FirmFuzz: Automated IoT Firmware Introspection and Analysis

Prashast Srivastava, Hui Peng, Jiahao Li,
Hamed Okhravi, Howard Shrobe, Mathias Payer

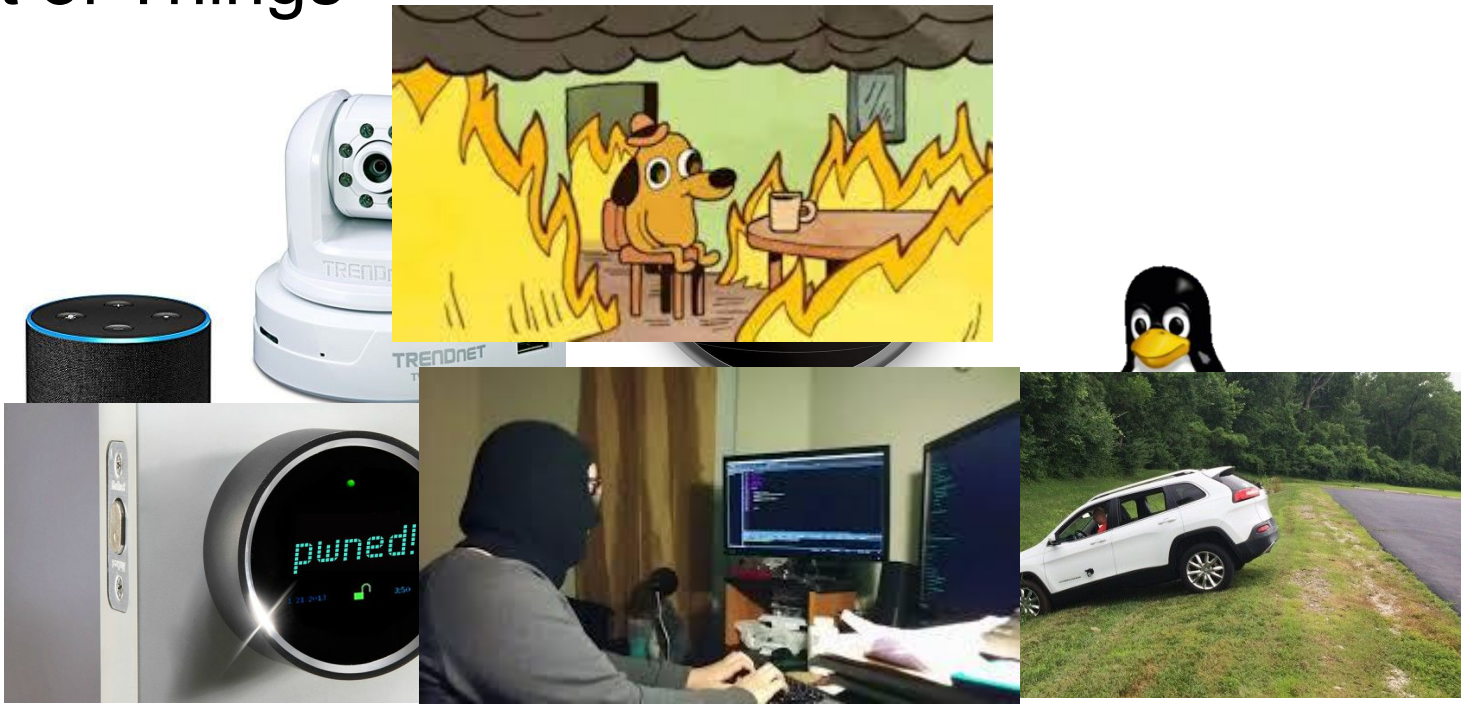
Internet of Things

Internet of Things

Internet of Things

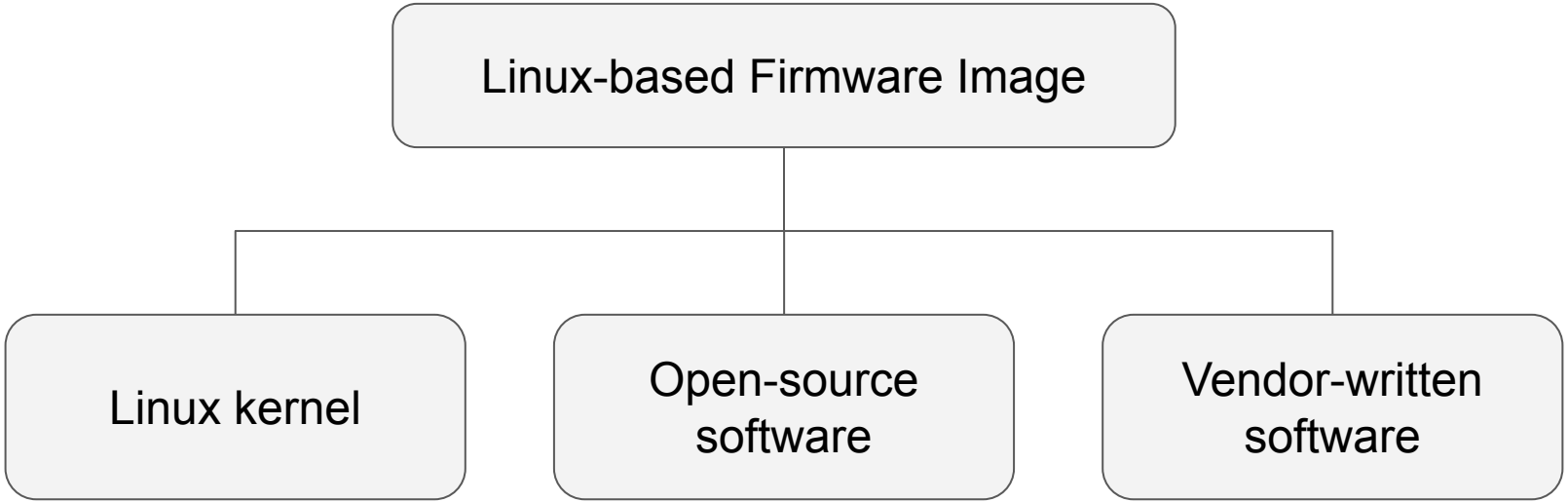
- 233 CVE’s assigned from Jan 2018 - Nov 2019

Internet of Things

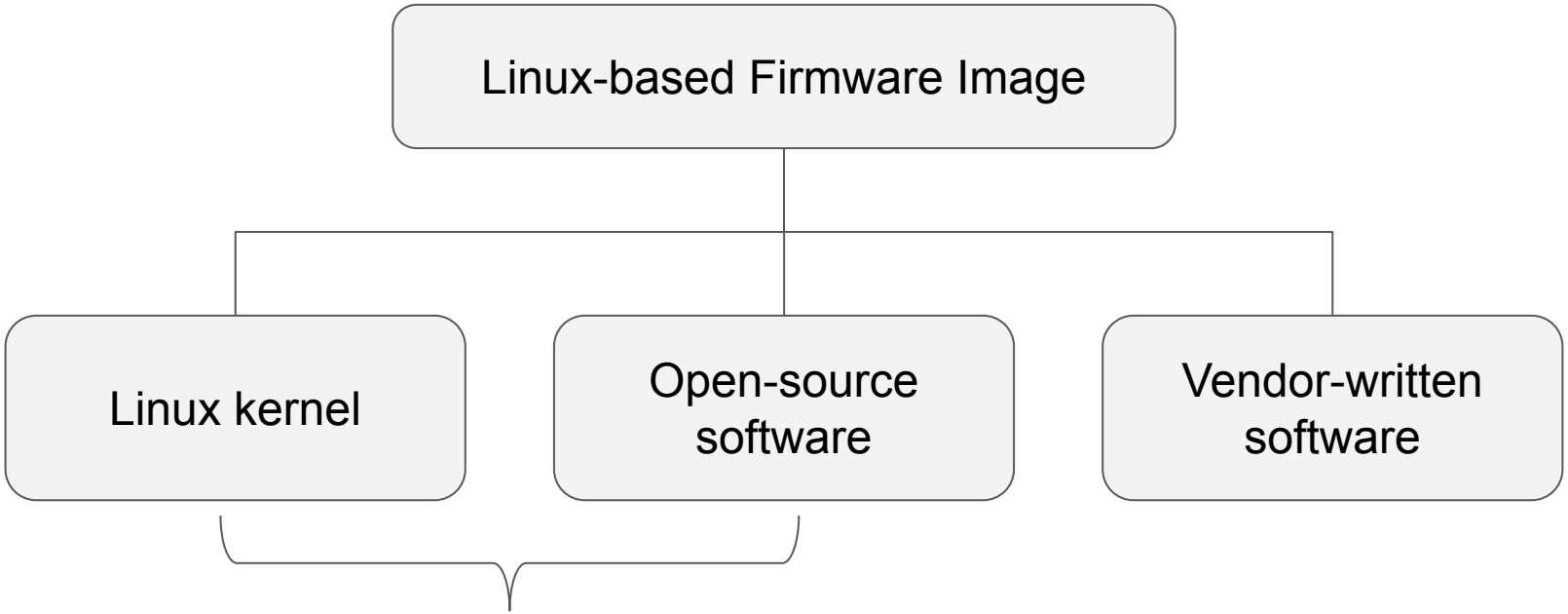


- 233 CVE’s assigned from Jan 2018 - Nov 2019

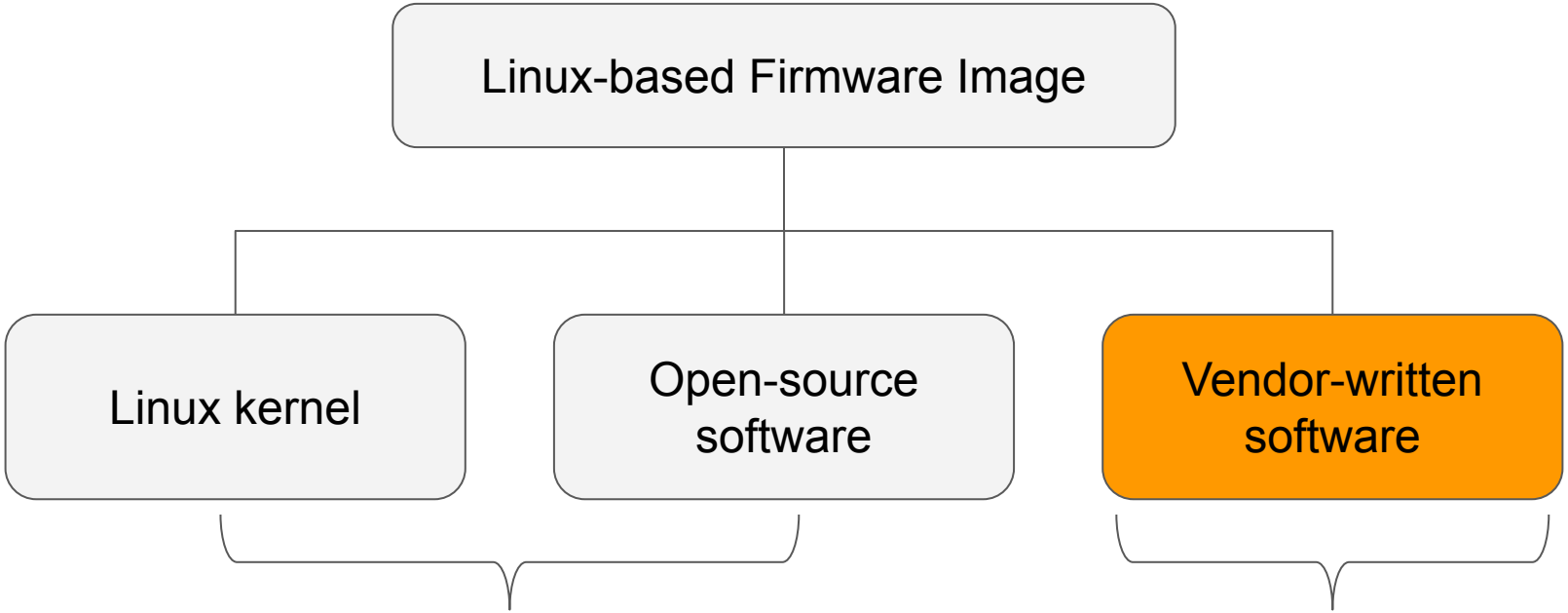
Fuzz Target


Linux-based Firmware Image
Linux kernel
Open-source software
Vendor-written software

Fuzz Target


Linux-based Firmware Image
Linux kernel
Open-source software
Vendor-written software
Can be independently analyzed

Fuzz Target


Linux-based Firmware Image
Linux kernel
Open-source software
Vendor-written software
Can be independently analyzed
~~Open-source~~
~~Openly analyzed~~

Deep Analysis

Challenges

Solutions

Deep Analysis

Challenges

Syntactically legal input generation

Solutions

Deep Analysis

Challenges

Syntactically legal input generation

Solutions

Utilize the web API

Deep Analysis

Challenges	Solutions
Syntactically legal input generation	Utilize the web API
Fine-grained vulnerability monitoring	

Deep Analysis

Challenges	Solutions
Syntactically legal input generation	Utilize the web API
Fine-grained vulnerability monitoring	Monitor injection into runtime environment

Deep Analysis

Challenges	Solutions
Syntactically legal input generation	Utilize the web API
Fine-grained vulnerability monitoring	Monitor injection into runtime environment
Device-independent dynamic analysis	

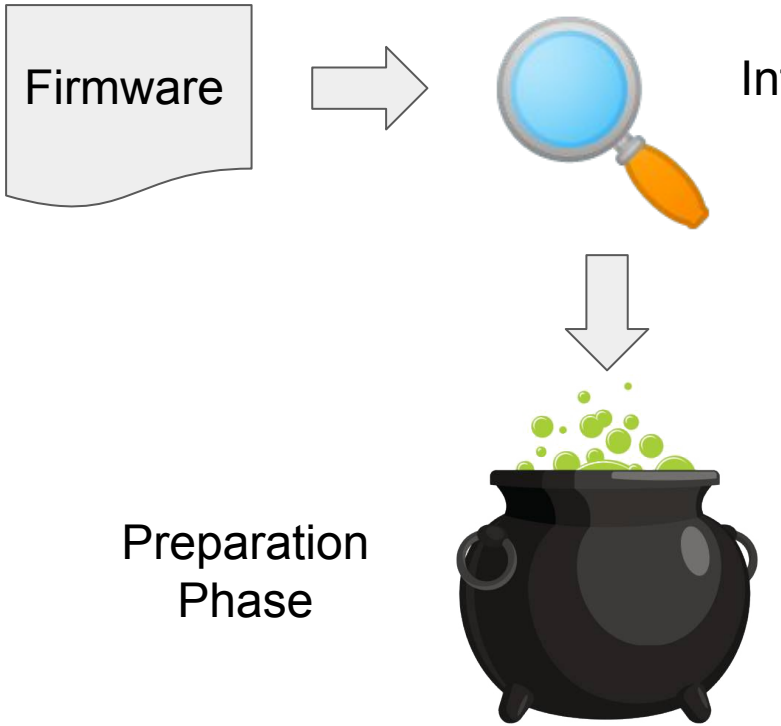
Deep Analysis

Challenges	Solutions
Syntactically legal input generation	Utilize the web API
Fine-grained vulnerability monitoring	Monitor injection into runtime environment
Device-independent dynamic analysis	Full-system emulation of firmware image

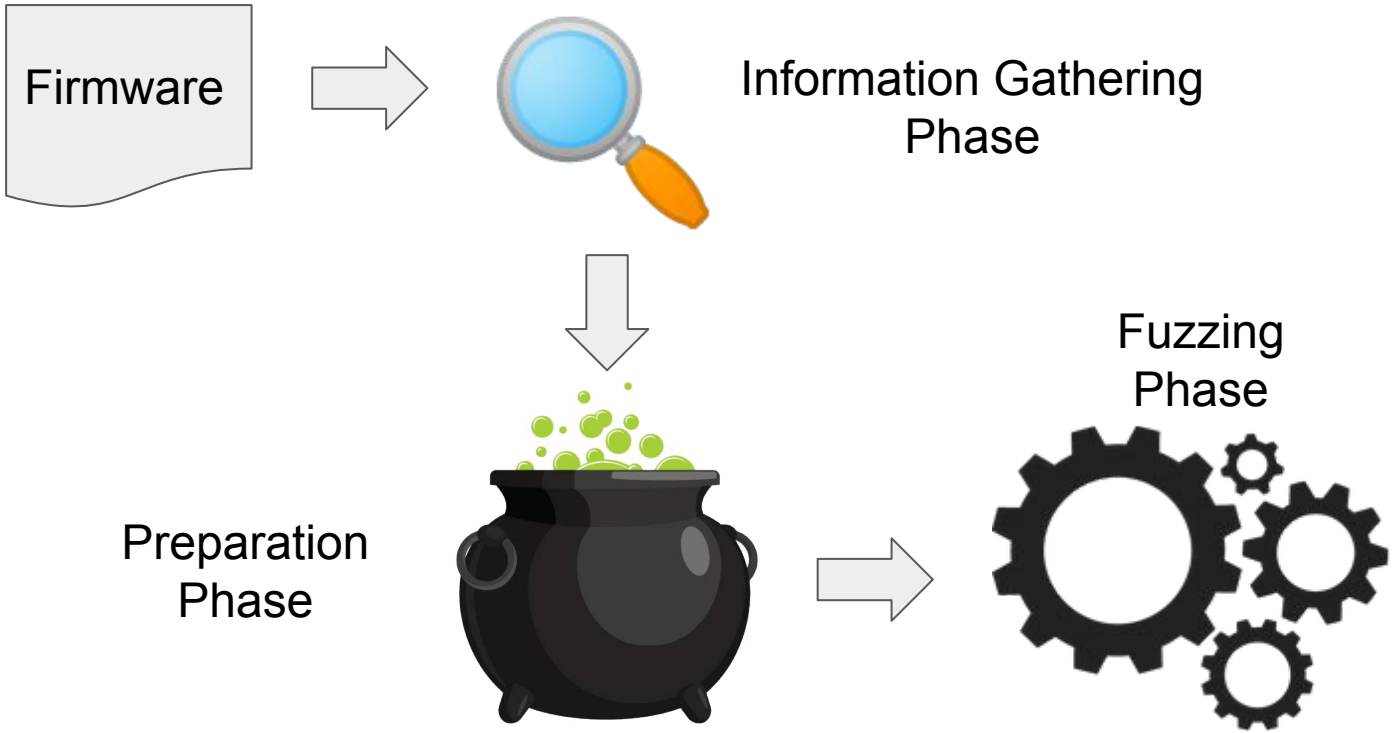
FirmFuzz Design

FirmFuzz Design

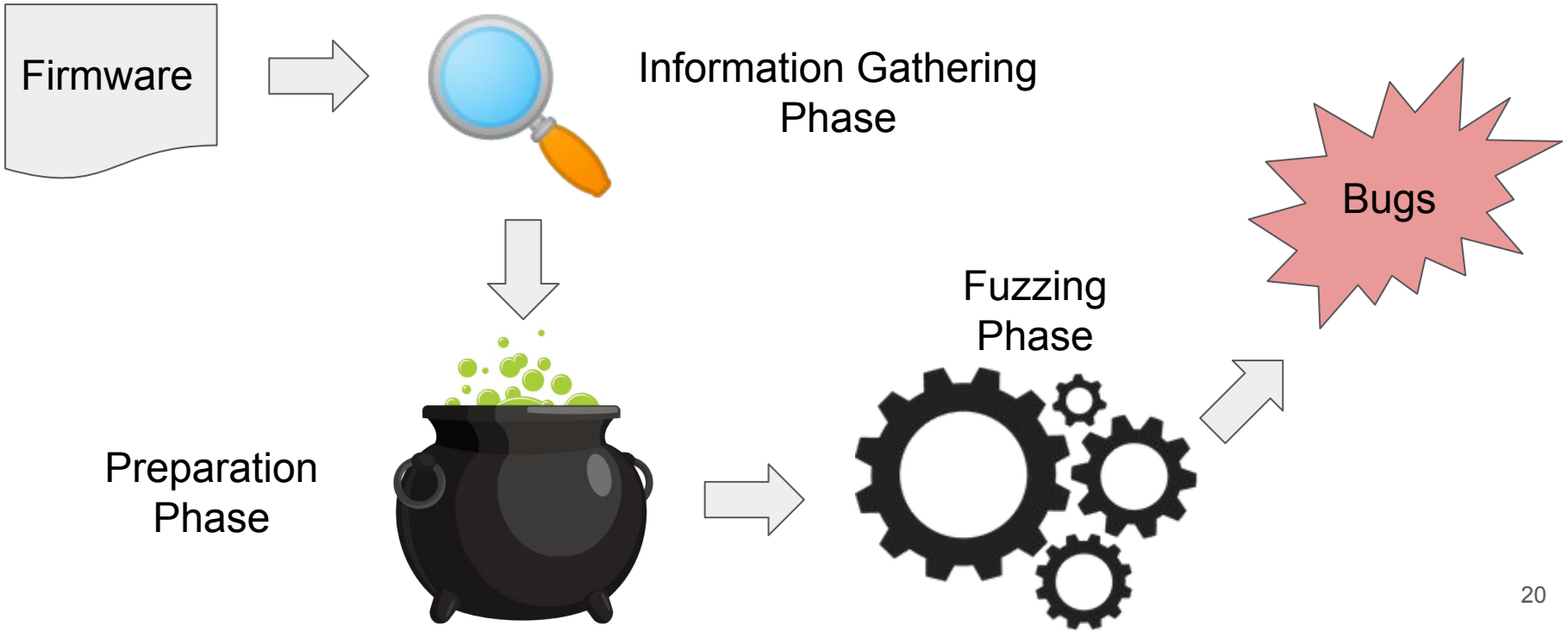
FirmFuzz Design



FirmFuzz Design



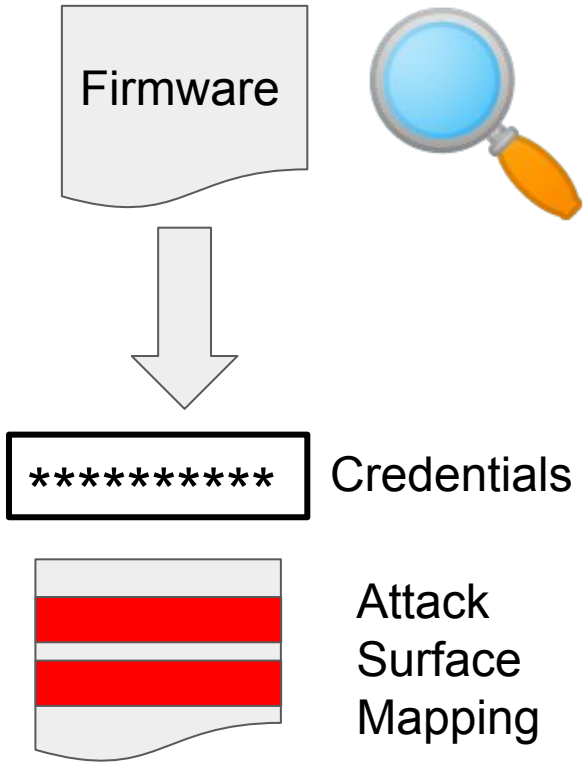
FirmFuzz Design



Information Gathering Phase

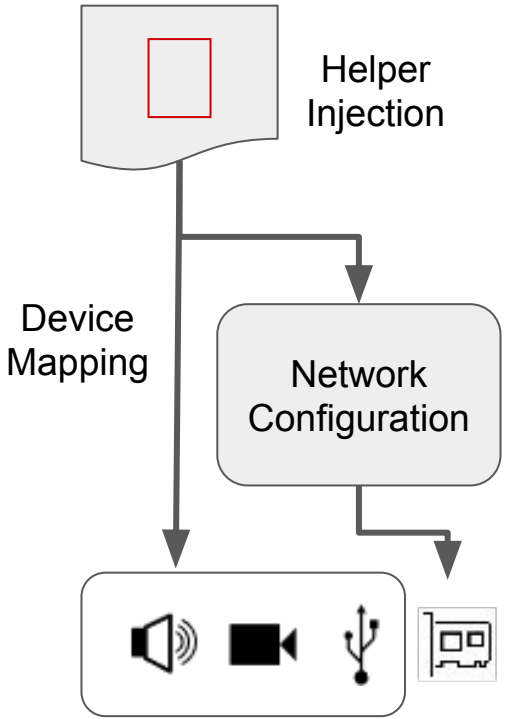
- Discover authentication credentials
  - Increase fuzzer coverage

- Static analysis of PHP scripts
  - Find inputs for vulnerable code paths
  - Perform taint analysis to build input constraints



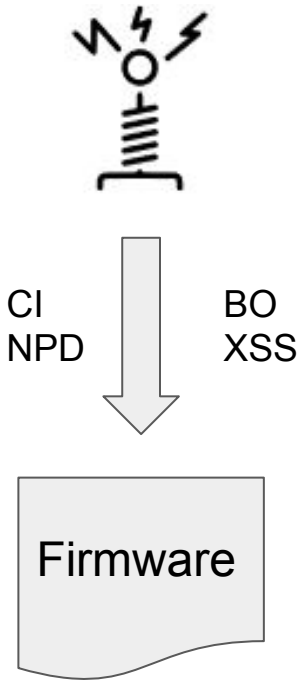
Preparation Phase

- Helper injection
  - Allows FirmFuzz to perform fine-grained vulnerability monitoring
    - CI — Helper binaries
    - BO, NPD — Exception handling mechanism of the kernel
    - XSS — Host-side monitoring
- Peripheral mapping
  - Firmware may require unsupported peripherals during runtime
  - FirmFuzz automatically creates mappings to a *fake* peripheral
- Network configuration
  - FirmFuzz logs interactions with the kernel networking interface
  - Creates an appropriate virtual network configuration

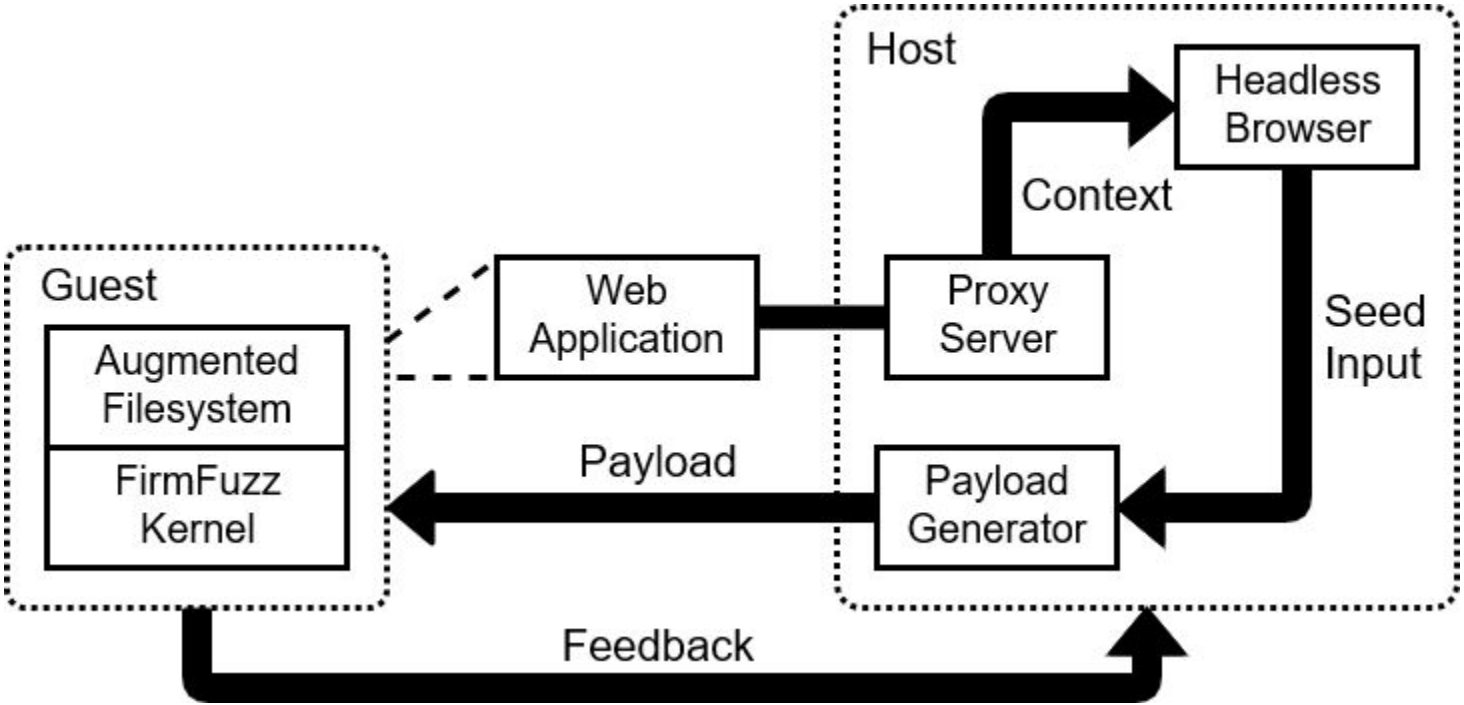


Fuzzing Phase

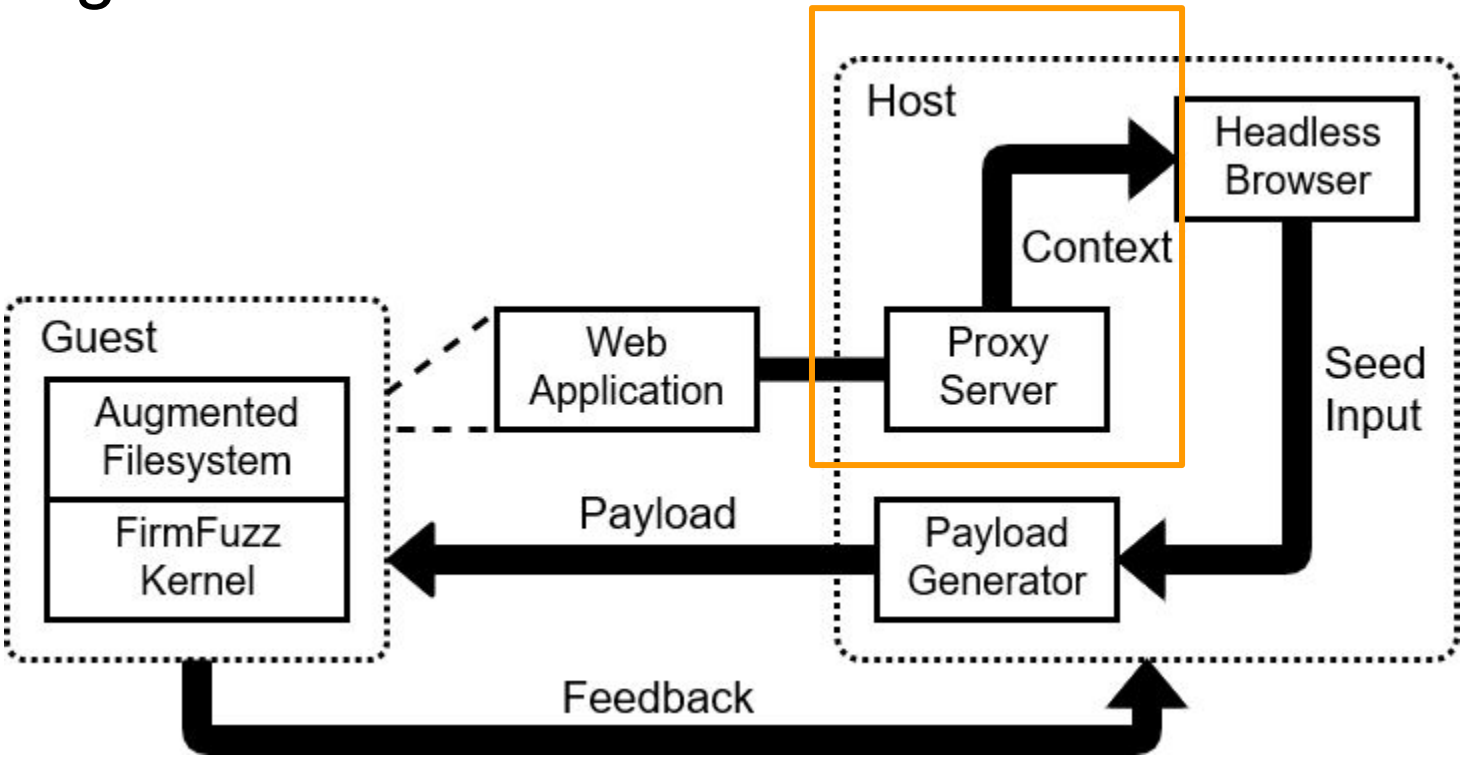
- Syntactically legal input generation
  - Use headless browser for interaction with web API
- Deterministic vulnerability detection
  - Leverage runtime monitors for vulnerability detection
- Fuzzing side-effects elimination
  - Use snapshots to revert firmware to a consistent state
- Payload delivery
  - Bypass web API validation checks by generating raw requests



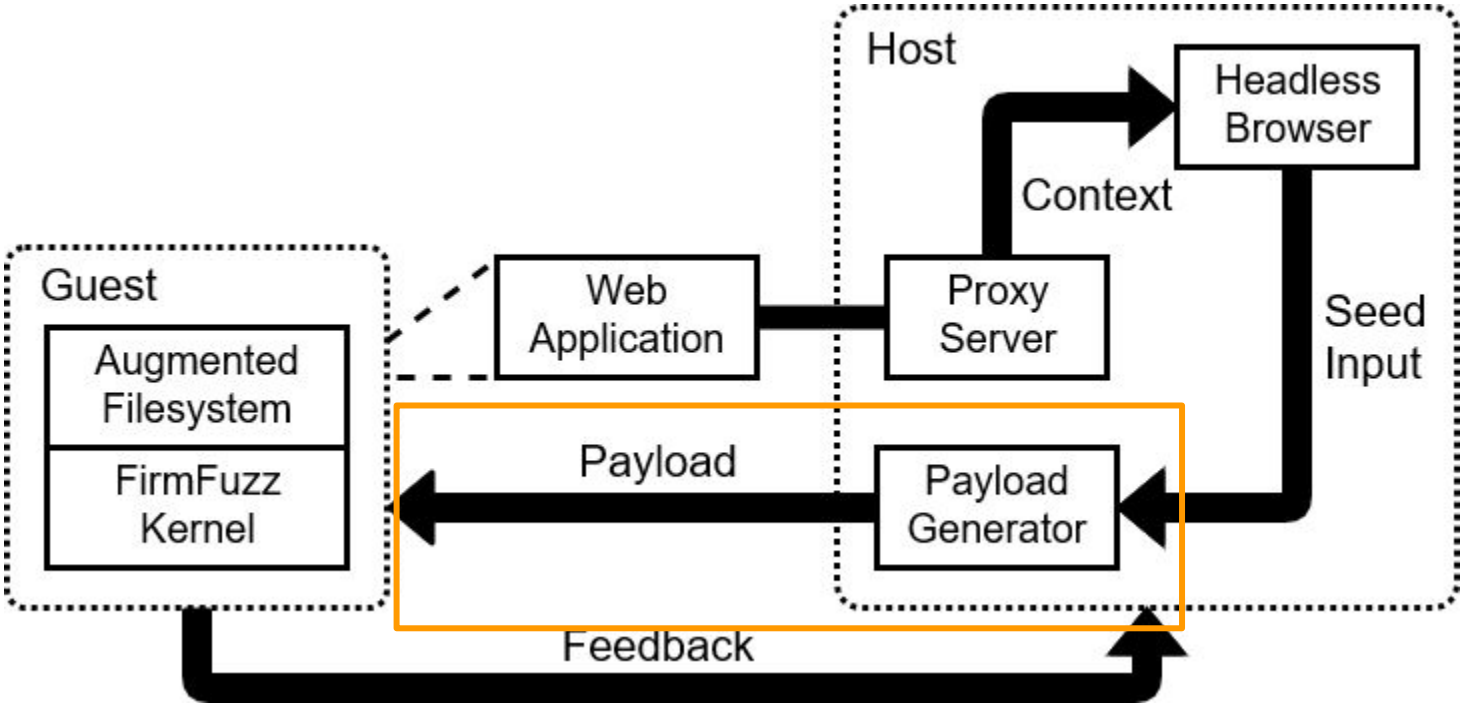
Fuzzing Workflow



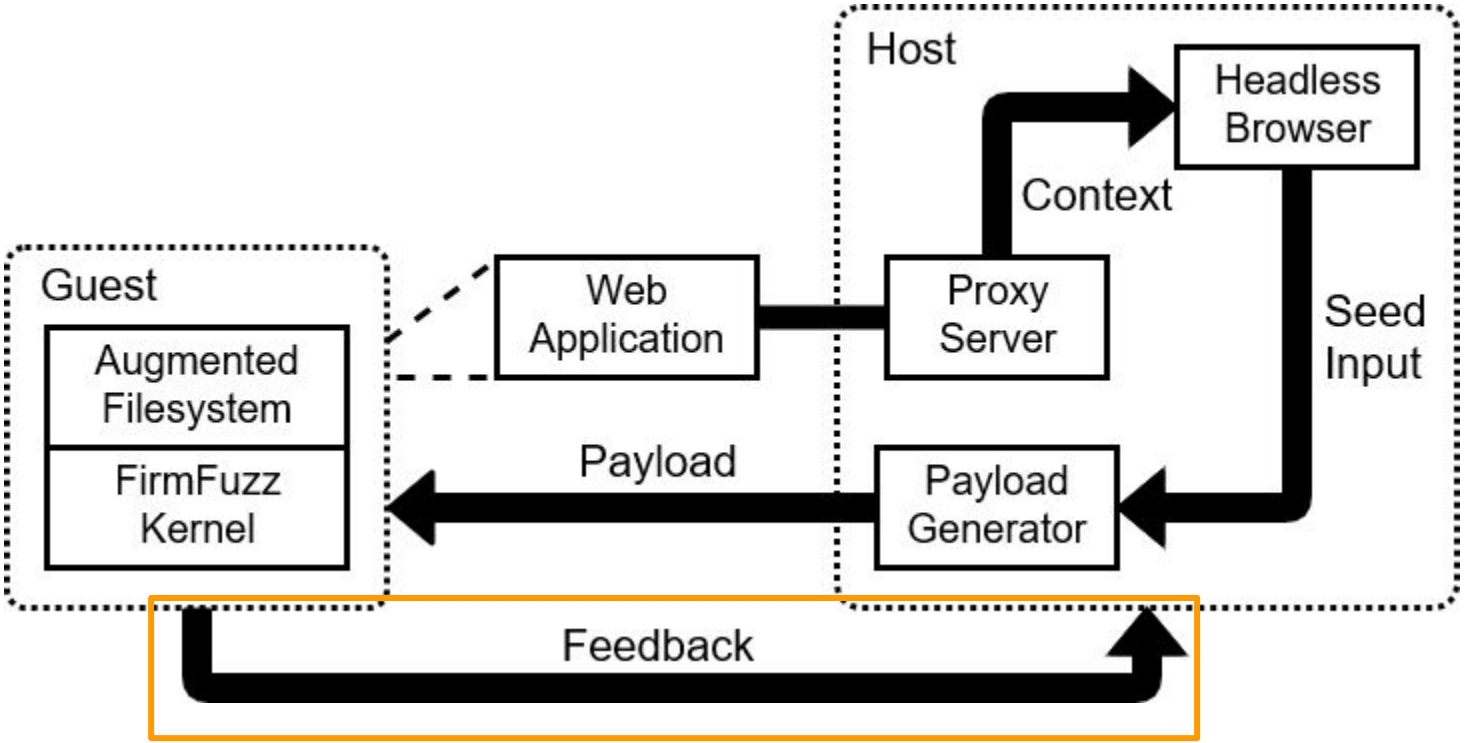
Fuzzing Workflow



Fuzzing Workflow



Fuzzing Workflow



Evaluation

- Analyzed 6427 firmware images scraped from three vendors
- Found 7 vulnerabilities across 6 different devices
- Average runtime for the fuzzing phase was 16.7 minutes

Firmware Image Breakdown

Vendor	**Network Inferred**	**Fuzzed (Unique Devices)**	**Unique Web UI**
TRENDnet	26	6 (5)	2
Netgear	162	20 (17)	3
D-Link	15	6 (5)	1
Total	203	32 (27)	6

Firmware Image Breakdown

Vendor	Network Inferred	Fuzzed (Unique Devices)	Unique Web UI
TRENDnet	26	6 (5)	2
Netgear	162	20 (17)	3
D-Link	15	6 (5)	1
Total	203	32 (27)	6

Sharp drop-off between network inferred and fuzzed images

Firmware Image Breakdown

Vendor	Network Inferred	Fuzzed (Unique Devices)	Unique Web UI
TRENDnet	26	6 (5)	2
Netgear	162	20 (17)	3
D-Link	15	6 (5)	1
Total	203	32 (27)	6

High reusability of web interfaces between different devices

Comparison Against Existing Work

Number	Vulnerability	CVE-ID	FirmFuzz	Web vulnerability scanners	Firmadyne
1	CI	CVE-2018-19239	✔	×	×
2	XSS	-	✔	✔	×
3	BO	CVE-2018-19242	✔	×	×
4	BO	-	✔	×	×
5	BO	CVE-2018-19240	✔	×	×
6	BO	CVE-2018-19241	✔	×	×
7	NPD	-	✔	×	×

Conclusion

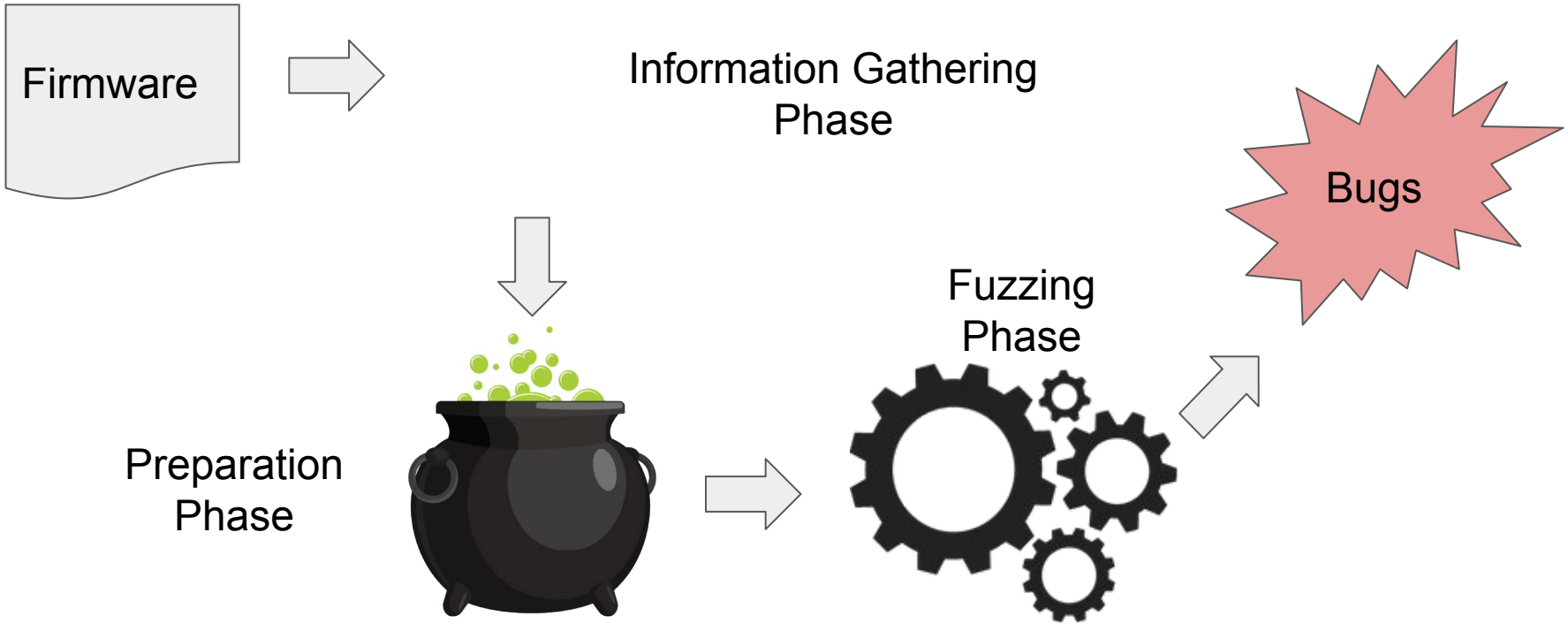
- We presented FirmFuzz, an automated dynamic analysis framework for finding deep vulnerabilities

- A generational fuzzer that leverages runtime monitors to aid the vulnerability discovery

- We found seven unknown vulnerabilities across six different devices

Questions ?

hexhive



Source code: https://github.com/Hexhive/Firmfuzz