CABLE-TEC EXPO® 2017

SCTE · ISBE

THE NEXT BIG...

DEAL
CONNECTION
INNOVATION
TECHNOLOGY
LEADER
NETWORK

SCTE·ISBE CABLE-TEC EXPO 2017

DENVER, CO
OCTOBER 17-20

2017 Fall Technical Forum
SCTE·ISBE • NCTA • CABLELABS

SCTE · ISBE

Device Risks to Network Operators from IoT

Brian Scriber
Principal Architect
CableLabs

SCTE·ISBE CABLE-TEC EXPO 2017
DENVER, CO
OCTOBER 17-20

Device Identity

Onboarding/AAA

Confidentiality

Integrity

Availability

Lifecycle Management

Upgradeability
& Future Security

- **Attestable:** Algebraic proof of possession of private key
- **Immutable:** Cannot change the identity of the device
- **Unique:** No two devices duplicate identity or secrets

- **PKI:** Public Key Infrastructure with centralized management
  - Verifiable proof of passing certification(s): Ecosystems, Pen tests
  - **Revocation (changing authorization of the device after sale)**
  - **Non-repudiation (proof the device received the directive)**
  - **Network identification of bad actors**

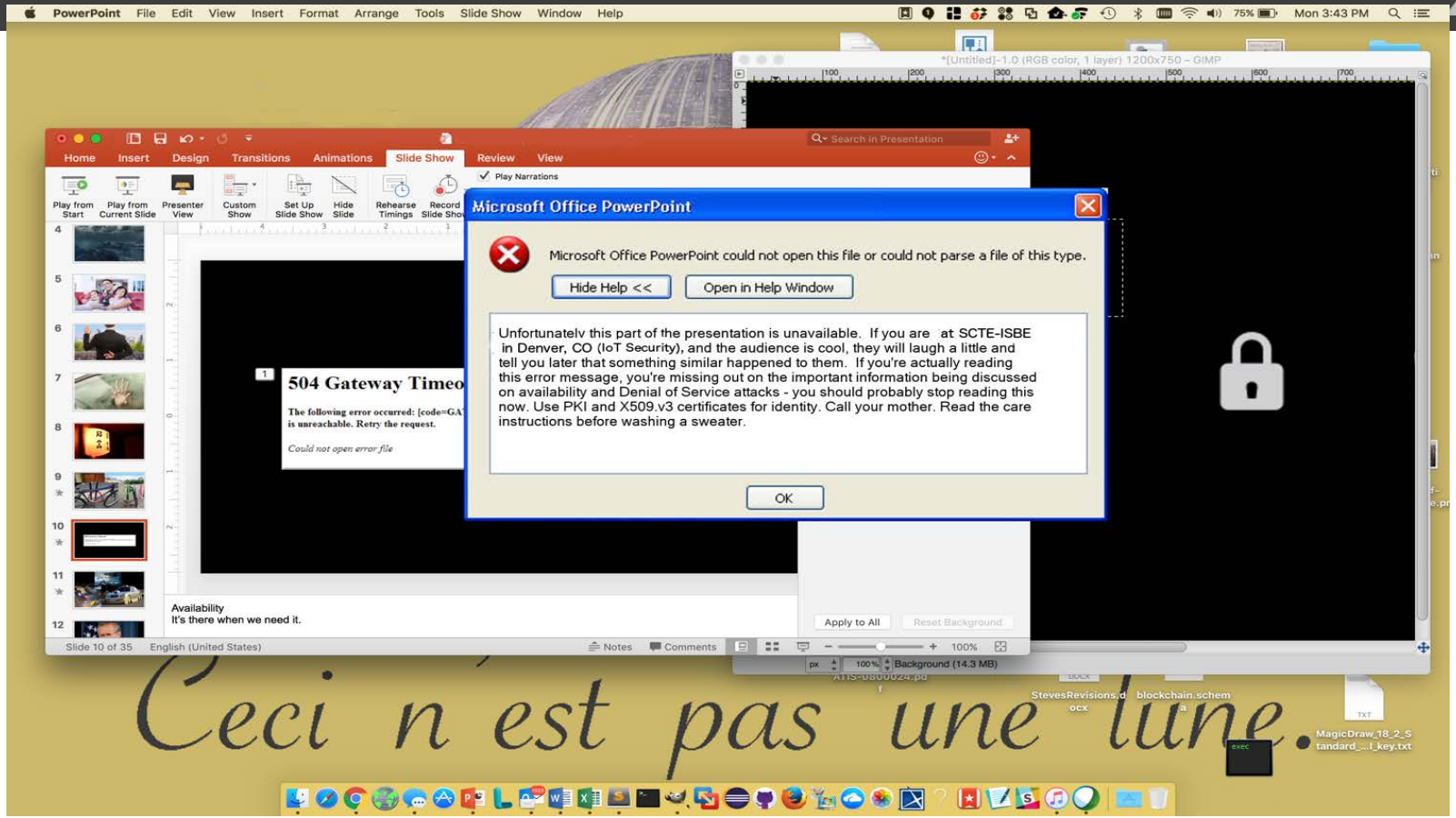
- **Authentication:** Device can prove its Identity
  - Use only **STRONG** authentication
  - **UNIQUE** credentials only (no shared default credentials)
  - **VERIFY** ecosystem credentials against CRL/OCSP/Blockchain
  - Confirm **ISSUANCE** of credentials
  - Confirm current **VALIDITY** of credentials

- **Accounting:** Actions on/by the device are logged
  - **Standardized** format
  - **Auditable** link between actions and both AuthN & AuthZ
  - **Immutable**
  - Perfect World:
    - **Distributed**
    - **Private** (Encrypted)
    - **Alerts**

- **Authentication:** Device can prove its Identity
  - Use only **STRONG** authentication
  - **UNIQUE** credentials only (no shared default credentials)
  - **VERIFY** ecosystem credentials against CRL/OCSP/Blockchain
  - Confirm **ISSUANCE** of credentials
  - Confirm current **VALIDITY** of credentials

- **Identify Sensitive Info:** PHI, PII, creds, etc. and protect it
  - **At Rest:** Protect sensitive data at rest with encryption
  - **In Use:** Protect credentials while in use (they remain in the TPM)
  - **In Transit:** Application-level (end-to-end) encryption for traffic
- **Anonymous Discovery:**
  - Provide an ephemeral identifier
  - Limit information provided

- Use AAA to CONFIRM: **Device ID**, **Execution Environment**, **Configuration**, and **Communication** are all authorized/appropriate.
- **Harden:** SEE, TPM, JIL/FIPS
- Minimize attack surface: **Close ports**
- Disable unnecessary services
- Use a secure bootloader
- Validate configuration
- Use non-repudiation for critical communications


PowerPoint File Edit View Insert Format Arrange Tools Slide Show Window Help
Mon 3:43 PM
Microsoft Office PowerPoint
Microsoft Office PowerPoint could not open this file or could not parse a file of this type.
Hide Help <<
Open in Help Window
Unfortunatelv this part of the presentation is unavailable. If you are at SCTE-ISBE in Denver, CO (IoT Security), and the audience is cool, they will laugh a little and tell you later that something similar happened to them. If you're actually reading this error message, you're missing out on the important information being discussed on availability and Denial of Service attacks - you should probably stop reading this now. Use PKI and X509.v3 certificates for identity. Call your mother. Read the care instructions before washing a sweater.
OK
504 Gateway Timeo
Availability
It's there when we need it.
Ceci n'est pas une lune.

- **DEVICE AVAILABILITY:**
  - Plan for jamming attacks
  - Plan for loss of power and/or network connectivity
  - Limit protocols allowing for anonymous requests
  - Audit all outages, evaluate changes during outage

- **NETWORK AVAILABILITY:**
  - Use **restrictive**, not permissive, default network traffic
  - **Monitor** for inappropriate/unusual traffic

- **PROCEDURAL:**
  - Disclose vulnerabilities, remedies
  - Disclose support period
- **TECHNICAL:**
  - Provide for **SECURE STANDARDIZED AUTOMATED UPDATES**
  - Implement EOL functionality
  - Allow for credential renewal and revocation

- Support for longer key lengths
- Stronger/different algorithms
- Response to cryptographic library weakness/vulnerabilities
- Consider hardware-based security changes
- Prepare for changes in adversaries and

SCTE · ISBE

THANK YOU!

Brian Scriber
b.scriber@cablelabs.com

SCTE·ISBE CABLE-TEC EXPO 2017 | DENVER, CO OCTOBER 17-20

CableLabs®