Gig ‘Em Bytes
Texas A&M University

Andrew Chin

Justin Metzinger

Jonathan Saenz

Advised by Dr. Martin Carlisle

Outline

- Design Phase
  - Overview
  - What would we do differently?
- Attack Phase
- General Comments
- Closing Remarks

Design Phase: Overview

- Confidentiality of songs
  - Speck Cipher - CBC Mode
- Integrity & authentication
  - Secret keys – one for metadata, one for song chunks
  - Keyed Blake3 hashes of song chunks
- PINS
  - Use username as salt and hash PINs with Blake3

Design Phase: Overview

- Metadata Hash = IV + DRM Metadata
- Audio Chunk Hash = audio chunk + IV
  - Including the IV prevents swapping audio blocks

Design Phase: What Would We Do Differently?

- Start implementing EARLY
- Make a detailed design document – non-technical details are just as important as the technical details
- Adopt better code review process (which should involve testing attacks on our design!!!)
  - Would have easily found critical bug that led to easy Region Lock/Unauthorized Play captures

Attack Phase

- From the rules: “music that fails integrity or authentication checks should not be played”
- Erroring out midway through a song is a valid Music Tamper capture!
- 3 out of the 6 teams in the attack phase verified song chunks **on-the-fly** with no pre-checks

General Comments

- What design elements made things difficult for you as an attacker?
  - Teams correctly utilized secure memory for sensitive operations
  - Strong integrity & authentication checks on song headers

General Comments

- What are two pieces of advice that you would give to future eCTF participants?

1. Cannot stress enough: start planning your design early! Things will change and you want to have ample time attack other teams' designs

2. Test your design for functionality and security

General Comments

- What would you do differently if you had to participate in this same competition again?
  - Change our recruiting process
  - Again: start earlier!
  - Thoroughly document design

Closing Remarks

- For our first eCTF, this was a grueling competition, esp. since there were only 3 of us
- However, we learned an incredible amount through our participation and getting to see other teams' great designs!
- We're incredibly excited to come back stronger next year!

Questions?