UCI University of California, Irvine

MITRE eCTF 2023-24

Common Vulnerabilities

Jinyao Xu (jinyaox@uci.edu)

NOI Competition (Entry Level Q1)

We have a total N dollars of funding. The ECTF team wants to purchase 3 items.

- In and out burger combo: 7 dollars because it's my favorite

- *Concept of Programming Language :*3 dollars because it's a shitty book

- TIVA C TM4C123gh6PM : 5 dollars

GOAL:

1. 7a+3b+5c=n
2. IF 1 ==> Buy as many combo as possible
3. IF 2 ==> maximize a+b+c

Approach: Give a set of solutions, can we find the best one?

Why Firmware Fails

1. Bad Programming (Root of all issues).
2. Predictable Nonce Generation
3. Buffer Overflow (more technical, perhaps the hardest one)
4. And More… Let's see UNHaven's Report Findings

Plain text = P

Encrypted text = C

Jet: $[k_{p_1}, k_{p_2}, k_{p_3}]$

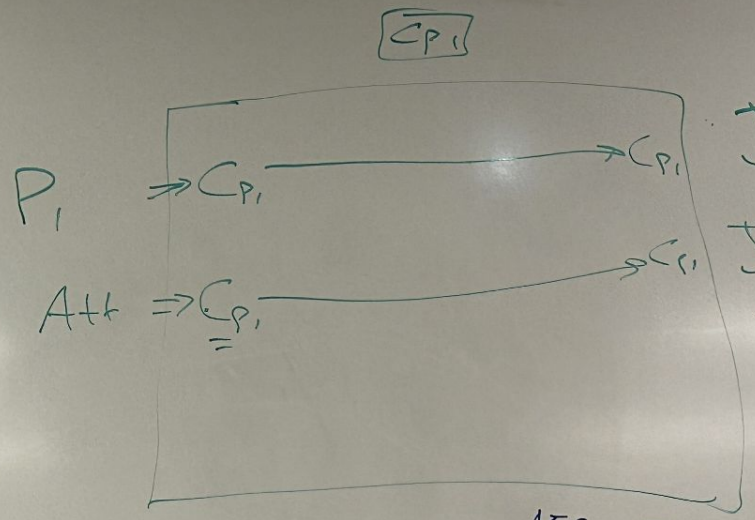
$P_1 : k_{p_1}$

$P_2 : k_{p_2}$

$P_3 : k_{p_3}$

$E(P \cdot k_{p_1} \cdot N) = C_{p_1}$

$D(C \cdot k_{p_1}) = P_{p_1}$



AES: 2 ms.

1. Goal 1 : Ciphertext indistinguishability.

CSV file.

- py. load procs.
- py. generate nonce.
- py. validate
- py. send out.

Interval: 0.1 sec.

100 ms.

JET

Pilot

- EEPROM STORE info. AES private key
- [Recieve Encrypt Send.] = Button push

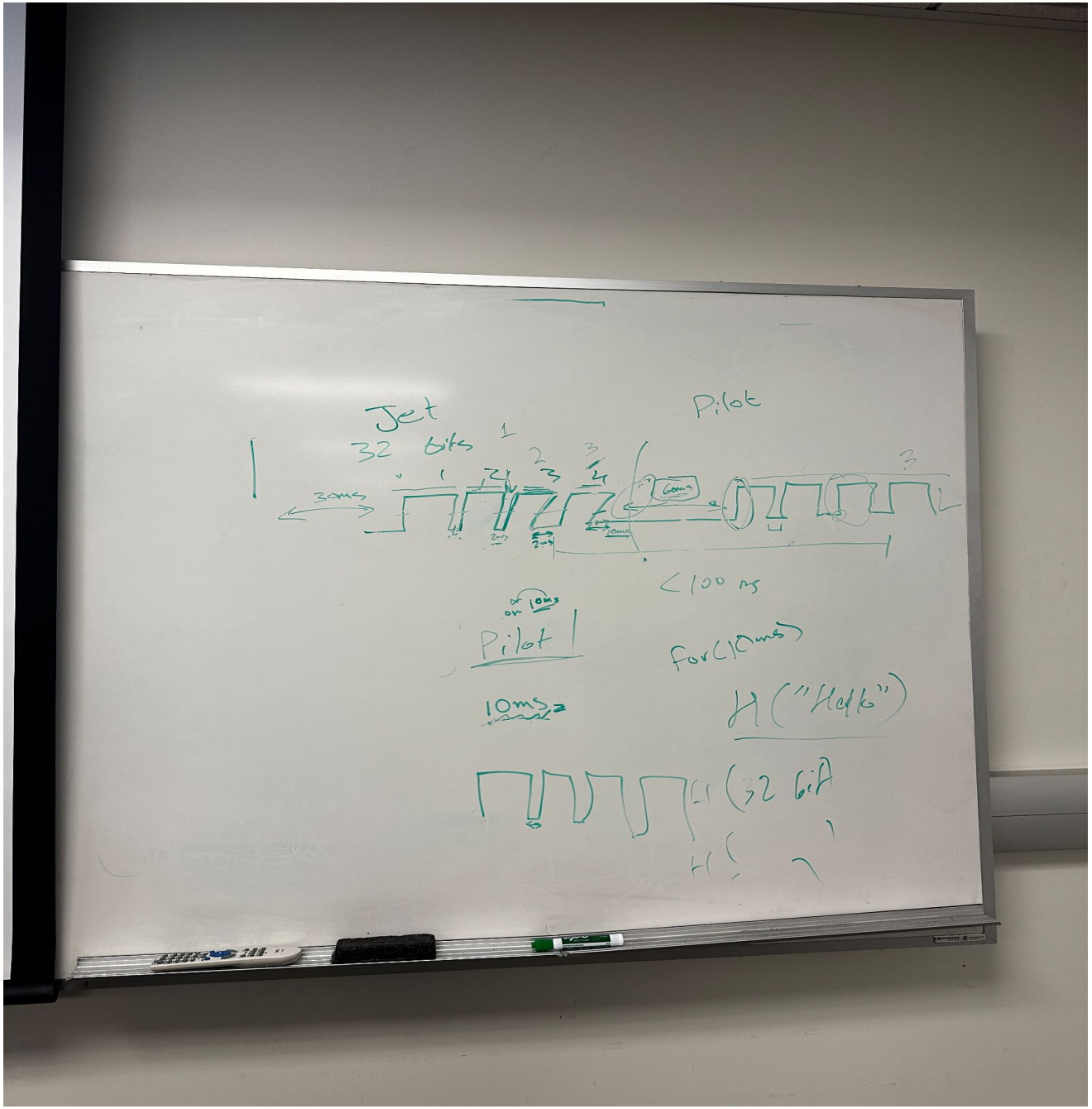
K_{P1} → 3 →

← C_{P1}

$D_{K1}(C_{P1}) = 3$

K_{P1} UART Rx AES Lib UART Tx

$E_{K1}(3) = C_{P1}$


Jet
32 bits
Pilot
30ms
< 100 ms
Pilot
10ms
for 10ms
H("Hello")