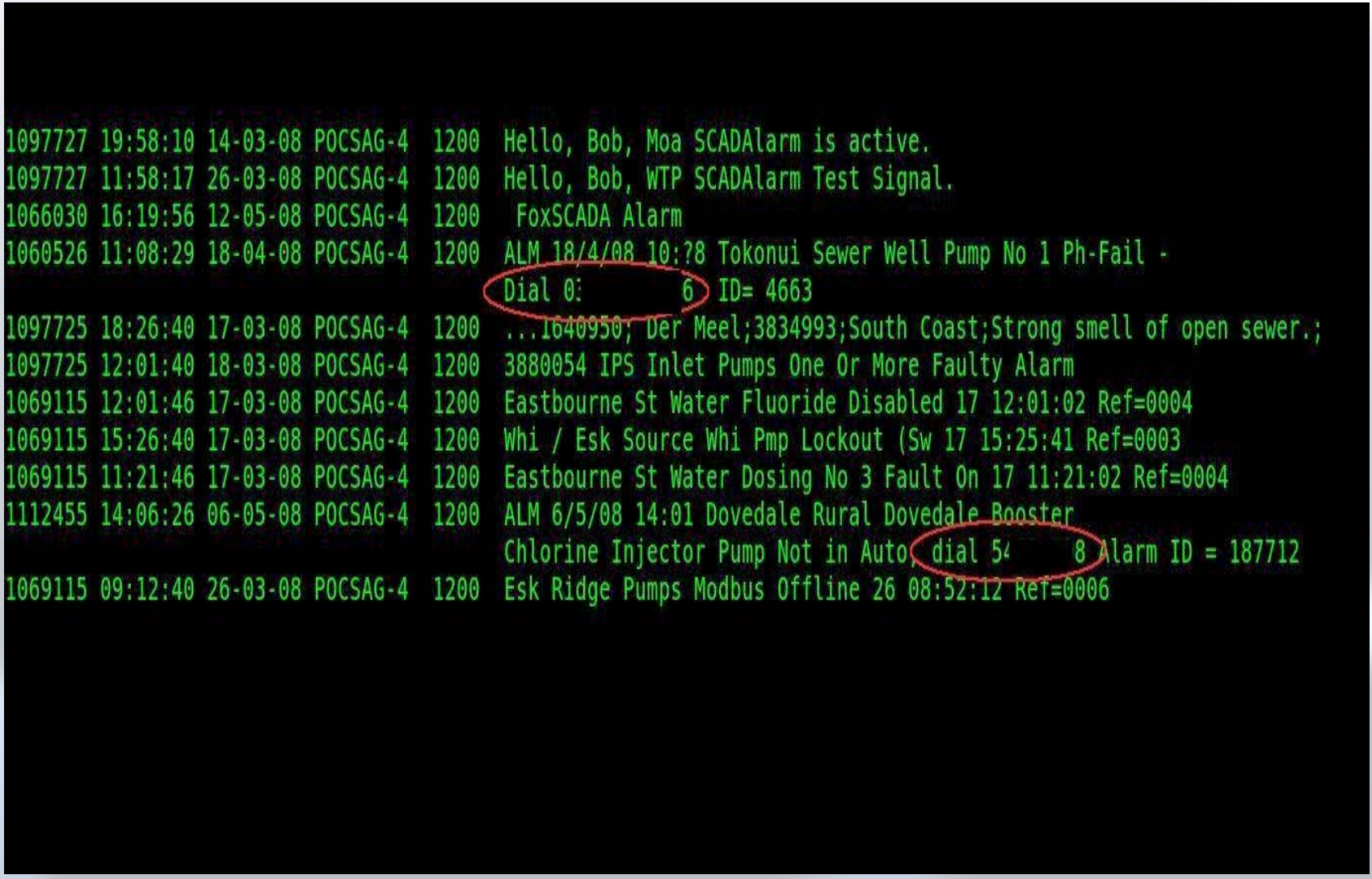
© 2007 Security-Assessment.com

Software Used

```
1097727 19:58:10 14-03-08 POCSAG-4  1200  Hello, Bob, Moa SCADAlarm is active.
1097727 11:58:17 26-03-08 POCSAG-4  1200  Hello, Bob, WTP SCADAlarm Test Signal.
1066030 16:19:56 12-05-08 POCSAG-4  1200   FoxSCADA Alarm
1060526 11:08:29 18-04-08 POCSAG-4  1200  ALM 18/4/08 10:?8 Tokonui Sewer Well Pump No 1 Ph-Fail -
                                          Dial 0:       :6  ID= 4663
1097725 18:26:40 17-03-08 POCSAG-4  1200  ...1640950; Der Meel;3834993;South Coast;Strong smell of open sewer.;
1097725 12:01:40 18-03-08 POCSAG-4  1200  3880054 IPS Inlet Pumps One Or More Faulty Alarm
1069115 12:01:46 17-03-08 POCSAG-4  1200  Eastbourne St Water Fluoride Disabled 17 12:01:02 Ref=0004
1069115 15:26:40 17-03-08 POCSAG-4  1200  Whi / Esk Source Whi Pmp Lockout (Sw 17 15:25:41 Ref=0003
1069115 11:21:46 17-03-08 POCSAG-4  1200  Eastbourne St Water Dosing No 3 Fault On 17 11:21:02 Ref=0004
1112455 14:06:26 06-05-08 POCSAG-4  1200  ALM 6/5/08 14:01 Dovedale Rural Dovedale Booster
                                          Chlorine Injector Pump Not in Auto, dial 5     8 Alarm ID = 187712
1069115 09:12:40 26-03-08 POCSAG-4  1200  Esk Ridge Pumps Modbus Offline 26 08:52:12 Ref=0006
```

© 2007 Security-Assessment.com

Dial-Up Numbers for System Control???????



© 2007 Security-Assessment.com

- Information Leaking
  - "SCADAlarm™ alarm and event-notification software provides a telecommunications link to industrial automation software systems. Based on the Microsoft® Windows® operating system, SCADAlarm enables real-time intelligent alarm and event notification, data acquisition capabilities and remote control. SCADAlarm provides an open, easy to configure interface for constant monitoring and communication with processes regardless of location." – http://us.wonderware.com/products/scadal
  - "Users can listen to and acknowledge alarms, change set points, hear exact values of variables, and operate equipment via telephone from remote locations, saving valuable time and money."



© 2007 Security-Assessment.com

- Information Leaking
  - SCADAlarm provides an IVR SCADA control system
  - This is an invaluable attack vector. Remote access to control software via the telephone networks allows manipulation of a SCADA network from the safety of an attackers bedroom
  - Authentication (if enabled) is done via caller ID
  - Modern VoIP techniques allow relatively trivial caller ID spoofing making this reasonably trivial to bypass

© 2007 Security-Assessment.com

- Information Leaking
  - SCADAlarm provides an IVR SCADA control system
  - This is an invaluable attack vector. Remote access to control software via the telephone networks allows manipulation of a SCADA network from the safety of an attackers bedroom
  - Authentication (if enabled) is done via caller ID
  - Modern VoIP techniques allow relatively trivial caller ID spoofing making this reasonably trivial to bypass
  - Broadcasting in clear-text over radio the number of the system to dial for remote control of your SCADA systems seems like a bad idea...
  - What else can be found via the Plain Old Telephone System???

© 2007 Security-Assessment.com

- War-Dialing
  - The ancient art of dialing lots of numbers to see what's on the other end
  - The name for this technique originated in the 1983 film WarGames. In the film, the protagonist programs his computer to dial every telephone number in Sunnyvale, CA in order to find other computer systems.
  - Traditionally numbers are dialed in large blocks in order to enumerate computers, modems, and other systems



© 2007 Security-Assessment.com

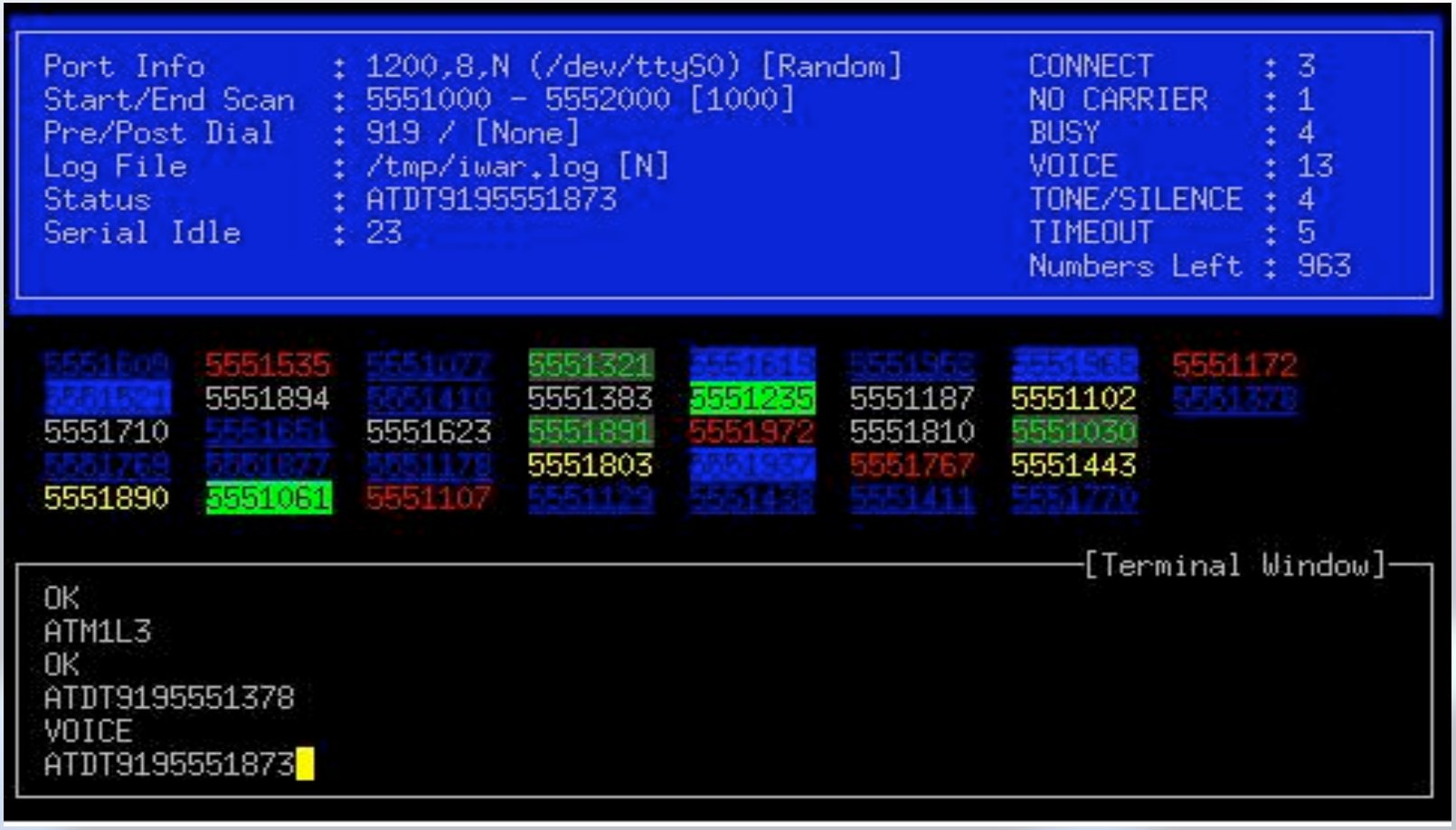
- War-Dialing
  - There are several free software solutions which can be used to perform war-dialing for intelligence gathering purposes
  - Tone-Loc – The original war-dialer
  - THC Scan – written by Van Hauser. Scans for carriers, tones and faxes. Hard to configure with multiple modems
  - Next Generation War Dialing

© 2007 Security-Assessment.com

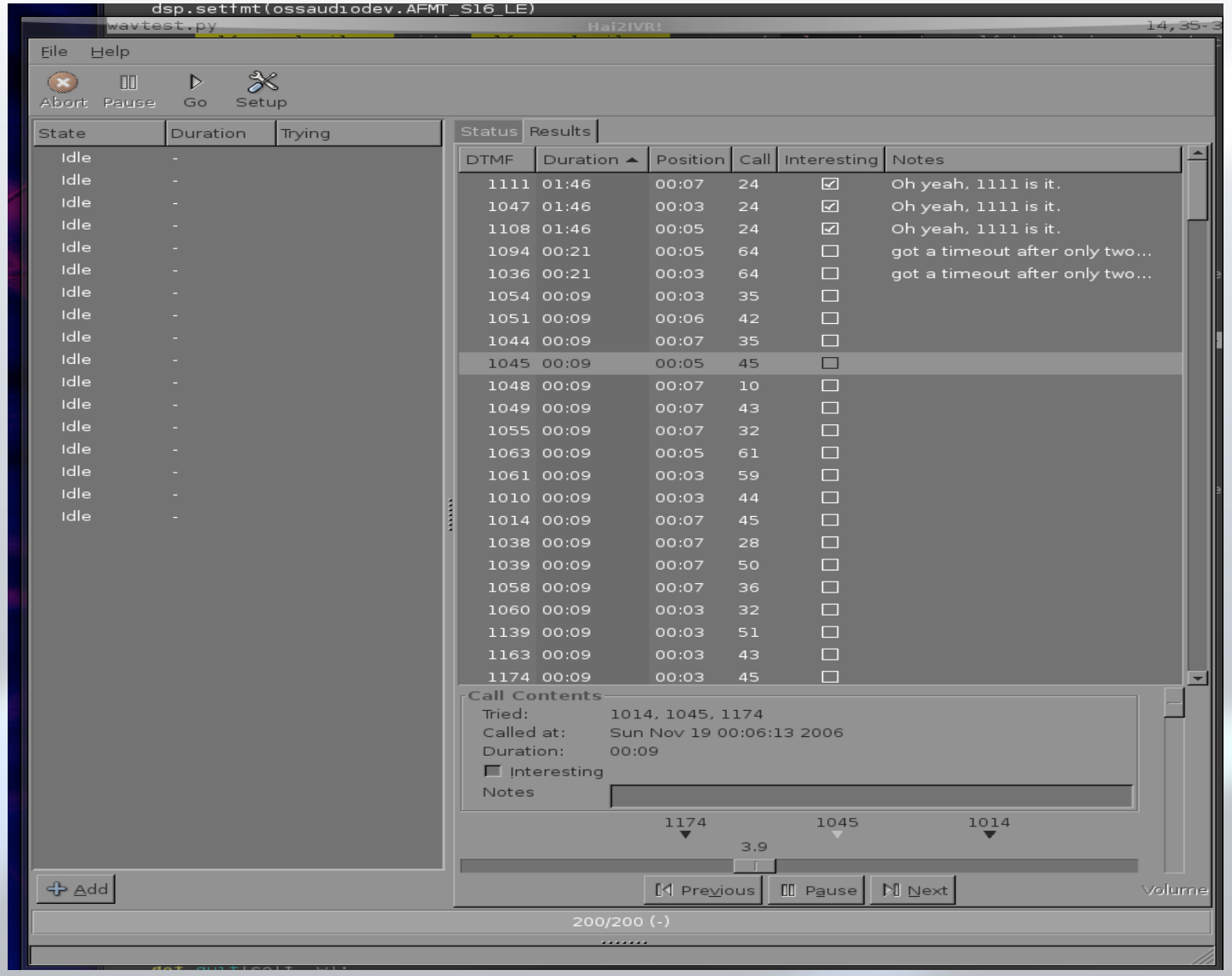
- War-Dialing
  - There are several free software solutions which can be used to perform war-dialing for intelligence gathering purposes
  - Tone-Loc – The original war-dialer
  - THC Scan – written by Van Hauser. Scans for carriers, tones and faxes. Hard to configure with multiple modems
  - Next Generation War Dialing – VOIP
    - iWAR - http://www.softwink.com/iwar/
    - Hai2IVR – http://storm.net.nz/projects/22

© 2007 Security-Assessment.com

- iWar in standard serial mode dialing one number at a time, detecting carriers, recording and checking banners.



© 2007 Security-Assessment.com



© 2007 Security-Assessment.com

- And the results????

© 2007 Security-Assessment.com

- And the results????
- Direct un-authed connection to SCADA systems? Surely not...

© 2007 Security-Assessment.com

```
CONNECT 1200

OAS Heat Computer
324-6 & 328-30 EAST 19      10:22A Tue Nov 15, 2005

MODE: ?
COMMANDS:
R = CURRENT REPORT
S = SET POINTS
P = PROGRAMMING (ALSO P1,P2,P3,P4)
T1,T2,T3 = HOURLY TEMPERATURE RECORDS
E = EVENTS
H = DAILY HISTORY (HA,HB = THE TWO PARTS SEPARATELY)
W1,W2,W3 = WATER RECORDS
D1,D2,D3 = T1,T2,T3 + E + H + W1,W2,W3
XD1,XD2,XD3 = MORE HOURLY RECORDS
L = LOGON MESSAGE (ADDRESS AND DATE)
V = VERSION (MODEL NUMBER, DATE AND NOTES)


SPECIAL KEYS:
<?> = HELP
<CTRL-C>, <ESC> = ABORT CURRENT MODE
<CTRL-S> = PAUSE TRANSMISSION
<CTRL-Q> = RESUME TRANSMISSION
<BACKSPACE> = DELETE LINE


MODE: R
 TIME 245A 245B 245C 245D 285A 285B 285C 285D   9   10  OUT  AQS  DHW CHW STK
 8:38P  69   78   69   73   68   67   70   68   <5*  <5*| 61  181  119 202 136

 OFF(B) AUT(K) WINTER

 BURNER  HEAT  BYP  MAL  BAT  HI  LO
   3:45  2:30  0:00  0:00  0:00  64  52

 H-A  H-W  L-W  H-S    WTR
 212  156   95  588     10
```

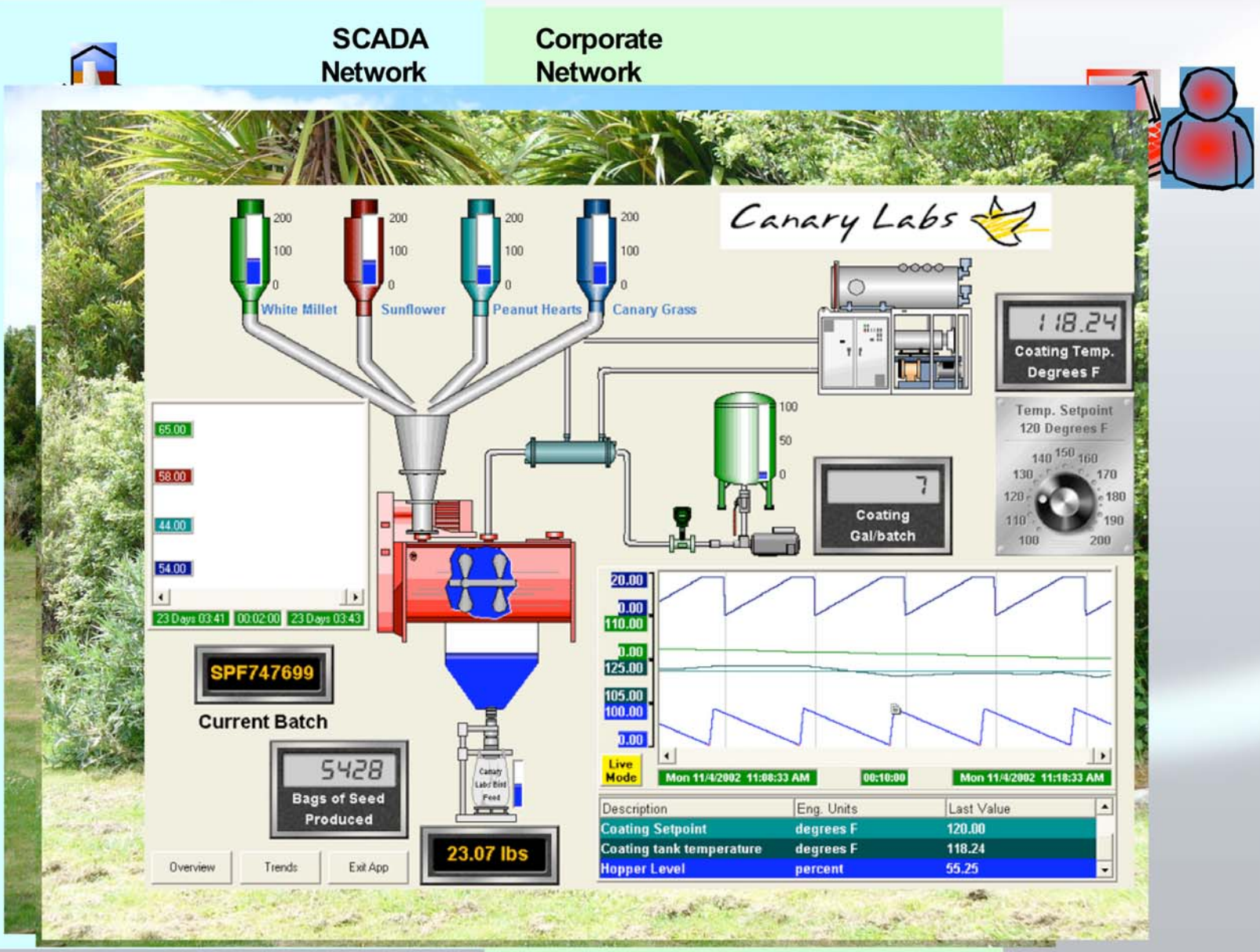
© 2007 Security-Assessment.com

- Scada hacking for the practical security consultant

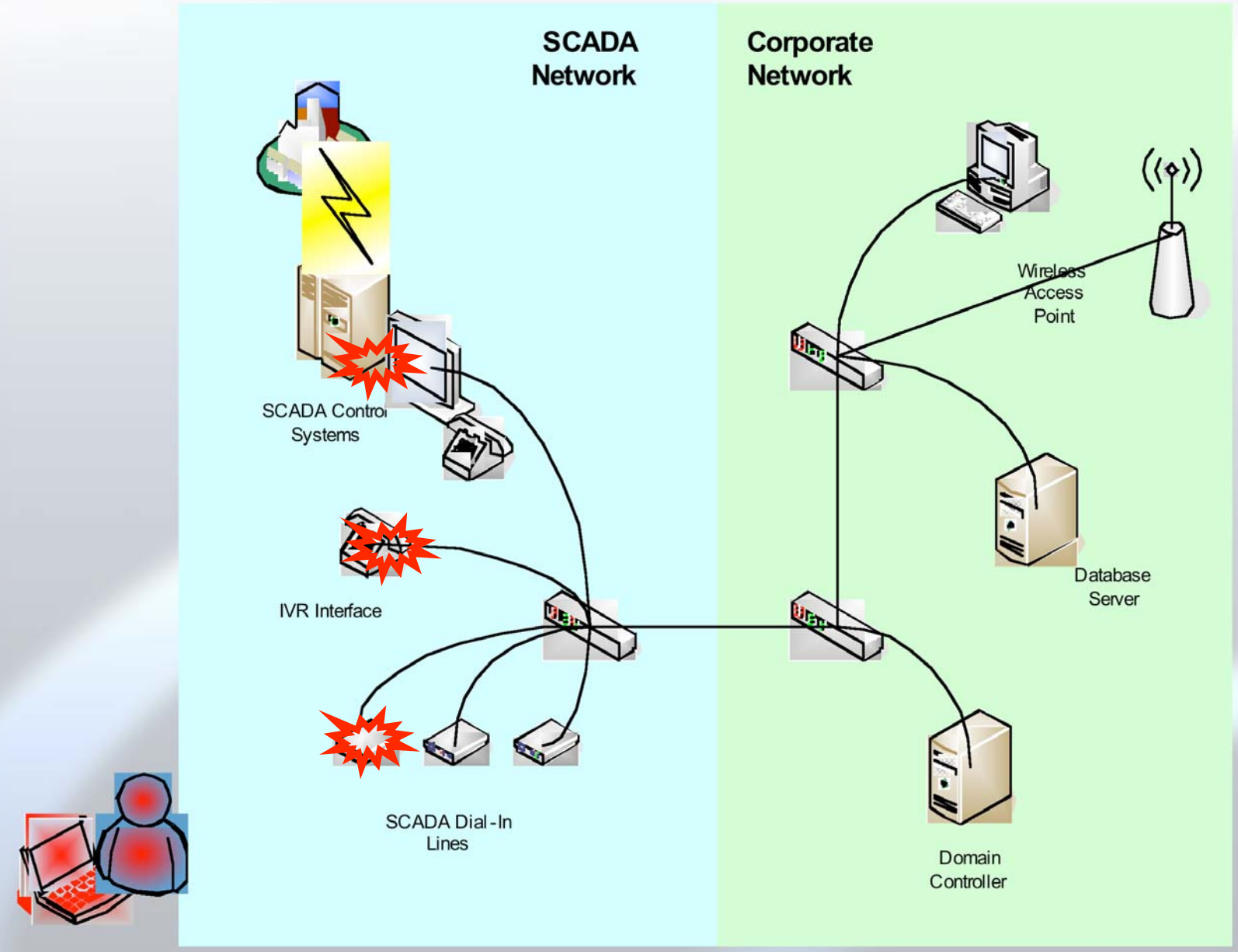
© 2007 Security-Assessment.com

- Company X:
  - Poorly secured wireless allowed access to Corporate Internal
  - Corporate Network was found to be one large flat network
  - Direct Access to SCADA systems from corporate desktop LAN
  - SCADA management systems unpatched windows hosts
  - Several dial-in lines to SCADA communcations processors were discovered
  - Default manufacturer passwords provided access to several SCADA systems

© 2007 Security-Assessment.com



© 2007 Security-Assessment.com



© 2007 Security-Assessment.com

- From these examples what general conclusions can we draw?

© 2007 Security-Assessment.com

- It's a Brave New Interconnected World
  - It was a commonly held belief that SCADA networks were isolated
  - In reality there are frequently NUMEROUS connections
  - Dial-in networks, radio backdoors, wireless, LAN connections, dual-homing via support laptops, connected to corporate LAN for ease of management and convenient data flow

© 2007 Security-Assessment.com

- Insecure By Design
  - Anonymous services - telnet/ftp (no users remember?)
  - Passwords default or simple, NEVER changed
  - Access controls not used as Firewalls cause delays which can impact responses which must happen in real-time
  - All protocols clear-text. Speed more important confidentiality

© 2007 Security-Assessment.com

- Lack of Authentication
  - I don't mean lack of strong authentication. I mean NO AUTH!!
  - There's no "users" on an automated system
  - OPC on Windows requires anonymous login rights for DCOM (XPSP2 breaks SCADA because anonymous DCOM off by default)
  - Normal policies regarding user management, password rotation etc etc do not apply

© 2007 Security-Assessment.com

- Can't Patch, Won't patch
  - SCADA systems traditionally aren't patched
  - Install the system, replace the system a decade later
  - Effects of patching a system can be worse than the effects of compromise?
  - Very large vulnerability window

© 2007 Security-Assessment.com

- SCADA has a different security model to traditional IT Networks

Aspect of IT	Corporate IT	Process Control IT
Anti-virus	widely used	often difficult / impossible to deploy
Lifetime	3-5 years	5-20 years
Outsourcing	widely used	rarely used for operations
Patching	frequent (often daily)	slow (required vendor approval)
Change	frequent	rare
Time criticality	delays OK	critical, often safety dependent
Availability	outages OK (overnight)	24 / 7 / 365
Security skills and awareness	fairly good	poor
Security testing	widely used	must be used with care
Physical security	usually secure and manned	often remote and unmanned

© 2007 Security-Assessment.com

- Good things happening in SCADA security
  - There are a growing number of standards in SCADA Security

BS7799-ISO27000 Information sec. management systems – Specification with guidance for use

ISO/IEC 17799:2005 Information Technology – Code of practice for information sec. management

ANSI/ISA S.99.1 Security for Manufacturing and Control Systems

ANSI/ISA SP99 TR2 Integrating Electronic Sec. into Manufacturing and Control Systems Env.

ISO/IEC 15408 Common Criteria

NIST System Protection Profile for Industrial Control Systems (SPP-ICS)

CIDX Chemical Industry Data Exchange - Vulnerability Assessment Methodology (VAM) Guidance

ISPE/GAMP4 – Good Automated Manufacturing Practices

PCSF Process Control System Forum ; NERC standards ; AGA standards ; NISCC Guidelines

- Some excellent practical guides a la NIST from NSA and other critical infrastructure groups.
- Let's do some good!

© 2007 Security-Assessment.com

- Securing Your SCADA
  - Not an all-inclusive list!!
  - Lots of good information online
  - Much of it is common sense / Industry Best Practice
  - Some practical steps...

© 2007 Security-Assessment.com

- Identify All Connections to SCADA Networks

© 2007 Security-Assessment.com

- Identify All Connections to SCADA Networks
  - Internal LAN, WAN connections, including business networks
  - The Internet
  - Wireless network devices, including radio, satellite etc
  - Modem or dial-up connections
  - Connections to vendors, regulatory services or business partners

© 2007 Security-Assessment.com

- Identify All Connections to SCADA Networks
  - Internal LAN, WAN connections, including business networks
  - The Internet
  - Wireless network devices, including radio, satellite etc
  - Modem or dial-up connections
  - Connections to vendors, regulatory services or business partners
- Conduct a thorough risk analysis to assess the risk and necessity of each connection to the SCADA network
- Develop a comprehensive understanding of how these connections are protected

© 2007 Security-Assessment.com

- Disconnect Unnecessary Connections to SCADA Networks

© 2007 Security-Assessment.com

- Disconnect Unnecessary Connections to SCADA Networks
- Isolate the SCADA network from other network connections to get the highest degree of security possible.
  - While connections to other networks allow efficient and convenient passing of data, it's simply not worth the risk.
- Utilisation of DMZs and data warehousing can facilitate the secure transfer of data from SCADA to business networks.

© 2007 Security-Assessment.com

- Conduct Physical Security Surveys

© 2007 Security-Assessment.com

- Conduct Physical Security Surveys
  - Any location which has a connection to the SCADA network must be considered a target (especially unmanned or unguarded sites)
  - Inventory access points. This includes:
    - Remote telephone
    - Cables / Fiber Optic Links that could be tapped
    - Terminals
    - Wireless / Radio

© 2007 Security-Assessment.com

- Conduct Physical Security Surveys
  - Any location which has a connection to the SCADA network must be considered a target (especially unmanned or unguarded sites)
  - Inventory access points. This includes:
    - Remote telephone
    - Cables / Fiber Optic Links that could be tapped
    - Terminals
    - Wireless / Radio
- Ensure that this includes ALL remote sites connected to the SCADA network

© 2007 Security-Assessment.com

- Conduct Physical Security Surveys



© 2007 Security-Assessment.com

- Intrusion Detection and Incident Response
  - To be able to respond to cyber-attacks you need to be able to detect them
  - Alerting of suspicious activity for network administrators is essential
  - Logging on all systems
  - Incident response procedures must be in place to allow effect response to an attack

© 2007 Security-Assessment.com

- Conduct penetration testing
  - There's no substitute for having an actual human attempt an intrusion into your network
- Implement:
  - Firewalls
  - Intrusion Detection / Prevention Systems (IDS/IPS)
  - Vulnerability Assessment
  - Regular Audits

© 2007 Security-Assessment.com

- SCADA IDS/Firewall – Industrial Defender
  - Rebranded Fortigate with twist of SCADA
  - Understands DNP3, MODBUS
  - Big red button for turn off all controls in event of emergency
  - Fancy box

© 2007 Security-Assessment.com

- SCADA IDS/Firewall – Industrial Defender
  - Rebranded Fortigate with twist of SCADA
  - Understands DNP3, MODBUS
  - Big red button for turn off all controls in event of emergency
  - Fancy box
  - IPS functionality as Virtual Patching!!

© 2007 Security-Assessment.com

- SCADA IDS/Firewall – Industrial Defender
  - Rebranded Fortigate with twist of SCADA
  - Understands DNP3, MODBUS
  - Big red button for turn off all controls in event of emergency
  - Fancy box
  - IPS functionality as Virtual Patching!!



© 2007 Security-Assessment.com

- Harden Your SCADA Networks!

© 2007 Security-Assessment.com

- Harden Your SCADA Networks!

- SCADA control servers built on commercial or open-source operating systems frequently run default services
  - This issue is compounded when SCADA networks are interconnected with other networks
- Remove unused services especially those involving internet access, email services, remote maintenance etc
- Work with SCADA vendors in order to indentify (in)secure configurations

© 2007 Security-Assessment.com

- Harden Your SCADA Networks!

- SCADA control servers built on commercial or open-source operating systems frequently run default services
  - This issue is compounded when SCADA networks are interconnected with other networks
- Remove unused services especially those involving internet access, email services, remote maintenance etc
- Work with SCADA vendors in order to indentify (in)secure configurations
- The NSA have a some useful guidelines in this area

© 2007 Security-Assessment.com

- Implement Security feature provided by SCADA vendors
  - While most older SCADA systems have no security features newer SCADA systems often do

© 2007 Security-Assessment.com

- Implement Security feature provided by SCADA vendors
  - While most older SCADA systems have no security features newer SCADA systems often do
  - More often than not though, these are turned off by default for ease of installation
  - Factory defaults often provide maximum usability and minimum security
  - Ensure that strong authentication is used for communications. Connections via modems, wireless, and wired networks represent a significant vulnerability to SCADA networks

© 2007 Security-Assessment.com

- Implement Security feature provided by SCADA vendors
  - While most older SCADA systems have no security features newer SCADA systems often do
  - More often than not though, these are turned off by default for ease of installation
  - Factory defaults often provide maximum usability and minimum security
  - Ensure that strong authentication is used for communications. Connections via modems, wireless, and wired networks represent a significant vulnerability to SCADA networks.
  - ^ ^ ^ ^ Successful war-dialing / war-driving could by pass all other access controls!!!!@#$@#$

© 2007 Security-Assessment.com

"The threat from a Red Team is real... If someone exposes a control system security flaw, I'll make my best effort to patch it in a timely fashion. But I'm not capable of hardening our system to the point where I can anticipate and deal with such attacks.

In the scheme of every day threats, this one doesn't rate. We're paid to defend against the likely and knowable threats – not the possibility of attack by a nation state. I can't harden my control system against another nation state. I can't put our operators through that degree of security. I have to worry about the lower tech approaches first. Who can get at the UPS for example...

We don't have guards with submachine guns and flak vests guarding our plants. We don't have military grade security software either. That's what we pay taxes for. I hate to say this, ...I have other far more likely scenarios to worry about."

---Jake Brodsky

http://www.wsscwater.com/

© 2007 Security-Assessment.com

- All the good stuff that you know and love... (with catch phrases that you've heard a million times before)
  - Backups / Disaster Recovery
  - Background checks
  - Limit network access (principle of least privilege)
  - Defense-in-depth
  - Training for staff (avoid social engineering)

© 2007 Security-Assessment.com

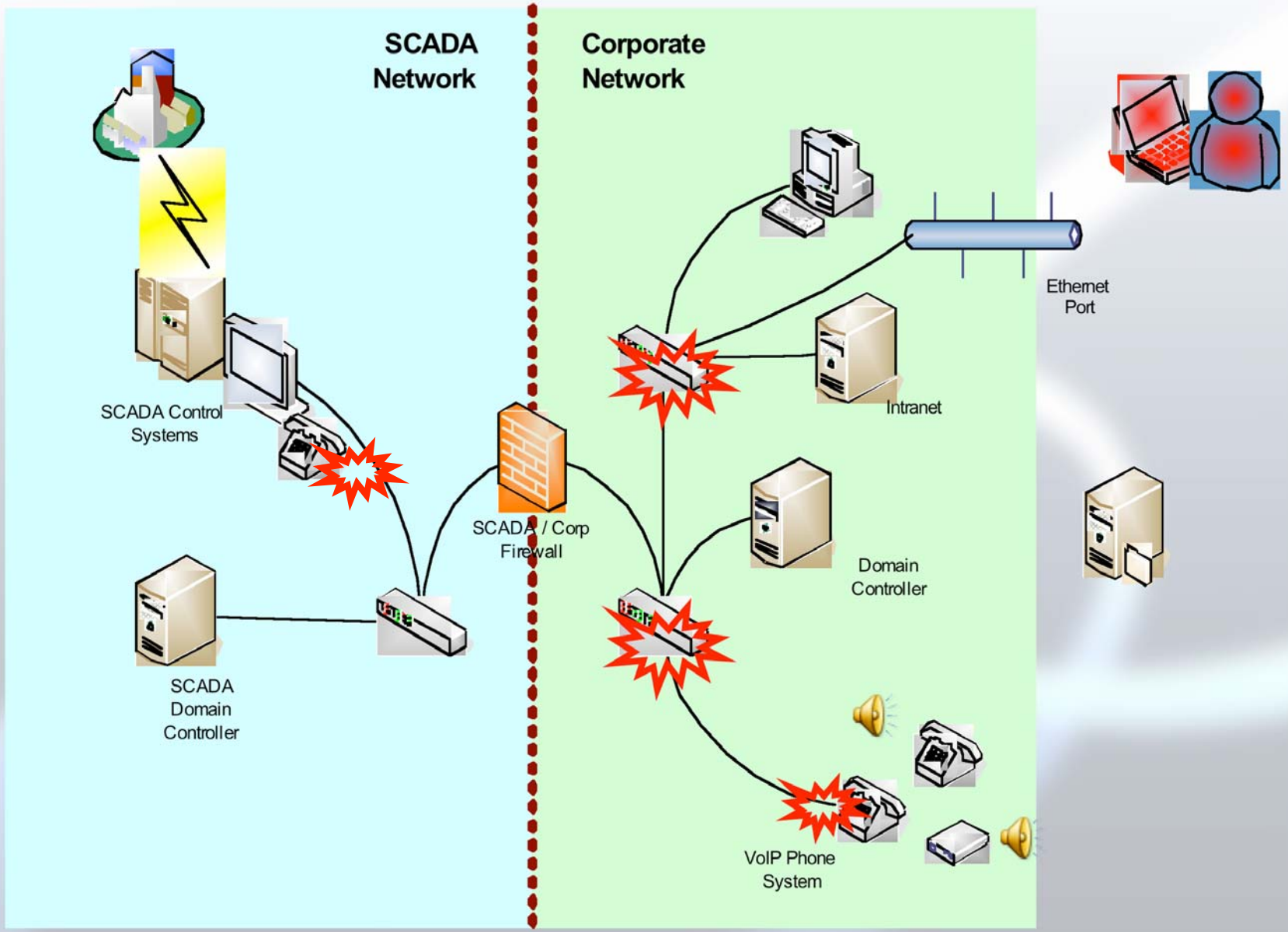
- Any access to internal network at all can be escalated to full control of SCADA
  - No sophisticated attacks required
  - Poor, missing, weak or reused passwords
  - Plenty of helpful documentation lying around
  - Physical access to network ports = SCADA



- Security separation controls administered from less trusted corporate side
  - Firewalls, routers, switches (VLANs)
  - Phones!

© 2007 Security-Assessment.com

Extra Credit: Phone System



© 2007 Security-Assessment.com

- Don’t Rely on Security Through Obscurity
- Some SCADA systems use unique, proprietary protocols
  - Relying on these for security is not a good idea
- Demand that vendors disclose the nature of vendor backdoors or interfaces to your SCADA systems
- Demand that vendors provide systems that can be secured!

© 2007 Security-Assessment.com

Conclusion

- IMHO, the threat of SCADA-based attacks are overblown today, but will become more serious in the coming years.
- The FUD shouldn't be overwhelming
- This is not something asset owners can do on their own!
- It is something that vendors need to address based on pressure from asset owners and regulatory agencies.

© 2007 Security-Assessment.com

- This would not have been possible without:
  - Bunny Brixton
  - Krusher
  - Sham
  - Metlstorm
- Many thanks to
  - SoSD
  - SLi
  - SA.com

© 2007 Security-Assessment.com

Questions?

http://www.security-assessment.com
morgan@security-assessment.com

© 2008 Security-Assessment.com