# BEYOND THE GUIDEBOOK

How to characterize the attack surface of a non-IT platform



Major George M. Van Osterom
Phone: (DSN) 945-6730
george.vanosterom@us.af.mil

# AGENDA

Why Cybersecurity?

6-phase overview

Defining our SUT

Characterizing the Attack Surface

- Criticality
- Susceptibility
- Characterization

Summary

# WHY

THE VERGE

iPad app issue gr
American Airline

EDITION: UNITED STATES

REUTERS

Politics | Economy | Society | Sports | Culture | Interviews | Karat

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

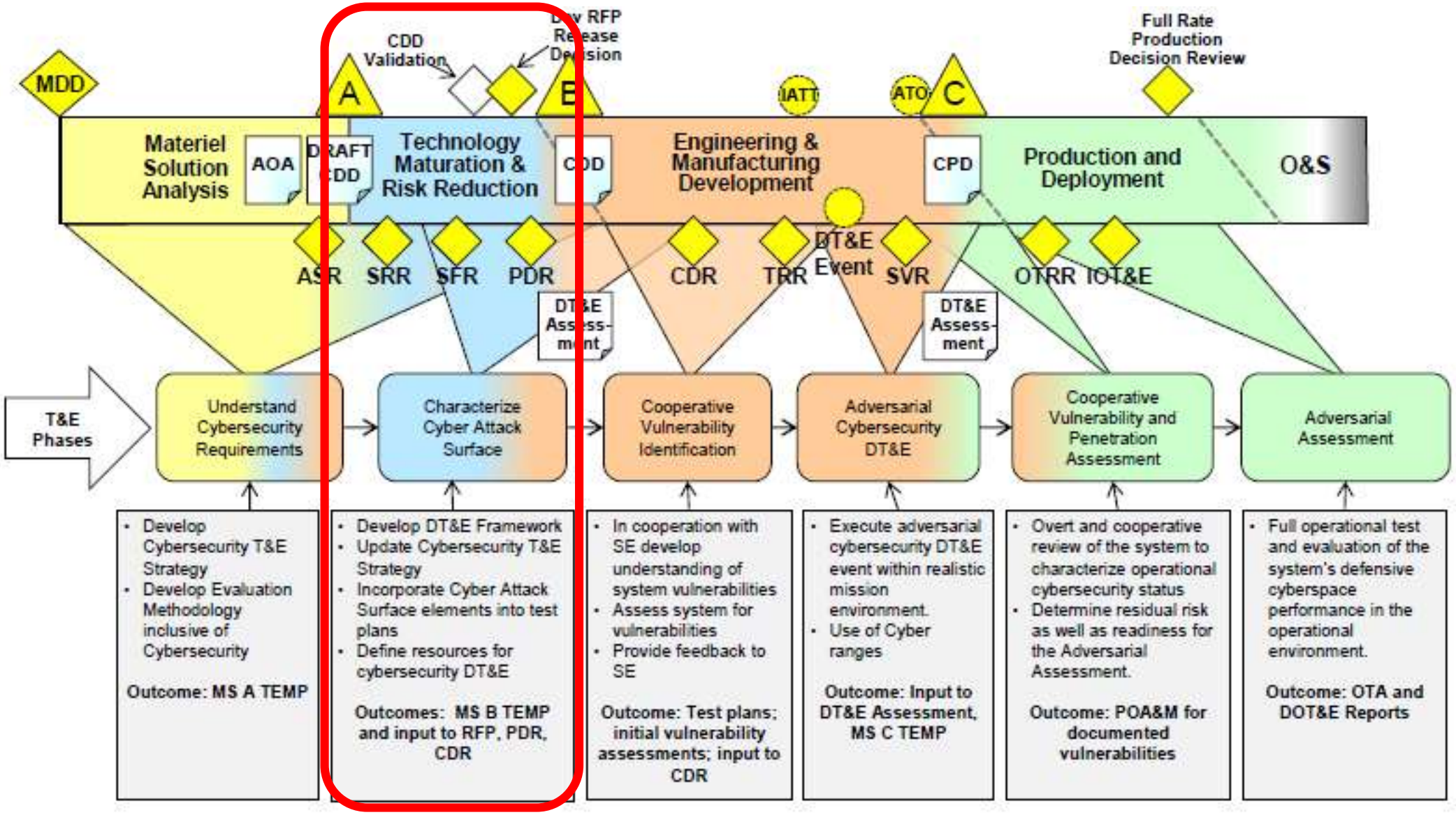
Fri 08 January 2016 08:09 GMT | 12:09 Local Time

Text size:

***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.***

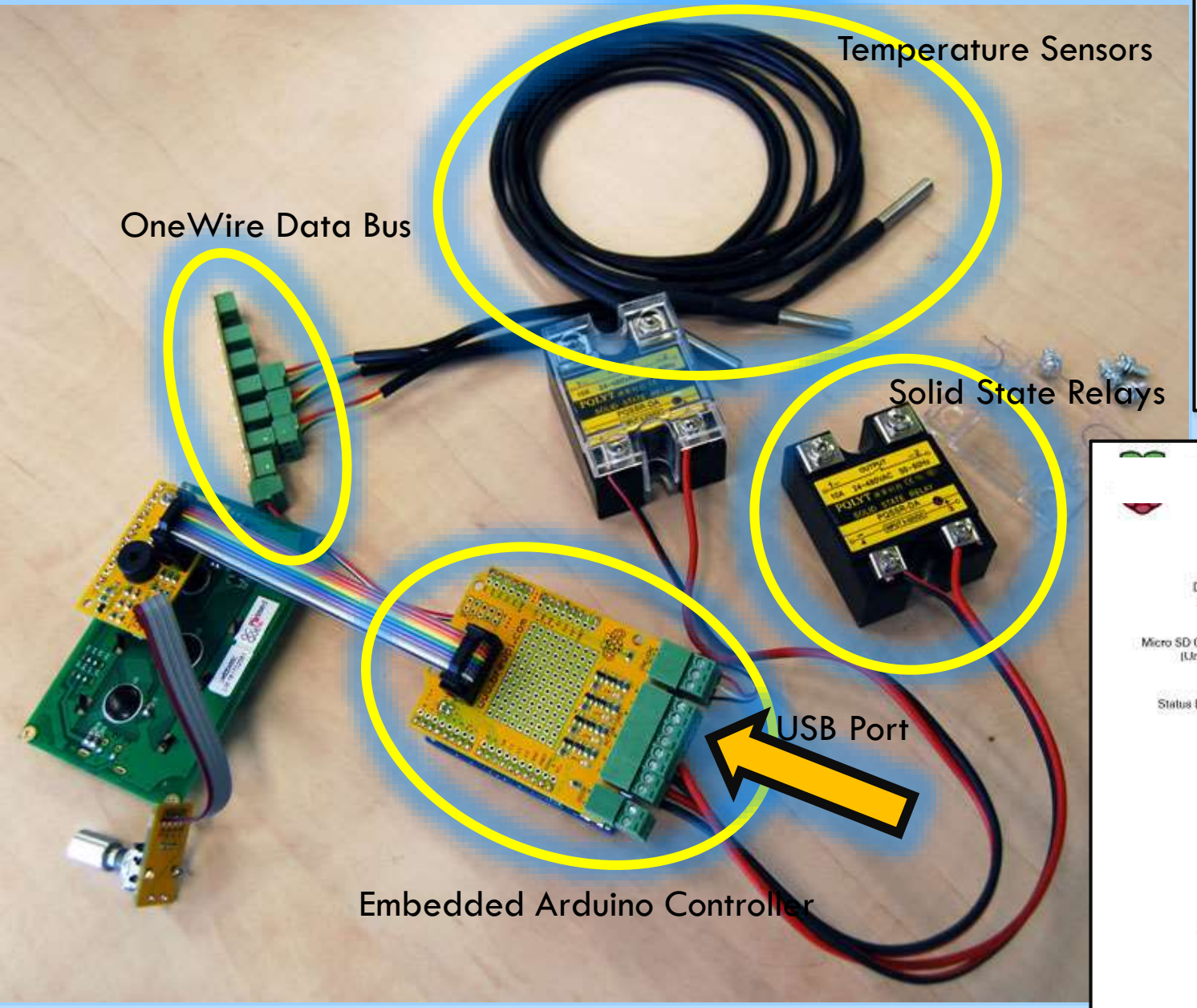
The couple Jay and Sarah were alarmed to discover that a stranger had hacked into their baby monitor and was spying on their toddler, sometimes speaking disturbing messages into the device, as CBS News describes, The San Francisko Globe reports.

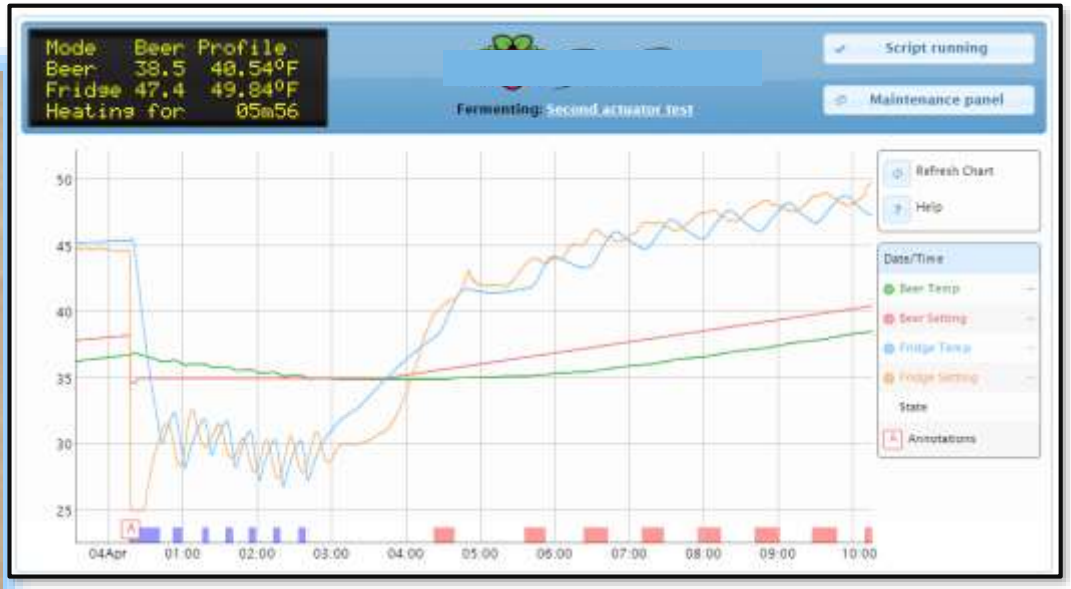
# 6-PHASE CYBERSECURITY T&E PROCESS

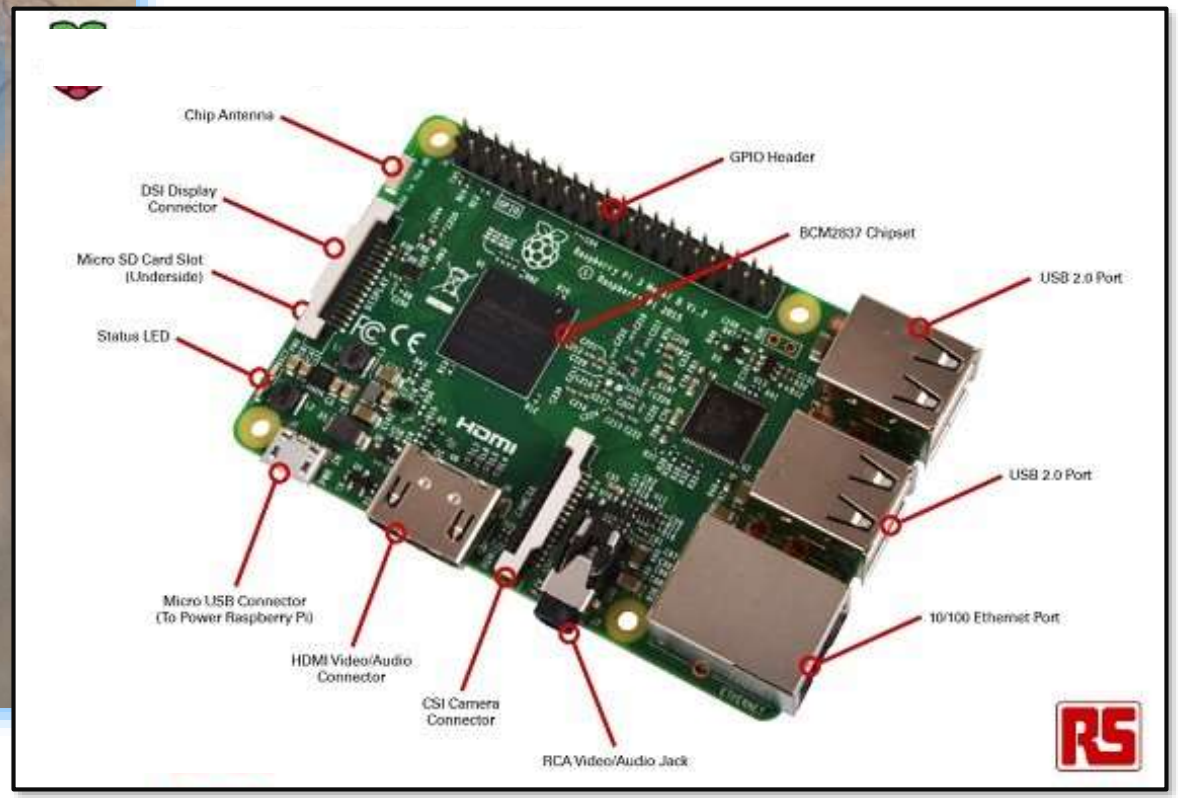


# OUR SUT


Mode Beer Constant
Beer 22.9 19.0 °C
Fridge 22.5 4.0 °C
Cooling for 258 s


Temperature Sensors
OneWire Data Bus
Solid State Relays
USB Port
Embedded Arduino Controller


Mode Beer Profile
Beer 38.5 40.54°F
Fridge 47.4 49.84°F
Heating for 05m56
Fermenting: Second actuator test
Script running
Maintenance panel
Refresh Chart
Help
Date/Time
Beer Temp
Beer Setting
Fridge Temp
Fridge Setting
State
Annotations
50
45
40
35
30
25
04Apr
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00


Chip Antenna
DSI Display Connector
Micro SD Card Slot (Underside)
Status LED
GPIO Header
BCM2837 Chipset
USB 2.0 Port
USB 2.0 Port
10/100 Ethernet Port
Micro USB Connector (To Power Raspberry Pi)
HDMI Video/Audio Connector
CSI Camera Connector
RCA Video/Audio Jack
RS

# 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

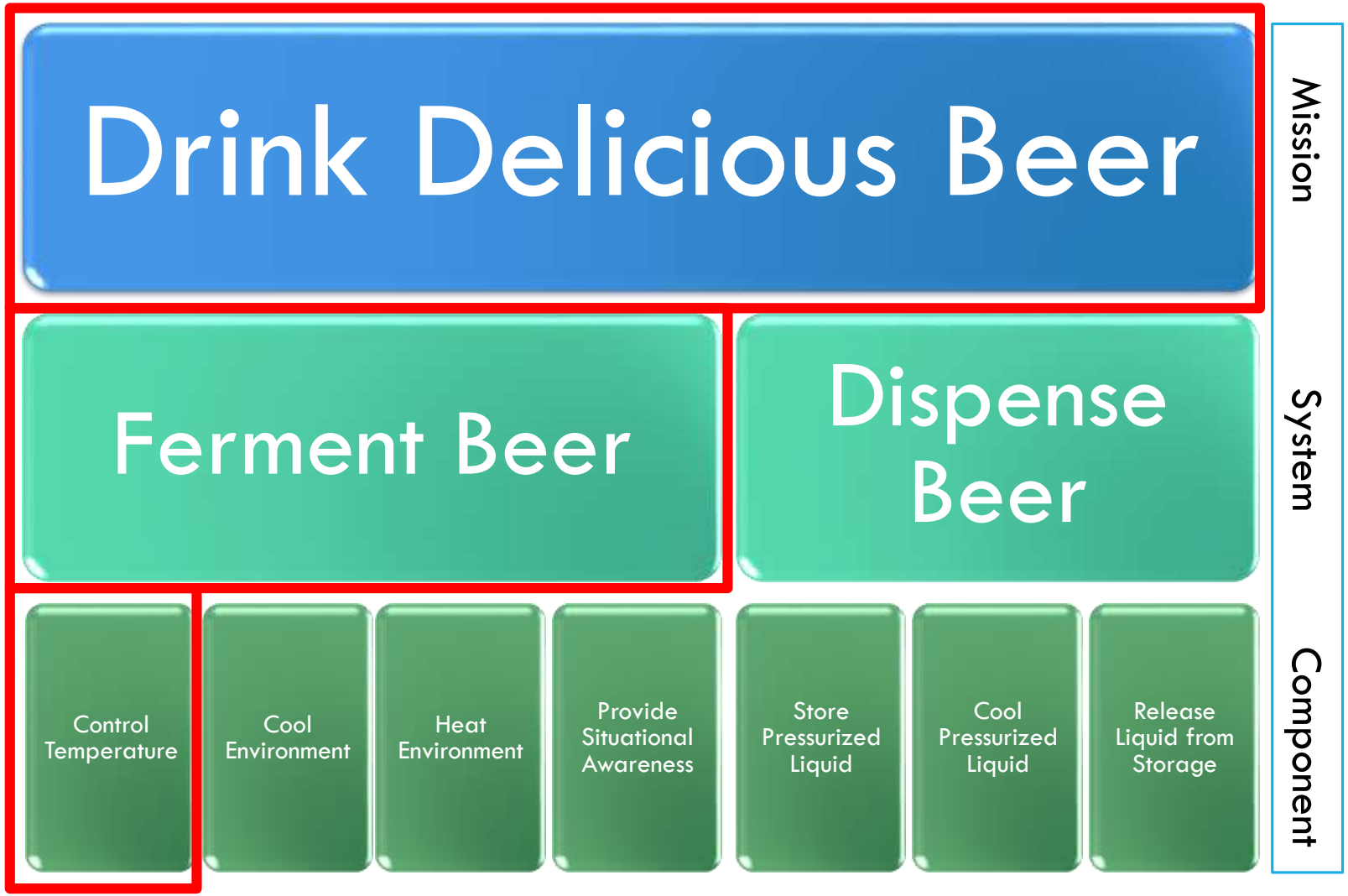
Identify the “important” functions of the SUT

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

# EXEMPLAR - CRITICALITY

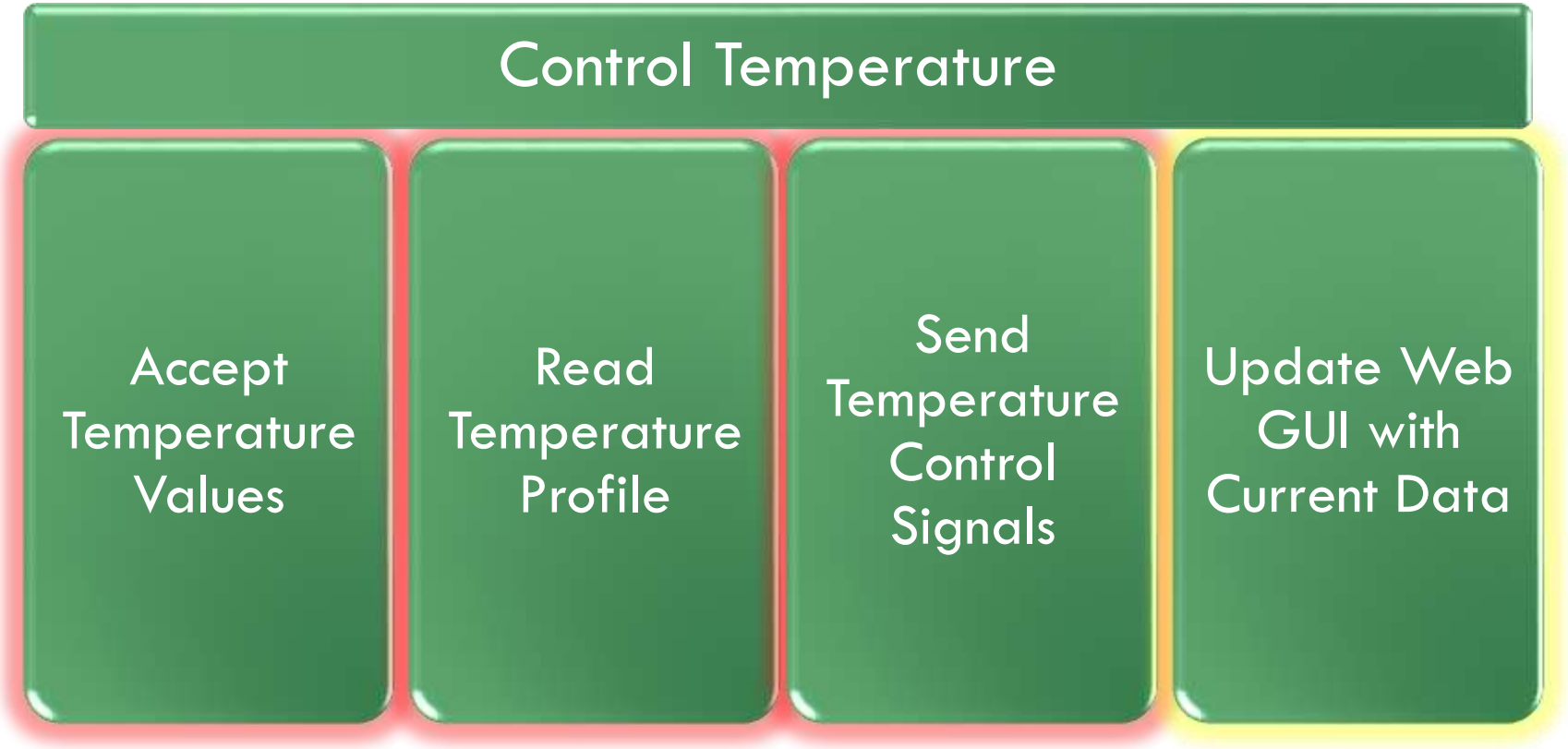
Identify Mission

- Define functionality from component level through mission thread



# EXEMPLAR - CRITICALITY

## List Mission Essential Functions



# AGENDA

Why Cybersecurity?

6-phase overview

Defining our SUT

Characterizing the Attack Surface

- Criticality
- Susceptibility
- Characterization

Summary

# PHASE II, PART 2: HOW TO IDENTIFY ~~VULNERABILITIES~~ Susceptibilities

How could the adversary access the system?

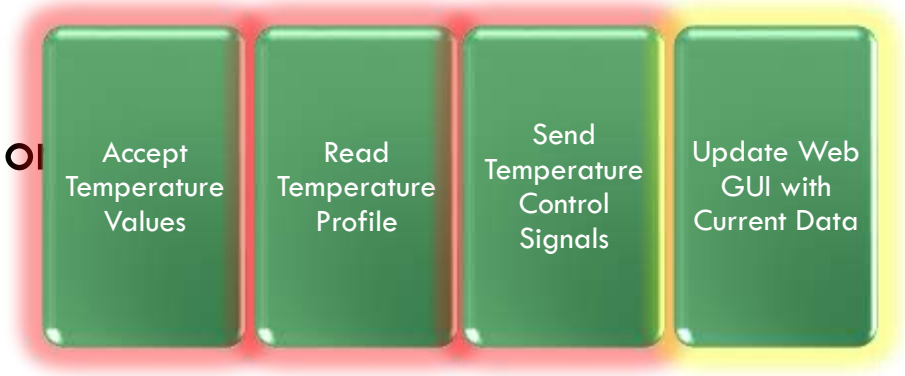
- Map cyber dependencies
- Draw information boundary of SUT
- Enumerate info exchange requirements
- Characterize information flows

System vulnerability is defined to be the intersection of a system susceptibility or flaw, access to the flaw, and the capability to exploit the flaw.

# EXEMPLAR – IDENTIFYING SUSCEPTIBILITIES

## 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

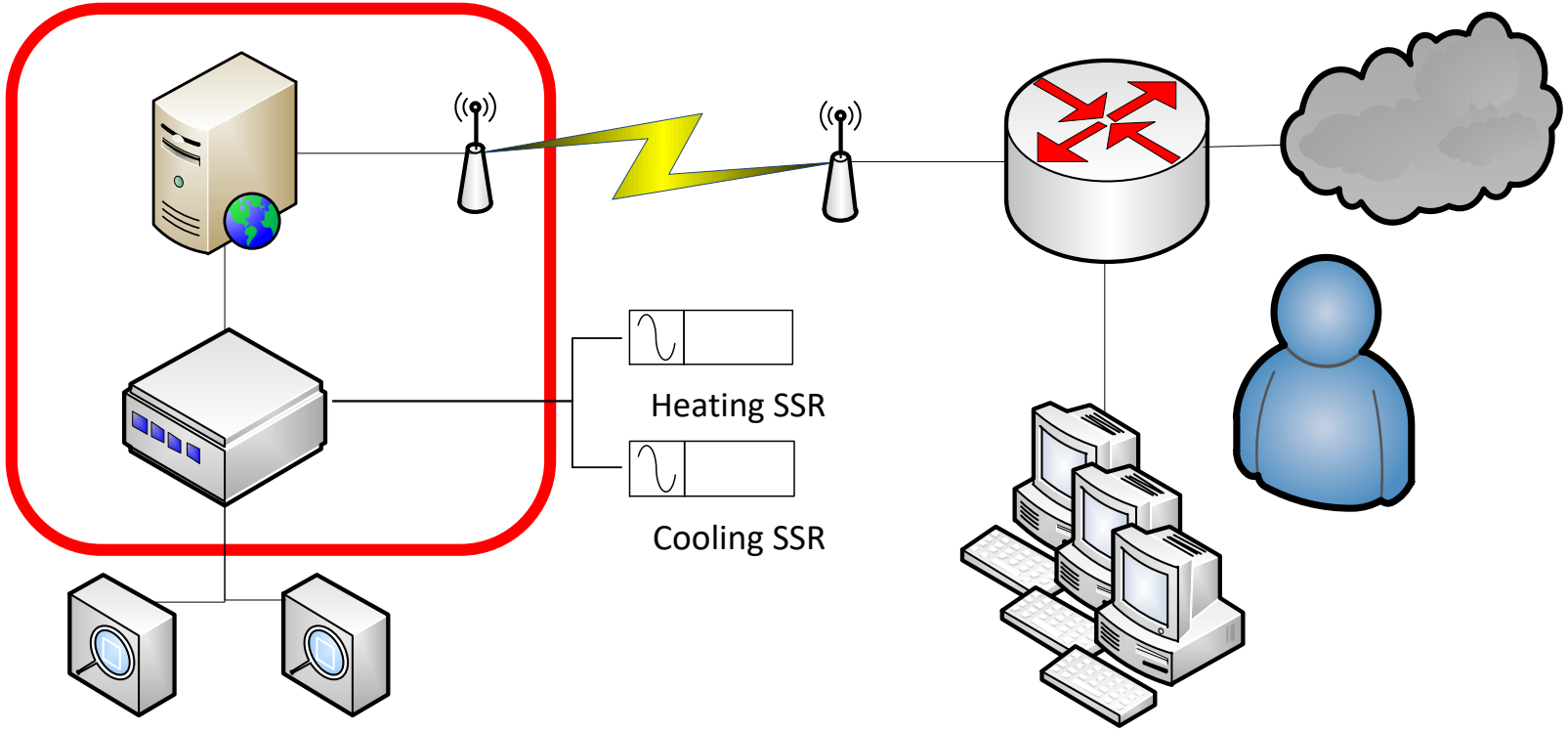


# EXEMPLAR – IDENTIFYING SUSCEPTIBILITIES

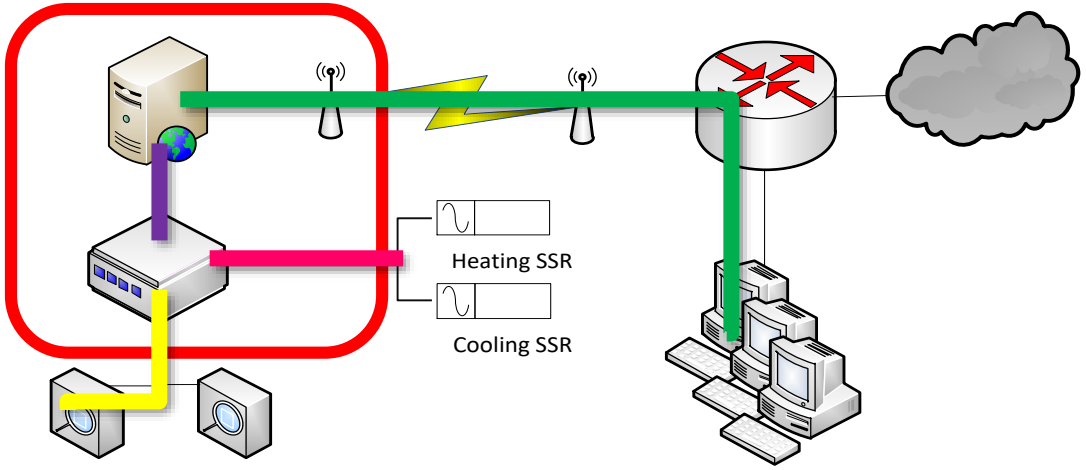
Draw SUT

Information

Boundary



# 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

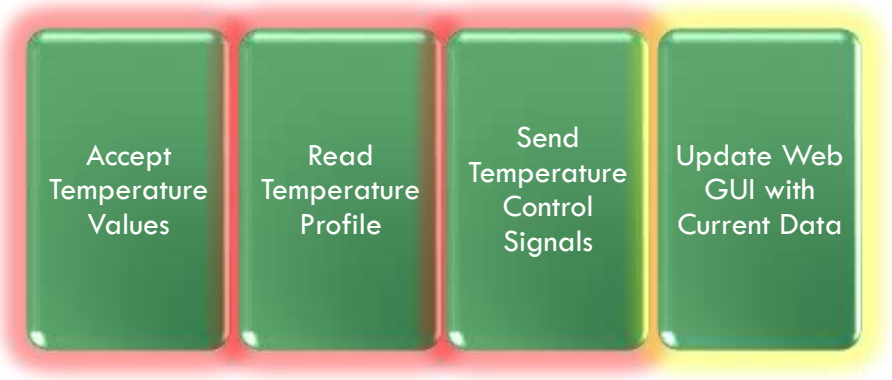
Defining our SUT

Characterizing the Attack Surface

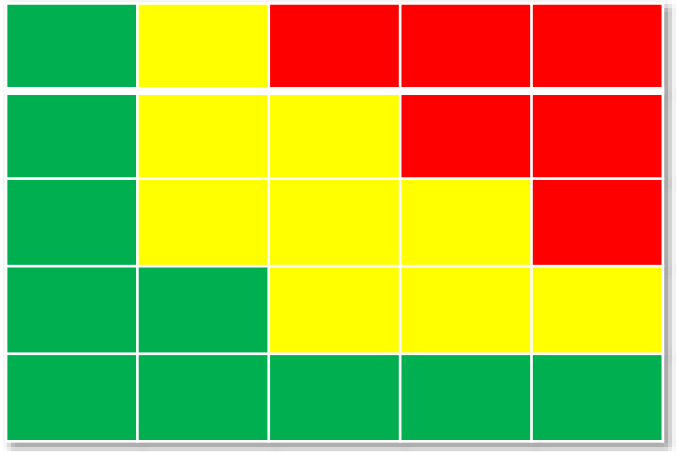
- Criticality
- Susceptibility
- Characterization

Summary

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




+ **Susceptibilities** =



Identify component impacts

Establish D5 effects to the system and mission

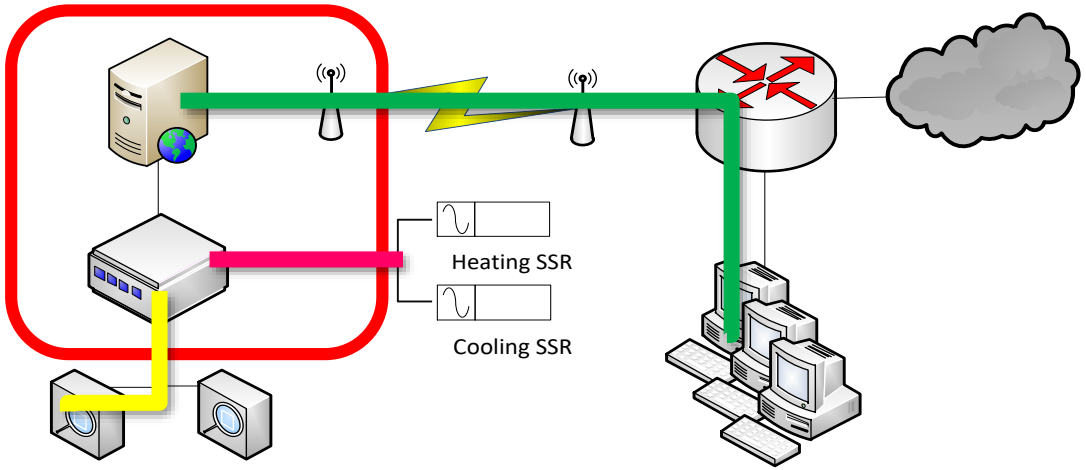
Categorize susceptibilities (architectural, system, or implementation)

… All these Phase II checkpoints feed into Methods of Test for Phase III

# EXEMPLAR – CHARACTERIZE ATTACK SURFACE

Identify impact at the <u>component</u> 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

| Component Impact | Component Effect | System Effect | Mission Impact |
|---|---|---|---|
| Send "on" signal to cooling element | Temperature chamber too cold | Degrade fermentation process | Beer tastes sweet and watery– Effect degraded my delicious beer |
| Send "on" signal to heating element | Temperature chamber too warm | Degrade fermentation process | Beer tastes like commercial solvent – Effect destroyed my delicious beer |
| Send inaccurate temperature value to temp controller | Temperature controller improperly adjusts control signals based on inaccurate info | Degrade fermentation process | Beer tastes {bad/worse} – Effect degraded my delicious beer |
| Alter time signal | Temperature controller improperly adjusts control signals based on inaccurate info | Degrade fermentation process | Beer tastes {bad/worse} – Effect degraded my delicious beer |
| Manipulate text strings sent to UI | Web UI does not display accurate information | Degrade situational awareness of fermentation process | No mission impact |

# 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

# SUMMARY