Review “Analysis SmartApps”

Name: Wenhui Zhang

*Paper Name：*

Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In *Security and Privacy (SP), 2016 IEEE Symposium on* (pp. 636-654). IEEE.

**Contribution:**

This paper performs empirical security analysis of a [Samsung SmartThings.](https://www.smartthings.com/) It evaluates the platform's security design, and coupled that with an analysis of 499 SmartApps and 132 device handlers using static code analysis tools that we built. It finds that: (1) SmartApps can be overprivileged; (2) events that carry sensitive information such as lock pincodes are not protected by this platform.

**Motivation:**

Smart home frameworks supports easier development of IoT applications, however they also bring exposure of significant security risks to users.Samsung-owned SmartThings is one of the largest impact platform, so analysis its security related issues is a must.

**Related works:**

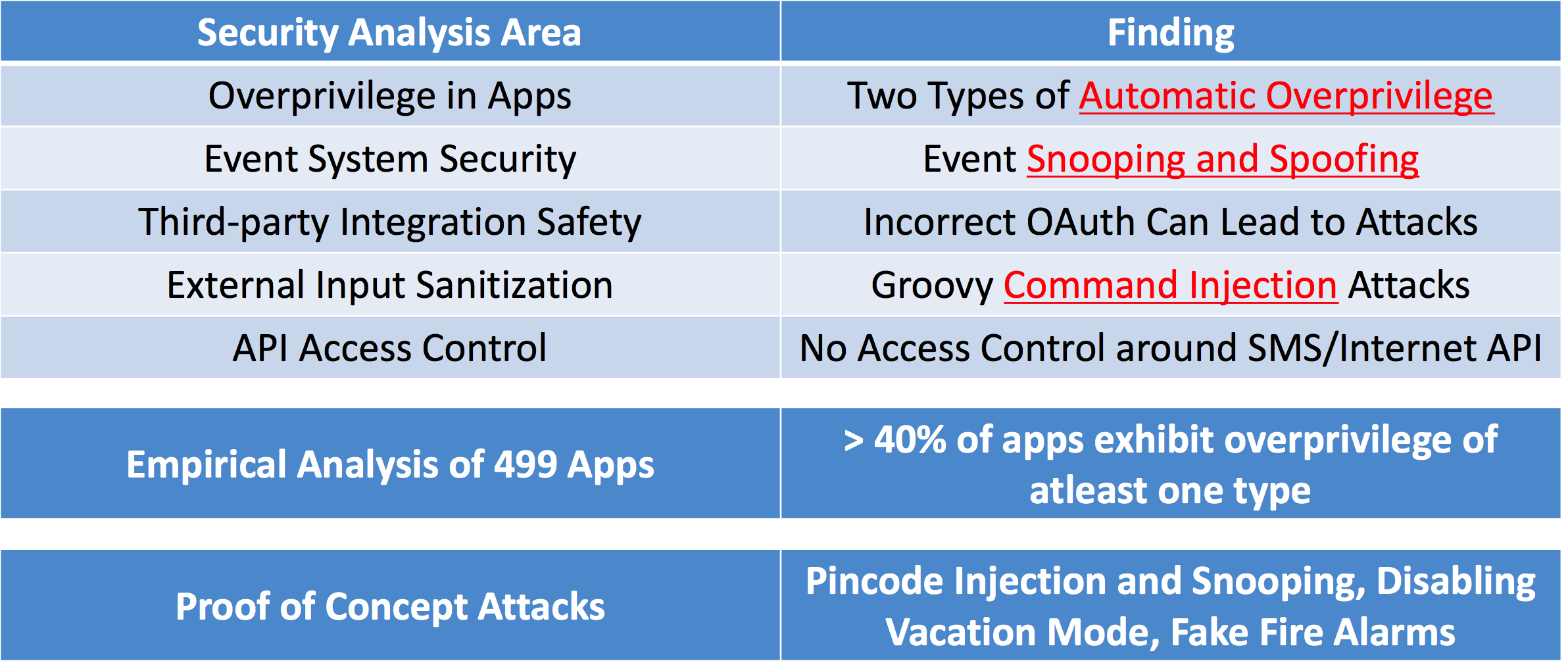
(1)Insecurity of Third-Party Integration[OAuth Demystified for Mobile Application Developers,CCS’14]; (2) Flooding[ Computer Security and the Modern Home, CACM’13]

**Methodology:**

They exploited framework design flaws with 4 PoCs: (1) secretly planted door lock codes; (2) stole existing door lock codes; (3) disabled vacation mode of the home; and (4) induced a fake fire alarm. It releases (1) Static analysis tool that computes overprivilege in SmartApps; (2) Python script that automatically creates skeleton device handlers inside the SmartThings IDE; (3) Capability documentation that we used in our analysis.

Github: https://github.com/earlence/SmartThingsAnalysisTools

**Results:**



**Take away:**

This paper points out 2 design issues for SmartApps platforms, (1) over-privilege due to Coarse grained capabilities, and Coarse SmartApp-SmartDevice Binding(55% apps); (2) sensitive events not protected.