# ETSI TR 103 869 V1.1.1 (2022-05)

TECHNICAL REPORT

**Cybersecurity;**
**Network Router Security Threat Analysis**

Reference

DTR/CYBER-0064

Keywords

cybersecurity, router, 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.

# 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.

# 1 Scope

The present document analyses security threats that are related to network router hardware, software, data and protocols.

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

[i.3] Recommendation ITU-T X.805: "Security architecture for systems providing end-to-end communications".

NOTE: Available at https://www.itu.int/rec/T-REC-X.805-200310-I/en.

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

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

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

**Provider:** owner of the IP network, especially telecommunications network

## 3.2 Symbols

Void.

## 3.3 Abbreviations

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

ADSL Asymmetric Digital Subscriber Line
AGG Access Aggregation Gateway

| | |
|---|---|
| ARP | Address Resolution Protocol |
| BFD | Bidirectional Forwarding Detection |
| BGP | Border Gateway Protocol |
| BIOS | Basic Input Output System |
| BNG | Broadband Network Gateway |
| CF | Compact Flash |
| CPE | Customer Premise Equipment |
| CPU | Central Processing Unit |
| DC | Data Centre |
| DC-GW | Data Centre Gateway |
| DDoS | Distributed Denial of Service |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| EOAM | Ethernet Operations, Administration and Maintenance |
| FTP | File Transfer Protocol |
| HG | Home Gateway |
| ICMP | Internet Control Message Protocol |
| IGMP | Internet Group Management Protocol |
| IGW | Integration Gateway |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IPTV | Internet Protocol Television |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| IS-IS | Intermediate System to Intermediate System |
| ISP | Internet Service Provider |
| L2VPN | Layer 2 Virtual Private Network |
| L3VPN | Layer 3 Virtual Private Network |
| LAD | Locally Administered Addresses |
| LDP | Label Distribution Protocol |
| LI | Lawful Interception |
| LLDP | Link Layer Discovery Protocol |
| MAN | Metropolitan Area Network |
| MLD | Multicast Listener Discovery |
| MPLS | Multi-Protocol Label Switching |
| MSDP | Multicast Source Discovery Protocol |
| MSTP | Multiple Spanning Tree Protocol |
| ND | Neighbour Discovery |
| NFV | Network Functions Virtualisation |
| NMS | Network Management System |
| NPE | Network Provider Edge |
| NTP | Network Time Protocol |
| O&M | Operation & Maintenance |
| OS | Operating System |
| OSPF | Open Shortest Path First |
| P | Provider |
| PE | Provider Edge |
| PIM | Protocol Independent Multicast |
| QoS | Quality of Service |
| RAN | Radio Access Network |
| RSVP | Resource ReserVation Protocol |
| SDN | Software-Defined Networking |
| SNMP | Simple Network Management Protocol |
| SRv6 | Segment Routing over IPv6 |
| SSH | Secure Shell |
| STRIDE | Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege |
| TCP | Transmission Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TE | Traffic Engineering |
| TELNET | Teletype Network |
| TVRA | Threat Vulnerability and Risk Analysis |

| | |
|---|---|
| UDP | User Datagram Protocol |
| UPE | User-end Provider Edge |
| VoIP | Voice over Internet Protocol |
| VPN | Virtual Private Network |
| VRRP | Virtual Router Redundancy Protocol |

# 4 Network router introduction

## 4.1 Network router overview

In the Internet model, constituent networks are connected by IP datagram forwarders which are called routers or IP routers.

A router connects to two or more logical interfaces, represented by IP subnets or unnumbered point-to-point lines. Thus, it has at least one physical interface. Forwarding an IP datagram generally requires the router to choose the address and relevant interface of the next-hop router or (for the final hop) the destination host. This choice, called relaying or forwarding, depends upon a route database within the router. The route database is also called a routing table or forwarding table. The term "router" derives from the process of building this route database.

The route database is usually maintained dynamically to reflect the current topology of the Internet system. A router typically accomplishes this by participating in distributed routing and reachability algorithms with other routers.

Routers provide datagram transport only, and they seek to minimize the state information necessary to sustain this service in the interest of routing flexibility and robustness.

Packet switching devices operate at the Link Layer, and such devices are usually called bridges. Network segments connected by bridges share the same IP network prefix and form a single IP subnet.

There are many types of routers. The home and small office routers, which simply forward IP packets between the home computers and the Internet, are out of the scope of the present document. The present document only discusses the network routers that are enterprise routers or ISP routers.

The network routers usually form a complete structure of network solution, which provides large enterprises or ISPs with network traffic forwarding capability. The network routers are typically based on distributed hardware forwarding architecture and non-blocking switching technology. The operating system generally adopts a powerful general routing platform. The network router could provide the following characteristics:

1) It has telecommunication-level reliability, forwarding performance, expansion ability, QoS mechanism, and business processing ability.

2) With convergence access capability and multiple characteristics support, the L2VPN, L3VPN, multicast, multicast VPN, MPLS TE, QoS, SRv6, and other functions can be on-demand deployed to realize reliable services.

3) It fully supports IPv6 and can provide the transition from IPv4 to IPv6.

## 4.2 Network router generic architecture

**Physical Architecture**

A network router uses the modular architecture. The physical architecture is shown in Figure 1.

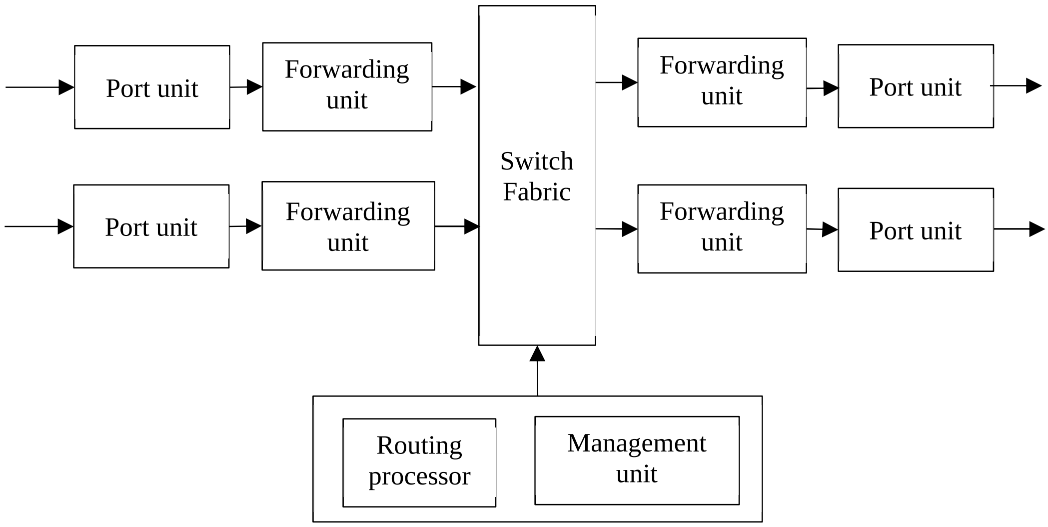


**Figure 1: Physical Architecture of a network router**

**Logical Architecture**

The logical architecture of a network router consists of three planes: data plane, control plane, and management plane, as shown in Figure 2.

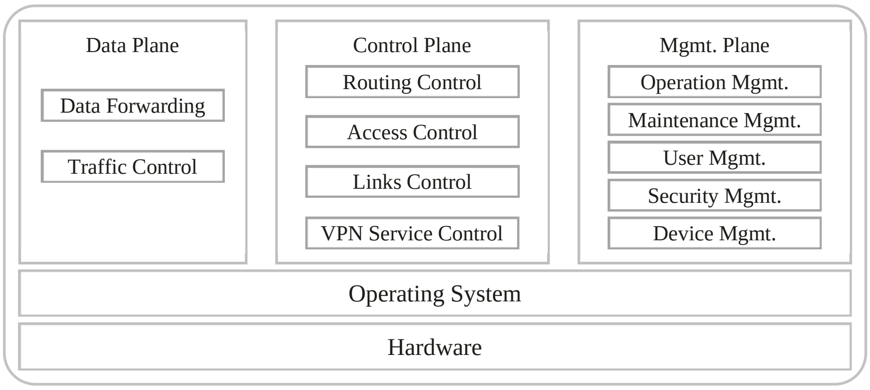


**Figure 2: Logical architecture of a network router**

The data plane is responsible for processing and switching of data packets. It forwards IPv4/IPv6/MPLS/etc. packets and performs QoS.

The control plane typically involves router to router communications that allow the router to obtain the necessary information. It provides all control functions including processing routing/MPLS protocols, such as OSPF, BGP and LDP. It also provides the functionality of the maintenance of the routing table.

The management plane provides management functions, such as configuration and status report.

## 4.3 Network router typical use cases

This clause demonstrates two application scenarios of a network router, the IP backbone network and IP metro network, to show how the network routers are used.

1) IP Backbone Network

   As the core of an entire network and an upper layer of an IP Metropolitan Area Network (MAN), an IP backbone network functions as an outlet allowing IP MANs to access external networks and as a hub enabling interchange between IP MANs. An IP backbone network typically uses a mesh topology, as shown in Figure 3.

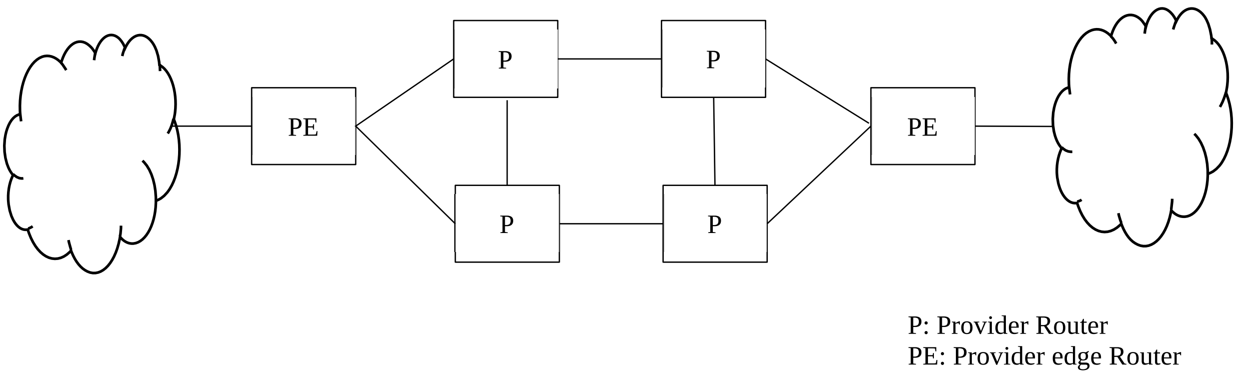


**Figure 3: Topology of IP Backbone Network**

   With service and network convergence, the core network carries richer and richer types of services, including Internet service, VPN service, and DC interconnection. There are PE and P devices in the IP backbone network. IP Metro networks, IP RAN networks, Enterprise networks connect to the IP backbone networks through PE and IGW in the Internet outlet. In this scenario, the provider router and provider edger router are network routers.

2) IP Metro Network

   The IP Metropolitan Area Network (MAN), also known as IP metro network, provides Internet access, VoIP and IPTV services for home users, and enables large-, medium-, and small-size enterprise users to access communication network services through leased lines. An IP metro network typically uses a mesh topology, as shown in Figure 4.

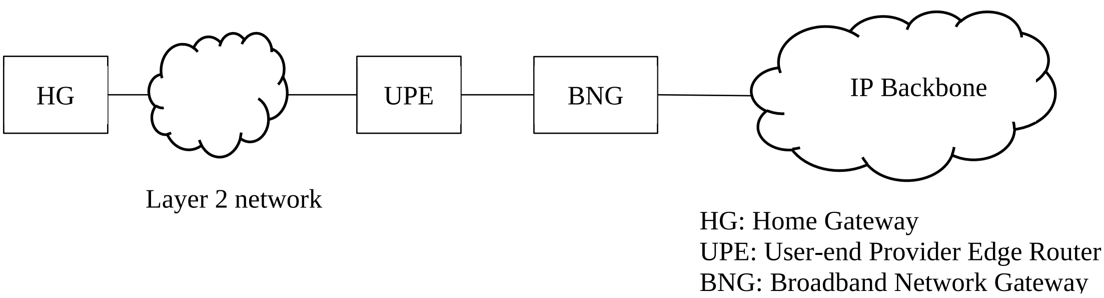


**Figure 4: Topology of IP Metro Network**

   In this scenario, the User-end Provider Edge Router and Broadband Network Gateway are network routers.

## 4.4 Security challenges for network routers

The emergence of new businesses and technologies, such as IoT, cloud, and edge computing, has brought diverse access and network requirements. Networks are becoming more complex to accommodate more businesses, and network devices, including network routers, also expose more attack surfaces. As a result, network routers face more severe security challenges because more attackers can attempt to exploit these exposed surfaces. The new business also brings new requirements and raises security expectations for the network routers.

Attackers become stealthy and cautious, lurking in the network for long periods of time and trying to move horizontally to compromise more devices. Attackers' intentions are often complex as well, and when they finally do attack, the consequences are always quite dramatic. Network routers need to seek countermeasures proactively.

Supply chain attacks, including hardware and software tampering, are becoming an increasingly common attack trend.

Due to the complexity of services, the wide application of SDN/NFV requires more openness and standardization of network routers to better interconnect with products from different vendors, which makes network routers easier to attacks.

As the system provides more and more functions, the components included in the products become more complex, which increases the possibility of vulnerabilities.

In view of the increasing security challenges, protecting critical network infrastructure, which includes network routers, has become a national cybersecurity strategy for countries around the world.

# 5 Network router threat analysis

## 5.1 The approach to network router risk analysis

Clause 5 identifies the key assets of network routers and analyses the vulnerabilities of these assets in detail. The key assets of network routers are determined by the architecture and main functions of network routers. The threats to network routers are analysed based on the main scenarios.

The present document follows the methodology of ETSI's TVRA as defined in ETSI TS 102 165-1 [i.2], combined with Recommendation ITU-T X.805 [i.3].

**Table 1: Threats to security objective types (from ETSI TS 102 165-1 [i.2]) extended with X.805**

| Threat | Objective type | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Access control | Authenticity | Non-repudiation | Data confidentiality | Communication security | Data integrity | Availability/ Resilience | Privacy |
| Interception (eavesdropping) | X | X | | X | X | | X | X |
| Unauthorized access | X | X | | X | X | X | X | |
| Masquerade | X | X | | X | X | | | |
| Forgery | X | | | | X | X | X | |
| Loss or corruption of information | | X | | X | X | | X | X |
| Repudiation | | X | X | | | | | |
| Denial of service | X | X | | | | | X | |

As shown in Table 1, the security objective types are extended with the 8 security dimensions defined in Recommendation ITU-T X.805 [i.3].

The present document adds a new attribute of Resilience to the dimension of Availability. The Resilience attribute ensures that the system can withstand in a known state (including a degraded state) while against attack, and recover from or adapt to adversity in a time frame consistent with mission needs.

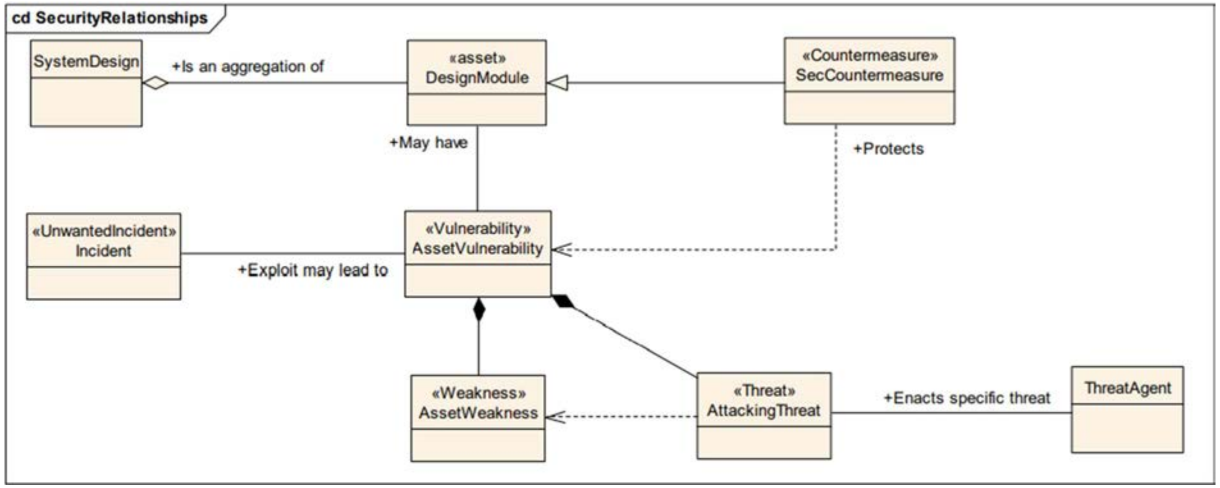


**Figure 5: Generic security TVRA model**

A pictorial view of the asset-threat-weakness-vulnerability-countermeasure relationship to system design is given in Figure 5. Following this methodology defined in ETSI TS 102 165-1 [i.2], the assets, vulnerabilities, and threats should be identified.

The present document also refers to the STRIDE [i.1] threat analysis method developed by Microsoft Corporation™ to identify threats faced by devices on the network. STRIDE [i.1] defines six types of threats, which correspond to the threat classification of TVRA.

## 5.2 Network router key assets

### 5.2.1 Introduction

Based on the scenarios of the network router, clause 5.2 identifies its key assets which are to be protected from the attackers, as shown in Table 2, as well as the vulnerabilities of these assets.

**Table 2: Key assets list of a network router**

| Assets Main Category | Assets |
|---|---|
| Software | Service software, O&M management software, security management software, and OS/BIOS. |
| Hardware | Service hardware: service boards, CPUs, chips, optical modules, optical fibres, chassis, power supplies, fans, CF cards, and flash memory.<br>Interface hardware: service interfaces and management interfaces. |
| Data | Configuration data, accounts and passwords, digital certificates, logs/alarms, keys. |
| Protocols | Basic TCP/IP protocols, such as IP, TCP, UDP, ARP, ND, VRRP, DHCP, ICMP, and NTP.<br>Control plane protocol, such as OSPF, IS-IS, BGP, LDP, RSVP, PIM, MSDP, IGMP, MLD, BFD, EOAM, MSTP, LAD, and LLDP.<br>Management protocol, such as TELNET, SSH, SNMP, NETCONF, and FTP. |

### 5.2.2 Software

Software assets include BIOS/OS, service software, O&M management software, and security management software. The vulnerabilities of software assets are listed in Table 3.

**Table 3: Vulnerabilities of Software Assets**

| Category | Vulnerability | Vulnerability No. |
|---|---|---|
| Service software | Disrupted service running | VUL.SW.0001 |
| | Improper allocation of running resource | VUL.SW.0002 |
| O&M management software | Improper interactive interface design | VUL.SW.0003 |
| | Improper allocation of user permissions | VUL.SW.0004 |
| Security management software | Lack of authentication or poor authentication techniques for access to the information of security management components | VUL.SW.0005 |
| | Insufficient security strength of security management components | VUL.SW.0006 |
| OS/BIOS | Improper setting of OS account permissions | VUL.SW.0007 |
| | Improper memory management | VUL.SW.0008 |
| | Improper setting of OS access rights | VUL.SW.0009 |
| | Improper allocation of OS resource | VUL.SW.0010 |
| General | Lack of integrity protection before running | VUL.SW.0011 |
| | Lack of integrity protection during operation | VUL.SW.0012 |
| | Improper control of component permissions | VUL.SW.0013 |
| | Improper control of Virtualization components' permissions, management, and file configuration | VUL.SW.0014 |
| | Lack of effective isolation mechanism | VUL.SW.0015 |
| | Existence of security vulnerabilities | VUL.SW.0016 |
| | Lack of security detection mechanism | VUL.SW.0017 |
| | Lack of recovery mechanism | VUL.SW.0018 |

### 5.2.3 Hardware

Hardware assets include service hardware which directly forwards user data, such as CPUs, and interface hardware. The vulnerabilities of hardware assets are listed in Table 4.

**Table 4: Vulnerabilities of Hardware Assets**

| Category | Vulnerability | Vulnerability No. |
|---|---|---|
| Service hardware | Lack of encryption capability | VUL.HW.0001 |
| | Lack of QoS capability | VUL.HW.0002 |
| | Lack of protection for critical communications | VUL.HW.0003 |
| | Critical data communications have processing capability bottlenecks or lack data filtering and QoS mechanisms | VUL.HW.0004 |
| | Lack of protection for device clocks | VUL.HW.0005 |
| Interface hardware | Lack of access control or improper access control mechanisms for hardware interfaces | VUL.HW.0006 |
| | Lack of side channel attack defence mechanism | VUL.HW.0007 |
| General | Exposure of chip debugging interface or other redundant physical interfaces with insufficient access control | VUL.HW.0008 |
| | Lack of protection for physical chip circuits or cabling | VUL.HW.0009 |
| | Existence of unclosed reserved bits in general purpose circuits and logic prior to production | VUL.HW.0010 |

### 5.2.4 Data

Data assets include service data that directly affects services, such as configuration data, as well as management data generated for device management, such as accounts and logs. The vulnerabilities of data assets are listed in Table 5.

**Table 5: Vulnerabilities of Data Assets**

| Category | Vulnerability | Vulnerability No. |
|---|---|---|
| Service data | Improper default configuration of service processing logic, or insecure and unreasonable service configuration | VUL.DA.0001 |
| Management data | Non-compliance with confidentiality requirements in the protection mechanism for stored sensitive data | VUL.DA.0002 |
| | Lack of explicit access control policies and enforcement for access to sensitive data | VUL.DA.0003 |
| | Lack of integrity protection mechanisms for the generation and transmission of audit logs | VUL.DA.0004 |

### 5.2.5 Protocols

Protocol assets include basic TCP/IP protocols, control plane protocols, and management protocols. The vulnerabilities of protocol assets are listed in Table 6.

**Table 6: Vulnerabilities of Protocol Assets**

| Category | Vulnerability | Vulnerability No. |
|---|---|---|
| Control-plane protocol | Lack of control-plane protocol identity awareness for critical exchange information or information flow paths (e.g. route hijacking, DHCP spoofing) | VUL.PO.0001 |
| | Use of fields vulnerable to spoofing bypass for control plane protocol authentication (e.g. IP address, reverse DNS resolution results, etc.) | VUL.PO.0002 |
| General | Lack of logging or statistical records for protocols, or improper handling of logging statistics | VUL.PO.0003 |
| | Lack of identity authentication or insecure authentication mechanism | VUL.PO.0004 |
| | Lack of protection of critical interaction information | VUL.PO.0005 |
| | Insufficient strength of security mechanisms | VUL.PO.0006 |
| | Lack of blocking function for unauthorized connections and messages | VUL.PO.0007 |
| | Lack of protocol traffic control mechanism | VUL.PO.0008 |
| | Lack of session management and recovery mechanisms | VUL.PO.0009 |

## 5.3 Network router threats

### 5.3.1 Introduction

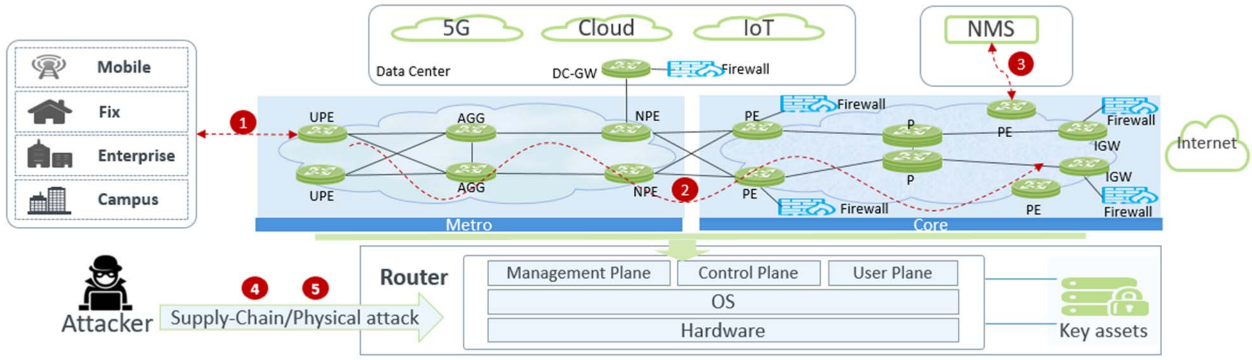


**Figure 6: Application Scenarios of Network Routers**

Based on the application scenarios of network routers, the attack scenarios can be divided into 5 types:

- ①Access-side attacks;
- ②Inter-device horizontal attacks;
- ③O&M attacks;
- ④Supply-Chain attacks; and
- ⑤Physical attacks.

### 5.3.2 Access-side attacks

Access-side attacks are mainly from network users, including:

1) The mobile access network devices, such as mobile base stations, Wi-Fi® devices, etc. These devices are connected to mobile, Wi-Fi® and other personal users.

2) The fixed access network devices, such as fibre access devices, ADSL access devices, etc. These devices are connected to home broadband and other home users.

3) The enterprise network access devices, such as enterprise branch CPE equipment. These devices are connected to the internal network of the enterprise.

4) The campus network access devices, such as campus network access switches. These devices are connected to the campus network users.

The threats on the access-side attacks mainly come from network users. Figure 7 depicts the threats, with details in Table 7.

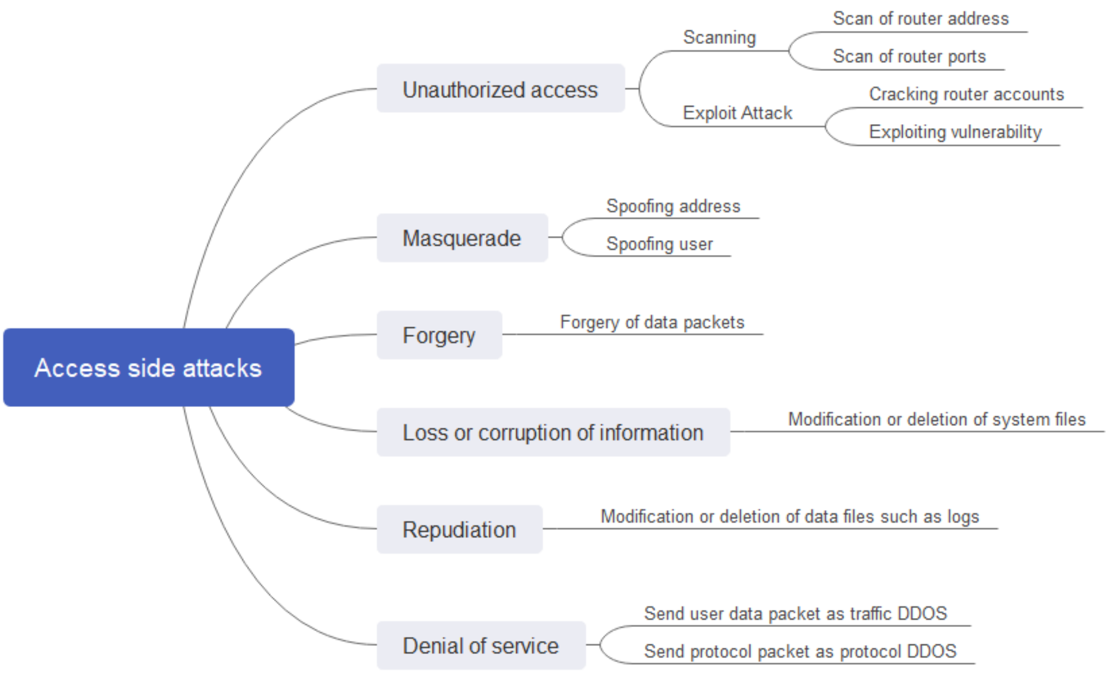


**Figure 7: Threats on the access**

**Table 7: Threats from Access-side Attacks**

| Access side attacks | | | |
|---|---|---|---|
| **Threat Type** | **Threat** | **Threat Scenario No.** | **Description** |
| Unauthorized access | Scan of router address | Threat.Access.01 | Scan critical network addresses to prepare for attacks from user side. |
| | Scan of router ports | Threat.Access.02 | Scan the software and hardware ports of routers from user side. |
| | Cracking router accounts | Threat.Access.03 | Crack router accounts from user side. |
| | Exploiting vulnerability | Threat.Access.04 | Exploit router's vulnerabilities from the user side to launch various attacks, such as injection of malicious code, stack overflow, CPU overload, etc. to cause different consequences, including service degradation, service interruption, or even physical damage. |
| Masquerade | Spoofing address | Threat.Access.05 | Forge reply packets such as ARP and ND packets from authorized users from user side. |
| | Spoofing user | Threat.Access.06 | Forge a multicast user to accept multicast packets from user side. |
| Forgery | Forgery of data packets | Threat.Access.07 | Forge user packets from user side. |
| Loss or corruption of information | Modification or deletion of system files | Threat.Access.08 | Modify or destroy system files required for system running from user side. |
| Repudiation | Modification or deletion of data files such as logs | Threat.Access.09 | Modify or destroy logs and diagnostic information files from user side. |
| Denial of service | Send user data packet as traffic DDoS | Threat.Access.10 | Send attack packets as user data to occupy router's port bandwidth from user side. |
| | Send protocol packet as protocol DDoS | Threat.Access.11 | Send protocol packets to occupy router's computing resources from user side. |

## 5.3.3 Inter-device horizontal attacks

Inter-device attacks are attacks from other routers on the network side, including attacks on the local network and devices across networks. Figure 8 depicts the threats with details in Table 8.

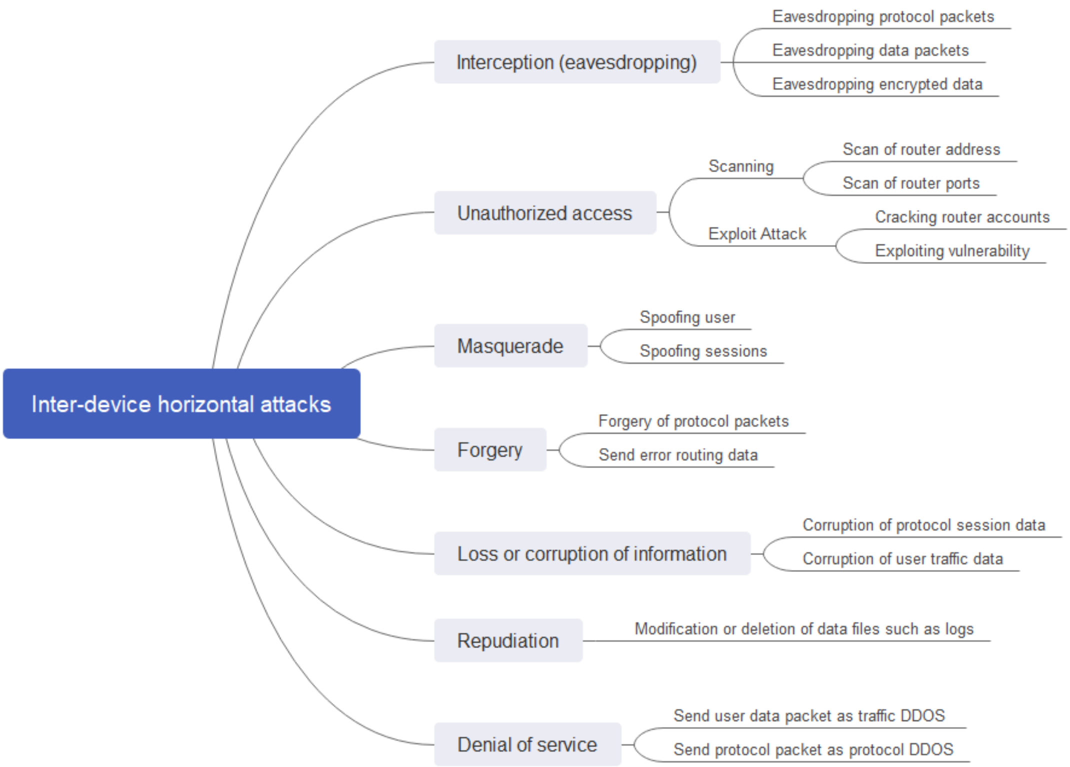


**Figure 8: Inter-device threats**

**Table 8: Threats from Inter-device Horizontal Attacks**

| Inter-device horizontal attacks | | | |
|---|---|---|---|
| **Threat Type** | **Threat** | **Threat Scenario No.** | **Description** |
| Interception (eavesdropping) | Eavesdropping protocol packets | Threat.Inter-device.01 | Listen to protocol session packets to obtain sensitive information without permission, attacking from inter-device link. |
| | Eavesdropping data packets | Threat.Inter-device.02 | Listen to user data packets to obtain sensitive information without permission, attacking from inter-device link. |
| | Eavesdropping encrypted data | Threat.Inter-device.03 | Listen to data packets in encrypted channels to obtain sensitive information without permission, attacking from inter-device link. |
| Unauthorized access | Scan of router address | Threat.Inter-device.04 | Scan critical network addresses to prepare for attacks from inter-device link. |
| | Scan of router ports | Threat.Inter-device.05 | Scan the software and hardware ports of routers from inter-device link. |
| | Cracking router accounts | Threat.Inter-device.06 | Crack router accounts from inter-device link. |
| | Exploiting vulnerability | Threat.Inter-device.07 | Exploit router's vulnerabilities from the inter-device link to launch various attacks, such as injection of malicious code, stack overflow, CPU overload, etc. to cause different consequences, including service degradation, service interruption, or even physical damage. |
| Masquerade | Spoofing user | Threat.Inter-device.08 | Spoof users intrude into devices, attacking from inter-device link. |
| | Spoofing sessions | Threat.Inter-device.09 | Spoof neighbours to connect to an existing session, attacking from inter-device link. |

| Inter-device horizontal attacks | | | |
|---|---|---|---|
| **Threat Type** | **Threat** | **Threat Scenario No.** | **Description** |
| Forgery | Forgery of protocol packets | Threat.Inter-device.10 | Forge protocol session packets to attack valid sessions, attacking from inter-device link. |
| | Send error routing data | Threat.Inter-device.11 | Unintentionally send protocol packets including error routing data, e.g. BGP route leakage due to a faulty operation or configuration. |
| Loss or corruption of information | Corruption of protocol session data | Threat.Inter-device.12 | Destroy valid session data between devices, attacking from inter-device link. |
| | Corruption of user traffic data | Threat.Inter-device.13 | Destroy inter-device traffic data, attacking from inter-device link. |
| Repudiation | Modification or deletion of data files such as logs | Threat.Inter-device.14 | Destroy logs and diagnostic information files, attacking from inter-device link. |
| Denial of service | Send user data packet as traffic DDoS | Threat.Inter-device.15 | Port bandwidth occupied by sending attack packets, attacking from inter-device link. |
| | Send protocol packet as protocol DDoS | Threat.Inter-device.16 | Send protocol packets, occupying computing resources, attacking from inter-device link. |

### 5.3.4 O&M attacks

O&M attacks come from management network units. The NMS can be attacked by social engineering, viruses, Trojan horses, or maloperations of management personnel. Figure 9 depicts the threats with details in Table 9.

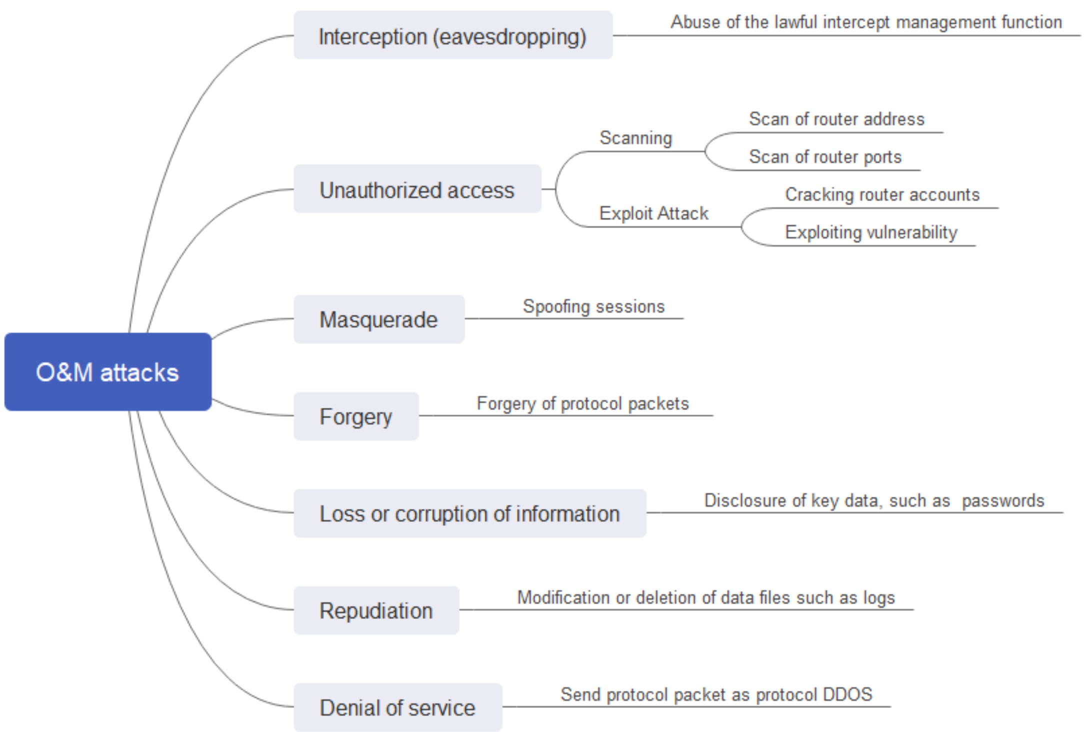


**Figure 9: O&M threats**

**Table 9: Threats from O&M Attacks**

| O&M attacks | | | |
|---|---|---|---|
| **Threat Type** | **Threat** | **Threat Scenario No.** | **Description** |
| Interception (eavesdropping) | Abuse of the lawful interception management function | Threat.OM.01 | Abuse the lawful interception management function, attacking from management plane. |
| Unauthorized access | Scan of router address | Threat.OM.02 | Scan critical network addresses to prepare for attacks, attacking from management plane. |
| | Scan of router ports | Threat.OM.03 | Scan the software and hardware ports of routers, attacking from management plane. |
| | Cracking router accounts | Threat.OM.04 | Cracking router accounts, attacking from management plane. |
| | Exploiting vulnerability | Threat.OM.05 | Exploit router's vulnerabilities, attacking from management plane, to launch various attacks, such as injection of malicious code, stack overflow, CPU overload, etc. to cause different consequences, including service degradation, service interruption, or even physical damage. |
| Masquerade | Spoofing sessions | Threat.OM.06 | Spoof management sessions connections to router, attacking from management plane. |
| Forgery | Forgery of protocol packets | Threat.OM.07 | Forge management protocol session packets to attack valid sessions, attacking from management plane. |
| Loss or corruption of information | Disclosure of key data, such as passwords | Threat.OM.08 | Steal key data, such as keys and passwords, attacking from management plane. |
| Repudiation | Modification or deletion of data files such as logs | Threat.OM.09 | Destroy logs and diagnostic information files, attacking from management plane. |
| Denial of service | Send protocol packet as protocol DDoS | Threat.OM.10 | Send protocol packets, occupying computing resources, attacking from management plane. |

## 5.3.5 Supply-Chain attacks

A supply chain attack is an attack targeting the less-secure elements in the supply chain. Figure 10 depicts the threats with details in Table 10.

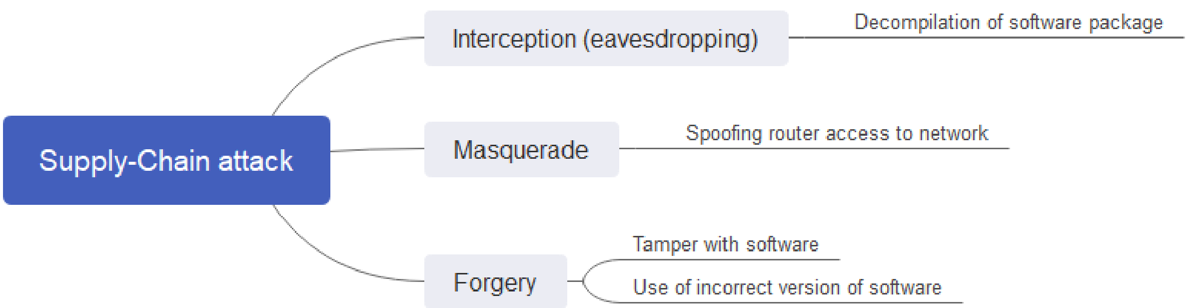


**Figure 10: Supply chain threats**

**Table 10: Threats from Supply-Chain Attacks**

| Supply-Chain attack | | | |
|---|---|---|---|
| **Threat Type** | **Threat** | **Threat Scenario No.** | **Description** |
| Interception (eavesdropping) | De-compilation of software package | Threat.SC.01 | Obtain key, credential information and other exploitable vulnerabilities from reverse engineering in software package. |
| Masquerade | Spoofing router access to network | Threat.SC.02 | Spoof router to access an existing network without permission. |
| Forgery | Tamper with software | Threat.SC.03 | Tamper router's software. |
| | Use of incorrect version of software | Threat.SC.04 | Intentionally use the incorrect version of software. |

## 5.3.6 Physical attacks

If the device cannot be physically secure after being installed, a physical attack can also occur. Figure 11 depicts the threats with details in Table 11.


**Figure 11: Physical threats**

**Table 11: Threats from Physical Attacks**

| Physical attack | | | |
|---|---|---|---|
| **Threat Type** | **Threat** | **Threat Scenario No.** | **Description** |
| Unauthorized access | Side channel attack of cryptographic key material | Threat.Physical.01 | Obtain key material through analysis of side channel information, such as timing information, power consumption, etc. This threat is considered as impractical. |
| | Physical damage or degradation | Threat.Physical.02 | Damaging or degrading the devices and links through physically manual operations, to permanently or temporally disrupt normal services. |

### 5.3.7 Summary

**Table 12: Threats summary**

| Threat Type | Threat | Threat Scenario No. |
|---|---|---|
| Interception (eavesdropping) | Eavesdropping protocol packets | Threat.Inter-device.01 |
| | Eavesdropping data packets | Threat.Inter-device.02 |
| | Eavesdropping encrypted data | Threat.Inter-device.03 |
| | Abuse of the lawful interception management function | Threat.OM.01 |
| | De-compilation of software package | Threat.SC.01 |
| Unauthorized access | Scan of router address | Threat.Access.01<br>Threat.Inter-device.04<br>Threat.OM.02 |
| | Scan of router ports | Threat.Access.02<br>Threat.Inter-device.05<br>Threat.OM.03 |
| | Cracking router accounts | Threat.Access.03<br>Threat.Inter-device.06<br>Threat.OM.04 |
| | Exploiting vulnerability | Threat.Access.04<br>Threat.Inter-device.07<br>Threat.OM.05 |
| | Side channel attack of cryptographic key material | Threat.Physical.01 |
| | Physical damage or degradation | Threat.Physical.02 |
| Masquerade | Spoofing address | Threat.Access.05 |
| | Spoofing user | Threat.Access.06<br>Threat.Inter-device.08 |
| | Spoofing sessions | Threat.Inter-device.09<br>Threat.OM.06 |
| | Spoofing router access to network | Threat.SC.02 |
| Forgery | Forgery of data packets | Threat.Access.07 |
| | Forgery of protocol packets | Threat.Inter-device.10<br>Threat.OM.07 |
| | Send error routing data | Threat.Inter-device.11 |
| | Tamper with software | Threat.SC.03 |
| | Use of incorrect version of software | Threat.SC.04 |
| Loss or corruption of information | Modification or deletion of system files | Threat.Access.08 |
| | Corruption of protocol session data | Threat.Inter-device.12 |
| | Corruption of user traffic data | Threat.Inter-device.13 |
| | Disclosure of key data, such as passwords | Threat.OM.08 |
| Repudiation | Modification or deletion of data files such as logs | Threat.Access.09<br>Threat.Inter-device.14<br>Threat.OM.09 |
| Denial of service | Send user data packet as traffic DDoS | Threat.Access.10<br>Threat.Inter-device.15 |
| | Send protocol packet as protocol DDoS | Threat.Access.11<br>Threat.Inter-device.16<br>Threat.OM.10 |

# Annex A: TVRA Assessment Guidance

## A.1 General

Whether a network router is a critical infrastructure depends on the application scenario and deployment. For a detailed risk assessment, it is also necessary to determine the router application scenarios, deployment, and specific services carried on the network. The analysis in clause 5.3 identifies the threats faced by network routers in different scenarios. For a detailed risk assessment for a specific network, the network operator can refer to the guidelines in this annex.

The threat level is a value attributed to the combination of the capability and motivation of a threat agent to attack these assets. The capability of a threat agent is quite different from each other and should be discussed in different events. The motivation of the threat agent depends on the services carried on the network, such as financial and government data can be very attractive, and ordinary personal Internet service only can attract the attention of junior hackers. So, the threat level should be calculated correctly when the actual attack happens.

The attack factors (i.e. Time + Expertise + Knowledge + Opportunity + Equipment) will give the overall attack potential rating. Most of these factors are different in the specific attack events. So, the likelihood of an attack is closely associated with attacking events and network environments. But, for each type of threat, only a few main factors have major effects. The present document tries to identify these important factors and describes how these factors affect the attack event.

The impact of the attack event depends on the services carried on the network. Therefore, a rank used to express the different levels of data and services is needed to help assess the impact.

## A.2 Interception (eavesdropping)

**Eavesdropping protocol packets:** Listen to protocol session packets to obtain sensitive information without permission.

The main obstacle to intercepting data attacks is physical access to networks links or interfaces of devices. If links and devices are exposed to attackers without any protection, the possibility of attacks is high. Otherwise, the possibility of attacks is low. Eavesdropping protocol packets usually require professional skills. The value of factors should be as listed in Table A.1, and other factors will be defined according to the real attack scenario.

**Table A.1: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Expertise | Expert | 6 |
| Knowledge | Restricted | 3 |
| Opportunity | Difficult | 10 |
| Equipment | Bespoke | 7 |

**Eavesdropping data packets:** Listen to user data packets to obtain sensitive information without permission.

Eavesdropping data packets does not require identification of the protocols, so it is easier than eavesdropping protocol packets. The value of factors should be as listed in Table A.2.

**Table A.2: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Expertise | Proficient | 3 |
| Knowledge | Public | 0 |
| Opportunity | Difficult | 10 |
| Equipment | Bespoke | 7 |

**Eavesdropping encrypted data:** Listen to data packets in encrypted channels to obtain sensitive information without permission.

The main difficulty of eavesdropping encrypted data is to obtain secret materials and needs higher level of expertise. The value of factors should be as listed in Table A.3.

**Table A.3: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Expertise | Multiple experts | 8 |
| Knowledge | Sensitive | 7 |
| Opportunity | Difficult | 10 |
| Equipment | Bespoke | 7 |

**Abuse of the lawful interception management function:** Abuse the lawful interception management function, attacking from management plane.

For **abuse of the lawful interception management function**, it is difficult to gain access to the function. The usual way to get it is to exploit management vulnerabilities or exploit software vulnerabilities to steal management rights. Once the LI permission is obtained, the user's data can be obtained without the user's knowledge, which poses several risks to the user. The value of factors should be as listed in Table A.4.

**Table A.4: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Time | ≤ 2 months | 7 |
| Expertise | Multiple experts | 8 |
| Knowledge | Critical | 11 |

**De-compilation of software package:** Obtain key, credential information and other exploitable vulnerabilities from reverse engineering in software package.

De-compilation can be performed only when the software of the attacked version is obtained. The de-compilation tools are easy to obtain. Therefore, attacks are likely to occur. The difficulty of de-compilation attacks is to analyse the de-compilation result and obtain the required key data. In most cases, the information got from de-compilation is limited and needs other conditions to start a real attack. The value of factors should be as listed in Table A.5.

**Table A.5: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Time | ≤ 2 months | 7 |
| Expertise | Multiple experts | 8 |
| Knowledge | Public | 0 |

# A.3 Unauthorized access

**Scan of router address:** Scan critical network addresses to prepare for attacks.

**Scan of router ports:** Scan the software and hardware ports of routers.

Scan is normally easy to implement and the result of scan can provide the conditions for further attacks. Scan also can be a kind of DDoS attack. The value of factors should be as listed in Table A.6.

**Table A.6: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Time | ≤ 1 day | 0 |
| Expertise | Layman | 0 |
| Knowledge | Public | 0 |
| Opportunity | Unnecessary/Unlimited access | 0 |
| Equipment | Standard | 0 |

**Cracking router accounts:** Crack router accounts.

**Exploiting vulnerability:** Exploit router's vulnerabilities to launch various attacks, such as injection of malicious code, stack overflow, CPU overload, etc. to cause different consequences, including service degradation, service interruption, or even physical damage.

**Side channel attack of cryptographic key material:** Obtain key material through analysis of side channel information, such as timing information, power consumption, etc. This threat is considered as impractical.

Exploit attacks and side-channel attacks require the attacker to have certain technical capabilities, and it is uncertain whether the attacked device has the required vulnerabilities. The value of factors should be as listed in Table A.7.

**Table A.7: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Expertise | Expert/Multiple experts | 6/8 |
| Knowledge | Sensitive/Critical | 7/11 |
| Opportunity | Difficult | 10 |
| Equipment | Specialized | 4 |

**Physical damage or degradation:** Damaging or degrading the devices and links through physically manual operations, to permanently or temporally disrupt normal services.

Damaging or degrading the devices and links through physically manual operations requires the attacker to access the links or devices physically. The value of factors should be as listed in Table A.8.

**Table A.8: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Expertise | Layman | 0 |
| Knowledge | Public | 0 |
| Opportunity | Difficult | 10 |
| Equipment | Standard | 0 |

# A.4 Masquerade

**Spoofing address:** Spoof reply packets such as ARP and ND packets from authorized users.

**Spoofing user:** Spoof user to obtain management plane permission of router.

**Spoofing sessions:** Spoof neighbours to connect to an existing session.

It is not difficult to launch attacks using spoofing to achieve the result of DDoS attacks. But it is difficult to obtain key data. The value of factors should be as listed in Table A.9.

**Table A.9: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Expertise | Expert/Multiple experts | 6/8 |
| Equipment | Standard | 0 |

**Spoofing router access to network:** Spoof router to access an existing network without permission.

Spoofing router to access an existing network can access the network to facilitate attackers to exploit devices with software and hardware vulnerabilities. The value of factors should be as listed in Table A.10.

**Table A.10: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Equipment | Bespoke | 7 |

# A.5 Forgery

**Forgery of data packets:** Forge traffic packets.

Sending forgery packets to disrupt user data streams can be initiated without professional skills and can generate DDoS attacks. The value of factors should be as listed in Table A.11.

**Table A.11: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Expertise | Proficient | 3 |
| Opportunity | Moderate | 4 |

**Forgery of protocol packets:** Forge protocol session packets to attack valid sessions.

Forging protocol packets to hijack sessions or inject manipulated information requires attackers to have a deep understanding of compromised protocols and services. The value of factors should be as listed in Table A.12.

**Table A.12: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Expertise | Expert | 6 |
| Opportunity | Moderate | 4 |

**Send error routing data:** Unintentionally send protocol packets including error routing data, e.g. BGP route leakage due to a faulty operation or configuration.

Unintentionally sending protocol packets that include error routing data, can cause service interruption on a large scale. This is usually caused by a faulty operation or configuration. The value of factors should be as in Table A.13.

**Table A.13: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Opportunity | Difficult | 10 |

**Tamper with software:** Tamper router's software.

**Use of incorrect version of software:** Intentionally use the incorrect version of software.

Tampering software brings great potential risks and requires attackers to have high capabilities. The value of factors should be as listed in Table A.14.

**Table A.14: Recommended value for assessment**

| Factors | Recommended Range | Recommended Value |
|---|---|---|
| Expertise | Multiple experts | 8 |
| Knowledge | Sensitive | 7 |
| Opportunity | Difficult | 10 |

# A.6 Loss or corruption of information

**Modification or deletion of system files:** Modify or destroy system files required for system running.

**Disclosure of key data, such as passwords:** Steal key data, such as keys and passwords.

Damage of system files requires exploiting software and hardware vulnerabilities of system. The value of factors should be as listed in Table A.7.

**Corruption of protocol session data:** Destroy valid session data between devices.

Corruption of protocol data can interrupt the protocol sessions. The value of factors should be as listed in Table A.12.

**Corruption of user traffic data:** Destroy inter-device traffic data.

Corruption of user data can interrupt the service. The value of factors should be as listed in Table A.11.

# A.7 Repudiation

**Modification or deletion of data files such as logs:** Modify or destroy logs and diagnostic information files.

Modification of data file can interrupt the service or obstruct audits. The value of factors should be as listed in Table A.7.

# A.8 Denial of service

**Send user data packet as traffic DDoS:** Send attack packets as user data to occupy router's port bandwidth.

Sending user data packets to launch the DDoS attack can interrupt the normal services by occupying router's port bandwidth. The value of factors should be as listed in Table A.11.

**Send protocol packet as protocol DDoS:** Send protocol packets to occupy router's computing resources.

Sending protocol packets to launch the DDoS attack can interrupt the normal services by occupying router's computing resources. The value of factors should be as listed in Table A.12.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | May 2022 | Publication |
| | | |
| | | |
| | | |
| | | |