How I Pwned The ICS Data During My Internship
Who Am I

❖ Shail Patel (bind_tcp)

❖ Security Research Engineer @NREL

❖ Focusing on ICS/SCADA/OT/IoT security & network protocols, Energy Security & Resiliency

@shail_official
Motivation

❖ Prior work: Develop, validate and deploy a unique innovative Data-Enhanced Hierarchical Control (DEHC architecture)
❖ Cybersecurity testing scoped as an analysis of communications between devices as well as analysis of device level security
❖ Perspective: System, network and application perspective
❖ Capture communications between elements
❖ Access the cybersecurity functions of each vendor device
❖ Determine the kind of security controls for Beagleboard local controller
❖ Source code review
❖ Hunting in the wild for fun and profit
Industrial Control Systems Cybersecurity

❖ What is Industrial Control Systems?
ICS are used in machinery throughout a wide range of industries all over the world.

❖ Comprises of various control systems used in industrial process control for manufacturing and production that includes Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Human Machine Interface (HMI), Distributed Control Systems (DCS), etc.
Industrial Control Systems Cybersecurity

How is OT different than IT?

❖ IT system == Datacentric
❖ No priority for the confidentiality of the data in Operational Technology
❖ OT is concerned with physical processes
❖ “Unusual” Operating Systems and Applications
❖ “Unusual” Security Architectures and risk management goals
❖ “Different” performance and reliability requirements
Why do we care?

- Challenges for a secure and resilient infrastructure often being overlooked
- ICS often support critical infrastructure
- Very limited computing resources
- Who should be responsible?
- Do I know what I have installed in the field?
- What about control system policies?
- Human error is almost indispensable
Getting started

❖ Testbed: Hardware in the Loop (HIL) capability with Beagleboard local controller, and PV Inverter.

❖ Goal: Capture Modbus traffic between the two communication models.
Things to Know

❖ Beagleboard to control the PV inverter.

First things first...

❖ Modbus Basics?
  Serial communications protocol originally published by Modicon

❖ Modbus Applications: Used to establish master/slave communication between intelligent devices.
  Openly published and royalty-free.
  Enables communication between several devices connected to the same n/w.
Things to Know

More about Modbus...

- Communication between Modbus devices:
  - Only master can initiate queries
  - Slaves respond by providing the requested data to the master.
Set of actions performed here are reading or writing to a set of four data, used by the Modbus application layer.

<table>
<thead>
<tr>
<th>Primary Tables</th>
<th>Object Type</th>
<th>Type of</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrete Input</td>
<td>Single bit</td>
<td>Read-Only</td>
</tr>
<tr>
<td>Coils</td>
<td>Single bit</td>
<td>Read-Write</td>
</tr>
<tr>
<td>Input Registers</td>
<td>16-bit word</td>
<td>Read-Only</td>
</tr>
<tr>
<td>Holding Registers</td>
<td>16-bit word</td>
<td>Read-Write</td>
</tr>
</tbody>
</table>
About the controller

Beagleboard Basics:

BeagleBone Black

What is BeagleBone Black?
BeagleBone Black is a low-cost, community-supported development platform for developers and hobbyists. Boot Linux in under 10 seconds and get started on development in less than 5 minutes with just a single USB cable.

Processor: AM335x 1GHz ARM® Cortex-A8
- 512MB DDR3 RAM
- 4GB 8-bit eMMC on-board flash storage
- 3D graphics accelerator
- NEON floating-point accelerator
- 2x PRU 32-bit microcontrollers

Connectivity
- USB client for power & communications
- USB host
- Ethernet
- HDMI
- 2x 46 pin headers

Other BeagleBone derivatives »

Software Compatibility
- Debian
- Android
- Ubuntu
- Cloud9 IDE on Node.js w/ BoneScript library
- plus much more

Purchase
Select distributor to buy
A testbed coordinator setup to synchronize the two simulation platforms (OpenDSS), OPAL-RT in real-time.

System/hardware under test divided into two paths; one of the paths include ADMS, DER aggregator, Beagleboard local controller and a PV inverter.

Programmed Beagleboard to control the PV inverter.

Inverter converts direct current (DC) of the PV modules into grid-compliant alternating current (AC), feeds this into the public grid. Continuously monitors the power grid.

Power optimization, monitoring and securing, communication, temperature measurement, protection.
Packet Capture Modbus

- Wireshark and Dualcomm ETAP-2306 for sniffing Modbus traffic between Beagleboard and PV inverter.

- Plug-and-Play without disrupting the network.
Packet Capture Modbus

- Input values for coil disclosed in plaintext...

Setpoints exposed!!!
Packet Capture Modbus

❖ Now that PV setpoints captured in register values.
❖ Want to alter the set points? Use only the IP address for asset discovery.

[https://store.chipkin.com/products/tools/cas-modbus-scanner](https://store.chipkin.com/products/tools/cas-modbus-scanner) (FREE!!)

Can read: coil status (0xxxx), input status (2xxxx), inpute registers (3xxxx), holding registers (4xxxx).

Connect the IP address of the target.
In case of Serial Modbus, select the option and enter the comm port.
Note down register addresses while still allowing it to discover...

Start polling

I suggest allow at least 10 mins to discover all the devices.
Packet Capture Modbus


Same process: Connect to the Target IP

To save time, use register Value addresses from CAS Scanner
Packet Capture Analysis

❖ Capture the traffic between RT-OPF and RTAC.

❖ Real-Time Optimal Power Flow (RT-OPF) is a python script to schedule the decision variables of the power system in an optimal way to satisfy power flow balance equations, nodal voltage and apparent power in the feeders.

❖ Real-Time Automation Controller (RTAC) originally used in utility-scale solar and other grid applications. Now also can act as PV plant controller for connection to other substation devices, and for sending command and control to the devices out in the field.
Packet Capture Analysis

- Two Serial Streams of data disclosed in the string format...

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.000033</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>66</td>
<td>30039 Len=24</td>
</tr>
<tr>
<td>7.000035</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>98</td>
<td>30039 Len=56</td>
</tr>
<tr>
<td>8.000071</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>66</td>
<td>30039 Len=24</td>
</tr>
<tr>
<td>8.000071</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>98</td>
<td>30039 Len=56</td>
</tr>
<tr>
<td>9.000318</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>66</td>
<td>30039 Len=24</td>
</tr>
<tr>
<td>9.000321</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>98</td>
<td>30039 Len=56</td>
</tr>
<tr>
<td>10.000233</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>66</td>
<td>30039 Len=24</td>
</tr>
<tr>
<td>10.000234</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>98</td>
<td>30039 Len=56</td>
</tr>
<tr>
<td>11.000144</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>66</td>
<td>30039 Len=24</td>
</tr>
<tr>
<td>11.000146</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>98</td>
<td>30039 Len=56</td>
</tr>
<tr>
<td>12.000157</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>66</td>
<td>30039 Len=24</td>
</tr>
<tr>
<td>12.000158</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>98</td>
<td>30039 Len=56</td>
</tr>
<tr>
<td>13.000411</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>66</td>
<td>30039 Len=24</td>
</tr>
<tr>
<td>13.000412</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>98</td>
<td>30039 Len=56</td>
</tr>
<tr>
<td>14.000314</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>66</td>
<td>30039 Len=24</td>
</tr>
<tr>
<td>14.000316</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>98</td>
<td>30039 Len=56</td>
</tr>
<tr>
<td>15.000381</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>66</td>
<td>30039 Len=24</td>
</tr>
<tr>
<td>15.000384</td>
<td>10.79.91.42</td>
<td>10.79.91.81</td>
<td>UDP</td>
<td>98</td>
<td>30039 Len=56</td>
</tr>
</tbody>
</table>

Frame 1168: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Schwitz_15:33:85 (00:30:a7:15:33:85), Dst: c8:ff:50:36:6c:0f (c8:ff:50:36:6c:0f)
Internet Protocol Version 4, Src: 10.79.91.42, Dst: 10.79.91.81
User Datagram Protocol, Src Port: 30039, Dst Port: 30039
Data (24 bytes)
Data: 0c056146666863f3333733f00000000000000000000000000000000

Time to play some CTF now!! 😊
Packet Capture Analysis

- DualComm ETAP-2306 plugged in to capture the PCAP.

- Two fields of data recorded here: a. Binary plaintext stream, b. Hex encoded string

- Binary values for no good.
Packet Capture Analysis

- Decoded the Hex string to Little-Endian floating format

- Discloses analog communication between the RTAC and RT-OPF.

Reported to the Power Systems team
Packet Capture Analysis

- Capture the traffic between ADMS and RTAC

- ADMS for optimizing the performance of the distribution grid, outage restoration, support for microgrids...

- DNP3 capture include SCADA measurements, control setpoints and feedback
Packet Capture Analysis

Filter search for DNP3 and start inspection.

Cap. Bank values disclosed when ADMS and RTAC communicates
Packet Capture Analysis

Telemetered RTAC values that are sent to ADMS in plaintext (V or kVAR).

Data stored in the form of analog objects.
Beaglebone Security Analysis

❖ A mix of NMAP, SPARTA, OpenVAS to find open ports, services, banners and known CVEs...

Vulnerable Javascript Cloud9 IDE

Hit default web interface

root@beaglebone:/# nmap -A 192.168.7.2

Starting Nmap 7.40 (https://nmap.org) at 2019-09-11 15:45 UTC
Nmap scan report for 192.168.7.2
Host is up (0.00999s latency).
Not shown: 995 closed ports

PORT STATE VERSION
22/tcp open ssh

OPENSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)

ssh-hostkeys:

Key fingerprint:

root@beaglebone:/# nmap -A 192.168.7.2

Starting Nmap 7.40 (https://nmap.org) at 2019-09-11 15:45 UTC
Nmap scan report for 192.168.7.2
Host is up (0.00999s latency).
Not shown: 995 closed ports

PORT STATE VERSION
22/tcp open ssh

OPENSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)

ssh-hostkeys:

Key fingerprint:

Hit default web interface

Vulnerable Javascript Cloud9 IDE
Beaglebone Security Analysis

- **Modular Architecture**: The Beaglebone is designed with a modular architecture that allows for easy customization and expansion.

- **Security Analysis**: The image shows a screenshot of a security analysis tool, likely used to scan for vulnerabilities. The analysis includes information on services, scripts, and notes, indicating the presence of open directories and potential vulnerabilities such as directory listing attacks.

- **Vulnerability Details**: The tool highlights specific vulnerabilities, including:
  - **Microsoft IIS Security Advisory**: A vulnerability in the IIS server, with a severity rating and affected host details.
  - **OSVDB-3268**: A vulnerability related to directory indexing, with a severity rating and a note about the potential for attacks.
  - **OSVDB-3276**: Another vulnerability found in the Beaglebone's configuration.

- **Actions**: The analysis tool also provides actions to mitigate or address these vulnerabilities, emphasizing the importance of regular security checks and updates.

- **Dependency on Software**: The Beaglebone relies on various software components, each with its own security implications. Regular updates and patches are essential to maintain a secure environment.

- **Network Security**: Understanding the network topology and implementing robust access controls is crucial for securing the Beaglebone platform.

Overall, the Beaglebone Security Analysis highlights the need for continuous monitoring and updating to ensure the device remains secure against evolving threats.
Beaglebone Security Analysis

Critical: Look for Shellshock and Apache exploits!!!

Beaglebone affected due to default config settings
RT-OPF Static Code Analysis

- Env: Python
- Tools used for checking source code redundancies: Bandit, Dlint, Pylint, Prospector
Vendor Device Security Analysis

- Grid Edge Management System

Using TLS 1.1, vulnerable to OpenSSL, Heartbleed, and POODLE attacks

https://github.com/mpgn/heartbleed-PoC
Vendor Device Security Analysis

- Advanced Distributed Management System
  - DNP3 transit in plaintext while setup
  - Poor asset management
  - False Data Injection likelihood
Vendor Device Security Analysis

Got in through Default credentials ;)

Juicy information In datasheets!!
More misconfigurations and Vulnerabilities

❖ Logic-bomb as a backdoor for the HMI to obtain a simple reverse shell, Django default and many more...

Pwn Blue Teams
In the wilderness for fun and profit

- Shodan is a search engine that lets you find specific types of devices (routers, servers, etc.) on the internet using a variety of queries and filters. Some have also described it as a search engine of service banners, which are meta-data the server sends back to the client.

- In May 2013, CNN Money released an article detailing how SHODAN can be used to find dangerous systems on the Internet, including traffic light controls and other control systems, including ICS.

- In December 2013, the website SCADA Strangelove posted over 500 banner search terms to find connected SCADA devices via SHODAN and/or Google.
In the wilderness for fun and profit

❖ How does Shodan work?
❖ Crawl all IP addresses in the IPv4 space
❖ Try to initiate connections with known ports
❖ Record the responses/banners that are received
❖ Append to any records that exist for that IP
❖ You can also create reports or find security exploits for specific ports/services
In the wilderness for fun and profit

- Why is this interesting?
- Some banners can give information to the state of the device
- What type of device (make/model)
- Default user/admin passwords
- Misconfigured systems
- No authentication!
- Combined with domain knowledge (or Google) we can find useful things!
Electric Meters are on the internet

Power Meters and Cloud Energy Management
Networks in the wild

Routers openly exposed

WHY WOULD YOU USE

THE SAME PASSWORD FOR ALL YOUR LOGINS!!?
Printers love the Internet!!

Unauthorized Access.
No login required
Check cartridge, battery status, connection,...
Control Units like the Internet too!!

No authentication required
Unauthorized file upload

Uses IEC 60870-5
Complete takeover & control
### DASHBOARD

- **GNSS position**: 34.54° N, 129.53° E
- **Vessel heading**: 250.3°
- **Satellite profile**: Dual Antenna System
- **Satellite position**: 1.0° W
- **RX polarisation**: Vertical
- **TX polarisation**: X-pol
- **RX RF frequency**: 11.880920 GHz
- **LNB LO frequency**: 10.250000 GHz
- **TX RF frequency**: 14.200000 GHz
- **BUC LO frequency**: 12.800000 GHz
- **Tracking RF frequency**: 11.880920 GHz

### MODERN

- **Model**: Dual Antenna Master
- **RX locked status**: Locked
- **Signal level**: 0 (pwr)

###_slave:

- **ACU part name**: TT-7010A
- **Antenna part name**: TT-7008A
- **ACU serial number**: 81141110
- **Antenna serial number**: 81144014
- **Software version**: 1.62 build 31

### POINTING

- **Azimuth, elevation geo**: 155.3°, 40.8°
- **Azimuth, elevation rel**: 225.2°, 43.9°
- **Polarisation skew**: 8.4°

### SHODAN

Search term: "Cobham Satcom OR ("Sailor" OR "VSAT")"
Welcome to the Main Menu of the Solar-Log 1200

Yield data / Current values / Energy flow

32.40 kW Production

Configuration / Devices / Definition / Interfaces

Interface assignments

Device class | Manufacturer | Type | Interface
-------------|--------------|------|---------
Inverters    | Solenia      | V4   | (9600bps)
Various Electrical Supplies
Webcams, Wind Portals,...
What does it all mean?

- Lazy access to “devices” for operational/monitoring purposes
- Most are not secure for anything other than local access
- Accessed these sites through HTTP using a basic web browser
- These systems were not initially built to face externally, also not an accident!
- Security through obscurity ≠ device access.
- No firewall rules in place to protect from external access
- Default credentials work half the time
- So these devices should not be on the Internet, right?
Lessons Learned

❖ Use Modbus over TLS
❖ Datagram Transport Layer Security (DTLS) to secure UDP streams
❖ Implementing DNP3 Secure Authentication (DNP3-SA) over serial links/IP suites, use of Smart Energy Profile (SEP2) protocol, ICCP, and IEC 62351 security standard for best practices
❖ Firewall unnecessary ports, disable Cloud9 IDE while in production, run system-level updates, update bash for shellshock mitigation
❖ Updating OpenSSL, TLS and changing hardcoded/default credentials for vendor device security
Departing Thoughts

❖ Moving beyond perimeter-based security
❖ Need for people to sustain ICS security
❖ First know what's installed out there in the field
❖ Obtain the model of trust for device outputs and the correct documentation for systems
❖ More IR capabilities to remediate grid-based attacks
Thanks for tuning in!

@shail_official

https://github.com/spwn3r49sd3r00