ETSI TS 103 994-1 V1.1.1 (2024-03)

Cyber Security (CYBER);
Privileged Access Workstations;
Part 1: Physical Device

Reference
DTS/CYBER-00115

Keywords
cybersecurity

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

Any function that has administrative permissions is critical to the security of the associated system or network. Such permissions can, for example, enable unrestricted access or allow system protection mechanisms to be bypassed. Because of the dangers of accounts with these privileges being compromised, it is important that administrative actions are performed from well protected and highly trusted source devices, a Privileged Access Workstation (PAW).

Using a PAW device restricts the attack surface of the system, thereby limiting its wider network connectivity, and reducing the application list will limit the ability of an adversary to gain access to the administrative network.

The present document covers the PAW device and the technical specification that would ensure the confidentiality of the end user device. Additional documents will cover other aspects of PAWs that can work in conjunction with each other to meet the needs of the overall system architecture and the relevant security aims.

Introduction

Security incidents happen frequently and, as detection mechanisms increase in ability so do the complexity and sophistication of attacks. The administrative functions within a network are the most critical assets of any network. If an adversary can gain access and modify these administrative functions, by design they are often able to access any data that they retain. This data can then be accessed, modified or monitored for whatever purpose the adversary intended and, with privileged access to administrative functions, logging and auditing can often be subverted to ensure that access can be maintained.

Attacks are often conducted by using techniques such as phishing to trick or socially engineer a human operator but using a PAW significantly reduces the likelihood of such attacks being able to gain access to administrative functions.

The present document describes a set of best practices for Privileged Access Workstations (PAWs) that would help industries to achieve a consistent baseline for protecting high privileged interfaces to their systems. PAWs can mitigate many security threats and can reduce the attack surface of an Operator, their vendors and service providers. Standardisation of these concepts will provide greater consistency, ensure that costs can be reduced for all parties and will help to create a common understanding for implementation.

It is important to note that there is not a one size solution that fits all and there is not an off the shelf solution that will solve the problem. However, designing access carefully for each use case and following the principles below it is possible to limit the attack surface.

1 Scope

The present document provides requirements that are specific enough to define the desired security outcomes, but flexible enough that there can be innovation and different ways for how they can be achieved. Whilst it is initially targeted towards the Telecoms Sector, the principles are designed to be industry agnostic.

The present document covers the device only. Additional documents will cover other aspects of PAWs that can work in conjunction with each other to meet the needs of the overall system architecture and achieve the relevant security aims.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

Not Applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Telecommunications Security Code of Practice (publishing.service.gov.uk).

[i.2] https://attack.mitre.org/.

[i.3] https://uefi.org/sites/default/files/resources/ACPI_Spec_6_5_Aug29.pdf.

[i.4] Internet Network - Artifact Details | MITRE D3FEND™.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

internet: network of multiple, connected networks

NOTE: Internetworking is the practice of connecting a computer network with other networks through the use of gateways that provide a common method of routing information packets between the networks. The resulting system of interconnected networks are called an internetwork, or simply an internet. Internetworking is a combination of the words inter {"between") and networking; not internet-working or international-network. This is defined in [i.4].

Privileged Access Workstation (PAW): appropriately secured device that enables an admin user to access data and/or make changes to security critical functions via a management plane

NOTE: This is defined in [i.1].

Security Critical Function (SCF): 'security critical function' in relation to a telecoms provider means any function of the network or service whose operation is likely to have a material impact on the proper operation of the entire network or service or a material part of it

NOTE: This is defined in [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AV	Anti-virus
CA	Certificate Authority
CIS	Center for Internet Security
EDR	Endpoint Detection and Response Software
MFA	Multi-Factor Authentication
NAT	Network Address Translation
OEM	Original Equipment Manufacturer
OS	Operating System
PAW	Privileged Access Workstation
PIN	Personal Identification Number
SCF	Security Critical Function
SIEM	Security Information and Event Management
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
XSS	Cross Site Scripting

4 PAWs

A Privileged Access Workstation (PAW) shall be a physical device (e.g. laptop). It is designed to be a highly trusted device enabling secure system administration to be undertaken. The PAW device and management system shall be designed to mitigate well known, common types of attacks faced by running an externally facing network e.g. the internet.

The PAW device by design shall significantly limit the ability of threat actors to take control of the devices and any connected networks. The PAW device and management system shall be designed in a way to mitigate the risks identified with running a low confidence device. It shall ensure that all activity carried out by a person is non-repudiable, logged and auditable.

A PAW itself is not the only element required to ensure the security of the management network, and security best practice should always be followed. Additional mitigations may be required if the PAW is also used for other activities.

5 Threats

The MITRE Attack framework [i.2] describes a number of persistence, privilege escalation and defence evasion techniques that could be used with the overall aim being to gain access to privileged information and exfiltrate data. These are the threats that the present document focusses on addressing.

Threat Vector	Risk
Drive by Compromise	Access can be gained from visiting a website with malicious content e.g. JavaScript, iFrames or XSS (Cross site-scripting). This could be down to the user clicking a link - often a referrer or shorten link without knowing the true destination. Alternatively, it could be that a known website has been hijacked and malicious content has been embedded which would execute without the user knowing.
Exploitation of Application or Remote Services	A running service which exposes a TCP/IP port on a device can be used to gain access to the device, whilst end user devices are typically behind a NAT (Network Address Translation), (which means they are not directly reachable from the internet) this does not stop a local attacker gaining access to the device (e.g. where the device is on an untrusted network - Open Wi-Fi®) or where an attacker has already gained network access and can now move laterally within a network.
Phishing	A very common attack vector is to send genuine looking emails from a known good source hoping to gain the users trust so that they click a link or open a file. This file or browser link would then contain some form of first stage executable with the aim of gaining privileged access to the system. As the device is internet connected this foothold can then be used by an adversary to initiate further access to the device.
Software Supply Chain	Software supply chain attacks are becoming far more common. This is where a 3rd party's software has been compromised and the malicious code is then filtered down through software patches. Due to the device having open internet access, malicious code would be able to communicate back to the originator, thus enabling further access.
Removable Media	A USB Drive/SD Card is used to transfer files; however, the volume could contain malicious code which can execute as the drive is attached to the device, thus providing an adversary with a foothold into the device.
Valid account access	The use of a valid user account to gain privileged access into a system. The attacker could be using a stolen device with poor password management, or it could be a stolen authentication token used to gain remote access.

6 Specification

A PAW shall be a physical device.

A PAW shall support UEFI, secure boot and a hardware root of trust (e.g. TPM 2.0 or later) and shall ensure these are enabled.

A PAW shall have a unique set of credentials (i.e. not shared with a Corporate Identity Provider) and shall use hardware based Multi-Factor Authentication (MFA) i.e. "something you know or something you are".

The PAW operating system image shall originate and be verified from a trusted source (i.e. the OEM or OS Vendor). For example, using a validated checksum.

A PAW shall use an approved application list. The operating system mechanism shall enforce this approved application list and log any attempts of execution by unapproved applications. This will minimize the potential for malicious code execution.

A PAW shall only have limited access to publicly available internet services where there is a requirement to access these services for its function as a PAW. For example, Device Management Services, Endpoint protection applications (e.g. AV/EDR). These services should be explicitly allowed via URL filtering/firewall rules, with the default position to block all other services.

Application isolation features (e.g. Application Guard) where a local hypervisor is used to provide application separation should also be considered for any internet connecting applications.

The PAW shall not be allowed direct access to communication services (i.e. email/messaging applications) or document storage drives that are accessible from outside of the PAW network.

A PAW shall support and use data-at-rest encryption backed by a hardware root-of-trust.

A PAW shall be kept patched and up to date with a supported OS throughout its lifetime. This will require a patch import solution specifically designed for the PAW.

Patches shall be deployed to PAWs as soon as practicable and robust alternative mitigations put in place until the relevant patch has been deployed. **Critical patches** should be applied to PAWs within 14 days.

A PAW shall prevent the execution of unauthorized code such as binaries or macros within documents.

A PAW shall use data-at-rest encryption to maintain security of data in case of theft or loss. This should incorporate use of a hardware-backed element such as a TPM, and in the case of full-disk encryption this should be unlocked with a PIN or passphrase prior to boot.

All new deployments of equipment shall be administered via secure, encrypted, and authenticated protocols. Insecure or proprietary security protocols shall be disabled.

Approved removable media list - removable media use should be blocked by default, and only used by exception. Regular data transfer should be performed via a specially designed Import/Export function.

Use of 'regular' user accounts - network administrators should use non-privileged accounts on their local PAW device for performing administrative activity within the network. I.e. Least privilege at all times.

Feed into monitoring - all PAW-like devices should be incorporated into available security monitoring systems for the detection of malicious or unusual activity.

The device shall have a policy applied that provides the following (as a minimum):

- Operating System lockdown, restrict/remove any function that is not required for the device's usage as a PAW (e.g. CIS Hardening guidelines).
- Prevention of unauthorised code execution e.g. use of restricted application lists and block the execution of alternative binary's (e.g. .dll).

- Policy shall define that full Audit/Logging events are created (e.g. Success and Failure and stopping of services such as AV) and ensure logging is captured into the PAW Network. This should be incorporated into available security monitoring systems for the detection of malicious or unusual activity.
- The use of cryptography shall be defined by policy.

If additional CAs (Certificate Authority Root Keys) need to be trusted (e.g. for third party access) these shall be defined in policy and shall not be installable by the end user.

7 How does a PAW mitigate the threats

Given all the defensive mechanisms in place against the initial access threats, the ability of an adversary to gain further access is severely limited. All event logging shall be captured and sent to a SIEM system where it should be monitored. The restrictive policy lockdown and the limited application scope should mean that event logging should be predictable, and any logging that occurs outside of the normal scope should be easily identifiable and investigated.

Taking each of the previous threats it is possible to see how an effective PAW can mitigate these.

Threat Vector	Mitigation	Effect on Attack Vector
Drive by Compromise	Removal of directly internet connected services	The device does not have access to services outside of the privileged network. This makes it extremely difficult for an adversary to send any form of malicious payload via scripting or iframe insertion.
Exploitation of Application of Remote Services	Significantly reduced attack surface	A PAW device is designed to be locked down and no local services should be accessible via the local network. Suitable policy should be in place to enforce this (e.g. Firewall policy). Without open ports the attack surface of the device is significantly reduced, and so the ability of an adversary is reduced.
Phishing	Removal of directly internet connected services	A PAW device has no direct access to internet services such as email or Instant Messaging services, therefore the ability to send malicious links directly to the PAW device via the user is removed. If a user is accessing email or internet services via a cross domain solution, this shall contain any malicious execution within that network segmentation.
Software Supply Chain	Removal of directly internet connected services	Software packages used within the PAW shall come from a trusted source, and the software should be approved and limited to only what is required to operate as a PAW. Even if software on the device is compromised, without direct internet access it would be severely limited in its ability to operate within a closed network especially with restricted removable media access. Policy lockdown should prevent and log software operating outside of its intended function. The audit logs of the device should be reviewed regularly (i.e. by SIEM Dashboard/SOC) and unusual activity should be spotted by these processes.
Removable Media	Significantly reduced attack surface by limited this access	Policy lockdown on the device should restrict the ability for the user to use any removable media, removing the ability for adversary to spread or exfil via this method.
Valid account access	Significantly reduced attack surface due the closed network and use of MFA	Accounts for the PAWs network should only be usable within the restricted network (used for system administration) meaning an outside attack should not be possible. Whilst a PAW device could be stolen, the use of MFA and encryption at rest (including a TPM) should minimize the opportunity for the thief to make use of the device.

Annex A (informative): Bibliography

- https://attack.mitre.org/tactics/TA0001.
- CNI system design: Secure Remote Access - NCSC.GOV.UK.
- ETSI GR NFV-SEC 007 (V.1.1.1): "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".
- ETSI TR 103 308 (V1.1.1): "CYBER; Security baseline regarding LI and RD for NFV and related platforms".

Annex B (informative): Change history

Date	Version	Information about changes
December 2023	0.0.1	First draft
February 2024	0.0.2	Now drafted as a TS. A few other changes made. Stable draft
February 2024	0.0.3	Updated with minor comments during #Cyber37
February 2024	0.0.4	General tidy up ready for remote consensus
February 2024	0.0.5	Final tidying - including document title

History

Document history		
V1.1.1	March 2024	Publication