Future Tokens for Derived PIV Credentials (Future Revision of SP 800-157)

Bill Burr, Dakota Consulting
wburr@nist.gov

Public Review: no Bluetooth Tokens

- Several comments on failure to consider Bluetooth LE connected tokens
  - Pointed out AES CCM encryption
  - Proximity tokens
    - Not exactly “derived PIV” but potentially could contribute to mobile device management & improve mobile security
  - Bluetooth PIV card readers
  - Actual Bluetooth key fob derived PIV token including a PIV chip

Bluetooth

- Low power radio interface standard
  - UHF ISM band (2.4-2.485 GHz)
    - Shared with WiFi and other services
  - “Personal Area Networks”
  - Begun by Ericsson in 1994
  - Now specified/managed/licensed by Bluetooth SIG
  - Ubiquitous mobile device support
  - Two major variants with different spread spectrum radios
    - Classic Bluetooth
    - Bluetooth LE (Low Energy)

Classic Bluetooth

- Stream oriented packet radio
  - Master and up to 7 slaves in “piconet”
  - Nominal range: 1 to 100 m depending on class
  - 1-3 Mbit/s nominal signaling rate, payload 0.7–2.1 Mbit/s
  - Coexist with WiFi in 2.4 GHz band
- Applications
  - Headset, microphone, mouse, game controller, speakers
  - M2M: mag. stripe reader, industrial automation
- Low Power
  - Think AA or AAA battery or equivalent for weeks or months of operation

Bluetooth LE

- Packet radio for discrete events
  - Master/slave protocol, low complexity, fast connections, almost no state
  - Nominal range: 150 m
  - Low (6 ms) latency
  - 1 Mbit/s signaling, .27 Mbps nominal payload
  - Coexist with WiFi & classic Bluetooth in 2.4 GHz
- Applications
  - Watches, fitness bands, proximity, health monitors, industrial automation, sensors, beacons…. really anything with relatively low data rates and duty cycle
- Very low power
  - Think coin cell battery or equivalent for months of operation

Bluetooth & PIV

- A Bluetooth PIV interface could be a wireless PIV smart-card reader, or a wireless interface built into a derived PIV "key fob"
- Both Classic Bluetooth and Bluetooth LE seem to have adequate data rates for typical PIV applications, but
- PIV crypto functionality is only partly provided by PIV chips, which hold private keys and do exponentiation, and
- The rest of the crypto for a signature (formatting, padding and hashing) is done mobile device software, so
- *A Bluetooth PIV reader or device potentially exposes the private key operations to eavesdroppers.*
  - *Potential trouble with FIPS 140 validation*

Classic Bluetooth PIV Interface

- Could potentially use Classic Bluetooth
- Classic Bluetooth offers encryption with E_0, a 128-bit feedback shift register stream cipher
- E_0 has been broken
  - Lu, Meier and Vaudenay find key with $2^{23.8}$ ciphertexts and 2^{38} computations
  - a nominally practical key recovery attack, but would you ever generate $2^{23.8}$ ciphertexts with a PIV token?
  - E_0 is not a FIPS approved algorithm
  - NIST is not likely to approve this

Bluetooth LE PIV Interface

- Bluetooth LE wireless encryption is AES-128 in CCM mode
  - Should be solid encryption
  - FIPS 140 validation is probably practical
- The very low power (or small batteries) of Bluetooth LE is a very good fit for the mobile derived PIV application.

Bluetooth LE Pairing

- Long Term Key (LTK) established during pairing
- Three Pairing modes:
  - *Just Works*: a passive eavesdropper (on the pairing) learns the LTK
  - *Passkey Entry*: Uses 6-digit passkey in LTK derivation. A pairing eavesdropper can exhaustively compute the possibilities & learn the LTK
  - *Out of band (OOB)*: Requires a separate secure channel (eg USB, Near Field … to exchange randoms)
    - Secure, but not much product support

Bluetooth LE Encryption

- Seems that we ought to be able to just do the pairing in a secure location and we're good to go, but
- There apparently is a way for an attacker to break pairing and force repairing (Ryan)
- Hacker and cryptographic literature on Bluetooth eavesdropping & MITM attacks
- Commercially available tools

Paranoid Scenario: Instrumented Room

- Hotel room, meeting room…
- Jam cell tower & bug wifi, or use cell site simulator (DRT box, Stingray, etc.) to read over the air traffic
- Force Bluetooth LE re-pair to eavesdrop on g^{xy}
- Lots of possibilities & variations
  - Even if you're paranoid somebody may still be trying to get you

Bluetooth LE Re-Pairing

- Nobody seems to make OOB pairing devices
  - Implies something like a USP port on derived PIV key fob, or possibly near field radio
  - Can government create a market?
- Six digit Passkey can quickly be exhausted
- Is just works, plus warnings about where you re-pair, enough in many cases?

Proximity Tokens

- Largest group of the Bluetooth LE comments were about “proximity tokens.”
  - Basic idea seems to be that the mobile periodically pings the token, or maybe the the way around: “are you still there?” If not, either
    - lock the PIV private keys, and/or
    - the token sounds a “where’s your phone?” alarm
  - Some comments seemed to bill proximity tokens as a superior alternative to Mobile Device Management (MDM) more than as PIV.

Proximity Tokens

- Prox. tokens aren't inherently PIV
  - But might be combined with PIV in one key fob
- Prox. token choices and issues
  - Industry standards?
    - Is broad interoperability a goal as with PIV cards?
  - Bound to PIV directly or only to mobile device
    - Most effective way to lock a key on the phone might be to keep a key-share on the token.
- Prox. tokens might deserve a separate discussion and a specification of their own.

What's an LOA 4 token?

- Conceptually it's easy to add a separate PIV element to the mobile device System On Chip, but
- This would be easy to FIPS validate vendors are unlikely to do this
  - Rapidly implementing hardware protected environments for cryptography, key rings, key stores, etc. for more general use
- When can we consider PIV crypto using normal device services to be "hardware" not "software" and FIPS validate them at a high enough level for SP 800-63-2 LOA 4?
  - FIPS 140 validation of high volume SOC commercial products is a big practical problem
- To me this is the $64 k question.
  - Or is the $64 k question "should we change SP 800-63?"

Conclusions

- Bluetooth LE is a potential enabler for mobile PIV card readers or key fob derived PIV tokens
  - Issues: pairing, details of FIPS 140 validation &
- Proximity tokens are an interesting idea
  - Might be linked to derived PIV or stand alone
  - May deserve a separate document

Bluetooth Crypto Attack References

- Y. Lu, W. Meier, and S. Vaudenay, “The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption”, In Advances of Cryptology, CRYPTO 2005 vol. 3621, pages 97–117, August 2005. http://lasec.epfl.ch/pub/lasec/doc/LMV05.pdf
- Tomáš Rosa, “Bypassing Passkey Authentication in Bluetooth Low Energy,” https://eprint.iacr.org/2013/309.pdf
- Mike Ryan, “Bluetooth: With Low Energy comes Low Security,” http://lacklustre.net/bluetooth/Ryan_Bluetooth_Low_Energy_USENIX_WOOT.pdf