

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: SB1-R4

U-Boot, I-Hack

Carlota Bindner

Security Associate
Rapid7
@carlotabindner

Andrew Bindner

Manager, Penetration Testing
Rapid7
@schlpr0k

RSA®Conference2019

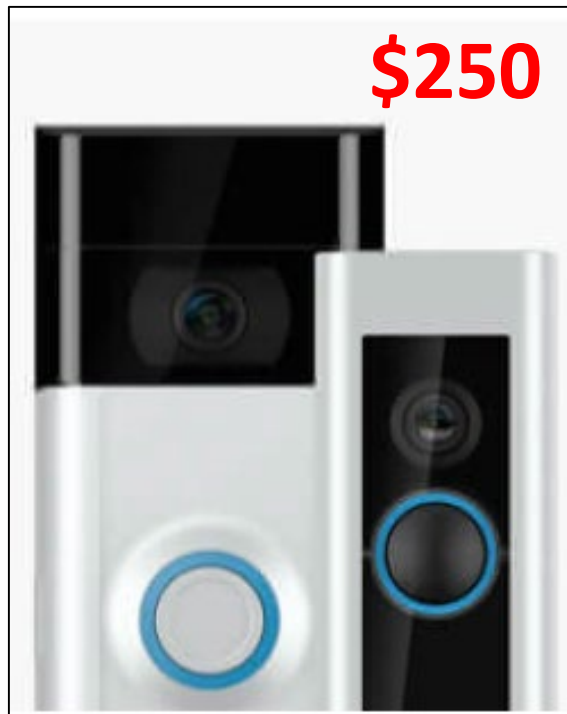
IoT Product Security



Risks IoT Product Security

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

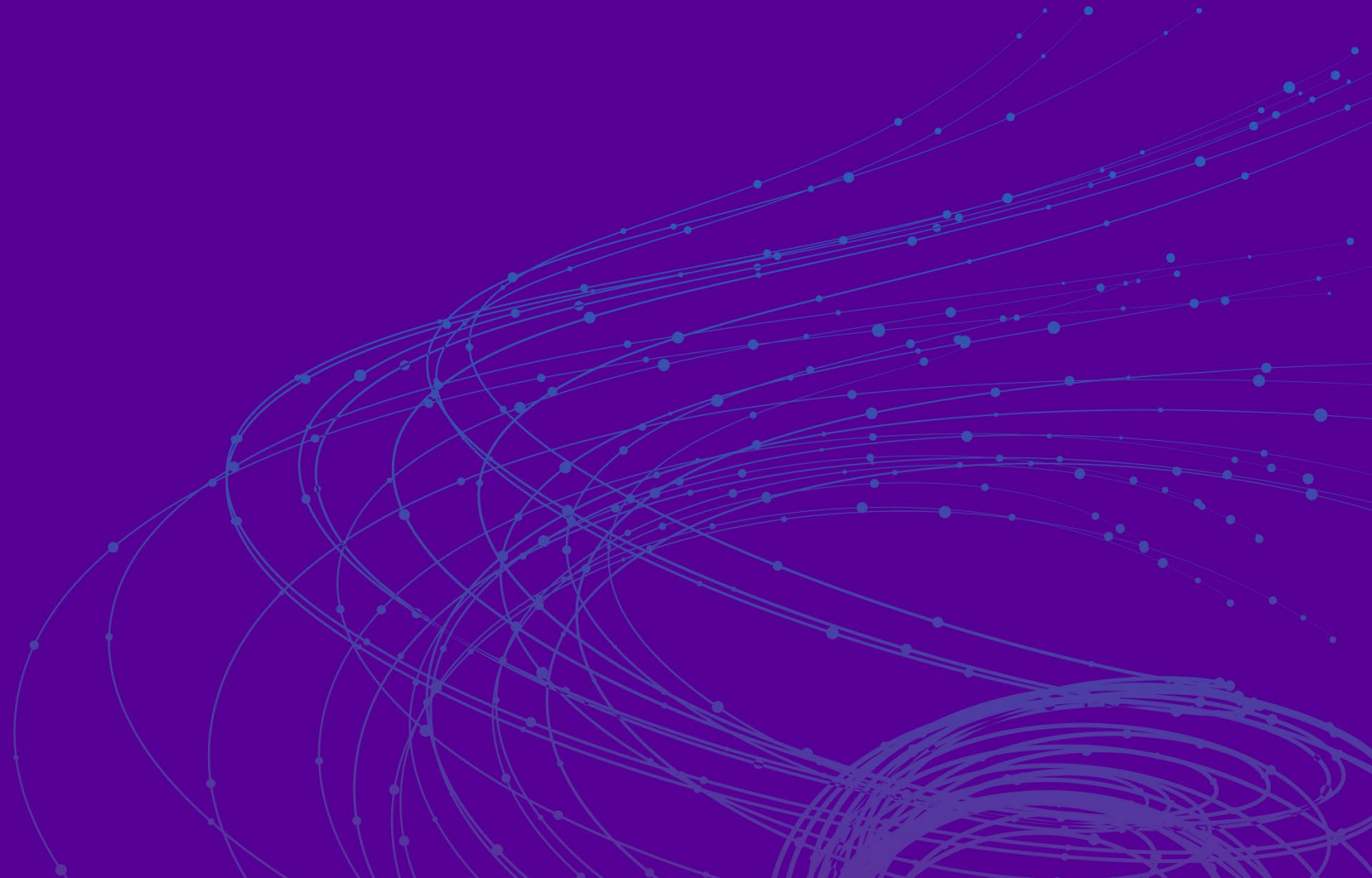
Intellectual Property



The image shows three Amazon product listings for doorbell cameras. Each listing includes a discount percentage, product features, and a price tag with the original price crossed out. The first listing shows a -88% discount with a price tag of \$24 (was \$212) and 7 purchases. The second listing shows a -90% discount with a price tag of \$19 (was \$199) and 100+ purchases, including the text 'Almost Gone!'. The third listing shows a -91% discount with a price tag of \$26 (was \$324) and 100+ purchases. All listings feature icons for 'Doorbell', 'WiFi', 'APP', and 'Full HD 1080'. A vertical purple line is positioned to the left of the listings.

RSA®Conference2019

Das U-Boot

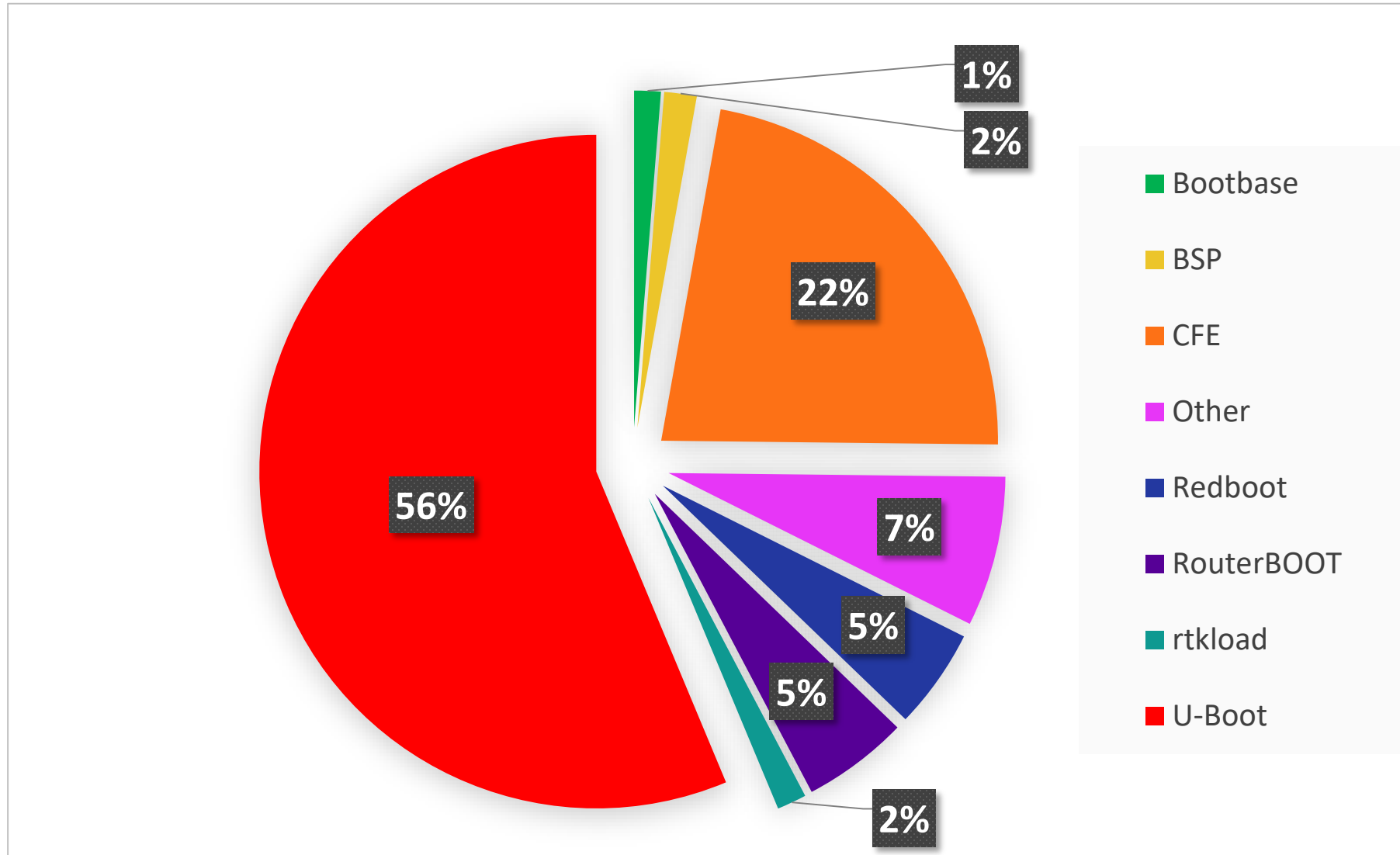


Why Attack U-Boot?

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



Market Share



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

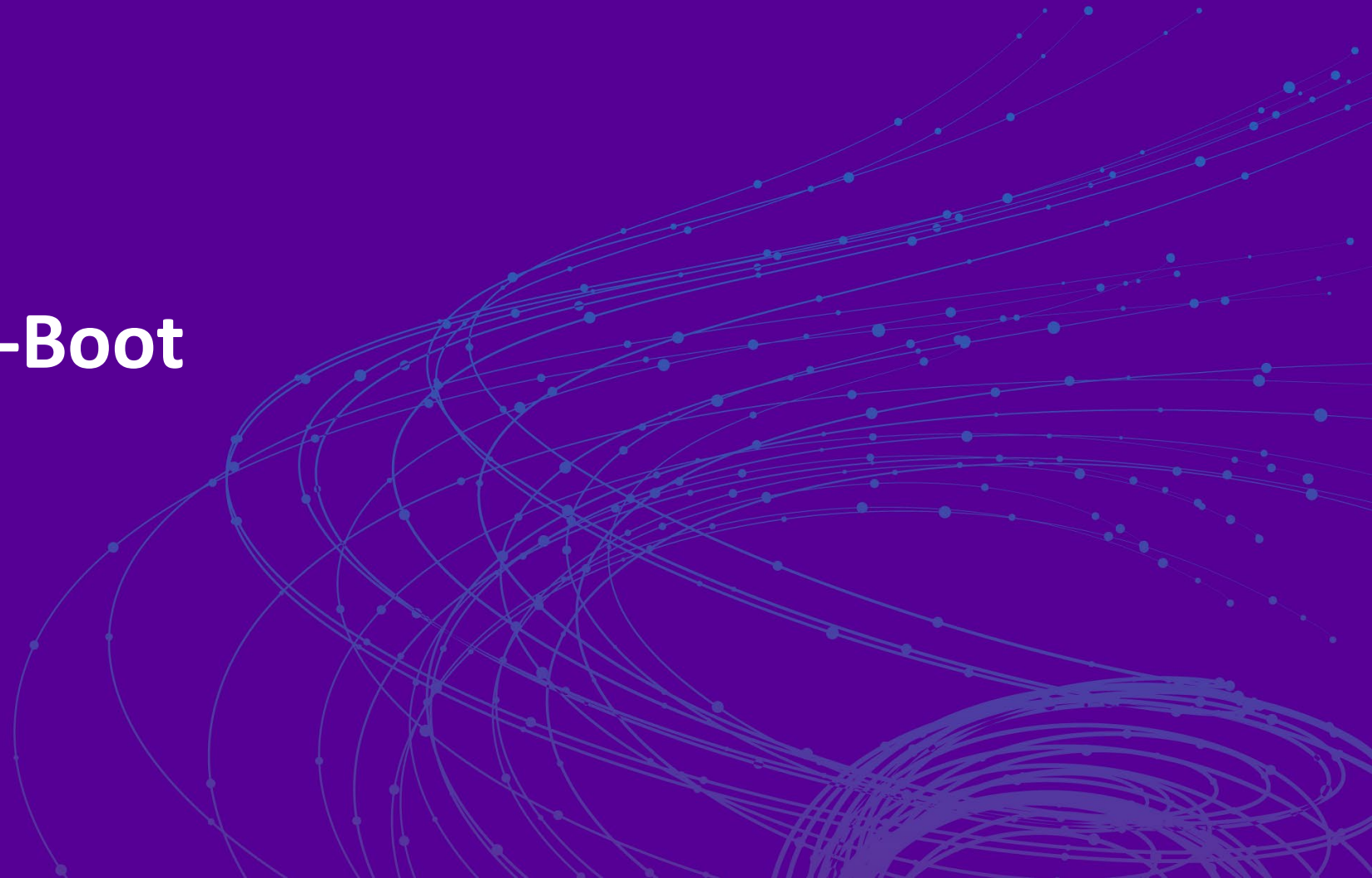
Impact of Accessing Firmware

- 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

| | Management | Development |
|---|-------------------------------------|-------------------------------------|
| • Life Cycle & Regular Review | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| • Develop Internal Policies & Checklists | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| • Enable Verified/Secure Boot | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| • Implement Encryption | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| • Protect Firmware in Transit and at Rest | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| • Ecosystem Security Assessment | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |