Rambus

Securing the Infrastructure

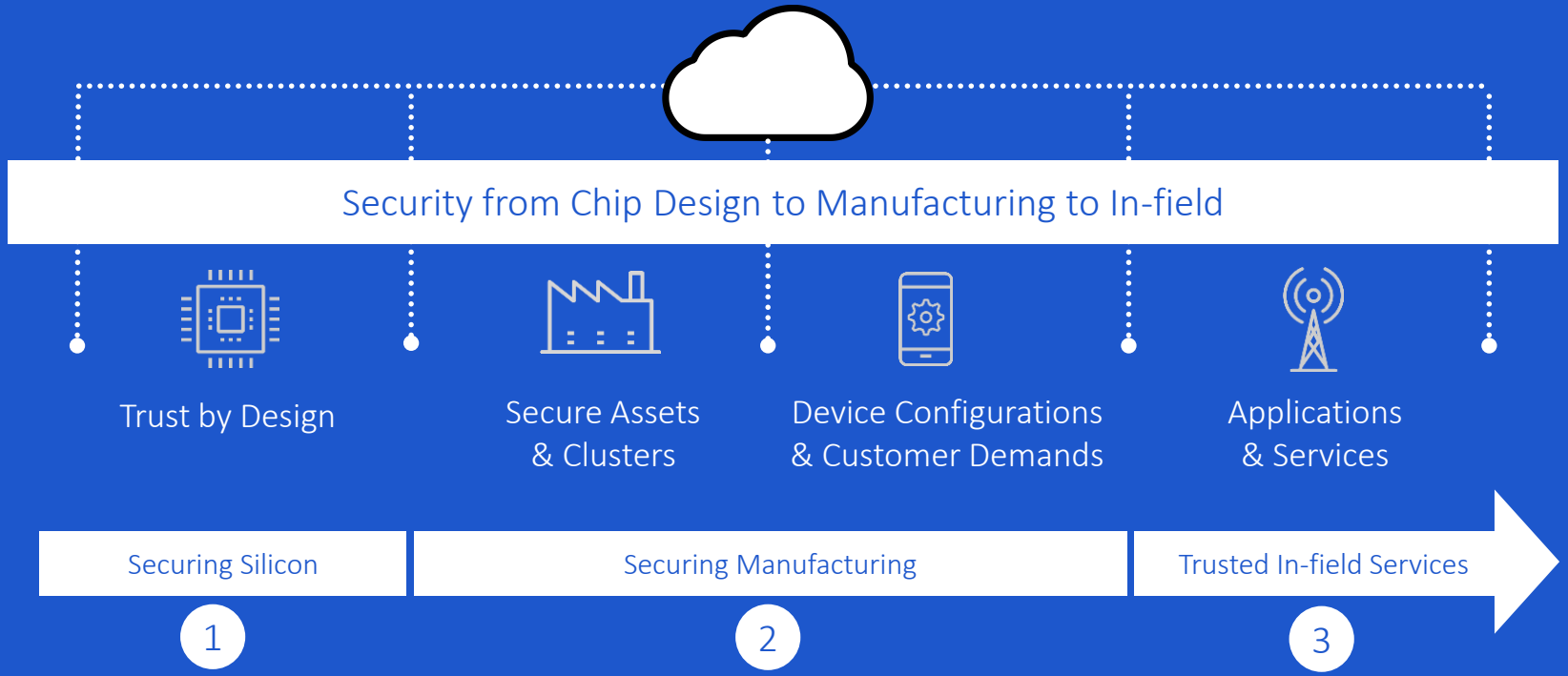
Neeraj Paliwal
VP of Products

18 June 2019

Securing the Infrastructure : Problem Statement

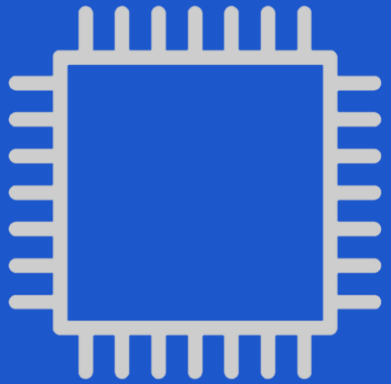
- Infrastructure = Smart Connected Devices
- Cloning and counterfeiting are on the rise
- Systems and people are at risk by grey market chips
- Lack of robust controls and audit capabilities risk revenue
- People make mistakes; some steal
- Lifecycle management of devices can be compromised

Securing the Infrastructure : The Solution



Securing Infrastructure Part 1: Securing Silicon

- CPU Performance optimized for speed
- Increased complexity leads to security flaws
- Change the paradigm from "security vs complexity" to "security by design"
- Starts with a Hardware Root of Trust
- Siloed security co-processor



Securing Infrastructure Part 2: Securing Manufacturing

- Chip/device security can only be as good as manufacturing security
- Ensure chips have a unique and immutable identity
- Trust must be placed in robust provisioning systems
- Every chip and device must be provided with a trusted identity
- Identity must be cryptographically bound to the chip ID
- Secure internal facilities, contract manufacturers, and the cloud
- Starts at the fab and extends throughout the value chain

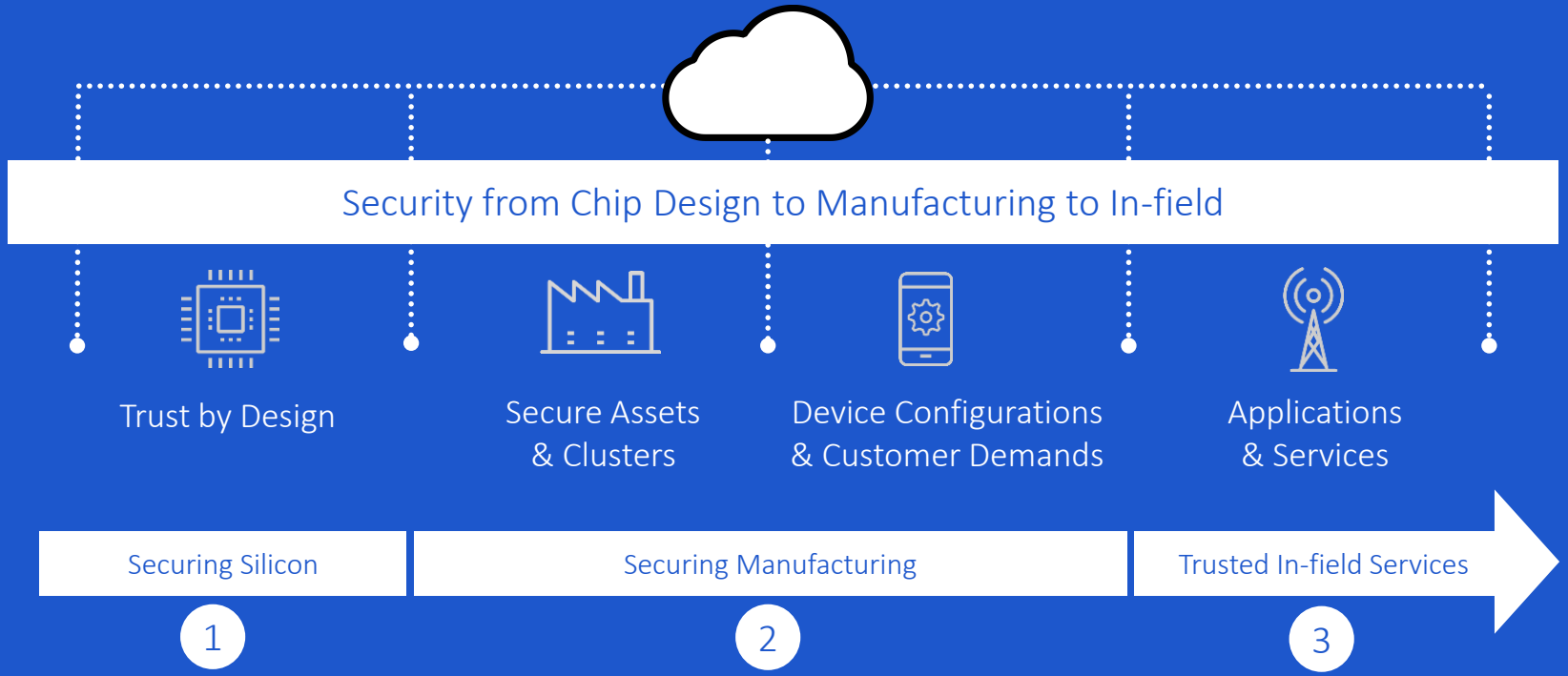
Securing Infrastructure Part 2: Securing Manufacturing

- Don’t take shortcuts – follow a proven recipe for secure manufacturing
- Establish trust in the chain of custody of provisioned keys and data
- Robustly protect all high-value keys and associated data
- Remove the human element from provisioning security
- Cryptographically bind all chip ID data and provenance to its unique keys
- Stay within the secure boundary of hardware security modules (HSMs)
- Secure audit and logging mechanisms down to individual transactions
- Ensure uploaded information is shielded from tampering

Securing Infrastructure Part 3: Trusted In-Field Services

- You can’t trust data from a device if you can’t trust the device itself
- Strong authentication & attestation are the foundation of ecosystem trust
- Securely provisioned keys are the foundation of a trusted supply chain
- Enable a chip or device to authenticate itself with cloud key management
- Trusted attestation enables a suite of product security features

Securing the Infrastructure : The Solution



Thank you

Neeraj Paliwal
linkedin.com/npaliwal

Rambus
Data · Faster · Safer