Zero Touch Device Onboarding for IoT Control Platforms

Jennifer Gilburg
Director IoT Identity
Intel® Platform Security Division
Instant Poll

How long does it take to securely onboard† 10,000 IoT lightbulbs?

†Onboard = From out-of-box to securely streaming data
Establish Trust in Edge Devices Now!

“There is a small - and rapidly closing - window to ensure that IoT is adopted in a way that maximizes security and minimizes risk.”

- Report to President on IoT

Time is Expiring on IoT Security. Are you ready for the coming wave?

Complex, long device lifecycles. Infrequent updates.

ODM  OEM  Admin  User  EOL

7+ years
Establish Trust in Edge Devices Now!

"There is a small - and rapidly closing - window to ensure that IoT is adopted in a way that maximizes security and minimizes risk."

- Report to President on IoT

Volume of sensors/devices coming online will overwhelm today’s security management capabilities

IT/Ops ability to secure today

Source: Bi Intelligence Investments-2014
Things on the Road
Your next self-driving mobile Wi-Fi® hotspot

Demonstrated attacks:

Untitled CC2.0 Flickr - Daniel Olnes; Brake! CC2.0 Flickr - Alan; Prius Power Button CC2.0 Flickr - Thom Watson; AmazinCorn GPS track map CC2.0 Flickr - Omega Man
Your home is your castle. And it’s under attack.
Things Public and Critical

If you need to control it, you need someone else not to.
You shouldn’t have to choose between privacy and security. You can have both.

LizardStresser IoT Botnet Part of 400Gbps DDoS Attacks

ASERT says an unknown group of cybercriminals are running this latest iteration of the LizardStresser botnet via approximately 100 command-and-control servers, manipulating about 1,300 webcams and launching attacks as large as 400Gbps.

Creepy ‘Hello Barbie’ Doll Will Spy on Your Kids CC2.0 Flickr – Mike Licht
New Recognition that HW Delivers Essential Foundation for Security Use Cases

- Attacks have compromised traditional defenses
- Layered security still required
- New hierarchy of trust must leverage isolated protections delivered by embedded security

HW security is trust anchor that is inherently trusted to make the entire IoT security stack more secure as a comprehensive system

Source: AGC Partners 2017
• Intel® Enhanced Privacy ID (Intel® EPID)
• TCG/ISO standard with privacy preserving group authentication scheme
• Used to authenticate & open secure, authenticated channel for remote attestation
• Open source SDK
• Used by Intel solutions & emerging ecosystem of processor & MCU providers

Prevents Attack Mapping- Protects device data vs PKI that reveals data to hack device

Baseline Minimum
HW Root of Trust

HW Identity

Attest SW

Secure App Container "TEE"

EPID Identity

EPID vs. PKI

Intel® EPID

Traditional PKI

1-to-many key match, unique signature every time, anonymous

1-to-1 key match, standard signature every time

Pvt-Key

Pvt-Key 1

Pvt-Key 2

…

Pvt-Key X

Pvt-Key
EPID 2.0 Ecosystem

Issuer (Intel)
- Group Public Key
- Group Private Key
- Group Issuing Private Key

Private Keys 1.. n

Chip OEM

Device OEM

ACE

Inherent Key Distribution

EPID Attestation

Intel TSI
- Certificate Path Validation
- Revocation Lists

CLOUD SERVICE

Member (Edge Device)

EPID SDK

Verifier
Instant Poll

How many EPID Keys have been shipped since 2008?

2.5B

Bunch of keys CC2.0 Flickr – pixishared
billions and billions served CC2.0 Flickr-Bon Adrien
Manual IoT Onboarding Today

- **Device arrives on-site**
- **Technician installs, turns on device**
- **Manual configuration & provisioning**
- **IT backend accepts device credentials & connects it to device management system**
- **Device starts working**

... & now to type in the 256 character key... on my cell phone... on top a 20-ft. ladder... how "convenient"...

- **Major Barrier for IoT** - Only way we get to 50B devices by 2020 is automation. Tremendous ROI drag.
- **Missing Element for Security** - Must solve Mirai style attacks: “ship default passwords" for headless devices and users
- **Privacy** - Need to preserve device anonymity
- **Traditional PKI Identity** - Still has role to play for IoT buy too heavyweight & costly to embed in hardware at scale

**Ecosystem wants automated “SIM” like” approach that ties identity to platform initiated activation. Nobody solving!**
• **Separate Roles** – Installer plugs in & IT takes control of device to get on network and control platform

• **Proxy Installation by Trust Broker Service** – Sales transaction can automatically start provisioning of users account to control platform. No passwords!

• **Privacy** – Attackers cannot trace devices from factory to owner. Unlike PKI, EPID does not reveal endpoint authentication details.

A trust broker service is needed for all devices
Component Flow

Silicon Providers - EPID SDK

Device

- TEE
- EPID SDK
- TB Client
- Mgr Agent

Onboarding Service

Initial Device Identification (EPID Attestation)

Trust Broker Service

- TB Service Identification
- Take Ownership

CSP IoT Platform Service

- Platform Registration Service
- Trust Brokerage SDK/API
- Platform Manager Service

Supplier

New Owner

Ownership Proxy

CSP/ISV Toolkit - integrate TB API into their IoT Platform

OEM Development Toolkit - board and gateways - integrate TB client software into their boot code

Device securely on-boarded - under Normal Platform Control
Power On, Phone Home, Securely Onboarded
<1min/device, anonymous rendezvous, 2-way trust, enterprise scalable

Hi, I am 123. Where is my management service?
Here is my EPID signature, I am Device with GUID=123
Try 11.11.11.11.
I manage GUID 123. I'm available at this IP: 11.11.11.11
Here is my Ownership Proxy, I am Owner for g=123. Here is device configuration, too!
Tremendous ROI

- Customer: Simplifies field installer job by order of magnitude. 20 min per device to seconds e.g. x 10K lightbulbs = Big Savings
- ODM: No need to preload & validate each IoT platform provider’s onboarding agents - works for all
- Customer: IT & OT friction reduced as IT not a bottleneck to getting devices into production
- Installer: Eliminates potential security holes that come with manual security config by a human installer
- ODM: No need to ship hackable default passwords
- Customer: Deploy more devices faster > accelerate IoT revenue
- IoT Platform ISV: Easier to put wider range of devices under management increasing market share

$ ROI

MIN MAX
# Smart Parking Garage

<table>
<thead>
<tr>
<th>Problem:</th>
<th>Solutions:</th>
<th>Value:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wasted fuel, excess lighting costs, frustrating parking experience to navigate to open spot and garage operations not able to monitor or direct</td>
<td>Smart cameras, status lights, &amp; IoT Gateway for edge analytics onboarded to central OT Garage/security management platform</td>
<td>Reduced install time. Operations can be run at remote management location. Secure baseline for software updates</td>
</tr>
</tbody>
</table>

## How It Works

### Onboard
- @ power on EPID onboarding to Gateway then broker service, then Security Management platform

### Operate
- Leverage EPID secured comms channel to attest SW & deliver mgt agents & patches
- Relay gateway data analytics to cloud analytic services & OT operations

[Diagram of how it works]
Apply and Engage

EARLY ACCESS PROGRAM - LEARN HOW TO ENABLE SOLUTIONS
EMAIL: IOTONBOARDING@INTELCOM