CERIAS

The Center for Education and Research in Information Assurance and Security

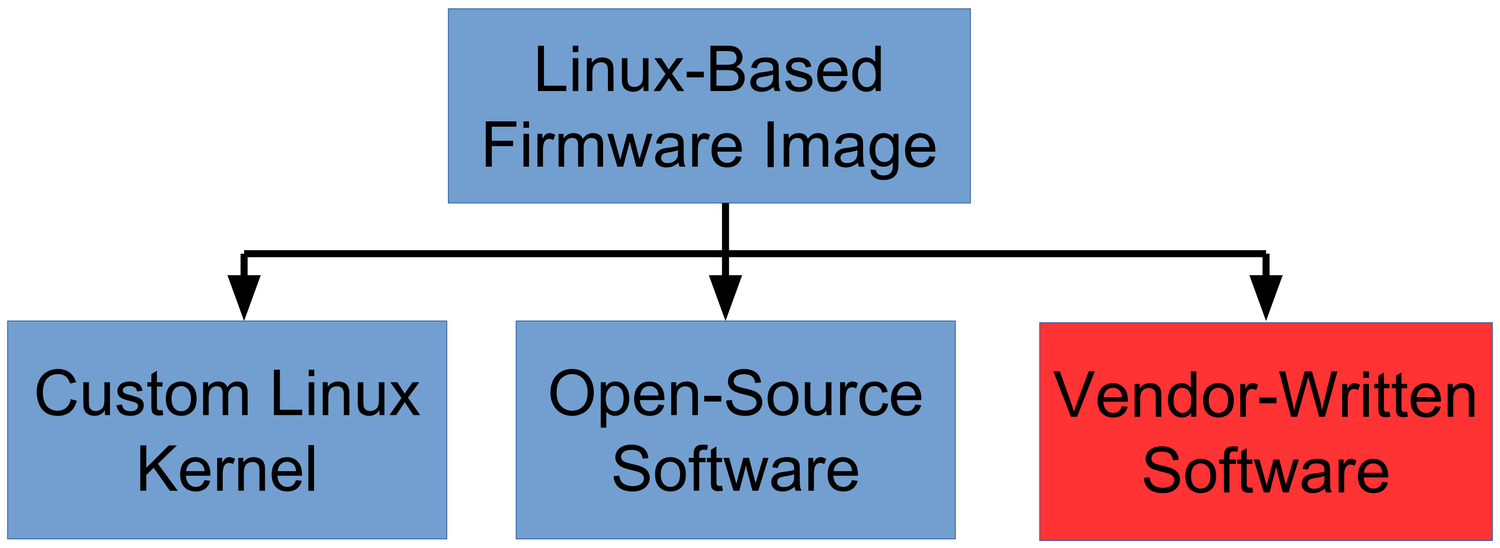
FirmFuzz: Automated IoT Firmware Introspection and Analysis

Prashast Srivastava[1], Hui Peng[1], Ryan Berg[2], Nathan Burow[1]
Howard Shrobe[2], Hamed Okhravi[2], Mathias Payer[1]
[1] *Purdue University* [2] *MIT*

Internet of Things

- 30 billion expected devices by 2020
- 142 vulnerabilities reported between Jan 2016 – Feb 2018

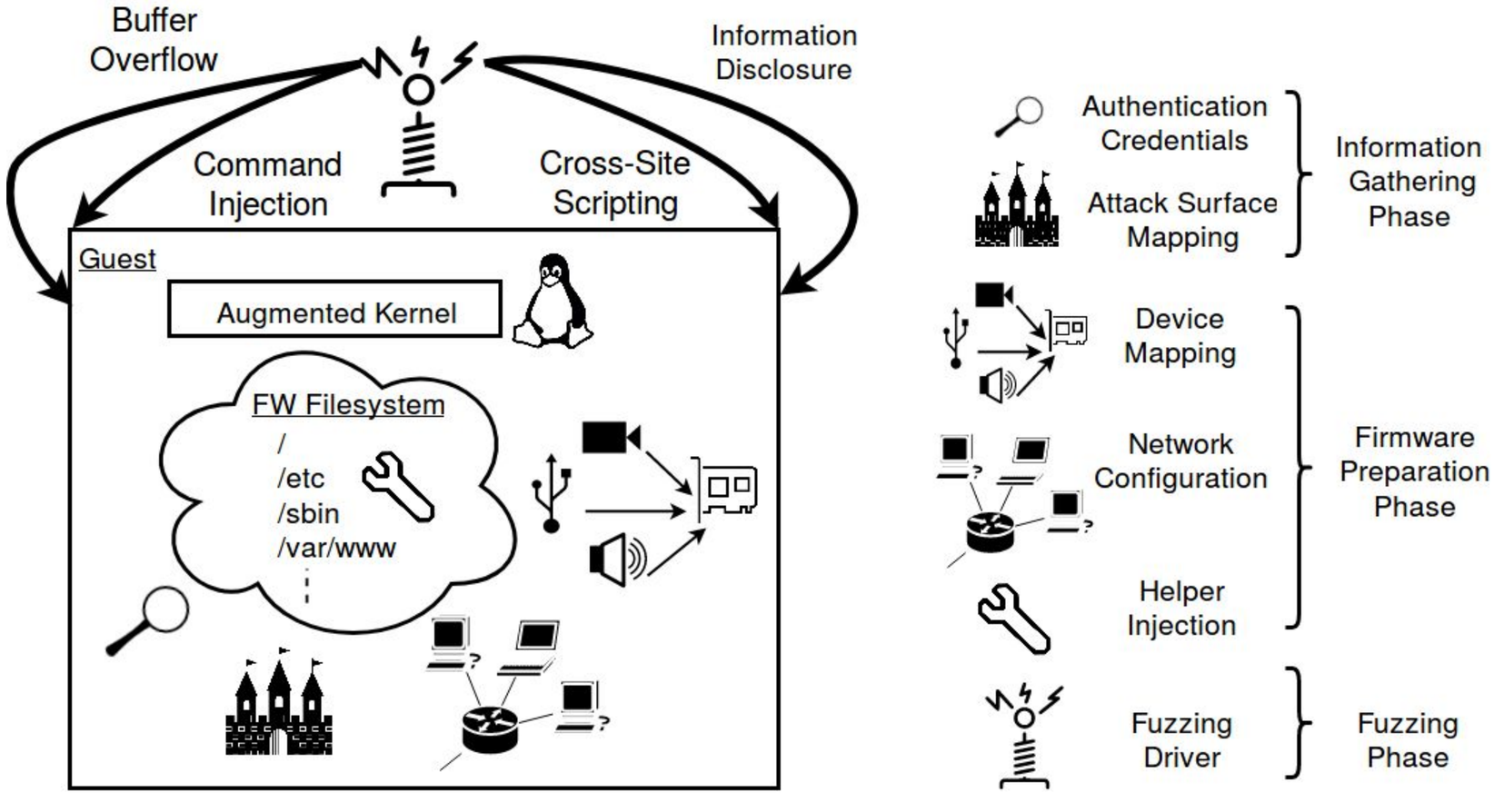
Attack Surface



Challenges

- Emulate the firmware image to remove device dependence
- Generate inputs targeted towards vendor-written SW

FirmFuzz Architecture



Vulnerability Detection Performance

Number	Vulnerability	Device	FirmFuzz	ZAP
1	Command Injection	TEW-673GRU	✓	✗
2	Reflected XSS	TEW-673GRU	✓	✓
3	Reflected XSS	TEW-673GRU	✓	✓
4	Buffer Overflow	TEW-673GRU, TEW-632BRP	✓	✗
5	Buffer Overflow	TV-IP110WN, TV-IP121WN	✓	✗
6	Buffer Overflow	TV-IP110WN, TV-IP121WN	✓	✗
7	Buffer Overflow	TV-IP110WN, TV-IP121WN	✓	✗
8	Reflected XSS	TV-IP121WN	✓	✓

Conclusion

- We presented FirmFuzz, an automated framework for emulation and fuzzing Linux-based firmware images
- We reported 8 previously undiscovered vulnerabilities across 4 different devices

PURDUE UNIVERSITY Discovery Park

CERIAS