Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on January 8, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Abstract

A separate document [I-D:draft-taddei-smart-cless-introduction] (CLESS) attempts to establish the capabilities and limitations of endpoint-only security solutions and explore potential alternative approaches. That document discusses endpoints in general terms. It has been suggested that there are classes of endpoints that have different characteristics. Those classes may have completely different threat landscapes and the endpoints may have completely different security capabilities. In support of the work on CLESS, this document provides a taxonomy of endpoints that is intended to provide a foundation for further work on CLESS and research on approaches to providing endpoint security alternatives in a diverse group of settings.

Table of Contents

1. Introduction...................................................3
2. Conventions used in this document..............................4
3. Problem Statement..............................................4
4. The Endpoint in CLESS..........................................
5. Taxonomy......................................................5
   5.1. Traditional and Enterprise Computing Equipment [TECE]....6
      5.1.1. Description..........................................
      5.1.2. Endpoint characteristics...........................
      5.2. Personal Computing Equipment..........................
      5.2.1. Description..........................................
      5.2.2. Endpoint characteristics...........................
      5.3. Human Interface Devices...............................8
      5.3.1. Endpoint description................................
      5.3.2. Endpoint characteristics...........................
      5.4. Human Sensor Devices..................................8
      5.4.1. Endpoint characteristics...........................
      5.5. Non-human Sensor Devices..............................9
      5.5.1. Endpoint Description................................
      5.5.2. Endpoint characteristics...........................
      5.6. Peripheral Computing Equipment and Embedded Endpoints....10
      5.6.1. Endpoint Description................................
      5.6.2. Endpoint characteristics...........................
      5.7. Internet Infrastructure Devices........................11
      5.7.1. Endpoint Description................................
      5.7.2. Endpoint characteristics...........................
      5.8. Application Layer Endpoints............................12
      5.8.1. Description..........................................
      5.8.2. Endpoint Characteristics...........................12
6. Security Considerations.....................................12
1. Introduction

A document entitled "Capabilities and Limitations of an Endpoint-only Security Solution (CLESS) [I-D. draft-taddei-smart-cless-introduction-00] attempts to initiate research into the limits of endpoint-only security solutions. The document identifies changes in technology, economics and protocol development that have impacted the provision of endpoint security.

The CLESS introduction focuses on endpoints that are User Equipment rather than hosts. Even so, this encompasses an enormous variety of possible endpoints. CLESS takes a unified view of endpoints - seeing them all as one type.

However, it seems reasonable to suggest that, in the huge variety of types of endpoints, there are categories of similarity. These categories are important because categories of endpoint devices may share particular advantages or limitations for endpoint security. While CLESS provides a clear model for understanding some of the limitations of endpoint security in today’s networks, it is very likely that more specificity is needed.

This draft attempts to suggest a Taxonomy of Endpoints as a foundation for further work on CLESS. The goal is to identify classes of endpoints with similar characteristics. Those characteristics may lead to the discovery that the devices in a particular category share similar characteristics for endpoint security.

It is essential to understand that this taxonomy is intended as a foundation for work on CLESS and is not an all-purpose guide to the enormous breadth of devices that are or could be endpoints on public or private networks. Others have attempted to provide classifications for end devices, but they are not focused on the issues related to endpoint security. In addition, most are almost immediately out-of-date when published.

This document takes a different approach: the taxonomy here is intended to support the work of CLESS and provide a classification system that may make it possible to group endpoints in related
categories for the purpose of discussing their security characteristics. While a general-purpose taxonomy of Internet endpoints might be useful in a variety of settings, it is not the intended goal of this document.

In addition, this document does not attempt to assess and document the endpoint security characteristics of each part of the taxonomy. The work of identifying advantages and limitations of specific classes of endpoints is envisioned as future work on CLESS.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Problem Statement

CLESS attempts to provide an analysis of the current state of the provision of endpoint security. It does that by providing a provisional definition of an endpoint and then examining the advantages and limitations of providing security at that endpoint.

The original approach to CLESS divides the universe of endpoints into User Equipment (UE) and hosts - and then focuses entirely on User Equipment.

User Equipment encompasses a very broad set of endpoints. It may be possible to provide a stronger set of device type groupings. Endpoints in the same groups may share security characteristics that are particular to that group. The fundamental question is: can a taxonomy of endpoint devices be created that allows for grouping of endpoints that have similar security characteristics?

If it is possible to answer that question in the affirmative, then research can be done on the security characteristics of each category and influence the development of protocols that have the greatest impact for those type of devices.

4. The Endpoint in CLESS

CLESS simplifies the representation of an endpoint by making the following generalization:
This simplification means that there are many combinations of hardware, operating systems, execution environments and applications. It also means that any of these three layers can be an endpoint for the purposes of a discussion of endpoint security.

CLESS suggests that we consider endpoints including those which have a variety of power, computational, storage and network capacities. It is possible that grouping devices with similar characteristics will help in identifying categories of devices that share similar endpoint security characteristics.

5. Taxonomy

Others have attempted to provide general-purpose taxonomy and device classification guides (informative references to be provided in a later draft version). In some settings automated detection and classification of devices provides an essential step in providing appropriate access control and security services.

General-purpose classification systems tend to ossify or become enormously complex. Classification has come from commercial entities, computer science organizations, the academic community and even regional collections of cooperating national governments.

For the purposes of providing a taxonomy for CLESS, we limit the discussion to a taxonomy for endpoints only. We divide endpoints into nine different classes and then attempt to carefully describe the characteristics of devices in each class.
5.1. Traditional and Enterprise Computing Equipment [TECE]

5.1.1. Description

Traditional and Enterprise Computing Equipment is characterized by its extremely high-capacity for transactional volume, storage and shared user population. TECE forms the backbone of high-volume, high-availability transactional computing and is provided in both physical and virtualized forms.

Traditional computing endpoints are shared computing environments characterized by centralized, shared computing. These endpoints are often in large scale data centers. These endpoints are capable of high-availability, substantial requirements for power and environmental control. These endpoints are also characterized by very complex operating systems and user environments.

5.1.2. Endpoint characteristics

- Cost - these endpoints are characterized by extremely high cost.
- Physical size - these are very large endpoints, not suitable or intended for use by an individual.
- Network link characteristics - capable of supporting extremely high bandwidth.
- User interface - very complex and shared among multiple individuals.
- Processing power - extremely high processing capability.
- Physical power - requires substantial provision of electrical power and environmental controls.
- Code complexity - Extremely high support for very complex code including parallelism, multitasking and multithreaded execution.

5.2. Personal Computing Equipment

5.2.1. Description

These are endpoints designed or intended to be used by an individual. They can be delivered as fixed, portable or virtual instantiations of the endpoint. It should be noted that virtual instantiations of endpoints introduce complexities in defining the characteristics of the endpoints. In each case, the device supports a mechanism for
human-interface and has the capability for both local storage and processing. The personal computing equipment class is also characterized by relatively low cost and power requirements.

This class of endpoint is also characterized by the devices supporting multiple purpose use. This class is divided into two subclasses: fixed and mobile endpoints. The mobile subclass is further divided into four other subclasses: laptops, tablets, intelligent phones, and ultraportable personal computing equipment.

Personal computing endpoints usually have at least one, and often many, network links - often supporting a variety of network connectivity technologies. These endpoints are also characterized by having a human interface - either integral to the computing device itself or supplied externally to the computing device.

5.2.2. Endpoint characteristics

- **Cost** - these endpoints have a huge range of costs, from extremely inexpensive for simple "personal computer on a board" endpoints to moderately expensive for specially configured laptop and fixed devices.

- **Physical size** - the physical size of these devices range from handheld to a small cabinet for fixed, desktop units.

- **Network link characteristics** - personal computing endpoints are often characterized by supporting multiple connectivity technologies.

- **User interface** - personal computing endpoints are characterized by having user interfaces designed for an individual. The interface varies from simple, text-based interaction to gesture, touch and voice control.

- **Processing power** - these endpoints are characterized by a significant range of processing power: from single CPU units to endpoints that can support multiple concurrent processes.

- **Physical power** - personal computing endpoints are characterized by using either traditional mains power or power supplied by a battery.

- **Code complexity** - personal computing endpoints support complex code and often parallel and multithreaded execution of code.
5.3. Human Interface Devices

TBD.

5.3.1. Endpoint description

5.3.2. Endpoint characteristics

- Cost
- Physical size
- Network link characteristics
- User interface
- Processing power
- Physical power
- Code complexity

5.4. Human Sensor Devices

Description

These are endpoints whose primary purpose is to sense, store, transmit or process information about a human being. These endpoints are characterized as having use cases in health and wellness monitoring, human performance enhancement, personalized medicine and human safety.

The endpoints are characterized as sensor devices with the capacity to sense, store and report on data collected on an individual. The sensor may be multimodal. These endpoints are almost always characterized by have a battery for power and having limited storage, networking and processing capabilities.

5.4.1. Endpoint characteristics

- Cost - Human Sensor Endpoints can range in cost from very low (for instance a heartbeat sensor) to quite expensive (a sensor built into an implanted device).

- Physical size - human sensors are very small and almost always portable.
5.5. Non-human Sensor Devices

5.5.1. Endpoint Description

These endpoints are capable of sensing, storage, communication and possibly some computation. They are characterized by having very low bandwidth radios, a battery for power, sensor technology and a small processor. Unlike in Section 5.4, these devices are not intended to sense human-related information.

Compared with Human Sensors, non-human sensors often have a variety of communications technologies available - for instance, self-organizing into mesh networks.

5.5.2. Endpoint characteristics

- Cost - Non-human Sensor Endpoints can range in cost from very low (for instance, a simple temperature sensor) to quite expensive (a sensor built into an implanted device).

- Physical size - Non-human sensors are often small and almost always portable.

- Network link characteristics - Non-human sensors usually have a single network like technology available but the topology of those network links can be highly varied. Quite often these devices are capable of very limited bandwidth utilization on the link to which they are attached.
o User interface - non-human sensors have extremely limited, or no, user interface.

o Processing power - non-human sensors are characterized by having limited processing power - often incorporating only the ability to collect store and forward sensed information. Some non-human sensors have the capability to process stored data, but usually this is limited.

o Physical power - -

o Code complexity - non-human sensors are not usually capable of running complex code. Often, the capability of the endpoint is to simply sense, store and forward data without reporting and analysis of that data.

### 5.6. Peripheral Computing Equipment and Embedded Endpoints

#### 5.6.1. Endpoint Description

These are endpoints that are "embedded" in devices that may have a different primary function. An example is a network endpoint in a printer that supports remote access, configuration and printing. Another example is an endpoint in an appliance that has a different primary function (for instance, a refrigerator).

In either case, the endpoint is characterized as being added to another system, machine or peripheral.

These devices are characterized as being specialized for their particular use case and function. Their specific characteristics often depend upon the system, device or peripheral in which they are being hosted. As an example, the embedded endpoint gets its physical power and networking capabilities from the device in which it is connected.

#### 5.6.2. Endpoint characteristics

- Cost - almost never available as a standalone device - instead, always embedded into the peripheral or system which is hosting it.

- Physical size - almost always very small - to be embedded into some other system or device.

- Network link characteristics - dependent on network services available from the host device and not always IP-based.
5.7. Internet Infrastructure Devices

5.7.1. Endpoint Description

Internet Infrastructure endpoints are the physical components that are used to deploy a network. There is a huge variety of these devices, but they all share two common properties: they are building blocks of the underlying network infrastructure and they also can be endpoints of a network conversation.

But, there’s an important question here. CLESS specifically rules out network infrastructure in its discussion. Should the taxonomy for CLESS incorporate endpoints that are part of the network infrastructure? Said a different way: is network infrastructure out of scope for CLESS?

5.7.2. Endpoint characteristics

TBD, depending on the answer to the question in section 5.7.1

- Cost
- Physical size
- Network link characteristics
- User interface
- Processing power
- Physical power
- Code complexity
5.8. Application Layer Endpoints

5.8.1. Description

A significant trend in the contemporary public Internet is to have applications act as completely independent agents - a situation where the application itself provides the necessary infrastructure (for instance, domain name resolution) to provide services. An example would be a web browser that independently resolved domain names and established secure communication channels independently.

The traffic between the application and the servers it uses might not be available for analysis by security software. As a result, application-based endpoints would have the characteristic of having to provide security services (for instance, traffic security or malware detection) for itself.

This type of endpoint also has the characteristic of potentially having adverse impacts on other applications running on the same platform. For example, if several applications are provisioning their own infrastructure services, then those services are being duplicated on that platform. For security related infrastructure there would be no common, platform-wide approach to securing the applications or the traffic generated between the application and external servers.

5.8.2. Endpoint Characteristics

TBD

6. Security Considerations

INFO (REMOVE): Every draft MUST have a Security Considerations section.

TBD, descriptive

7. IANA Considerations

This document has no requirements or actions for IANA

8. References

8.1. Normative References

8.2. Informative References

TBD

9. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.
Appendix A. Document History

[[ To be removed from the final document ]]

~0

Initial Internet Draft
Authors’ Addresses

Mark McFadden
Internet policy advisors ltd
Madison Wisconsin US

Email: mark@internetpolicyadvisors.com

Phone: <optional>
Email: <Your email address>