Terms/Glossary

- **8088 processors:**
  The very slow microprocessor used in the original IBM PC, dating from 1980. See http://www.old-computers.com/museum/computer.asp?c=274
- **Access control granularity:**
  “When I let you do something, how broad is that grant of access?” Is it everything-or-nothing, or quite specific? Can you do any command, or just the specific commands needed to do a particular task you’re assigned?
- **Accountability:**
  The ability to tell what caused an event to occur. The ability to accurately point the finger at a responsible party.
- **Auth system:**
  Authentication system (“How do I know who you are?”). This may be something you know (a password), something you have (a key or ATM card, for example), or something you are (biometric authentication via fingerprint, retinal scan, etc.)
  Authorization system (“What are you allowed to do?”): A well designed authorization system will insure that a user can access what they need to do their work, while simultaneously preventing them from accessing things they don’t need/shouldn’t have access to.

Terms/Glossary (2)

- **Best effort:**
  The way the Internet works: we'll try to deliver your network traffic, but no promises. If we drop some packets, or some packets get delayed, um, sorry about that, send 'em along again, eh? (contrast that with assured delivery)
- **Block valve:**
  Valve which blocks product flow in both directions when closed. Contrast with other sorts of values such as a check valve (which allows product flow in only one direction), or a pressure relief valve (a valve which is normally closed, but which opens to relieve an overpressure condition).
- **Breaker:**
  Device that "trips" and opens an electrical circuit when a specific condition occurs (e.g., at the consumer scale, you may have seen a circuit breaker open when you have too many appliances plugged into an outlet)
- **Congestion:**
  More network traffic than a given network path has capacity to carry.
- **DCS:**
  Distributed control system. Industrial plant-scale SCADA. See the excellent discussion of other differences between DCS and SCADA at http://members.iinet.net.au/~ianw/archive/x4371.htm

Terms/Glossary (3)

- **Denial of service attack (DOS):**
  Flooding a computer system or network with so much traffic or so many superfluous requests for service as to prevent normal work/usage.
- **DHS:**
  Department of Homeland Security
- **Embedded controller, embedded system:**
  A computer that is built into some device for some purpose other than to provide general purpose computing.
- **Encryption:**
  Using a cipher to protect a file or network traffic from unauthorized access or modification during transmission or storage. SSL (“https” secure web pages), ssh (secure shell), and pgp/gpg (Pretty Good Privacy/Gnu Privacy Guard) are examples of some software products that do encryption.
- **Encryption overhead:**
  The extra work a computer must go through when converting plain text into encrypted form for transmission or storage (there will also typically be decryption overhead as well).

Terms/Glossary (4)

- **Enterprise network:**
  The general corporate/business network, where traffic might consist of email, the world wide web, accounting applications, video conferencing traffic, etc. Contrast with the SCADA or process control networks
- **Ethernet:**
  The most common network used for local area networks today.
  See http://www.ethermanage.com/ethernet/ethernet.html for details.
- **Ethernet/IP:**
  Industrial ethernet (see http://www.ethernet-ip.org/)
- **Ethereal:**
  a popular protocol analyzer (e.g., a program used to diagnose and troubleshoot computer network traffic (www.ethereal.com)
- **Fiber ring:**
  Wide area network fiber tends to be deployed in a ring topology, with each node connected by two pairs (four total strands) of fiber. With that topology, if one pair of fibers get cut, the nodes on either side of the cut can still be accessed via the protect pair. Likewise, if one node is lost, all other nodes will still have at least one communication path remaining. Cisco has a nice discussion at http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r40docs/454ref40/r40etopl.htm

Terms/Glossary (5)

- **Firewall:**
  Network device that sits between the Internet-at-large and a protected set of computers, watching traffic and filtering unwanted packets, thereby offering the sheltered systems some degree of additional protection from attack.
- **Frame relay:**
  One way of interconnecting sites over a wide area network. Rather than purchasing a dedicated point-to-point circuit (“private line”), the customer connects to a telco frame relay “cloud” instead. Frame relay service is typically lower cost than equivalent private line service, however that lower cost may be accompanied by a greater risk of congestion due to shared infrastructure in the frame relay cloud (at least as normally provisioned).
- **Gas gathering line:**
  Because it has specific regulatory impact, this is a very contentious and tightly defined term of art within the natural gas industry; see, for example: “Guidelines for the Definition of Onshore Gas Gathering Lines” (63 pps) at http://www.ooga.org/issues/Pipeline%20Safety/RP80pages.pdf
  Informally, it is a local gas line designed to bring gas from a gas field to its first aggregation point or first processing plant.

Terms/Glossary (6)

- **Gas transmission line:**
  The longer-haul gas pipelines that move gas from region to region, or to downstream customers, storage facilities, etc.
- **Honeypot:**
  A system that appears to be a routine insecurely configured computer, but which is actually closely monitored, designed to detect intrusion attempts.
- **HMI or MMI:**
  Human Machine Interface or Man Machine Interface. How a computer system shows the user what's happening, and how the user tell the system what to do. On a general purpose PC, the HMI is usually a display screen, keyboard and mouse; on a cell phone, the HMI will be a smaller display window and a keypad; on a SCADA system, the HMI may be a digital representation of the control system being monitored, complete with filling tanks, spinning pumps, etc., or just simple strip charts and indicator lights controlled with a keyboard and mouse.
- **Intrusion detection system:**
  A network traffic monitoring device that has been programmed with rules or patterns which allow it to identify and/or block malevolent network traffic. Common examples includes Snort and Bro

Terms/Glossary (7)

- **Jitter:**
  Variation in interpacket delivery times. Contrast a low jitter/consistent flow <packet>..<packet>..<packet>..<packet>..<packet> with a high jitter flow <packet>……..<packet><packet>.<packet>…<packet>………<packet>
- **Ladder logic**
  A way of implementing control system structures in programable logic controllers. See the brief example/discussion at “The Basics of Ladder Logic” (http://www.ecmweb.com/ops/electric_basics_ladder_logic)
- **LAN**
  A Local Area Network, commonly running over ethernet. The network within most businesses or agencies or schools is a LAN.
- **LE**
  Law enforcement
- **Life cycle**
  The span of a project, from concept to design, construction, operation, upgrade(s), replacement/decommisioning.
- **Logging**
  Process of recording time stamped information about events as they occur for subsequent review and analysis.

Terms/Glossary (8)

- **Miscreant:**
  Hacker/cracker, online attacker. (researchers have actually developed formal typologies/categories for the various sorts of these folks; e.g.: http://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-parker.ppt)
- **Modbus/TCP:**
  The most widely used protocol in the industrial manufacturing environment for communication between intelligent devices over ethernet.
- **Modem:**
  Interface device allowing a computer to communicate over regular telephone lines. Comparatively slow speed relative to broadband options such as DSL or cable modem, but a convenient (if potentially insecure) way to set up intermittent connections.
- **MTUs:**
  Master terminal units. The central control stations to which RTUs connection. Operators use an HMI running on the MTU to operate the SCADA system.
- **NTSB:**
  National Transportation Safety Board. Federal entity charged with investigating accidents involving pipelines, railroads, etc.

Terms/Glossary (9)

- **OS:**
  Operating System. The basic software loaded onto a computer which tells the system how to do basic functions such as schedule tasks for execution, access files, authenticate users, accept input from a keyboard or mouse, put output onto a display or printer, talk to the Internet, etc. Microsoft Windows is an example of an operating system, as is Linux or Mac OS X.
- **P2P:**
  Peer-to-peer networking, an interconnection architecture where there is no central server; all hosts are equals ("peers"). Contrast with "client server" architectures, where clients are serviced by a core server. P2P is most commonly associated with file sharing programs such as Kazaa.
- **Packet filter:**
  A rule, implemented in a firewall or other network infrastructure, designed to block a particular category of traffic.
- **Patch**
  Typically small software modification designed to fix a problem with a program.
- **Plain text transmission**
  Unencrypted traffic which is vulnerable to being sniffed (intercepted, evesdropped upon)

Terms/Glossary (10)

- **PLC:**
  Programmable Logic Controller. SCADA interface device attached to a motor, valve, sensor, which can be configured to allow the SCADA system to manipulate that device. PLCs normally connect to RTUs.
- **Poke a hole (in a firewall):**
  Configure the firewall to allow a particular type of traffic to pass, or traffic to or from a particular destination.
- **Port (network port):**
  On the Internet or a typical LAN, systems connect to each other via agreed upon (“well known”) numeric ports, for example port 80 is normally used for WWW traffic, port 25 is normally used for the transfer of email, etc. Modbus/TCP, a popular SCADA protocol, uses port 502.
- **Probing, to probe:**
  To attempt to connect to well known services which may be running on a system; done to see if the system exists, and potentially to identify the software it is running.
- **Process control network:**
  The opposite of the general purpose corporate business network; the SCADA or DCS network.

Terms/Glossary (11)

- **Protocol:**
  Agreed up mechanism/standardized rules for exchanging traffic, interconnecting devices, etc. The Internet uses a series of protocols which are documented in “RFC’s” (see http://www.ietf.org/rfc.html). Modbus/TCP is an example of a common SCADA protocol.
- **Protocol analyzer:**
  Software package, often running on a laptop or other portable system, which allows sniffed network traffic to be decoded and examined.
- **Psig:**
  Pressure in pounds per square inch gauge. Pipelines have a maximum rated operating pressure in psig, and many pipeline failures are associated with conditions that cause pressures to materially exceed that number.
- **Realtime operating system:**
  Operating system designed for use in embedded systems where events need to be processed in real time, typically as part of an embedded system. Example might be the control system for the space shuttle or a nuclear reactor. Contrast with a general purpose operating system, where the objective is customarily non-time critical, or processing is of a more general nature.

Terms/Glossary (12)

- **Replay attacks:**
  Hacker/cracker attack which involves capturing traffic sent over the network, and then reinjecting it again later, causing commands to be executed twice. Timestamps and a variety of other mechanisms are designed to prevent replay attacks.
- **ROM:**
  Read only memory. Unlike most memory chips, which can be read and written to, read only memories are designed to be burned (programmed) and then not change. Convenient way to store an operating system on an embedded system. PROMs (Programmable Read Only Memory) allow for in-the-field upgrading of stored code, while otherwise acting just like a ROM.
- **RTUs:**
  Remote terminal unit. Satellite device, perhaps at a pumping station or other node in a SCADA system, to which PLCs connect. The RTUs in turn connect upstream to the MTU.
- **SCADA:**
  Supervisory Control and Data Acquisition system. Plant or infrastructural automation of functions formerly performed manually, typically on a large scale.

Terms/Glossary (13)

- **Scanning (or Port Scanning):**
  Process by which a hacker/cracker systematically checks a series of ports on a set of computers, looking for vulnerabilities. NMAP is a common tool for port scanning; Nessus is a common security vulnerability scanner.
- **Serial lines:**
  Comparatively short-range and slow speed direct point-to-point connections over which transmissions are made by sending one bit after another. The analogical opposite of serial connections would be parallel connections, where multiple data lines are used to send a set of bits at the same time. Serial connections have largely disappeared, surplanted by ethernet.
- **Slammer:**
  A computer worm from January 2003 which exploited vulnerabilities in Microsoft SQL Server, and which generated so much network traffic it caused a general denial of service to occur. For information about Slammer, see: http://secunia.com/advisories/7945/?menu=repo
- **SNMP:**
  Simple network management protocol. An agreed upon framework by which network devices can share information about their status. Cisco has a nice discussion of SNMP at http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

Terms/Glossary (14)

- **SNMP community strings:**
  SNMP jargon for an SNMP “password.” Access to SNMP data about a device is controlled by setting an SNMP community string. There are normally two community strings: one which allows read-only access (by convention, this is often the literal “public”), and another secret value which allows read and write access.
- **Snort:**
  Snort is a popular intrusion detection system. See www.snort.org
- **Spoofing attacks:**
  Generation of outbound network traffic pretending to be from somewhere else, typically used in a denial of service attack. Well run networks filter outbound spoofed traffic and do not allow it to be sent onto the Internet.
- **STAMPs:**
  Popular small programmable microcontrollers. STAMPs can be used to control a robot, for example, or for industrial control tasks. See: http://www.parallax.com/
- **Statistical Multiplexing:**
  Sharing a circuit by realizing that most of the time multiple speakers won’t want to talk at the same time, and if they do collide and interrupt each other, they can wait a random interval and then try again. Contrast with TDM.

Terms/Glossary (15)

- **TDM:**
  Time division multiplexing, often implemented using SONET. TDM shares a circuit by dividing capacity into a fixed series of windows or slots, rigidly allocating capacity regardless of current needs for more or less. Traditional phone systems are TDM based.
- **Telnet:**
  An Internet protocol that allows a user to create a terminal session across the network. Terminal sessions predate graphical user interfaces (such as Windows), and allowed users to type in commands to do tasks such as create or modify files, copy files, rename files, etc. Unix users normally refer to terminal sessions as “working at the shell prompt.” Telnet is a plain text protocol, and vulnerable to being evesdropped upon, or “sniffed” by a protocol analyzer. The encrypted analog of telnet is ssh.
- **Testbed:**
  Small scale proof of concept or demonstration system, designed to allow experimentation.

Terms/Glossary (16)

- **UPS:**
  Uninterruptible power supply. Usually a system based around one or more lead acid batteries, used to provide temporary emergency power in the event primary power fails.
- **VoIP:**
  Voice over IP; the ability to carry voice traffic along side data traffic on a LAN or the Internet. Vonage is an example of a commercial VoIP company.

- **Some other glossaries…**

  -- electrical transmission lines:
  www.osha.gov/SLTC/etools/electric_power/illustrated_glossary/index.html

  -- pipeline:
  http://www.alyeska-pipe.com/Pipelinefacts/GlossaryOfTerms.html
  http://www.safebellingham.org/glossary.htm