Abstract

This document relates to the WG ballot of P802E/D1.4 and proposes content for a revised section ‘7. Privacy threat model’ completely replacing the current section ‘7. Privacy threats’. Revision marks are used to indicate the relation of the revised and amended text to the balloted text.

~~Specific questions designed to identify the presence of these and similar opportunities in specific technologies, and thus prompt consideration of alternative designs to reduce privacy risks are posed in Clause 8. These questions are designed to prompt consideration by groups developing standard and by individual and organizations reviewing these standards.The information conveyed in the user data frames that support the Media Access Control (MAC) Service (IEEE Std 802.1AC [B3]) provided by all IEEE 802 MAC technologies is typically specified by application or higher-layer protocol standards outside the scope of this recommended practice. Unwanted disclosure of personal information in that user data is expected to be prevented by cryptographic confidentiality protection. All the user data may be protected, e.g. as specified in IEEE Std 802.11 [B6] or IEEE Std 802.1AE [B4], or just the data conveyed by a higher-layer protocol [e.g. by TLS (IETF RFC 8446, [B19]).~~

~~IEEE 802 MAC technologies do not communicate explicit personal information other than in MAC Service user data frame fields. However an adversary can correlate the observable properties of communication (including, but not necessarily limited to, other frame fields, the sizes and transmission timing of both confidentiality protected and other frames, physical layer signaling and power use and negotiation) with the characteristics of devices used by an individual or a small group of people (Clause 6.2) or with specific applications. An adversary can use that correlated information to fingerprint (Clause 6.3) those devices and applications.~~

~~Common ways in which IEEE 802 technologies contribute to fingerprinting and the resulting privacy threats are described in Clause 7. This recommended practice is concerned with privacy, and specifically with the unwanted disclosure of personal information (Clause 6) as a result of communication using procedures specified by IEEE 802 standards. Privacy definitions and the need for privacy are reviewed in Clause 1.5, and possible goals of adversaries seeking access to, or making use of that personal information, are further described in Clause 6.4.~~

~~In general, a threat model facilitates methodical identification of threats to resources or activities, risks associated with those threats, and possible counter-measures.~~ ~~**1.3 The Privacy Threat Model**~~

7 Privacy threat model

In general, a threat model facilitates methodical identification of threats to resources or activities, risks associated with those threats, and guides towards possible counter-measures. The following clauses introduce a privacy threat model for IEEE 802. Based on a generic network architecture and generic protocol principles, the components and aspects of maintaining privacy in IEEE 802 networks are presented.

7.1 IEEE 802 communications architecture

IEEE 802 LAN standards specify the operation of physical layer (PHY) and media access control (MAC) methods and protocols that support frame-based network communication.

IEEE 802 protocols are deployed for communications either between terminals and their peers, or between routers forwarding packets based on network addresses across wide area networks. Peers of terminals can either be other terminals or an access router, which forwards data frames

based on IP addresses.

Figure 1 below depicts deployments of IEEE 802 protocols for the various sections of an end-to-end communication architecture.

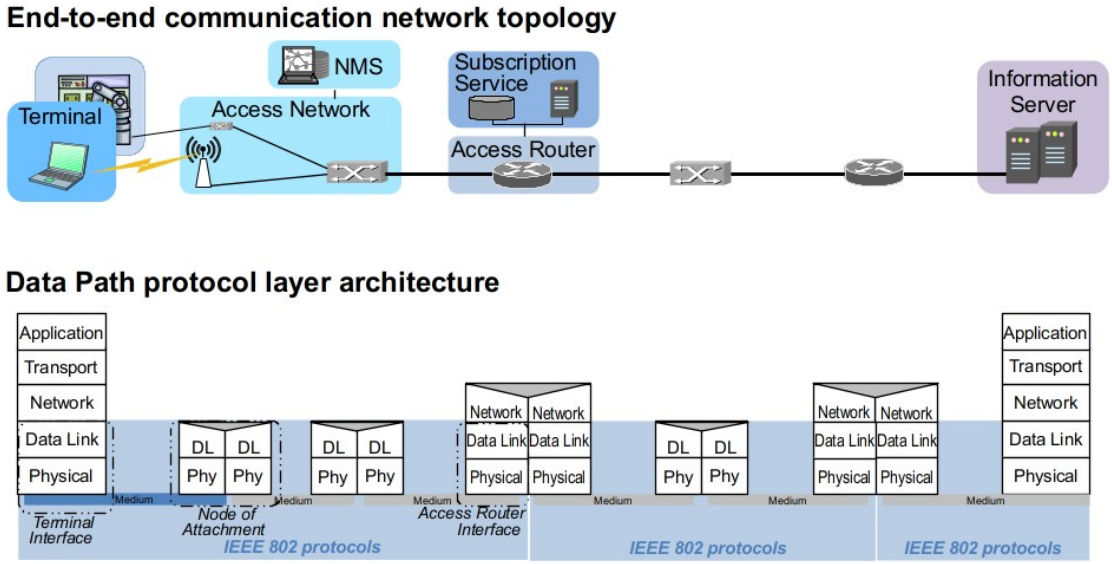

Figure 1: Usage of IEEE 802 protocols in communications networks.

IEEE 802 protocols operate between end-stations, potentially intercepted and forwarded by intermediary bridges. End-stations terminate the protocols and forward the service data unit through the DL SAP to higher layer protocols for further processing. End-stations are terminals, routers, or information servers.

The exchange of information through communication networks is usually organized in layers. Each layer deals with a particular aspect of the communication, and IEEE 802 protocols provide the service to forward network layer information frames over physical medium through MAC layer and Physical Layer protocol and functions.

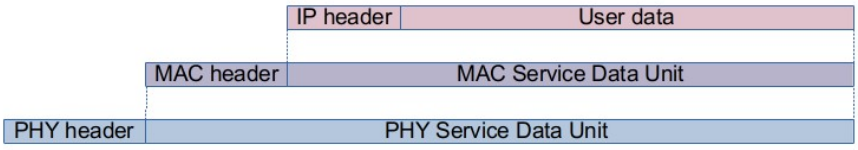

Figure 2: Protocol layering

As shown in figure 2 above, the IEEE 802 MAC protocol transparently carries the complete IP packet including IP header and user data in its MAC service data unit. For forwarding over physical medium MAC frames are amended by the PHY layer by header information to provide for the particularities of the various physical media, IEEE 802 supports through its various technologies.

IEEE 802 technologies do not communicate explicit personal information other than in MAC Service user data frame fields. However an adversary can correlate the observable properties of communication (including, but not necessarily limited to, other frame fields, the sizes and

transmission timing of both confidentiality protected and other frames, physical layer signaling and power use and negotiation) with the characteristics of devices used by an individual or a small group of people or with specific applications. An adversary can use that correlated information to fingerprint those devices and applications.

Common ways in which IEEE 802 technologies contribute to fingerprinting and the resulting privacy threats are described in the following clauses.

7.2 Higher layer protocol aspects

The information conveyed in the user data frames that support the Media Access Control (MAC) Service (IEEE Std 802.1AC [B3]) provided by all IEEE 802 MAC technologies is typically specified by application or higher-layer protocol standards outside the scope of this recommended practice. Unwanted disclosure of personal information in that user data is expected to be prevented by cryptographic confidentiality protection. All the user data may be protected, e.g. as specified in IEEE Std 802.11 [B6] or IEEE Std 802.1AE [B4], or just the data conveyed by a higher-layer protocol [e.g. by TLS (IETF RFC 8446, [B19]).

7.3 MAC layer aspects

All IEEE protocol frames contain a Physical and MAC layers. Each layer performs specific operations, which can be used to fingerprint the device. For example, frames can contains sequence numbers or seed values that may be sequential or predictable. Monitoring such values can be sufficient to fingerprint a device.

MAC procedures and various protocol frame formats and fields can be used to identify personal devices, their attributes, and their use to support specific networking applications and activities. As described in Clause 6, an adversary can use this information to obtain PII and PCI. The location of mobile personal devices and thus presumably the location of the person using that device can be tracked. The fact that users of personal devices are communicating with each other can be detected. A person's behavior can be monitored.

This clause describes some of the protocol elements and MAC characteristics that can be exploited by an adversary. It makes no claim to be an exhaustive list of privacy threats related to current IEEE 802 standards and standards under development. Annex B proposes detailed examples of such elements.

An adversary can require access to the medium supporting the MAC for an individual LAN (e.g. near enough to the target for adequate radio reception in the case of a wireless medium) to exploit some of the threats described. To exploit others access to any LAN in part of a bridge network is sufficient, while the information associated with others is potentially available throughout the Internet. Some threats require, or are more effectively exploited, by an active adversary which can discourage an adversary who does not wish to be detected.

7.3.1 Information elements in MAC frames

7.3.1.1 IEEE 802 MAC layer cCommon fields: SA and DA

All IEEE 802 protocol frames begin with a Destination MAC Address (DA) and a Source MAC Address (SA). In order to simplify the analysis, these are considered independently and apply to all use cases. The analysis is written as if a target is initiating frames, where the SA can possibly

be PII. (Of course, for frames directed to the target the DA would be considered PII.)

An SA is considered PII if it is associated with a target (i.e., is considered a "personal device" as defined by this standard). Not every device emitting frames is considered a target. For example, a bridge within a network is not generally associated with a person, and therefore would not be considered a target. However, the SA associated with a residential gateway network device is very much associated with its subscriber (i.e., a user or household of users), and thus would be considered a target.

Some IEEE standards further identify systems on the path of the frame, even if they are not directly SA or DA respectively. For example, In addition to the SA and DA MAC addresses, IEEE 802.11 uses the Transmitter Address (TA) and the Receiver Address (RA), to allow relay of frames through an intermediate device. The TA can be considered a target when associated with a personal device. Similarly, the RA can be considered a target when associated with a personal device.

7.3.1.2 Encapsulated MAC addresses~~/IEEE 802 MAC Operations~~

~~All IEEE protocol frames contain a Physical and MAC layers. Each layer performs specific operations, which can be used to fingerprint the device. For example, frames can contains sequence numbers or seed values that may be sequential or predictable. Monitoring such values can be sufficient to fingerprint a device.~~ Some IEEE 802 protocols include an encapsulated MAC address. Threats to MAC addresses identified in this clause apply to these MAC addresses. Additionally, a bridge can be considered to be PCI if it is located at a network edge associated with people (e.g., a residential gateway). The Bridge Address associated with the bridge is required to be a universal address, and it can be used to locate host addresses (e.g., those embedded in a Stream Identifier).

Repeated use of a MAC address can lead to an attacker correlating the use of that address across networks or over time (see clause 6.3). Correlation of a target MAC address is not always a threat to privacy. A person can 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). However, when the correlation is not authorized it can be considered a threat to privacy.

7.3.1.3 Flow Identifiers

IEEE 802 standards can include parameters aimed at identifying a particular frame, and distinguish this frame from other frames transiting through the network, and distinguish this frame from other frames exchanged between the sender and the receiver. As such, an adversary can be able to observe these frames and, distinguishing them from other frames, acquire information about specific flows or segments. This information can be used directly or through correlation to identify a specific endpoint and expose PII (see Annex B for additional flow identifiers).

7.3.1.4 Optional Fields

IEEE 802 standards can allow a transmitter to include optional elements in its frames. These elements can indicate support of specific capabilities described by the standard or vendor-specific. Support of these capabilities, or the way these capabilities should be supported, is sometimes left to vendor implementation. These elements can be used by an adversary to recognize the transmitter type, or sometimes uniquely identify the transmitter.

Network Discovery frames

IEEE 802 standards commonly include discovery mechanisms, by which endpoints explore the network services available before connection or before data frame transmission. These mechanisms often use specific frames, which can specifically target a given service. Observing the occurrence of such frames and their specific characteristics can help an adversary uniquely identify the station requesting such service. These mechanisms can also require the infrastructure device to mention support for specific parameters, through general announcements mentioning feature support, or through specific responses to endpoint queries. These parameters can also be used to uniquely identify the infrastructure device and PII when the infrastructure device is a personal device.

Discovery and range

IEEE 802 standards share privacy threats due to their capacity to provide communication for frame-based data networks. In addition, radio-based technologies in IEEE 802 standards have unique privacy threats due to their expansive discovery processes and the ability of an adversary to eavesdrop on those communications.

The process of network discovery by radio-based standards such as IEEE 802.11 can rely on transmission of probes which search for available and suitable networks in which to connect. This exposes the DA/SA common fields threat vector (see Clause 7.2) to anyone within range of the device's radio.

It is also possible for radio-based technologies to permit transactional forms of discovery of network services. These frame exchanges can expose PII that may aid correlation and fingerprinting depending on the form of the particular type of service being searched for.

Authentication and Access Control

Most IEEE 802 Standards include mechanisms to control access to the network or its resources. In order to allow access, exchanges are required, during which frames are sent that can provide information to uniquely identify the end device. The end device may be mobile and fingerprinted through these exchanges. In some cases, the infrastructure device can be a personal device, and these exchanges can also uniquely identify the infrastructure device.

Directed query or instruction frame

7.1 Once network discovery is completed, some IEEE 802 Standards implement a mechanism by which an endpoint can query an infrastructure device, or an infrastructure device can query an endpoint, to enable a particular service, or perform a specific function. In many cases, the query and its response are optional in the standard, but may be accompanied by specific IEEE 802 frames or exchange sequences. The ability to perform such a query, the service queried and / or the reply can be used by an adversary to uniquely identify the endpoint or the infrastructure device.

7.3.2 Frame timing and autocorrelation

Some IEEE standards rely on timing synchronization between device communication functions, for example to ensure the proper allocation of resources at the time of a particular device transmission. The resulting transmission timing can facilitate the association of frames with a particular device and thus support device identification for a period of time.

7.3.3 Frame size exposure

Many of the exchanges described in this clause may rely on the use of frames with specific characteristics of format. Other frames (for example carrying data) may also be drawn to carry a specific amount of payload (e.g. driven by the application exchange characteristics or function of the device communication driver). Such characteristics can be used to fingerprint a device exchanging flows for a specific application. Avoidance of such fingerprinting possibilities is commonly the task of the application designer.

7.3.4 MAC operations

IEEE 802 technologies deploy MAC control messaging to detect the existence of access nodes and access networks, to determine the network to connect to, to perform association and authentication, to communicate authorization and statistics parameters, and to perform particular operations to enhance, modify or terminate connections. For each of these MAC layer functions related messaging and exchange of configurations parameters are defined. The information contained in the MAC control frames as well as the frequency and the individual frame sizes could be leveraged by an adversary by fingerprinting principles to identify and track terminals to find out about PII and PCI.
The potential threats occurring in MAC control messages and procedures depend on the particular IEEE 802 technologies. A number of examples are illustrated in Annex B.

7.4 PHY layer aspects

PHY layer protocol frames contain a header portion with specific information elements for operation of the encoding and transmission of MAC frames for the transmission over the medium. For example, PHY headers can contains encoding parameters or option fields that may be specific to a particular terminal or terminal type. Monitoring such values can be sufficient to fingerprint a device.

== end of chapter 7 ==