2023 eCTF Kickoff

Kyle Scaplen

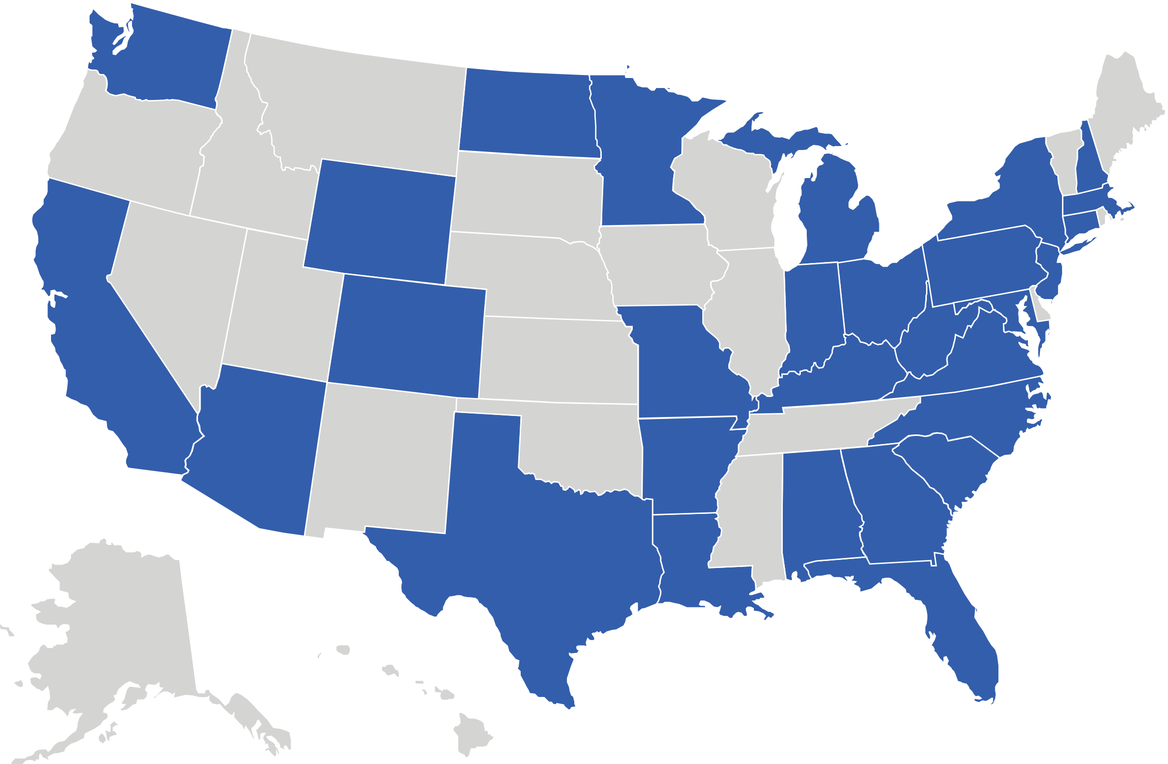
January 18, 2023

SOLVING PROBLEMS
FOR A SAFER WORLD®

Outline

1. **Welcome**
2. Competition Overview
3. Challenge Overview
4. Requirements
5. Flags
6. Attacker Resources
7. Getting Started

Nationwide Competition



This year we have teams from:

29 States

78 Schools

4 Countries

Participating Schools

Air Force Institute of Technology	ISD 196	Rose-Hulman Institute of Technology	University of Edinburgh
AJ College of Science and Technology	Johns Hopkins University	Searcy High School	University of Illinois at Urbana-Champaign
Amrita Vishwa Vidyapeetham University	Kilgore College	Singapore Management University	University of Maryland College Park
Baldwin Wallace University	Lakota East High School	Springfield-Clark County CTC	University of Massachusetts Amherst
BASIS Chandler	Louisiana State University	SRM Institute of Science and Technology	University of New Hampshire
Carnegie Mellon University	Marriotts Ridge High School	Symbiosis Institute of Technology	University of New Haven
Center I (Albemarle County Public Schools)	Massachusetts Institute of Technology	Texas A&M University	University of North Dakota
Clarendon High School	Michigan State University	Thadomal Shahani Engineering College	University of Texas at Dallas
Clemson University	Morgan State University	The Harker School	University of Texas at Arlington
Delaware Area Career Center	Mount Saint Dominic Academy	Thomas Jefferson High School for Science and Technology	University of Washington
Essex North Shore Agricultural and Technical School	New Century Technology High School	Tufts University	University of Wyoming
Farmington High School	New York University	United States Military Academy	US Air Force Academy
Florida Atlantic University	Norfolk State University	University at Buffalo	Virginia State University
Florida International University	North Carolina State University	University of Alabama in Huntsville	Virginia Tech
Georgia Institute of Technology	Northern Virginia Community College	University of Arizona	Wellington High School
Hanze University of Applied Sciences	Nova Southeastern University	University of California Irvine	West Virginia University
Harmony Science Academy	Parkway Spark!	University of California Santa Cruz	Worcester Polytechnic Institute
Huntsville City Schools Cyber Academy	Penn State Abington	University of Colorado, Colorado Springs	Xavier University
Indian Institute of Technology Madras	Purdue University	University of Connecticut	Key:
Indiana Institute of Technology	River Hill High School	University of Dayton	New Participant Returning Champion High School

Organizers

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 @MITRECorp

Thank You Sponsors

Thank you to our sponsors, who make this event possible.

Platinum

ANALOG DEVICES

FORTINET®

CROWDSTRIKE

Gold

BCI

Bronze

Rambus

Outline

1. Welcome
2. **Competition Overview**
3. Challenge Overview
4. Requirements
5. Flags
6. Attacker Resources
7. Getting Started

Unique Competition Design

Focus on Embedded

Physical hardware opens scope to physical and proximal attacks

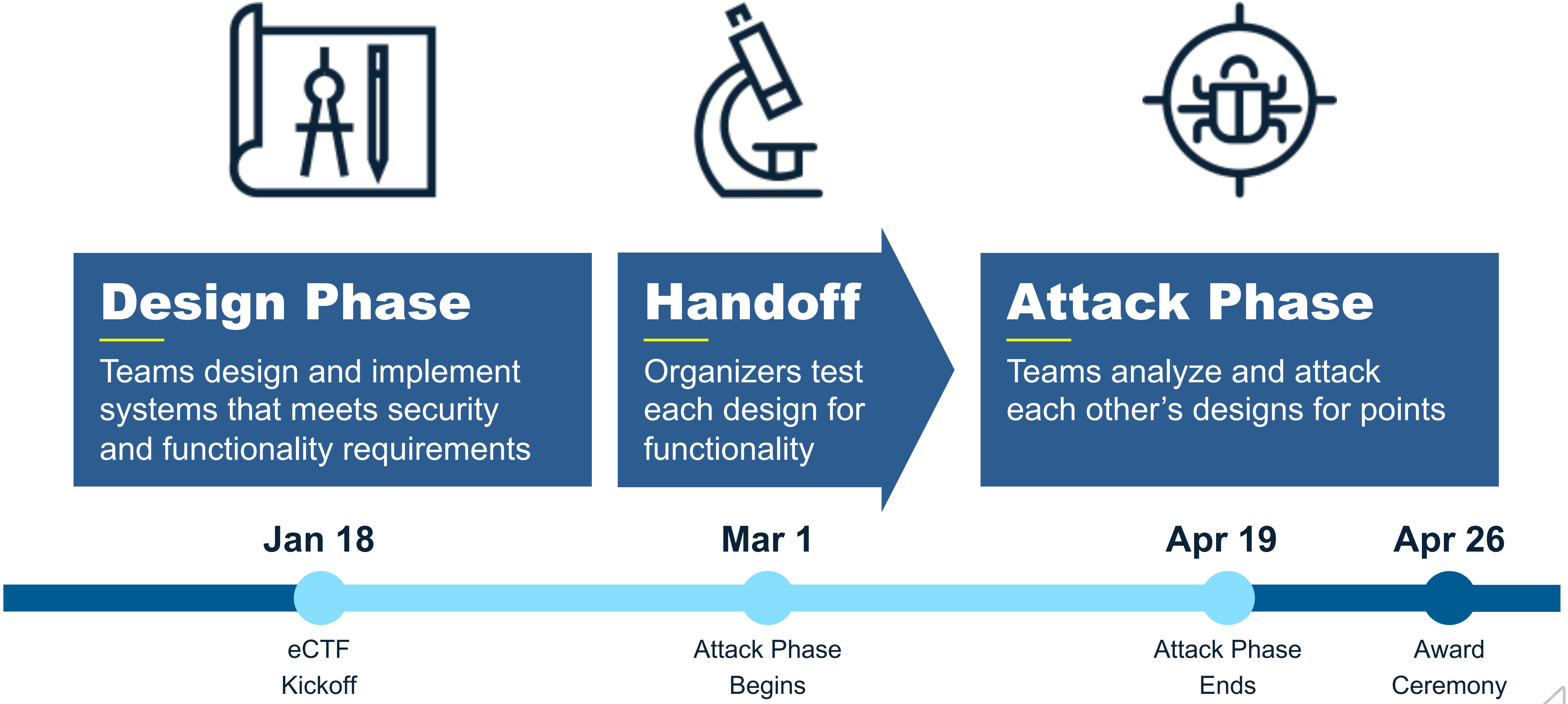
Attack and Defend

Students wear both “hats” by acting as both red team and blue team

Extended Time

Semester-long competition opens door to advanced attacks and countermeasures

Competition **Phases**



Design Phase

Teams design and implement systems that meets security and functionality requirements

Handoff

Organizers test each design for functionality

Attack Phase

Teams analyze and attack each other's designs for points

Jan 18
eCTF
Kickoff

Mar 1
Attack Phase
Begins

Apr 19
Attack Phase
Ends

Apr 26
Award
Ceremony

What Teams are Given

Functional Requirements

Security Requirements

Hardware

Example Code
(Reference Design)

Automated Testing

Organizer Support

Prizes and Competition Qualification Requirements

- **This year the eCTF will award up to $5000 in prizes to the winning teams**
  - 1st Place: $2000
  - 2nd Place: $1000
  - 3rd Place: $500
  - Additional Awards: Up to $1500 (may be split among multiple teams)

- **To receive prize money, you must meet certain eligibility requirements**
  - Check our website (ectf.mitre.org) for award eligibility terms

Competition Rules

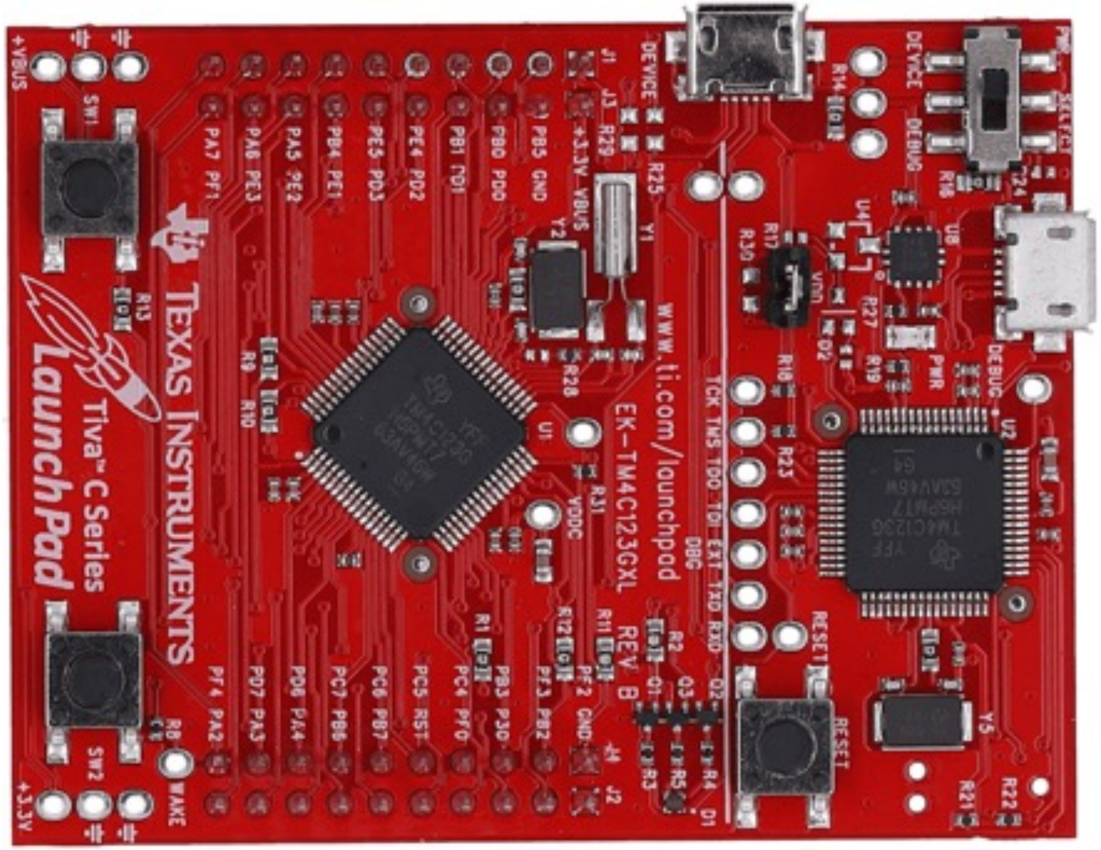
- **Several policies and processes have been put in place to ensure fairness**
  - All questions and requests for help are taken on a first-come-first-serve basis
  - Write-ups are anonymized before judging
  - Competition organizers will not discuss the eCTF with participants outside of official channels

Outline

1. Welcome
2. Competition Overview
3. **Challenge Overview**
4. Requirements
5. Flags
6. Attacker Resources
7. Getting Started

Platform

- Texas Instruments TM4C123GXL Evaluation Kit
  - 80 MHz 32-bit Arm Cortex-M4F CPU
  - 256KB Flash
  - 32KB SRAM
  - 2KB EEPROM
  - UART, SPI, I2C, CAN
  - Programmable RGB LED
  - 2 programmable user buttons
  - https://www.ti.com/tool/EK-TM4C123GXL

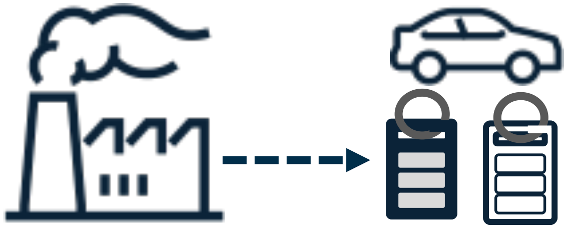


Challenge

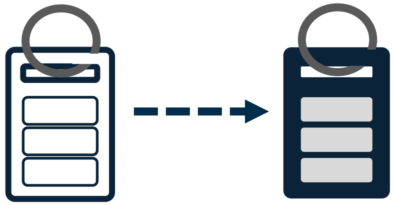
- Your team is tasked with designing and implementing secure firmware for a key fob and a car
  - Protected Automotive Remote Entry Device, or PARED
- Your system must protect against an adversary with physical access to the devices
- Deliverables
  - Car firmware for a Texas Instruments Tiva C microcontroller
  - Fob firmware for a Texas Instruments Tiva C microcontroller
  - Software tools for interacting with and controlling the devices

Functional Overview

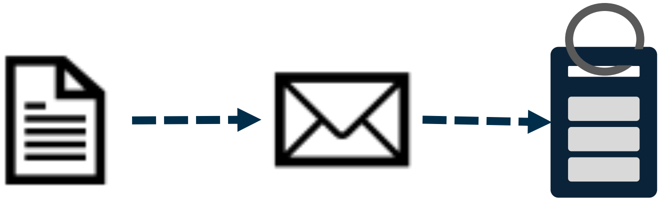
1. **Build System**
   - Build cars and fobs



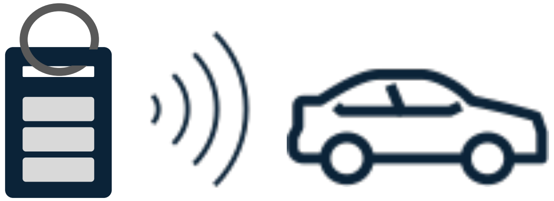
2. **Pair Fob**
   - Pair an unpaired fob with a car



3. **Package and Enable Feature**
   - Enable a new optional feature on a fob

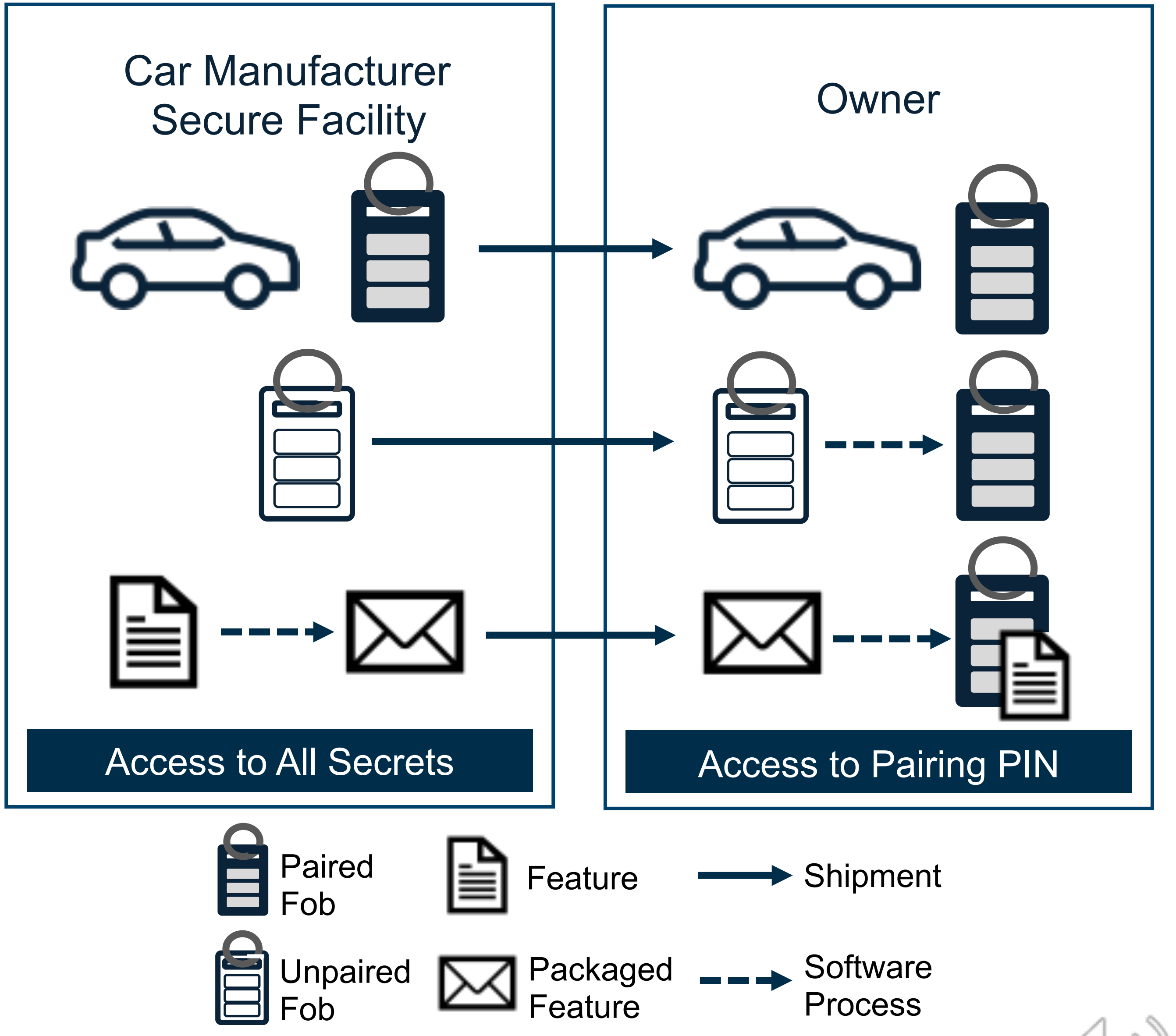


4. **Unlock Car**
   - Use a fob to unlock a car



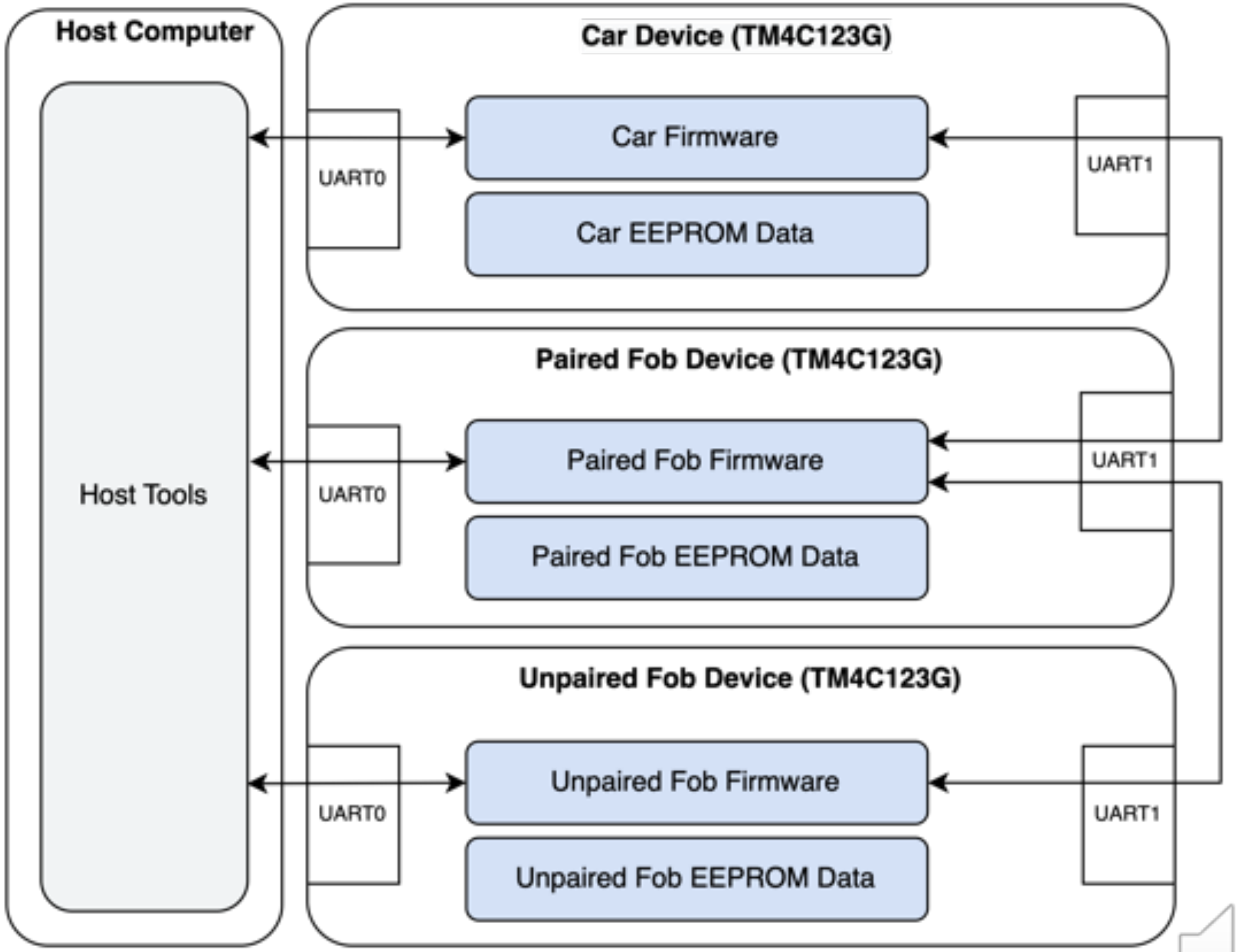
Example Scenario

- Car manufacturer builds cars and fobs in a secure facility
- The owner receives their car with a paired fob and the pairing PIN
- The owner can buy new unpaired fobs from the dealer and pair them using the pairing PIN and their other paired fob
- Paired fobs can enable different features on the car
- Features are packaged at the dealership and sent to the owner to enable them on their fob



System Overview

- **The system has four main components**
  - Host Computer
  - Car Device
  - Paired Fob Device
  - Unpaired Fob Device

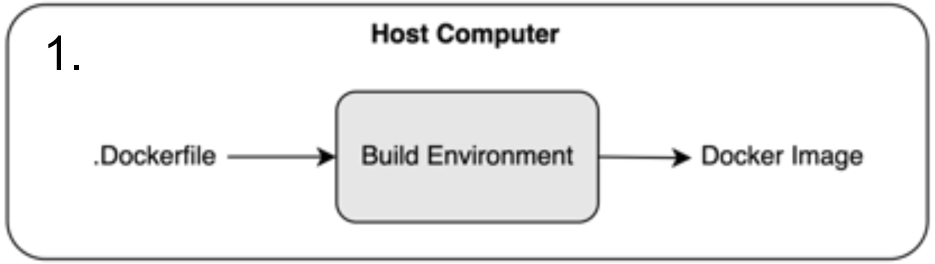


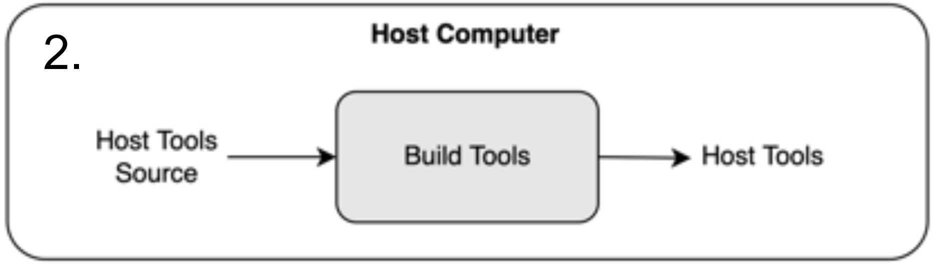
Outline

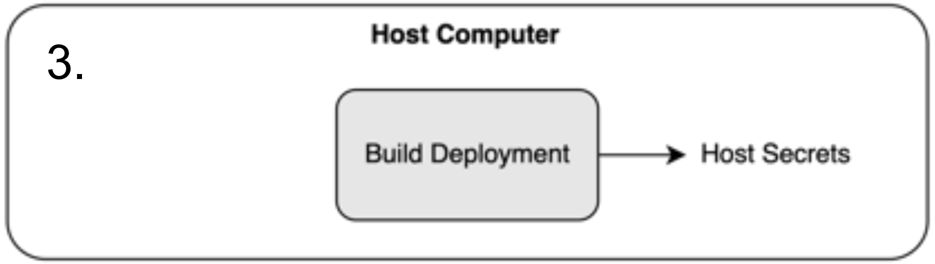
1. Welcome
2. Competition Overview
3. Challenge Overview
4. **Requirements**
5. Flags
6. Attacker Resources
7. Getting Started

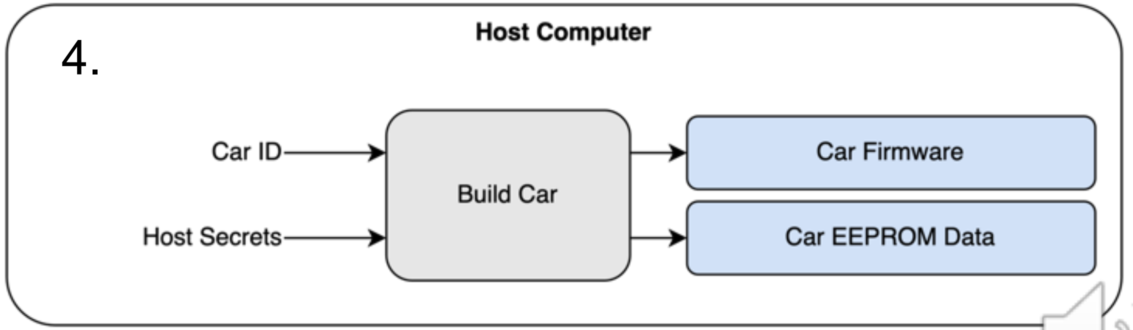
Build Requirements

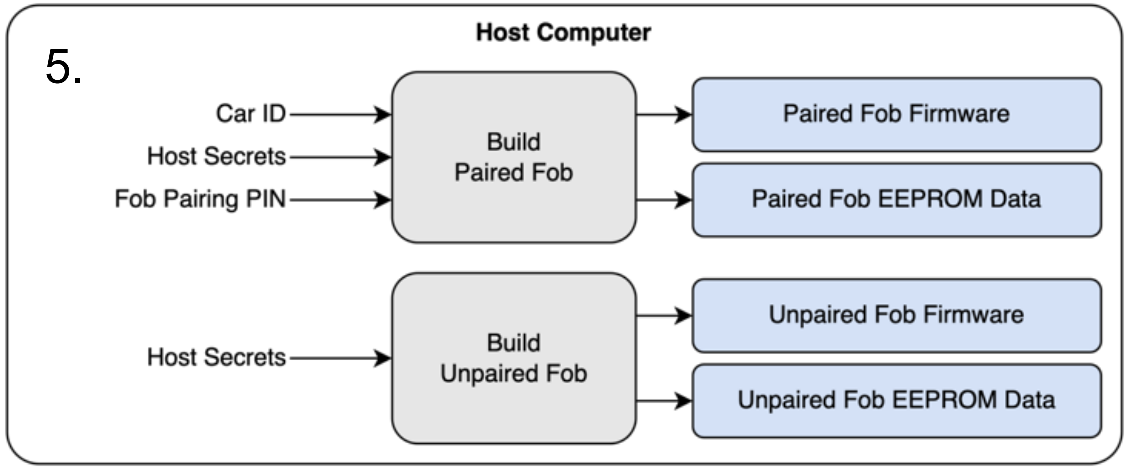
1. Build runtime environment
2. Create a host tool package
3. Generate system secrets
4. Compile the car
5. Compile the fobs (paired and unpaired)





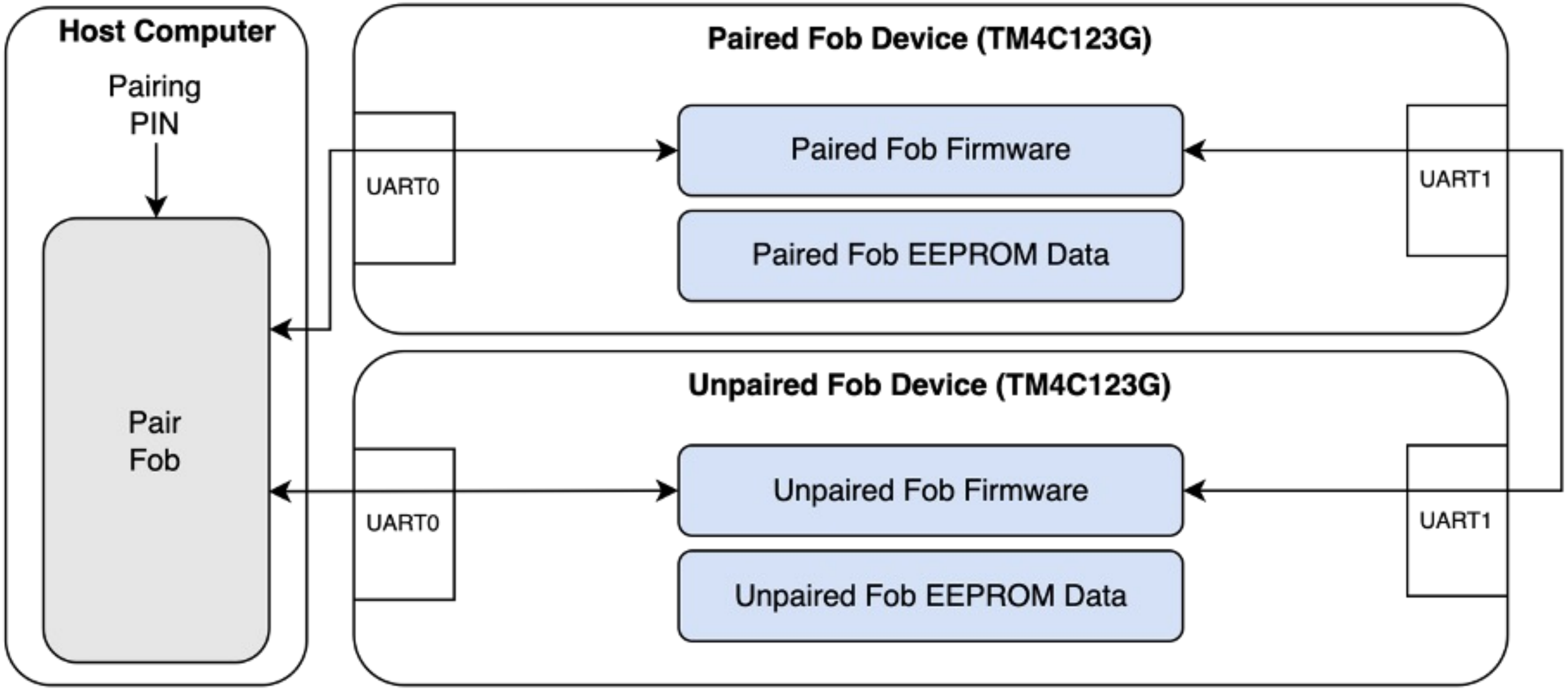






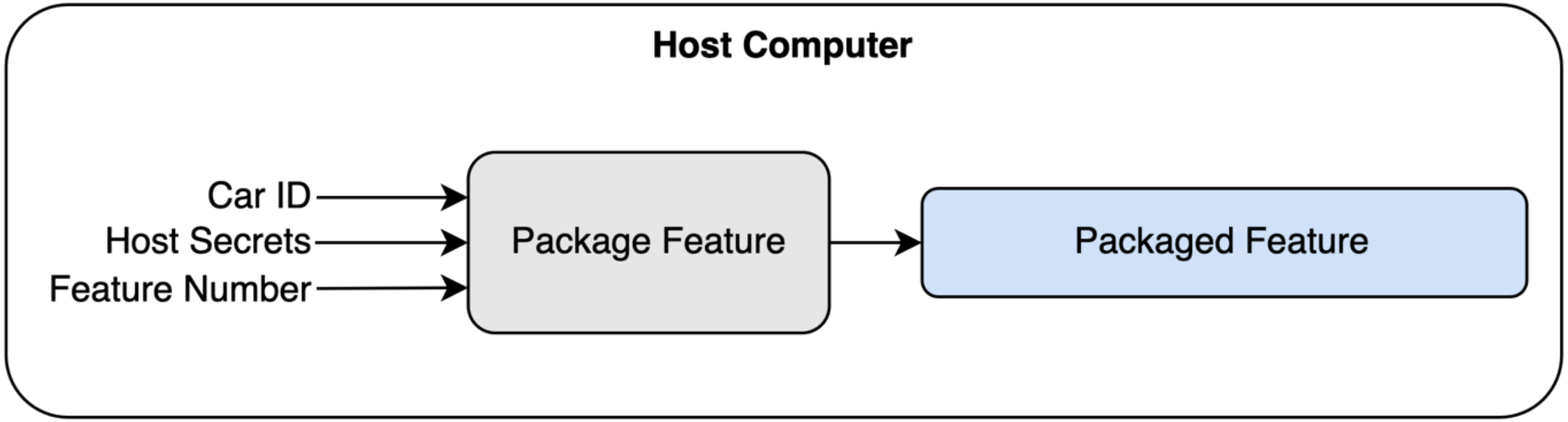
Pair Fob (Host Tool) Requirements

- Pair an unpaired fob with a pairing PIN and a paired fob.



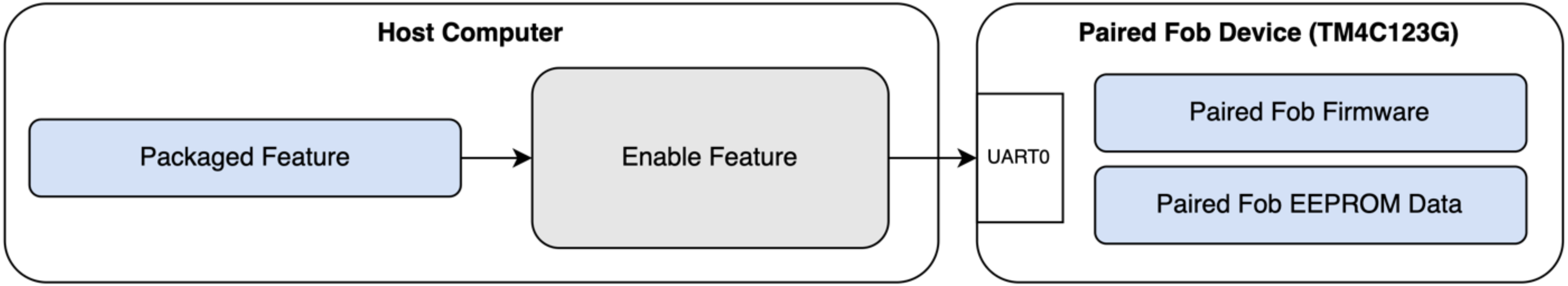
Package Feature (Host Tool) Requirements

- Create a packaged feature as a binary file given a car ID number and a feature number. This file will later be used to enable the feature on a fob.
- Has access to the host secrets



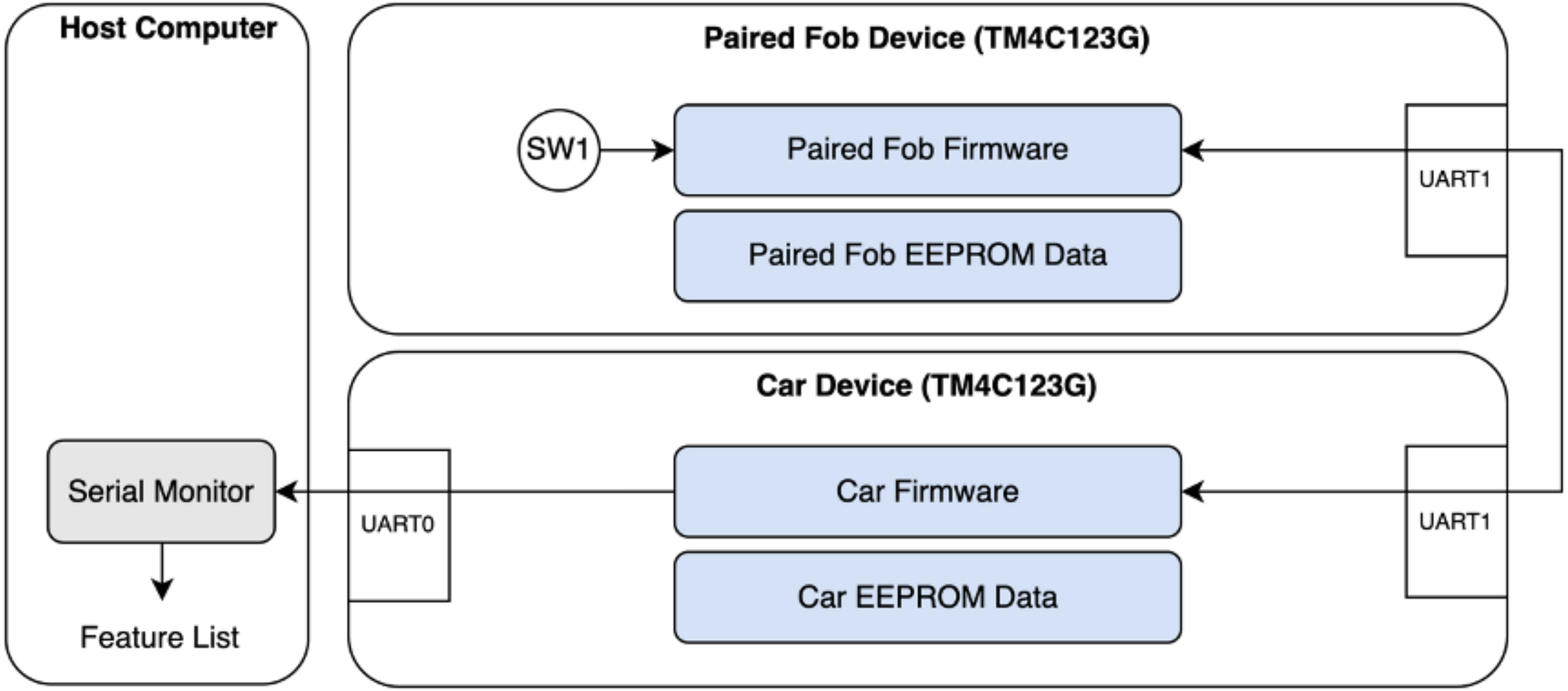
Enable Feature (Host Tool) Requirements

- Send a packaged feature to the paired fob device
- Once the paired fob has the feature enabled, the car should recognize it when that fob is later used to unlock the car.



Unlock Car Requirements

- A paired fob must unlock the car when pressing the SW1 button on the paired fob device. The fob can communicate with the car over the UART1 connection.



Security Goals

1. A car should only unlock and start when the user has an authentic fob that is paired with the car
2. Revoking an attacker’s physical access to a fob should also revoke their ability to unlock the associated car
3. Observing the communications between a fob and a car while unlocking should not allow an attacker to unlock the car in the future
4. Having an unpaired fob should not allow an attacker to unlock a car without a corresponding paired fob and pairing PIN
5. A car owner should not be able to add new features to a fob that did not get packaged by the manufacturer
6. Access to a feature packaged for one car should not allow an attacker to enable the same feature on another car

Outline

1. Welcome
2. Competition Overview
3. Challenge Overview
4. Requirements
5. **Flags**
6. Attacker Resources
7. Getting Started

Design Phase Flags

DEADLINE	MILESTONE	DESCRIPTION
Jan 25	Read Rules	If you read all the rules, you'll know
Feb 1	Boot Reference Design	Provision and boot the example design to receive a flag
Feb 3	Design Document	Submit an initial design document containing high-level descriptions of how each host tool and system function will work and how the security requirements are addressed.
Feb 8	Submit Reference Design for Testing	Submit the reference design for testing. Learning how to use the testing infrastructure can help you validate your design continues to meet functional requirements as you develop security features.
Mar 1 – Apr 19	Final Design Submission	The Attack Phase opens on March 1. Teams should submit their completed design for testing before or on March 1 to enter the attack phase on time.
Rolling	Bug Bounty	Submit fixes to functional errors in the tools and example design.

Attack Phase Flags

FLAG	DESCRIPTION
New Car Unlock	Unlock a new car you don’t have the fob for
Temporary Fob Access	Unlock a car you previously had the fob for
Passive Unlock	Unlock a car you intercepted an unlock transaction for
Leaked Pairing PIN	Unlock a car you have the pairing PIN for
PIN Extract	Extract the programming pin
Enable Feature	Enable a feature you have had access to on a different car

Outline

1. Welcome
2. Competition Overview
3. Challenge Overview
4. Requirements
5. Flags
6. **Attacker Resources**
7. Getting Started

Provisioning Your PARED System for Attacking Teams

- During the Attack Phase, teams will have access to six different cars
- Each car is provisioned with different flags you are trying to capture
- Building the environment, host tools, deployment, and unpaired fob will happen only once
- After this point, each car and its paired fob will be built in sequence
- Features will be packaged for each of the cars
- After provisioning, the attackers will have access to different components depending on what flag they are trying to capture/what car they are attacking
- **The Rules Document contains more detailed information on the exact list of resources available for each system**

Attacker Resources

✓ = Full Access

✔ = Temporary Access

	Car	Paired Fob	Unpaired Fob	Logic Analyzer Capture of Unlock	Pairing PIN	Packaged Feature 1	Packaged Feature 2
Car 0 Your Car (No Flags)	✓	✓	✓		✓	✓	✓
Car 1 New Car	✓		✓			✓	✓
Car 2 Temporary Fob Access	✓	✔	✓			✓	✓
Car 3 Passive Unlock	✓		✓	✓		✓	✓
Car 4 Leaked Pairing PIN	✓		✓		✓	✓	✓
Car 5 PIN Extraction, Enable Feature	✓	✓	✓			✓	

MITRE

Additional Resources

- Attacking teams always have access to…
  - All source code (with the .git directory removed)
  - The most recent documentation for the target system
  - Your team’s host tools
  - Available car ID numbers
  - Available feature numbers

Outline

1. Welcome
2. Competition Overview
3. Challenge Overview
4. Requirements
5. Flags
6. Attacker Resources
7. **Getting Started**

Words of Advice

- **Start development early**
- **Verify functionality as you go and learn how to use a debugger**
- **Always think like an attacker**
- **Understand what attackers have access to**
- **Don’t go overboard with countermeasures**
- **Use Slack for help**
  - # tech-support for most questions
  - # ask-the-organizers Slackbot app for design-sensitive questions

Next Steps

- **Get on Slack**
- **Meet with your team**
  - Schedule meetings
  - Discover everyone’s interests and skills
- **Read the challenge rules**
  - Develop your understanding of all functional and security requirements
  - Consider potential attacks on each flag
- **Set up your development environment**
- **Get the reference design running**
- **Plan your design and development timeline**
  - 6 weeks until the handoff
  - Make sure to hold yourselves to milestones and goals

MITRE

Awards Ceremony

April 26, 2023

Mark Your Calendars!

Thank You Sponsors

PLATINUM

ANALOG DEVICES

FORTINET

CROWDSTRIKE

GOLD

BCI

BRONZE

Rambus

MITRE ENGENUITY

A Foundation for Public Good