Rate my nuke: Bringing the nuclear power plant control room to iPad

Mikko Niemel

Rate My Nuke: Bringing the Nuclear Power Plant Control Room to the iPad

GIAC (GSLC) Gold Certification

Author: Mikko S. Niemelä, mikko@silverskin.com
Advisor: Manuel Humberto Santander Peláez

Accepted: 27th September 2014

Abstract

In this document, security architecture for securing network access to the control room of a nuclear power plant is described. The design takes advantage of existing, thoroughly tested components. This minimizes the amount of custom code needed, which in turn assists in vulnerability and change management. Furthermore, this paper focuses on the over-the-internet communication between mobile devices and the Control Room of nuclear power plants. There are SCADA and ICS security architecture frameworks, which can be used to plan the requirements, implementation and testing of the lower layers. These publications include SANS 20 critical security controls, Secure Data Transfer Guidance for Industrial Control and SCADA Systems published by the U.S. Department of Energy, and SANS ICS Security Resource Poster.

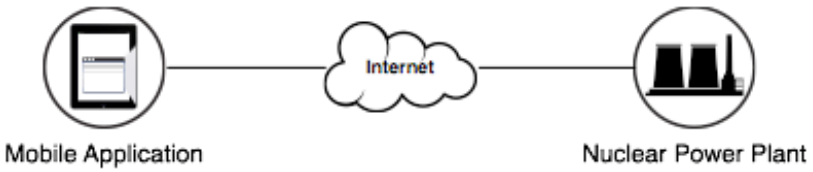
Mikko S. Niemelä, mikko@silverskin.com

1. Introduction

Industrial Control Systems monitor and control industrial processes that exist in the physical world and by design, are isolated from public networks. However, the prevailing use case, connectivity, and integration of mobile devices in the workplace has impacted the industrial environment. These isolated control system networks are now under pressure due to market demand to become Internet-accessible. Therefore, a security architecture for mobile device usage in th industrial environment must be designed with security controls and proper certificate-based authentication.

2. Introducing System Components

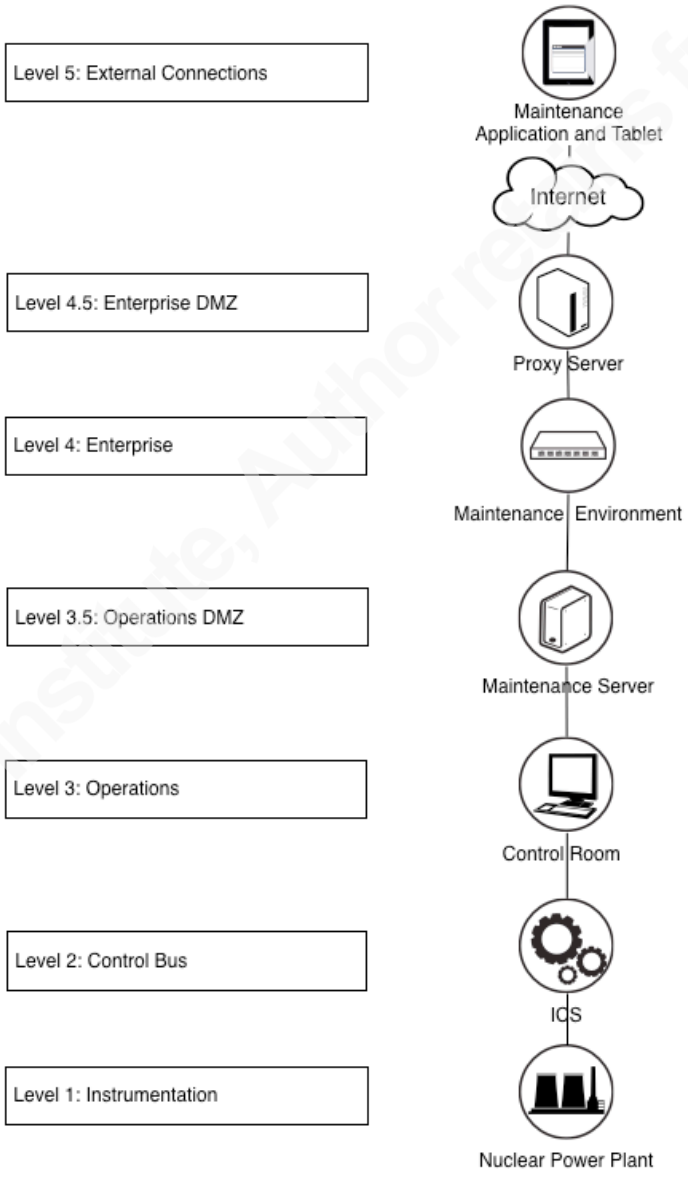
Although there are numerous SCADA-related apps located in the Apple AppStore, these applications do not provide the mobile access to critical infrastructure or internal networks hosting SCADA devices. Instead, these apps work as an interface for the user. In order to gain access to critical infrastructure, a proper network connection is required. However, connecting mobile devices to restricted environments cause immediate problems; the lack of secure design and architecture in critical infrastructure present multiple vulnerabilities and security issues. Critical infrastructure components were originally designed to stay in restricted environments without any interaction with public networks. Securing this connection cannot be solved with a single component nor a direct connection (example shown below):



In order to enable Internet connectivity with critical infrastructures, many components are required to ensure a secure connection. Evidently, a wide range of readymade controls and mitigations has been developed that can be easily leveraged as components. Commonly applied controls include network controls (e.g., firewalls, Intrusion Detection Systems [IDS], Intrusion

Prevention Systems [IPS], encryption, integrity checking), host-based controls (e.g., host-based IPS/IDS, file integrity checks, authentication, authorization, auditing), and application controls (e.g., input validation, authentication, and authorization) (Clarke, 2009).

The following image shows identified components for this architecture and a comparison to SCADA-architecture layers:



(Mahan, Fluckiger, Clements, Tews, Burnette, Goranson & Kirkham, 2011) (SANS™ Institute, 2013)

In the following table, the system components are briefly introduced:

Component	Function	Protects against
Maintenance App	Tablet application. Maintenance person uses an app in a tablet to check reactor temperature and other statistics.	Unauthorized access to client-side certificates.
Maintenance Tablet	The Tablet on which the Maintenance App runs. Connects to Proxy Server.	Tampering with Maintenance App source code or configuration.
Proxy Server	Enables secure connection with client-side certificates, forwards legitimate traffic to Maintenance Server.	Unauthorized protocols and unauthorized access. Reconnaissance.
Maintenance Environment	Network segment after Proxy Server.	Clearing tracks/Bypassing audit trail.
Maintenance Server	Server that authorizes clients and transfers legitimate commands to Control Room.	Malicious input and output. Privilege escalation. Violation of access rights.
Control Room & Industrial Control System (ICS)	Receives requests from Maintenance Server, performs operations in restricted environment.	Invalid protocols and commands.
Nuclear Power Plant	Component of critical infrastructure.	

2.1. Maintenance App

Maintenance Apps can be downloaded from a digital distribution platform (e.g., the Appstore, Android market, Nokia OVI). As a simple interface for making calls to the Control Room via the Maintenance Server, the Maintenance App perform connects to a Proxy Server through certificates. This allows mutual authentication to occur and establishes a secure communication channel. The App sends HTTP requests to the Maintenance Server. Then, the Maintenance Server provides a web server, which receives the requests. The requests are later translated to Control Room calls transmitted with lower level network protocols (TCP/UDP). Control Room devices transform these to valid ICS protocols, depending on the setup.In essence, the Proxy Server proxies the network traffic, and the Maintenance Server proxies the functionality. This architectural separation allows the separation of duties principle to occur on different layers (network & application). The App can only send HTTP messages which can be validated by the Maintenance Server and in this way performs whitelisting.

Latency is critical for SCADA systems, especially when the lower level field devices include Phasor Measurement Units (PMU). Network devices, like firewalls, may introduce too much latency (Mahan, Fluckiger, Clements, Tews, Burnette, Goranson & Kirkham, 2011). As the method for traffic to reach the Maintenance Tablet varies from GSM and 3G networks to Wi-Fi connections, network latency cannot be controlled. Theremore, it is important to understand that introducing control room features to internet reachable mobile devices should be limited to features that are not latency-sensitive.

The main security function of the App is to provide client-side certificate-based authentication. The Maintenance App itself cannot be trusted but should be designed to protect the client-side certificate, which is stored in the configuration.

The security features of the Maintenance Application include:

- The certificate store functionality of the underlying operating system to provide secure storage for cryptographic keys (e.g., iOS, Android, etc)

• A unique device fingerprint that is created for each device at the time of installation to ensure that client software cannot be moved to other devices, turning the devices into reliable authentication tokens (Schneider, Lee & Schell, 2004)

• The PKI authentication, which is used together with the device fingerprinting to ensure that secure remote access is comparable to that of a 2-factor authentication solution (typically used in financial and military sectors)

• The security of confidential information not being stored on the device. All security-relevant functionalities and data are stored on the Maintenance Server side.

2.2. Maintenance Tablet

The Maintenance Tablet is the acting device platform for the App. It provides a safe running environment for the App and prevents unauthorized access. The tablet is considered to be an off-the-shelf product (e.g., iPad, Galaxy Note, Nokia tablet) and has the capability to detect anomalies in app source code and configuration as downloadable apps are digitally signed by the distributor; all major distribution platforms provide certificate-based signing of the software. Using this method, the tablet provides additional security for detecting any tampering with the Maintenance App. (Schneider, Lee & Schell, 2004)

2.3. Proxy Server

When both the App and tablet are considered as client-side components, the Proxy Server is the first to act as a server-side component. As communication is sent from the tablet to the Proxy Server, the Proxy Server forwards certificate-based validated traffic, through the Maintenance Environment, to the Maintenance Server.

The Proxy Server controls access to the Maintenance Environment by authenticating clients based on client-side certificates and allows authenticated clients to access Maintenance Server functionalities based upon their entitlements. All other connection attempts are blocked at the Proxy Server, i.e., at the network edge.

Client certificates are used for client authentication. Clients are required to present valid client certificates to the Proxy Server in order to access the Maintenance Server functionalities. The Proxy Server verifies that all client certificates are issued and digitally signed by the Certificate Authority (CA) in the Maintenance Server. Unauthorized or revoked access requests

are denied before the communications reach the Maintenance Server. Therefore, the Proxy Server provides a secure bastion host and a strong network edge security layer in the front of the rest of the network.

The Proxy Server prevents reconnaissance of the internal network as it blocks any attempt to connect without a valid client certificate. The server only forwards valid whitelisted protocols to selected destinations. All other traffic is dropped.

2.4. Maintenance Environment

The Maintenance Environment is the network segment between the public Internet and the Control Room. The Proxy Server forwards all allowed traffic through the Maintenance Environment to the Maintenance Server. TLS is terminated at the Proxy Server. As the traffic enters this network segment in clear text, it is possible to implement a required intrusion detection system and additional logging capabilities (Laing, Christopher, Badii, Atta, Vickers, Paul, 2012).

The Maintenance Environment provides an audit trail of all network activity between the clients and the Maintenance Server. Network level audit logging occurs in the Maintenance Network.

2.5. Maintenance Server

The Maintenance Server provides over-the-Internet maintenance functionalities to Maintenance Apps. It operates as a centerpiece between clients and the Control Room. The security functions of the server include:

- running a Certificate Authority service that issues and revokes certificates
- authorizing clients, after a successful authorization, CA grants unique client-side certification
- receiving and validating client requests through the Proxy Server and the Maintenance Environment
- validating input from incoming traffic
- authenticating users

- performing output sanitization for commands to the Control Room
- logging system level audit
- detecting application level attacks

The security of the Maintenance Server environment is based on the use of Public Key Infrastructure (PKI). PKI is a standardized way of creating, managing, and revoking digital certificates. In the context of the Maintenance Environment, PKI certificates are used to control client access to the Maintenance Server via the Proxy Server (Request for Comments: 2459).

All Maintenance Tablets are authenticated using Client Certificate Authentication: all clients must have a valid certificate that is signed by the proper Certificate Authority. The authentication is performed on the Transport Layer of the OSI Model to make it transparent to the application layer.

The PKI implementation of the Maintenance Environment relies on an automatic and self-managed Certification Authority (CA) that issues and revokes certificates for all clients. (The CA server is explained in the following chapter.) Three different certificate categories are used in the CA hierarchy:

- The issuing CA certificate: This certificate is used to issue and revoke other certificates. The public key related to the CA can be utilized with no concern for its confidentiality. The private key of the CA is the most critical component in the security of the Maintenance Environment. If the private key is compromised, all certificates must be re-issued.
- Proxy Server Certificate: This certificate is issued by the Issuing CA for the Proxy Server. The Proxy Server needs the certificate because clients need to be able to verify the authenticity of the Proxy Server at the time of client authentication.
- Client certificates: Each client has a unique certificate that is issued individually by the CA server. Each certificate contains a unique client identifier, a Distinguished Name (DN) field that is tied to the identity of the client.

2.5.1. Certification Authority (CA)

The Certification Authority service is an internal part of the Maintenance Server. The role of the service is to issue and revoke client certificates. When a new client needs to access the network, the CA receives a request to create a new certificate. A new certificate signing request is created that contains the unique client identifier number. The signing request is signed by the CA after which the fresh client certificate is created and transferred to the requesting client.

When a client's access to the network and Maintenance Environment is revoked (i.e., access rights are removed), the CA service adds the related client certificate to a Certificate Revocation List and digitally signs the list.

In this setup, the CA controls access to the Maintenance Server. A client using a global certificate can obtain access only to a service that provides private certificate delivery service. Once the client receives a private certificate, it is allowed to connect to the main functionality of the Maintenance Server. This method enforces the separation of duties principle. Before the client can connect to the main functionality, management functions need to grant permission to retrieve the client-side certificate.

2.5.2. Client Certificate Enrollment

The initial request for a new certificate is processed over TLS from the Maintenance Tablet to the Maintenance Server via the Proxy Server by using a "shared, global client certificate." This global certificate is installed in the client's operating system's certificate store at the time of software installation. The global certificate is used for the sole purpose of transferring the per-client unique authentication certificate safely to the client (only encryption, i.e., confidentiality is a requirement at this point). After the enrollment phase, the global certificate is no longer used. The global certificate only allows access to the Maintenance Server's Certificate Enrollment Service.

The benefit of using a shared global certificate during enrollment is allowing only those clients that have installed the Maintenance Tablet software to request a new certificate from the Maintenance Server. In other words, even though the Proxy Server and Maintenance Server are connected to the Internet, only installed Maintenance Tablets are able to send requests to them. Most of the public Internet is silently blocked out.

The client enrollment process always requires that the client and user arecreated in the Maintenance Server prior to certificate enrollment. The user must enter a unique code in the client application to make the request to the Maintenance Server. The unique code is generated by the authorizing party. It can be delivered in physical form; for example, a receptionist could hand it over to a customer. The user enters the unique code to the App, and the App delivers the request message with the code to the Maintenance Server in order to retrieve the matching private certificate. When the App initializes a new connection with the private certificate, the Proxy Server forwards its traffic to another port in the Maintenance Server. The main functionalities are run on that port.

2.5.3. Certificate Revocation List (CRL)

The Clients are blocked out of the network by using a Certificate Revocation List. The CA service on the Maintenance Server creates a new CRL file whenever a client's access rights are removed. For example, when a user is removed from the user database, the Maintenance Server runs the revoke command automatically on the corresponding client certificate. The client certificate is then added to a Certificate Revocation List, and the list is consequently signed by the CA service. The CRL file is then automatically transferred to the Proxy Server and put into use immediately. This provides a very robust way of assuring that access control to the application is protected:

1. When access rights are removed, the client will be unable to access the Maintenance Server application again (unless the client receives new access rights and a new client certificate).

2. The access is blocked on the network edge, at the Proxy Server, rather than on application level.

3. A revoked certificate cannot be re-used. This provides a unique and cryptographically strong audit trail for logging each successful and failed connection request by each client.

4. The CRLs cannot be faked. Only the CA is able to sign a verifiable new version of the CRL. If the CRL is faked somehow, the Proxy Server could not verify its signature, and thus, all clients would be blocked out.

5. If the CRL file becomes unavailable, the Proxy Server blocks access to the network (fail safe mode).

2.6. Control room and ICS

Industrial control systems (ICS) control and monitor communications for closed loop process automation. In the lower level, ICS equipment and process automation devices gather data from sensors and send signals to implement control algorithms to process changes (National Security Agency, 2010).

The setups of Control Room and ICS/SCADA devices vary greatly. The idea behind this concept is to have one device capable of communicating network level protocols (e.g., TCP or UDP) to the Maintenance Server and then translating these messages to valid ICS protocol calls (e.g., Modbus, etherCAT, CIP) for other ICS/SCADA devices.

The Control Room's and Industrial Control System's security feature is to perform whitelisting for all system calls. Validation is performed for all incoming calls. Access control and logging also occur to provide accountability (Mahan, Fluckiger, Clements, Tews, Burnette, Goranson & Kirkham, 2011).

2.7. Nuclear Power Plant

The Nuclear Power Plant is the power generation component of this system. This architecture enables the plant operations personnel to operate from distant locations. Plant operations personnel in a control center monitor the status of processes on PC-based operator workstations and/or on large system mockup displays. Closed loop process automation is monitored, and independent monitoring systems trigger alarms to operations personnel if safety limits are reached.

3. System Component Requirement

As the components perform different security roles, different requirements apply to each of them. Listing and reviewing all requirements in the design phase are recommended in order to ensure that they are included in the project scope. Security requirements act as an input to architecture design.

3.1. Maintenance App

The Maintenance App provides a user interface for the maintenance personnel. Without any physical control of the device the App is stored in, we cannot assume that the Maintenance App is safe or even trusted. However, the Maintenance App plays a significant role in the holistic approach of this system security. The App needs to be designed so that it will provide the best effort to protect the client-side certificate and the configuration information. The valid configuration file and certificate should be hashed with reasonable one-way hashing algorithms.

3.2. Maintenance Tablet

Like the App above, the Maintenance Tablet cannot be trusted. It is still important that users of Maintenance Tablets make every effort to protect their devices. This raises the barrier to perform reconnaissance or any other planning activities for the attack (Schneider, Lee & Schell, 2004) (Laing, Christopher, Badii, Atta, Vickers, Paul, 2012).

Acceptable usage of the tablet needs to be defined in a security policy. The acceptable use policy and the requirements considering Maintenance Tablet usage are similar to workstation environment requirements.

The following table describes Maintenance Tablet protection requirements:

Requirement	Benefit	Threat
Centrally manage the configurations of clients	Assets can be managed efficiently (i.e., security, etc.)	Uncontrollable client environment
Run antivirus solution on each client	Provide protection against mobile malware	Mobile malware
Deploy a remote wipe functionality on clients	In case of stolen device, safely remove sensitive data from the device	Stolen or lost device

3.3. Proxy Server

The Proxy Server is the perimeter of the critical network area and therefore under the greatest threat of offensive actions. If Maintenance Tablets are always used from the same network area (or same IP-range), it is possible to reduce the attack surface by firewall rules that eliminate connections from elsewhere.

However, in a typical case, the Proxy Server needs to be accessed from the public Internet. The Proxy Server should not respond to anything other than valid requests with valid protocols and a valid certificate.

The Proxy Server's security requirements are two-fold: protecting the actual functionality (secure communication) and protecting itself (operating system hardening and reducing overall attack surface).

3.3.1. Secure communication requirements

Secure client-server communication requires the following security features:

Security feature	Benefit	Threat
Use only secure and robust communication protocols	Assurance that the communication protocols can be trusted	• Exploiting of communication protocols' weaknesses
Encrypt data communications	Provides a trusted communications channel	• Eavesdropping • Modification attacks, i.e., impersonation
Secure authentication	Authenticates each client uniquely and creates a verifiable audit trail of all activities	• Man-in-the-middle attacks • Unauthorized use

		Impersonation
Secure management of cryptographic keys	Provides assurance that the security mechanisms are implemented correctly	• Impersonation • Breach of security controls

Communication protection is of the utmost importance when using wireless communication protocols, as wireless traffic can be intercepted more easily than traditional wired communication.

Data in-transit is always encrypted by strong encryption protocols, either SSLv3 or TLS, using what is currently understood as strong cryptographic ciphers. Conversely, ciphers that are known to contain cryptographic weaknesses should be disabled.

Recommended encryption key lengths and algorithms:

1. CA Server certificate: 2048 bit RSA with SHA1
2. Proxy Server certificate: 1024 bit RSA with SHA1
3. Client certificates: 1024 bit RSA with SHA1

The App and Proxy Server certificates use 1024 bit keys because the clients use hardware with low-end processing power. At the time of writing, 1024 bit RSA keys are considered to be very secure. It is possible to increase the client key length to 2048 bits if the cryptographic threat landscape evolves and 1024 bit RSA is no longer considered to be secure enough (Klima & Sigmon, 2012).

3.3.2. Operating system hardening requirements

The most crucial point in the security architecture is the Proxy Server, as it protects the rest of the architecture from cyber threats on the Internet. The Proxy Server is designed to act as a high-security bastion host that forwards requests back and forth between clients and the Maintenance Server.

The Proxy Server operating system should be hardened. Implementing operating system hardening greatly reduces the attack surface and server visibility to public networks. The recommendation is to meet the security requirements of The Center for Internet Security (CIS) security benchmark or any other relevant benchmark (Stewart, 2004). All used libraries and binaries should be reviewed so as not to include any known vulnerabilities. Scheduled network level vulnerability scans can be used to detect known vulnerabilities from outside (Beaver, 2006) (Cunningham, Dykstra, Fuller, Gatford, Gold, Hoagberg, Hubbard & Snedaker, 2007).

3.4. Maintenance Environment

The Maintenance Environment varies from a dedicated network segment to a more general internal network. Network level monitoring takes place here. Depending on the functionalities of the Maintenance Server application logic, different alerts and monitoring systems can be deployed. If HTTP protocol is used, possible malicious payloads might be transferred in fragmented packets. In order to inspect HTTP, normalizing the traffic and applying necessary rules is recommended. The Maintenance Environment also hosts the Maintenance Server, which is the main functioning server in the network segment. It is important that the Maintenance Server is not spoofed and that any spoofing attempt is noticed. Both ARP cache poisoning detection and HTTP normalization can be deployed using Snort's preprocessors (arpspoof for ARP cache poisoning and http_decode for HTTP normalization) (Orebaugh, Biles & Babbin, 2005).

The packet inspection can be performed on different levels depending on the business needs and compliance requirements of the system. When the packet log is available, it can be compared to the application log to verify certain events. The level of accuracy should be in line with data retention policies and legal and business archival requirements.

This architecture enables everything other than whitelisted protocols to be dropped at the Proxy Server. TLS is terminated at the Proxy Server and has accepted traffic flows in clear text in the Maintenance Environment. Intrusion detection rules can be applied to clear text traffic.

The concept of whitelisting has many functions. Whitelists can be defined for a variety of network and security metrics including users, assets, applications, and others. Network protocols can be actively enforced via a deny policy on a firewall or IPS. Dynamic controls can also be put into place. For example, if an exception to a policy is detected, a script can be run to tighten the

specific perimeter defenses of the Proxy Server (Laing, Christopher, Badii, Atta, Vickers, Paul, 2012)(Weiss, Joseph,2010).

3.5. Maintenance Server

All previous components create a chain that ensures that a connection to the Maintenance Server is authenticated and an audit trail exists. The Maintenance Server's security requirements are at the application level because the server provides application level functionality to the App. The Maintenance Server needs to be capable of detecting when privileges are changed or access to restricted information takes place.

Security requirement	Benefit	Threat
Input validation and output sanitation	Filter and validate any data that servers receive, allowing only known-good input to be passed to the Control Room	Input validation attacks; injections
User authentication	Allow access to all authorized users	Unauthorized access
Application level audit logging	Establish an audit trail to provide documentary evidence of server events	Attacks and compromise go unnoticed for a long time
Application level attack detection	Detect, log and drop malformed and malicious attacks (known attack patterns in HTTP)	Malicious probes and attacks to Maintenance Application and system compromise

3.6. Control Room & ICS

When it comes to cyber security, the electric industry has received more attention than any other industry. Consequently, the efficacy of this implementation holds great importance, as it will probably be applied to other industries. The North American Electrical Reliability

Corporation (NERC) Control System Security Working Group (CSSWG) has issued several documents that should be relevant to different industries. They include an annual top-ten ICS vulnerability list, ICS patching guidelines, ICS time-stamping guidelines, and ICS business-network connectivity guidelines. The North American bulk electric system (transmission and generation) is under the purview of the U.S. Federal Energy Regulatory Commission (FERC).

4. Security testing the components

Implementing defense-in-depth architecture requires comprehensive security testing on each layer individually and on the architecture as a whole. Testing the Maintenance App depends on the implementation and chosen programming language. Testing should focus on client-side certificates and configuration protection and anti-tampering functionality.

The Maintenance Tablet is considered to be an off-the-shelf product and is out of testing scope. The Proxy Server is facing the public Internet and needs to be thoroughly evaluated from outside as well as from inside.

The Maintenance Environment is highly customized and is therefore out of scope for general testing. Penetration tests that focus on application level security controls should be conducted against the Maintenance Server.

4.1. Proxy Server

The Proxy Server is directly connected to the public network and is thus constantly probed by various scanners and targeted by malicious entities. The Proxy Server must be hardened from the outside as well as from the inside. The outside is evaluated using service discovery and vulnerability scanning. The inside is evaluated using operating system level verification combined with configuration checks to detect any unauthorized changes within the system.

4.1.1. Service Discovery

Service discovery is a method of finding processes that listen to network traffic. The method is divided into port scanning and service identification. By performing service discovery, we ensure that nothing other than mission critical services are visible to the public network. Both port scanning and service discovery can be done with Nmap, the famous port scanning tool, which supports service identification (Allen, 2012) (Henry, 2012).

4.1.2. Vulnerability Scan

Vulnerability scanning is conducted to find known vulnerabilities within the processes that must be running on the server. There are open source tools like Nmap and Scapy and many commercial products such as Nessus, Nexpose, Core Impact, etc. For common protocols and services, vulnerability databases such as exploit-db.com and OVDB can be used. A Nmap scripting engine combined with an exploit database and Nmap version scan can be used to find known vulnerabilities from available services.

For proprietary protocols, fuzz testing is conducted. Fuzzing is used to discover unknown vulnerabilities and weaknesses at the protocol level. Tools like Nessus or Scapy can be used for fuzzing (Allen, 2012)(Clarke, 2009).

4.1.3. Verifying secure configuration

After service and vulnerability scanning, the Proxy Server should look sound from the outside. To ensure that installation has been successful and security requirements regarding operating system hardening are met, internal configuration can be verified. There are many readymade tools for that. Verification can also be done manually.

Lynis is a command line tool for auditing linux and unix operating system configuration. It provides a numerical result for the current state. It can also be set as a cronjob to compare the current state to the known good configuration to verify if any changes have happened. Lynis can be downloaded from: http://www.rootkit.nl/projects/lynis.html.

CIS-CAT is a security benchmark verification tool offered by Center for Internet Security (CIS). It compares the current state of the operating system against the CIS Benchmark. The benchmarks can be used for free for personal use. However, to automatize the audit, the CIS-CAT tool is available only as a commercial product. More information about the CIS-CAT tool can be found at: http://benchmarks.cisecurity.org/downloads/audit-tools/.

Bastille is a hardening tool to “lock down” the operating system. It has a walkthrough wizard that helps to set the correct hardening settings. After asking questions about relevant and mission critical services, it creates rollback script to be used in case something goes wrong. Bastille also comes with an assessment mode to evaluate the current state of the operating system. Bastille can be found here: http://www.bastille-linux.org/.

It is possible to verify the configuration manually. In order to begin, an inventory needs to be created from mission critical binaries and services. Next, a comparison of used binaries and services takes place. For example, all files in use can be listed by the lsof command in linux. Processes and services can be listed with ps and netstat (Cunningham, Dykstra, Fuller, Gatford, Gold, Hoagberg, Hubbard & Snedaker, 2007).

4.2. Maintenance Server

Maintenance Server logic depends on the Control Room and ICS systems behind it. Penetration testing is recommended against the Maintenance Server to verify that application layer security controls are in place and work properly. Performing penetration testing provides current information about the system's security state. It is essential to schedule recurring penetration tests and mitigate the findings in order to ensure that the Maintenance Server is able to withstand or resist attacks from internal or DMZ networks (Henry, 2012) (Allen, 2012).

The primary focus of application level testing are the input and access control mechanisms of the Maintenance Server. The tests demonstrate whether or not the Maintenance Server is able to reject malicious input and only process requests where all input fields contain valid, expected values. It is important that the requests are rejected and that a log entry is created indicating an attack.

5. Conclusion

Securing network access from the public Internet to the control room of a nuclear power plant (or critical infrastructure) is possible with some limitations. This can be achieved by assigning security attributes or roles to each component in the system. The first component only allows incoming network traffic from clients having a valid certificate and blocks all other traffic. The environment monitors and logs all traffic thereafter. The architecture design is all about defining what traffic can be considered legitimate. The more detailed the definition, the easier it is to use whitelisting to detect anomalies and generate an alarm.

Only one component receives packets from the Internet. The required actions are to validate the input (ensuring that it conforms to specifications) and check authorization. Only then are messages from the client translated to ICS-compatible protocols and forwarded to the target system.

An audit trail is created for each step and all components perform validation based on their security role. By implementing all defined components, security is no longer dependent on one main control – the isolation of the network.

6. References

Allen, L. (2012). Advanced penetration testing for highly-secured environments: The ultimate security guide. Packt Publishing.

Beaver, K. (2006). Hacking for dummiesÂ®, 2nd edition. For Dummies.

Clarke, T. (2009). Fuzzing for software vulnerability discovery. In Department of Mathematics, Royal Holloway, University of London. Retrieved from https://www.ma.rhul.ac.uk/static/techrep/2009/RHUL-MA-2009-04.pdf

Cunningham, B., Dykstra, T., Fuller, E., Gatford, C., Gold, A., Hoagberg, M. P., Hubbard, A., & Snedaker, S. (2007). The best damn it security management book period. Syngress.

Dubrawsky, I. (2009). Eleventh hour security . Syngress.

Fernandez-Buglioni, E. (2013). Security patterns in practice: Designing secure architectures using software patterns. John Wiley & Sons.

Henry, K. M. (2012). Penetration testing: Protecting networks and systems. IT Governance Ltd.

Klima, R., & Sigmon, N. (2012). Cryptology: Classical and modern with maplets. Chapman and Hall/CRC.

Laing, Christopher, Badii, Atta, Vickers, Paul (2012). Securing Critical Infrastructures and Critical Control Systems. IGI Global

Mahan, R., Fluckiger, J., Clements, S., Tews, C., Burnette, J., Goranson, C., & Kirkham, H. (2011). Secure data transfer guidance for industrial control and scada systems. Pacific Northwest National Laboratory Richland.

McNab, Chris (2007). Network Security Assessment, Second Edition.. O'reilly

National Institute of Standards and Technology. (2009). Recommended security controls for federal information systems and organizations. NIST. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

National Security Agency (2010). A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS). Retrieved November 23, 2013, from http://www.nsa.gov/ia/_files/ics/ics_fact_sheet.pdf.

Orebaugh, A., Biles, S., & Babbin, J. (2005). Snort cookbook. O'Reilly Media, Inc.

Request for Comments: 2459, . "Internet X.509 Public Key Infrastructure Certificate and CRL Profile." . N.p., n.d. Web. 16 Jan 2014. <http://www.ietf.org/rfc/rfc2459.txt>.

SANS Institute (2014). 20 Critical Security Controls. 20 Critical Security Controls. Retrieved from http://www.sans.org/critical-security-controls/guidelines.php

SANS Institute. (2013). Ics security resource poster & brochure [Web]. Retrieved from https://ics.sans.org/resources/ics-security-resource-poster

Schneider, H., Lee, V., & Schell, R. (2004). Mobile applications: Architecture, design, and development. Prentice Hall.

Stewart, J. M. (2004). Security + fast pass. Sybex.

The Center for Internet Security. (2007). Center for internet security benchmark for debian linux v1.0. The Center for Internet Security. Retrieved from http://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf

Weiss, Joseph (2010). Protecting Industrial Control Systems from Electronic Threats. Momentum Press

Last Updated: September 17th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Dallas Fall 2019	Dallas, TXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
SANS Riyadh October 2019	Riyadh, SA	Oct 05, 2019 - Oct 10, 2019	Live Event
SANS Baltimore Fall 2019	Baltimore, MDUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS October Singapore 2019	Singapore, SG	Oct 07, 2019 - Oct 26, 2019	Live Event
SANS Lisbon October 2019	Lisbon, PT	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS San Diego 2019	San Diego, CAUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SIEM Summit & Training 2019	Chicago, ILUS	Oct 07, 2019 - Oct 14, 2019	Live Event
SANS Doha October 2019	Doha, QA	Oct 12, 2019 - Oct 17, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WAUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS SEC504 Madrid October 2019 (in Spanish)	Madrid, ES	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Denver 2019	Denver, COUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS London October 2019	London, GB	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Cairo October 2019	Cairo, EG	Oct 19, 2019 - Oct 24, 2019	Live Event
SANS Santa Monica 2019	Santa Monica, CAUS	Oct 21, 2019 - Oct 26, 2019	Live Event
Purple Team Summit & Training 2019	Las Colinas, TXUS	Oct 21, 2019 - Oct 28, 2019	Live Event
SANS Training at Wild West Hackin Fest	Deadwood, SDUS	Oct 22, 2019 - Oct 23, 2019	Live Event
SANS Orlando 2019	Orlando, FLUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Houston 2019	Houston, TXUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Amsterdam October 2019	Amsterdam, NL	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS DFIRCON 2019	Coral Gables, FLUS	Nov 04, 2019 - Nov 09, 2019	Live Event
Cloud & DevOps Security Summit & Training 2019	Denver, COUS	Nov 04, 2019 - Nov 11, 2019	Live Event
SANS Paris November 2019	Paris, FR	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Sydney 2019	Sydney, AU	Nov 04, 2019 - Nov 23, 2019	Live Event
SANS Mumbai 2019	Mumbai, IN	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Bahrain September 2019	OnlineBH	Sep 21, 2019 - Sep 26, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced