

Crypto for Constrained Devices

SESSION ID: MASH-W04A



Ray Potter

CEO
SafeLogic
@SafeLogic_Ray



Whitfield Diffie

Technical Advisor
SafeLogic



Crypto in Constrained Devices

- ◆ 2013: NSA publication of Simon and Speck algorithms
- ◆ Conspiracy Theories
- ◆ Growing prevalence of constrained devices



Crypto in Constrained Devices

Use Case: Wearables



Crypto in Constrained Devices

- ◆ Use Case: Constrained Devices
 - ◆ Industrial
 - ◆ Consumer



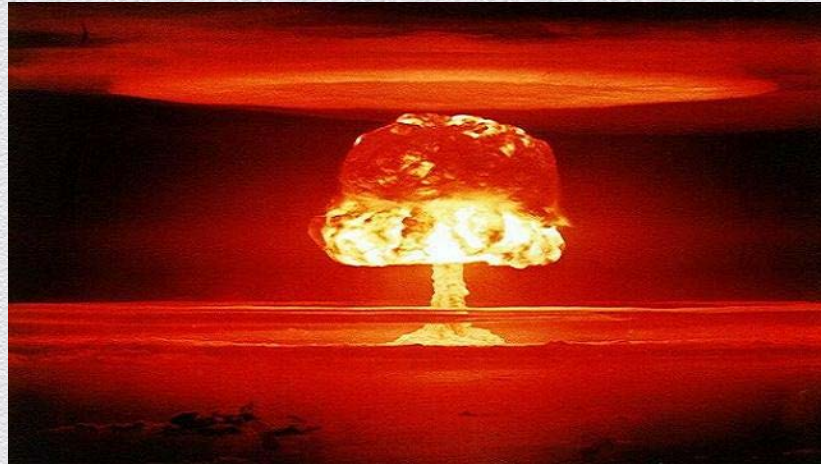
Crypto in Constrained Devices

- ◆ Challenges
 - ◆ Space Constraints
 - ◆ Performance Standards
 - ◆ Validation



Crypto in Constrained Devices

Without strong cryptography in these use cases, what would happen?





RSA[®]CONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Thanks!

**Come chat with us
directly after this
at Booth #1809**