What’s the DFIRence for ICS?

EMBEDDED DEVICE FORENSICS

Chris Sistrunk, PE
Senior ICS Security Consultant, Mandiant
@chrissistrunk
Agenda

• Digital Forensics and Incident Response Overview
• DFIR for ICS
  • What’s the DFIRence?
• Embedded Devices
  • What to Collect
  • What to Analyze
• RTU Examples
Incident Response Overview
“Find Evil”

• Assess the situation
• Define objectives
• Collect evidence
• Perform analysis
• Communicate
• Develop remediation plan
• Document findings

http://www.cumbriafire.gov.uk/about/photo.engines/incident-response.asp
Digital Forensics Overview

• Data Collection
  • Data Files
  • OS (volatile and non-volatile)
  • Network Traffic
  • Applications
• Examination
• Analysis
• Reporting
Traditional DFIR tools

Mature
- Tools
  - Redline
  - Volatility
- Websites
- Cheatsheets
WHAT'S THE DFIRENCE FOR ICS?
## DFIR for ICS

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>IT/OT Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess the situation</td>
<td>• When/Where/How is the ICS affected?</td>
<td><img src="image" alt="Similar" /></td>
</tr>
<tr>
<td>Define objectives</td>
<td>• Return the ICS to normal quickly and safely</td>
<td><img src="image" alt="Physical Processes" /></td>
</tr>
<tr>
<td>Collect evidence</td>
<td>• ICS devices have RTOS and ICS protocols</td>
<td><img src="image" alt="Must be collected manually" /></td>
</tr>
<tr>
<td>Perform analysis</td>
<td>• Analysis must be done to verify anomalies</td>
<td><img src="image" alt="No ICS-specific DFIR tools" /></td>
</tr>
<tr>
<td>Communicate</td>
<td>• Regularly report status to management</td>
<td><img src="image" alt="Similar" /></td>
</tr>
<tr>
<td>Develop remediation plan</td>
<td>• How/When to regain control of the ICS</td>
<td><img src="image" alt="ICS devices have constraints" /></td>
</tr>
<tr>
<td>Document findings</td>
<td>• Write a report of what exactly happened</td>
<td><img src="image" alt="Similar" /></td>
</tr>
</tbody>
</table>
ICS anomaly → incident?

- An anomaly of some kind has occurred
  - Increased network activity, strange behavior, failure
- Now we need to **investigate** the anomaly
- Is it known bad?
- Is it unknown bad?
- Do we **escalate** this to a security incident?
- Who do we call?
  - Engineers, Admins, PR, Safety
  - Vendors
Don’t!

-HAVE YOU TRIED
TURNING IT OFF AND ON AGAIN?
ICS forensics collection tools

• No ICS-specific DFIR tools...especially embedded devices
• But, we can collect data manually using other tools
Embedded devices: What to collect?

**Physical data**
- Exact location of device
- Device description
- Identifying info (manufacturer, S/N, P/N, name)
- Connections (serial, ethernet, USB)
- Front/back panel LED status
- Power consumption
- Temperature (if running hot)
- Evidence of tampering

**Digital data**
- Running configuration (including user accounts)
- Last-known good configuration
- Running firmware, approved firmware
- CPU usage %, Memory usage % (RAM, Storage)
- Running processes
- Active ports (serial, ethernet, USB, etc)
- Logs (security, events)
- Memory dump (if possible)
Embedded devices: What to analyze?
Find Evil…or ways for evil to do evil

First Responders: ICS Engineer or Technician, Network Engineer, Vendor

• What do the user and event logs reveal? (these need to be viewed first as they may rollover)
• Does the configuration match the firmware? Is the firmware approved from FAT/SAT?
• Running config / last known good config / standard config
• Is the configuration and logic correct for the process?
• Are communications (serial, ethernet, USB, wireless) normal as compared with known good?

Vendor, Digital Forensics Specialist, Embedded Systems Analyst

• Analyze embedded OS files, captured data at rest, captured data in transit
• Volatile memory if possible (to look for code injection and potential rootkits)
Let’s do DFIR on two substation RTUs
Time to...RTFM
Data Collection: D20MX

Specs
- 667 MHz embedded PowerQUICC II Pro
- 1024 MB of 266 MHz DDR2 RAM with ECC
- 16 MB NVRAM for persistent event storage
- 8 MB boot flash, 256 MB firmware flash
- VxWorks RTOS

Tools to use
- D20MX Product Documentation Binder.pdf
- GE SGconfig software
- Terminal (Tera Term, PuTTY)
- WinSCP
Data Collection: D20MX

You will need three manuals from the binder pdf:

1. **994-0140** D20MX Substation Controller Instruction Manual
   - Chapter 11: Troubleshooting
2. **B014-1NUG** Westmaint II+ for D20MX User’s Guide
   - Shows how to use the D20 console interface, menus, error and user logs
3. **SWM0080** D20MX Shells User’s Guide

<table>
<thead>
<tr>
<th>Shell</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>D20M</td>
<td>D20M&gt;</td>
</tr>
<tr>
<td>C</td>
<td>-&gt;</td>
</tr>
<tr>
<td>CMD</td>
<td>[vxWorks]#</td>
</tr>
</tbody>
</table>
Data Collection: D20MX

Error Log and User Log

The **error log** tells what’s wrong with the configuration.

The **user log** shows logins, logouts, and all user activity. Can be exported to CSV. This data also gets put into the **syslog**.
The power of the 3 Shells

• You can access the shell remotely with SSH, but the most powerful access is through the front serial port.

• Some of these commands require assistance from GE unless you really know what you are doing.

6.3 D20MX Shells

The D20MX Shells (formally called the “68K Monitor”) are three troubleshooting and diagnostics tools that give you low-level access to your equipment, as mentioned in GE System Maintenance and Configuration Tools.

The three “shells” available on the D20MX are the “D20M” shell, the “C” shell and the “CMD” shell. The first shell, “D20M” shell, is accessed via the WESMAINT menus. Once inside the D20M shell the second shell, “C” shell, may be accessed. From there the third shell, “CMD” shell, may be accessed.
The main shell

- D20M Shell is the main shell
- Very similar to 68k monitor shell in older D20s
- Incident Responders will want to collect data from this shell
- All of the commands are explained in detail in the D20MX Shells UG
Data Collection: D20MX

- Running configuration
  - Use SGConfig, ConfigPro, or TeraTerm
  - Very common task
- Last-known good configuration
  - Look in email, config database, engineer’s laptop, or it may be on a USB in the cabinet
- Running firmware - **img**

### CPU usage %, Memory usage %
- **pr** – performance monitor
- **qr** – query ram (volatile and nvram)

#### D20M>qr /0

<table>
<thead>
<tr>
<th>status</th>
<th>bytes</th>
<th>blocks</th>
<th>avg block</th>
<th>max block</th>
</tr>
</thead>
<tbody>
<tr>
<td>current</td>
<td>979342168</td>
<td>23</td>
<td>42580094</td>
<td>97917656</td>
</tr>
<tr>
<td>free alloc</td>
<td>97902616</td>
<td>11</td>
<td>7491</td>
<td>–</td>
</tr>
<tr>
<td>internal</td>
<td>648</td>
<td>3</td>
<td>213</td>
<td>–</td>
</tr>
<tr>
<td>cumulative alloc</td>
<td>89738516</td>
<td>16476</td>
<td>5946</td>
<td>–</td>
</tr>
<tr>
<td>peak alloc</td>
<td>87717016</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

#### D20M>qp

<table>
<thead>
<tr>
<th>NAME</th>
<th>PRIO</th>
<th>STMSZ</th>
<th>Uxworks</th>
<th>Process List</th>
<th>TID</th>
<th>PARENT TID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROOT</td>
<td>240</td>
<td>10000000</td>
<td>04e56ca0</td>
<td>00000000</td>
<td>00b8dca0</td>
<td>04be47a0</td>
</tr>
<tr>
<td>V2KL</td>
<td>55</td>
<td>12601100</td>
<td>00556319</td>
<td>00000000</td>
<td>01e8010</td>
<td>00b8dca0</td>
</tr>
<tr>
<td>V2NL</td>
<td>240</td>
<td>1260028a</td>
<td>00555058</td>
<td>00000000</td>
<td>01e62d23</td>
<td>00b8dca0</td>
</tr>
<tr>
<td>V2NL</td>
<td>51</td>
<td>12600300</td>
<td>01e66a8a</td>
<td>00000000</td>
<td>01e57220</td>
<td>00b8dca0</td>
</tr>
<tr>
<td>BD19</td>
<td>250</td>
<td>10000000</td>
<td>01e65778</td>
<td>00000000</td>
<td>01e6bf60</td>
<td>00b8dca0</td>
</tr>
</tbody>
</table>
Data Collection: D20MX

Serial analyzer

- Very popular shell command (what’s Wireshark?)
- In the D20M shell, use
  - `sa com#`
    where # is the port number
  - Turn on logging in TeraTerm beforehand to save the traffic
  - This example is DNP3
Data Collection: D20MX

- Dump memory
  - **si** – shows system information including the memory base addresses
  - **d** – dumps memory, but you have to tell it where to start and stop
  - Serial for snippets, SSH for full image
- Hand the output to someone who understands VxWorks for analysis
- Look for strings, injected code, or rootkits
Data Collection: D20MX

C Shell
- Low-level shell only accessible from RS-232 port
- Mainly used by GE customer support for troubleshooting

CMD Shell (VxWorks)
- OS level shell, mainly used by GE
- VxWorks Kernel Shell Command Reference 6.9
- We can use some commands for forensics
  - netstat, ipf (firewall), syslog, show devices, show drivers, show history, ifconfig, route, and even pcap!

Example:
```
pcap -f /ram/temp.cap qefcc0 start
Wait a few minutes...
pcap qefcc0 stop
```
Now use a program such as WinSCP to transfer the file from the D20MX to a PC. Then use Wireshark on the PC to view the file.
Data Collection: SEL-3530 RTAC

Specs

- 533 MHz Power PC
- 1024 MB DDR2 ECC RAM
- 2GB Storage
- Embedded SEL Linux

Tools to use

- SEL-3530 RTAC Instruction Manual
- SEL-5033 Instruction Manual
- SEL-5033 software
- Web Browser (Chrome, FireFox, etc)
- Terminal for SSH (Tera Term, PuTTY)
Data Collection: SEL-3530

Digital data
- Running configuration
- User Accounts
- Running firmware
- CPU usage %
- Memory usage %
- POST checks
- Reports (several)

Physical Data
- Password jumper
These are the screenshots from when I sent a malformed DNP3 message that caused the RTAC to lose the configuration.

Data Collection: SEL-3530

- Section 3: Testing and Troubleshooting
- Section 5: Web HMI and Logging
- Section 6: Security
- There are tags in the RTAC database that are assigned to help troubleshoot but are also useful for forensics as well.

- Several log types
  - SOE report
  - IED report
  - syslog
Data Collection: SEL-3530

- Example of IED Report
- Can be accessed via web or ODBC (MS Access)
- No Linux Shell
- Pros & cons
  - No SSH Interface with RTAC
  - SSH used for engineering remote access to relays
Data Collection: SEL-3530

- The RTAC can capture ethernet and serial traffic
  - SEL-5033 software and the Comm Monitor
- AG2012-15 *Using Wireshark® to Troubleshoot Protocol Communications Issues on an RTAC*
  - DNP3 example
- AG2015-15 *Using Wireshark® to Decode RTAC Serial Line Messages and SEL Protocols*
  - SEL Fast Messaging example
- SEL published several serial Wireshark dissectors
  - SELFM, Telegyr 8979
QUESTIONS?

Find Evil