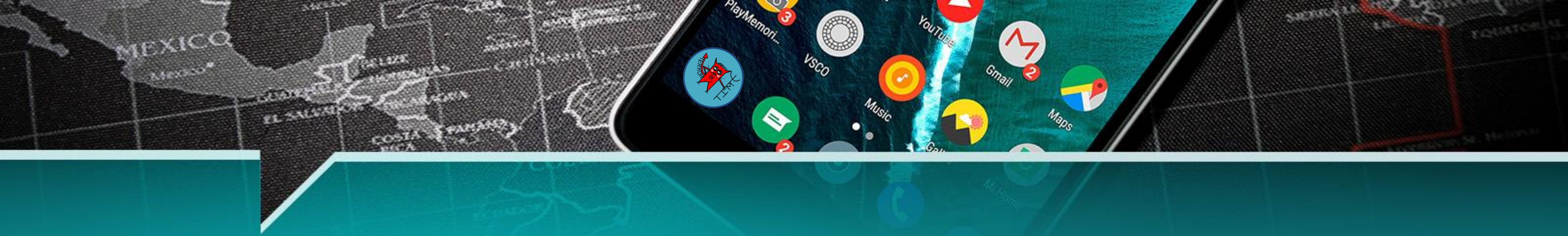
NSA's Codebreaker Challenge

Fall 2019



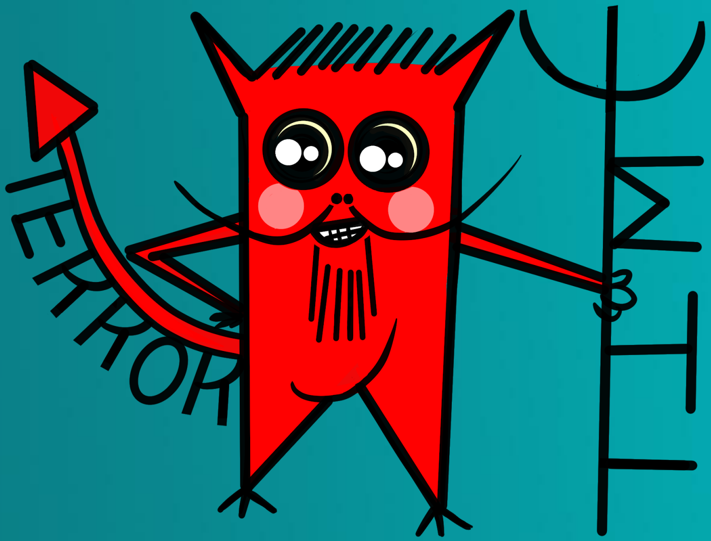
Agenda

- Introduction
- Tasks
- Technical Background

What is the Codebreaker Challenge?

- Annual Cyber Challenge Event
- Nationwide
- 2018 Top-Finishers
    1. Oregon State
    2. Georgia Institute of Technology
    3. University of North Georgia
    4. New Mexico Institute of Mining & Technology
    5. University of Tulsa

2019 Scenario



* custom Android secure messaging app

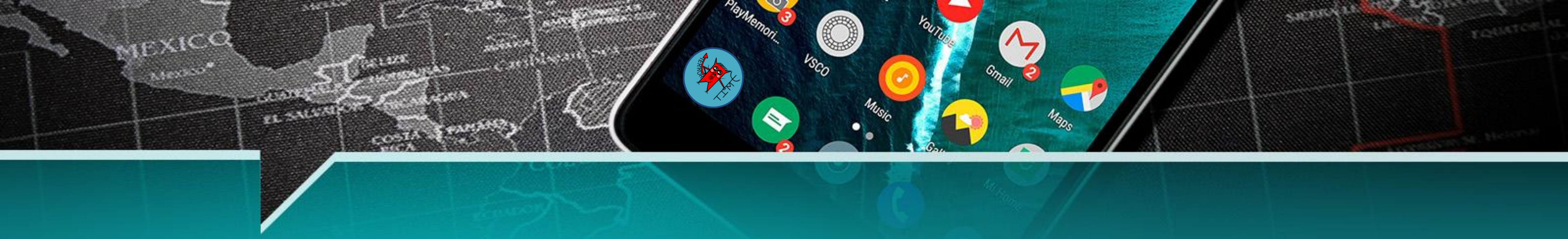
Mission

- Reverse engineer and develop new exploitation capabilities against TerrorTime to enable:
  - **Message spoofing**
  - **User masquerades**
  - **Message decryption**

- Discover and thwart future attack plans!

Key Skills

1. Network Traffic Analysis
2. Android App Analysis
3. Cryptanalysis
4. Binary Reverse Engineering
5. Vulnerability Analysis
6. Exploitation Development



Agenda

- Introduction
- Tasks
- Technical Background

To Break the Code

1: **Extract** a copy of TerrorTime APK from network traffic

2: **Analyze** APK for app permissions and certificate information

3: **Investigate** SQLite database from captured device to discover the server addresses

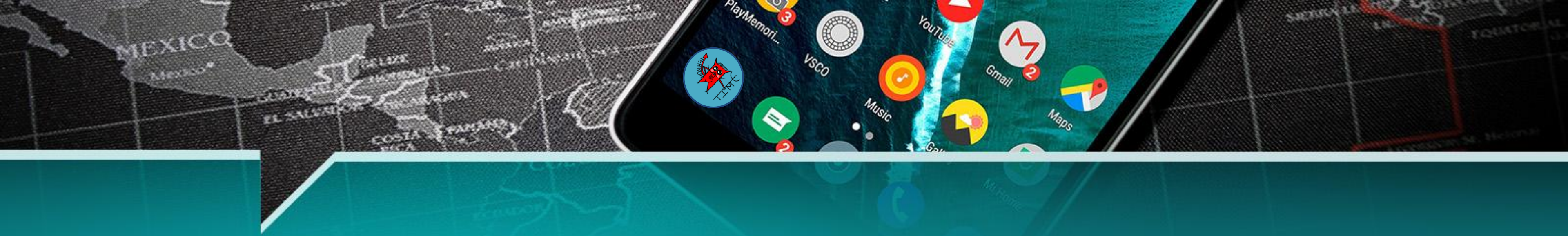
4: **Recover** user credentials and attack plans

To Break the Code (continued)

5: **Develop** exploit to masquerade into TerrorTime as another user

6: **Develop** exploit to enable message spoofing

7: **Reverse** engineer encryption scheme and develop exploit to decrypt conversations



Agenda

- Introduction
- Tasks
- Technical Background

Network Traffic Analysis

- Recommended tools: **Wireshark**, **Burp Suite**
- Cross platform, parsers for many protocols
- Features/Functionality:
    - Display filters to focus in on traffic
    - TCP stream following
    - Extract files from packet payloads
    - Dissect custom payloads
    - Traffic statistics/characterization
- Traffic interception / manipulation
- https://www.wireshark.org and https://portswigger.net/burp

Binary Reverse Engineering

Ghidra	IDA Pro	Binary Ninja

Binary Reverse Engineering

- General tips
  - Examine strings
  - Look for clues
  - Leverage xrefs to find relevant code
- Utilize symbols (function names, etc.)
- Online resources
  - Intel manuals, RE Lectures, tutorials

Ghidra Resources

https://ghidra-sre.org

Ghidra SRE Cheat Sheet

GHIDRA

Android Applications

- Android package (APK) file
- https://developer.android.com/
- Emulator setup steps
  - ○ Resources Page

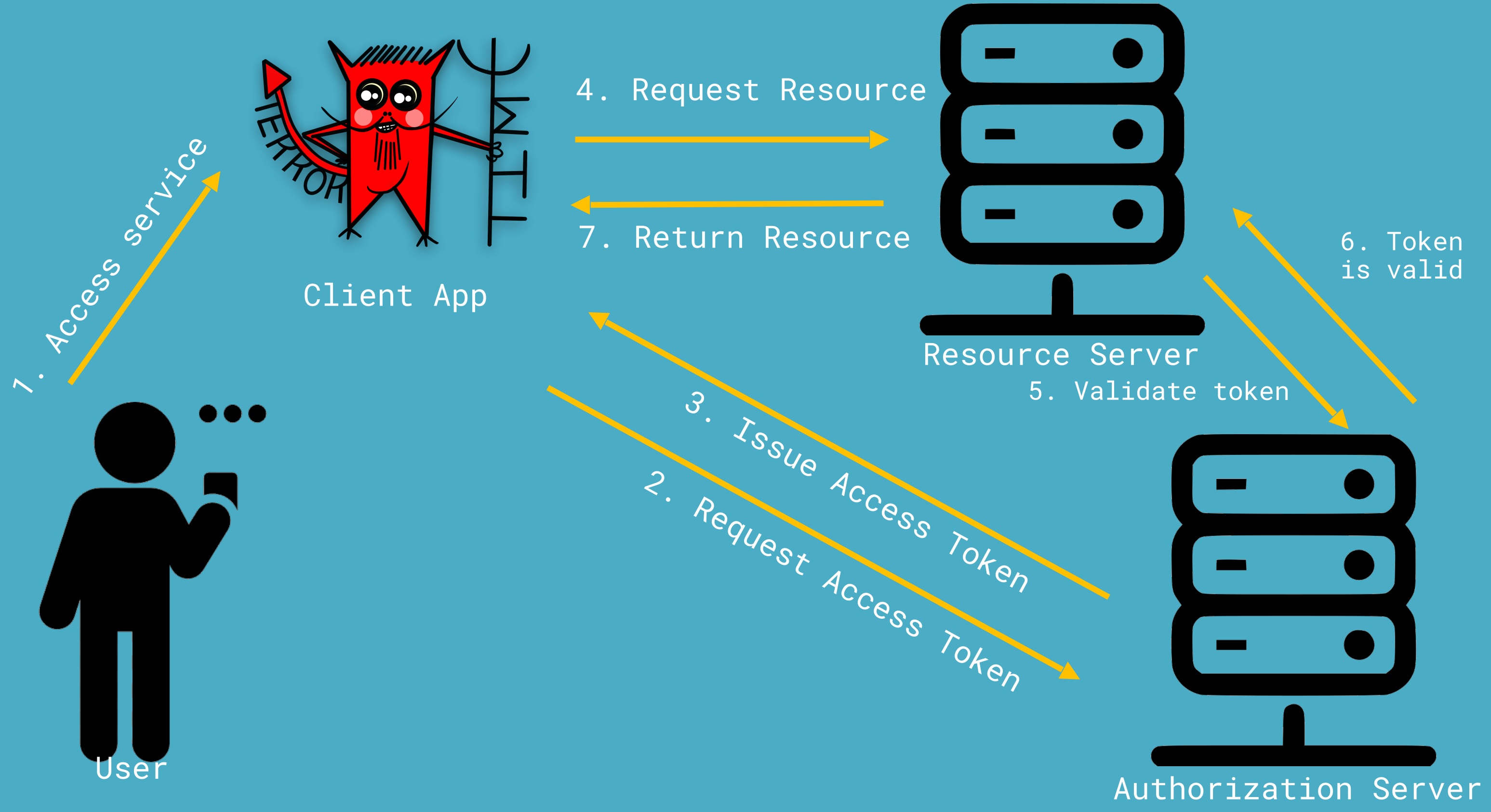
Android App Analysis

Android Studio	Visual Studio Emulator
Ghidra	JEB

OAUTH

- Grant 3rd Party Access to Data
- Requires TLS (https)
- Roles:
  - User
  - Client
  - Servers - Resource and Authorization

OAUTH Protocol Diagram



1. Access service

Client App

4. Request Resource

7. Return Resource

Resource Server

5. Validate token

6. Token is valid

3. Issue Access Token

2. Request Access Token

User

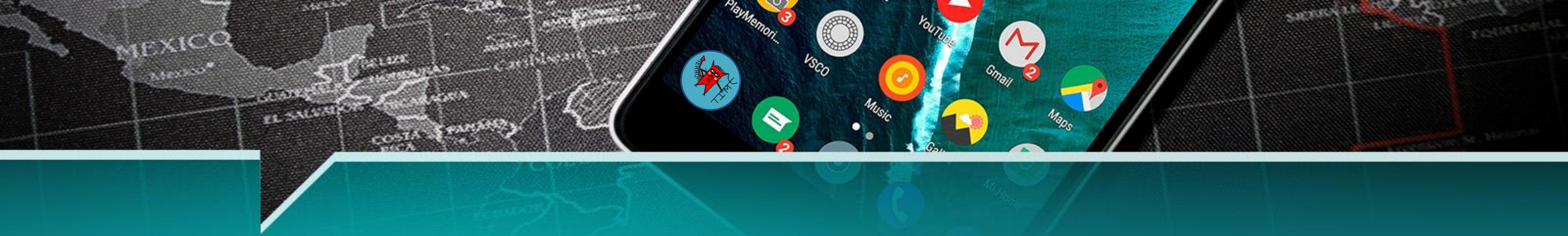
Authorization Server

To Get Started

1. https://codebreaker.ltsnet.net

2. **.edu** email address

3. Learn and have fun!



Questions?

codebreaker@nsa.gov

2018
Codebreaker Challenge Walkthrough

Special thanks to **Jonathan Armer** for sharing his detailed write up at

https://armerj.github.io/CodeBreaker-2018-Overview/