AGENDA

Why Cybersecurity?
6-phase overview
Defining our SUT
Characterizing the Attack Surface
  - Criticality
  - Susceptibility
  - Characterization

Summary
WHY CYBERSECURITY?

"Multiple American Airlines flights were thrown into chaos tonight as an app issue with the onboard iPads used by pilots made it impossible to take off."

"During the attack, hackers remotely switched breakers in a way that cut power after installing malware."

---

Stranger hacks family’s baby monitor and talks to child at night - VIDEO

Fri 08 January 2016 08:09 GMT | 12:09 Local Time

A family living in Washington is speaking out about the horrors they experienced while operating a baby monitor inside their 3-year-old son’s bedroom.

The couple Jay and Sarah were alarmed to discover that a stranger had hacked into their baby monitor and was spying on their toddler, sometimes speaking disturbing messages into the device, as CBS News describes, The San Franciskso Globe reports.
6-PHASE CYBERSECURITY T&E PROCESS
OUR SUT
OneWire Data Bus
Temperature Sensors
Solid State Relays
Embedded Arduino Controller
USB Port
PHASE II — CHARACTERIZE THE ATTACK SURFACE

Goal: Identify opportunities an attacker may use to exploit the system

Characterization will prioritize attacks based on
- Criticality
- Vulnerability

Characterization will lay foundation for effective Cooperative Vulnerability Identification/Cybersecurity Test
AGENDA

Why Cybersecurity?
6-phase overview
Defining our SUT
Characterizing the Attack Surface
- Criticality
- Susceptibility
- Characterization

Summary
PHASE II, PART 1: CRITICALITY

Identify the “important” functions of the SUT

- ID mission of SUT — both as a component, system, and mission thread
- List mission essential functions
EXEMPLAR - CRITICALITY

Identify Mission

- Define functionality from component level through mission thread

Mission               System           Component

Drink Delicious Beer

Ferment Beer

Dispense Beer

Control Temperature  Cool Environment  Heat Environment  Provide Situational Awareness  Store Pressurized Liquid  Cool Pressurized Liquid  Release Liquid from Storage
EXEMPLAR - CRITICALITY

List Mission Essential Functions

- Accept Temperature Values
- Read Temperature Profile
- Send Temperature Control Signals
- Update Web GUI with Current Data

Control Temperature
AGENDA

Why Cybersecurity?
6-phase overview
Defining our SUT
Characterizing the Attack Surface
- Criticality
- Susceptibility
- Characterization

Summary
How could the adversary access the system?

- Map cyber dependencies
- Draw information boundary of SUT
- Enumerate info exchange requirements
- Characterize information flows
Map cyber dependencies

- **Accept Temperature Values**: Read One-Wire data bus for temperature from sensors
- **Read Temperature Profiles**: Access to profile data on filesystem; Synchronize time with upstream NTP server
- **Send Temperature Control Signals**: Access to reference power for SSRs
- **Provide Situational Awareness**: Read the temp profile stored values; Read current temperature value of wort; Read current temperature of fermenter
EXEMPLAR — IDENTIFYING SUSCEPTIBILITIES

Draw SUT

Information

Boundary

Heating SSR

Cooling SSR
EXEMPLAR — IDENTIFYING SUSCEPTIBILITIES

Enumerate information exchange requirements
- Draw the lines

Characterize information flows
- User/Internet => Pi
  - Temperature profile, beer name, start/stop control (JSON over HTTP)
  - Time data (NTP over UDP)
- Pi => Arduino
  - Start/stop control, temperature set points, sensor assignments (JSON over USB)
- Arduino => Temp Controllers
  - On/Off (Reference Power)
- Temp Sensor => Arduino
  - Temperature (OneWire databus)
- Arduino => Pi
  - Available sensors, current temperatures (JSON over USB)
- Pi => User
  - Current temperature of wort, current temperature of enclosure, temperature profile to follow (JSON over HTTP)
AGENDA

Why Cybersecurity?
6-phase overview
Defining our SUT
Characterizing the Attack Surface
- Criticality
- Susceptibility
- Characterization

Summary
PHASE II: FINALLY- HOW TO CHARACTERIZE THE ATTACK SURFACE

Identify component impacts
Establish D5 effects to the system and mission
Categorize susceptibilities (architectural, system, or implementation)

... All these Phase II checkpoints feed into Methods of Test for Phase III
EXEMPLAR — CHARACTERIZE ATTACK SURFACE

Identify impact at the component level

- Send “on” signal to cooling element
- Send “on” signal to heating element
- Send inaccurate temperature data to temp controller
- Manipulate text strings sent to UI
- Manipulate time signals
## EXEMPLAR — CHARACTERIZE ATTACK SURFACE

<table>
<thead>
<tr>
<th>Component Impact</th>
<th>Component Effect</th>
<th>System Effect</th>
<th>Mission Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send “on” signal to cooling element</td>
<td>Temperature chamber too cold</td>
<td>Degrade fermentation process</td>
<td>Beer tastes sweet and watery—Effect degraded my delicious beer</td>
</tr>
<tr>
<td>Send “on” signal to heating element</td>
<td>Temperature chamber too warm</td>
<td>Degrade fermentation process</td>
<td>Beer tastes like commercial solvent — Effect destroyed my delicious beer</td>
</tr>
<tr>
<td>Send inaccurate temperature value to temp controller</td>
<td>Temperature controller improperly adjusts control signals based on inaccurate info</td>
<td>Degrade fermentation process</td>
<td>Beer tastes {bad/worse} — Effect degraded my delicious beer</td>
</tr>
<tr>
<td>Alter time signal</td>
<td>Temperature controller improperly adjusts control signals based on inaccurate info</td>
<td>Degrade fermentation process</td>
<td>Beer tastes {bad/worse} — Effect degraded my delicious beer</td>
</tr>
<tr>
<td>Manipulate text strings sent to UI</td>
<td>Web UI does not display accurate information</td>
<td>Degrade situational awareness of fermentation process</td>
<td>No mission impact</td>
</tr>
</tbody>
</table>
EXEMPLAR — CHARACTERIZE ATTACK SURFACE

Categorize susceptibilities (architectural, system, or implementation)

- Is it a flaw in the codebase itself? (Architectural)
  - The embedded controller copies data provided by the temperature sensors to a buffer without bounds checking data length

- Is it an issue with how components communicate with each other? (System)
  - The UI cannot parse Unicode or whitespace characters in configurations

- Is the assembly or use of components ineffective? (Implementation)
  - Web UI does not have a login, but is connected to the Internet
NEXT STEPS

Feed into Cooperative Vulnerability Identification

Develop Methods of Test

Drink Results of SUT