Recommended Practice for Privacy Considerations for IEEE 802 Technologies

Date: 2016-07-26

Authors:

Name	Affiliation	Phone	Email
Jerome Henry	Cisco Systems	+1 919 392 2503	jerhenry@cisco.com

Abstract

The slide set provides a summarized update on the 802E specification.

IEEE 802

Privacy
Some common definitions:

- Merriam-Webster's Dictionary:
  - 1a: the quality or state of being apart from company or observation: seclusion
    1b: freedom from unauthorized intrusion one's right to privacy
  - 2. archaic: a place of seclusion
  - 3a: secrecy
    3b: a private matter: secret

- According to Yael Onn et al., Privacy in the Digital Environment. Haifa Center of Law & Technology, 2005:

  "The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets, and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner, and timing of the use of those parts we choose to disclose."

EEE
802

PII
Personally Identifiable Information

- Privacy:

  "The fair and authorized "processing" of Personally Identifiable Information (PII)

- Personally Identifiable Information

  Formally: Any data that identifies an individual or from which identity or contact information of an individual can be derived

  Practically: Includes otherwise non-personal information when associated or combined with personal information

EEE
802

What does this mean for 802?

- 802 protocols typically do not <u>directly</u> contain PIIs

- However, they may be transmitted by:
  - Personal devices
  - Common service devices

What does this mean for 802?

- If 802 transmissions allow you to fingerprint a device…

- And if devices is a personal device…

- Then as soon as correlation is made between the device and a person, you can track and monitor the person as you track and monitor the device

EEE
802

What does this mean for 802?

- If 802 transmissions allow you to fingerprint a device…
- And if devices is a personal device…

- Then as soon as correlation is made between the device and a person, you can track and monitor the person as you track and monitor the device
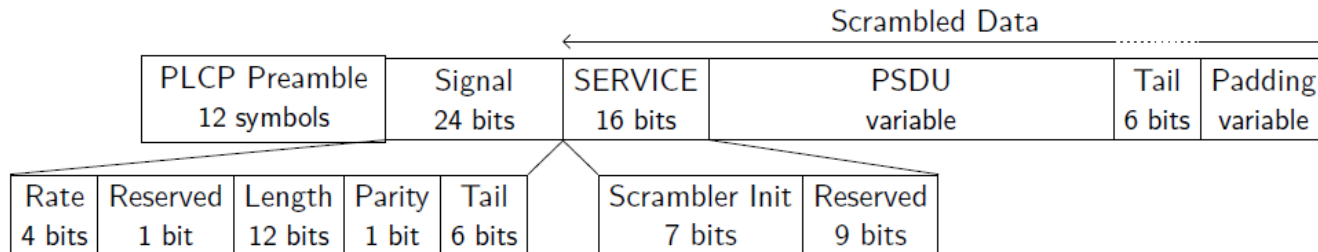
EEE
802

Fingerprinting

- Some identification methods are well known
  - "Tell me you MAC address, I'll tell you who you are"
- Some other methods are less obvious

EEE
802

Fingerprinting - Scrambler Example

Scrambler seed
- Scrambler in OFDM frames of 802.11 PHY
  - Scrambler used from the SERVICE field to the end
  - Seed contained in the 7 first bits of SERVICE field

- Observed behaviors
  - Freewheeling: State of the LFSR at the end of a frame is reused for the next frame
    - Sometime with a constant number of shift of the LFSR
  - Constant seed, or limited to a small set (bug ?)
  - Incremental: seed value is incremented by one at each frame

* http://www.ieee802.org/1/files/public/docs2016/e-cunche-dot11-tracking-0416.pdf

So, what are we doing?

- Examining 802 protocols
  - 802.1 complete, 802.11 in progress, others in the pipeline
- Looking for mechanisms that may allow for fingerprinting
  - Evaluate if these mechanisms may apply to personal devices

- Next phase will be to reflect on possible remediation and mitigation

EEE 802

Summary

- 802E purpose is to promote a consistent approach by IEEE 802 protocol developers to mitigate privacy threats identified in the specified privacy threat model and provide a privacy guideline.

- First step is to identify threat models for Personal Identifiable Information (PII)
  - Identify PIIs
  - Decide which PII elements require protection
  - Identify the potential threats
  - Understand the possible effects of protecting target PII
  - Provide privacy guidelines

- An initial draft will be built to host contributions

EEE 802