**3GPP TSG-SA5 Meeting #156 *S5-245089***

Maastricht, Netherlands, 19 - 23 August 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.3* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network | **X** | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | S5 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** | A |  | | | | | ***Release:*** | | |  |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases:* *Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)  Rel-20 (Release 20)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | As requested by 3GPP IETF coordinator, there are some references to IETF drafts which are already published as RFCs need to be updated. The changes to the published RFCs do not affect 3GPP SA5 OpenAPI interfaces. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Update the references to IETF drafts to published RFCs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incorrect references to IETF drafts which are already published as RFCs exist in the specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex A | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

|  |
| --- |
| **Begin of modifications** |

Annex A (informative):  
Protocols for IP Network Security to Support Itf-N

Many security threats exist to the management plane of the telecommunications networks. In addition, new security threats to the management plane are being introduced as the network evolves. The purpose of this document is to provide security guidelines for using IP Network security protocols such as Internet Protocol Security (IPsec), SSL/TLS (Secure Socket Layer/Transport Layer Security) and Secure Shell(SSH) to help mitigate security risks to the management network. The security provided by IP Network security protocols may be obtained by implementing these protocols within network equipment or through the use of external mechanisms such as IPsec VPN devices.

In some telecommunications networks, management traffic is transmitted on a separate network from that carrying the service provider's end-user traffic. In these networks, security threats to the management plane are isolated from malicious activity on the end-user plane. With evolving telecommunications networks however, management traffic is often combined on a single network with end-user traffic. Combining traffic in this manner minimizes costs by requiring only a single integrated network infrastructure; however, new security challenges are introduced. Threats in the end-user plane now become threats to the management plane since the management plane becomes accessible to the multitude of end-users. Thus security, which was very important before, becomes even more critical with the evolving network.

Scope

This document provides recommendations and guidelines for using IP Network security protocols such as Internet Protocol Security (IPsec), SSL/TLS (Secure Socket Layer/Transport Layer Security) and Secure Shell (SSH) to help mitigate security risks for management traffic. The use of IP Network security protocols can be used to provide a basic level of network security for the 3GPP Itf-N interface and underlying network used to transport management traffic. In addition to the use of IP Network security protocols, other aspects of security including operator authentication/authorization, operating system hardening and security event logging must also be considered to provide an overall secure solution, however these aspects are beyond the scope of this document.

Framework Model

The framework model used by this document is from Figure 1, clause 5.1.1 of TS 32.101 [TS 32.101]. This diagram, reproduced below in Figure 1, identifies a set of interfaces used by 3GPP. The recommendations of this document apply specifically to management interfaces of Type 2 [EM-NM; also known as Interface N], including the underlying IP transport network used to support this interface.

The recommendations and guidelines in this document may also be considered in future to provide security for other interfaces such as the Type 1 [NE-EM] interface.



Figure A.1: 3GPP Management System Interactions

Security Threats

A number of serious security threats are commonly associated with the OAM&P management network infrastructure. Security threats include Masquerade, Eavesdropping, Unauthorized Access, Loss/Corruption of Information, Repudiation, Forgery and Denial of Service.

Attacks may be launched from inside the network by insiders such as disgruntled employees and also from external sources such as hackers. IP Network security protocols such as IPsec, SSL/TLS and SSH can be effective in mitigating many of these security threats. In addition, other security services may be able to make use of security provided by the IP Network security protocols. For example passwords used for application level authentication will be protected against eavesdropping when transmitted over a network infrastructure secured by IP Network security protocols.

Table 1, taken from ITU-T Recommendation M.3016, illustrates a mapping of security functions required to mitigate identified security threats [M.3016]. In Table 2, the general capabilities of IP Network security protocols (IPsec, SSL/TLS and SSH) is mapped against required security functions. This illustrates how IP Network security protocols can help mitigate security vulnerabilities.

Table A.1: Correlation of Security Management Functional Area with Threats  
(from ITU-T Recommendation M.3016 [2])

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Functional Requirement Area | Security Management | Masquerade | Eavesdropping | Unauthorized  access | Loss/corruption  of information | Repudiation | Forgery | Denial of Service |
| Verification of identities | | **x** |  | **x** |  |  |  |  |
| Controlled access and authorization | |  |  | **x** |  |  |  | **x** |
| Protection of confidentiality | |  | **x** | **x** |  |  |  |  |
| Protection of data integrity | |  |  |  | **x** |  |  |  |
| Activity logging | | **x** |  | **x** |  | **x** | **x** | **x** |
| Alarm reporting | | **x** |  | **x** | **x** |  |  | **x** |
| Audit | | **x** |  | **x** |  | **x** | **x** | **x** |

Table A.2: Correlation of Security Functional Area with Security Services Provided by IP Network Security Protocols

|  |  |
| --- | --- |
| **Functional Requirement Area** | **Threat Mitigation Measures Provided by IP Network Security Protocols.** |
| Verification of identities | Machine-to-machine (server-to-server) authentication services can be provided based on password or X.509 certificates. Application layer authentication is not provided. |
| Controlled access and authorization | Network/transport layer packet filtering service can reject non-authorized packets. |
| Protection of confidentiality | Confidentiality service is provided by underlying encryption technology within the Network Security protocol. The strength of the encryption service can vary to extremely strong dependent on underlying encryption algorithm and key length chosen. |
| Protection of data integrity | Strong data integrity service is provided by underlying cryptographic service within the Network Security protocol. (E.g. Keyed Hashed Message Authentication Code with Secure Hash Algorithm-1). |
| Activity logging | Not provided. |
| Alarm reporting | Not provided. |
| Audit | Not provided. |

Security Solutions

Application Layer Security

Application layer security provides a security solution targeted specifically to a particular application, which must be implemented in the end hosts. Application layer security has the advantage of easy access to user credentials because it operates in the context of the user, which makes user AAA services easier to implement. Also, an application can be extended for security without having to depend on the operating system to provide these services.

The disadvantage of application level security is that security mechanisms must be designed independently for every application that needs to be secured. Thus, it is very difficult to create seamless and scalable security architectures using only application layer security.

Transport Layer Security

Transport layer security provides security services at the Transport layer (Layer 4). SSL, which has been revised and standardized by the Internet Engineering Task Force (IETF) as TLS, is the security protocol that provides security at the transport layer.

A single SSL/TLS instance can be used to create multiple SSL/TLS sessions through an Internet protocol (IP) network to provide security for various applications. Modifications are required to each application to allow that application to request SSL/TLS security services. SSL/TLS is the de-facto standard for Web-based HTTP traffic, and all standard Web browsers include built-in SSL/TLS technology.

Because SSL/TLS technology does not operate in the context of the user, obtaining user context is difficult, making it harder to implement user AAA services. SSL/TLS is applicable only to TCP traffic and cannot be used to protect UDP traffic.

Network Layer Security

Network layer security provides security services at the Network layer (Layer 3). The IETF IPsec Suite is the security protocol that provides security at the network layer. IPsec is optional for IPv4 and a mandatory component of IPv6. IPsec can be used to protect data from any different application or transport protocols. No modifications are required to the applications, and the security services appear transparent to the applications. IPsec is the de-facto standard used for creating network layer virtual private networks. (IPsec VPN).

Because IPsec technology does not operate in the context of the user, obtaining user context is difficult, making it harder to implement user AAA services.

Recommendations

Service providers are increasingly using in-band network management and thus logical separation of management traffic through the use of IP network security protocols is a beneficial security practice. Also, security statistics show that up to 70% of all compromises of resources are caused by “insiders”. Use of IP network security protocols for management traffic provides a good degree of protection against insiders with the exception of the small group of insiders that have legitimate access to the encryption keys.

It is recommended to provide baseline infrastructure security between machines communicating across the Itf-N through the use of IP network security protocols such as IPsec, SSL/TLS and SSH. These IP network security protocols employ security services through the use of cryptographic mechanisms and provide services including data confidentiality, data integrity, machine-to-machine authentication, and others. The recommended IP network security protocols are IPSec (Internet Protocol security suite), Secure Shell (SSH), and Secure Socket Layer/Transport Layer Security (SSL/TLS), and the choice and use of a particular IP network security protocol is based on particular service provider requirements.

External IPsec VPN devices may also be used to meet these recommendations for protection of management traffic. Using an external IPSec VPN instead of embedded IPsec solutions however introduces extra complexity and does not provide end-to-end protection between management servers. Thus the preferred longer-term solution is to incorporate the capability directly into the management platforms.

All of the IP network security protocols rely on underlying cryptographic algorithms such as AES (Advanced Encryption Standard), DES (Data Encryption Standard), TDEA (Triple Data Encryption Algorithm), HMAC-MD5 (Hashed Message Authentication Code with Message Digest 5), HMAC-SHA-1 (Hashed Message Authentication Code with Secure Hash Algorithm-1), RSA (Rivest, Shamir, Adleman) and other cryptographic algorithms to provide the security services. Please note that the choice of particular cryptographic algorithms and key lengths for use with IP network security protocols is based on particular service provider and market requirements, and no specific recommendations are made in this document. {References [FIPS-46-3], [FIPS-197], [RFC 2403], [RFC 2404], [RFC 2437]}.

IPsec Security Services:

Overview and Capabilities

IPsec addresses security at the IP layer, provided through the use of a combination of cryptographic and protocol security mechanisms. IPSec protocol runs between the Network layer (Layer 3) and the Transport layer (Layer 4) and can be used to protect any type of data traffic (TCP or UDP) and is independent of applications. IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered by IPsec includes:

a) Data integrity

b) Data origin authentication based on IP address

c) Machine-to-machine authentication

d) Anti-Replay Protection

e) Data confidentiality

f) Cryptographic key exchange

These objectives are met through the use of two traffic security services, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. AH service provides data origin authentication, machine-to-machine authentication and data integrity for IP packets. ESP service provides data confidentiality service in addition to data origin authentication, machine-to-machine authentication and data integrity for IP packets. IPsec mechanisms also designed to be cryptographic algorithm-independent to permits selection of different sets of algorithms without affecting the other parts of the implementation.

Key Management is provided by the Internet Key Exchange (IKE) protocol. Both manual and automatic mechanisms for key negotiation between endpoints are provided. Automatic key negotiation can be based on pre-shared keys (e.g. passwords) or X.509 certificates.

Recommendations for use of IPsec for Itf-N Security

This section provides basic recommendation for the use of IPsec for protection of network management traffic crossing the Itf-N interface, and is not intended to be exhaustive.

a) The Itf-N servers operate in a client-server (host to host) environment and therefore the use IPsec transport mode versus IPsec tunnel mode is recommended.

b) ESP service is recommended versus AH service since it can provide encryption service and/or authentication services. AH service can only provide authentication service.

c) It is recommended to use always use the optional ESP authentication service when using ESP encryption service.

d) If only authentication services are needed, it is recommended to use ESP service with null encryption to accomplish this.

e) It is recommended to choose underlying cryptographic algorithms depending on service provider and market requirements. (For North American applications 128 bit AES should be strongly considered).

f) References [RFC 2401], [RFC 2402], [RFC 2403], [RFC 2404], [RFC 2405], [RFC 2406], [RFC 2407], [RFC 2408], [RFC 2409], [RFC 2410], [RFC 2411], [RFC 2412], [RFC 3602], [RFC 2451], [FIPS-197].

SSL/TLS Security Services:

Overview and Capabilities

The Secure Sockets Layer (SSL) security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection at the transport layer (layer 4). SSL is currently at revision 3.0. Transport Layer Security (TLS) is the IETF standardized version of SSL which includes security enhancements over SSL including:

- Required Diffie-Hellman and DSA digital signatures algorithm (DSA) support, with optional RSA support.

- Use of stronger hashed message authentication algorithm (HMAC) instead of a non-standard SSL defined MAC algorithm.

- Modified key generation algorithm which uses MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1) with the HMAC.

The SSL/TLS protocol runs above the Network Layer (Layer 4) and works with Transport Control Protocol (TCP) protocol only and cannot work with User Datagram Protocol (UDP). The application layer protocols that commonly run on top of SSL/TLS include, but are not limited to, Hypertext Transport Protocol (HTTP), the Lightweight Directory Access Protocol (LDAP), and the Internet Messaging Access Protocol. Higher application-level protocol can work above SSL/TLS without any regard for SSL/TLS; however the application level must be linked to SSL/TLS through the use of I/O callbacks.

The SSL/TLS protocol provides three security functions for TCP traffic: data confidentiality, data integrity and authentication.

The SSL/TLS security protocol architecture provides two layers which run over TCP: The SSL/TLS Upper Layer Protocols, and the SSL/TLS Record Protocol.

The SSL/TLS Upper Layer Protocols includes the SSL/TLS Handshake Protocol, SSL/TLS Cipher Change Protocol, and the SSL/TLS Alert Protocol for notifications. SSL/TLS sessions are initially created by the SSL/TLS handshake protocol which provides:

a) Negotiation of authentication and security mechanisms.

b) Authentication of client and server. (Using the server and client public/private keys).

c) Establishment of security keys.

Once the SSL/TLS session is established, the SSL/TLS Record Protocol is used for bulk data transport services. The SSL/TLS Record Protocol provides:

a) Data origin authentication based on the server keys.

b) Data integrity.

c) Confidentiality.

Recommendations for use of SSL/TLS for Itf-N Security

This section provides basic recommendation for the use of SSL/TLS for protection of network management traffic crossing the Itf-N interface, and is not intended to be exhaustive.

a) Where SSL/TLS is required, either SSLv3 or TLS may be used . However, it is noted that TLS has enhanced security over SSL.

b) SSL/TLS allows either unidirectional authentication where the server is authenticated to the client only, or bidirectional authentication where both client and server authenticate to each other. Unidirectional authentication is the usual method used in the public internet, however for network management applications bidirectional authentication is recommended to allow both parties to know they are communicating with the desired endpoint.

c) References [RFC 2246], [RFC 3546], [SSL V3].

SSH Security Services:

Overview and Capabilities

SSH is an Application Layer (Layer 7) security protocol commonly used to directly replace insecure protocols Telnet and File Transfer Protocol (FTP) protocols. Telnet and FTP are insecure protocols which transmit passwords and all other data in the clear. SSH can also be used to protect other protocols through the use of port forwarding, so it can be used as a general network security protocol.

There are two versions of SSH: SSHv1 and SSHv2. SSHv1 was developed in 1998 and is now considered insecure/obsolete.

Secure Shell 2 features are:

- Full replacement for Telnet, Rlogin, Rsh, Rcp, and FTP protocols to provide secure file transfer and file copying.

- Automatic authentication of users. (no passwords sent in clear-text).

- Bi-directional authentication (both the server and the client are authenticated).

- Tunnelling of arbitrary TCP/IP-based applications through the use of port forwarding.

- Encryption of data for data confidentiality.

- Multiple authentication options including passwords, public key, and SecureID authentication

- Multiple ciphers suites available.

The SSHv2 architecture is consists of three major components:

- The Transport Layer Protocol [RFC 4253] provides server authentication, data confidentiality, and data integrity. It may optionally also provide compression.

- The User Authentication Protocol [RFC 4252] authenticates the client-side user to the server.

- The Connection Protocol [RFC 4254] multiplexes the encrypted tunnel into several logical channels.

The connection protocol provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding ("tunnelling") arbitrary TCP/IP ports and connections.

Port number 22 has been registered with the IANA as the standard port to use for SSHv2 applications.

Recommendations for use of SSH for Itf-N Security

This section provides basic recommendation for the use of SSH for protection of network management traffic crossing the Itf-N interface, and is not intended to be exhaustive.

a) It is recommended to use SSHv2 where SSH protocol is required because of its widespread acceptance and enhanced security over SSHv1.

b) SSHv1 should be considered insecure/obsolete.

c) Interoperating with an SSHv1 protocol is not recommended and SSHv1 connection attempts should be rejected.

d) References [RFC 4251], [RFC 4253], [RFC 4252], [RFC 4254].

Conclusions/Recommendations

IP Network Security protocols (IPsec, SSL/TLS or SSH) can be used to provide baseline infrastructure security between machines communicating across the Itf-N. It is recommended to use these IP Network security protocols to provide underlying security for the 3GPP OA&M network, with the choice of protocols and cryptographic dependant on particular service provider and market requirements.

References

|  |  |
| --- | --- |
| [TS 32.101] | 3GPP TS 32.101: "Telecommunication management; Principles and high level requirements". |
| [M.3016] | ITU‑T Recommendation M.3016 (1998): "TMN security overview". |
| [RFC2401] | IETF RFC 2401, "Security Architecture for the Internet Protocol", November 1998, S. Kent, R. Atkinson;  <http://www.ietf.org/rfc/rfc2401.txt?number=2401> |
| [NDS/IP] | 3GPP TS 33.210, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security. |
| [RFC 2402] | IETF RFC 2402, "Internet Protocol Authentication Header", November 1998, S. Kent, R. Atkinson;  <http://www.ietf.org/rfc/rfc2402.txt?number=2402> |
| [RFC 2403] | IETF RFC 2403, " The Use of HMAC-MD5-96 within ESP and AH,” <http://www.ietf.org/rfc/rfc2403.txt?number=2403> |
| [RFC 2404] | IETF RFC 2404, " The Use of HMAC-SHA-1-96 within ESP and AH,” <http://www.ietf.org/rfc/rfc2404.txt?number=2404> |
| [RFC 2405] | IETF RFC 2405, "The ESP DES CBC Cipher Algorithm with Explicit IV,”  <http://www.ietf.org/rfc/rfc2405.txt?number=2405> |
| [RFC 2406] | IETF RFC 2406, "IP Encapsulating Security Payload (ESP),” <http://www.ietf.org/rfc/rfc2406.txt?number=2406> |
| [RFC 2407] | IETF RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP,”  <http://www.ietf.org/rfc/rfc2407.txt?number=2407> |
| [RFC 2408] | IETF RFC 2408, " Internet Security Association and Key Management Protocol,”  <http://www.ietf.org/rfc/rfc2408.txt?number=2408> |
| [RFC 2409] | IETF RFC 2409, "Internet Key Exchange,” <http://www.ietf.org/rfc/rfc2409.txt?number=2409> |
| [RFC 2410] | IETF RFC 2410, “The Null Encryption Algorithm and Its Use with IPsec,”  <http://www.ietf.org/rfc/rfc2410.txt?number=2410> |
| [RFC 2411] | IETF RFC 2411, “IP Security Document Roadmap,” <http://www.ietf.org/rfc/rfc2411.txt?number=2411> |
| [RFC 2412] | IETF RFC 2412, “The OAKLEY Key Determination Protocol,” <http://www.ietf.org/rfc/rfc2412.txt?number=2412> |
| [RFC 3602] | IETF RFC 3602, “[The AES-CBC Cipher Algorithm and Its Use with IPsec](http://www.ietf.org/rfc/rfc3602.txt)”  <https://www.rfc-editor.org/rfc/rfc3602.txt> |
| [RFC 2451] | The ESP CBC-Mode Cipher Algorithms  <http://www.ietf.org/rfc/rfc2451.txt> |
| [RFC 2246] | IETF RFC 2236, “The TLS Protocol, Version 1.0”  <ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt> |
| [RFC 3546] | IETF RFC 3546, “Transport Layer Security (TLS) Extensions”  <ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt> |
| [SSL V3] | Secure Socket Layer Version 3.0 Specification, Netscape Communications.  <http://wp.netscape.com/eng/ssl3/> |
| [RFC 4251] | IETF RFC 4251, "The Secure Shell (SSH) Protocol Architecture"  <https://www.rfc-editor.org/rfc/rfc4251.txt> |
| [RFC 4253] | IETF RFC 4253, "The Secure Shell (SSH) Transport Layer Protocol"  <https://www.rfc-editor.org/rfc/rfc4253.txt> |
| [RFC 4252] | IETF RFC 4252 "The Secure Shell (SSH) Authentication Protocol"  <https://www.rfc-editor.org/rfc/rfc4252.txt> |
| [RFC 4254] | IETF RFC 4254, "The Secure Shell (SSH) Connection Protocol"  <https://www.rfc-editor.org/rfc/rfc4254.txt> |
| [FIPS-46-3] | Data Encryption Standard. (Describes both DES and 3DES).  <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf> |
| [FIPS-197] | Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001.  <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf> |
| [FIPS-197] | Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001.  <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf> |
| [RFC 2437] | PKCS #1: RSA Cryptography Specifications Version 2.0. B. Kaliski, J. Staddon. October 1998  <http://www.ietf.org/rfc/rfc2437.txt?number=2437> |

|  |
| --- |
| **End of modifications** |