RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SB1-R4

U-Boot, I-Hack

Carlota Bindner

Security Associate
Rapid7
@carlotabindner

Andrew Bindner

Manager, Penetration Testing
Rapid7
@schlpr0k

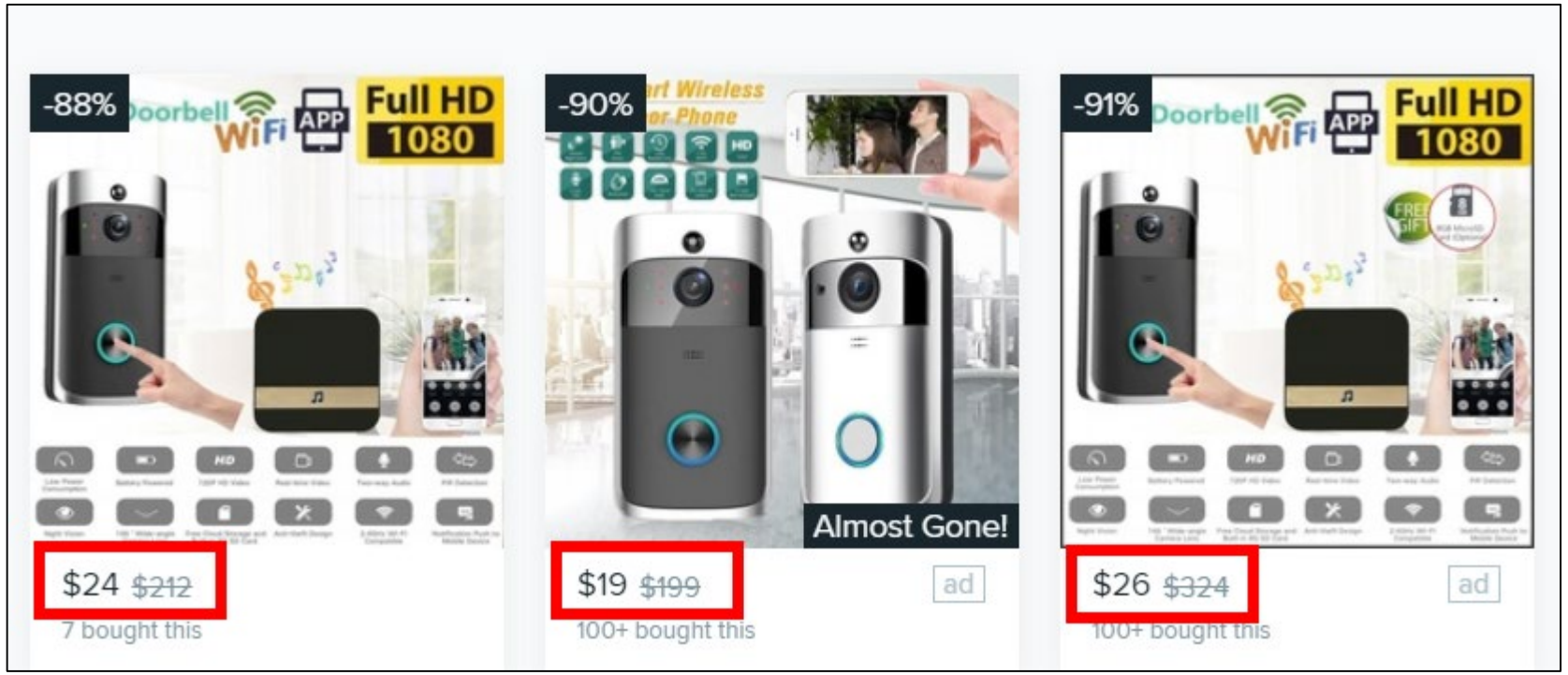
RSAConference2019

IoT Product Security

Risks IoT Product Security

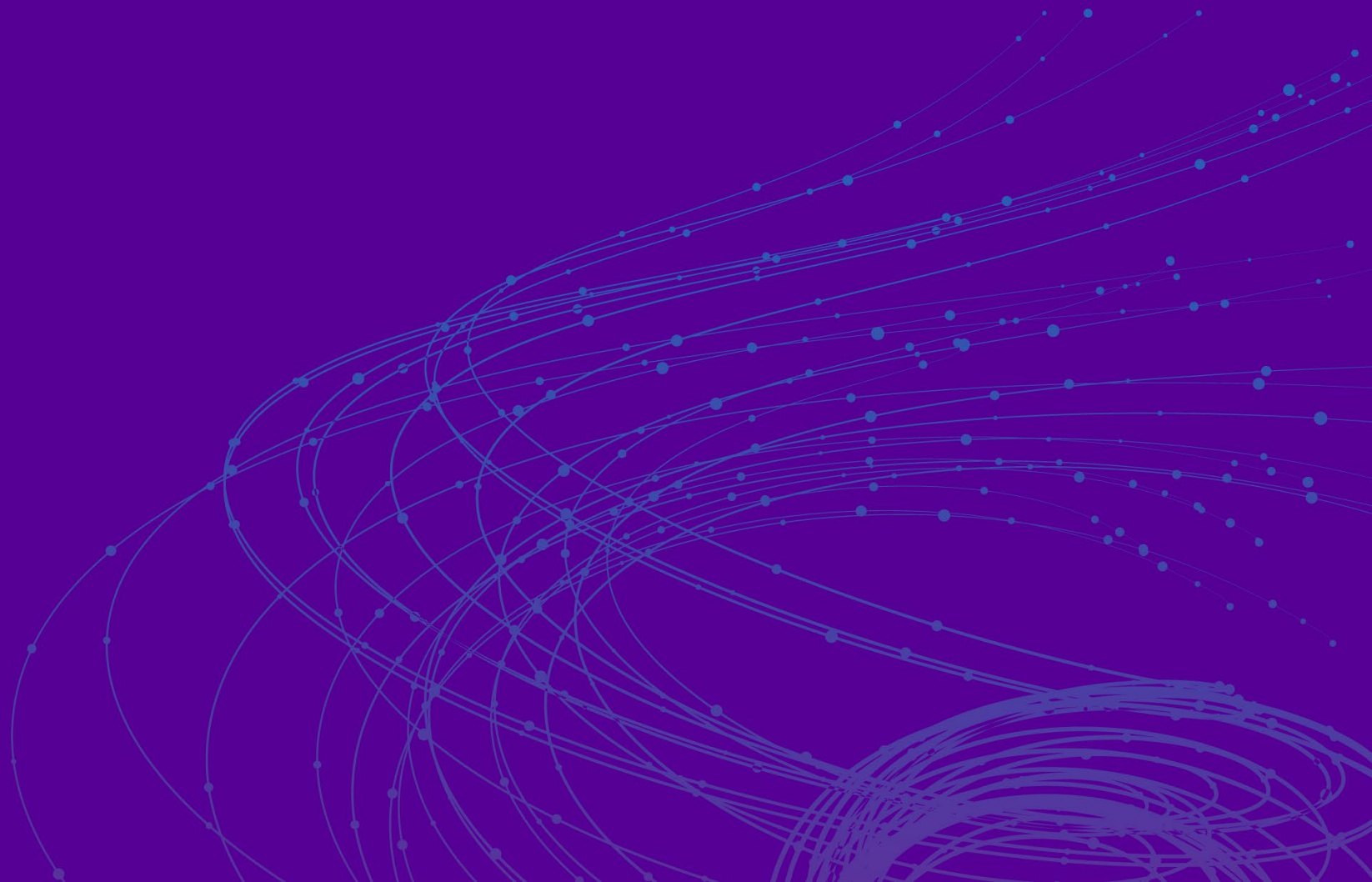
- How does your company approach product security?
- Is it effective?
- System and User Security Protections
- Intellectual Property

Intellectual Property



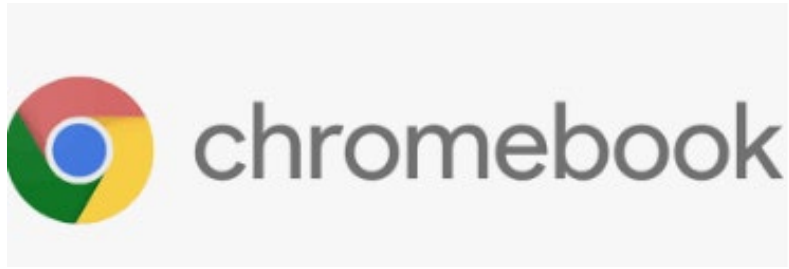
RSAConference2019

Das U-Boot

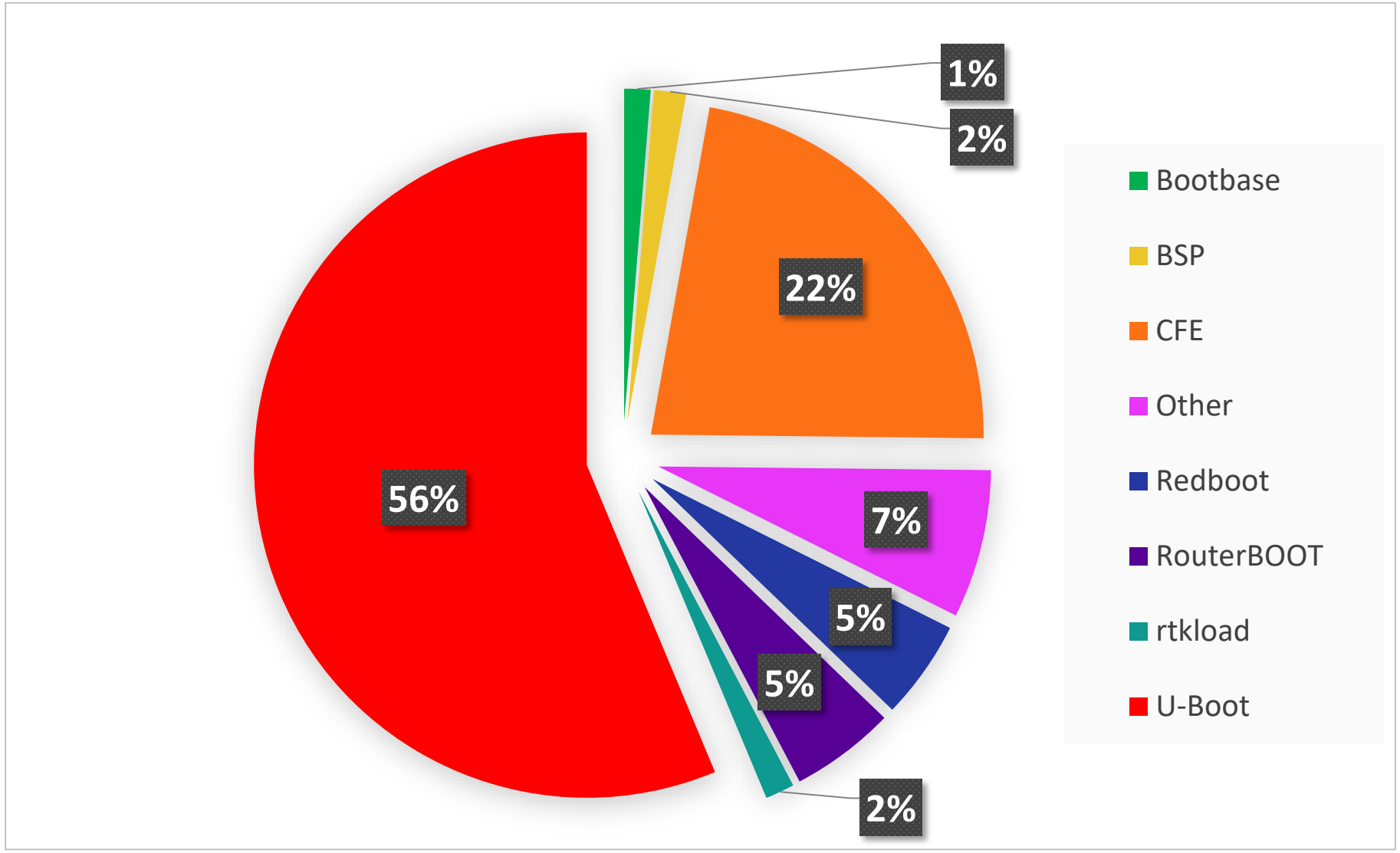


Why Attack U-Boot?

- Universal Boot Loader
- Multi-arch support
  - ARM, MIPS, x86, etc.
- Supports Onboard Storage
- Supports Serial Ports
- Network Boot Capability



Market Share



Source: https://wikidevi.com/wiki/Property:Stock_bootloader/full

Importance of Boot Loader Security

- Boot Loader Sits Outside of the Kernel
- Attack Surface:
  - Tamper with Firmware
  - Deny Firmware from Loading
  - Variable Manipulation
  - Start/Stop Services
  - Data Theft/Injection
  - Exploitation into other parts of the ecosystem

Demo #1 – Variable Manipulation

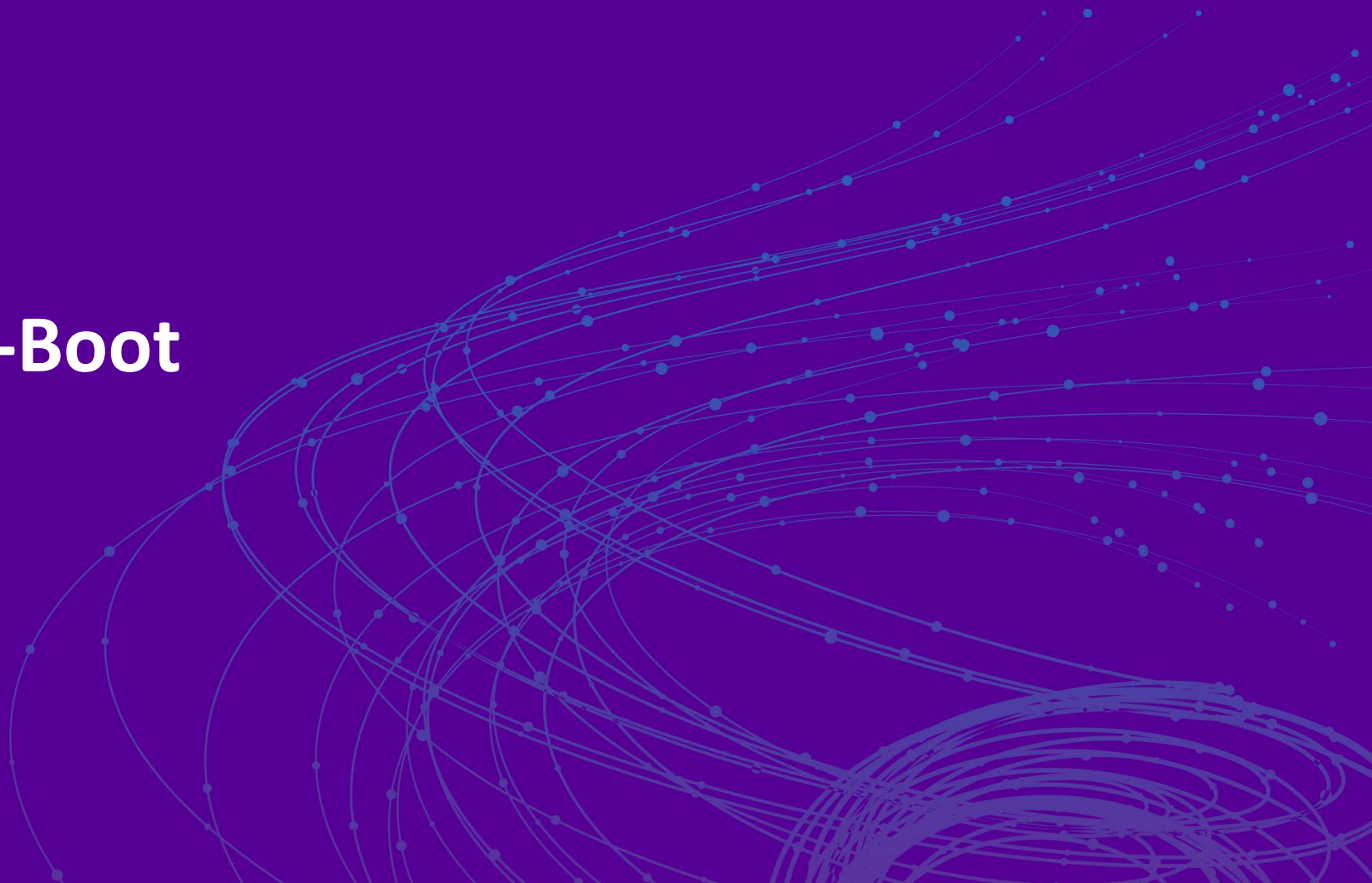
Demo #2 – TFTP Boot Manipulation

Impact of Accessing Firmware

- Stored Credentials
- Remote Sessions
- Controlling Other Devices
- Source Code
- API & Web App Info
- Potential Information Leakage
- Intellectual Property Loss

RSAConference2019

Hardening U-Boot



Establish Security During Development

- Physical Hardware Security Considerations
- Verified/Secure Boot
- Encryption
- Trusted Zones
- Review Security for Chip Data Sheets
- Disable Debug Interfaces *BEFORE* Production
- Other Ecosystem Protections

Follow-up Actions