Industrial Control Systems Security
A Perspective on Product Design

Tien Van
Tracy Amaio, Ph.D.
tvan@sequi.com
teamaio@sequi.com
INDUSTRIAL CONTROL SYSTEMS (ICS)

Characteristics:
- Long operational life (10+ yrs)
- Small to large geographic area
- Highly complex and found everywhere
- Field RTUs/PLCs are in the open, most are unprotected
- Routable (TCP/IP) protocols
- “Legacy” non-routable (serial) protocols:
  - Radio, leased line, dial-up, and multi-drop links
  - Low data throughput
  - Slow telemetry polling
  - Modbus, DNP3 protocols (MTU – RTU communications)
  - Difficult to add security to existing software
  - Little/no auditing, logging
VULNERABILITIES – THE PROTOCOLS

Most legacy protocols do not have authentication making them easy to exploit and attack

- Modbus was designed to program controllers by sending Read and Write I/O registers commands, for example:
  - List defined points and their values
  - Request information about Modbus servers, PLC configurations...
  - Clear, erase, or reset diagnostic information
  - Force slave devices into “listen only” mode

<table>
<thead>
<tr>
<th>Modbus RTU</th>
<th>Start 3.5 char time</th>
<th>Addr 1-byte</th>
<th>Func 1-byte</th>
<th>Data 0-252</th>
<th>CRC 2-byte</th>
<th>End 3.5 char time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modbus ASCII</td>
<td>Start :</td>
<td>Addr 2-byte</td>
<td>Func 2-byte</td>
<td>Data 2x (0-252)</td>
<td>LRC 2-byte</td>
<td>End CR LF</td>
</tr>
</tbody>
</table>

- DNP3 has source and destination addresses that can be useful in Man-in-the-Middle attacks, such as:
  - Turn off unsolicited reporting to stifle specific alarms
  - Spoof unsolicited responses to the Master to falsify events and trick the operator into taking inappropriate actions
  - Issue unauthorized stops, restarts, or other functions that could disrupt specific operations

<table>
<thead>
<tr>
<th>DNP3 [Header + Data]</th>
<th>Max frame size: 292 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header = 0x05 1-byte</td>
<td>0x64 1-byte Len 1-byte Ctrl 1-byte Dst 2-byte Src 2-byte CRC 2-byte</td>
</tr>
</tbody>
</table>
COMMON ICS ATTACKS

- **Maintenance port**
  To install a malicious program

- **Spoofing**
  To masquerade as another to initiate an unauthorized action

- **Replay**
  To record and retransmit valid data (manipulating time variable) to trigger unpredictable results

- **Man-in-the-Middle (MITM)**
  To intercept, alter, and relay a communication message
  - A simple radio MITM can be setup by a combination of directional transmitter & jammer
RISK MANAGEMENT - LEGACY SYSTEMS

AVOIDANCE

“Eliminate back door”
(remove risk)

RETENTION

“Do nothing”
(accept risk and budget for it)

REDUCTION

“Take action”
(lessen the risk)

USE

ENCRYPTION

Protect against the threat of:
- Eavesdropping
- Message replaying
- Data altering
## LEGACY RETROFIT ISSUES

<table>
<thead>
<tr>
<th>Top Questions</th>
<th>What Customers Want</th>
</tr>
</thead>
</table>
| How do we plan for migration?                      | • To choose when & how much security to apply  
• To have encrypted & clear communications on the same channel                                                 |
|                                                    | ...Easy migration                                                                                              |
| Do we make changes to our ICS software or equipment? | Not to change existing ICS software or equipment                                                              |
|                                                    | ...Easy installation                                                                                           |
| Do we make changes to our operational control?     | Not to change existing operational control                                                                     |
|                                                    | ...Hassle-free                                                                                                 |
| Will it impact performance?                        | Strong security without impacting performance                                                                  |
|                                                    | ...No impact                                                                                                   |
| Will it impact our existing configuration?         | Not to change existing configuration                                                                            |
|                                                    | ...Flexibility                                                                                                 |

Support for:
• Modbus RTU/ASCII, DNP3
• Async 300 to 115200 bps
• Point-to-point and multi-drop
• Radio, dial-up, leased lines
SEQUI presented “IEEE 1711-2010 Security for Legacy SCADA Protocols”
http://www.us-cert.gov/control_systems/icsjwg/presentations/fall2011/D1-09-0200pm_Track2_Amaio-Van_rr_Title-IEEE1711-2010SecforLegSCADAProt.pdf
European Network and Information Security Agency (ENISA) conducted a survey to identify threats, risks, and challenges to ICS and found that untrusted and legacy devices and protocols are the biggest threat to security of ICS.

Conforms to IEEE 1711-2010:
- Encrypts and secures serial data links
- Operates without modification to network/application
Provides a web-based interface for easy management
- Up to 65,533 secure tunnels (IPSec-like)
- Each tunnel has its own Encryption Key & Authentication Key and protects one/more RTU
# HARDWARE DESIGN - CRITERIA

<table>
<thead>
<tr>
<th>Category</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>µProcessor</strong></td>
<td>• Not too fast and not too slow</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>• Hardware co-processor*</td>
</tr>
<tr>
<td><strong>I/O</strong></td>
<td>• Ethernet</td>
</tr>
<tr>
<td></td>
<td>• Three UARTs (RS-232/422/485)</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>• Product longevity (10+ yrs)</td>
</tr>
<tr>
<td><strong>Development Tools / Support</strong></td>
<td>• Mature and proven</td>
</tr>
</tbody>
</table>

*Encryption delay:
- Caused by block protocol encryption overhead, i.e., Header, Trailer, Message Authentication Code + Encryption processing
- The delay impact is greater for small messages
Controlled area
- Parts with very fast rise times, and those that are thermally hot, are noisy, or are high voltage
  - Signal timing considerations, such as differential pairs, critical clock signals, etc
  - Signals that might need to be guard banded

Power/Ground gridding
- High voltage and/or high current traces

Impedance controlled nets and their terminations
- 75 || 100 Ohm

Bypass caps
## HARDWARE DESIGN - CONNECTORS

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Connectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet (LAN)</td>
<td>RJ-45</td>
</tr>
<tr>
<td>Management</td>
<td>RS-232</td>
</tr>
<tr>
<td>Local</td>
<td>RS-232/422/485</td>
</tr>
<tr>
<td>Remote</td>
<td>RS-232/422/485</td>
</tr>
<tr>
<td>Local/Remote</td>
<td>RS-422/485</td>
</tr>
<tr>
<td></td>
<td>Terminal Block 10-pin</td>
</tr>
</tbody>
</table>
FIRMWARE DESIGN - OPERATING SYSTEM

- LynxOS
- VXWorks
- OSE
- Windows CE
- QNX
- FreeRTOS
- RTLinux
- uClinux

uClinux
Pros

- Full Linux 2.6 kernel
- Built-in IP connectivity, file systems, applications...
- Lightweight (under 300KB)
- Faster than Linux (context switches: no cache flushes)
- Royalty free

Limitation

- No memory protection (no MMU)
FIRMWARE DESIGN – CODING & DEBUGGING

- uClinux
  - Initialization/boot loader tailored to processor
  - Kernel config to fit requirements

- Add-ins:
  - RTAI (Real Time Application Interface) - allows applications with strict timing constraints
  - Encryption drivers
  - Speed buffering
  - Modem emulation AT command set

- IEEE 1711 functionality
Table 3: Session state machine for one dynamic session

<table>
<thead>
<tr>
<th>Action / Event</th>
<th>Current State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>closed</td>
</tr>
<tr>
<td>send OPN</td>
<td>wait_ACK, 3</td>
</tr>
<tr>
<td>send DTA</td>
<td>X</td>
</tr>
<tr>
<td>send CLS</td>
<td>X</td>
</tr>
<tr>
<td>rcv OPN</td>
<td>wait_BEG, 5</td>
</tr>
<tr>
<td>rcv ACK</td>
<td>closed, 1</td>
</tr>
<tr>
<td>rcv BEG</td>
<td>closed, 1</td>
</tr>
<tr>
<td>rcv DTA</td>
<td>closed, 7</td>
</tr>
<tr>
<td>rcv CLS</td>
<td>closed, 1</td>
</tr>
<tr>
<td>rcv ERR</td>
<td>closed, 1</td>
</tr>
<tr>
<td>rcv bad</td>
<td>closed, 1</td>
</tr>
<tr>
<td>ACK timeout</td>
<td>X</td>
</tr>
<tr>
<td>BEG timeout</td>
<td>X</td>
</tr>
</tbody>
</table>

Note: X = cannot occur

An IEEE 1711 compliant implementation shall perform the following actions specified in Table 3:

1: do nothing
2: process payload
3: start ACK timer
4: cancel ACK timer, send ACK, start BEG timer
5: send ACK, start BEG timer
6: cancel ACK timer, send BEG
7: send ERR
8: cancel BEG timer, send ACK, start BEG timer
9: cancel BEG timer
10: cancel ACK timer
11: close current session D, send ACK, start BEG timer

// Source code for the session state machine

```c
void session_state (void)
{
    // Execute action = f(event, state)
    switch (ucActionTable[ucEvent][ucState]) {
    case DO NOTHING: // action 1 of Table 3
        break;
    case PROCESS_PAYLOAD: // action 2
        process_payload();
        break;
    case START_ACK_TIMER: // action 3
        start_ACK_timer();
        break;
    case SEND_ACK: // action 4
        cancel_ACK_timer();
        send_ACK();
        start_BEG_timer();
        break;
    // action 5 ... action 11
    default:
        break;
    }

    // Update next state: state = f(event, state)
    ucState = ucStateTable[ucEvent][ucState];
}
```

© SEQUI, Inc.
BOA and thttpd:
- Small, lightweight, and fast
- Popular among embedded crowd, esp. for embedded Linux
SOFTWARE DESIGN – USER INTERFACE

Configuration

- **System** – Configure operating parameters
- **Serial** – Configure port and data communications settings
- **Access** – Add user login accounts
- **Advanced** – Configure SCADA settings, cipher settings, and encryption
Configuration > System

Software Design – User Interface
Configuration > Serial
Policies > Add

EncryptorPak™

Policies
Configuration

Add

Policy Name

SCADA Dest Addr
- Single
- Range 200 - 061 to 200 - 064

Communications
- Encrypted
- Clear

EncryptorPak Dest Addr: 200 - 061

Static CipherSuite: AES128 CBC-mode, HMAC SHA150, with holdback

Dynamic CipherSuite: AES128 CFB-mode, HMAC SHA150, no holdback

ENC Key (min. 6 chars)
Confirm ENC Key

MAC Key (min. 6 chars)
Confirm MAC Key

Session Life (hr): 3
The lifetime during which the secure session is valid

Save Cancel
The trend is to integrate serial SCADA protocols with corporate network for effective management and real-time business decisions. However:

- Serial protocols remain insecure, lack authentication (they’re simply wrapped inside TCP/IP packets!)
- The backdoor risk is still there
- TCP/IP has its own vulnerabilities (that are widely shared within the computer underground!)

Numerous FREE scanning, vulnerability discovery, and attack tools are available, such as nmap, TCPview, Nessus, Attacker Tool Kit (ATK), Sniffit, Netcat, Wireshark.

Visit “Top 100 Network Security Tools” at http://sectools.org/
Examples of vendor-added functionality:

- Management functions, such as audit logs, reports...
- Secure *Serial-over-Ethernet*
- Dial-up access control via *session negotiation*
- Interface to *low-cost wireless*, such as ZigBee® IEEE 802.15.4
- Custom embedded analog/digital remote I/O and data acquisition
ENHANCEMENTS – AUDIT LOGS, REPORTS

The table below describes pages of the Web interface and their access level permissions.

<table>
<thead>
<tr>
<th>NAVIGATION PAGE</th>
<th>DESCRIPTION</th>
<th>ACCESS LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Administrator</td>
</tr>
<tr>
<td>Configuration</td>
<td>Clicking the tab opens the Product Information page</td>
<td>✓</td>
</tr>
<tr>
<td>System</td>
<td>Settings for protocol, source address, IP address, Web timers, and reset button</td>
<td>✓</td>
</tr>
<tr>
<td>Serial</td>
<td>Settings for serial ports</td>
<td>✓</td>
</tr>
<tr>
<td>Access</td>
<td>Setup login accounts</td>
<td>✓</td>
</tr>
<tr>
<td>Advanced</td>
<td>Settings for timeout, rebuffer, broadcast mode, and advanced cipher settings</td>
<td>✓</td>
</tr>
<tr>
<td>Policies</td>
<td>Clicking the tab opens the Policies Table page</td>
<td>✓</td>
</tr>
<tr>
<td>Add</td>
<td>Add a policy</td>
<td>✓</td>
</tr>
<tr>
<td>Copy</td>
<td>Copy a policy</td>
<td>✓</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit a policy</td>
<td>✓</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete policies</td>
<td>✓</td>
</tr>
<tr>
<td>DiagUp</td>
<td>Establish connection to remote device</td>
<td>✓</td>
</tr>
<tr>
<td>DiagDn</td>
<td>Terminate connection to remote device</td>
<td>✓</td>
</tr>
<tr>
<td>Select</td>
<td>Selected policy is in effect when point-to-point link is established</td>
<td>✓</td>
</tr>
<tr>
<td>Audit</td>
<td>Opens the Audit page for a summary of Encryptor/Pak activity</td>
<td>✓</td>
</tr>
<tr>
<td>Info</td>
<td>Opens the Info page for a quick view of Encryptor/Pak configuration settings</td>
<td>✓</td>
</tr>
<tr>
<td>Logout</td>
<td>Returns to the Login page</td>
<td>✓</td>
</tr>
</tbody>
</table>

1 The Administrator level can be assigned to more than one login user.
2 The User level is intended primarily for users with testing responsibilities.
3 Access page only allows changing own password.
4 Available on menu bar only when Point-to-Point protocol is selected.

Table 4. Description of Navigation Pages and Access Level Permissions
ENHANCEMENTS – SECURE SERIAL-OVER-ETHERNET

- Modbus TCP/IP
- Modbus UDP/IP
- Modbus RTU Over TCP/IP
- Modbus RTU Over UDP/IP
- Modbus ASCII Over TCP/IP
- Modbus ASCII Over UDP/IP
- DNP3 over TCP/IP
1. Receives an incoming call (RI toggle) and auto-answers (DCD active)
2. Transmits challenge data
3. Receives response data
4. If “failed” challenge, drop DTR
5. Modem disconnects call (DCD inactive)
ENHANCEMENTS – LOW-COST WIRELESS

ZigBee® Wireless
Thank you

Please feel free to send your comments or questions

Tien Van
Tracy Amaio, Ph.D.
tvan@sequi.com
temaio@sequi.com