



black hat[®]


ASIA 2018

MARCH 20-23, 2018

MARINA BAY SANDS / SINGAPORE



 #BHASIA / @BlackHatEvents



UbootKit: A Worm Attack for the Bootloader of IoT Devices

{Jingyu YANG, Chen GENG}@Tencent

About Speakers

- Jingyu YANG
 - Tencent Anti-Virus Lab
 - HaboMalHunter
 - Malware Analysis
 - IoT Security Research
- Chen GENG
 - Tencent Anti-Virus Lab
 - Malware Analysis

Outline

- Introduction
- Attack Vector Analysis
- Implementation
- Mitigation
- Conclusion

UbootKit = Uboot + rootkit

1

Ubootkit is able to propagate without physical access.

2

The infected IoT devices still work normally but have been controlled by the attackers.

3

UbootKit is difficult to be cleaned even by pressing the reset button

Introduction

- Suitability Analysis
 - Devices, CPU, BootLoader, OS
- Impact Estimation
 - Root Privilege
- Elimination Difficulty
 - Reset Button

start process for IoT devices

On-Chip Code



```
graph TD; A[On-Chip Code] --> B[Uboot]; B --> C[Linux Kernel]; C --> D[File System];
```

The diagram illustrates the boot process for IoT devices as a sequential flowchart. It consists of four blue rectangular boxes arranged in a descending staircase pattern from top-left to bottom-right. The boxes are labeled 'On-Chip Code', 'Uboot', 'Linux Kernel', and 'File System' in white text. Three light blue arrows point downwards from the right side of each box to the right side of the next box below it, indicating the flow of the boot process.

Uboot

Linux Kernel

File System

Techniques

Writeable Flash

- mtd_write

Injection for Uboot

- After decompression of Linux Kernel
- Before the Uboot transfers the control

Inline hook for Kernel

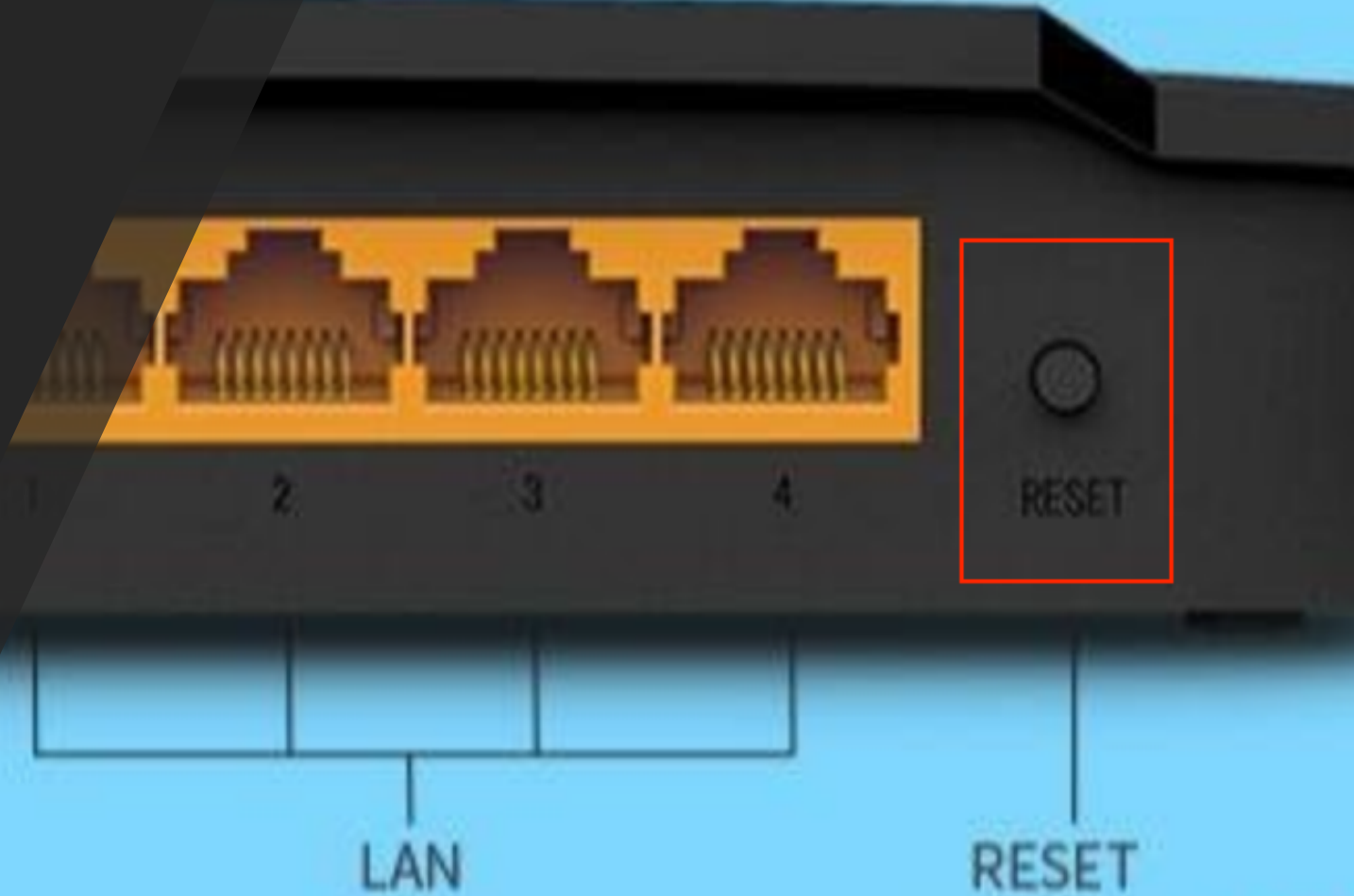
- Init_post() function

Autorun Shell Script

- /etc/init.d/rcS

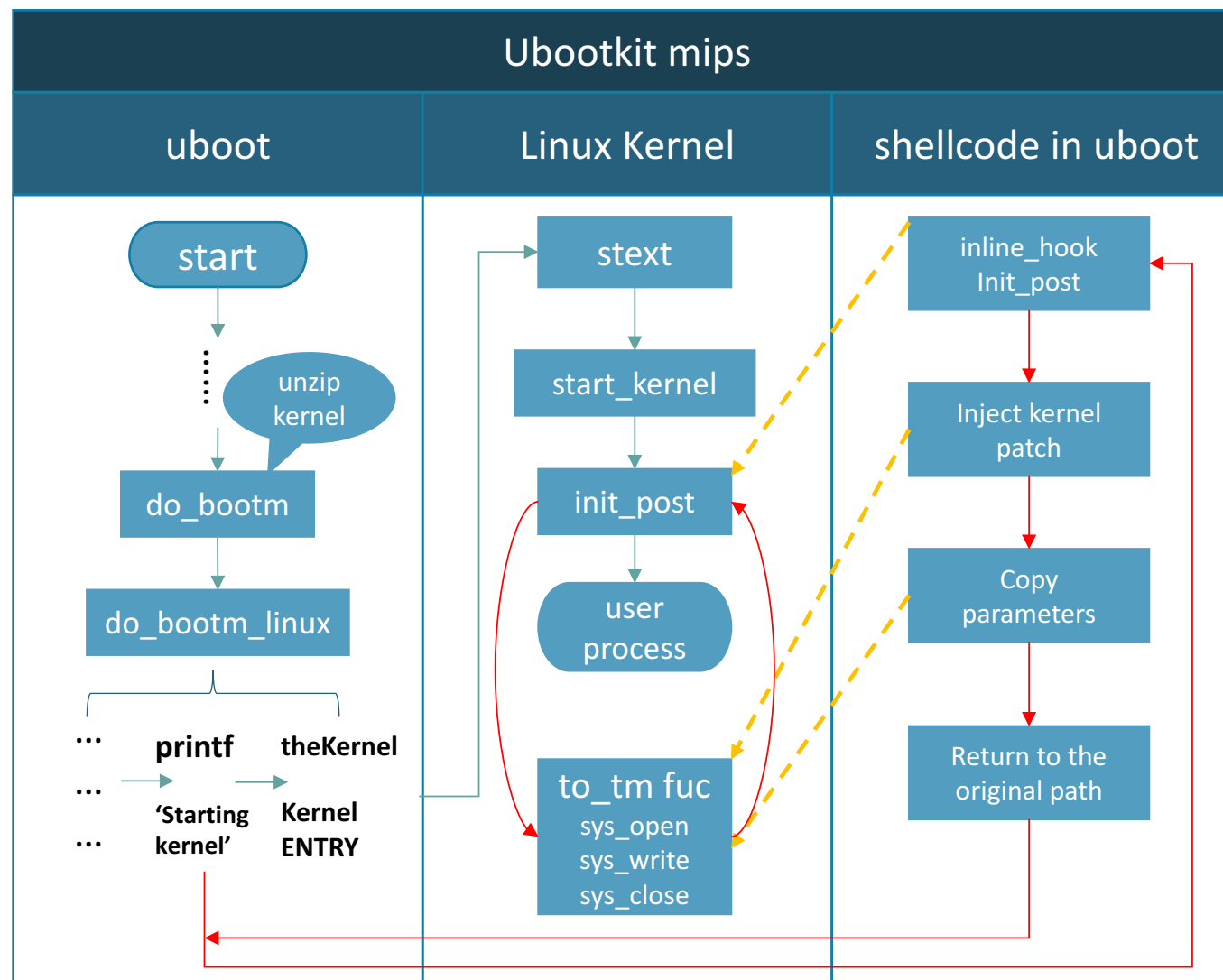
Bypass Security Methods

- Reset Button
- Uboot Verification
 - FIT_SIGNATURE
 - FIT_ENABLE_SHA256_SUPPORT
 - CONFIG_CRC32_VERIFY
- Write Protection
 - MTD_BIT_WRITEABLE
 - Write protection instruction: lock&unlock



Implementation

- Intrusion
- Infection
- Propagation

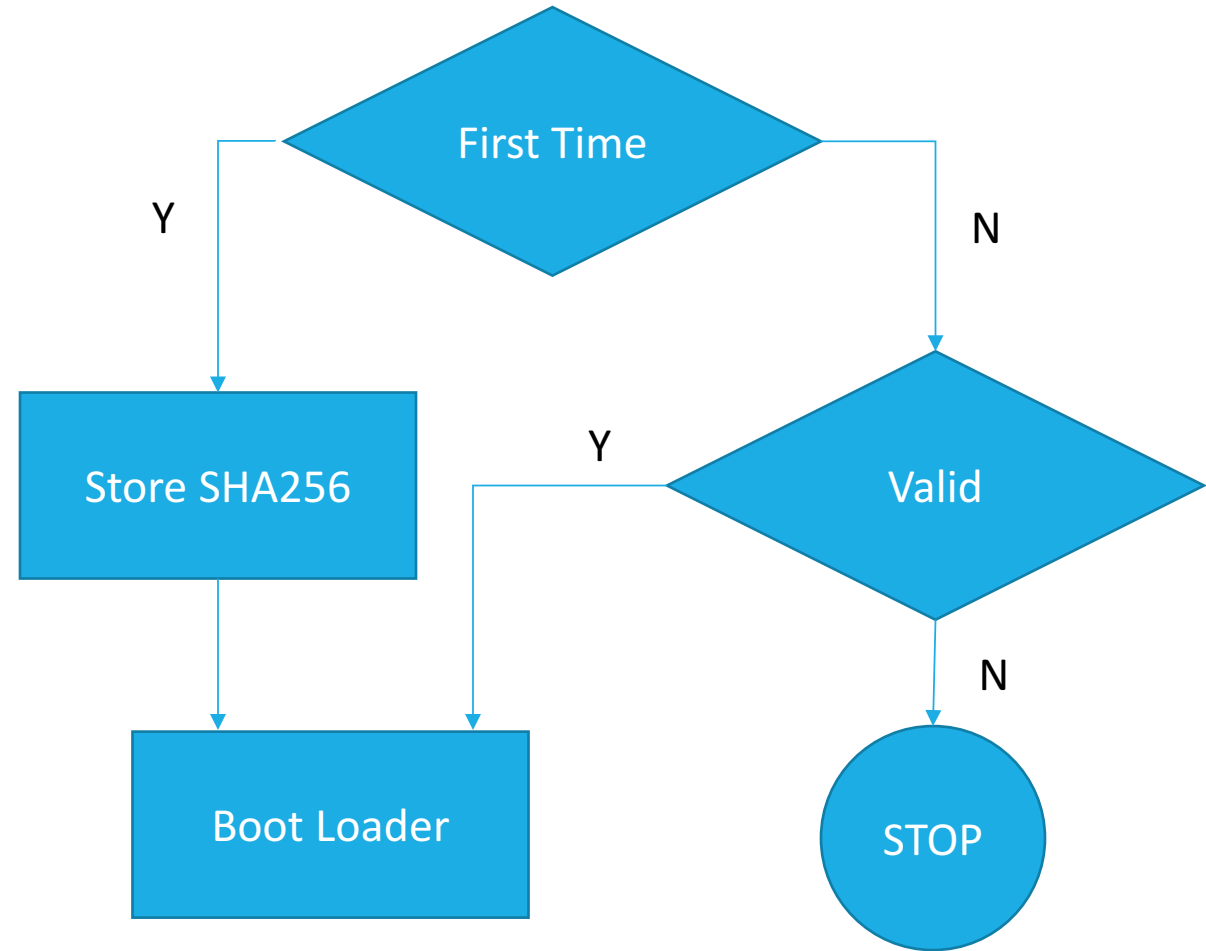


Demonstration

A demo video will be played.

Mitigation

- On-Chip code verification method



Related Work

Name	Year	Character
CIH	1998	The first virus that overwrite BIOS with junk data.
UEFI Rootkit	2015	UEFI based Rootkit but need physical access.
Mirai	2016	The first worldwide IoT malware, but can be removed by pressing the reset button.
IoT Brickerbot	2017	The infected IoT devices will no longer be able to work.
Ubootkit	2018	Evolution

Future Work

Offence

- Self Protection Technology
- Stop Re-flash Bootloader
- Detection Prevention

Defence

- On-chip Integrity Verification Solution
- Password Protection
- Monitoring Filesystem

Conclusion

- bootloader attack against IoT devices
- A real UbootKit demonstration
- Inspiration to find more vulnerabilities

Acknowledgements

- Authors
- Tencent
 - Jingyu YANG, Chen GENG, Bin WANG, Zhao LIU, Chendong LI, Jiahua GAO, Guize LIU, Jinsong MA
- Princeton University
 - Weikun YANG

References

1. Antonakakis M,et al. Understanding the Mirai Botnet, 2017
2. Texas Instruments Incorporated, "AM335x Processors,"
3. J. Teki, "U-Boot: Verified RSA Boot on ARM target," 2013.
4. Alex Matrosov, Eugene Rodionov, "UEFI Firmware Rootkits:Myths and Reality"
5. P. Lin, "Hacking Team Uses UEFI BIOS Rootkit to Keep RCS 9 Agent in Target Systems," Trendmicro
6. C. Cimpanu, "New Malware Intentionally Bricks IoT Devices,"
7. Texas Instruments, "Basic Secure Boot for OMAP-L138 C6748,"

The background features three overlapping circles in two shades of blue (a medium blue and a darker teal) on a dark gray background. A horizontal white band is positioned across the middle of the image, containing the text.

Thank you very much