

IoT Security: Firmware Testing

Yue Duan

Outline

- Research paper:
 - A Large Scale Analysis of the Security of Embedded Firmwares
 - AVATAR: A Framework for Dynamic Security Analysis of Embedded Systems' Firmwares
 - Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware

A Large Scale Analysis of the Security of Embedded Firmwares

Andrei Costin, Jonas Zaddach, Luca Bruno,
Aurélien Francillon, Davide Balzarotti

USENIX SEC 2014

Motivation

Routers



Firefox Reverse Engineering a D-Link B... +

www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/

Based on the source code of the HTML pages and some Shodan [search results](#)

D-Link devices are likely affected:

- DIR-100
- DIR-120
- DI-624S
- DI-524UP
- DI-604S
- DI-604UP
- DI-604+
- TM-G5240

Additionally, several Planex routers also appear to use the same firmware:

- BRL-04R
- BRL-04UR
- BRL-04CW

You stay classy, D-Link.

Printers

Networked Printers at Risk 0

By Jimmy Shah on Dec 30, 2011



Multifunction printers (MFPs) have been common in offices for years. They let employees print, scan, and copy documents. Two separate talks at the 28th Chaos Communications Congress (28c3) show how attackers can infect these trusted office devices.

Hacking MFPs

In Andrei Costin's presentation "Hacking MFPs," he covered the history of printer and copier hacks from the 1960s to today. The meat of the talk concerned executing remote code on an MFP using crafted PostScript. Just printing a particular document can get code to run on the machine. Previous research proof of concepts have done exactly that, once with a specially designed Word document and once with a Java applet.



Motivation

VoIP

FBI: Criminals Auto-dialing With Hacked VoIP Systems

By Robert McMillan, IDG

Criminals are taking advantage of VoIP systems to let them pump out thousands of calls per minute, the FBI says. In a warning issued last week, the FBI said that criminals are using hacked VoIP systems to conduct auto-dialing attacks.

The FBI didn't say which specific VoIP systems are being targeted, but it did advise users to upgrade to the latest version of the software. Asterisk is an open-source product that lets users turn a Linux computer into a VoIP (Voice over Internet Protocol) telephone exchange.

In so-called vishing attacks, scammers usually use a VoIP system to set up a phony call center and then use phishing e-mails to trick victims into calling the center. Once there, they are prompted to give private information. But in the scam described by the FBI, they apparently are taking over legitimate Asterisk systems in order to directly dial victims.

- Each of above is a result of an individual analysis
- Manual and tedious efforts, Does not scale

Cars

FORBES 7/24/2013 @ 9:00AM | 506,516 views

Hackers Reveal Nasty New Car Malware That Can Steal Your Car And The

...bes.



Motivation

- Goal: Perform a large scale analysis to provide a better understanding of the problem
- Problems with Large Scale Analysis:
 - Heterogeneity of
 - Hardware, architectures, OSes
 - Users, requirements
 - Security goals
 - Manual analysis does not scale, it requires
 - Finding and downloading the firmwares
 - Unpacking and performing initial analysis
 - Re-discovering the same or similar bug in other firmwares

Existing Approaches

- Test on real devices [Bojinov et.al CCS'09]
 - accurate results
 - does not scale well
- Scan devices on the Internet
 - Large scale testing [Cui et.al ACSAC'10]
 - Can only test for known vulnerabilities
 - Blackbox approach
 - More is too intrusive [Census2012]

Proposed Approach

- Collect a large number of firmware images
- Perform broad but simple static analysis
- Correlate across firmwares
- Advantages:
 - no intrusive online testing
 - no device needed
 - scalable
- But many **challenges**

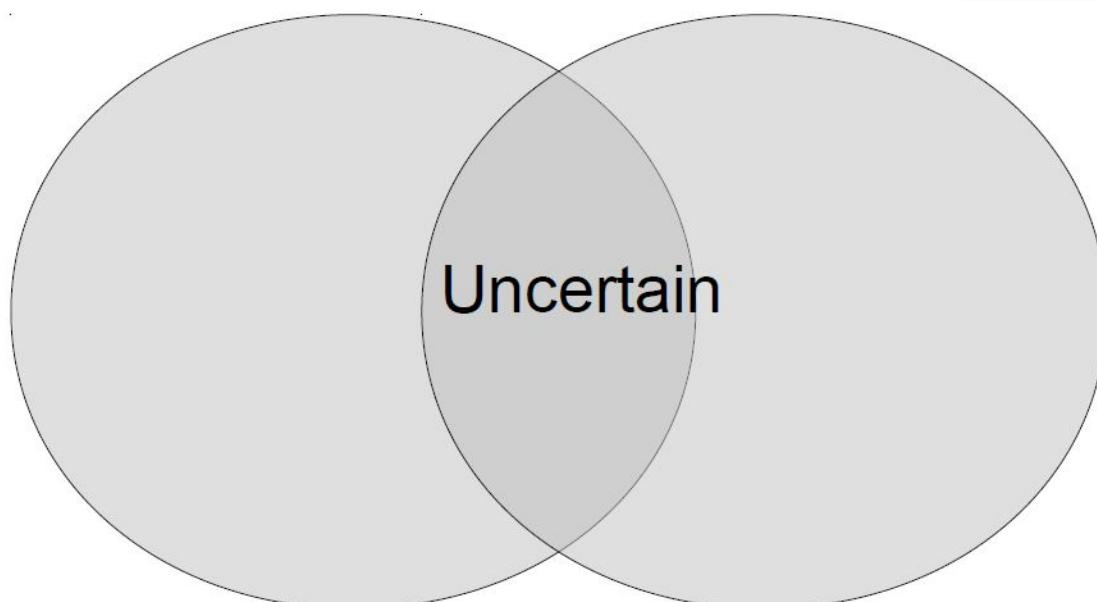
Challenge 1: Dataset

- No large scale firmware dataset yet
 - As opposed to existing datasets in security or other CS research areas
- We collected a subset of the firmwares available for download
- Many firmwares are not publicly available
 - Not intended to have an upgrade
 - Require product purchase and registration
- www.firmware.re project

Challenge 2: Firmware Identification

Clearly a firmware

Clearly not a firmware



Challenge 3: Unpacking & Custom Formats

- How to reliably unpack and learn formats?
- E.g., vendor provides a .ZIP 'firmware package'
 - .ZIP→.EXE + .PS
 - .EXE→self-extracting archive
 - Extract more or not?
 - Turns out to contain a printer driver inside
 - .PS→ASCII85 stream→ELF file that could be:
 - A complete embedded system software
 - An executable performing the firmware upgrade
 - A firmware patch
 - Often, a firmware image→just 'data' binary blob

Approach to Unpacking & Custom Formats

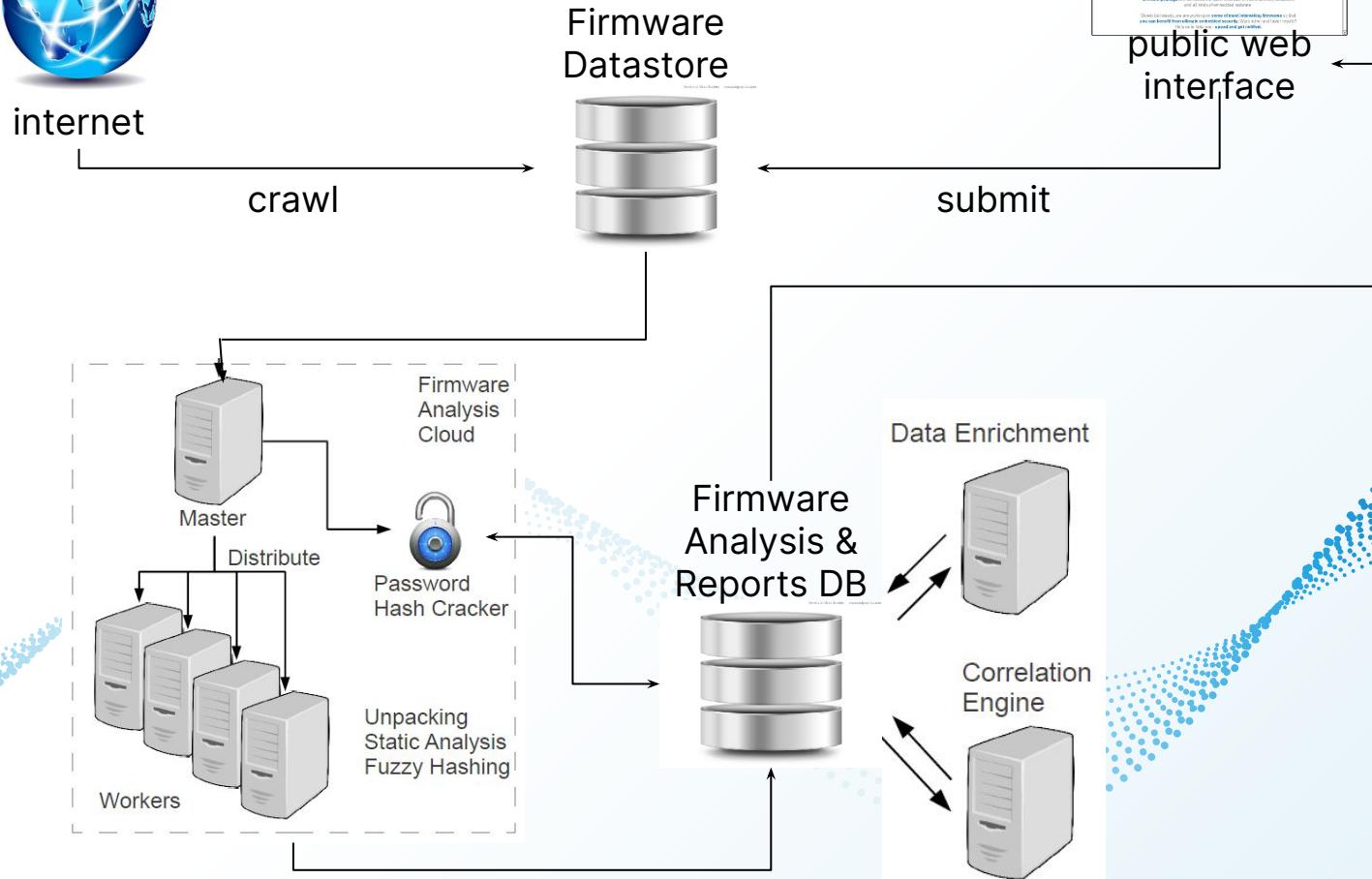
- Used BAT (Binary Analysis Toolkit)
 - Extended it with multiple custom unpackers
 - Continuous development effort
- Often, a firmware image → just 'data' binary blob
 - File carving required
 - Bruteforce at every offset with all known unpackers
- Heuristics for detecting when to stop

Challenge 4: Results Confirmation

- An issue found statically
 - May not apply to a real-device
 - Cannot guarantee exploitability
 - E.g., vulnerable daemon present but never started
- Issue confirmation is difficult
 - Requires advanced analysis (static & dynamic)
 - Often requires real embedded devices
 - Does not scale well in heterogeneous environments



Architecture



Crawler

- 759 K collected files, 1.8 TB of disk space
- FTP-index engines and GCSE

The screenshot shows a search results page from www.mmnt.net. The search bar contains "firmware download". The results are sorted by relevance, showing approximately 2,160 results found in 0.19 seconds. The results list several links to firmware download pages for various devices:

- Index of ftp://ftp2.zyxel.com/NSA310/firmware**
450AFK1C0.bin, 41.63Mb, August 14 2012 at 10:58. [ZIP] NSA310_4.22(AFK.0) C0.zip, 36.07Mb, August 24 2011. [ZIP] NSA310_4.22(AFK.1)C0.zip, 36.24Mb ...
www.mmnt.net/db/0/0/ftp2.zyxel.com/NSA310/firmware
- Index of ftp://ftp.d-link.co.za/dwr512/Firmware**
DWR-512 V1.01b06, 0.00b, October 9 2013 at 09:55. [DIR] Latest DWR-512 V1. 06b01.BIN, 0.00b, October 9 2013 at 09:55. [DIR] V 1.01b05 dwr512, 0.00b ...
www.mmnt.net/db/0/0/ftp.d-link.co.za/dwr512/Firmware
- Index of ftp://www.scansourceela.us/Bixolon/Firmware Download Utility**
350plus 352plus 500 370 372 275, 0.00b, January 18 2008. [TXT] Firmware Download, self-test,Hexdump manual for SRP-350, SRP-770 STP-103.pdf, 214.76 ...
www.mmnt.net/db/0/0/www...Firmware%20Download%20Utility
- Index of ftp://ftp.zyxeltech.de/SP-300E/firmware**
SP-300E Upgrade Utility ReleaseNote v1.00.00.txt, 516.00b, March 1 2012 at 18: 33. [TXT]
SP300E V1.03.txt, 1.52Kb, March 1 2012 at 18:33. [ZIP] ...
www.mmnt.net/db/0/0/ftp.zyxeltech.de/SP-300E/firmware
- Index of ftp://ftp2.zyxel.com/WAP3205/firmware**
100BFR7C0.bin, 3.31Mb, November 27 2012 at 05:11. [ZIP] WAP3205_1.00(BFR .0)C0.zip, 3.37Mb, July 27 2009. [ZIP] WAP3205_1.00(BFR.1)C0.zip, 3.38Mb ...
www.mmnt.net/db/0/0/ftp2.zyxel.com/WAP3205/firmware
- Index of ftp://ftp2.zyxel.com/NSA325/firmware**
450AFO1C1.rar, 41.22Mb, January 4 2013 at 01:46. [ZIP] NSA325_4.30(AAAJ.0) C0.zip, ...
www.mmnt.net/db/0/0/ftp2.zyxel.com/NSA325/firmware

On the right side of the search results, there are three additional sections:

- Current Firmware**
<https://support.nikonusa.com/.../current-firmware-downloads-available-for-nikon-products>
- Current Firmware downloads**
available for Nikon products.
Answer ID 13783| Published
12/06/2005 03:04 PM| Updated
07/16/2014 01:19 PM ...
- D5200 firmware: C: 1.02**
<https://support.nikonusa.com/.../d5200-firmware%3A-c%3A-1.02-upgrade>
Jan 14, 2014 ... This is the D5200 firmware upgrade download - Please review the information provided, and click the appropriate download at the bottom of ...
- Update Firmware**
support.nikonusa.com/faqid=14187
Nikon USA Support · My Account ·

Unpacking

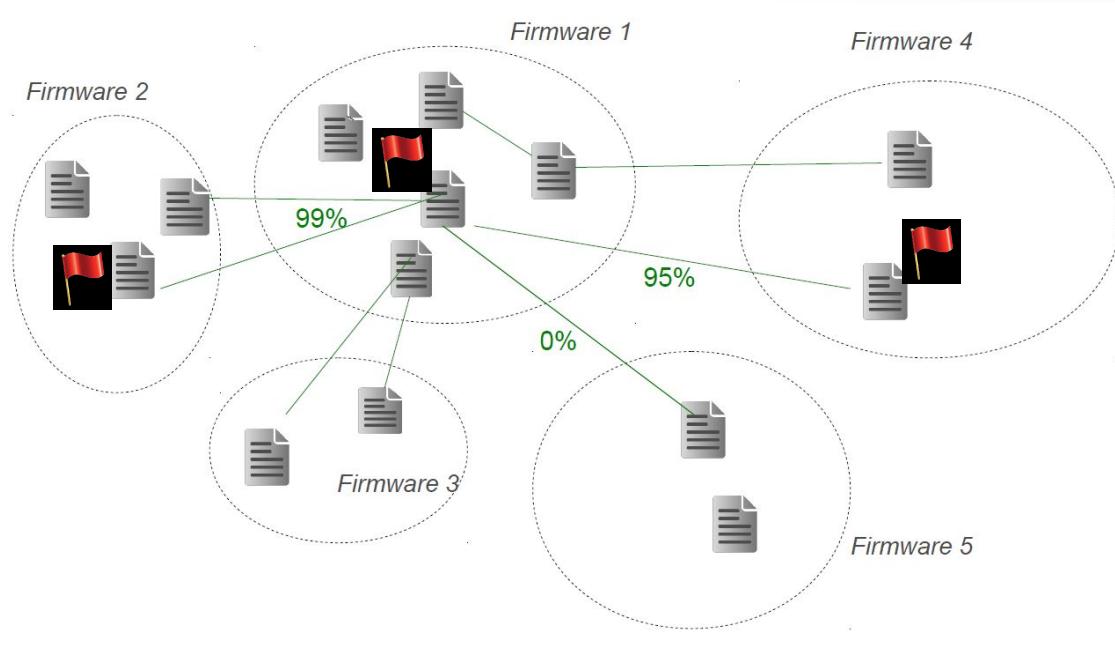
- 759 K total files collected
 - filtering
- 172 K filtered interesting files
 - random selection
- 32 K analyzed
 - successful unpacking
- 26 K unpacked (fully or partially)
 - unpacked files
- 1.7 M resulted files after unpacking

Static Analysis

- Correlation/clustering
 - Fuzzy hashes, Private SSL keys, Credentials
- Misconfigurations
 - Web-server configs, Credentials, Code repositories
- Data enrichment
 - Version banners
 - Keywords (e.g., telnet, shell, UART, backdoor)

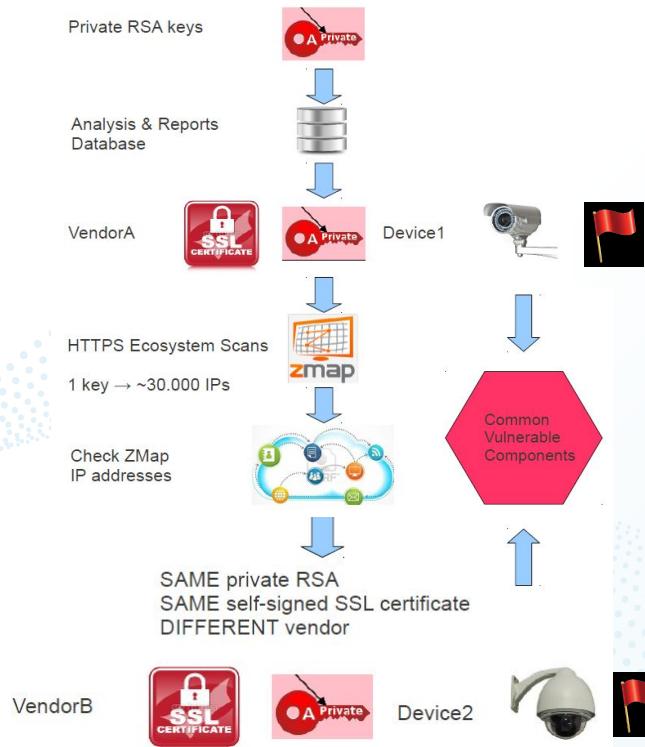
Correlation

- Correlation via fuzzy-hashes (ssdeep, sdhash)
 - E.g., Vulnerability Propagation



Correlation

- SSL keys correlation + vulnerability propagation



Results

- 38 new vulnerabilities (CVE)
- Correlated them to 140 K online devices
- Affected 693 firmware files by at least one vuln

AVATAR: A Framework for Dynamic Security Analysis of Embedded Systems' Firmwares

Jonas Zaddach, Luca Bruno, Aurélien Francillon, Davide Balzarotti

NDSS 2014

Embedded devices are everywhere

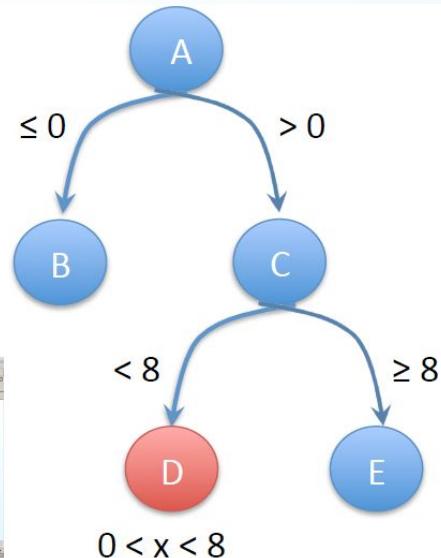
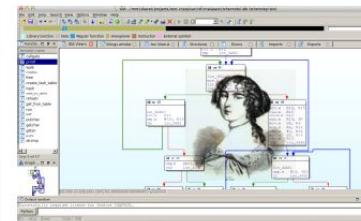
- Embedded devices are ubiquitous and diverse – but all of them run software
- Even if invisible, they are essential to your life
- Can operate for many years
 - **Legacy systems**, no (security) updates
- Have a **large attack surface**
 - Networking, forgotten debug interfaces, etc

Third Party Security Evaluation

- No source code available
- No toolchain available
- No documentation available
- Distinct tools (to flash and debug) for each manufacturer

Wishlist

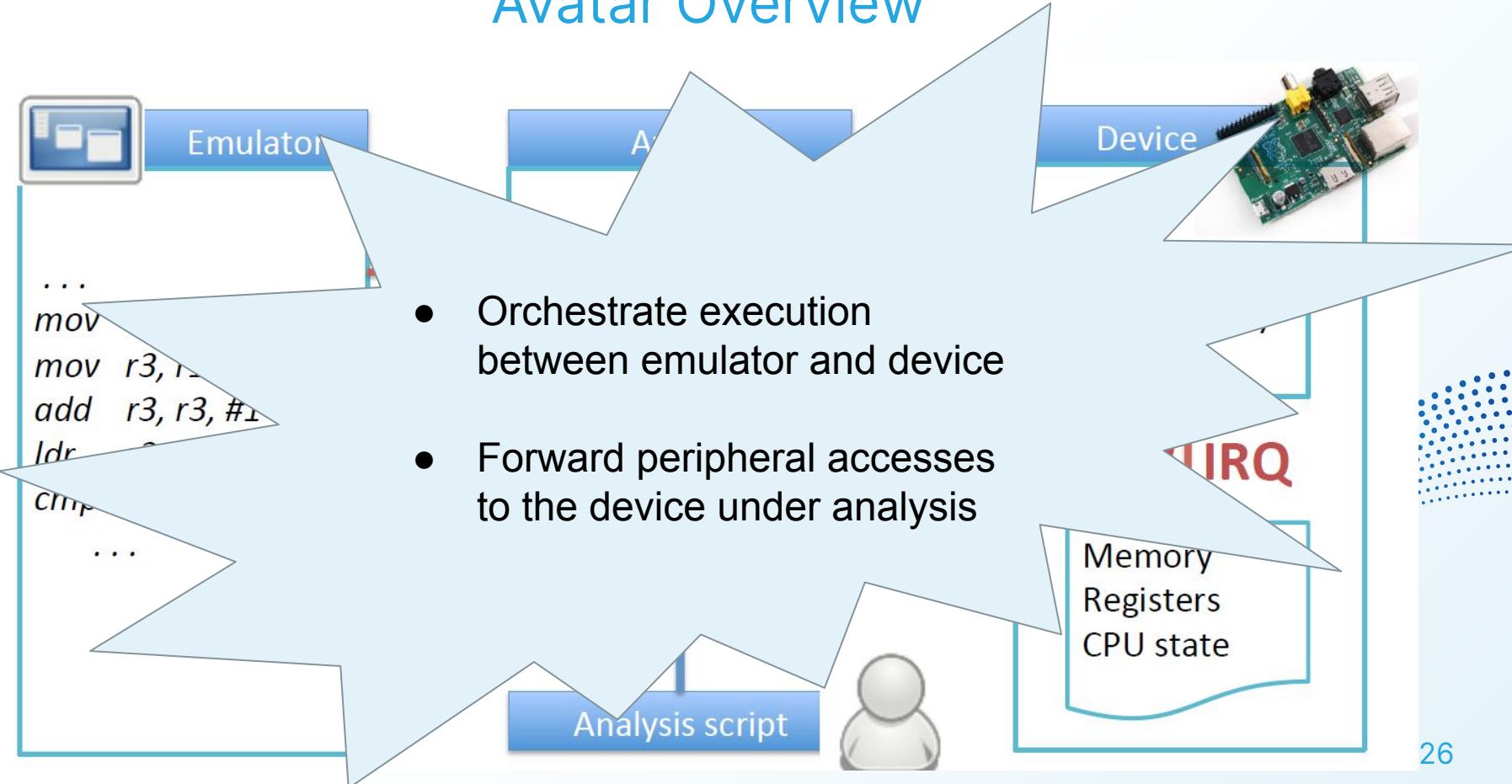
- Typical PC security toolbox
 - advanced debugging techniques
 - tracing
 - fuzzing
 - tainting
 - symbolic execution
 - Integrated tools
 - IDA pro
 - GDB



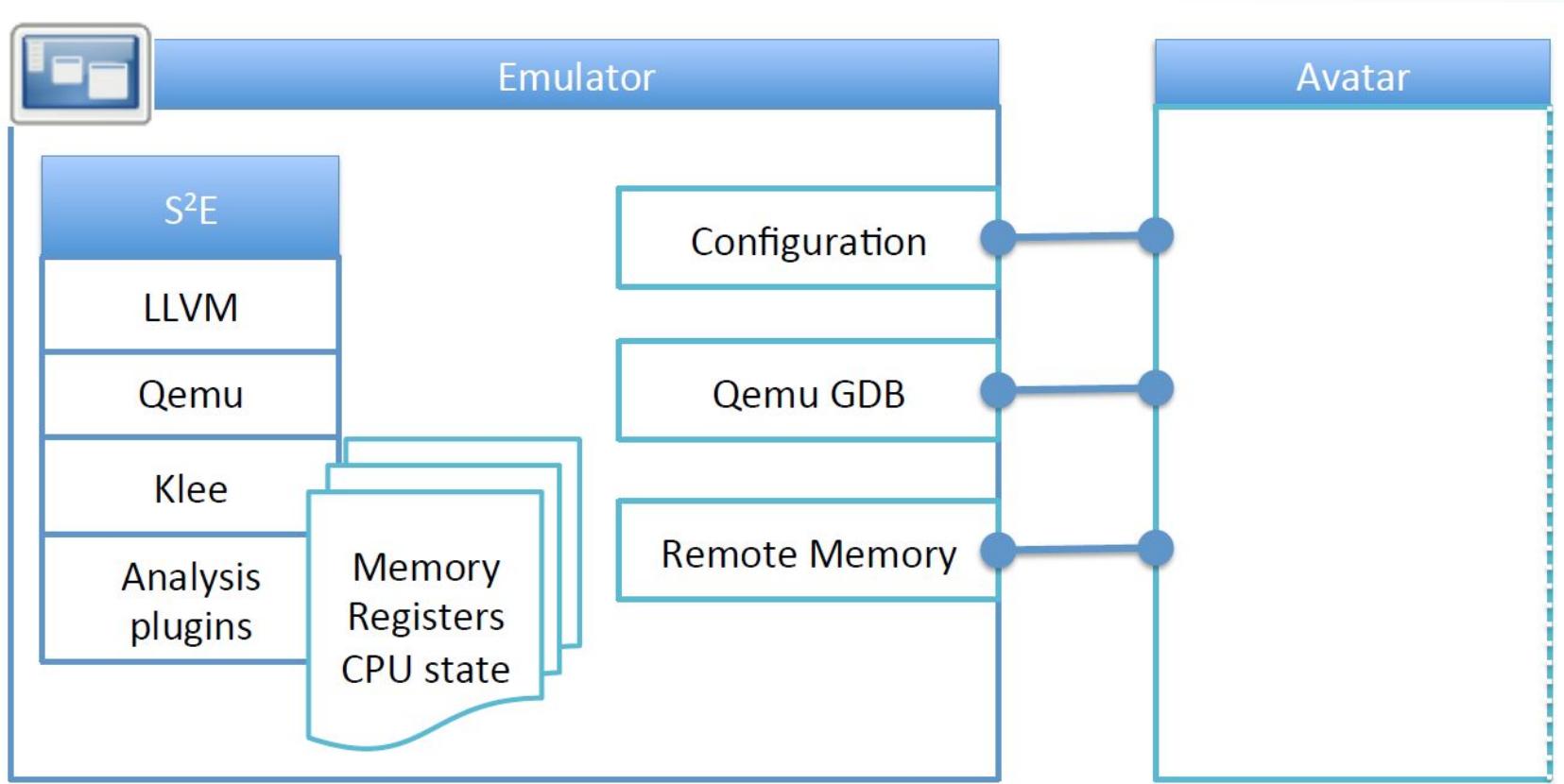
Challenges

- Advanced dynamic analysis needs emulation
- Full emulation
 - unknown peripherals
 - firmware fails if peripherals are missing
- Integration
 - support multiple vendors and platforms

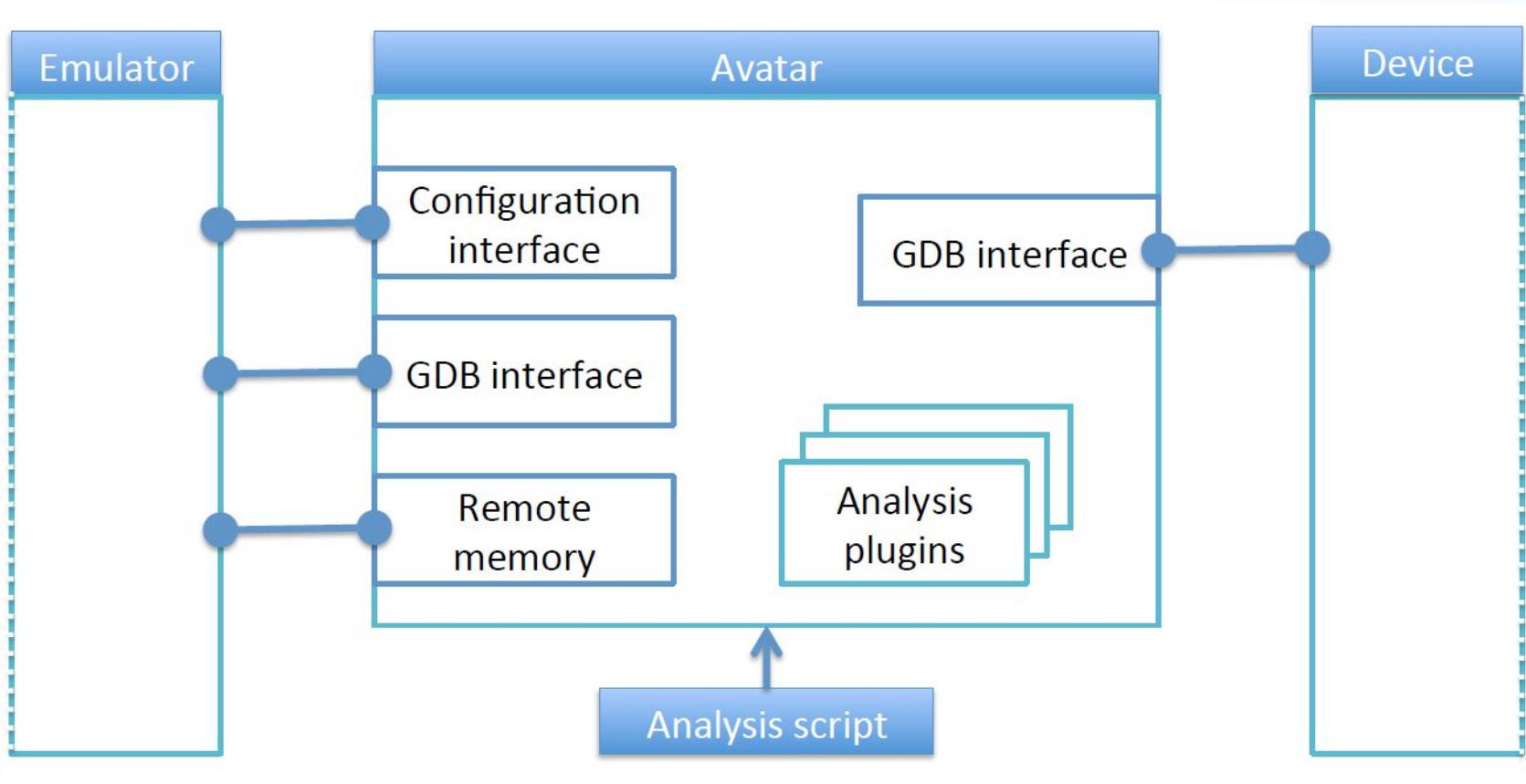
Avatar Overview



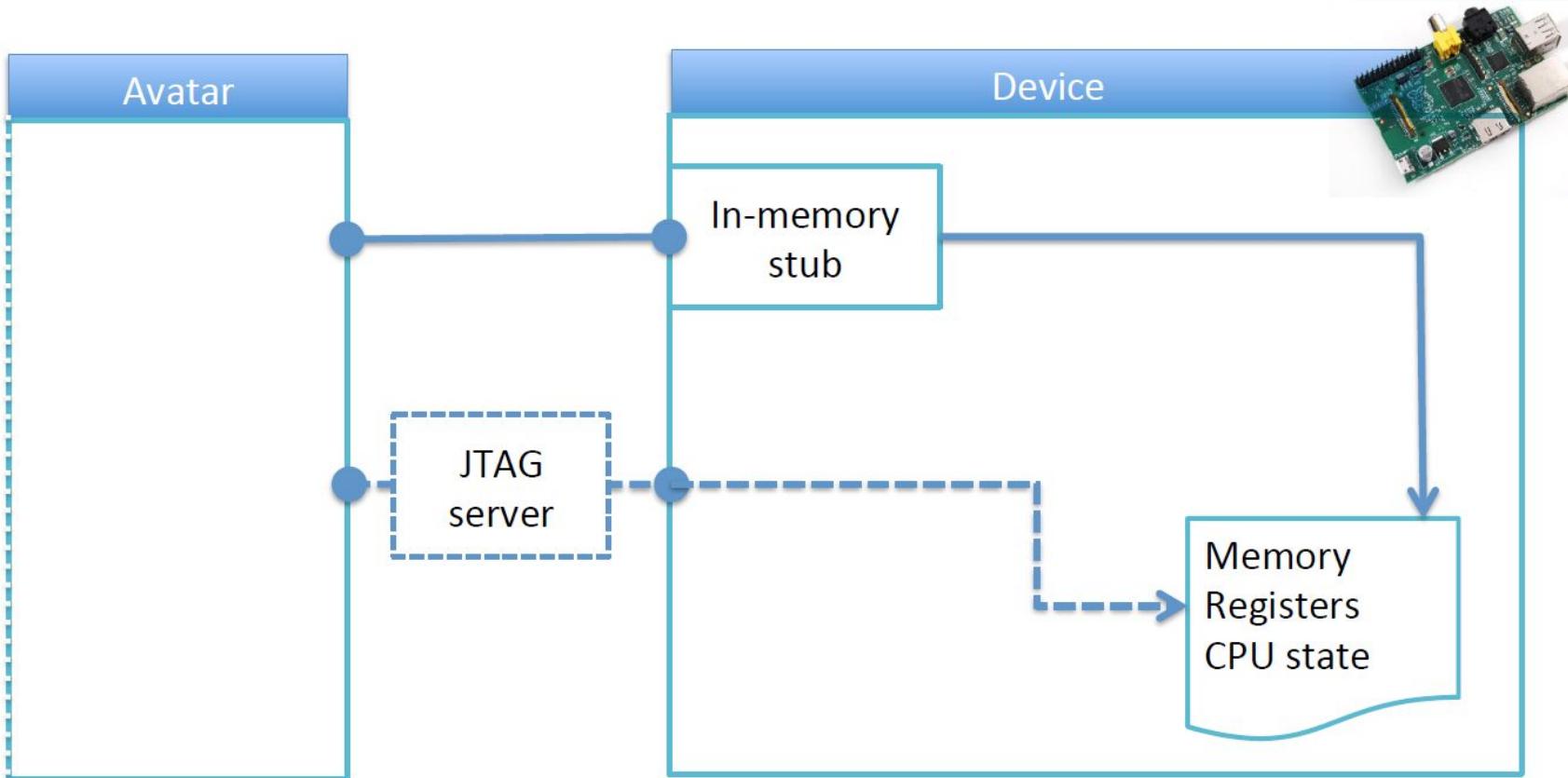
Emulator



Avatar Core



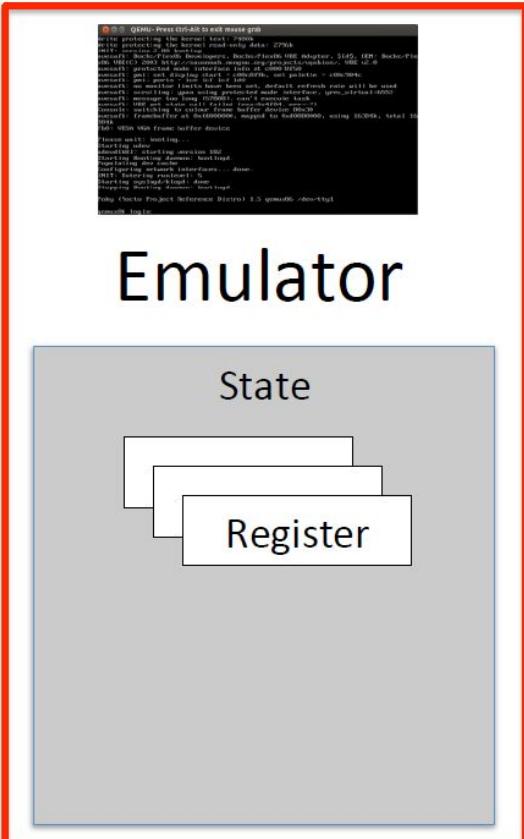
Embedded Target



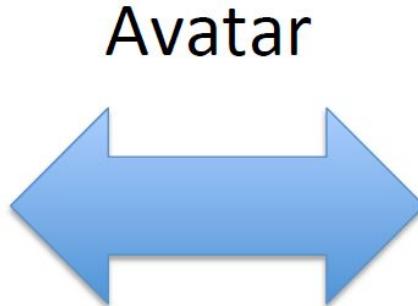
Bottlenecks

- Emulated execution is MUCH slower than execution on the real device
 - **memory access** forwarding through low-bandwidth channel
- Interrupts can saturate debug connection

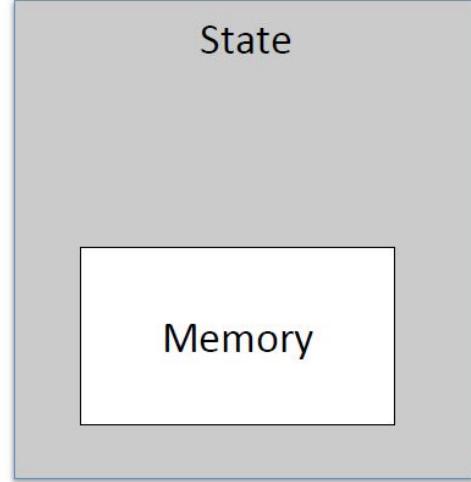
Memory Access Optimization



Emulator

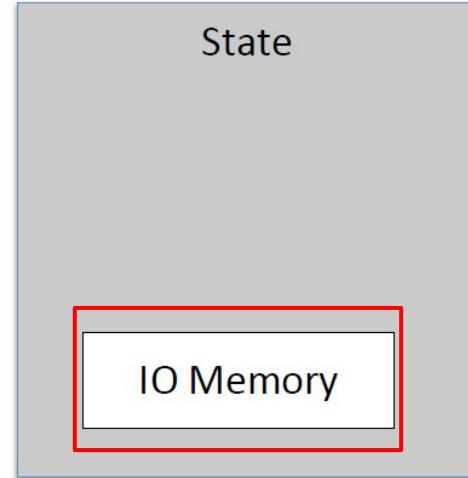
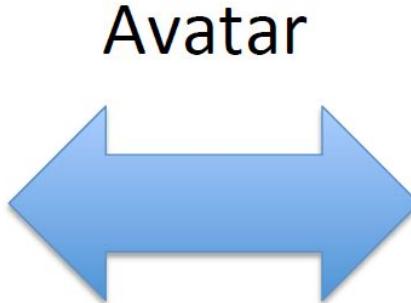
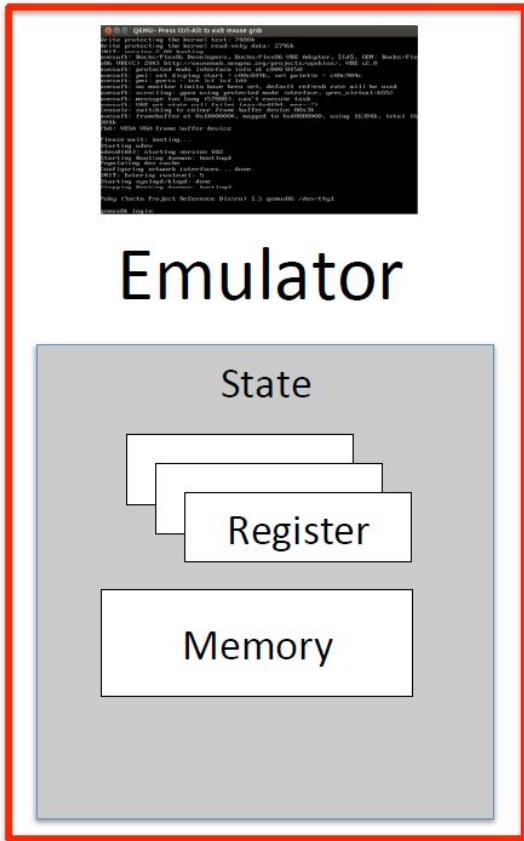


Avatar



Device

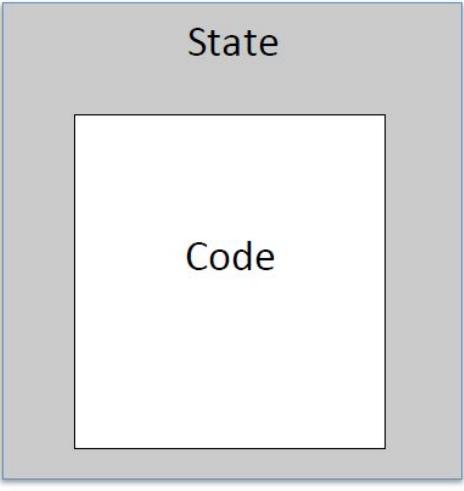
Memory Access Optimization



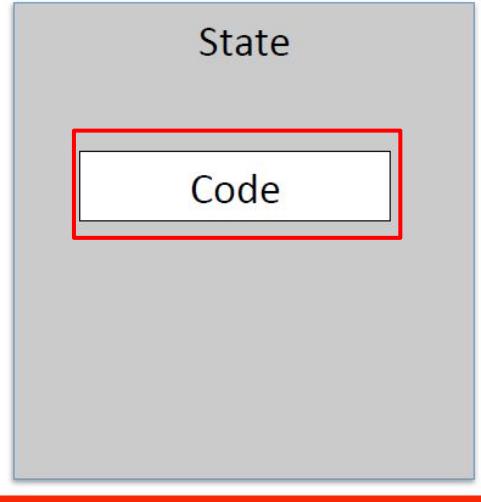
Execute Code Snippets

```
QEMU: Press Ctrl-Alt to exit mouse grab
writing protection: kernel text=48000
writing protection: kernel data=27000
monitor: Buschbox Development: BeagleBoard VNC Adapter, 5145, OEP: Remote File Transfer
monitor: protected mode interface data at 400000 bytes
monitor: protected mode interface code at 410000 bytes
monitor: guest physical address for net
monitor: PCI port 1: direct I/O
monitor: memory limit: 134217728 bytes, default refresh rate will be used
monitor: scrolling: open using protected mode interface, gen_virtuald(0)
monitor: scrolling: open using protected mode interface, gen_virtuald(1)
monitor: switching to older frame buffer device (fb0)
monitor: switching to older frame buffer device (fb0)
monitor: using framebuffer device fb0, supports fastbootmode, using 16Mbit, total 16M
monitor: using VGA frame buffer device
monitor: using VGA frame buffer device
monitor: starting version 1.02
monitor: using host interrupt controller
monitor: enabling dev random
monitor: setting up interface ... done
monitor: serial0: serial0
monitor: using virtio serial port
using Qemu Project Reference Directory 1.5 generating ./scriptfile
monitor: torque
```

Emulator



Device



Use Case: Hard Disk

- Recover bootloader protocol with symbolic execution
 - inject GDB stub
 - instrument flash loading
 - inject symbolic values for data read from serial port
 - keep track of which input leads into which code flow



Use Case: Hard Disk

- Search vulnerabilities in SMS decoding routine
 - connect through JTAG
 - execute on device until SMS decoding
 - replace SMS payload
 - with symbolic values
 - check for symbolic values in
 - program counter
 - load/store address



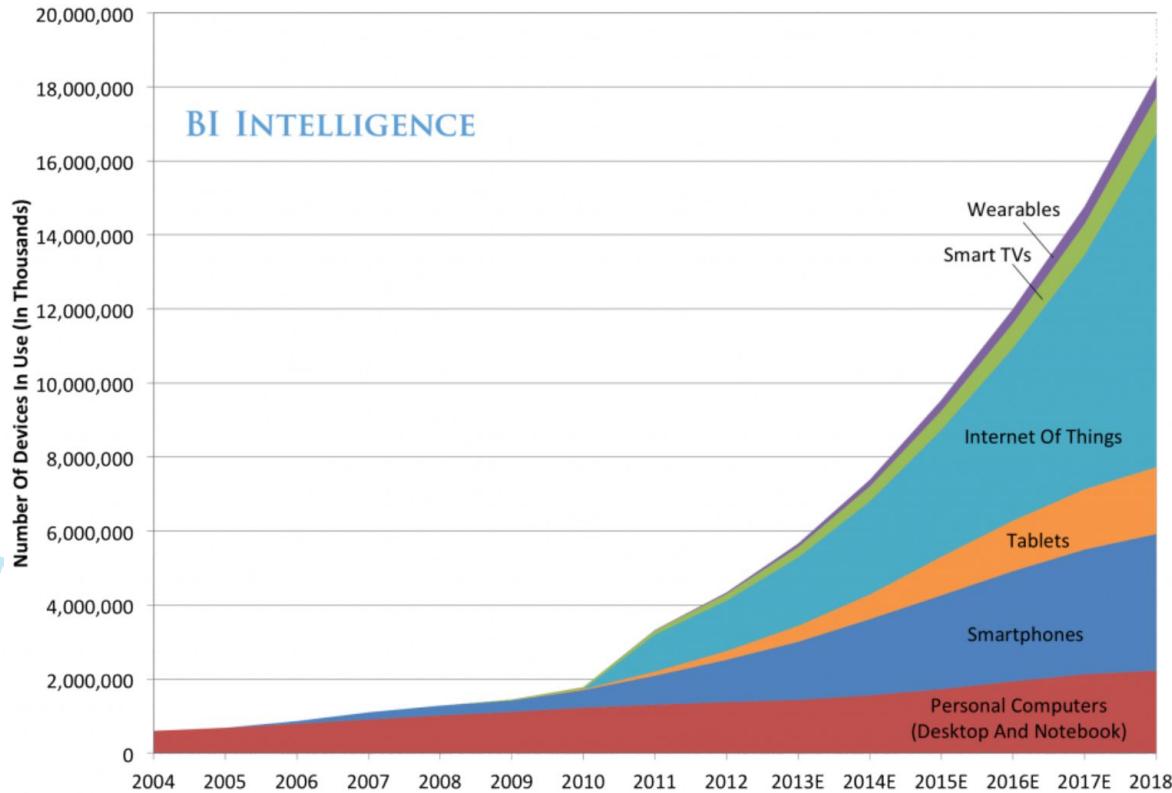
Firmalice Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware

Yan Shoshitaishvili, Ruoyu Wang, Christophe Hauser, Christopher Kruegel,
Giovanni Vigna

NDSS 2015

The Rise of Firmware

Global Internet Device Installed Base Forecast



Emergence of Backdoors

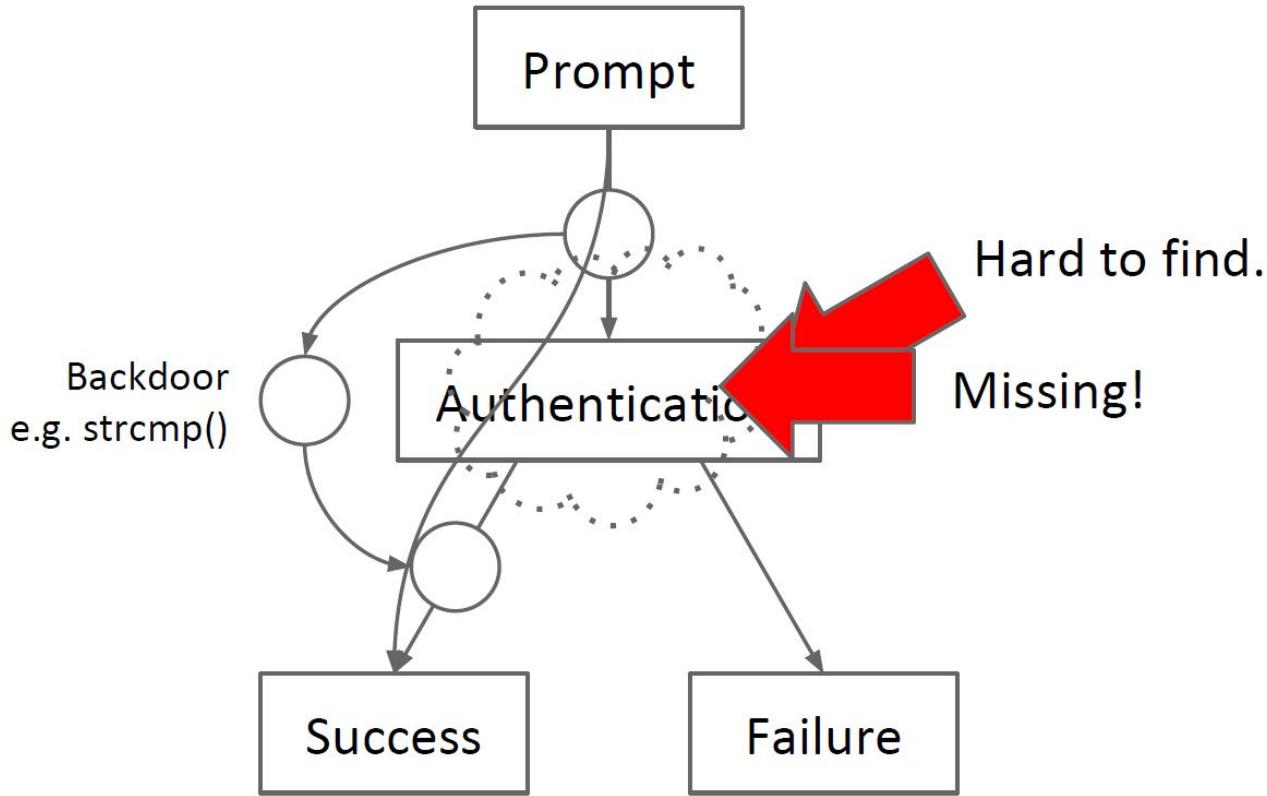
Santamarta, Ruben. "HERE BE BACKDOORS: A Journey Into The Secrets Of Industrial Firmware." *Black Hat USA* (2012).

Heffner, Craig. "Reverse Engineering a D-Link Backdoor" /dev/ttys0 (2013).

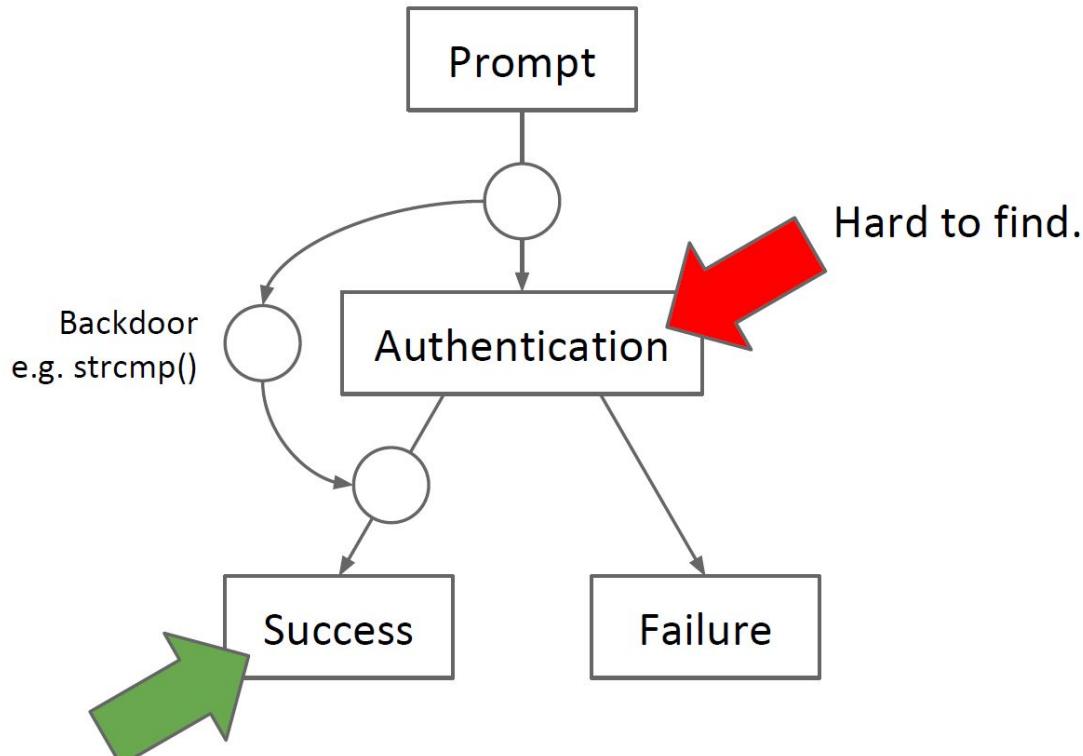
Vanderbecken, Eloi. "TCP/32764 backdoor, or how linksys saved Christmas!" GitHub (2013).

Heffner, Craig. "Finding and Reversing Backdoors in Consumer Firmware." EELive! (2014).

Backdoor Discovery

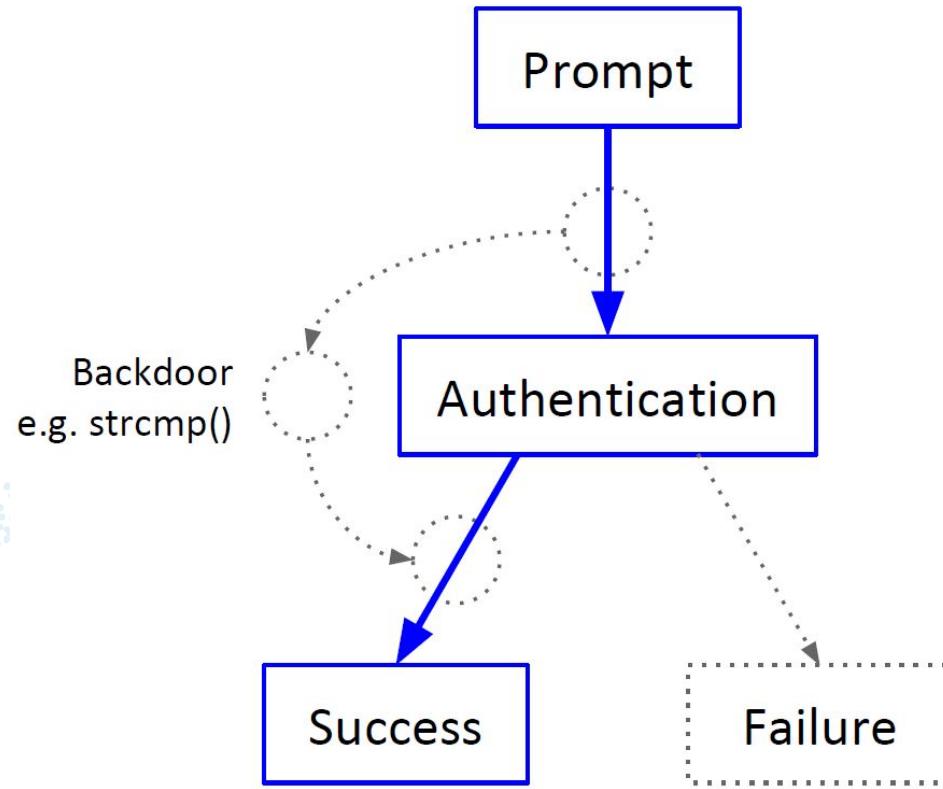


Our Solution: Input Determinism



Easier to find!

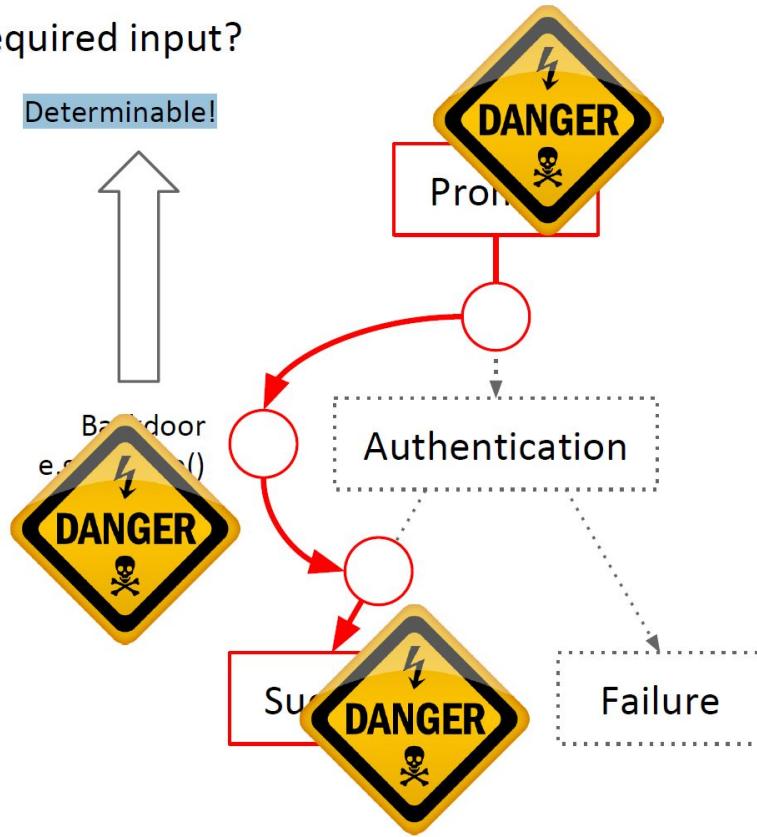
Input Determinism



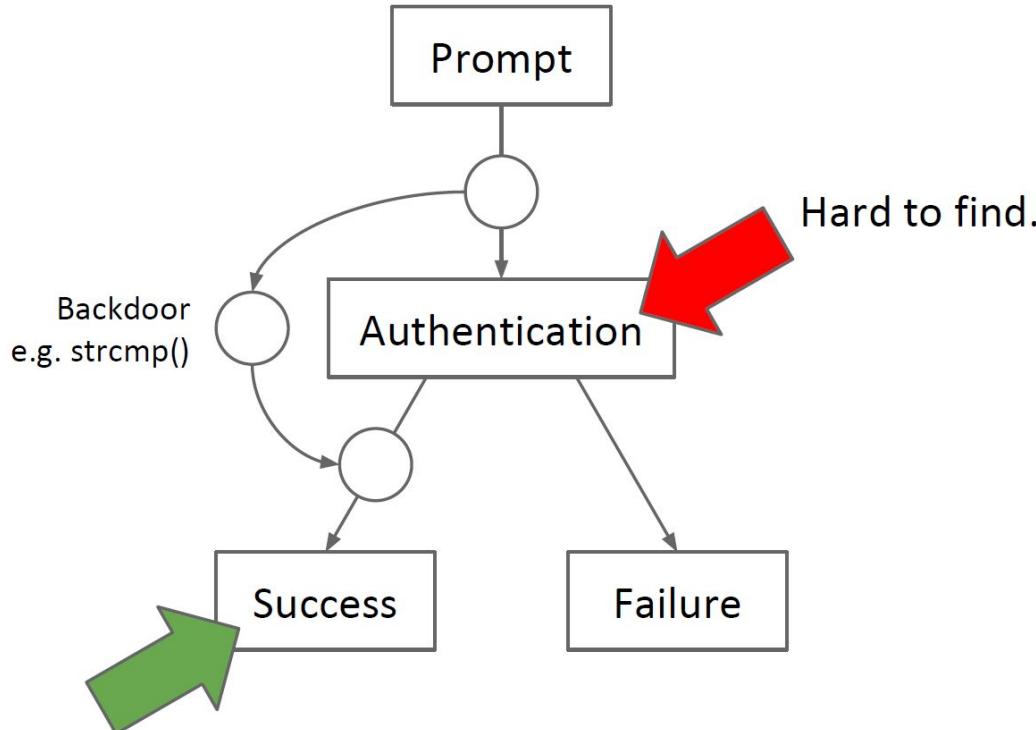
Input Determinism

Required input?

→ Determinable!



Challenge



Firmalice

Inputs:

- Firmware Sample
- Security Policy



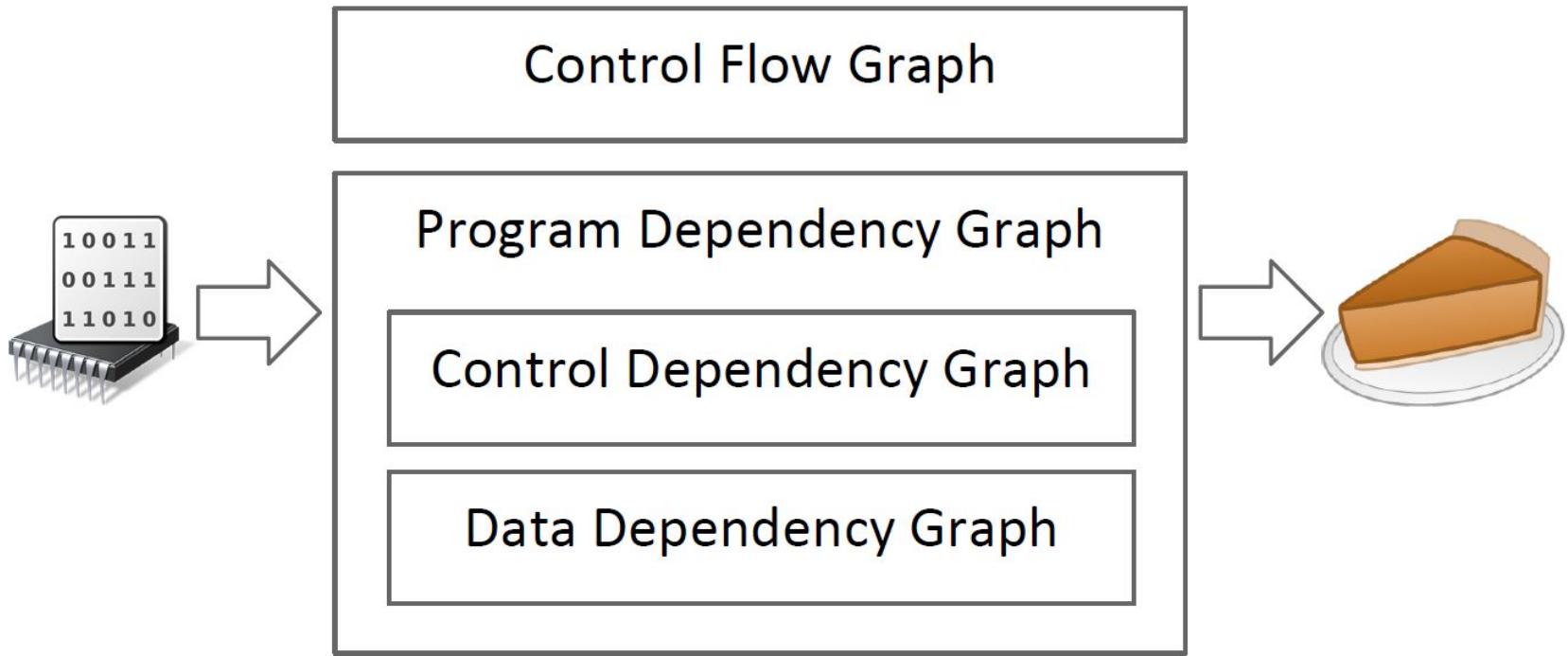
Challenges:

- Large binary programs
- Unrelated user input

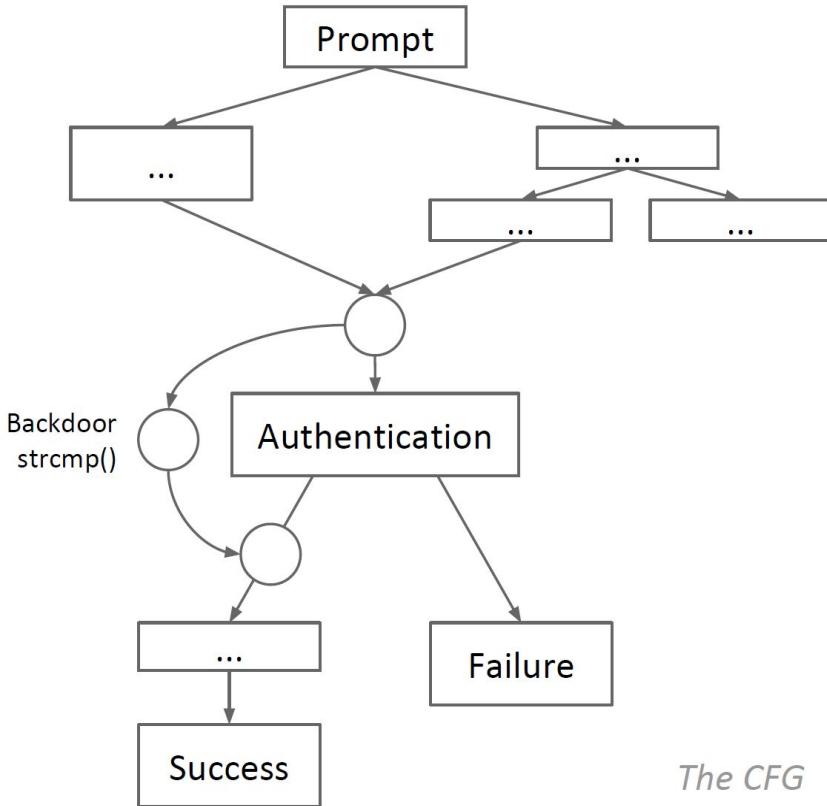
Analysis Steps:

- Static Analysis (backwards program slicing)
- Dynamic Symbolic Execution
- Authentication Bypass Check

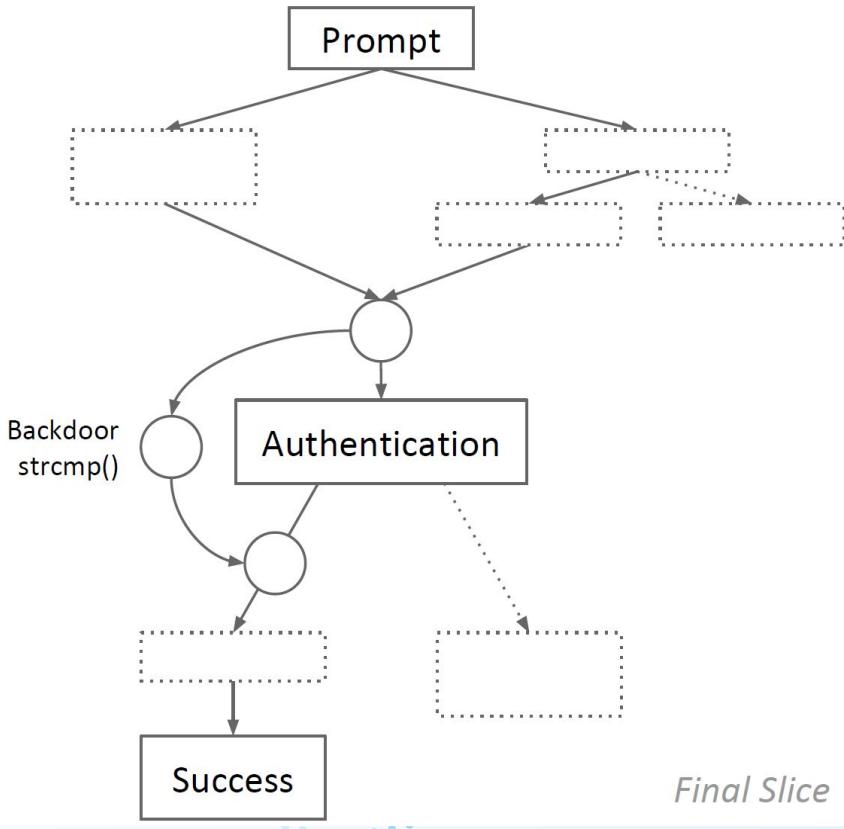
Static Analysis



CFG

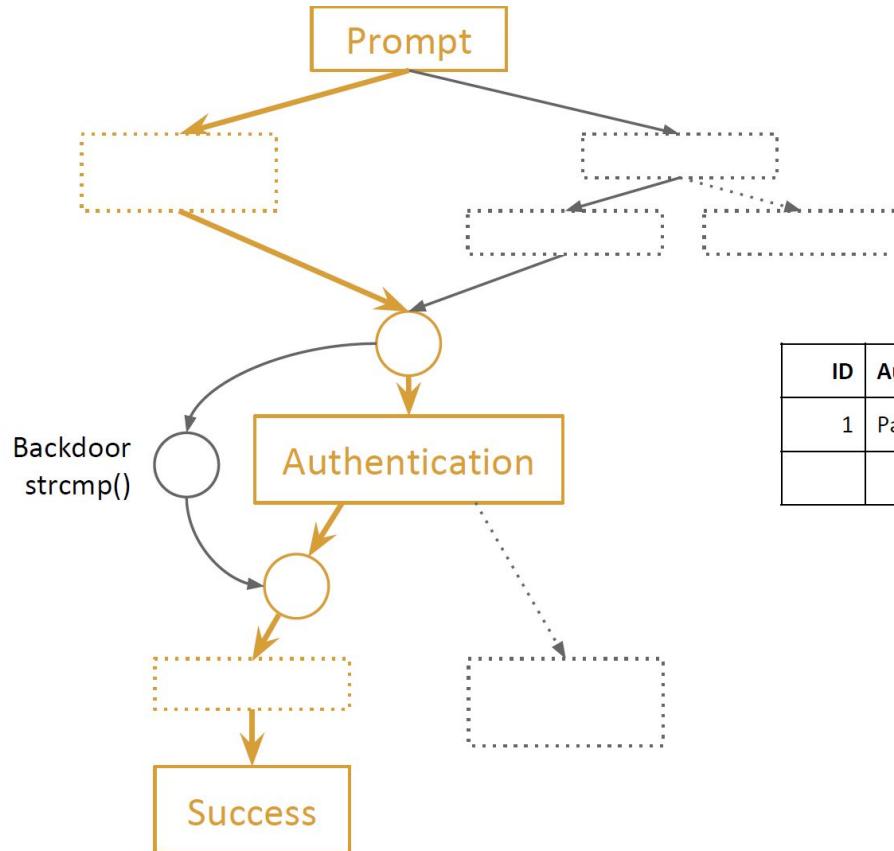


The CFG



Final Slice

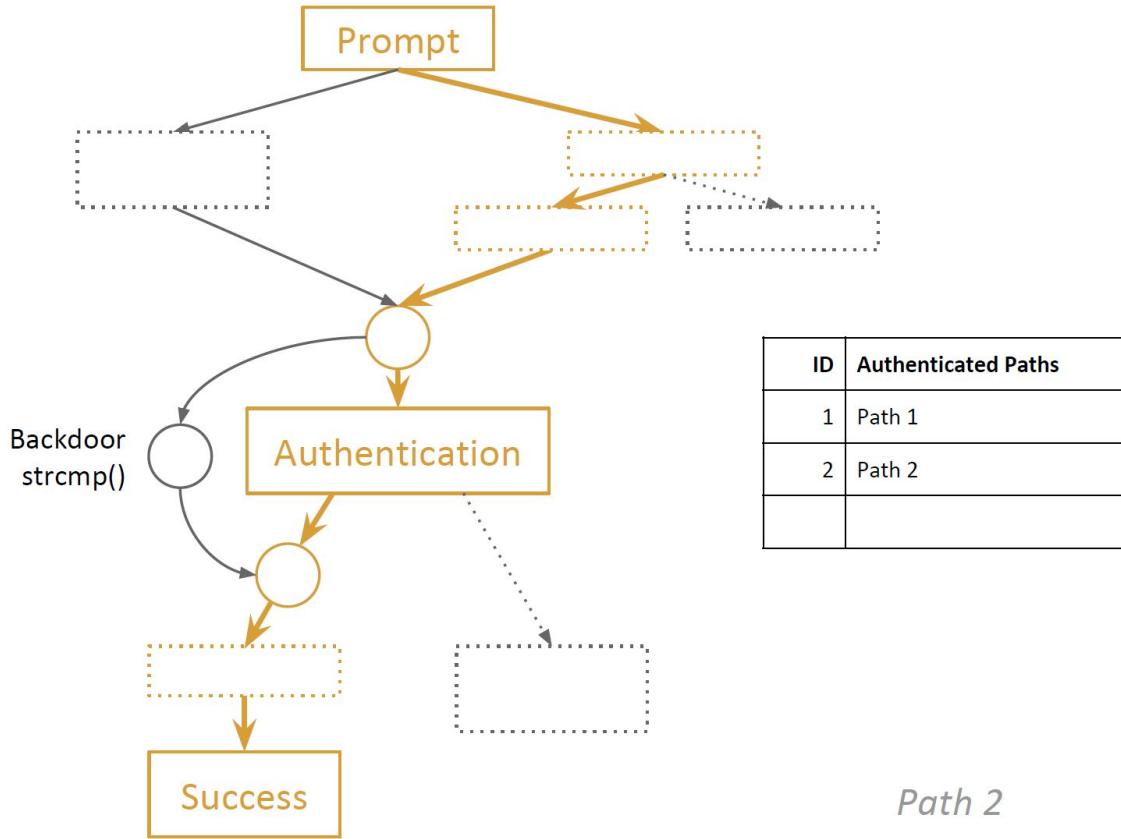
Dynamic Symbolic Execution



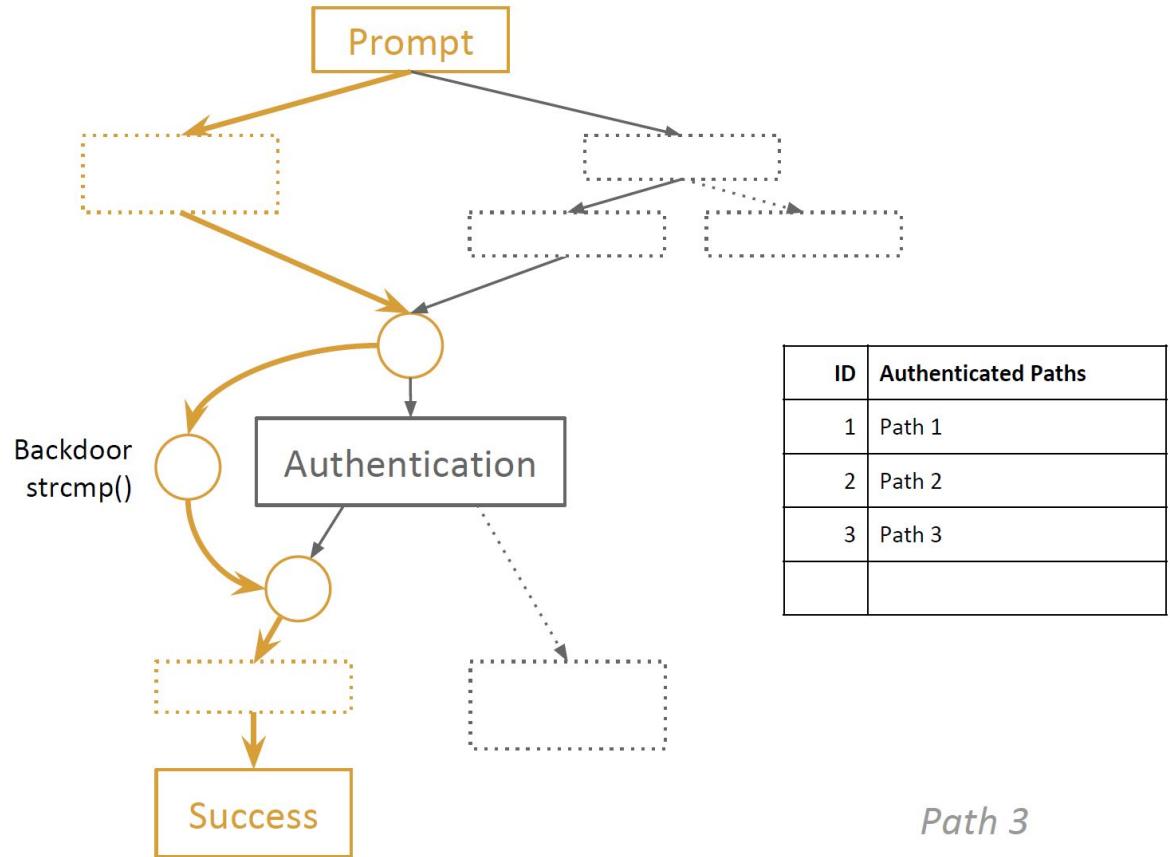
ID	Authenticated Paths
1	Path 1

Path 1

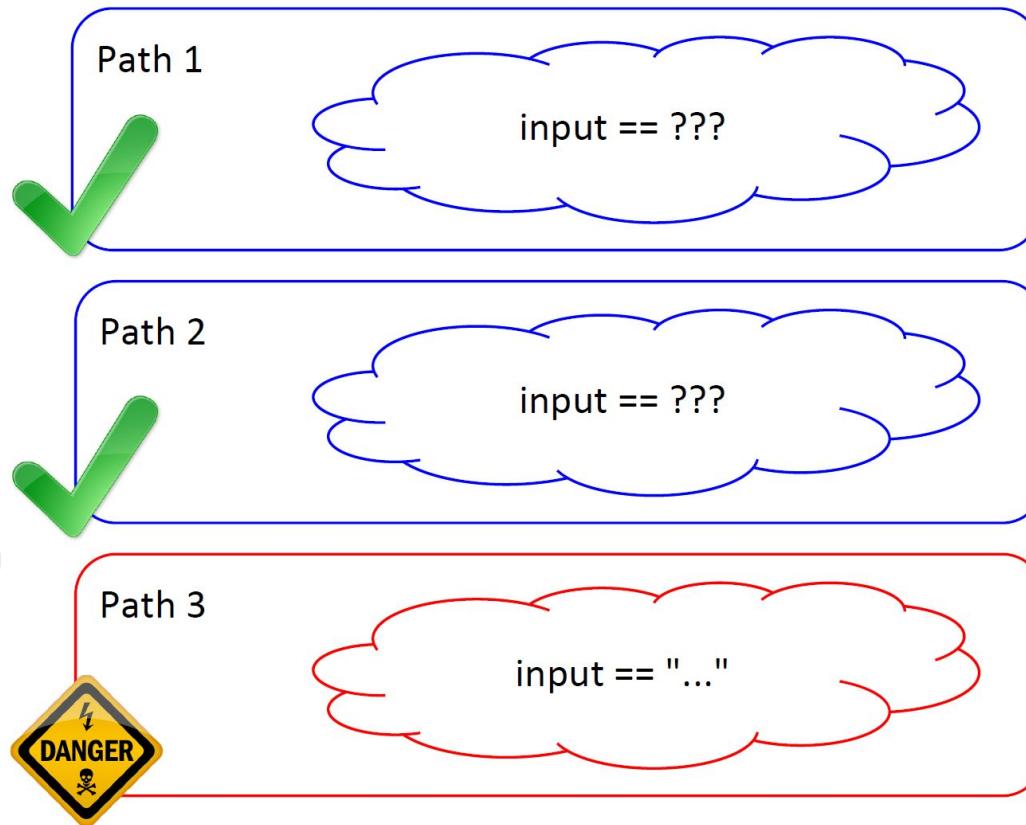
Dynamic Symbolic Execution



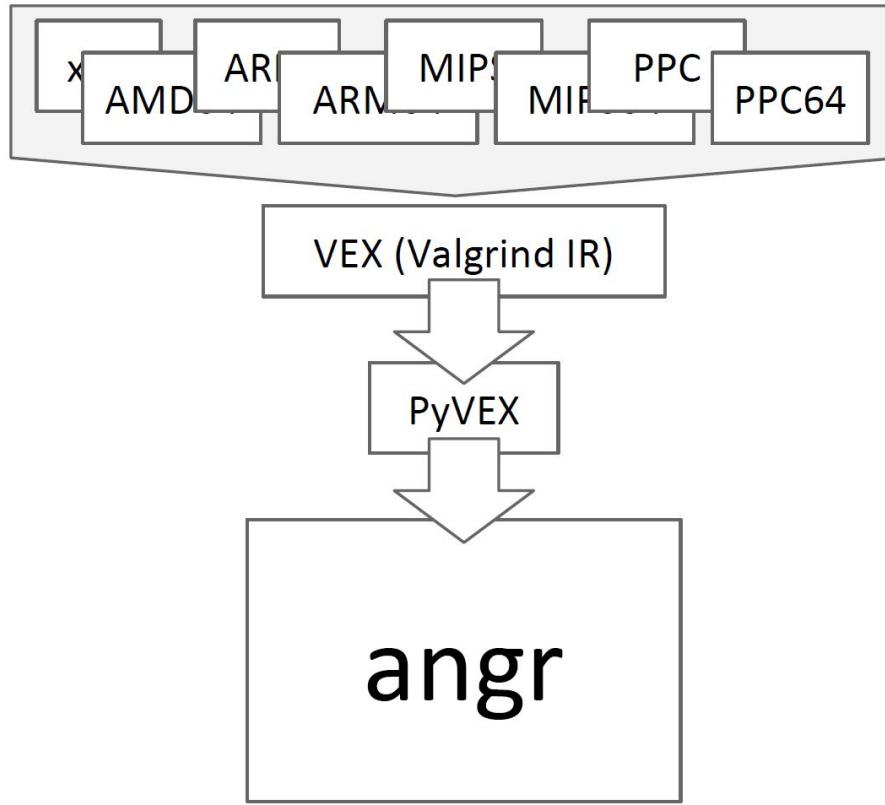
Dynamic Symbolic Execution



Authentication Bypass



Implementation



Backdoor Example: 3S Vision N5072



Slicing	→ 5m
	→ 212 bb
DSE	→ 26m

- Linux embedded device.
- HTTP server for management and video monitoring.
- Security Policy
 - Authentication required for footage access
 - "Image-Type" header
- Backdoor
 - Hard-coded user credentials
 - Username: 3sadmin
 - Password: 27988303

Thank you!

Questions?