Who hijacked My Smart Home

--A url hacked all IOT devices

Han Zidong@tencent
Self Introduction

- Han Zidong
  - Android security researcher from Tencent Mobile Security Lab
  - Focus on mobile security research, especially App vulnerability and IOT related security research
Agenda

- Smart home security introduction
- Traditional attack in IoT
- Our advanced approach
- Case of some vulnerabilities
- Q&A
Smart home security introduction

- Smart home architecture
- Vulnerability in IoT Device
IoT Bridge With Cloud Server
IoTBridge
Without
Cloud Server
Vulnerability in IoT Device

• Security in Smart Home
  • More and More IoT device (Smart Tv, lock, router, robot etc...)  
  • What makes security risks in Smart Device

• IoT Vulnerability  
  • The characteristic of “Internet of Everything” makes convenience of hacking  
  • Something bridges IoT with App in an insecure way
Vulnerability in IoT Device

• What do we do?
  • Analyze every risks of smart home
  • Hack IoT device in an advanced approach
  • Attack from only a URL and gain control during a short time
Tradtional attack in IoT

- Attack target device
  - Single point attack in IoT devices with more intelligent action
    - Smart Tv, Smart Router, Smart Speaker and etc...

- Combined Attack in IoT devices with gateway dependency
  - Smart lamp, Smart adapt, Smart cleaner robot, Smart lock and etc...
Traditional attack in IoT

- Common Attack Approach
  - Heap or Stack Overflow attack
  - Command Inject
  - Android/Linux N-Day CVE
  - External IP and sensitive interface exposure
Some New Attack Approach

- Why a url?
  - As a trap to attack more concealed
- What can a url do?
  - Gain control of IoT in some way
- Some Attack Surface
  - Attack IoT bridge protocol
  - Security in brain App of IoT
  - More ...
Expand ability of a remote url

• How to combine app and IoT Security
  • Exploit JSAPI of brain app

URL Attack Entry

Native Code with JSAPI

App Security in JSAPI

IoT Security Risk

XSS

JsBridge

CSRF

Download/Upload File

GetUserInfo

Command IoT Device

Code Inject

Info Disclose

RCE

Update Risk

Authorization Risk

Gain Root Control
Expand ability of a remote url

• Csrf and penetrate into private net
  • Dns-Rebinding
Url Attack Smart Home
Advanced target to Attack

• How to make attack more persistence and concealed
  • More intelligent, more chance
    ➢ Smart TV
    ➢ Smart Speaker
    ➢ Smart Router
  • Better attack approach to gain control
    • suddenly playing a horror film
    • Silent install the backdoor
    • Samsung TV turned off in a fake way to record user’s voice
- Attack open-port to get protocol type
- Analyze sensitive action or exposed interface
- Inject backdoor to access persisting RCE attack
Smart TV = Backdoor?
Cases Study

- Smart Tv attack case
- GeekPwn hacker-house case
Attack Smart Tv
Case 1

- Expose some Interface with no authorization
- Basically DLNA screen-mirroring
- Inject backdoor into Tv
### Attack Smart TV Case 1

- Dangerous Upnp Action
- Remote Download -> Install App -> Launch App
- Attacker hijacked private network
Attack Smart Tv Case 2

- Weak App Code Protection
- Communicate with Tv with no authorization
- Remote attack Smart Tv imitate Center App Action
A mini simulating smart home
Pwn all of IoT devices in this virtual house
Attack and hack IoT device from center brain app
Expand and exploit JSAPI ability to access smart home control
Achieve persistence and concealed
Case 1

- Analyze and Choose Attack Surface
- Pwn target devices with obvious showing
**Hacker-House Case 2**

- XSS
- JSAPI
- Brain App
- Mobile Phone
- Smart TV
- Router
- Speaker
- Smart Lock
- Remote Playing Music
- Get Talk Record
- Remote Opening Door
- On/Off
- Move
- Lamp
- Robotic Cleaner
- Camera
- Oauth Risk
- Dns-Hjack
- Install BackDoor
- Token DisClouse
- BLE Attack
- Remote Opening Door
Hacker-House Case 3

Vulnerability source:
- Brain App
- Mobile Phone

Vulnerability diffusion:
- Smart Tv
- Router
- Speaker

Vulnerability sink:
- Robotic Cleaner
- Lamp
- Camera
- SmartLock
We have found about 50 0-Day vulnerabilities in famous IoT Vendor within two month

- Code Execution
- Remote Control
- Information Disclosure
- Permanent denial of service

We were ranked #1 in GeekPwn Hacker-House in 2018
THANKs

Han Zidong@tencent