ETSI TR 103 743 V1.1.1 (2021-07)

CYBER;
Home Gateway Security Threat Analysis

Reference
DTR/CYBER-0056

Keywords
cybersecurity, home gateway, threat analysis

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

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

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.

Introduction

The aim of a Home Gateway (HG) is, in part, to enforce segregation of devices in the home network from the public internet.

An HG is most often installed in a "safe" environment from the perspective of the consumer. Whilst there is growing hearsay, evidence and understanding that "the internet" has many risks to the unwary user, there is often a less rigid and structured approach to safety and security in zones that are considered as safe environments, such as the home, where an HG is most likely to be deployed. As an instance of a complex IoT device the HG is expected to comply to the set of baseline security measures identified in ETSI EN 303 645 [i.7], it is also expected that the developer of the HG has completed the Implementation conformance statement provided in Annex B of ETSI EN 303 645 [i.7].

1 Scope

The present document provides an analysis of cyber security threats specific to Home Gateways (HGs) and an introduction to measures for risk mitigation posed by these threats.

Whilst the provisions of ETSI EN 303 645 [i.7] assist in moving towards having secure by default devices on the market, the deeper understanding of the forms of vulnerability faced by an HG are addressed in the present document. The present document is intended to give advice to suppliers and manufacturers of the risks of deployment of HGs in order to give confidence to consumers in the security of HGs deployed in the home.

The detailed specification of the measures to mitigate these risks will be addressed in a separate technical specification.

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] "The STRIDE Threat Model", Microsoft™ Corporation.

NOTE: Available at https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

[i.2] R. Klöti, V. Kotronis and P. Smith: "OpenFlow: A security analysis", 2013 21st IEEE International Conference on Network Protocols (ICNP), Goettingen, 2013, pp. 1-6, doi: 10.1109/ICNP.2013.6733671.

[i.3] BSI TR-03148: "Secure Broadband Router", Version 1.1, 30 April 2020.

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=1.

[i.4] IEEE 802.11™-2016: "IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

NOTE: Available at https://ieeexplore.ieee.org/document/7786995.

[i.5] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.6] B. Schneier: "Attack Trees Modeling security threats', Dr. Dobb"s Journal, December 1999.

[i.7] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.8] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.9] ETSI TR 103 370: "Practical introductory guide to Technical Standards for Privacy".

[i.10] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.11] IEEE 802.3™-2012: "IEEE Standard for Ethernet".

NOTE: Available at https://standards.ieee.org/standard/802_3-2012.html.

[i.12] ETSI TS 102 527-3: "Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT; Part 3: Extended wideband speech services".

[i.13] Recommendation ITU-T G.992.5: "Asymmetric digital subscriber line 2 transceivers (ADSL2)-Extended bandwidth ADSL2 (ADSL2plus)".

NOTE: Available at https://www.itu.int/rec/T-REC-G.992.5-200901-I/en.

[i.14] IEEE 802.15.1™-2002: "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)".

[i.15] ETSI TS 103 523-1: "CYBER; Middlebox Security Protocol; Part 1: MSP Framework and Template Requirements".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

non-volatile memory: random-access memory that retains data without applied power

open source software: source code that is made freely available for possible modification and redistribution

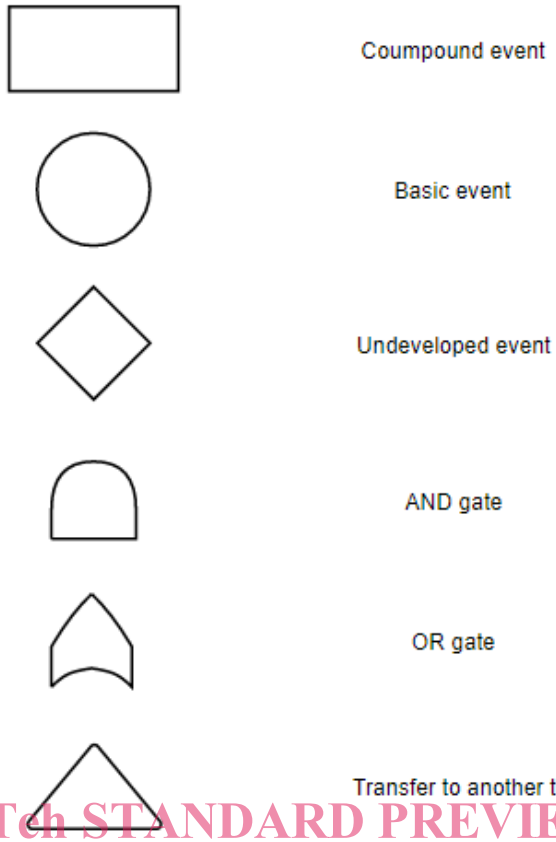
threat: potential cause of an incident that can result in harm to a system or organization

NOTE 1: A threat consists of an asset, a threat agent and an adverse action of that threat agent on that asset.

NOTE 2: A **threat** is enacted by a **threat agent**, and can lead to an **unwanted incident** breaking certain pre-defined security objectives.

3.2 Symbols

For the purposes of the present document, the following symbols apply for the visualization of the attack trees.



compound event: group of actions to be further broken down or a group of basic events

basic event: single action that can be readily performed

undeveloped event: group of actions, without further description

NOTE: Some well-known and versatile methods such as social engineering and man-in-the-middle attack are not further expanded in the attack tree.

AND gate: all of the child elements are executed

OR gate: at least one of the child elements is executed

transfer to another tree: attack tree is contained in another diagram

3.3 Abbreviations

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

ADSL	Asymmetric Digital Subscriber Line
BCS	British Computer Society
BSI	Bundesamt für Sicherheit in der Informationstechnik; Federal Office for Information Security (Germany)
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
ENISA	European Network Information Security Agency
GSM	Global System for Mobile communication
GSMA	Global System for Mobile communication Association
HG	Home Gateway
IP	Internet Protocol
ISP	Internet Service Provider

IT	Information Technology
JTAG	Joint Test Action Group
LAN	Local Area Network
NAT	Network Address Translation
NCSC	National Cyber Security Centre
NVM	Non-Volatile Memory
OS	Operating System
OWASP	Open Web Application Security Project
PCB	Printed Circuit Board
SC	Supply Chain
SQL	Structured Query Language
SSH	Secure Shell
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege
SW	SoftWare
SYN	SYNchronize
TC	Technical Committee
TVRA	Threat Vulnerability and Risk Assessments
USB	Universal Serial Bus
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi™	Wireless Fidelity (deprecated)

NOTE: Wi-Fi™ is a trademark of the non-profit Wi-Fi™ Alliance, which restricts the use of the term Wi-Fi™ Certified to products that successfully complete interoperability certification testing.

WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XSS	Cross-Site Scripting

4 Home Gateway Threat Analysis and Modelling

4.1 Home Gateway characteristics

For the purposes of the present document the Home Gateway (HG) is defined as a physical device that lies between the in-home network and the public network with a primary purpose of dividing and isolating home network traffic from external network traffic. It can be provided for retail purchase by the user or can be supplied as part of a service contract with the Internet Service Provider (ISP).

The HG can exist in a number of configurations. To simplify analysis for the purposes of the present document the HG is configured as containing the following functional components:

- Wi-Fi access point (IEEE 802.11 [i.4] as modelled by the Wi-Fi Alliance);
- LAN router (IEEE 802.3 [i.11] in 10BASE10, 100BASE10 or 1000BASE10 options);
- DECT [i.12] or VoIP phone connectivity;
- ADSL [i.13] or equivalent WAN connection;
- in addition the HG can offer additional proprietary wireless capabilities, e.g. IEEE 802.15.1 [i.14] (part of the Bluetooth® suite).

A typical configuration of the HG is presented in Figure 1.

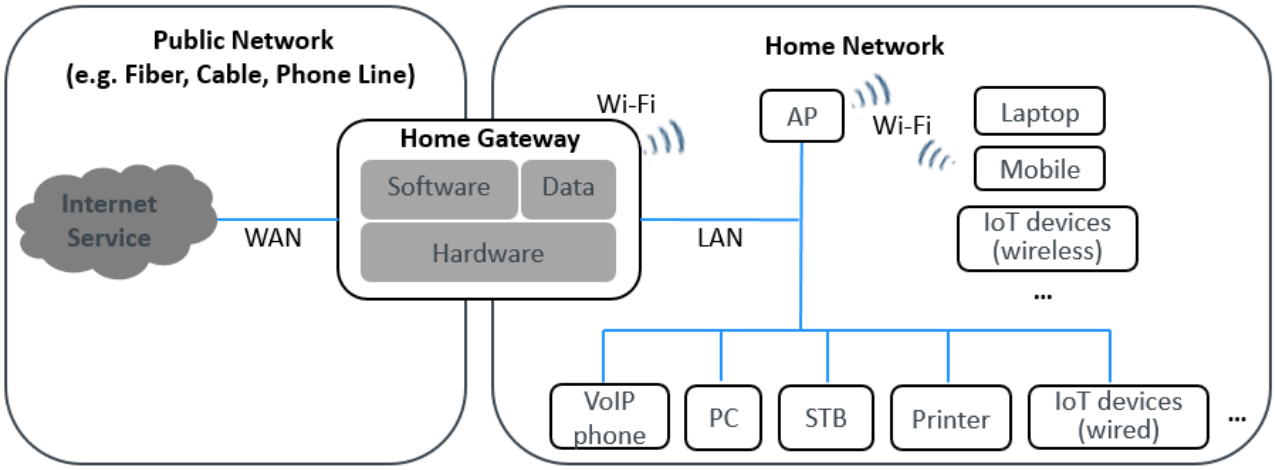


Figure 1: Typical HG configuration and deployment

There is assumed to be no restriction on availability of the HG and thus attackers are considered as having freedom of access to the HG. Adopting the metrics of ETSI TS 102 165-1 [i.5] the attacker can be assumed to have unrestricted access to an instance of the HG in order to develop attack strategies and to maximize each of system knowledge (i.e. of the HG), time (i.e. to optimize the time required to be able to launch an attack), expertise (i.e. time to develop knowledge of the HG's operation, weaknesses and vulnerabilities), and each of opportunity and equipment (i.e. develop means of access and any equipment in addition to the HG in order to launch an attack).

The HG should be provisioned in such a way that any sensitive configuration data is not accessible to normal user accounts, but rather a privileged administrator account should be required to update configuration or to analyse administrative data (e.g. log files).

4.2 Attack model

4.2.1 Introduction

Points of attack to the HG include the open interfaces of the home network side of the HG, interfaces open on the ISP side of the HG, and the supply chain of the HG, as shown in Figure 2.

NOTE: The owner/user of the HG can act as an attacker either deliberately or by accident, or act as a vector in some forms of attack.

The HG is considered as user accessible, i.e. the device can be opened and a user can examine the PCB and other components internal to the device. This is addressed in ETSI TS 102 165-1 [i.5] in consideration of the likelihood of attack and the metrics of ETSI TS 102 165-1 can be used to inform analysis of the STRIDE [i.1] approach.

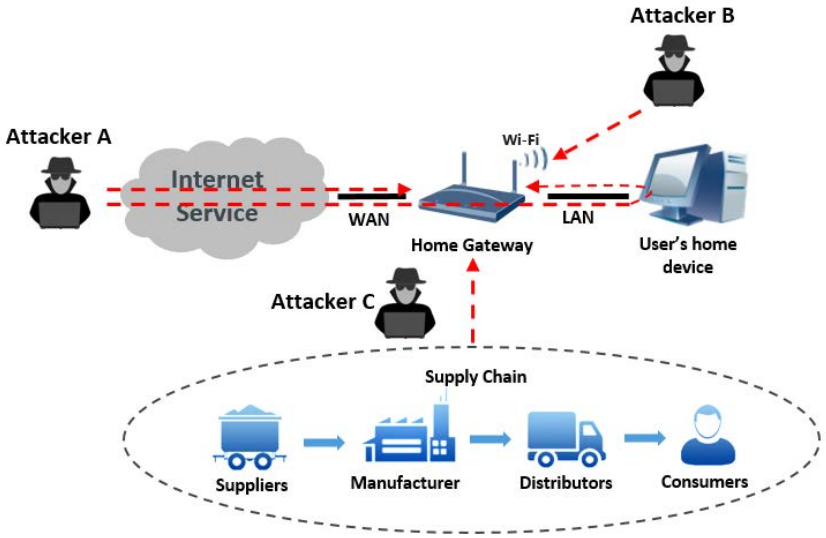
In adopting the risk measurement approach identified in ETSI TS 102 165-1 [i.5] where risk is the product of impact and likelihood it is noted that for a generic installation of an HG there is a wide range of impacts from any successful attack. The specific impact of any attack should therefore be considered in detail before use of any vulnerable equipment. The present document only addresses "medium" and "high" level of threat where the resultant impact of an attack addresses the interests of providers/subscribers and cannot be neglected. The threat analysis in the present document covers both attacks targeted at the device and attacks targeted at the transmission media, such as optical-fibre and cable, between the HG and other network elements at WAN side, and Wi-Fi at LAN side.

In the case where an attacker can access components a suitably motivated and skilled attacker can undertake sufficient reverse engineering on the HG to develop specific attacks, or to implement known attacks requiring specialized access. In addition, the normal safety provisions required for market access apply and warnings on loss of liability if a user interferes with the device should be taken as a basic precaution.

It is assumed that the HG can be reset to factory or ISP defined default wherein the default configuration is maintained in immutable storage.

The HG can include the ability for the vendor or the ISP, as instances of an authorized party, to remotely manage and maintain the device including delivering system configuration and firmware updates.

The attack analysis focuses on three sets of attack interfaces of the HG as shown in Figure 2.



NOTE: The model above is derived and extended from BSI TR-03148 [i.3].

Figure 2: Reference model of Attack interfaces (point of access)

Attacker A scenario in Figure 2 describes attacks via the Wide Area Network (WAN) interface.

Attacker B scenario in Figure 2 describes attacks via the Local Area Network (LAN) or Wireless LAN (WLAN) interface.

Attacker C scenario in Figure 2 describes attacks across the supply chain in a form of an insider attack.

EXAMPLE: Attacker C exploits supply chain weakness and plants malicious advertising software or crypto-money mining software in the HG for monetary gain.

The threat analysis in the present document takes the capabilities of all the three attackers depicted above into consideration.

4.2.2 The approach to HG risk analysis

ETSI's TVRA as defined in ETSI TS 102 165-1 [i.5], combined with the STRIDE™ [i.1] and [i.2] methodology for the identification of computer security threats, has been applied to the HG attack scenarios framework in the present document.

Table 1: Threats to security objective types (from ETSI TS 102 165-1 [i.5]) extended to STRIDE

Threat	STRIDE (see note)	Objective type				
		Confidentiality	Integrity	Availability	Authenticity	Accountability
Interception (eavesdropping)	Information disclosure	X				
Unauthorized access	Information disclosure Elevation of Privilege	X	X		X	X
Masquerade	Spoofing	X	X		X	X
Forgery	Spoofing Tampering		X	X	X	X
Loss or corruption of information	Tampering Information disclosure		X	X		
Repudiation	Repudiation		X		X	X
Denial of service	Denial of Service			X		
NOTE: The STRIDE method categorizes the threats into six threat types, mapped to the conventional threats in this table.						

4.2.3 Attack Trees as a modelling tool

The attack tree is an attacker-centric approach to reveal the vulnerabilities of a system and visualizes the decomposition of the final goal of an attack into different sub-goals and attack paths, the branches in a tree structure. The tree structure simplifies the overview even over complex attack paths. An overview of the use of attack trees to model how an attacker can achieve a goal is given by Schneier [i.6] and a worked example is given in "OpenFlow: A security analysis" [i.2].

A number of attacker goals are analysed in the present document using the attack tree approach, with weightings applied to each leaf of the attack tree according to the metrics of ETSI TS 102 165-1 [i.5] modified as shown in the present document. As defined by Schneier [i.6] the root node of an attack tree is the goal of the attack and different ways to achieve that goal are leaf nodes. In many attacks several individual leaves of the tree need to be instantiated to achieve success. The attack tree is itself a representation of a logic equation and can be represented in Boolean logic (see symbols defined in clause 3.2).

EXAMPLE: The attack goal is to obtain access to the HG from LAN side. For this attack to succeed, the attacker needs to be in range of the Wi-Fi connection AND connect to the HG AND hack the administrator account. To connect to the HG, the attacker can obtain the guest Wi-Fi first AND jump to main Wi-Fi through crosstalk OR hacking the main Wi-Fi credentials with WEP OR WPA cracking. Administrator account can be obtained through password-based hacking techniques which is extended in another subtree. This goal is characterized by the attack tree as shown in Figure 3.