Getting from Nothing to Something

AKA: Bootstrapping, Commissioning, Pairing, ...

Cullen Jennings, PhD
Cisco

Smart Object Security Workshop
March 2012

Goal

- So Cisco sold me this super constrained, super smart, super thing! Good grief, now what ?
- “support highly constrained devices that are cheap to manufacture and simple enough for the average skilled person to install” - Paul Chilton
- At installation, there is is not relation between the light and the switch, how do we get to the point where we can apply standard COMSEC

Constraint Space

At installation:

- UI: Button, LED, digit display, nothing
- Power at installation time: scavenger, none
- Replacement: disposable vs cloneable, transferable
- Network: broadcast support, none

Solution: Push Buttons

- Controller is put in promiscuous mode
- Device has button pressed to enroll
- Devices broadcasts and finds the controller
- Range of broadcast is proximity limited
- If attacker is in proximity during enrollment, this is unlikely to end up secure
  - Caveat: the DH with RF trick is cool

Code Display

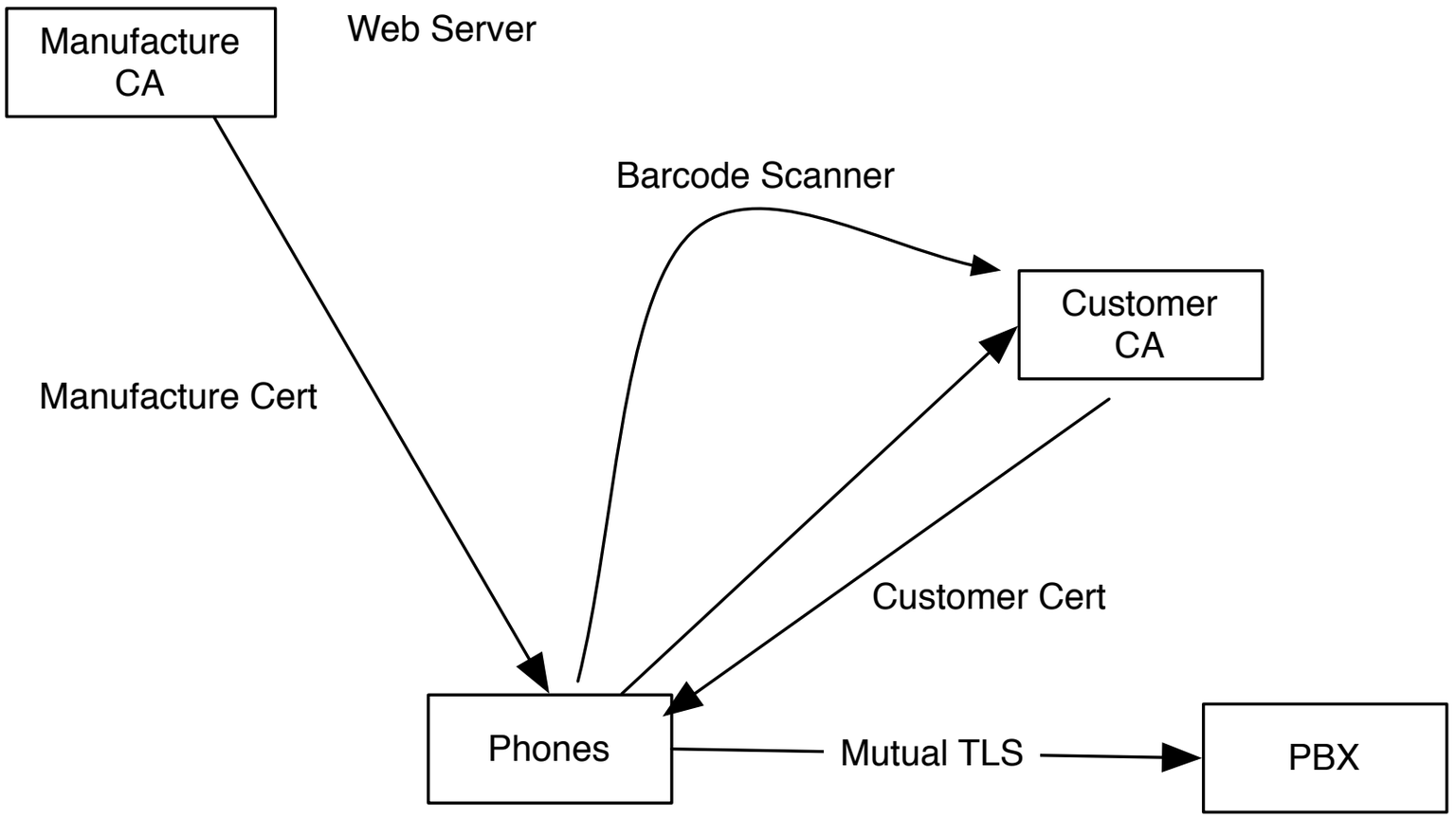
- Like pushbutton but both sides display a code that a human need to verify matches
- In practice code are not verified (see bluetooth “0000” in C. Bran paper)
- Code is typically done after enrollment making it difficult for no power installations

Device Label Solutions

- Device has a label with some secret that a human helps transfer from the device to the controller
- Label can be digits, barcode, RFID, blinking light, etc.
- PAKE allows for short labels
- Major problem is label interception by attacker

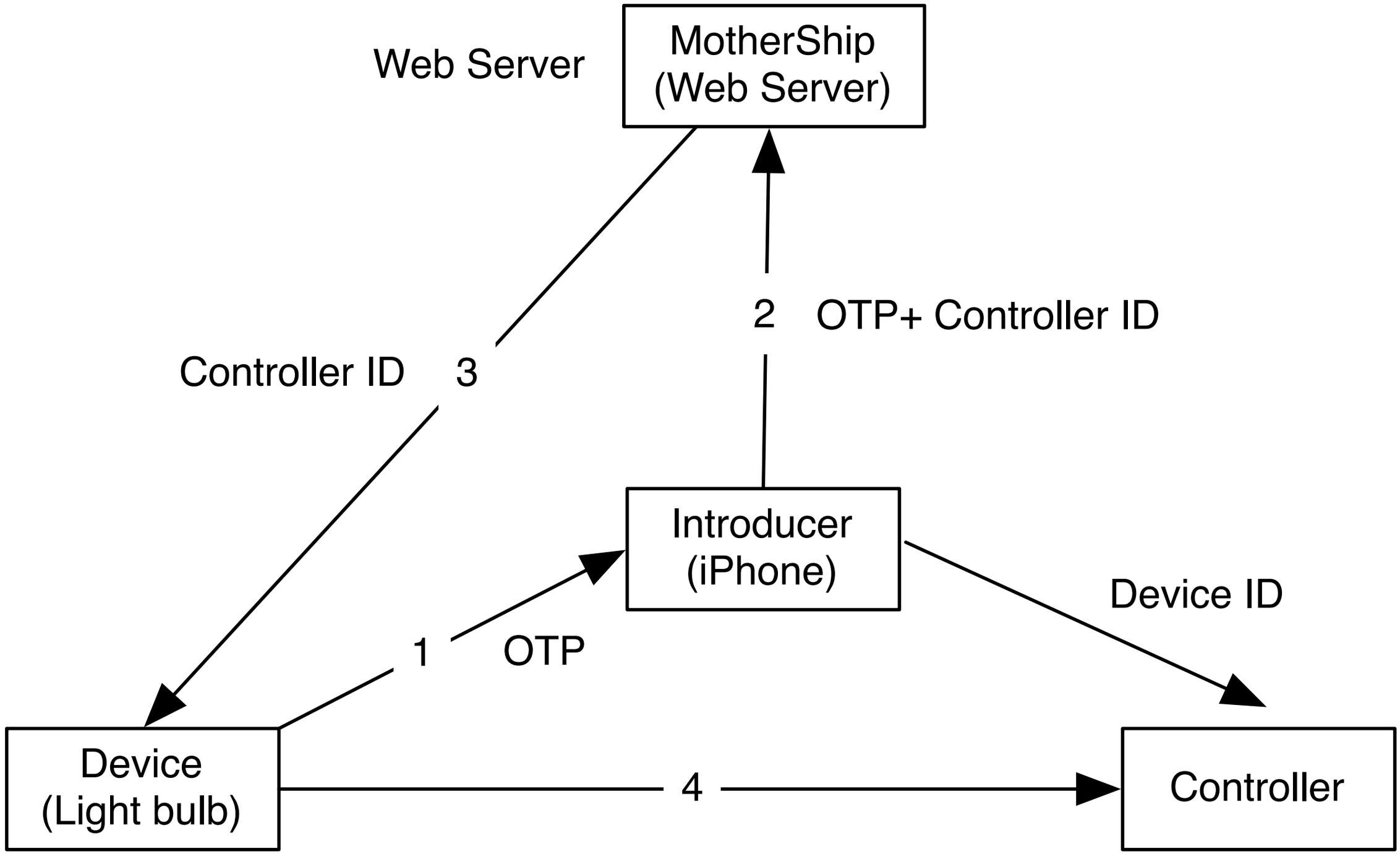
A specific label example

Phones ...



A New Label Example

- Each device has a label with a one-time key encoded as a QR code
- smart phone serves as a trusted label reader/ introducer
- Manufacturer web server (mother ship) coordinates device/base station introduction process


Web Server
MotherShip
(Web Server)
2 OTP+ Controller ID
Controller ID 3
Introducer
(iPhone)
Device ID
1 OTP
Device
(Light bulb)
4
Controller

Characteristics

- Mothership detects and fails intercepted labels
- Grandma can enroll a light bulb (do you believe this?)
- Installer can enroll all lights in building before power or network is installed
- Low cost to manufacture
- Randy can find the 16th device - even if it's asleep
- Can provide credentials for TLS-PSK systems
- Does not require anyone to do anything they have no incentive to do
- Only enrollment hardware is standard smart phone