ETSI TR 103 421 V1.1.1 (2017-04)

CYBER;
Network Gateway Cyber Defence

Reference

DTR/CYBER-0015

Keywords

cyber security, information assurance, privacy

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**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

The present document provides an overview and recommendations concerning cyber defence capabilities at network gateways. The capabilities are implemented using what are usually referred to as "middleboxes" that may be integrated into traffic routers that typically exist at boundaries between networks. Network gateways are critically important points for implementing cyber defence in conjunction with other essential functions.

The present document notes that network gateway cyber defence related standards activities have increased significantly because of an array of use cases combined with the rapidly increasing encryption of traffic occurring between end points where network application servers are interacting directly with software clients on end user devices. The use cases consist of an array of business and compliance obligations. The present document then continues to derive a set of related cyber defence technical requirements that include:

1) secure and controlled exposure of traffic observables;

2) sufficient observable information for acquisition and analysis for defence measures; and

3) the ability to institute defence measures as part of gateway management.

The present document then examines the emerging new challenges and mechanisms for gateway cyber defence. The challenges include virtualization implementations, 5G mobile systems, Internet of Things deployments, Over The Top services, and "encrypt everything" initiatives. On the positive side, the considerable industry and academic research and development efforts have produced a combination of existing protocol adaptations and effective new protocols and platforms that have considerable promise - especially one known as mcTLS.

The present document concludes with several recommendations that include a consensus view on what information and secure access capabilities are required to support gateway cyber defence, what steps the ETSI Cybersecurity Technical Committee should take for a new Technical Specification to support the requirements, and how collaboration with external bodies might encourage use of gateway cyber defence capabilities.

Introduction

A network gateway is a device that enables or facilitates the interconnecting of networks or applications via those networks. They have existed since the origins of electronic communication. With the emergence of packet data networks, they have assumed many different roles, including cyber defence. Those additional roles are commonly denominated as "middlebox" functions [i.3]. An especially common network gateway used for cyber defence purposes is referred to as a *firewall* - defined by 3GPP as a functional entity which blocks or permits the flow of various traffic types based on a set of policy rules and definitions. All signalling to internal network resources can be directed via a network gateway dedicated to that purpose.

Network gateways serve many critical needs that include management of network traffic and meeting service level agreement or regulatory requirements. One of those critical needs is that of cyber defence - which can be met through the detection and prevention of threats at the external border point of all kinds of networks ranging from a national infrastructure to an organization or home network. Deep Packet Inspection capabilities are widely deployed to facilitate these capabilities. However, the appearance of ever more sophisticated threats and adaptive malware is proving challenging to detection and blocking efforts.

A significant cyber security challenge emerging today is the combination of Over the Top services combined with "encrypt everything" initiatives that generated potentially huge amounts of traffic between some arbitrary service portal somewhere in the world, and an end user's terminal - even an application on a device. Some Internet of Things implementations also fall into this category. While these steps meet significant needs today, these practices may have adverse effects such as impeding detection of malware and other cyber security threats, as well as managing network traffic and meeting a broad array of business, organizational, and regulatory requirements. A balanced approach is needed that provides support to all the requirements that exist today.

The emergence of NFV-SDN implementations is engendering considerable new efforts to virtualize network gateway capabilities. These efforts include the use of on-demand Big Data Analysis to more rapidly detect and mitigate threats.

Many different industry forums today are examining network gateway requirements and solutions available - largely as insular work items and projects. The present document assembles an understanding of the related ecosystem, models, protocols, and implementation mechanisms for gateway-based cyber defence.

1 Scope

The present document provides an overview and recommendations concerning cyber defence capabilities at network gateways. It analyses the network gateway cyber defence ecosystem, technical requirements, new challenges and techniques and then draws recommendations for new standardization work in that area.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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] SIGCOMM '15, Naylor et al., Multi-Context TLS (mcTLS): "Enabling Secure In-Network Functionality in TLS", August 17- 21, 2015, London, United Kingdom.

NOTE: Available at http://conferences.sigcomm.org/sigcomm/2015/pdf/papers/p199.pdf.

[i.2] ETSI TR 103 456: "CYBER; Implementation of the Network and Information Security (NIS) Directive".

[i.3] IETF RFC 3224: "Middleboxes: Taxonomy and Issues", February 2002.

[i.4] IETF draft-mm-wg-effect-encrypt-04: "Effect of Ubiquitous Encryption", October 2016.

[i.5] OASIS CybOX™ Version 2.1.1. Part 01: "Overview".

NOTE: Available at http://docs.oasis-open.org/cti/cybox/v2.1.1/cybox-v2.1.1-part01-overview.pdf. See also, CybOX Project/specifications, https://github.com/CybOXProject/specifications/wiki.

[i.6] NIST SP 800-117: "Guide to Adopting and Using the Security Content Automation Protocol (SCAP)".

[i.7] SP 800-126 Revision 2: "The Technical Specification for the Security Content Automation Protocol (SCAP)".

[i.8] Recommendation ITU.T X.1500: "Overview of cybersecurity information exchange".

NOTE: See http://www.itu.int/itu-t/recommendations/rec.aspx?rec=11060.

[i.9] IETF RFC 7632: "Endpoint Security Posture Assessment: Enterprise Use Cases".

[i.10] IETF draft-ietf-sacm-requirements-15: "Security Automation and Continuous Monitoring (SACM) Requirements".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-sacm-requirements/.

[i.11] ETSI TS 101 331 (V1.4.1): "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.12] ETSI TS 133 106 (V13.4.0): "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Lawful interception requirements (3GPP TS 33.106 version 13.4.0 Release 13)".

[i.13] ETSI TS 102 656 (V1.2.2): "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".

[i.14] Recommendation ITU-T X.1038: "Security Requirements and reference architecture for Software-Defined Networking" (10/2016).

NOTE: Available at http://www.itu.int/itu-t/recommendations/rec.aspx?rec=13058.

[i.15] 5G PPP Architecture Working Group, View on 5G Architecture, Version 1.0, July 2016.

NOTE: Available at https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-July-2016.pdf.

[i.16] European Commission, Copyright and Neighbouring Rights.

NOTE: Available at , http://ec.europa.eu/internal_market/copyright/documents/index_en.htm.

[i.17] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[i.18] StepExchange: "Combatting nuisance calls and texts".

NOTE: Available at https://www.stepchange.org/Portals/0/documents/media/reports/additionalreports/Designed_nuisance_calls_appendix_final.pdf.

[i.19] ENISA: "Resilience and security of communication infrastructure, networks and services".

NOTE: Available at https://resilience.enisa.europa.eu/.

[i.20] CRS: "National Security and Emergency Preparedness Communications", 19 September 2012.

NOTE: Available at https://fas.org/sgp/crs/natsec/R42740.pdf.

[i.21] ACM: "Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking".

NOTE: Available at http://dl.acm.org/citation.cfm?id=3010079.

[i.22] Securebox: Toward Safer and Smarter IoT Networks.

NOTE: Available at https://www.cs.helsinki.fi/u/yding/publications/securebox-pre-camera.pdf.

[i.23] Embark: "Securely Outsourcing Middleboxes to the Cloud".

NOTE: Available at http://forum.stanford.edu/events/2016/slides/iot/Chang.pdf.

[i.24] Draft Recommendation ITU-T Y.gw-IoT-arch: "Functional architecture of gateway for IoT applications".

[i.25] Draft Recommendation ITU-T Y.IoT-cdn: "Framework of constrained-device networking in the IoT environments".

[i.26] ResearchGate: "Impact of Over the Top (OTT) Services on Telecom Service Providers".

NOTE: Available at https://www.researchgate.net/publication/276175550_Impact_of_Over_the_Top_OTT_Services_on_Telecom_Service_Providers.

[i.27] MarketsandMarkets: "Over the Top Market by Content Type, by Platform (Smart Devices, Laptops, Desktops, and Tablets), by Service (Consulting, Installation, and Maintenance), by Revenue Model, by Deployment Model, by Vertical, by User Type, by Region - Global Forecast to 2020".

NOTE: Available at http://www.marketsandmarkets.com/Market-Reports/over-the-top-ott-market-41276741.html.

[i.28] IAB: "The effect of encrypted traffic on the QoS mechanisms in cellular networks".

NOTE: Available at https://www.iab.org/wp-content/IAB-uploads/2015/08/MaRNEW_1_paper_25.pdf.

[i.29] BuiltWith®: "SSL by Default Usage Statistics".

NOTE: Available at https://trends.builtwith.com/ssl/SSL-by-Default.

[i.30] IAB: "Managing Radio Networks in an Encrypted World (MaRNEW) Workshop 2015".

NOTE: Available at https://www.iab.org/activities/workshops/marnew/.

[i.31] Fraunhofer FKIE: "White Paper on Encrypted Traffic Management", January 2016.

NOTE: Available at http://images.machspeed.bluecoat.com/Web/BlueCoat/%7Bab90f902-7c34-440d-a933-0a33f59718ce%7D_20160421-ETM-Paper_English_final.pdf.

[i.32] Layer 9: "Session 4 (Middleboxes) -- Paper 1: Multi-Context TLS (mcTLS): Enabling Secure In-Network Functionality in TLS".

NOTE: Available at http://www.layer9.org/2015/08/session-4-middleboxes-paper-1-multi.html.

[i.33] Intel®: "Intel® Software Guard Extensions (Intel® SGX)".

NOTE: Available at https://software.intel.com/en-us/sgx.

[i.34] Recommendation ITU-T X.1542: "Session information message exchange format".

3 Definitions and abbreviations

3.1 Definitions

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

firewall: functional entity which blocks or permits the flow of various traffic types based on a set of policy rules and definitions

middlebox: any intermediary box performing functions apart from normal, standard functions of an IP router on the data path between a source host and destination host, including network gateways [i.3]

network gateway: device or system that enables or facilitates the interconnecting of networks or applications via those networks

observable: described definitive characteristic of an object observed in the cyber environment that facilitates a common structure relating to the specification, capture, characterization and communication of events [i.5]

3.2 Abbreviations

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

3GPP	Third Generation Partnership Project
5GPPP	5G Infrastructure Public Private Partnership
ACM	Association for Computing Machinery
ALPN	Application-Layer Protocol Negotiation

API	Application Program Interface
ARF	Asset Reporting Format
AT-TLS	Application Transparent Transport Layer Security
ATTM	Access, Terminals, Transmission and Multiplexing committee
CA	Certification Authority
CAGR	Compound Annual Growth Rate
CBOR	Concise Binary Object Representation
CCSS	Common Configuration Scoring System
CN	Core Network
CPE	Common Platform Enumeration
CRS	Congressional Research Service
CTI	Cyber Threat Intelligence
CYBEX	Cybersecurity Information Exchange
CybOX	Cyber Observable Expression
DLP	Data Loss Prevention
DMCA	Digital Millennium Copyright Act
DPI	Deep Packet Inspection
ECMA	European Computer Manufacturers Association
ECN	Explicit Congestion Notification
ENISA	European Union Agency for Network and Information Security
ETI	Encrypted Traffic Inspection
EV	Extended Validation
FKIE	Fraunhofer Institute for Communication, Information Processing and Ergonomics
GSM	Global System for Mobile communication
GSMA	GSM Association
HICCUPS	Handshake-based Integrity Check of Critical Underlying Protocol Semantics
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure (also HTTP over TLS)
IAB	Internet Architecture Board
IACD	Integrated Adaptive Cyber Defence fabrics
ID	Identity
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPR	Intellectual Property Requirements
IPS	Intrusion Prevention Systems
ISG	Industry Specification Group
ISP	Internet Service Provider
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
LTE	Long Term Evolution
MAEC	Malware Attribute Enumeration and Characterization
MAMI	Measurement and Architecture for a Middleboxed Internet
MARCOM	Marketing and Communications
mbTLS	Middlebox Transport Layer Security
mcTLS	Multi-Context Transport Layer Security
MITM	Man In The Middle
MNO	Mobile Network Operator
MSP	Multihoming Service Provider
NAT	Network Address Translation
NFV	Network Functions Virtualisation
NFV-SDN	Network Functions Virtualisation-Software Defined Networks
NGFW	Next Generation FireWalls
NIS	Network and information systems
OASIS	Organization for the Advancement of Structured Information Standards
OpenC2	Open Command and Control
OS	Operating System
OSP	Online Service Provider
OTT	Over The Top
OVAL	Open Vulnerability and Assessment Language
PPP	Public Private Partnership
RAN	Radio Access Network

RAR	Rotate And Release
RFC	Request For Comments
SACK	Selective Acknowledgment
SACM	Security Automation and Continuous Monitoring
SCAP	Security Content Automation Protocol
SCP	Smart Card Platform
SDN	Software Defined Network
SEMI	Stack Evolution in a Middlebox Internet
SGX	Software Guard Extensions
SIMEF	Session Information Message Exchange Format
SPAN	Services and Protocols for Advanced Networks
SPUD	Substrate Protocol for User Datagrams
SSL	Secure Sockets Layer
STIX	Structured Threat Information eXchange
TCP	Transmission Control Protocol
TG	Throughput Guidance
TGK	Telekommunikationsgesetz (Telecommunications Law)
TIPHON	Telecommunications Internet Protocol Harmonization Over Networks
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TLS-AUX	Transport Layer Security Auxiliary Data
TLS-RaR	Transport Layer Security Rotate and Release
TMSAD	Trust Model for Security Automation Data
UDP	User Datagram Protocol
UE	User Entity
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USD	US Dollars
VM	Virtual Machine
WAN	Wide Area Network
XCCDF	Extensible Configuration Checklist Description Format

4 Network gateway cyber defence ecosystem: activities and use cases

4.1 Introduction - the gateway as a protection element

This clause provides an overview of the gateway as a protection element by describing the diverse standards activities occurring in industry bodies as well as gateway cyber defence business and compliance obligation use cases.

As stated in the introduction a system may be protected by a firewall that exposes the system through managed entry points. The normal visualization of a wall is misleading and in fact a more realistic visualization is that of an enclosing sphere, with the entry point, the gateway, being the only access to the protected domain. Thus, for a gateway to work the core assertion for security is that the gateway is the only access point to the protected domain.

A gateway as the point of access to the internal network may need to prevent access to hostile users, traffic and content. In order to achieve this, the capabilities at the gateway are necessarily broad in scope and deep in terms of protocol stacks. For example, protection against malicious payloads may require that file transfers are cached at the gateway and examined to identify the presence of viruses or Trojan horses and similar. If a protected domain is subject to a Denial of Service attack it may be necessary to distribute the gateway itself away from the protected domain.

A gateway may act to police traffic leaving the protected domain in addition to policing traffic entering the protected domain. This may be achieved using the same techniques in each direction. Port filtering of IP packets has been used but such practices can be bypassed, and if this is done, the bypass should not result in a security leak. Thus, middlebox techniques to ensure safe and secure firewall traversal may be required to be implemented at the gateway.