

Cyber Security Who's got your back?



Steve Bowles
Southeast Regional Mgr

www.garrettcom.com

678.947.6079 office

Email: sbowles@garrettcom.com

What is Cyber Security?

- The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

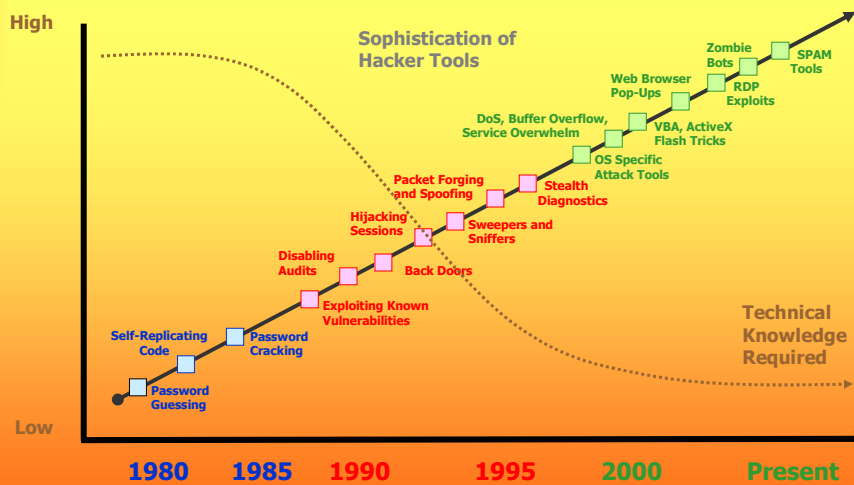
US-CERT: United States Computer Emergency Readiness Team



GarrettCom, Inc.

3

The trend of the hacker...



GarrettCom, Inc.

4

A message from George W

Our national critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, the defense/industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, and fiber-optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security...These computer networks also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radar, and stock markets, all of which exist beyond cyberspace...Many industries in America have radically transformed the way they control and monitor equipment over the last 20 years by employing digital control systems (DCS) and supervisory control and data acquisition systems (SCADA).

George W. Bush

The National Strategy to Secure Cyberspace
The White House, February 2003

The USA Patriot Act

Critical infrastructure is defined in the USA PATRIOT Act as those “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

Patriot Act- HR 3162, dated: October 24, 2001

<http://www.treas.gov/offices/enforcement/teoaf/legislation/usa-patriot-act.pdf>

What Threatens you?

- Virus, not the common cold- MyDoom, Blaster, Slammer, Sasser and many other unknown to date type of virus' and worms
- DoS- Denial of Service
- Physical attack on the network
- Internal attack via sabotage or disgruntled employees
- Hackers that are internal and external
- Espionage by foreign entity and/or competitors

GarrettCom, Inc.

7

Top 10 Security Mistakes Committed by Employees

1. Post-it Passwords, just hang a picture.
2. I Did It My Way, people are hard headed.
3. On but Gone, no secured screen saver or left on.
4. Gee, Wonder What's In this Attachment?
5. Failing Passwords, lets be more original.
6. Loose Lips sink ships, watch out what you say.
7. Laptops Have Legs and will walk away if given a chance.
8. Lax Enforcement with not enough bite.
9. The Threat Within.
10. Update now always, automatically or manually.

GarrettCom, Inc.

8

Our Reliance on IT

The growth of information technology (IT) and almost universal access to computers has enabled hackers and would-be terrorists to attack information systems and critical infrastructures worldwide because international boundaries have been eliminated in cyberspace.

Here are a few adverse national impacts from our increased reliance on computers and the Internet:

- Increased complexity of our information systems and added interconnectedness between and among infrastructures.
- Reduced operational buffer zones in most infrastructures as a vehicle for cost reduction and efficient operation.
- Enhanced accessibility of would-be terrorists to our defense, banking and financial institutions, and to other critical infrastructures.

Is it real or not?

Until recently, there was a belief that Cyber Terrorism had such a low threat that managers or technicians who attempted to discuss responding to computer terrorism were not taken very seriously.

Unless the business mission was directly involved in military defense, or had politically volatile roots, Cyber Terrorism was not mentioned as a concern worth occupying time or budget.

Securing SCADA Networks

- Define a security policy
- Secure the SCADA network and operating environment
- Secure the SCADA application
- Detection of unauthorized intrusions
- Regulate and monitor physical access to the SCADA network

Security Policy

A security policy should cover the following key components:

- Roles and responsibility of those affected by the policy
- What actions, activities and processes are allowed and which are not?
- What are the consequences of non-compliance?

Key personnel who need to be included in the development of the policy include:

- Senior management
- Information Technology department
- Human Resources and
- Legal

Secure the SCADA Network

Corporate networks linked to the Internet or that use wireless technology may be more easily accessible to cyber terrorists and hackers. An organization can heighten its level of network security by isolating its SCADA network thereby restricting channels of external access.

Counter measures:

- Firewalls – appliance or software
- Virtual Private Networks – remote access
- De-militarized Zones – buffer zone
- Authentication – encryption techniques and software

Secure the SCADA Application

Authentication is the software process of identifying a user who is authorized to access the SCADA system.

Authorization is the process of defining access permissions on the SCADA system and allowing users with permissions to access respective areas of the system.

Authentication and authorization are the mechanisms for single point of control for identifying and allowing only authorized users to access the SCADA system, thereby ensuring a high level of control over the system's security.

To provide effective authentication the system must require each user to enter a unique user name and password.

Detection of Intrusions

Firewalls and other simple boundary devices currently available lack some degree of intelligence, intrusion detection systems (IDS) are becoming increasingly important in helping to maintain network security.

An IDS is a specialized tool that knows how to read and interpret the contents of log files from routers, firewalls, servers and other network devices.

Types of Intrusion Detection

- **Host Based Intrusion Detection Systems** Operates on a host to detect malicious activity on that host.
- **Network Based Intrusion Detection Systems:** IDS systems that operate on network data flows.
- **Intrusion Prevention System** This is a system that actively monitors a network or host for attacks and blocks (prevents) those attacks from occurring.

<http://www.honeypots.net/ids/links>

<http://is-it-true.org/fw/fwtips6.shtml>

<http://www.nja-monitor.com/fact-sheets/ids-tips-main.htm>

http://www.windowsecurity.com/articles/What_You_Need_to_Know_About_Intrusion_Detection_Systems.html

Regulate Physical Access to the SCADA Network

Physical access to your network should be closely monitored:

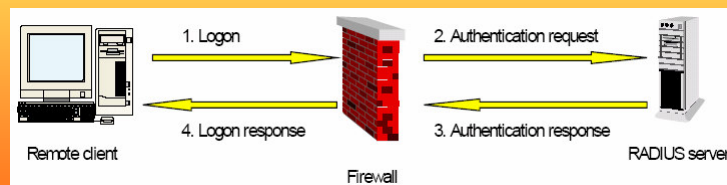
1. Use built-in Microsoft Windows features to require user authentication when perusing network shares.
2. Do not allow anyone that does not belong to your organization to connect to your network Ethernet or have physical access to your IT server room.
3. Monitor your network regularly for activity that may be suspicious and note the IP addresses when running sniffing software or hardware on the network.
4. Ensure that there are no foreign IP addresses on the list. If you find a foreign IP address, trace route to the IP address. Once you locate where this foreign IP address originates from you can take action. If you are unsure physically disconnect the segment where the potential intruder may be on the network.

Hardware/Software Methods to limit Cyber Threats and Violations

- **Firewalls** A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through.
- **NMS**- Network Management Software
- **SNMP**- Simple Network Management Protocol
- **TACACS and Radius Server**
- **SSL** Secure Socket Layer **and TLS** Transport Layer Security

Firewalls

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through.



GarrettCom, Inc.

19

NMS

Refers to the broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including:

- **Security:** Ensuring that the network is protected from unauthorized users.
- **Performance:** Eliminating bottlenecks in the network.
- **Reliability:** Making sure the network is available to users and responding to hardware and software malfunctions.

Castle Rock
Intravue
Intuit
HP OpenView
ExtraLAN

GarrettCom, Inc.

20

SNMP

Short for Simple Network Management Protocol, a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

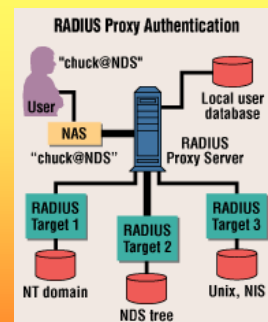
TACACS and Radius Server

RADIUS encrypts only the password, TACACS+ encrypts the entire packet.

Remote Authentication Dial-In User Service

RADIUS, 802.1x

Defines a mechanism for port-based network access control. It provides a means of authenticating and authorizing users and devices attempting to attach to LAN ports that have point-to-point connection characteristics such as wireless access. It also prevents access from that user in cases where the authentication and authorization fails.



TACACS

TACACS+

Terminal Access Controller Access Control System

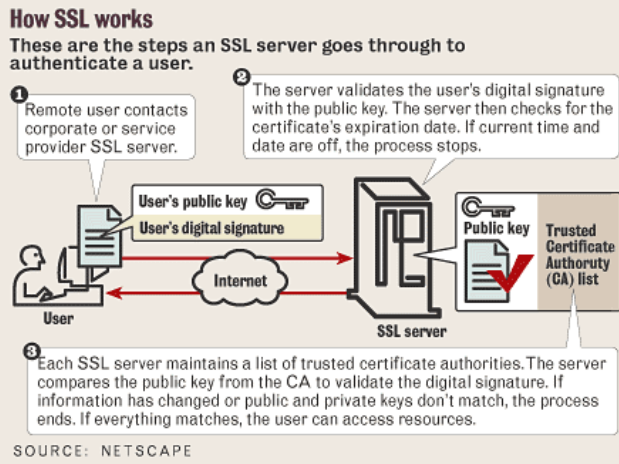
Provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

SSL and TLS

SSL- Secure Socket Layer is a layered protocol. At each layer, messages may include fields for length, description, and content. SSL takes messages to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, and transmits the result. Received data is decrypted, verified, decompressed, and reassembled, then delivered to higher level clients.

TLS- Transport Layer Security is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the SSL.

How SSL works?



GarrettCom, Inc.

25

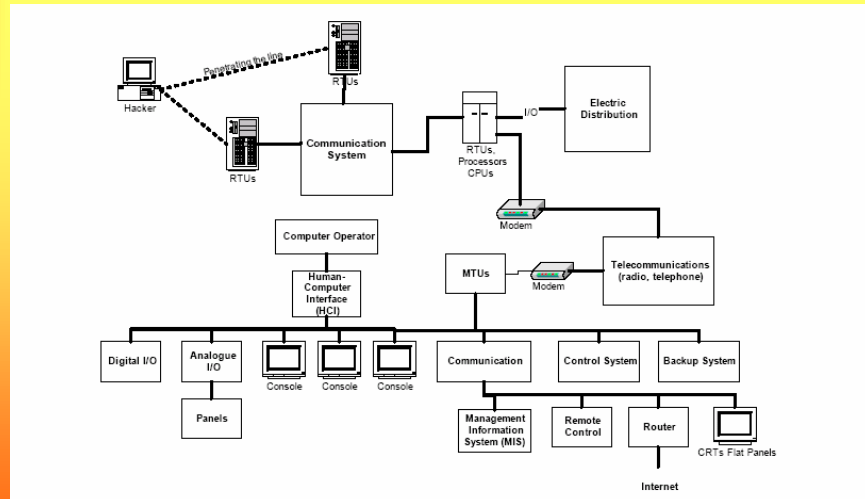
It is indeed, real.....

Industrial monitoring and control systems are directly connected to station equipment. A cyber terrorist attacking the control system layer can cause complete service interruptions, loss of generating capacity, environmental damage and unsafe working conditions.

GarrettCom, Inc.

26

Typical SCADA Layout



GarrettCom, Inc.

27

Security in Power Utilities

Steps are being taken to ensure the cyber security of control systems in several industries including electric power.

- In order to protect the electric power infrastructure, the North American Electric Reliability Council (NERC) Critical Infrastructure Protection Committee (CIPC) issued Urgent Action Standard 1200 (Cyber Security) to help secure utility control centers.
- NERC is currently working on a final standard to secure other critical facilities, including transmission substations and power plants.
- An important aspect of control system reliability and security is cyber security policies that specifically address control systems unique security issues that IT security policies were not developed to address.

www.nerc.com

GarrettCom, Inc.

28

Tips for Cyber Terrorism Defense:

1. Focus on the fact that you are a target. This is especially true for part of the Government and the 5 sectors of critical infrastructure: finance, health and safety, communications, transportation or public utilities.
2. Implement a full-scope Intrusion Management Strategy, not just Intrusion Detection. Understanding, planning, managing, detecting, responding, and recovering is critical to survival.
3. Understand that patterns evolve. Before a system can be compromised, an attacker needs to identify the perimeter defense and needs to find a weakness in that defense that allows them to gain access to a meaningful application.

Tips for Cyber Terrorism Defense:

4. Humans can recognize patterns faster than they can analyze data. Let the computer store and organize data, which it can do best, but let the human brain spot the offending pattern, its key strength.
5. An architecture must be resilient and easy to update. Cyber terrorists and attackers intelligently mutate their attack signatures; utilizing alternate channels. It is important to be able to change recognition methods and procedures for repelling such attacks quickly and effectively. There is not enough time to buy new equipment or change a software platform.

Summary

The risks of terrorism to information technology and to critical infrastructures should not be underestimated for the following reasons:

1. Cyber Terrorism is real
2. Cyber Security is critical to our economy
3. Security plans and policies are a must
4. Understand the technology and topology
5. Keep it simple and secure
6. Minimize risk and exposure
7. Audit frequently and enforce often

GarrettCom, Inc.



- Industrial hardened network switches
- Firewalls and routers
- Serial terminal servers with Ethernet
- PoE- power over ethernet, IP video
- Managed and unmanaged switches
- Power options, 12, 24, 48, 125VDC and AC
- Fiber options for 10, 100 and 1000Mb for single mode and multimode fiber
- Media converters and small form switches
- CSA/UL Class 1 Division 2 for combustibles
- Redundant fiber and power
- NERC/CIP, IEC61850, IEEE1613, NEBS and MilStds

Useful Links

US Computer Emergency Readiness Team

- www.us-cert.gov

Cyber Security Industry Alliance

- <https://www.csalliance.org/home>

Cyber Security Research and Policy Institute

- <http://www.cpi.seas.gwu.edu/>

Cyber Security- NERC Critical Infrastructure Protection Mandates

- <http://news.thomasnet.com/fullstory/521402>