RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SSC-W07

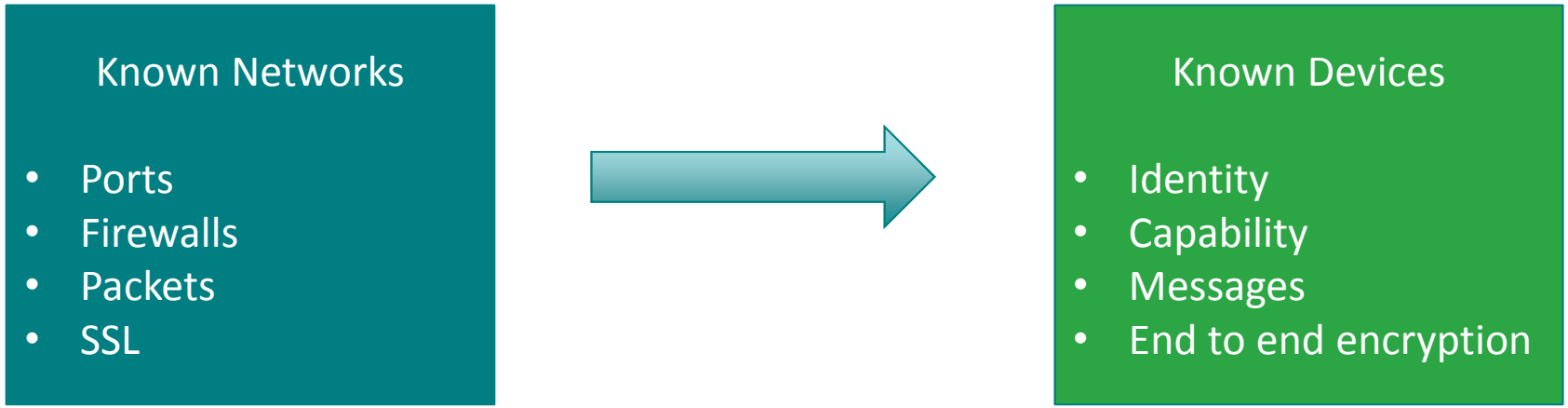
How I Learned to Stop Worrying and Love the Internet of Things

Steven Sprague

CEO
Rivetz Corp
@skswave

#RSAC

The Big Shift



The Problem

- Known networks but un-known devices
  - User centric architecture – Password, Tokens, Smartcards
  - User identity shared to multiple unknown devices
    - Phones, tablets, PC…cameras, doors, industrial controllers
  - Content delivered to unknown devices
  - Content creation on unknown devices
  - Content theft by malicious devices

Going mobile and moving to the cloud

- Devices have left the building
- Applications have left the building
- Everywhere anytime compute

Driving a shift to application security and content security

A network of known devices

The anatomy of a known device

- Hardware assured identity
- Trusted execution
- Trusted user Interface/ secure input
- Supply chain integrity / device health

Hardware Assured Identity

- Software tamper proof identity for all devices
- Multiple identities with proper privacy protection
- Multiple technical solutions
  - TPM – Trusted Platform Module (2.5 Billion PCs)
  - TEE – Trusted Execution Environment (500 million phones)
  - SIM (carrier mechanism for Identity on all mobile)
  - Secure Element (EMV payment model ApplePay)

Trusted Execution

- Provides isolated execution to create authorizations
- Provides a measured execution environment
- Arm Trustzone
  - Trustonic TEE OS
  - Qualcomm TEE OS
  - Multiple smaller solutions device specific
- Intel SGX and Intel ME part of VPRO

Trusted User Interface

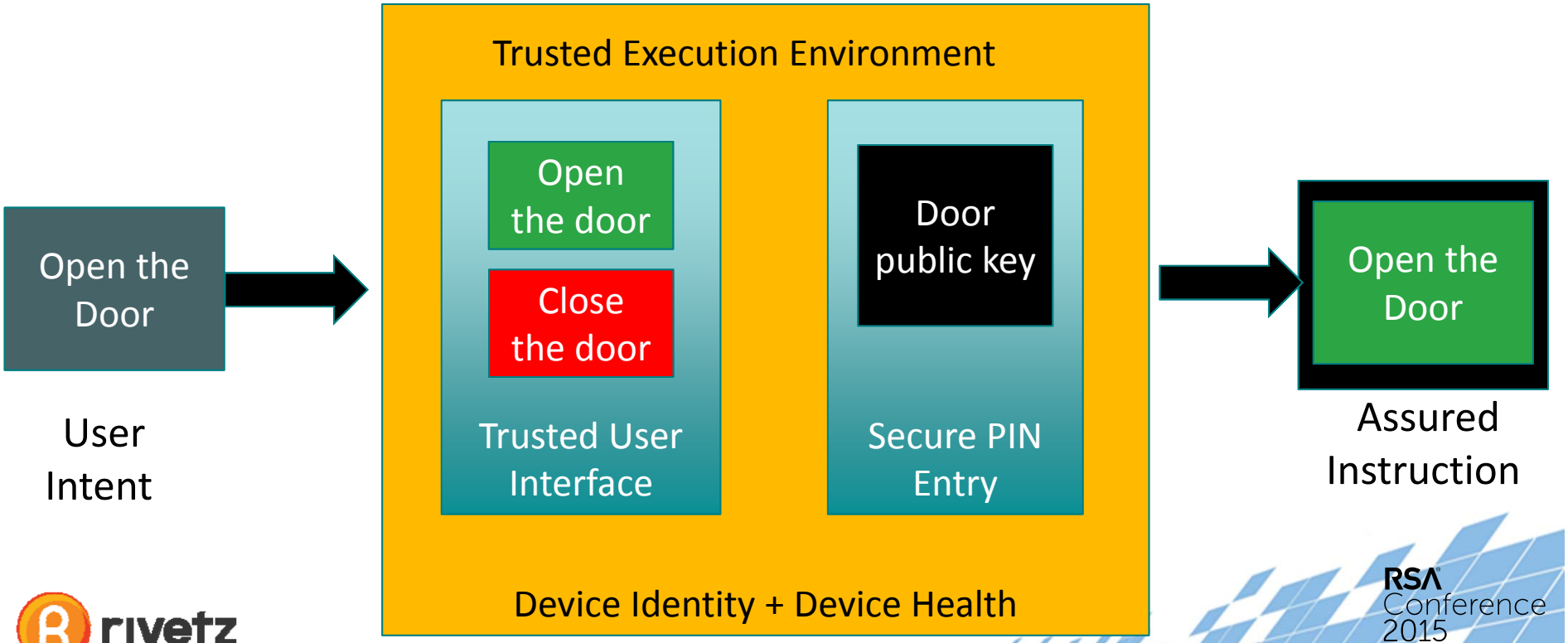
- Provides the collection of user intent and assured results
- Secure display isolated from the OS
- Secure pin entry without OS
- Isolated biometric match
- Already on millions of deployed devices

Supply Chain Integrity

- A device birth certificate
  - Device endorsement keys
  - Hashes of device embedded software
  - Reference device health/attestation measurement
  - Blockchain or similar storage of device certificate
- Registered reference health
- Verification of real-time attestation vs reference health
- A transaction multi-signature

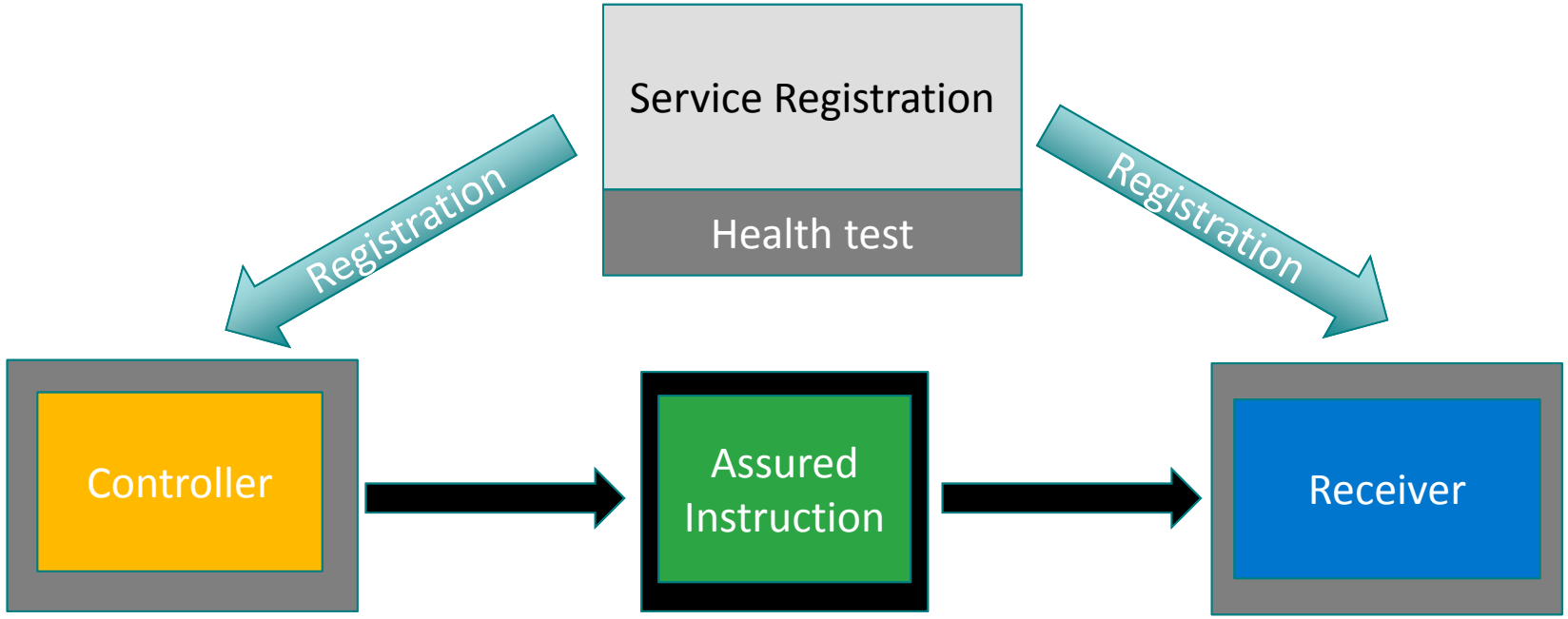
rivetz

IoT is a shift to authorizations



rivetz

Registration not Passwords



A network of authorizations

- Secure instructions not secure links
- End to end encryption and assurance
- A fully mobile network on all transport
- A reduced role for network security

A transition from secure links to secure messages

The IoT model applied today

- Smart Cities
  - Building access control from hotels to modern buildings
  - Industrial control from oil and gas to digital signage
- Industrial Control
  - Every sensor and every controller needs embedded security
  - Users need secure messaging for simple work
- Modern Finance
  - E-sign contracts from NDA's to building leases to business contracts
  - Crypto-currency and blockchain technology in global finance

Actions for today – tomorrow

- Procure the right device
  - Support for Trustonic TEE, or Global Platform TEE
  - Support for TPM 2.0 on all PCs and Tablets
- Require hardware device identity on new applications
- Enable Wi-Fi and VPN to use TPM 2.0 on all PCs
- Require cloud services to support enterprise defined tokens in mobile and PC not just SMS for multi-factor
- Include TEE protected keys as an option in any Android app development

Create Policy

Only known devices connected to sensitive networks and data

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Thank You

Steven Sprague
CEO
Rivetz Corp.

Steven@sprague.com