# 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

# 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

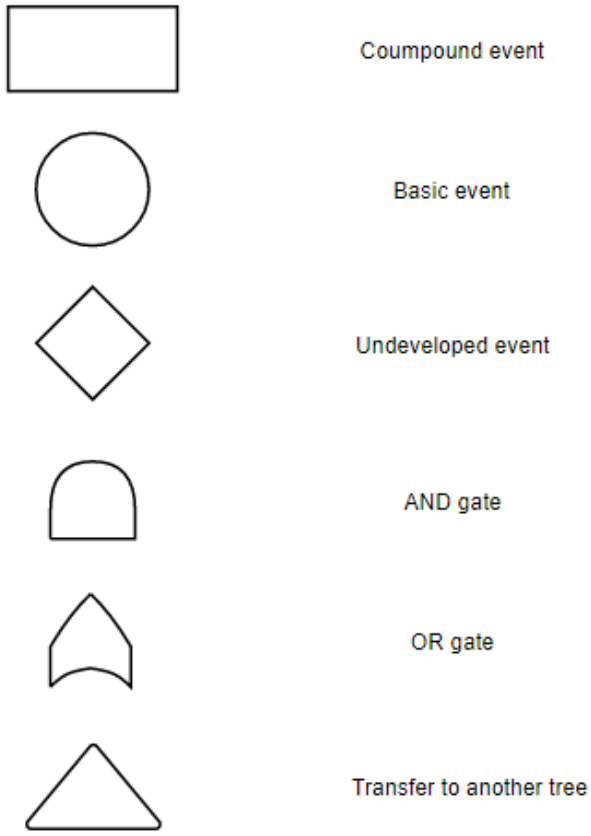
**threat:** potential cause of an incident that can result in harm to a system or organization

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;<br>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.

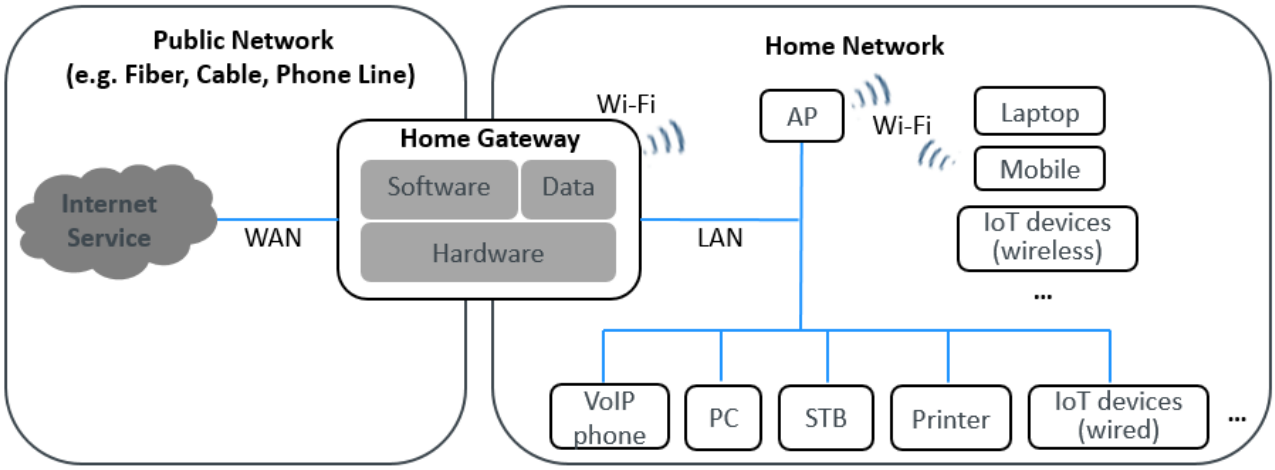



**Figure 1: Typical HG configuration and deployment**

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.

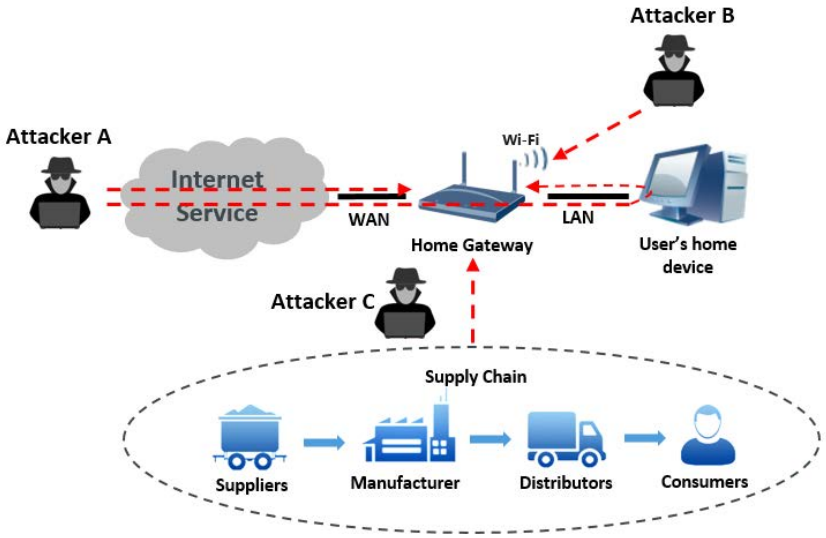
In adopting the risk measurement approach identified in ETSI TS 102 165-1 [i.5] where risk is the product of impact and likelihood it is noted that for a generic installation of an HG there is a wide range of impacts from any successful attack. The specific impact of any attack should therefore be considered 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<br>Elevation of Privilege | X | X | | X | X |
| **Masquerade** | Spoofing | X | X | | X | X |
| **Forgery** | Spoofing<br>Tampering | | X | X | X | X |
| **Loss or corruption of information** | Tampering<br>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.

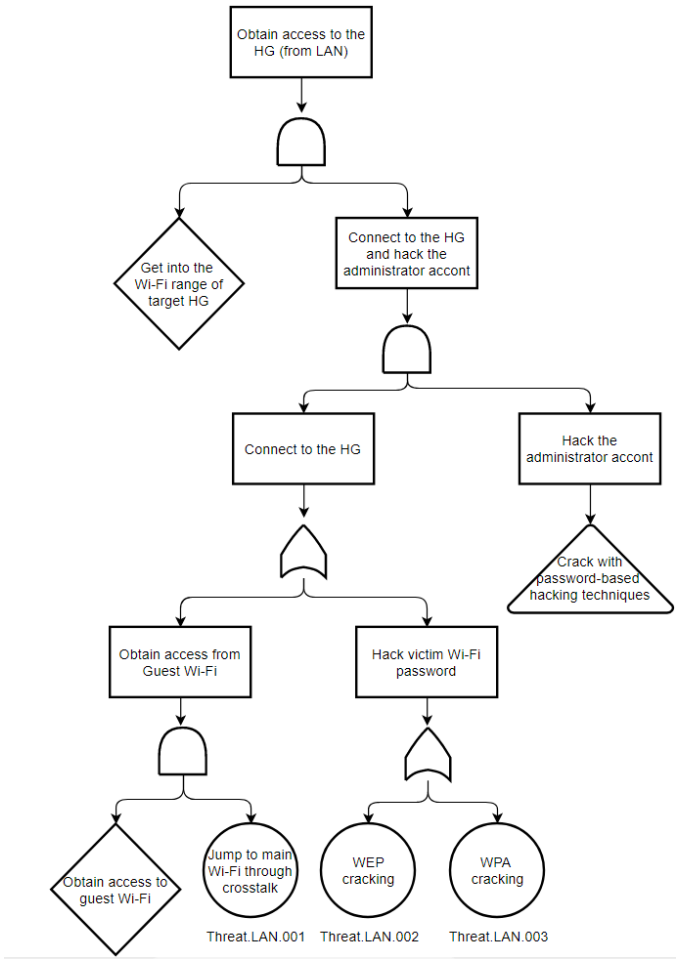



**Figure 3: Simplified attack tree for obtaining access to the HG from LAN**

In the present document, the attacks faced by the HG are categorized into WAN, LAN and supply chain, the three typical attack interfaces described in Figure 2. Then the attack tree visualizes the details for each attack. The major attack on the top-down direction of the tree is built out of several small attack paths or branches. The attack trees cover up-to-date attack strategies and methods to raise the awareness of security in home gateway design.

NOTE: The metrics described in ETSI TS 102 165-1 [i.5] to assess the attack potential required to exploit a vulnerability include the following: System knowledge; Time; Expertise; Opportunity; and, Equipment. In addition, clause 6.6.4 of ETSI TS 102 165-1 [i.5] addresses the role of motivation of an attacker which is combined with capability to properly assess likelihood of an attack.

## 4.3 Pre-existing work

ETSI EN 303 645 [i.7] offers baseline security provisions for consumer IoT devices. In addition ETSI TR 103 309 [i.8] and ETSI TR 103 370 [i.9] provide guidelines for security by default and privacy by design. For some aspects of design ETSI TR 103 305-1 [i.10] defines cyber security controls applied to IoT. For detection and mitigation purposes defences such as those defined for middle boxes may be applied in ETSI TS 103 523-1 [i.15] are relevant for home gateways.

# 5 Attacks via the WAN interface

## 5.1 Overview of attack surface and attacker goals

In this scenario, scenario A in Figure 2, the attacker is outside the consumer location and attacks the HG across the public Internet.

A number of assumptions apply to this scenario:

- if the HG is supplied by the ISP the ISP enables the connection and can, subject to appropriate contract and consent restrictions, manage the device;
- the ISP can perform certain actions that restrict the behaviour of the HG, e.g. traffic throttling;
- the technical makeup of the HG is such that there is a clear distinction between traffic in the external network (e.g. for scenario A attacks) and the internal network (e.g. for scenario B attacks); and
- logging of actions on the HG are maintained separately for each of the WAN and LAN sides of the HG.

Attacks launched or made available over the public internet are assessed to have unlimited access and any time factor to launch attacks is unrestricted.

The HG presents a single physical interface to the WAN, visible by the source IP address presented in any communication from the device.

NOTE 1: The provision of broadband access from the home premises is assumed to be subject to a contractual agreement between the ISP and the consumer and any action of either party in accordance with that contractual agreement, e.g. fair use criteria, is not considered as an attack in the context of the present document.

NOTE 2: In some states the provision of a broadband service to a consumer is covered by specific legislation which can impose conditions on the specifications of the HG to be supplied to consumers (e.g. for the United Kingdom The Electronic Communications (Universal Service) (Broadband) Order 2018 applies).

## 5.2 Primary attacker goals, scenario A

### 5.2.1 Inject and execute malware

In this attack scenario the attacker aims to inject malware and execute it on targeted HG for some (undefined) malicious gain. The attack tree is shown in Figure 4.

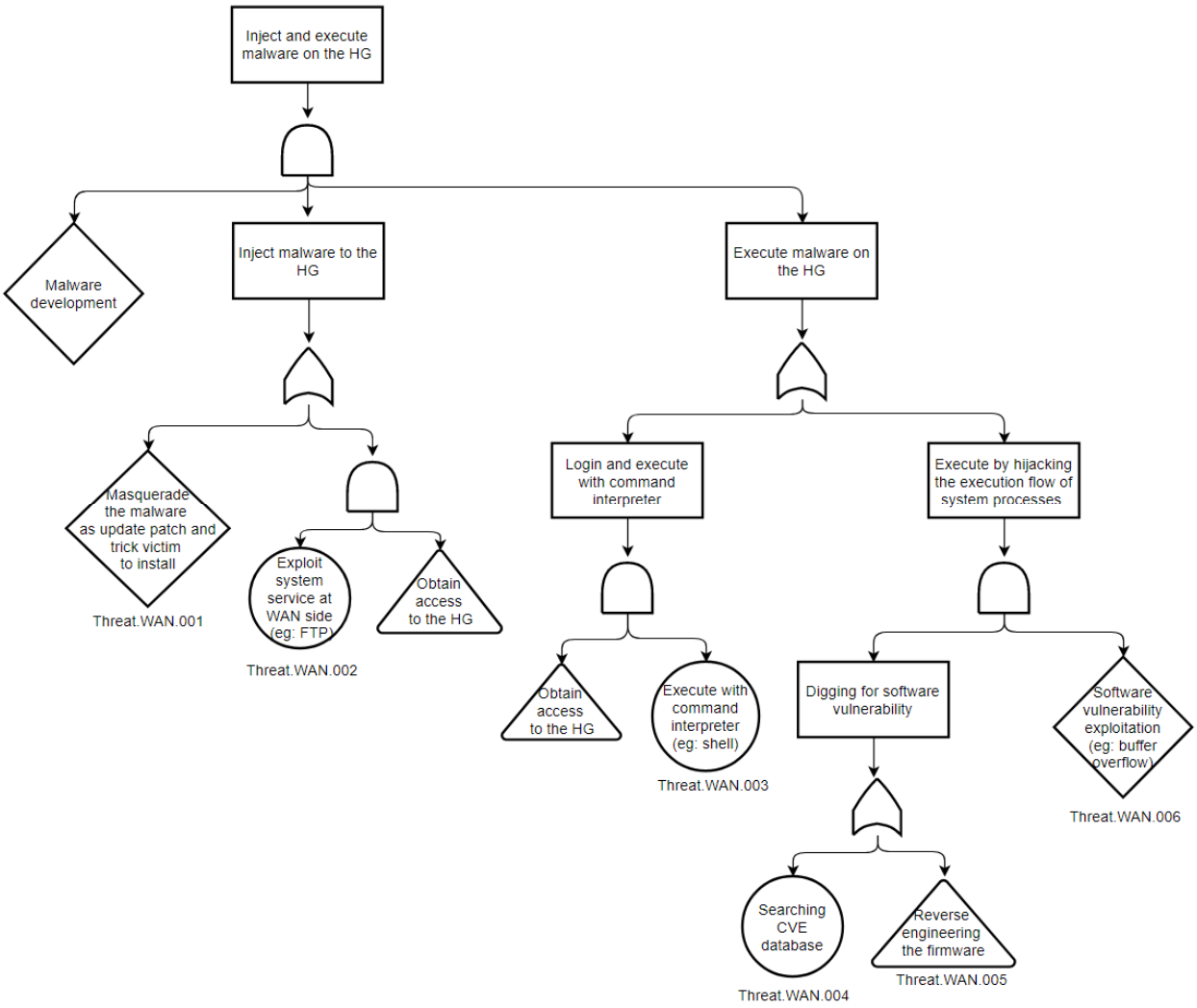



**Figure 4: Attack tree of injecting and executing malware on HG**

- **Threat.WAN.001** An attacker develops malware and masquerades it as update patch. The malicious update patch can then be pushed to the victim with means like phishing.
- **Threat.WAN.002** An attacker obtains control of the HG and transfers the malware to the target HG through services at the WAN side.
- **Threat.WAN.003** An attacker attempts to obtain access to the HG and then executes malware with command interpreter.
- **Threat.WAN.004** An attacker searches the CVE® database to identify reported software vulnerabilities to be further exploited.
- **Threat.WAN.005** An attacker reverses engineers software in order to identify vulnerabilities by in the firmware.
- **Threat.WAN.006** The attacker exploits identified software vulnerabilities to hijack the execution flow and execute malware.

The attacker has several paths to achieve the goal according to the attack tree in Figure 4. Each path indicates a specific threat to the HG. The assets involved in the attacks and the mitigation techniques is summarized as in Table 2.

**Table 2: Summary of threats and mitigation approaches for injecting and executing malware on HG**

| Asset Category | Asset | Threat | Description | Mitigation techniques |
|---|---|---|---|---|
| Software | Firmware | Threat.WAN.001 | An attacker develops malware and masquerade it as update patch. The malicious update patch can then be pushed to the victim with means like phishing. | Secure update, anti-rollback protection |
| | | Threat.WAN.005 | An attacker reverse engineers software in order to identify vulnerabilities in the firmware. | Firmware package encryption |
| | System application | Threat.WAN.002 | An attacker obtains control of the HG and transfers the malware to the target HG through services at the WAN side. | Authentication, Security by default |
| | | Threat.WAN.003 | An attacker attempts to obtain access to the HG and then execute malware with command interpreter. | |
| | | Threat.WAN.006 | The attacker exploits identified software vulnerabilities to hijack the execution flow and execute malware. | Secure coding |
| | OS | Threat.WAN.004 | An attacker searches the CVE® database to identify reported software vulnerabilities to be further exploited. | OS vulnerability management |
| | Plugins | Threat.WAN.004 | An attacker searches the CVE® database to identify reported software vulnerabilities to be further exploited. | 3rd party SW isolation |

### 5.2.2 Obtain access to HG from WAN

Obtaining access to the HG from the open Internet is a key milestone in many cyberattacks. To achieve the goal, the attacker needs to crack an administrator password and find an interface to log in the HG. The attack tree of this goal is described in Figure 5.

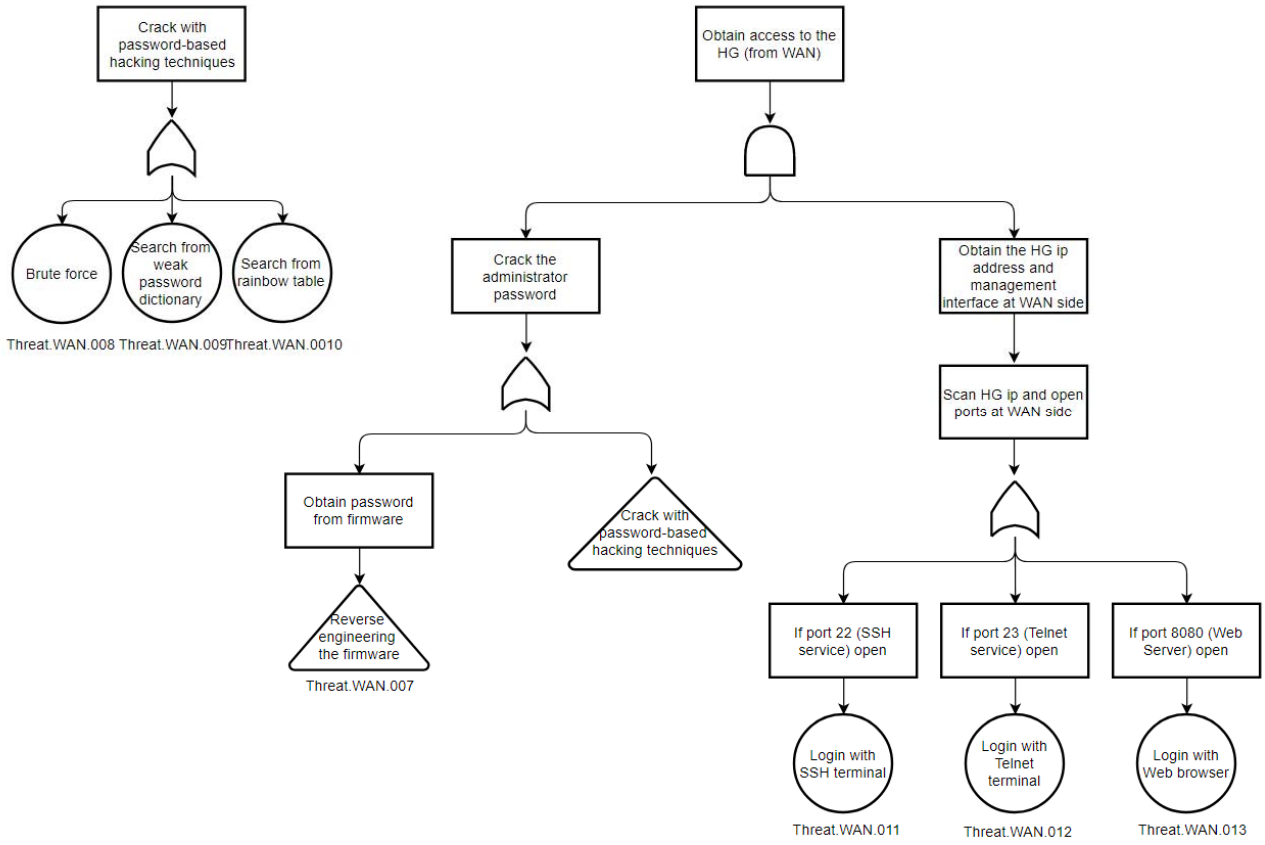



**Figure 5: Attack tree of obtaining access to HG from WAN**

- **Threat.WAN.007** The attacker attempts to obtain a hard-coded password from the firmware.
- **Threat.WAN.008** An attacker cracks the administrator password with a brute force technique.
- **Threat.WAN.009** An attacker cracks the administrator password with a dictionary-based attack.
- **Threat.WAN.010** An attacker cracks the hashed password with rainbow table searching.
- **Threat.WAN.011** The attacker logs into the HG with cracked credentials using SSH terminal.
- **Threat.WAN.012** The attacker logs into the HG with cracked credentials using Telnet terminal.
- **Threat.WAN.013** The attacker logs into the HG with cracked credentials through web browser.

NOTE 1: It is assumed that the attacker cannot access a password from user documentation or from service documentation for the specific HG model.

NOTE 2: Whilst threats WAN.011/012/013 refer to specific interfaces used for management protocols the general assumption is that all open management interfaces are vulnerable, including any proprietary protocols.

**Table 3: Summary of threats and mitigation approaches for obtaining access to HG from WAN**

| Asset Category | Asset | Threat | Description | Mitigation techniques |
|---|---|---|---|---|
| Software | Credential | Threat.WAN.007 | The attacker attempts to obtain a hard-coded password from the firmware. | Credential security |
| | | Threat.WAN.008 | An attacker cracks the administrator password with a brute force technique. | |
| | | Threat.WAN.009 | An attacker cracks the administrator password with a dictionary-based attack. | |
| | | Threat.WAN.010 | An attacker cracks the hashed password with rainbow table searching. | |
| | System application | Threat.WAN.011 | The attacker logs into the HG with cracked credential using SSH terminal. | Security by default |
| | | Threat.WAN.012 | The attacker logs into the HG with cracked credential using Telnet terminal. | |
| | | Threat.WAN.013 | The attacker logs into the HG with cracked credential through web browser. | |

## 5.2.3 Disrupt or disable the services

One motivation of attacking the HGs from open Internet is disrupting or disabling the HG in large scale. There are various tactics to achieve the goal. In the present document, two popular methods are analysed as shown in Figure 6.

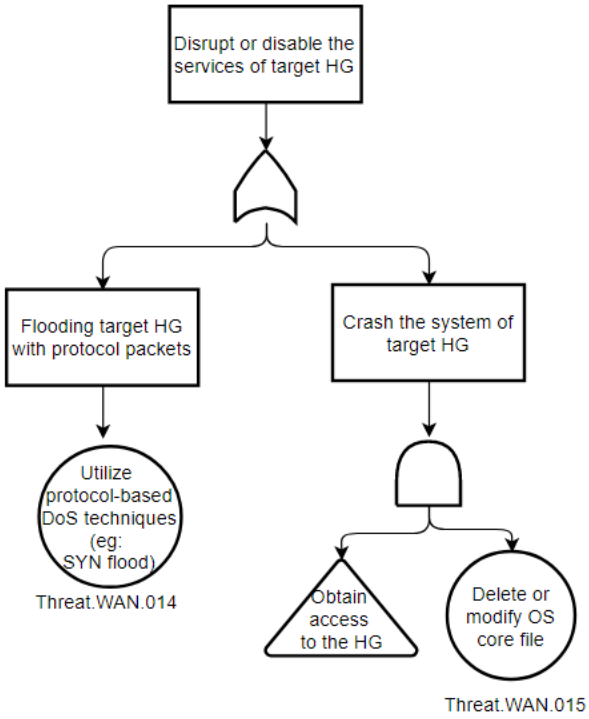



**Figure 6: Attack tree of disrupting or disabling the HG**

- **Threat.WAN.014** An attacker floods the target HG using protocol-based DoS techniques such as SYN flood.
- **Threat.WAN.015** An attacker obtains access to the HG first and modify OS core file to cause the system crash and denial of service (this threat and attack also addresses use of exploitable bugs in the OS).

The asset involved and mitigation techniques are summarized as in Table 4.

**Table 4: Summary of threats and mitigation approaches for disrupting or disabling the HG**

| Asset Category | Asset | Threat | Description | Mitigation techniques |
|---|---|---|---|---|
| Software | System Application | Threat.WAN.014 | An attacker floods the target HG using protocol-based DoS techniques such as SYN flood. | Firewall, Anti-DoS/DDoS, CPU-overload control |
| Data | Configuration file, System core data | Threat.WAN.015 | An attacker obtains access to the HG first and modify OS core file to cause the system crash and denial of service. | Access control, file integrity protection |

## 5.2.4 Packet interception (sniffing)

Information disclosure is another big threat to users. HG can be a weak point in data transmission if the data is not properly encrypted before going to the open Internet. Packet sniffing is such a goal for attackers to obtain user's traffic data. The attack tree is shown in Figure 7.

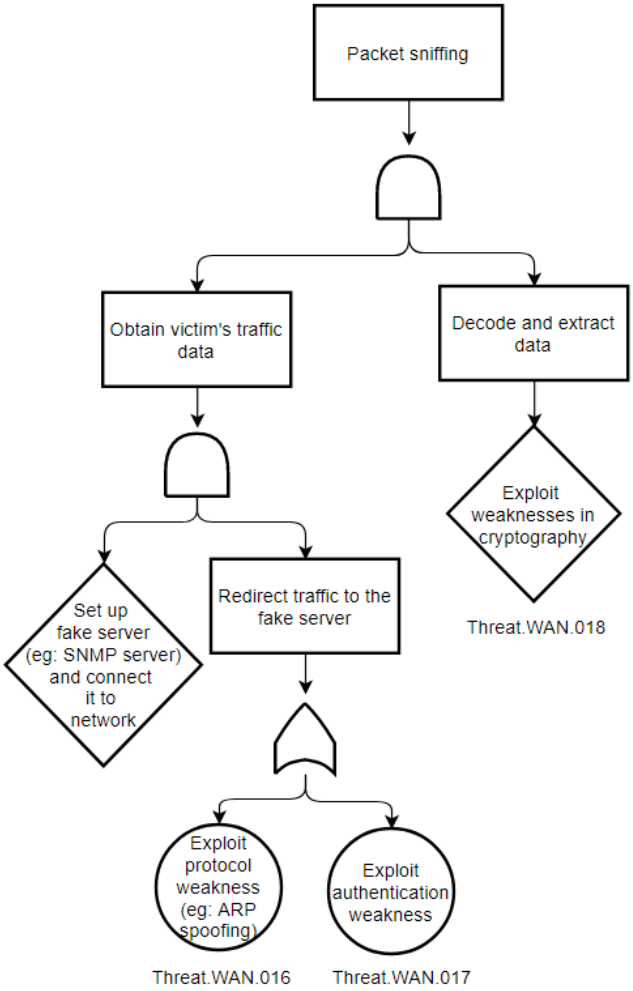



**Figure 7: Attack tree for packet interception**

- **Threat.WAN.016** An attacker redirects the victim's traffic to a fake server by exploiting protocol weakness.

EXAMPLE: ARP spoofing is such a technique to achieve the goal.

- **Threat.WAN.017** An attacker tricks the target HG to connect with a fake server by exploiting authentication weaknesses.

NOTE 1: One-way authentication is a weakness which can be exploited in this scenario since the HG does not authenticate the identity of the server communicating with it.

- **Threat.WAN.018** The attacker decodes and extracts plain text from the traffic data, which might be encrypted, by exploiting a weakness in cryptography, or by exploiting weaknesses in encoding that provides visibility of non-encrypted data that would not otherwise be seen.

NOTE 2: Weaknesses in cryptography include short encryption keys, legacy encryption algorithm, etc.

NOTE 3: Some weaknesses on the use of cryptography are imposed relating to the use of dual use technologies and applicable national or international restrictions.

The assets involved and the mitigation techniques are summarized as in Table 5.

**Table 5: Summary of threats and mitigation approaches for packet interception**

| Asset Category | Asset | Threat | Description | Mitigation techniques |
|---|---|---|---|---|
| Software | System Application | Threat.WAN.016 | An attacker redirects the victim's traffic to a fake server by exploiting protocol weakness. | Firewall |
| Data | Stream data | Threat.WAN.017 | An attacker tricks the target HG to connect with a fake server by exploiting authentication weaknesses. | Secure data transfer |
| | | Threat.WAN.018 | The attacker decodes and extracts plain text from the traffic data, which might be encrypted, by exploiting a weakness in cryptography. | Key management, Secure data transfer, voice service security |

## 5.2.5 Erasure of evidence of attacks

If the HG implements any security logging features, for example to record suspicious actions on the devices including but not restricted to such actions as illegal file modification, or to record unsuccessful login attempts, an attacker can attempt to clear any logged evidence of attack.

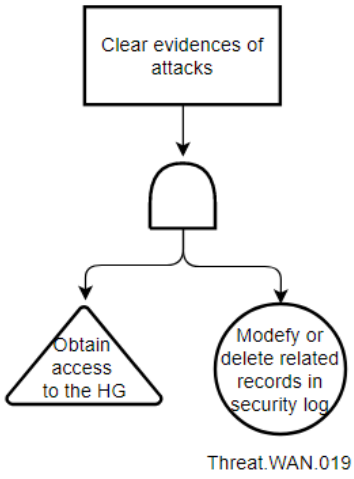



**Figure 8: Attack tree of clearing evidence of attacks**

- **Threat.WAN.019** An attacker modifies or deletes records in the security log to avoid being tracked.

The asset involved and mitigation techniques are summarized in Table 6.

**Table 6: Summary of threats and mitigation approaches for clearing evidence of attacks**

| Asset Category | Asset | Threat | Description | Mitigation techniques |
|---|---|---|---|---|
| Data | Log | Threat.WAN.019 | An attacker modifies or deletes records in the security log to avoid being tracked. | Access control, log backup |

# 6 Attacks via the LAN interface

## 6.1 Overview of attack surface and attacker goals

In this scenario, scenario B in Figure 2, the attacker is actually or virtually inside the consumer location and attacks the HG as if he were an inside attacker.

NOTE 1: If the attacker can physically access the HG the level of attack open to the attacker is increased substantially. The mitigation of such attacks (e.g. directly inserting a malicious device into an open port of the HG) is not considered in the present document as it often involves taking measures that are not unique to HGs but which are expected to be considered as part of a wider home security capability (e.g. locking doors and windows, restricting access to trusted individuals).

The HG in most consumer configurations presents multiple physical interfaces to the device, thus all of the Ethernet, USB and phone ports, the various radio interfaces, are all points of access to the HG.

It is assumed that the IP addresses used in the LAN are not visible outside of the LAN.

NOTE 2: The use of DHCP and similar give address segregation of the LAN and WAN, mostly using IPv4 addresses in the range 192.168.1.1 to 192.168.1.255 on the LAN side and use Network Address Translation (NAT) to map addresses inside the network to WAN addresses. Similar capabilities exist for IPv6 networks.

## 6.2 Primary attacker goals, scenario B

### 6.2.1 Obtain access to HG from LAN

The attack described in this clause is the generalization of the example given in Figure 3. The motives for this attack can change the impact adjudged by the user but do not alter the likelihood of an attack itself. As identified in the illustrated attack tree of Figure 3 the attacker needs physical proximity to the HG. The attack tree of this goal is shown in Figure 9.

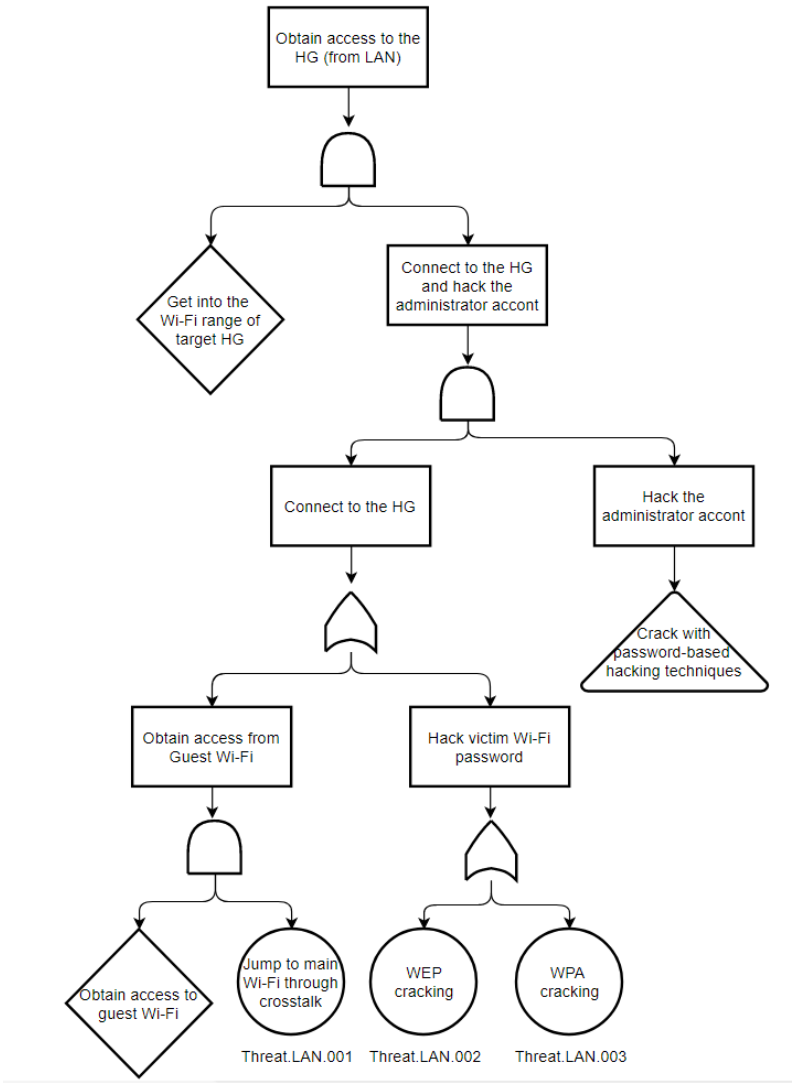



**Figure 9: Attack tree of obtaining access to HG from LAN**

- **Threat.LAN.001** An attacker connects to the guest Wi-Fi and exploits a crosstalk weakness to access the main Wi-Fi connection.
- **Threat.LAN.002** An attacker cracks the Wi-Fi credentials with WEP cracking technique.
- **Threat.LAN.003** An attacker cracks the Wi-Fi credential with WPA cracking technique.

The assets and mitigation techniques are summarized in Table 7.

**Table 7: Summary of threats and mitigation approaches for obtaining access to HG from LAN**

| Asset Category | Asset | Threat | Description | Mitigation techniques |
|---|---|---|---|---|
| Data | Stream Data | Threat.LAN.001 | An attacker connects to the guest Wi-Fi and exploits a crosstalk weakness to access the main Wi-Fi connection. | Wi-Fi Security |
| | | Threat.LAN.002 | An attacker cracks the Wi-Fi credentials with WEP cracking technique. | |
| | | Threat.LAN.003 | An attacker cracks the Wi-Fi credential with WPA cracking technique. | |

### 6.2.2 Reverse engineering the firmware

A malicious user of the HG can obtain firmware with physical means and reverse engineer the firmware to exploit vulnerabilities which can be further used in attacks from WAN side.

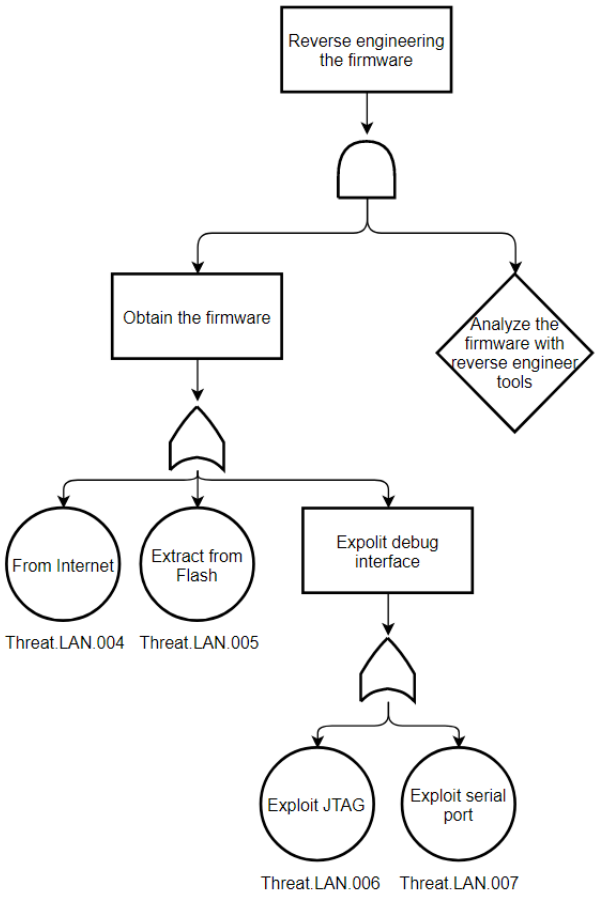



**Figure 10: Attack tree of reverse engineering the firmware**

- **Threat.LAN.004** An attacker downloads the firmware of the target HG class from the Internet.
- **Threat.LAN.005** An attacker extracts the firmware from NVM with hardware tools such as a flash reader.
- **Threat.LAN.006** An attacker obtains the firmware through the JTAG interface.
- **Threat.LAN.007** An attacker obtains the firmware by exploiting the serial port.

The assets involved and the mitigation techniques are summarized in Table 8.

**Table 8: Summary of threats and mitigation approaches for reverse engineering the firmware**

| Asset Category | Asset | Threat | Description | Mitigation techniques |
|---|---|---|---|---|
| Hardware | NVM | Threat.LAN.005 | An attacker extracts the firmware from NVM with hardware tools such as a flash reader. | NVM encryption |
| | Debug/test interfaces | Threat.LAN.006 | An attacker obtains the firmware through the JTAG interface. | Debug/Test interface security |
| | | Threat.LAN.007 | An attacker obtains the firmware by exploiting the serial port. | |
| Software | Firmware | Threat.LAN.004 | An attacker downloads the firmware of the target HG from the Internet. | Firmware package encryption |

# 7 Attacks across the supply chain

## 7.1 Overview of attack surface and attacker goals

In scenario C in Figure 2, the attacker is outside the consumer location and attacks the HG as a device somewhere in the supply chain. Attacks in this scenario include both the logistics supply chain delivering a personalized product to a particular customer, and attacks against the general class of devices from a manufacturer or integrator.

NOTE 1: This scenario by default includes attacks initiating at the original manufacturer.

NOTE 2: A class of device in this instance refers to a general instance of a device and not any bespoke or custom configured device.

The supply chain presents multiple physical and logical attack interfaces to the HG and can present a considerably higher level of risk and impact to the consumer.

## 7.2 Primary attacker goals, scenario C

### 7.2.1 Inject malware into firmware

The malware can be injected as described in clause 5.2.1, but a more concealed way to achieve the goal is compromising the supply chain. Since the infected firmware is burned into the devices in a large scale before the HG reaches the hands of customers and the firmware is typically trusted at the first boot up, the malware is difficult to be distinguished at runtime.

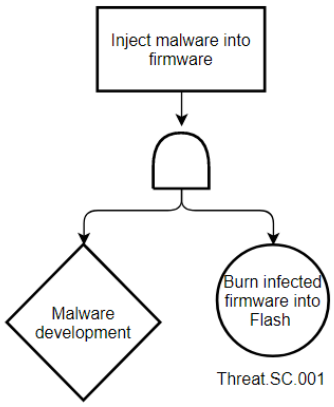



**Figure 11: Attack tree of injecting malware into firmware**

- **Threat.SC.001** An attacker performs a supply chain attack and plants malware into the firmware.

The assets and mitigation techniques are summarized in Table 9.

**Table 9: Summary of threats and mitigation approaches for injecting malware into firmware**

| Asset Category | Asset | Threat | Description | Mitigation techniques |
|---|---|---|---|---|
| Software | Firmware | Threat.SC.001 | An attacker performs a supply chain attack and plants malware into the firmware. | Secure boot |

# Annex A:
# Software development guidelines

On the assumption that the HG is not a programmable device from the perspective of the user/consumer, and that the HG does not allow for user installable software, the following guidelines address the supply chain and specifically mitigations to ensure compliance to the objectives of ETSI EN 303 645 [i.7].

In the absence of a single software development guideline from ETSI, a number of links are offered in Table A.1, to accredited and respected sources.

**Table A.1: Sources for software development guidance/guidelines**

| Source | Website | Scope |
|---|---|---|
| NCSC (UK National Cyber Security Centre) | https://www.ncsc.gov.uk/collection/developers-collection | Lifecycle |
| BCS (British Computer Society) | https://www.bcs.org/content-hub/10-best-practices-for-secure-software-development/ | Best practice |
| ENISA (European Network Information Security Agency) | https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/internet-infrastructure/secure-software-engineering | Lifecycle |
| GSMA (GSM Association) | https://www.gsma.com/security/resources/the-security-of-open-source-software-deployment/ | Best practice - Open Source software use |
| OWASP (Open Web Application Security Project®) | https://owasp.org | Best practice |

A recommendation of the present report is that a guide to software development is prepared by ETSI.

# Annex B:
# Indicative mapping to provisions of ETSI EN 303 645

The scope of ETSI EN 303 645 [i.7] makes it clear that home gateways are covered by its provisions. The following quote from the EN reinforces that ETSI EN 303 645 [i.7] applies to the same environment as the present document.

ETSI EN 303 645 [i.7] *"… specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. The associated services are out of scope. A non-exhaustive list of examples of consumer IoT devices includes:*

- *connected children's toys and baby monitors;*
- *connected smoke detectors, door locks and window sensors;*
- ***IoT gateways, base stations and hubs to which multiple devices connect;***
- *smart cameras, TVs and speakers;*
- *wearable health trackers;*
- *connected home automation and alarm systems, especially their gateways and hubs;*
- *connected appliances, such as washing machines and fridges; and*
- *smart home assistants".*

The highlighted example is the subject of the present document, therefore the present document should be seen as providing the basis of a more detailed examination, and specialization, of the provisions from ETSI EN 303 645 [i.7]. The present document does not of itself define the necessary specializations for HGs to build from ETSI EN 303 645 [i.7], such provisions are to be addressed in further technical specification that map to the provisions identified in the body of the present document and summarized in Tables 2 through 9. Table B.1 that follows gives an indicative mapping of results of the analysis to provisions of the EN which will be examined in more detail in future work.

**Table B.1: Indicative mapping of the present document to ETSI EN 303 645 [i.7] (for ratification in future work)**

| ETSI EN 303 645 [i.7] | Mitigation techniques proposed by the analysis of the present document |
|---|---|
| 5.1 No universal default passwords | Authentication and Security by Default in Table 2.<br>Credential Security and Security by Default in Table 3. |
| 5.2 Implement a means to manage reports of vulnerabilities | OS Vulnerability management in Table 2. |
| 5.3 Keep software updated | Secure update and anti-rollback protection in Table 2. |
| 5.4 Securely store sensitive security parameters | Credential Security and Security by Default in Table 3. |
| 5.5 Communicate securely | Credential Security and Security by Default in Table 3.<br>Key management, Secure data transfer, and voice service security in Table 5.<br>Wi-Fi security in Table 7. |
| 5.6 Minimize exposed attack surfaces | This is addressed in the guidance offered in Annex A. |
| 5.7 Ensure software integrity | Addressed in part by Secure boot in Table 9 and by firmware package encryption in Table 8. |
| 5.8 Ensure that personal data is secure | The HG should anonymize user's personal data, such as VoIP phone number, in system logs. Data transmitted through the HG should be encrypted with best practice cryptography. |
| 5.9 Make systems resilient to outages | The HG is the link between local and remote networks. It cannot continue to offer service if no external network exists. |
| 5.10 Examine system telemetry data | Access control and log backup in Table 6. |
| 5.11 Make it easy for users to delete user data | User data, such as phone number in VoIP log, stored in the HG should be anonymized. User data should be securely deleted when factory reset action is performed by user. |
| 5.12 Make installation and maintenance of devices easy | To be provided in user instructions using appropriate and in easy to understand language (guidelines from ETSI TC HF and USER group apply). |
| 5.13 Validate input data | An HG should not offer a user level interface, however where provided the web service provided by the HG should be able to defend against common web attacks such as SQL injection and XSS attack. |
| 6 Data protection provisions for consumer IoT | The HG should not hold any consumer data (note that the HG should not hold explicit knowledge of things such as restrictions placed on specific devices by being able to associate them to users). |

# History

| Document history | | |
|---|---|---|
| V1.1.1 | July 2021 | Publication |
| | | |
| | | |
| | | |
| | | |