SCADA Network Attacks-How Safe is our Critical Infrastructures?

Md. Sabbir Hossain

Supervisory Control and Data Acquisition (SCADA) systems are deeply ingrained in the fabric of critical infrastructure sectors. These computerized real-time process control systems, over geographically dispersed continuous distribution operations, are increasingly subject to serious damage and disruption by cyber means due to their standardization and connectivity to other networks. However, SCADA systems generally have little protection from the escalating cyber threats.

The current common practice of SCADA system leaves window open to various vulnerabilities. To name a few, the entrenched factors are not limited to public information like a company's network infrastructure, insecure network architecture, operating system vulnerabilities enabled trap doors to unauthorized users and the use of wireless devices. In particular, the lack of real-time monitoring and proper encryption is very detrimental.

Cyber-attacks on SCADA system can take routes through Internet connections, business or enterprise network connections and or connections to other networks, to the layer of control networks then down the level of field devices. More specifically, the common attack vectors are:

- Backdoors and holes in network perimeter
- Vulnerabilities in common protocols
- Attacks on field devices through cyber means
- Database attacks
- Communications hijacking and Man-in-the-middle attacks
- Cinderella attack on time provision and synchronization

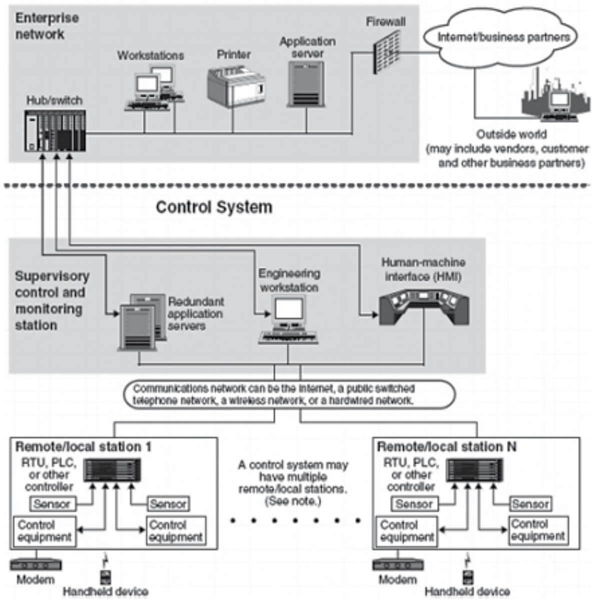

Enterprise network
Workstations
Printer
Application server
Firewall
Internet/business partners
Hub/switch
Outside world (may include vendors, customer and other business partners)
Control System
Supervisory control and monitoring station
Redundant application servers
Engineering workstation
Human-machine interface (HMI)
Communications network can be the Internet, a public switched telephone network, a wireless network, or a hardwired network.
Remote/local station 1
RTU, PLC, or other controller
Sensor
Sensor
Control equipment
Control equipment
A control system may have multiple remote/local stations. (See note.)
Remote/local station N
RTU, PLC, or other controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device
Modem
Handheld device

Figure: Typical SCADA Network

We Can Group the Possible Attacks as:

- Cyber Attack on Hardware:
- Attacks on Software
- Attacks on the communication stack
- Attacks on Implementation of Protocols

Cyber Attack on Hardware:

Attacker might gain unauthenticated remote access to devices and change their data set points. This can cause devices to fail at a very low threshold value or an alarm not to go off when it should. Another possibility is that the attacker, after gaining unauthenticated access, could change the operator display values so that when an alarm actually goes off, the human operator is unaware of it. This could delay the human response to an emergency which might adversely affect the safety of people in the vicinity of the plant. one of the representative attacks in this category is the **doorknob-rattling attack.** The adversary performs a very few common username and password combinations on serval computers that results in very few failed login attempts. This attack can go undetected unless the data related to login failures from all the hosts are collected and aggregated to check for doorknob-rattling from any remote destination.

Attack on Software

SCADA system employs a variety of software to meet its functionality demands. Also there are large databases reside in data historians besides many relational database applications used in cooperate and plant sessions. Main types of attacks on software are:

- **No Privilege Separation in Embedded Operating System:** VxWorks was the most popular embedded operating system in SCADA, which is a platform developed by Wind River Systems and has since been acquired by Intel. VxWorks itself is essentially a monolithic kernel with applications implemented as kernel tasks, this means that all tasks generally run with the highest privileges and there is little memory protection between these tasks.

- **Buffer Overflow:** Many attacks boil down to cause buffer overflow as their eventual means to corrupt the intended behavior of the program and cause it to run amok. Some general methods are stack smashing and manipulating function pointer. The effect of such attacks can take forms such as resetting passwords, modifying content, running malicious code and so on. The buffer overflow problem in SCADA system takes two fronts. One front is on the workstations and servers which are similar to standard IT systems. The other front manifests itself in field devices and other components that rely on RTOS thereof inherent the susceptible memory challenge. Exploits can take advantage of the fixed memory allocation time requirement in RTOS system to have more successful launchings. Let alone that many field devices run for years without rebooting. Therefore, these SCADA components, especially in legacy networks, are subject to accumulated memory fragmentation, which leads to program stall.

• **SQL Injection:** Most small and industrial-strength database applications can be accessed using Structured Query Language (SQL) statements for structural modification and content manipulation. In light of data historians and web accessibility in current SCADA systems, SQL injection, one of the top Web attacks, has a very strong implication on the security of SCADA system. The typical unit of execution of SQL which comes in many dialects loosely based around SQL-92 ANSI standard is query, which is a collection of statements that typically return a single result set. SQL injection occurs when an adversary is able to manipulate data input into a Web application, which fails properly sanitize user-supplied input, and to insert a series of unexpected SQL statements into a query. Thus it is possible to manipulate a database in several unanticipated ways. Moreover, if a "command shell" store procedure is enabled, an attacker can move further to prompt level. The process will run with the same permissions as the component that executed the command. The impact of this attack can allow attackers to gain total control of the database or even execute commands on the system. Intentionally malicious changes to databases can cause catastrophic damage.

Attacks on the Communication Stack

We break down the attacks on the communication stack by using the TCP/IP or the Internet reference model and highlight some of those may have more potentials in harming SCADA systems, in particular on network layer, transport layer, application layer and the implementation of protocols.

● ***Network Layer:***

➢ **Diagnostic Server Attacks Through UDP Port:** Adversaries have access to the same debugging tools that any RTOS developers do. They can read symbol tables, step through the assembly, etc., considering also that many attackers don't even need code-level knowledge. For example, Wind River Systems VxWorks weak default hashing algorithm in standard authentication API for VxWorks is susceptible to collisions, an attacker can brute force a password by guessing a string that produces the same hash as a legitimate password. Or through VxWorks debug service runs UDP on port 17185, which is enabled by default, an attacker can execute the following attacks without any authentication required while maintaining a certain level of stealthy ness such as remote memory dump, remote memory patch, remote calls to functions, remote task management.

➢ **Idle Scan:** is to blind port scan by bouncing off a dumb "zombie " host, often a preparation for attack. Both MODBUS and DNP3 have scan functionalities prone to such attacks when they are encapsulated for running over TCP/IP.

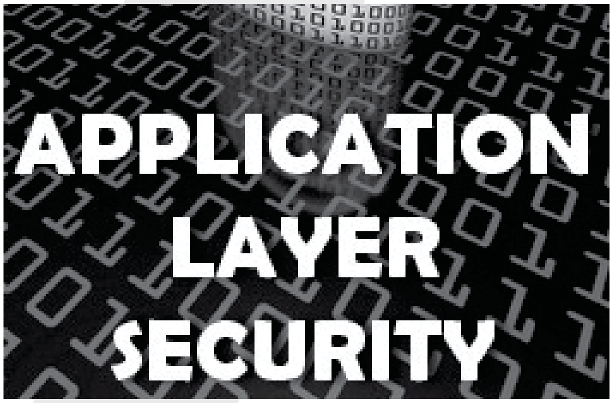
➢ **Smurf:** is a type of address spoofing, in general, by sending a continuous stream of modified Internet Control Message Protocol(ICMP) packets to the target network with the sending address is identical to one of the target computer addresses. In the context of SCADA systems, if an PLC acts on the modified message, it may either crash or dangerously send out wrong commands to actuators.

➢ **Address Resolution Protocol (ARP) Spoofing/Poisoning:** The ARP is primarily used to translate IP addresses to Ethernet Medium Access Control (MAC) addresses and to discover other connected interfaced device on the LAN. The ARP spoofing attack is to modify the cached address pair information. By sending fake ARP messages which contain false MAC addresses in SCADA systems, an adversary can confuse network devices, such as network switches. When these frames are false fully sent to another node, packets can be sniffed; or to an unreachable host, DoS is launched; or intentionally to a host connected to different actuators, then physical disasters of different scales are initiated.

➢ **Chain/Loop Attack:** In a chain attack, there is a chain of connection through many nodes as the adversary moves across multiple nodes to hide his origin and identity. In case of a loop attack, the chain of connections is in a loop make it even harder to track down his origin in a wide SCADA system.

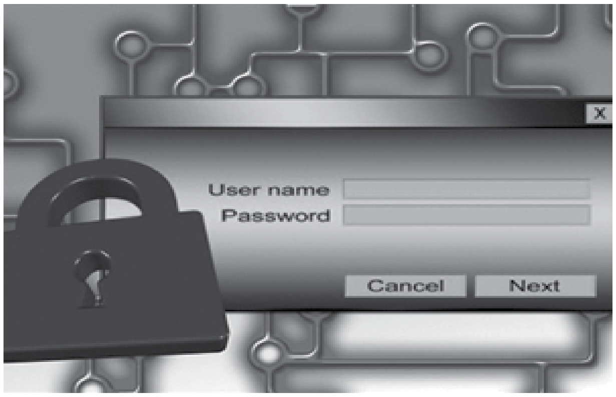
Transport Layer: SYN flood is to saturate resources by sending TCP connection requests faster than a machine can process. SCADA protocols, particularly those running over top of transport protocols such as TCP/IP have vulnerabilities that could be exploited by attacker through methodologies as simple as injecting malformed packets to cause the receiving device to respond or communicate in inappropriate ways and result in the operator losing complete view or control of the control device.

Application Layer: Currently, there is no strong security control in protocols used in SCADA systems, such as DNP3 without secure authentication, Modbus, Object Linking and Embedding (OLE) for Process Control (OPC), Inter-Control Center Communications Protocol (ICCP). Practically there is no authentication on source and data such that for those who have access to a device through a SCADA protocol, they can often read and write as well. The write access and diagnostic functions of these protocols are particular vulnerable to cyber and cyber induced physical attacks. One of possible attacks in both SCADA and conventional IT systems is DNS forgery. Such attack is to send a fake DNS reply with a matching source IP, destination port, request ID, but with an attacker manipulated information inside, so that this fake reply may be processed by the client before the real reply is received from the real DNS server.



Attacks on Implementation of Protocols

Protocol vulnerabilities can reveal themselves as segmentation faults, stack, heap or buffer overflows, etc., all of which can cause the protocol implementation to fail resulting in a potential exploit. Meanwhile, certain protocol implementations, such as ICCP servers, only allow users to read values, and there are a number of protocols that are in the process of adding security controls to address this deficiency. SCADA implementation vulnerabilities are more important than lack of security controls in SCADA protocols.



TCP/IP: First of all, in light of the migration to Windows from UNIX in operating system used by many sectors in SCADA systems, there are several attacks specifically exploit the implementation of TCP/IP protocols in Windows. Although there are patches available, restrained to be on-line continuously, it's very likely that these machines do not have up-to-dated patches. Here, we only name a few well known ones.

- WinNuke takes advantage of the absence of status flag URG in handling the TCP protocol.
- TearDrop/NearTear and Ssping utilize implementation error of fragmentation handling in TCP/IP protocol. A nightmare scenario can be that one company's network is compromised and a polymorphic worm takes down most servers and any unpatched SCADA servers running Windows.

Secondly, these protocol stacks can and do suffer from various vulnerabilities commonly found due to poor software design and coding practices.

OPC: OPC servers use Microsoft's OLE technology to provide real-time information exchange between software applications and process hardware. At the OPC interface level, the item write function takes two parameters: an item handle and a value to write to it. If the server maps handle to memory addresses and fails to validate a client-provided handle, the IO interfaces write function allows an attacker to write any value to any memory address, a primitive which can be easily exploited to run arbitrary code on the server (e.g. through stack return addresses). It is an even larger issue that an OPC server can be remotely compromised and used to launch attacks on other systems. Because OPC servers are often exposed in the Demilitarized Zone (DMZ), this could be a communication chain that could allow control system exploitation from the enterprise network or Internet.

Three possible OPC attack scenarios, of which are all associated with extra open ports:

- Collateral Damage by OPC-Unaware Malware;

- Opportunistic OPC Denial of Service Attack;
- Intelligent, aggressive attack against OPC hosts through a man-in-the-middle (MITM) technique

ICCP: The most serious and exposed SCADA protocol stacks are those that are used to exchange information with business partners, such as ICCP, or those used to exchange information between the corporate network and control center network. By sending a specially crafted packet to a vulnerable implementation, a remote attacker may be able to trigger the overflow to execute arbitrary code or crash a ICCP Server to cause a denial of service.

Conclusion: The cyber-physical security of real-time, continuous systems necessitates a comprehensive view and holistic understanding of network security, control theory and the physical system. Ultimately, any viable technical solutions and research directions in securing SCADA systems must lie in the conjunction of computer security, communication network and control engineering. The idea of looking into the problem in the context of control performance holds its solid bearings. However, the very large installed base of such systems means that in many instances we must for a long time to come rely on retrofitted security mechanisms, rather than having the option to design them in from scratch. This leads to a pressing need for robust SCADA-specific intrusion detection systems (IDS) and resilient control.

Reference:

[1] United States Government Accountability Office (GAO), Department of Homeland Securities (DHSs) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005)

[2] Probing a computer that is connected to the Internet to see if it has any vulnerabilities that can be exploited.

[3] VxWorks is a real-time operating system (RTOS) developed as proprietary software by Wind River of Alameda, California, US.

[4] A real-time operating system (RTOS) is an operating system (OS) intended to serve real-time applications which process data as it comes in, typically without buffering delays. Processing time requirements (including any OS delay) are measured in tenths of seconds or shorter increments of time.

[5] https://en.wikipedia.org/wiki/SQL-92

[6] User Datagram Protocol

[7] Zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or Trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction.

Author Details:

Md. Sabbir Hossain
C|CISO, CEH, COBIT5, ITIL Foundation V3, ISO/IEC 27001 LA, CLPTP