Detecting (Absent) App-to-app Authentication on Cross-device Short-distance Channels

Stefano Cristalli, Danilo Bruschi, Long Lu, Andrea Lanzi

December 13, 2019

University of Milan Italy Northeastern University Boston US

Outline

1. Introduction
2. Cross Device Authentication Scheme
3. Approach Overview
4. Technical Details
5. Experimental Evaluation
6. Case Studies
7. Discussion
8. Conclusion & Future works

Introduction

Context

- Cross-device communications allow nearby devices to directly communicate bypassing cellular base stations (BSs) or access points (APs) (e.g. **spectral efficiency improvement, energy saving, and delay reduction**, etc.)
- Without the need for infrastructure, **such a technology enables mobile users (e.g., Android) to instantly share information (e.g., pictures and videos)**
- Such technology is also predominat in **IoT environment** where a mobile device is direct connected to the embedded system.

Current Solutions

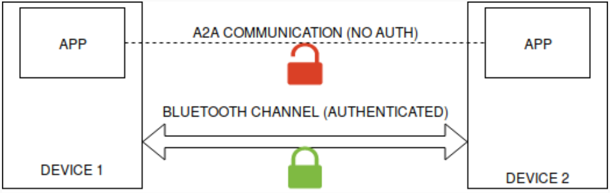
- Several solutions exist for securing cross-device communication. In the Android environment, they allow **authentication of devices and communication channels**.
- Others solutions **restricts apps access to external resources, such as Bluetooth, SMS and NFC**, by defining new SEAndroid types to represent the resources.
- Moroever such **solutions are not able to address several communication channels such as: SMS, Audio, Wi-Fi and NFC** due to of missing important information for the detection purpose.

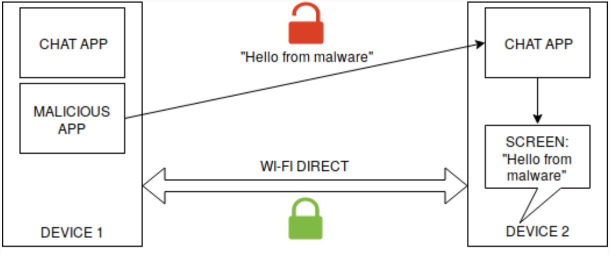
Contributions

- We identify a security problem called **cross-device app-to-app communication hijacking (CATCH)**, which commonly exists in Android apps that use short-distance channels, and afflicts all the tested Android version.
- We provide a solution to the CATCH problem by **designing and developing an authentication scheme detector** that analyzes Android apps to discover potential vulnerabilities
- **Validate the results of our system on Android apps** with manual analysis, and test its resilience in detecting the authentication scheme.

Cross Device Authentication Scheme

Cross-device Authentication Scheme


APP
A2A COMMUNICATION (NO AUTH)
APP
BLUETOOTH CHANNEL (AUTHENTICATED)
DEVICE 1
DEVICE 2



Threat Model & Attack

- The attacker is able to install a malicious app on the mobile's victim phone.
- The malicious app can therefore craft custom messages to send to the other device, which are displayed as if they were sent from the original app.
- Depending on the particular context, there are some scenarios in which the attack can become very dangerous: **Phishing, Malware delivery, Exploitation**.

Approach Overview

Challenges

text.....

Boundary Area: Entry & Exit Points

text.....

Detection Strategy

text.....

Technical Details

Technical Details

text.....

Experimental Evaluation

Experimental Evaluation

text..... Here we put the experiments that we did

Dataset Composition

text.....

Results

text.....

Case Studies

Data injection on BluetoothChat

text.....

Data injection on Wi-Fi Direct +

text.....

Discussion

Impact & Limitations

text.....

Conclusion & Future works

Conclusion

text.....

Thank you for attention

Questions?