2021 Collegiate eCTF Kickoff

Ben Janis

January 20th, 2021

SOLVING PROBLEMS FOR A SAFER WORLD™

Outline

1. Welcome
2. Competition Overview
3. Challenge Overview
4. Security Requirements
5. Attack Deployment
6. Flags

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1

Outline

MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Participating Schools

AMRITA VISHWA VIDYAPEETHAM

NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

UF | UNIVERSITY of FLORIDA

DACC DELAWARE AREA CAREER CENTER

PURDUE UNIVERSITY

UMass Amherst

DAKOTA STATE UNIVERSITY

TEXAS A&M UNIVERSITY

UNIVERSITY OF Nebraska Omaha

FIU FLORIDA INTERNATIONAL UNIVERSITY

Tufts UNIVERSITY

Massachusetts Institute of Technology

University at Buffalo

UNIVERSITY OF WYOMING

Northeastern

UCONN UNIVERSITY OF CONNECTICUT

WPI

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Organizers

MITRE

MITRE is a not-for-profit organization that operates research and development centers sponsored by the federal government. MITRE works with industry and academia to apply science, technology, and systems engineering that enables the government and the private sector to make better decisions.
Learn more at www.mitre.org

Follow us on Twitter, @MITREonCampus, @MITREcorp

RIVERSIDE RESEARCH

Riverside Research is a not-for-profit organization chartered to advance scientific research for the benefit of the US government and in the public interest. Riverside Research conducts independent research in machine learning, trusted systems, optics and photonics, electromagnetics, and plasma physics.
Learn more at www.riversideresearch.org

@RiversideRsch

Outline

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Competition Overview

Design

- **Begins January 20th, 2021**
- Teams design a secure system that meets all the challenge requirements
- Teams attempt to solve development challenges to retrieve design-phase flags

Handoff

- **Begins March 3rd, 2021**
- Teams submit their designs to the eCTF Organizers
- Organizers verify that each design has met all the functional requirements
- Organizers post verified designs for all teams to evaluate during the attack phase

Attack

- **Begins immediately after successful completion of Handoff**
- Teams perform a security evaluation of opposing teams' systems
- Teams demonstrate attacks by retrieving flags
- **Scoreboard closes April 16th, 2021**

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

New Features

- **Emulated hardware**
  - Development servers
- **Design Phase Points**
  - Reverse Engineering Challenge
  - Bug Bounty
- **ATT&CK/PIVOT Framework**
- **Side Channel Collection**

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Prizes and Competition Qualification Requirements

- **This year will have $5000 in prizes for the winning teams**
  - 1st Place: $2000
  - 2nd Place: $1000
  - 3rd Place: $500
  - Special Awards: $1500 (may be split among multiple teams)

- **Any student can compete in the eCTF, but to receive prize money you must meet certain eligibility requirements**
  - Check rules document for eligibility terms

- **Processes have been put in place to keep the competition fair**
  - Current and former MITRE employees and interns will be competing
  - Competition organizers are firewalled from MITRE participants – no discussions allowed outside of official channels
  - All questions and requests for help are taken on a first-come-first-serve basis
  - Write-ups are anonymized before judging

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Outline

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

The Scenario

- **Your team is tasked with designing and implementing a secure communications system for a UAV delivery system**

- **The communications system is called…**
  - …the Secure Common Embedded Wireless Link Bus or…
  - …the SCEWL Bus!

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

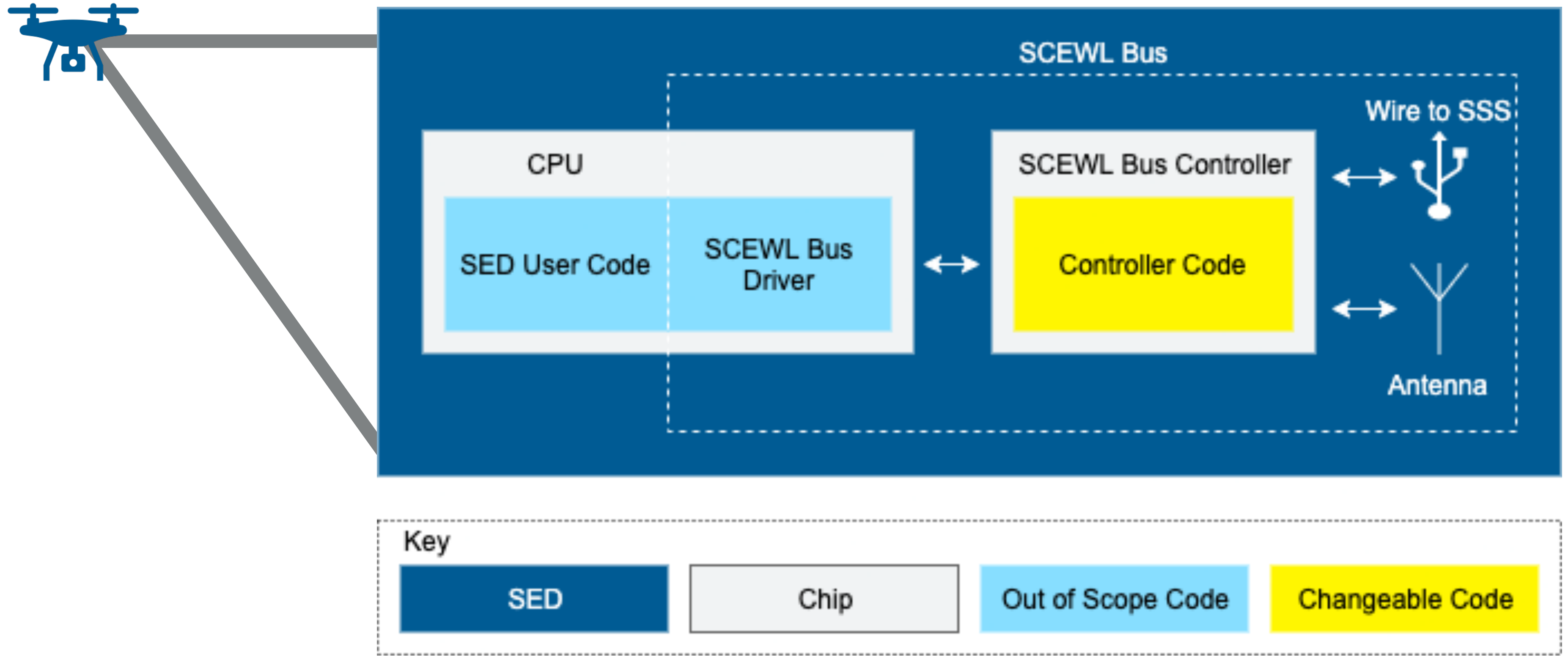
Deployment

- **A SCEWL Deployment has two components**
  - SCEWL-Enabled Devices (SEDs)
  - SCEWL Security Server (SSS)

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

SCEWL-Enabled Devices (SEDs)

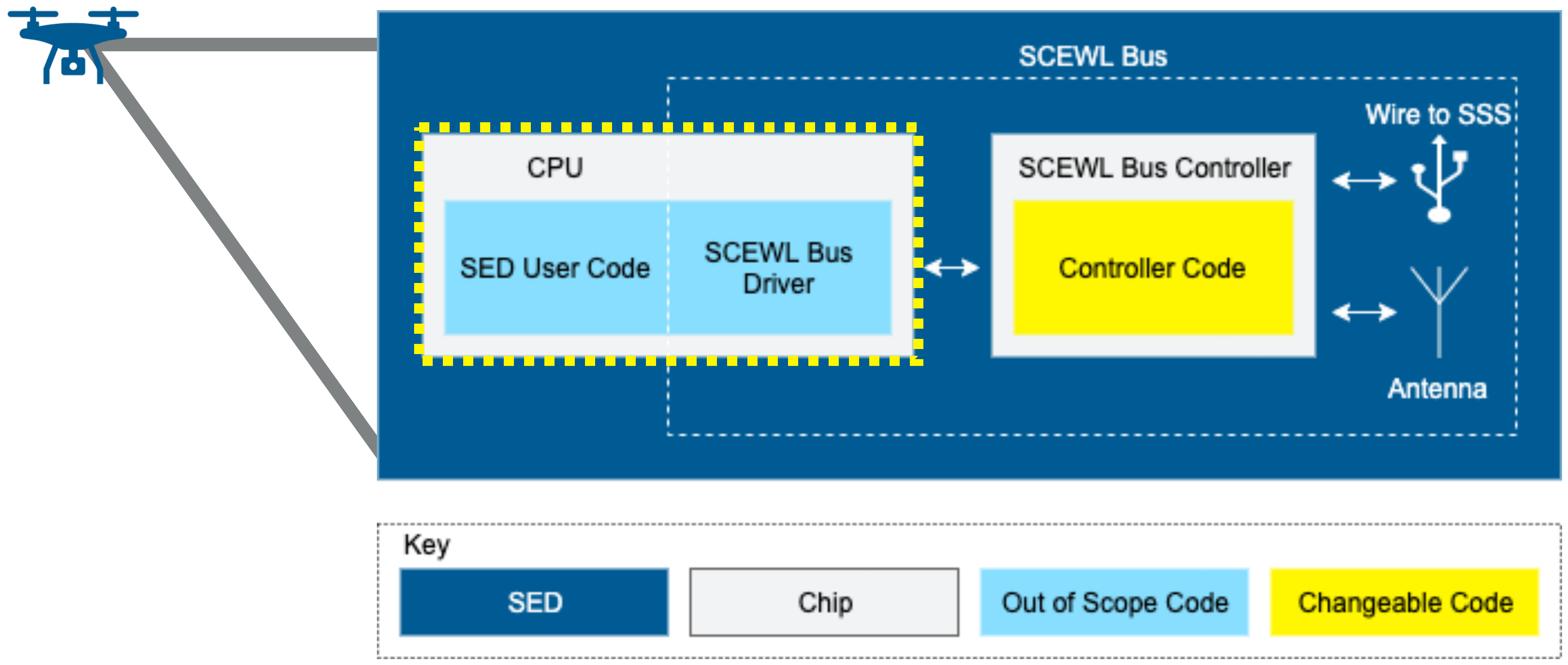
- **SEDs are any device with the SCEWL Bus**
  - Includes UAVs and command-and-control devices



MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

SCEWL-Enabled Devices (SEDs)

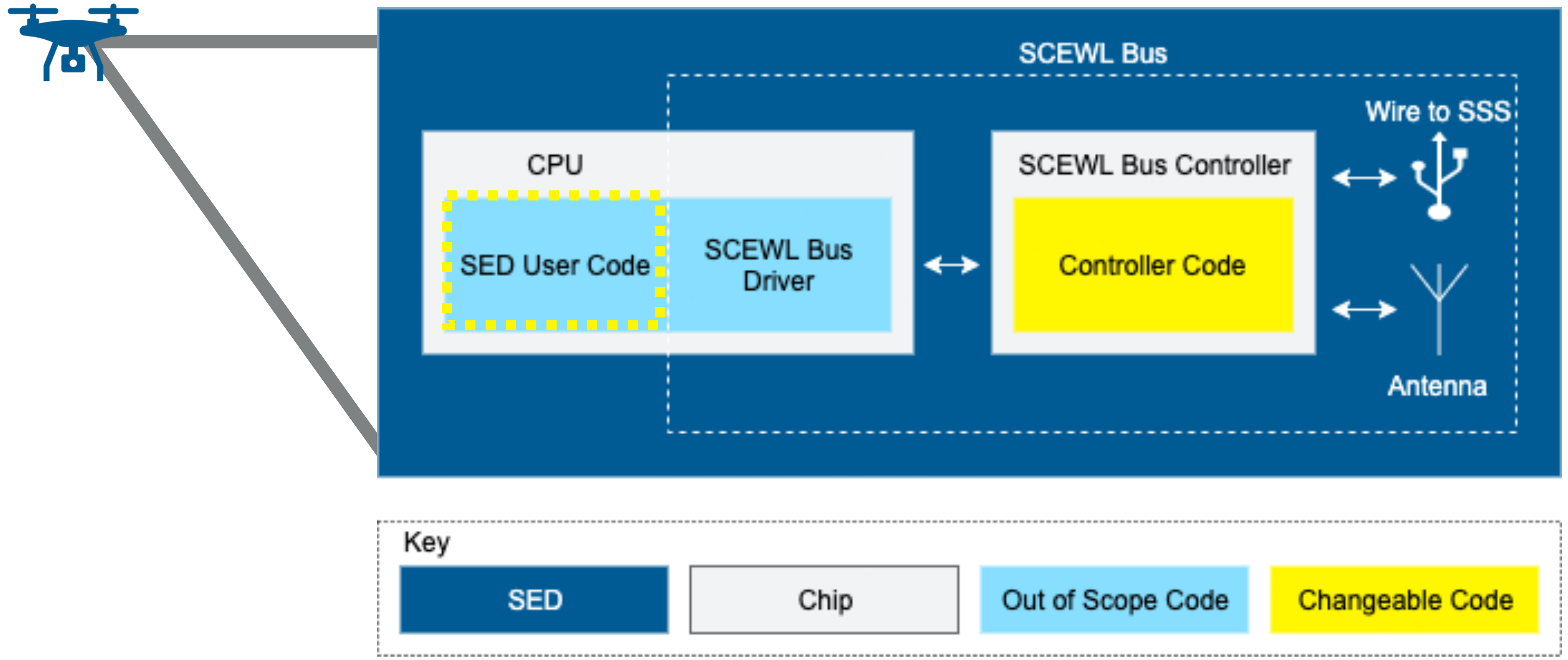
- **CPU**
  - Powerful embedded ARM CPU running an OS



© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

SCEWL-Enabled Devices (SEDs)

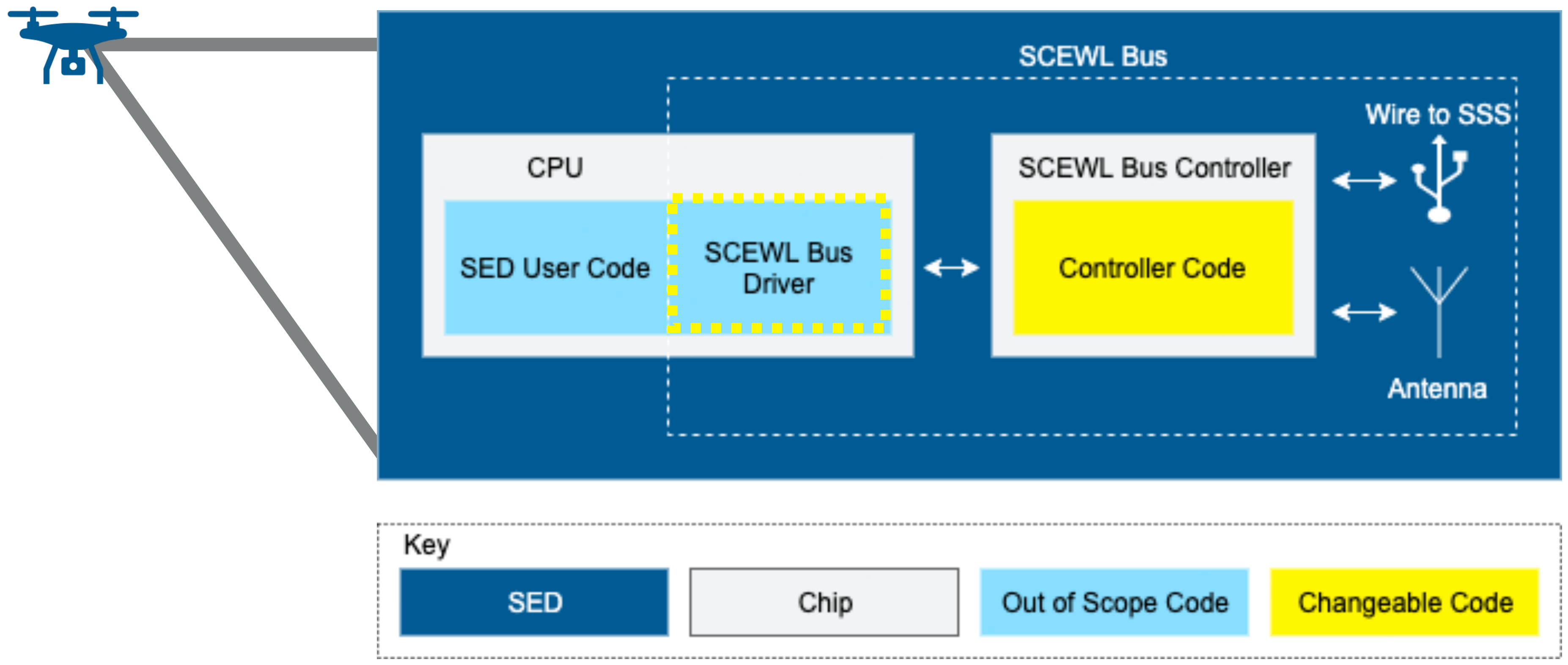
- **SED User Code**
  - Controls the operation of the SED



© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

SCEWL-Enabled Devices (SEDs)

- **SCEWL Bus Driver**
  - Driver library that interfaces with the SCEWL Bus

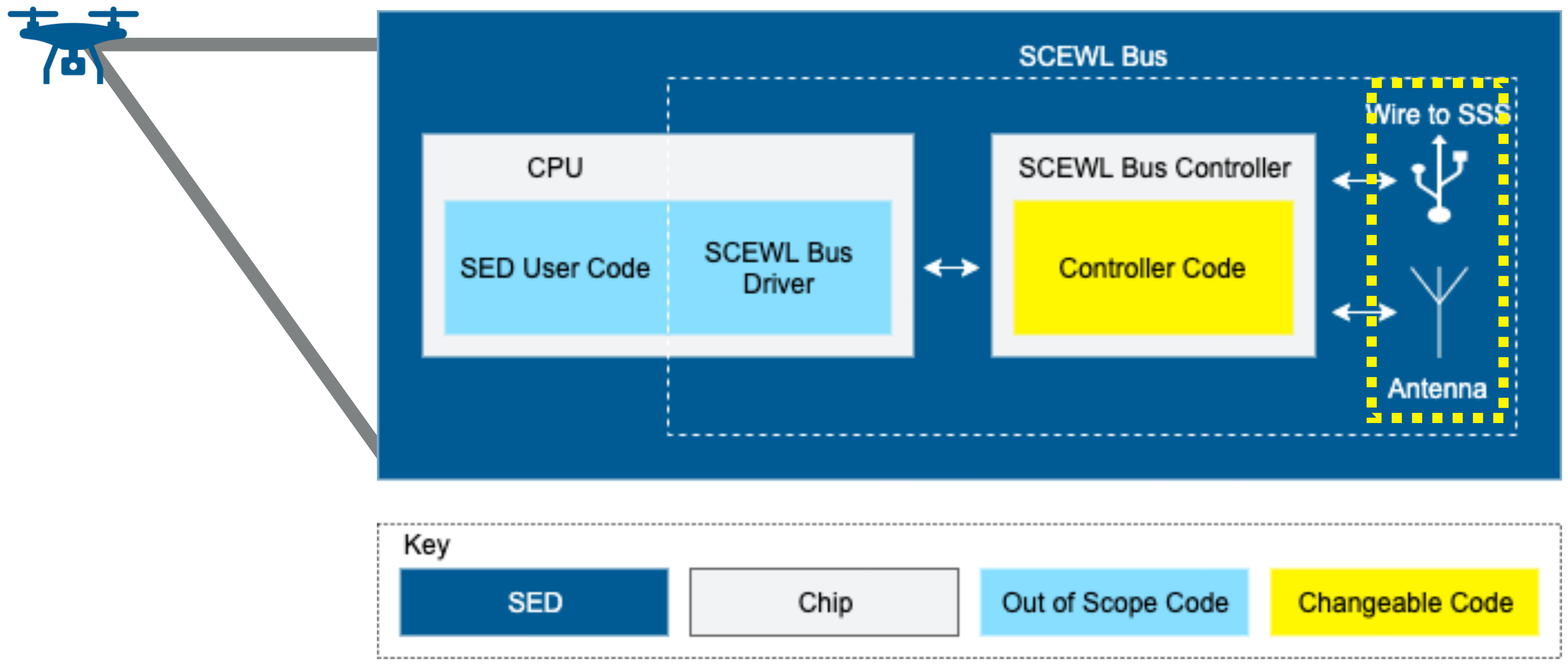


MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

SCEWL-Enabled Devices (SEDs)

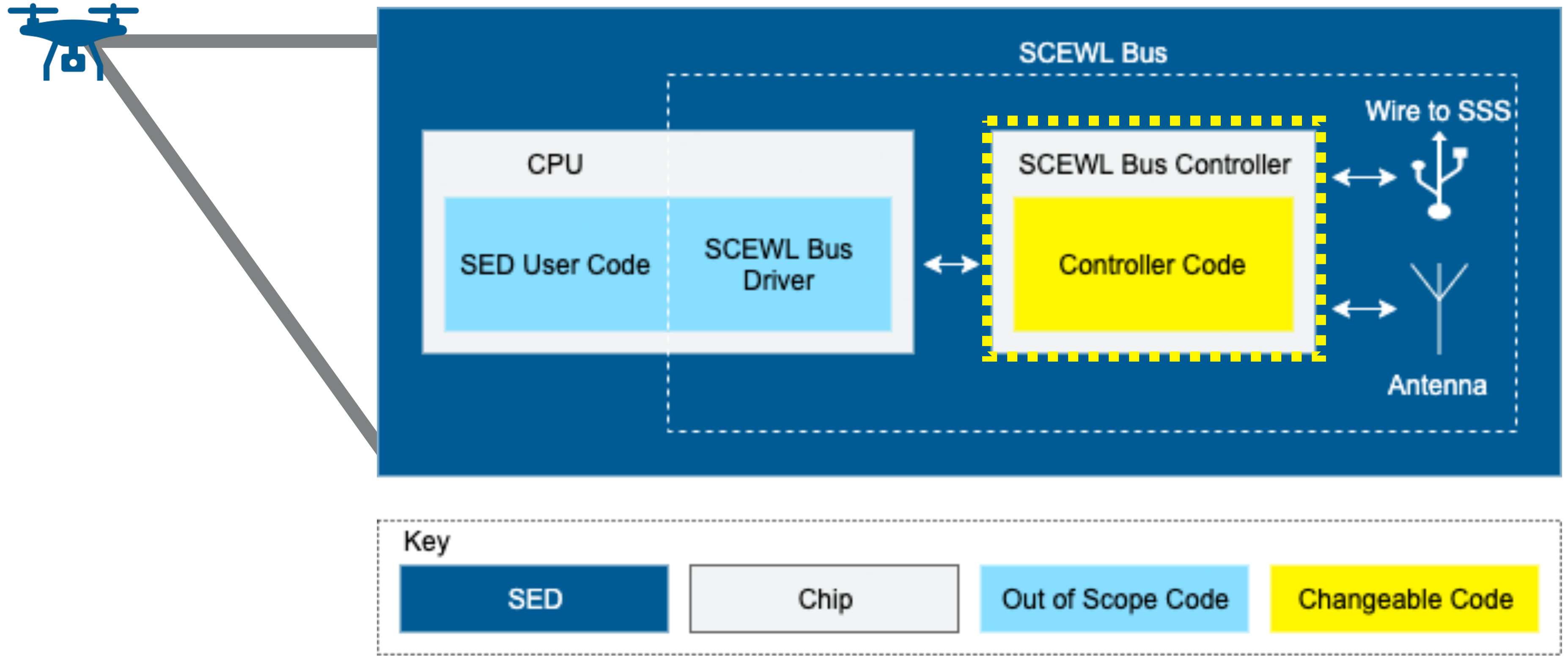
- **Hardware interfaces**
  - Wired communication to SSS and wireless communication over antenna



MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

SCEWL-Enabled Devices (SEDs)

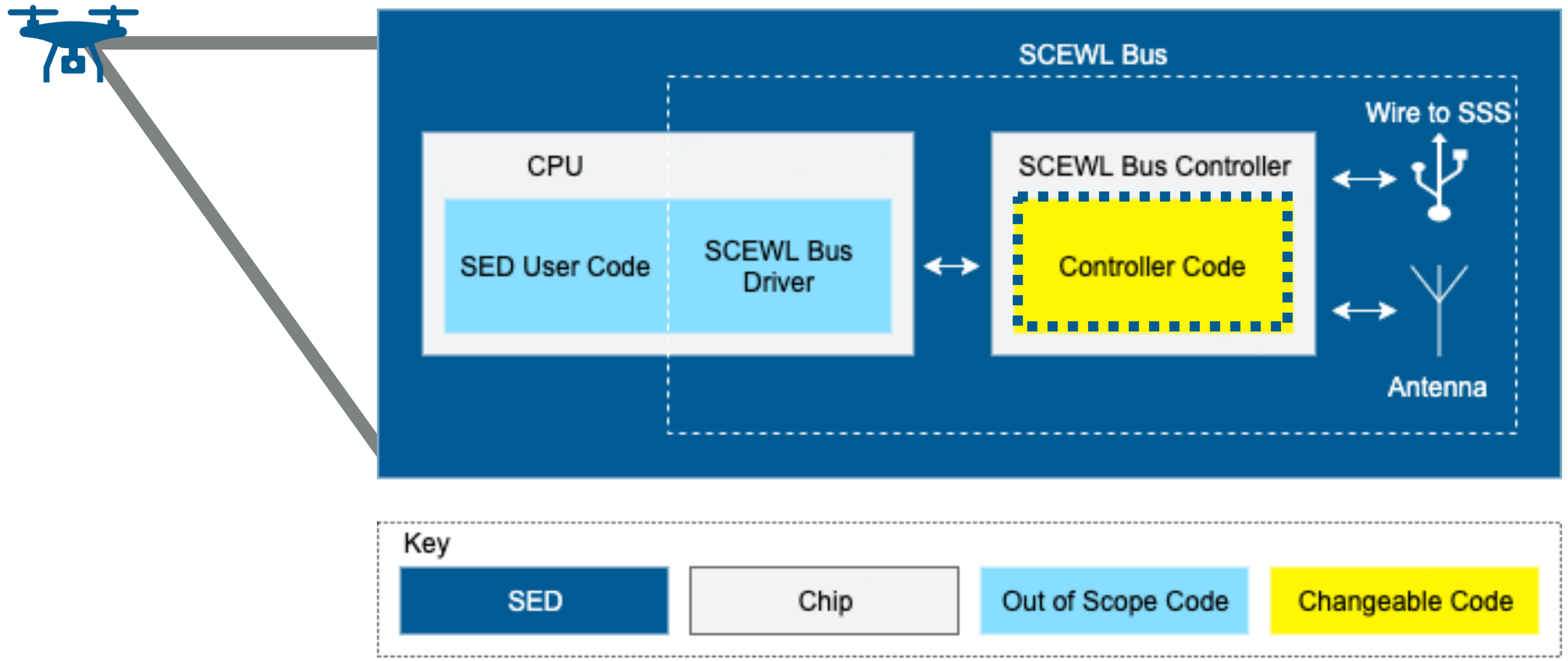
- **SCEWL Bus Controller**
  - Embedded ARM Cortex-M3 Microcontroller driving hardware interfaces



© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

SCEWL-Enabled Devices (SEDs)

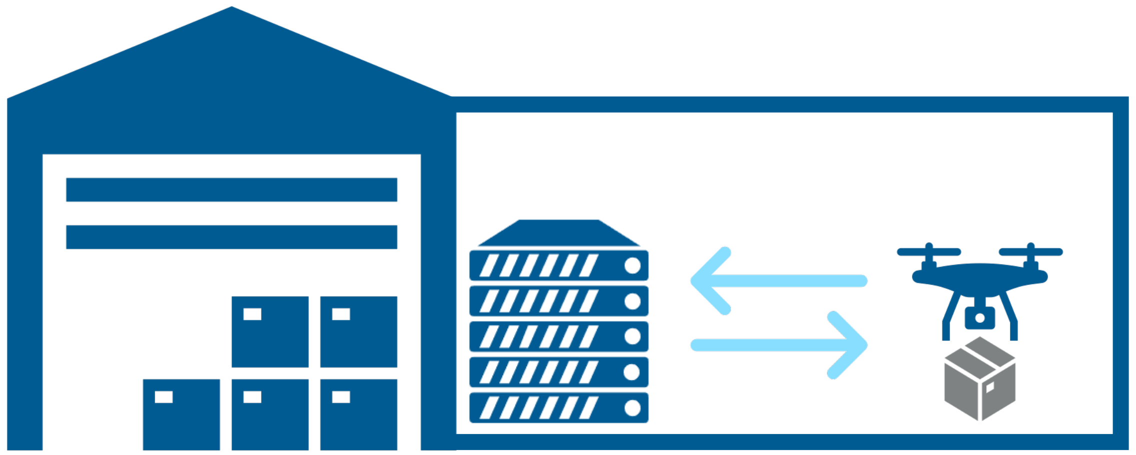
- **SCEWL Bus Controller Code**
  - Your code that handles security and message passing



© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

SCEWL Security Server (SSS)

- **Handles registration and deregistration of SEDs**
- **Registration is first thing SED does after powering on**
  - SSS can bootstrap SED with any necessary information
- **Deregistration is last thing SED does before powering off**
- **SEDs must be able to register again after deregistering**



MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Outline

MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Building Requirements

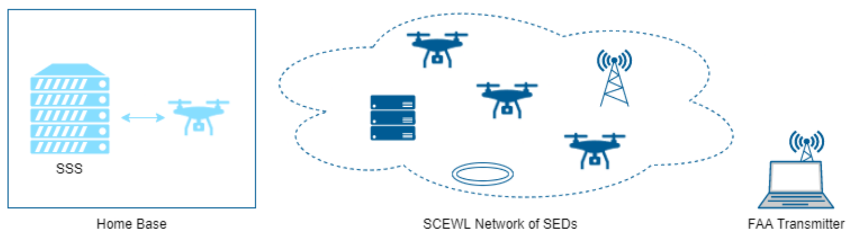
- Create the SSS
- Build and add an SED to the deployment
- Remove an SED from the deployment

MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

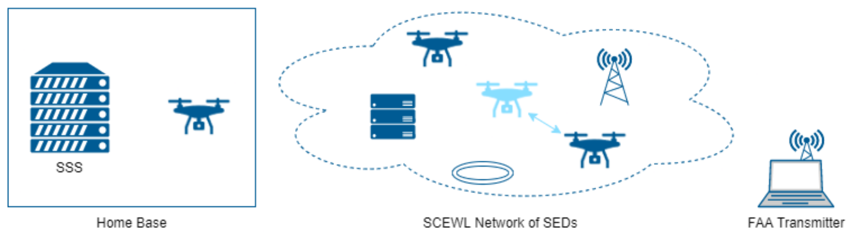
SED Functional Requirements

- **Register and deregister with SSS**
- **Send a direct transmission to another SED**
- **Send a broadcast to all active SEDs**
- **Communicate with an FAA Transmitter**
  - Must be in the clear

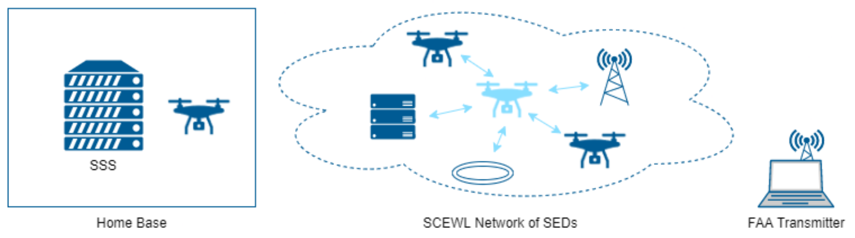
Registration/Deregistration



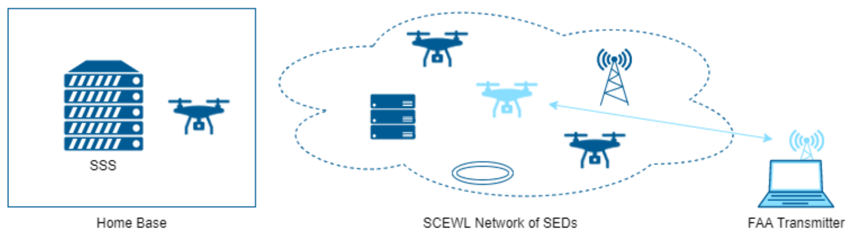
Direct Transmission



Broadcast



FAA Transmission



MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

SED Security Requirements

- **Confidentiality**
  - SCEWL Transmissions should not be readable by anyone other than the intended device(s)
- **Integrity**
  - SCEWL Transmissions should not be able to be modified by an attacker
- **Authentication**
  - Messages should not be able to be injected into the network by an attacker
  - An attacker should not be able to register a device with the SSS
- **Replay**
  - An attacker should not be able to have a device accept a message that has been recorded and replayed
- **Defense-in-Depth**
  - The SCEWL Bus Controller should be robust against arbitrary input from both the antenna and from the CPU

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Outline

1. Welcome
2. Competition Overview
3. Challenge Overview
4. Requirements
5. **Attack Deployment**
6. Flags

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Attack Phase Deployment

- This is the context in which your SCEWL Bus will be used
- Your team does not have to implement any of this functionality

Attack Phase SEDs

- **Unmanned Aerial Vehicle (UAV) SED**
  - Delivers packages to customers
  - Many deployed at once
  - Flies from home base to customers’ houses
- **Command and Control (C2) SED**
  - Gives delivery orders to UAV
  - Only one deployed
  - Located at home base
- **Drop Zone (DZ) SED**
  - Communicates with UAV to receive package
  - One located at each customer’s house

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

1. SSS Setup

- SSS Launches

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

2. Deployment Setup

- C2 server launches and registers with SSS
- DZs launch, register with SSS, and relocate to customers' houses

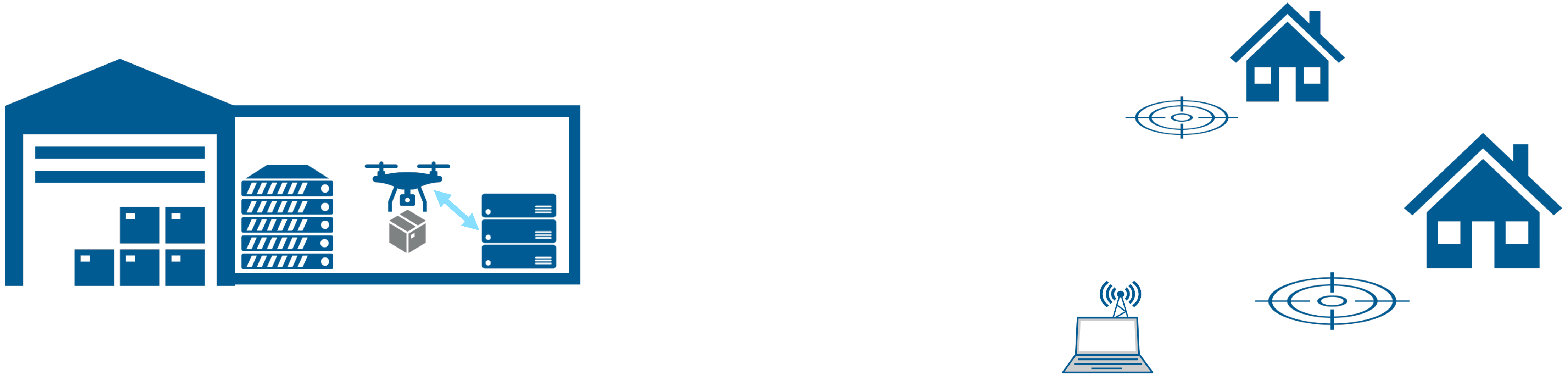
3. UAV Launches

- UAV powers on
- UAV registers with SSS

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

4. UAV Receives Orders

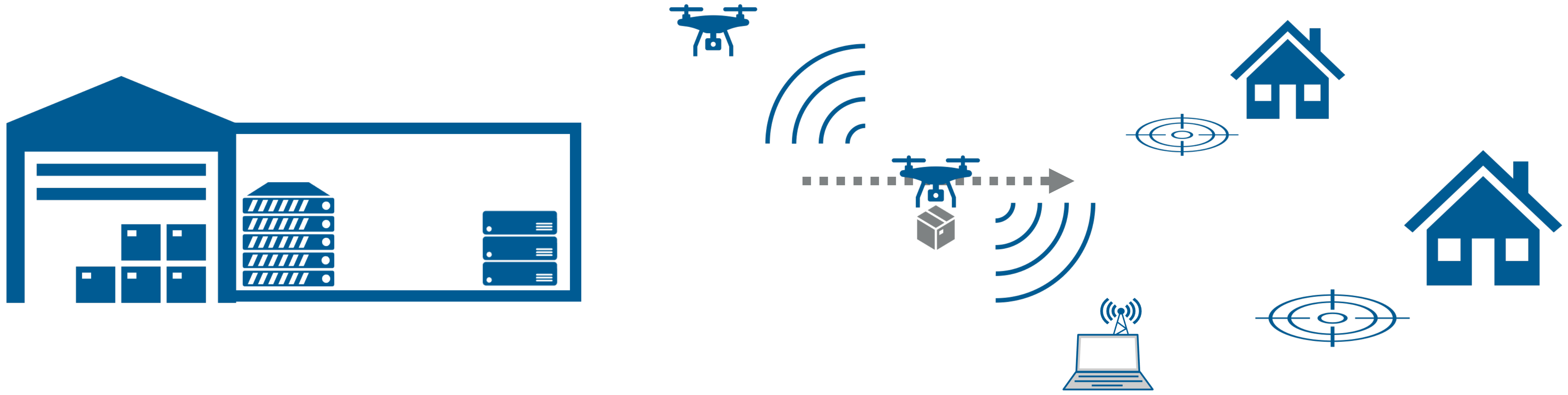
- **UAV Communicates with C2 to receive delivery order**



© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

5. UAV En Route

- UAV travels to customer's house
- UAV sends broadcast with its location at beginning of its transit and regularly on its way



© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

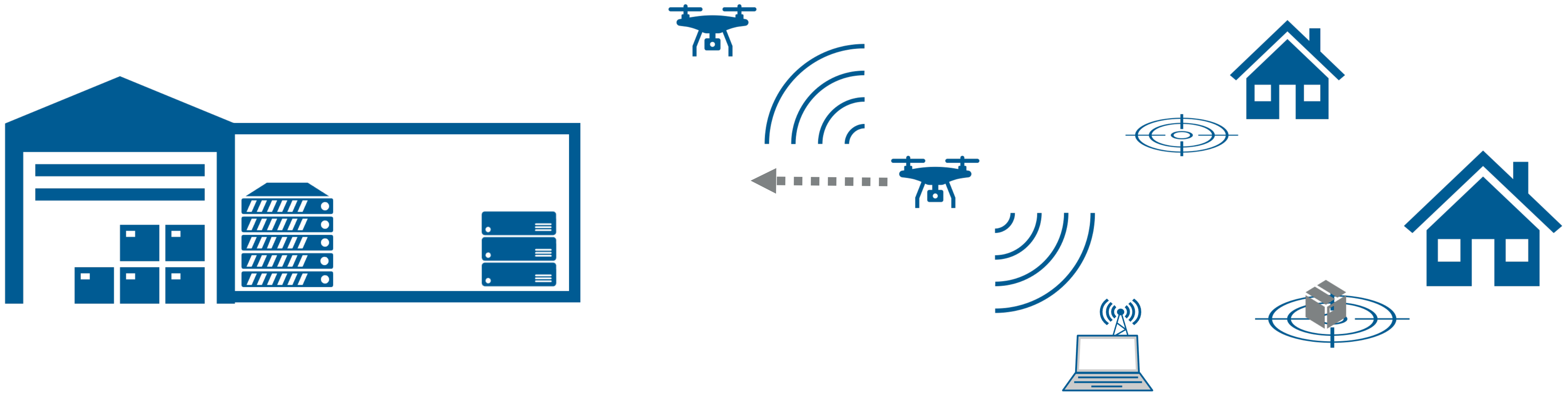
6. UAV Delivers Package

- UAV arrives at house
- UAV sends SYN to DZ
- DZ responds with ACK
- UAV distributes package

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

7. UAV Returns

- Similar process as the transit to the customer’s house



MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

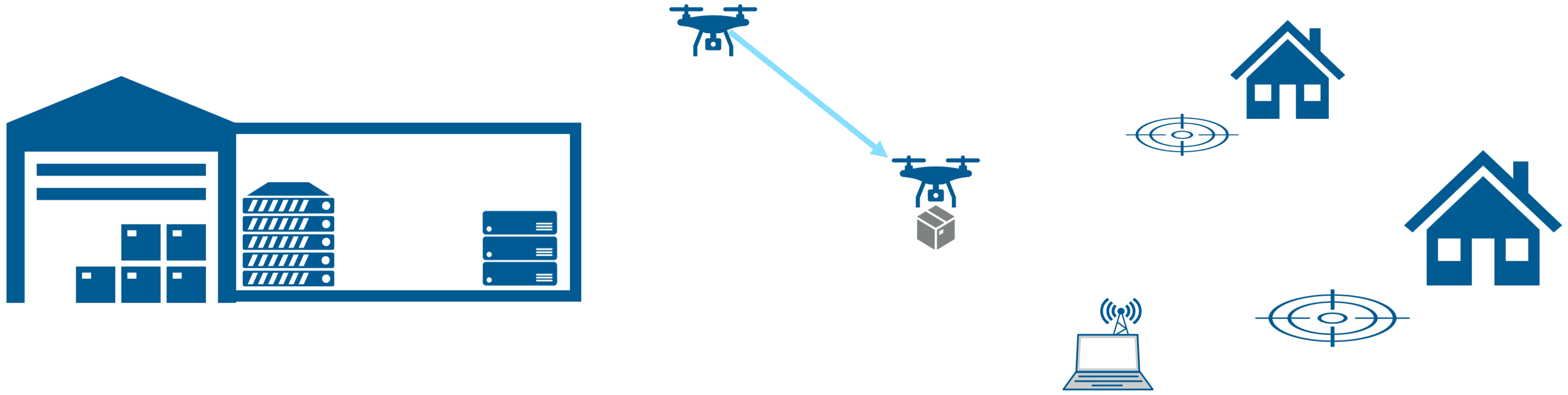
8. UAV Deregisters

- UAV deregisters from SSS and powers down

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

A. UAV Deconflict

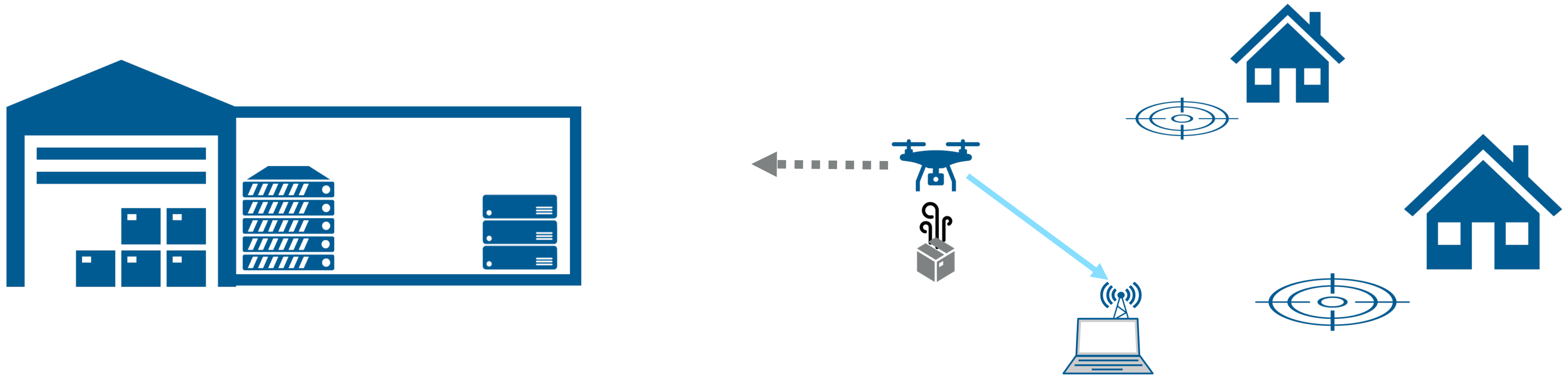
- Triggered if UAV receives a broadcast from another UAV saying it is flying at the same altitude
- Triggered UAV responds by telling other UAV to fly up 5m
- Other UAV flies up 5m and rebroadcasts new location



MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

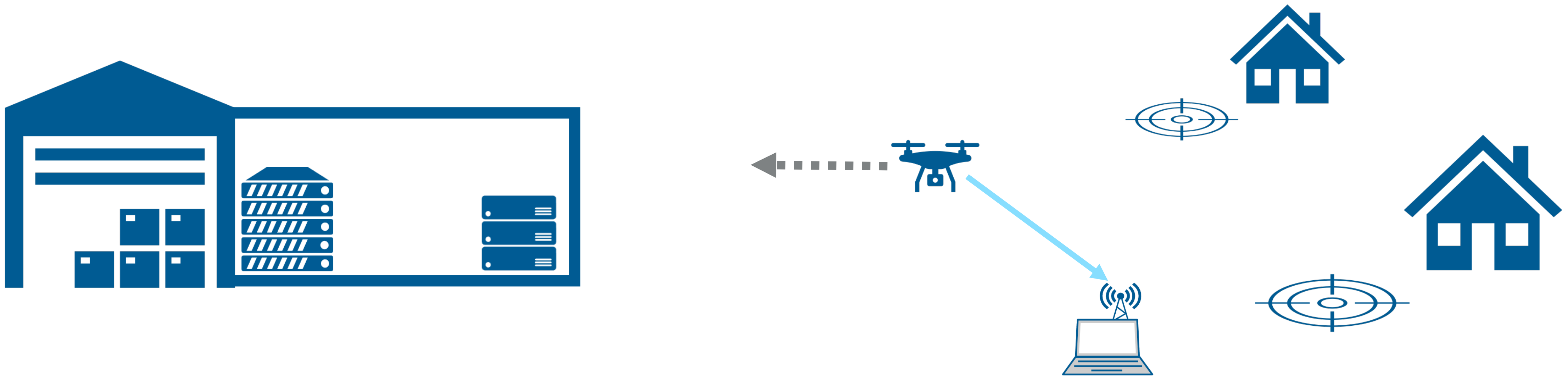
B. UAV Emergency Drop

- Triggered if UAV receives emergency drop message
- UAV sends emergency drop notification to FAA channel, drops package, and returns home



C. UAV Recovery

- Every message between SEDs contains a plaintext checksum
- Triggered if a UAV receives any message with a bad checksum
- UAV sends recovery message to FAA channel and returns home



MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

What Attackers Will be Given

- All source code (with the .git directory removed)
- Configurations used to build the attack-phase deployment
- The most recent documentation provided to the eCTF organizers
- An FAA receiver to communicate with the FAA channel
- A basic man-in-the-middle interface that teams can adapt to intercept, modify, inject, or drop messages sent across the SCEWL Network
- The SCEWL Bus Controller binary extracted from a “downed UAV” that has since been removed from the deployment
- The attacker’s DZ SED
  - Running insecure user code in the CPU from the reverse engineering challenge
  - Rigged with an interface to collect side-channel traces from the DZ’s SCEWL Bus Controller

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

UNDERSTAND WHAT THE ATTACKERS HAVE ACCESS TO

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Attack Phase Deployment

- This is the context in which your SCEWL Bus will be used
- Your team does not have to implement any of this functionality

Outline

1. Welcome
2. Competition Overview
3. Challenge Overview
4. Security Requirements
5. Attack Deployment
6. **Flags**

MITRE
© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Design Phase Flags

- **Encourages staying on track in development**

Milestone	Description / How to obtain the flag	Deadline Date
Read Rules	If you read all the rules, you'll know	1/27/21
Boot Reference	Provision and boot the scewl_echo and the scewl_echo_client SEDs (as explained in the REAME) to receive a flag.	1/27/21
Design Document	Submit a design document containing descriptions of how each command will work on your system. Your design may change after submitting this first draft.	2/3/21
Use Debugger	Use the debugger Makefile rule to step through a binary and retrieve a flag	2/10/21
Bug Bounty	Find and fix a bug in the reference design (first come, first serve)	3/3/21 (handoff)

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Reverse Engineering (RE) Challenge

- **Three CPU user code binaries to RE**
- **Increasing levels of difficulty**
- **General flow:**
  1. RE binary
  2. Determine correct input
  3. Run binary and send input to dispense flag
- **Third binary will be present in the attack phase deployment**
  - Teams that successfully RE the third binary will gain arbitrary code execution on CPU of DZ

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Attack Phase Flags

Flag Name	Capturing this flag proves that you can…	Requirement	To Submit this Flag…
UAV ID Recovery	Read a broadcasted SCEWL Transmission	Confidentiality	Obtain the UAV ID from the broadcasting UAV SED
Package Recovery	Read a targeted SCEWL Transmission	Confidentiality	Obtain a package not destined for the attacker-controlled DZ, which will be sent from the C2 to the UAV and from the UAV to the DZ
Recovery Mode	Modify the content of a SCEWL Transmission	Integrity	Corrupt the plaintext of a message so that the user code's checksum check fails and the UAV goes into recovery mode. Read the flag from the FAA channel
Drop Package	Have full control of the plaintext contents of a SCEWL Transmission	Integrity / Authentication	Have the user code of any deployed UAV SED receive the drop package message . Read the flag from the FAA channel
No-Fly Zone	Take control of the UAV	Integrity / Authentication / Replay Protection	Abuse the emergency redirect message to push the UAV into a no-fly zone. Read the flag from the FAA channel

MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Words of Advice

- Start development early
- Use a debugger
- Think like an attacker during design phase
- Use Slack for help
- Understand what attackers will have access to

MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Next Steps

- Read the rules
- Begin designing your system
- Get access to the development server
- Get the deployment running
- Begin development
- Start working on the RE challenge

MITRE © 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.

Good luck!

Ben Janis

btjanis@mitre.org

ectf@mitre.org

https://www.linkedin.com/groups/12371545/

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-03314-1.