Columbia University

Isabelle Friedfeld-Gebaide, Dan Ivanovich,
Andreas D. Kellas, and Emily Soto

Week 1

All White Party

```
/**********************************************************************/
Challenge: All White Party
/**********************************************************************/
Welcome!! Based on our records, your account has been located.
Enter account username (over serial):
10-digit MFA code sent to your phone. Enter 10-digit Pin on Keypad.
6666666666
Password SHA does not match:
32 117 74 65 206 Please try again
Welcome!! Based on our records, your account has been located.
Enter account username (over serial):
```

Our Challenges

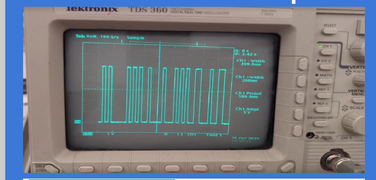
- Does the device vibrate longer?
- Does the device delay longer before vibrating?
- How to measure the vibration delay after sending message over serial?
- What 10 digit password produces the SHA received over serial connection

Our Approach

- Overview: Time side channel attack to leak the expected username (unable to get PIN)
- Sent letters and characters representing username over serial connection
  - Haptic sensor would vibrate after processing incorrect username
- Measured the signal from Arduino to haptic sensor, using an oscilloscope.
  - Originally measured the length the time the signal stayed high
  - Measured the *relative* vibration delay by controlling the time between each guess attempt.
  - Every correct letter in the username adds 300ms of delay before the device vibrates.
- Correct username was “Barry”
- Tried to brute force password by matching the hash of 10 digit number sequences and checking if first 5 bytes matches the hash received

Week 2

Operation SPItFire




```
10100101 00000101 01001000 01000101
01001100 01001100 01001111 00111001

a5 05 48 45 4c 4c 4f 39
      H  E  L  L  O
Header                    =CRC-8(a50548454c4c4f)

a5 05 46 4c 41 47 00 21
      F  L  A  G [NULL]
Same Header               =CRC-8(a505464c414700)
```

```
/**********************************************************************/
Challenge: SPI
/**********************************************************************/
Recieving message "HELLO"...
Please send the message "FLAG" in hex (over serial):
Sending your message...:
70 76 65 71

Recieving Flag...


/******************  YOU BEAT THE CHALLENGE!!!  ******************/
Well, almost... Decode the flag and put it in your report
/******************          Congrats!!!          ******************/
```

Our Solution

- Received messages in SPI Protocol format through measuring the relay’s voltage
  - Measures signals from relay using an oscilloscope
  - 8, 8-bit registers in sequence, 200 ms/bit
- Reverse engineered the structure of the SPI messages to achieve communication
  - First two bytes: header `a5 05`
  - Next five bytes: payload, must be 5 bytes
  - Last byte: CRC-8, calculated on first 7 bytes
- Sent messages over serial connection in hex:
  - Sent `a5 05 46 4c 41 47 00 21` over serial connection
- Received and decoded the 11 byte flag in SPI Protocol format
  - SPyBURNdy

Week 3

Sock and Roll

Our Challenges

- What audio to should be played back to microphone?
- Can a voltage pattern created using a function generator be sent directly to the microphone analog pin?
- Does the changing amount of periods in the received messages from the serial connection impacted when/which tones to play?
- What is the significance of the Lost TV show reference?

Our Approach

- Speaker output a repeated sequence of 1000 Hz tones
- Only other component receiving power was the microphone
- Over the serial connection received a message that when translated from French means: “He is outside. Please help us. Please help us.”
  - Message and iteration number is a reference to the TV show Lost
- When disconnecting the speaker or playing a loud tone of a different frequency received an error message

```
/**********************************************************************/
Challenge: Sock and Roll
/**********************************************************************/

Iteration 17294533: Il est dehors. Veuillez nous aider. Veuillez nous aider.... Glad to know things are OK. Enjoy your time at the factory!

Iteration 17294534: Il est dehors. Veuillez nous aider. Veuillez nous aider.... Glad to know things are OK. Enjoy your time at the factory!

Iteration 17294535: Il est dehors. Veuillez nous aider. Veuillez nous aider... Unable to dicipher message. Sorry, better luck next time!

Iteration 17294536: Il est dehors. Veuillez nous aider. Veuillez nous aider.. Glad to know things are OK. Enjoy your time at the factory!

Iteration 17294537: Il est dehors. Veuillez nous aider. Veuillez nous aider. Glad to know things are OK. Enjoy your time at the factory!

Iteration 17294538: Il est dehors. Veuillez nous aider. Veuillez nous aider.... Unable to dicipher message. Sorry, better luck next time!
```

Bluebox

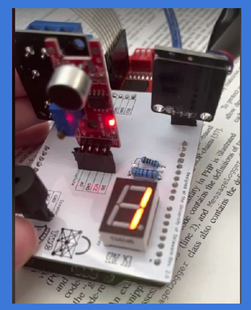
TABLE I
KEYPAD MAPPING TO FREQUENCY OF TONE GENERATED

Keypad	Hertz
1	953
2	1010
3	1067
A	1129
4	1180
5	1248
6	1307
B	1364
7	1426
8	1480
9	1543
C	1600
*	1664
0	1722
D	1838

Our Solution

- Arduino played a sequence of 4 notes
- Pressing buttons on the keypad resulted in the in a note being played
  - Each key played a different note, and the note seemed to be the same on every keypress
- We used a guitar tuner app to record the frequency of the tone played when pressing each of the 16 keys
- We let the board play its notes with the guitar tuning app open, recording its screen, then pressed the corresponding keys in the same order
- After the 4-tone sequence, we got a 8-tone sequence and repeated the process
  - The 8-tone sequence corresponded to the flag
    - B339B009

czNxdTNuYzM

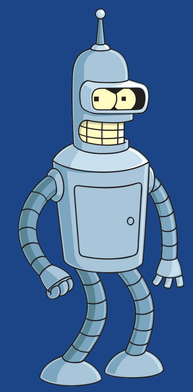


$$a(n+1) = \begin{cases} \dfrac{a(n)}{n} & \text{if } n \mid a(n) \\ a(n) * n & \text{else} \end{cases}$$

Our Solution

- The challenge name decodes from base64 to “s3qu3nc3,” a useful hint
- The 7-segment display flashed, seemingly randomly:
  - We found that playing a high-frequency note (we played a 1974 Hz B6) would slow down the 7-segment display, which output a series of numbers, underscores, and periods
  - By treating underscore-separated numbers as the digits of larger numbers, we got a sequence of 23 integers
- We are prompted over serial, “what comes next?”
  - Their sequence is a(n+1) = a(n)/n if n|a(n) else a(n)*n, starting at a(1) = 1
- The next item in the sequence is the flag
  - 97349616

Vender Bender



Our Solution

- Fault injection attack on a mock vending machine
- Measured the mock motor movement with an oscilloscope
  - When voltage measured high mock motor was moving in vending machine
- Sending an “ERR” message over serial connection injects faults into the mock motor
- Jamming the motor 5 times causes the Flag to be printed
  - mMmCaNdY

```
Motor movement SUCCESS. Snack was dispensed for $2. Insert another credit for a new snack.
After credit is reciever, send "ERR" to jam the motors.
Motor Error 5902 Reported. Slight but not signifigant motor movement detected. Retry Attempt 1/5
Motor Error 5902 Reported. Slight but not signifigant motor movement detected. Retry Attempt 2/5
Motor Error 5902 Reported. Slight but not signifigant motor movement detected. Retry Attempt 3/5
Motor Error 5902 Reported. Slight but not signifigant motor movement detected. Retry Attempt 4/5
Motor Error 5902 Reported. Slight but not signifigant motor movement detected. Retry Attempt 5/5


/******************  YOU BEAT THE CHALLENGE!!!  ******************/
Place the following flag in your report
mMmCaNdY
/******************          Congrats!!!          ******************/
```