ICS Security Architecture

Chris Hankin
Network Segmentation and Segregation

• Segmentation establishes security domains – uniform level of trust

• Minimise traffic across domain boundaries

• Segregation involves ruleset that defines which communications can happen across boundaries
Common techniques

• Logical network separation enforced by encryption or network device enforced
  • VLANS
  • Encrypted VPNs
  • Uni-directional gateways – for example data diodes
• Physical network separation
• Network traffic filtering – network layer, state-based, port and/or protocol layer, or application layer
OSI Model – 7 layers

1. Physical – raw bit streams
2. Data link – reliable transmission of data frames
3. Network – addressing, routing and traffic control
4. Transport – segmentation, ack and multiplexing
5. Session
6. Presentation – encryption/decryption
7. Application – high level APIs
Defense in Depth

• Apply techniques at more than the network layer
• Use the principle of least privilege and need-to-know
• Separate information and infrastructure based on security requirements
• Implement whitelisting rather than blacklisting
Boundary protection

- Gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, HIDS and NIDS, encrypted tunnels, managed interfaces, mail gateways and uni-directional gateways.

- Demilitarized Zones (DMZ) – host or network segment between security domains.

- Configuration of boundary protection devices to fail in predetermined state – safety versus security
Firewalls

• Packet Filtering – access controlled by a ruleset; operate at network layer: drop, forward or send message to originator
• Stateful Inspection – transport layer firewall keeping track of sessions
• Application-Proxy Gateway – application layer firewall
• High security but performance overheads
• Internal or between ICS and Corporate network
Firewalls contd

• Blocking communications except those specifically allowed
• Enforcing secure authentication
• Enforcing destination authorization
• Recording information flow
• Implementation of ICS operational policies
• Designed with documented and minimal connections outside the ICS
Block all incoming connections

Blocks all incoming connections except those required for basic internet services, such as DHCP, Bonjour and IPSec.

- Skype
- Skype Meetings App

Automatically allow built-in software to receive incoming connections

Automatically allow downloaded signed software to receive incoming connections

Enable stealth mode

Don't respond to or acknowledge attempts to access this computer from the network by test applications using ICMP, such as Ping.
<table>
<thead>
<tr>
<th>Area of Weakness</th>
<th>Rank</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boundary Protection</td>
<td>1</td>
<td>• Undetected unauthorized activity in critical systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Weaker boundaries between ICS and enterprise networks</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>2</td>
<td>• Lack of accountability and traceability for user actions if an</td>
</tr>
<tr>
<td>(Organizational Users)</td>
<td></td>
<td>account is compromised</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Increased difficulty in securing accounts as personnel leave the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>organization, especially sensitive for users with administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access</td>
</tr>
<tr>
<td>Allocation of Resources</td>
<td>3</td>
<td>• No backup or alternate personnel to fill position if primary is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unable to work</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Loss of critical knowledge of control systems</td>
</tr>
<tr>
<td>Physical Access Control</td>
<td>4</td>
<td>• Unauthorized physical access to field equipment and locations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provides increased opportunity to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Maliciously modify, delete, or copy device programs and firmware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Access the ICS network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Steal or vandalize cyber assets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Add rogue devices to capture and retransmit network traffic</td>
</tr>
<tr>
<td>Account Management</td>
<td>5</td>
<td>• Compromised unsecured password communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password compromise could allow trusted unauthorized access to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>systems</td>
</tr>
<tr>
<td>Least Functionality</td>
<td>6</td>
<td>• Increased vectors for malicious party access to critical systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rogue internal access established</td>
</tr>
</tbody>
</table>
Network Segregation

• Dual-homed computers can pass traffic from one network to another
• Only firewalls should be configured as dual-homed systems in an ICS
• In the next slide the Data Historian is a possible source of weakness
• The routers offer basic packet filtering services
• The architectures in the following slides are from NIST sp 800-82r2
Some issues

• Use different anti-virus software in the Corporate and ICS systems
• Actively patch servers in DMZ
• Firewall should only allow connections between the control network and the DMZ that are initiated by control network devices
• For multiple firewall solutions use firewalls from different providers
Defense-in-Depth

• Firewalls, DMZ and intrusion detection
• Security policies
• Training programme
• Incident response mechanisms
• Physical security
Attack vectors

• Backdoors and holes in network perimeter
• Vulnerabilities in common protocols
• Attacks on field devices
• Database attacks
• Comms hijacking and man-in-the-middle attacks
• Spoofing attacks
• Attacks on privileged and/or shared accounts
Firewall Policies

- Stateful rules that are both IP address and port (application) specific
- Restriction to secure protocols such as HTTPS; HTTP, FTP and other unsecured protocols represent a security risk
- Deny hosts outside the control network establishing connections to hosts inside
- If there is a DMZ insecure protocols can be used between the control network and the DMZ (Modbus/TCP) and the corporate network and the DMZ (HTTP)
Outbound rules

• Limited to essential communications

• Source and destination restricted by service and port

• Outbound filtering to prevent forged IP packets

• Internet access by devices on the control network should be strongly discouraged.
Firewall Rules for Specific Services

- Domain Name Service (DNS): No DNS requests into control network, No DNS requests from control to corporate, control to DMZ on a case-by-case basis.
- HTTP should not be allowed to cross from the public/corporate to the control network.
- FTP and Trivial FTP (TFTP): TFTP has no authentication, so disallow; FTP should only be used if secured by some other means.
- Telnet is unencrypted so disallow inbound and only allow outbound over VPN or encrypted tunnel.
**Firewall Rules for Specific Services**

- **Dynamic Host Config. Protocol (DHCP):** recommended to use static configuration, otherwise enable DHCP snooping to identify rogue servers.
- **SSH recommended for access into control network if necessary.**
- **Simple Object Access Protocols should only be used with deep packet inspection and/or application layer protocols.**
- **SMTP should not be allowed into the control network; outbound could be used for alerts.**
Firewall Rules for Specific Services

- SNMP should only be used in secure versions (V3 and above)
- Distributed Component Object Model (DCOM) underpins OPC which dynamically opens a wide range of ports. Should only be used between the control network and the DMZ.
- SCADA protocols (Modbus/TCP, Ethernet/IP, IEC 61850, ICCP and DNP3) should only be used within the control network
Specific ICS Firewall Issues

• Network Address Translation: private subnet IP 192.168.1.xxx to corporate net 192.6.yyy.zzz

• Placement of the Data Historian is problematic in two zone architectures

• Remote support access

• Multicast traffic (for example Ethernet/IP and Fieldbus) – good for time synchronization between multiple devices – and Network Address Translation issues.
Man-in-the-Middle Attacks

- Poisoning Address Resolution Protocol (ARP) caches. The ARP tables map between MAC addresses (Layer 2) and IP addresses (Layer 3).
- Replay attack
- False negative of false positive messages
Mitigations

• MAC Address Locking – locks a specific MAC address to a specific port on a managed switch
• Statically coded ARP tables
• Encryption prevents reverse engineering of protocol messages but has an overhead
• Strong authentication also provides resilience against MITM attacks
• Monitoring for ARP poisoning
Other issues to be considered

• Authentication (verifying claimed identity) and authorization (granting user access privileges)
• Monitoring, logging and auditing
• Incident detection, response and recovery