IEEE 802 Privacy Threat Analysis Overview

Date: 2016-07-26

Authors:

Name	*Affiliation*	*Phone*	*Email*
Brian Weis	Cisco Systems	+1 408 526 4796	bew@cisco.com

Abstract

These slides provide an overview of the Privacy Threat Analysis documented in 802E-weis-privacy-threat-analysis-0718-v01.pdf in the IEEE 802.1 public files site (http://www.ieee802.org/1/files/public/docs2016/).

What is a privacy threat analysis?

- We evaluate IEEE 802.1 protocols for PII, including protocol elements that can be used for “fingerprinting”
  - “PII in our standards, PII that is directly derived from our standards (e.g. IP derived from MAC), and PII in other standards that we use”.
- It is not a goal of the document to describe mitigations, other than perhaps by way of example.

Sample Terminology

- **PII.** Any data that identifies an individual or from which identity or contact information of an individual can be derived.
- **Personal Correlated Information.** Data gathered about a person by observing personal devices.
- **Target**. A machine emitting network frames that can be associated with a person, and on which an Adversary can fingerprint.
- **Adversary.** A threat agent who is taking steps to fingerprint one or more targets.
- **Respondent**. The network device to which a target is intending to communicate.

Analysis Stategy

- An “asset/risk/threat analysis” is used to determine privacy risks and threats to objects identified as having privacy considerations
  - Take each protocol in turn as an “asset”, consider each possible privacy ”risk” to a field in that protocol, and then translate each “risk” into a set of “threats” (a method by which an attacker could make use of the risk)
  - Finally, each threat is considered in context of the protocol use, to judge whether the threat is credible or not.

Example analysis

Asset: IEEE 802 Destination MAC Address and Source MAC Address

Risk	Threat	Threat Analysis
Adversary observes Target MAC address as DA or SA on the IEEE 802 frame	When the Adversary is close to the Target, it can monitor flows and detect changes to an SA	Adversary can detect the change from universal address to local address, or from one local address to a different local address.
	Adversary observes and logs the Target MAC address, correlates it with other network accesses to or from this Target	When the Target MAC address is a universal address, identification and correlation of Target MAC address across multiple networks in time and space is trivially possible.
Target MAC address Is embedded in the payload of the frame	Adversary observes and logs Target MAC address embedded in an IPv6 Source address	Same as above.
	Adversary observes and logs target MAC address located in an Ethernet frame that is tunneled within an Ethernet frame (e.g. as used in Provider Backbone Bridged Newtorks (“MAC-in-MAC”).	Same as above.

Privacy Threat Analysis Overview

IEEE 802.1 threats

1. IEEE 802 Common fields
   a. Destination MAC Address (DA) and Source MAC Address (SA)
2. IEEE 802.1
   a. Encapsulated MAC address
   b. Priority Code Point
   c. VLAN Identifier (IEEE 802.1Q)
   d. Congestion Notification Tag (IEEE 802.1Q)
   e. LLDP (IEEE 802.1AB)
   f. Port-Based Network Access Control (IEEE 802.1X)

Destination MAC Address (DA) and Source MAC Address (SA)

1. When the Target MAC address is a universal address, correlation of Target MAC address across multiple networks in time and space is possible. This includes cases where the MAC address is used as an SA or DA on the frame, or is included in a well-known network header (e.g., an encapsulated Ethernet header, IEEE 802.1Q I-TAG, or in an IPv6 header).

Destination MAC Address (DA) and Source MAC Address (SA)

2. Correlation of any Target MAC address can be used as an aid to
   - Track location of the Target MAC address when it is mobile.
   - Collect frames to and from the Target MAC address, to be used for further analysis. Further analysis might include the identification of MAC addresses that appear to be associated with an individual, or once it is associated with an individual to evaluate it to determine which individual.

Destination MAC Address (DA) and Source MAC Address (SA)

- NOTE: Correlation of a Target MAC address is not always a threat to privacy. An individual may authorize the correlation for his/her own benefit by, for example, explicitly “opting in” to the correlation after having been offered special treatment by the network owner (e.g., a business).

Encapsulated MAC address

- Some IEEE 802.1 protocols include an encapsulated MAC address:
  - IEEE 802.1Q Congestion Notification Message PDU
  - IEEE 802.1Q SRP StreamID,
  - IEEE 802.1Q VSIID,
  - IEEE 802.1AB Chassis ID,
  - IEEE 802.1AB Port ID,
  - IEEE 802.1X EAPOL-MKA SCI,
  - IEEE 802.1AE SecTag (System Identifier in Figure 1).
- Threats to MAC addresses described previously apply to these MAC addresses.

Encapsulated MAC address

- Additionally, a bridge may be considered to be a Personal Device if it is located at a network edge associated with people (e.g., a residential gateway).
  - In this case the Bridge Address associated with the bridge is required to be a universal address, and it may be used to locate host addresses (e.g., those embedded in a Stream Identifier)..

Priority Code Point

- A Priority Code Point (PCP) is found in several IEEE 802.1Q protocol elements
  - VLAN Tag
  - Congestion Notification Message PDU
  - MSRP Structure.
- Threats:
  1. Classes of Targets may be identified based on the PCP, if the adversary is aware of the PCP mappings. Some mappings are de-facto or actual standards. Identification of voice and video traffic are well known and can aid in the identification of classes of Targets.

VLAN Identifier

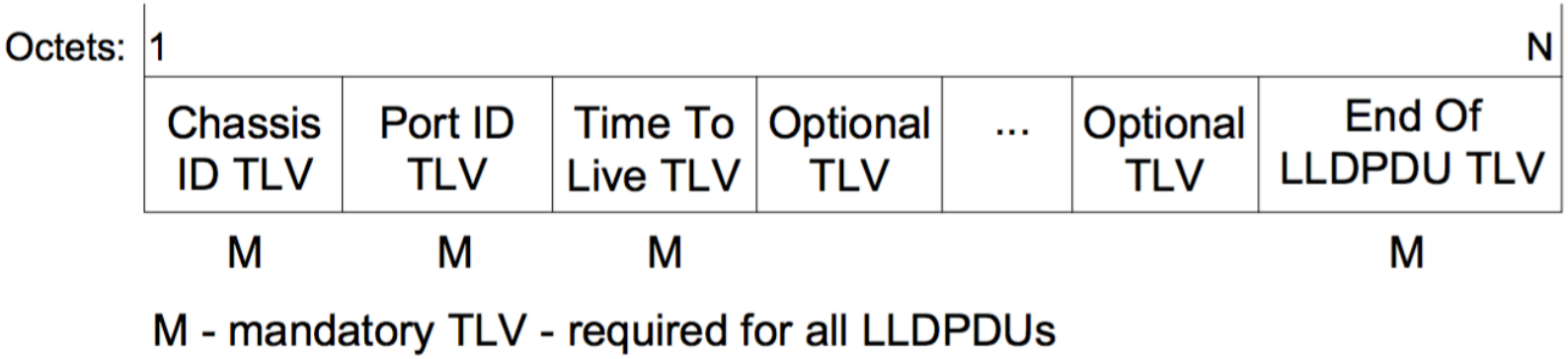
- A VID is often used to separate different types of traffic, such as traffic from different organizations or individuals with different roles in the organization. A VID can be included in a
  - Customer VLAN Tag
  - Service VLAN Tag
  - Backbone VLAN Tag
  - Backbone Service Instance Tag
- Threats:
  1. Classes of Targets (e.g., Organization, Role) may be identified based on the VID value, if the adversary is aware of the VID mappings. Such mappings are likely to be network specific, and less likely to be obvious to the adversary unless correlated with other traffic analysis.

Congestion Notification Tag

- An end station may add a Congestion Notification Tag (CN-TAG) to every frame it transmits from a congestion-controlled flow, which contains a Flow Identifier. The format of the Flow Identifier is not specified, but in order to be useful is likely to be persistent for a flow.
- Threats:
  1. A particular flow between a Target and Respondent may be identified based on a Flow Identifier, without the Adversary interpreting the value of the tag.
  2. An Adversary with knowledge of how to interpret the tag may be able to correlate flows between a Target and one or more Respondents.

LLDP

- Link Layer Discovery Protocol (LLDP) frames deliver information about a station as TLVs, which may be valuable to other peers on a network segment.



LLDP

- Threats: TLVs that be used to identify a Target:
  1. A network address (MAC address or IP address) in a network address TLV
  2. A system name subTLV can bused used to identify a target by domain name
  3. A System Capabilities TLV can identify a class of target (e.g., Telephone, DOCSIS cable device)
  4. Organizationally Specific TLVs may be defined to contain PII or Personal Correlated Information.

Port-Based Network Access Control

- Several types of management frames can be represented as EAP over LAN (EAPOL) frames
- Message types that could contain PII include:
  - EAPOL-EAP
  - EAPOL-MKA (MACsec Key Agreement)
  - EAPOL Announcements

Port-Based Network Access Control

Threats:

1. A passive adversary between the target and EAP authenticator can observe any information that an EAP method passes without confidentiality protection.
   - Some EAP methods (e.g., a “tunneled EAP” method such as TEAP (RFC 7170)) protect the complete contents of the authentication process from a passive adversary.
2. An active adversary between the target and EAP authenticator may be able to spoof a legitimate respondent in an EAP method to the point where the target presents its identity (e.g., the subject name in a client certificate).
3. A passive adversary in the broadcast domain of the target can observe Announcement data, and identify or deduce the class of target.
   - The KMD or NID may identity the organization; the set of announcement data presented may indicate the type of device.

TBD

- Threat analysis on:
  - 802.3
  - 802.11
  - 802.15
  - 802.21