3GPP TSG SA WG3 Security — S3#20 **S3-010430**

16 - 19 October, 2001 Sydney, Australia

3GPP TR 33.900 V0.4.1 (2001-08)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
A Guide to 3rd Generation Security
(Release 5)

Keywords
3GPP, SEC-1, Guidelines

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This document is intended to offer security guidance to those involved in 3GPP systems. All specifications have to take into account the cost and feasibility of security features and functions. It is important to realise possible risks and threats may exist. The document describes those security issues that have been identified in the formulation of the standards.

1 Scope

The present document gives a general description of the security risks and threats of the 3rd Generation Security standards. It is intended to provide an overview of security, for detailed explanation and the actual standards the reader is referred to the appropriate standards.

It also serves the purpose of identifying the potential risks and threats that have been highlighted and require careful consideration when implementing a third generat6ion mobile system.

Readers should note that some possible security attacks have been identified and omitted from this document, as the architecture does not protect against these attacks.

2 References

2.1 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 33.102: "3GPP Security; Security Architecture".

[2] 3GPP TS 33.103: "Security Integration Guidelines".

[3] 3GPP TS 33.105: "Cryptographic Algorithm Requirements".

[4] 3GPP TS 33.106: "Lawful Interception requirements".

[5] 3GPP TS 33.107: "Lawful interception architecture and functions".

[6] 3GPP TR 33.901: "Criteria for cryptographic algorithm design process".

[7] 3GPP TR 33.902: "Formal analysis of the 3GPP authentication protocol with a modified sequence number".

[8] 3GPP TS 33.120: "3GPP Security; Security Principles and Objectives".

[9] 3GPP TS 21.133: "3GPP Security; Security Threats and Requirements".

IETF documents:

[10] IETF RFC 792: "ICMP – Internet Control Message Protocol", 09/01/1981.

[11] IETF RFC 1191: "Path MTU Discovery", Nov 1990.

[12] IETF RFC 1981: "Path MTU Discovery for IP version 6", Aug 1996.

[13] IETF Internet Draft: "ICMP Traceback Messages", Mar 2000.

ISO documents

[14] ISO/IEC 17799: "Information technology. Code of practice for information security management".

3 Abbreviations

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

DoS	Denial of Service
SPC	Signalling Point Code

4 A brief overview of 3GPP Security

Consideration of previous security standards lead to the following enhancements in 3GPP:

- The security mechanisms include a protocol that ensures that the mobile can perform some degree of mutual authentication. This reduces the risk of a false base station attack.
- Key lengths were increased to allow for the possibility of stronger algorithms for encryption and integrity.
- Mechanisms were included to support security within and between networks.
- Security is taken back into the network, therefore links are also protected.
- Terminal identity (IMEI) a requirement that it cannot be easily changed within the standards.
- For the authentication algorithm guidance on choice will be given.
- When roaming between networks of different standards, only the level of protection supported by the mobile equipment will apply.

5 Counteracting envisaged 3GPP attacks

Many of the security enhancements required for 3GPP systems are intended to counteract attacks which were not perceived to be feasible in 2G systems. This includes attacks that are, or are perceived to be, possible now or very soon because intruders have access to more computational capabilities, new equipment has become available, and the physical security of certain network elements is questioned.

In order to perform the attacks the intruder has to possess one or more of the following capabilities to compromise communications security:

- Radio path attacks: **Eavesdropping.** This is the capability that the intruder eavesdrops signalling and data connections associated with other users. The required equipment is a *modified MS or specialised equipment.*
- Radio path attacks: **Impersonation of a user.** This is the capability whereby the intruder sends signalling and/or user data to the network, in an attempt to make the network believe they originate from the target user. The required equipment is again a *modified MS or specialised equipment.*
- Radio path attacks: **Impersonation of the network.** This is the capability whereby the intruder sends signalling and/or user data to the target user, in an attempt to make the target user believe they originate from a genuine network. The required equipment is modified *BS or modified MS.* Another scenario is where the intruder puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signalling and user data messages exchanged between the two parties. The required equipment is modified *BS in conjunction with a modified MS.*
- **Network security.** Where the attacker manages to intercept, eavesdrop or attack data or network elements.
- **Compromising authentication vectors in the network.** The intruder possesses *a compromised authentication vector*, which may include challenge/response pairs, cipher keys and integrity keys. This data may have been obtained by compromising network nodes or by intercepting signalling messages on network links, for example signalling system number 7.
- **Interruption of the communication.** This is the capability that the intruder sends enormous amount of bogus traffic to 3G network and users to block the signalling or user traffic, and therefore cause abusive usage of

network resources. This is also called Denial of Service attacks. The nature of the attacks is that the victim can not detect the real sender of the bogus traffic.

5.1 Radio path attacks

5.1.1 User de-registration request spoofing

Description:

An attack that requires a modified MS and exploits the weakness that the network cannot authenticate the messages it receives over the radio interface. The intruder spoofs a de-registration request (IMSI detach) to the network. The network de-registers the user from the visited location area and instructs the HLR to do the same. The user is subsequently unreachable for mobile terminated services.

Does 3GPP security architecture counteract the attack?

Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the de-registration request allows the serving network to verify that the de-registration request is legitimate.

5.1.2 Location update request spoofing

Description:

An attack that requires a modified MS and exploits the weakness that the network cannot authenticate the messages it receives over the radio interface. Instead of the de-registration request, the attacker spoofs a location update request in a different location area from the one in which the user is roaming. The network registers in the new location area and the target user will be paged in that new area. The user is subsequently unreachable for mobile terminated services.

Does 3GPP security architecture counteract the attack?

Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the location update request allows the serving network to verify that the location update request is legitimate.

5.1.3 Mobile connecting to a false BS

Description:

An attack that requires a modified BS and exploits the weakness that a user can be enticed to attach on a false base station. Once the target user selects the radio channels of a false base station, the target user is out of reach of the paging signals of the serving network in which he is registered.

Does 3GPP security architecture counteract the attack?

The security architecture does not counteract this attack. However, the denial of service in this case only persists for as long as the attacker is active unlike the above attacks, which persist beyond the moment where intervention by the attacker stops. These attacks are comparable to radio jamming which is very difficult to counteract effectively in any radio system.

5.1.4 Attaching on a false Radio Access Network

Description:

An attack that requires a modified BS/MS and exploits the weakness that a user can be enticed to attach on a false base station. A false BS/MS can act as a repeater for some time and can relay some requests in between the network and the target user, but subsequently modify or ignore certain service requests and/or paging messages related to the target user.

Does 3GPP security architecture counteract the attack?

The security architecture does not prevent a false BS/MS relaying messages between the network and the target user, neither does it prevent the false BS/MS ignoring certain service requests and/or paging requests. Integrity protection of critical message may however help to prevent some denial of service attacks, which are induced by modifying certain messages. Again, the denial of service in this case only persists for as long as the attacker is active unlike the above attacks, which persist beyond the moment where intervention by the attacker stops. These attacks are comparable to radio jamming which is very difficult to counteract effectively in any radio system. If encryption is kept always on then this will counteract this attack, as the mobile will be aware if encryption fails.

5.1.5 Passive identity catching

Description:

A passive attack that requires a modified MS and exploits the weakness that the network may sometimes request the user to send its identity in cleartext.

Does 3GPP security architecture counteract the attack?

The identity confidentiality mechanism counteracts this attack. The use of temporary identities allocated by the serving network makes passive eavesdropping inefficient since the user must wait for a new registration or a mismatch in the serving network database before he can capture the user's permanent identity in plaintext. The inefficiency of this attack given the likely rewards to the attacker would make this scenario unlikely. (Note however that the permanent identity may be protected in the event of new registrations or serving network database failure in order to guard against more efficient active attacks).

5.1.6 Active identity catching

Description:

An active attack that requires a modified BS and exploits the weakness that the network may request the MS to send its permanent user identity in cleartext. An intruder entices the target user to attach on its false BS and subsequently requests the target user to send its permanent user identity in cleartext perhaps by forcing a new registration or by claiming a temporary identity mismatch due to database failure.

Does 3GPP security architecture counteract the attack?

The identity confidentiality mechanism counteracts this attack by using an encryption key shared by a group of users to protect the user identity in the event of new registrations or temporary identity database failure in the serving network. Note however that the size of the groups should be chosen carefully: too small and the group identify may compromise the user identity itself; too large and the group encryption key might be vulnerable to attack. The enhanced user identity group key also protects against this attack.

5.1.7 Impersonation of the network by suppressing encryption between the target user and the intruder

Description:

An attack that requires a modified BS and that exploits the weakness that the MS cannot authenticate messages received over the radio interface. The target user is enticed to attach on the false BS. When the intruder or the target user initiates a service, the intruder does not enable encryption by spoofing the cipher mode command. The intruder maintains the call as long as it is required or as long as his attack remains undetected.

Does 3GPP security architecture counteract the attack?

A mandatory cipher mode command with message authentication and replay inhibition allows the mobile to verify that encryption has not been suppressed by an attacker.

5.1.8 Impersonation of the network by suppressing encryption between the target user and the true network

Description:

An attack that requires a modified BS/MS and that exploits the weakness that the network cannot authenticate messages received over the radio interface. The target user is enticed to attach on the false BS/MS. When a call is set-up the false BS/MS modifies the ciphering capabilities of the MS to make it appear to the network that a genuine incompatibility exists between the network and the mobile station. The network may then decide to establish an un-enciphered connection. After the decision not to cipher has been taken, the intruder cuts the connection with the network and impersonates the network to the target user.

Does 3GPP security architecture counteract the attack?

A mobile station command with message authentication and replay inhibition allows the network to verify that encryption has not been suppressed by an attacker.

5.1.9 Eavesdropping on user data by suppressing encryption between the target user and the intruder

Description:

An attack that requires a modified BS/MS and that exploits the weakness that the MS cannot authenticate messages received over the radio interface. The target user is enticed to attach on the false BS. When the target user or the intruder initiates a call the network does not enable encryption by spoofing the cipher mode command. The attacker however sets up his own connection with the genuine network using his own subscription. The attacker may then subsequently eavesdrop on the transmitted user data.

Does 3GPP security architecture counteract the attack?

A mandatory cipher mode command with message authentication and replay inhibition allows the mobile to verify that encryption has not been suppressed by an attacker.

5.1.10 Hijacking incoming calls in networks with encryption disabled

Description:

This attack requires a modified BS/MS. While the target user attaches on the false base station, an associate of the intruder makes a call to the target user's number. The intruder acts as a relay between the network and the target user until authentication and call set-up has been performed between target user and serving network. The network does not enable encryption. After authentication and call set-up the intruder releases the target user, and subsequently uses the connection to answer the call made by his associate. The target user will have to pay for the roaming leg.

Does 3GPP security architecture counteract the attack?

Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the connection accept message allows the serving network to verify that the request is legitimate. In addition, periodic integrity protected messages during a connection helps protect against hijacking of un-enciphered connections after the initial connection establishment. However, hijacking the channel between periodic integrity protection messages is still possible, although this may be of limited use to attackers. In general, connections with ciphering disabled will always be vulnerable to some degree of channel hijacking.

5.2 Infrastructure based attacks

5.2.1 Impersonation of the network by forcing the use of a compromised cipher key

Description:

An attack that requires a modified BS and the possession by the intruder of a compromised authentication vector; thus exploits the weakness that the user has no control upon the cipher key. The target user is attached on the false BS/MS. When a call is set-up the false BS/MS forces the use of a compromised cipher key on the mobile user. The intruder maintains the call as long as it is required or as long as his attack remains undetected.

Does 3GPP security architecture counteract the attack?

The presence of a sequence number in the challenge allows the SIM to verify the freshness of the cipher key to help guard against forced re-use of a compromised authentication vector. However, the architecture does not protect against force use of compromised authentication vectors, which have not yet been used to authenticate the SIM. Thus, the network is still vulnerable to attacks using compromised authentication vectors, which have been intercepted between generation in the authentication centre and use and destruction in the serving network. The user must trust the SN (through the HE) to handle authentication vectors securely. For instance, an attacker with a false BS may work in collusion with an SN to intercept unused authentication vectors, or the SN may expose itself to undue risks because it stockpiles large numbers of authentication vectors before they need to be used.

5.2.2 Eavesdropping on user data by suppression of encryption between the target user and the true network

Description:

An attack that requires a modified BS/MS and that exploits the weakness that the network cannot authenticate messages received over the radio interface. The target user is enticed to attach on the false BS/MS. When the target user or the genuine network sets up a connection, the false BS/MS modifies the ciphering capabilities of the MS to make it appear to the network that a genuine incompatibility exists between the network and the mobile station. The network may then decide to establish an un-enciphered connection. After the decision not to cipher has been taken, the intruder may eavesdrop on the user data.

Does 3GPP security architecture counteract the attack?

Message authentication and replay inhibition of the mobile’s ciphering capabilities allows the network to verify that encryption has not been suppressed by an attacker.

5.2.3 Eavesdropping on user data by forcing the use of a compromised cipher key

Description:

An attack that requires a modified BS/MS and the possession by the intruder of a compromised authentication vector and thus exploits the weakness that the user has no control the cipher key. The target user is enticed to attach on the false BS/MS. When the target user or the intruder set-up a service, the false BS/MS forces the use of a compromised cipher key on the mobile user while it builds up a connection with the genuine network using its own subscription.

Does 3GPP security architecture counteract the attack?

The presence of a sequence number in the challenge allows the SIM to verify the freshness of the cipher key to help guard against forced re-use of a compromised authentication vector. However, the architecture does not protect against force use of compromised authentication vectors, which have not yet been used to authenticate the SIM. Thus, the network is still vulnerable to attacks using compromised authentication vectors, which have been intercepted between generation in the authentication centre and use and destruction in the serving network.

The user must trust the SN (transitively via the HE) to handle authentication vectors securely. For instance, an attacker with a false BS may work in collusion with an SN to intercept unused authentication vectors, or the SN may expose itself to undue risks because it stockpiles large numbers of authentication vectors before they need to be used.

5.2.4 Impersonation of the user through the use of by the network of a compromised authentication vector

Description:

An attack that requires a modified MS and the possession by the intruder of a compromised authentication vector which is intended to be used by the network to authenticate a legitimate user. The intruder uses that data to impersonate the target user towards the network and the other party.

Does 3GPP security architecture counteract the attack?

The presence of a sequence number in the challenge means that authentication vectors cannot be re-used to authenticate SIMs. This helps to reduce the opportunity of using a compromised authentication vector to impersonate the target user. However, the network is still vulnerable to attacks using compromised authentication vectors, which have been intercepted between generation in the authentication centre and use and destruction in the serving network.

The user must trust the SN (transitively via the HE) to handle authentication vectors securely. For instance, an attacker with a false BS may work in collusion with an SN to intercept unused authentication vectors, or the SN may expose itself to undue risks because it stockpiles large numbers of authentication vectors before they need to be used.

5.2.5 Impersonation of the user through the use by the network of an eavesdropped authentication response

Description:

An attack that requires a modified MS and exploits the weakness that an authentication vector may be used several times. The intruder eavesdrops on the authentication response sent by the user and uses that when the same challenge is sent later on. Subsequently, ciphering has to be avoided by any of the mechanisms described above. The intruder uses the eavesdropped response data to impersonate the target user towards the network and the other party.

Does 3GPP security architecture counteract the attack?

The presence of a sequence number in the challenge means that authentication vectors cannot be re-used to authenticate SIMs.

6 Network issues

Every 3GPP network has sensitive network elements that must be properly managed; an example of these is given in Annex A.

6.1 Legitimate roaming partner identity spoofing

Description:

An attack that exploits the weakness that the network cannot authenticate the messages it receives over SS7 or IP for supporting internetwork roaming. The intruder spoofs the roaming partner’s identity or network node addresses (SPC or IP address) then send bogus signalling traffics to the victim’s networks.

Does 3G security architecture counteract the attack: Yes for IP based signalling; No for the SS7 based signalling.

Some Internet Firewalls have the functionality to perform IP packets filtering. Also using IPSec for securing signalling over IP can effectively prevent this type of attacks.

However, for SS7 based signalling there is no security protection at the SS7 layer. Need further investigation.

6.1.1 Push-service initiator identity spoofing

Description:

An attack that exploits the weakness that the 3G network cannot authenticate the user traffics it receives from a Push service initiator which is located on the Internet. The intruder spoofs the Push-service initiator's IP address, then send bogus IP packets to the victim 3G users to either block the core network traffic channel or radio interface traffic channel.

Does 3G security architecture counteract the attack: No at the moment.

Stateful Internet Firewalls may be developed to deal with various PUSH-type services.

6.1.1.1 Internet router identity spoofing

Description:

An attack that exploits the weakness that the 3G network cannot authenticate the Internet ICMP diagnostic messages it receives from Internet routers. The intruder spoofs the Internet routers IP addresses, then send various ICMP diagnostic messages to 3G network and users to interrupt the communication by abuse network resources.

Does 3G security architecture counteract the attack: Yes if all those diagnostic messages are blocked.

Although some stateful Firewalls can perform selective filtering of ICMP messages, the intruder can still utilise some diagnostic services to launch DoS attacks to 3G networks and users. One example of the diagnostic services is Path MTU Discovery.

6.2 Security policy

An example security policy for a 3G network is given in Annex A. Reference ISO/IEC 17799 [14] is also a useful source of information.

7 Inter Network Security

7.1 Signalling system Number 7

Mobile networks primarily use Signalling System no. 7 (SS7) for communication between networks for such activities as authentication, location update, and supplementary services and call control. The messages unique to 3GPP are MAP messages.

The security of the global SS7 network as a transport system for signalling messages e.g. authentication and supplementary services such as call forwarding is open to major compromise.

The problem with the current SS7 system is that messages can be altered, injected or deleted into the global SS7 networks in an uncontrolled manner.

In the past, SS7 traffic was passed between major PTO's covered under treaty organisation and the number of operators was relatively small and the risk of compromise was low.

Networks are getting smaller and more numerous. Opportunities for unintentional mishaps will increase, as will the opportunities for hackers and other abusers of networks.

With the increase in different types of operators and the increase in the number of interconnection circuits there is an ever-growing loss of control of security of the signalling networks.

There is also exponential growth in the use of interconnection between the telecommunication networks and the Internet. The IT community now has many protocol converters for conversion of SS7 data to IP, primarily for the transportation of voice and data over the IP networks. In addition new services such as those based on IN will lead to a growing use of the SS7 network for general data transfers.

There have been a number of incidents from accidental action, which have damaged a network. To date, there have been very few deliberate actions.

The availability of cheap PC based equipment that can be used to access networks and the ready availability of access gateways on the Internet will lead to compromise of SS7 signalling and this will effect mobile operators.

The risk of attack has been recognised in the USA at the highest level of the President's office indicating concern on SS7. It is understood that the T1, an American group is seriously considering the issue.

For the network operator there is some policing of incoming signalling on most switches already, but this is dependent on the make of switch as well as on the way the switch is configured by operators.

Some engineering equipment is not substantially different from other advanced protocol analysers in terms of its fraud potential, but is more intelligent and can be programmed more easily.

The SS7 network as presently engineered is insecure. It is vitally important that network operators ensure that signalling screening of SS7 incoming messages takes place at the entry points to their networks and that operations and maintenance systems alert against unusual SS7 messages. There are a number of messages that can have a significant effect on the operation of the network and inappropriate messages should be controlled at entry point.

Network operators network security engineers should on a regular basis carry out monitoring of signalling links for these inappropriate messages. In signing agreements with roaming partners and carrying out roaming testing, review of messages and also to seek appropriate confirmation that network operators are also screening incoming SS7 messages their networks to ensure that no rouge messages appear.

In summary there is no adequate security left in SS7. Mobile operators need to protect them selves from attack from hackers and inadvertent action that could stop a network or networks operating correctly.

Operators should note that HPLMN control over a subscriber roaming in a VPLMN using different MAP release could be limited. To avoid this, operators should assure that their roaming partners use the current MAP version, as specified by the 3GPP Association.

7.2 TCP/IP Internet protocol connections

Most communications nodes will have some form of Ethernet connection running the TCP/IP protocol. The capabilities and vulnerabilities of this connection largely depend on the operating system in use on the node. This connection should be regarded as somewhat insecure. It can be assumed that the operator has an internal Intranet data network that is connected to the Internet via adequate firewall protection.

Where nodes use standard operating systems such as Unix or variations of Unix the configuration of the systems needs to be carefully considered. Where systems use in-house operating systems the systems should be designed and built with reference to the known vulnerabilities in standard operating systems and their components.

The resources of CERT Co-ordination Centre, the Computer Incident Advisory Capability (CIAC), and National Computer Security Centre (NCSC), and other resources should be consulted and monitored with respect to the vulnerabilities of the operating system and other components.

8 Intra network security

8.1 3GPP Network elements and interfaces

Unauthorised, local or remote access to 3GPP network elements can result in access to confidential data stored by system entities, unauthorised access to services and resources, misuse of the network element to gain access to data or services or denial of service. The following section gives an outline of potential threats related to attacks on 3GPP network elements and recommendations.

8.1.1 Home Location Register - HLR

An unauthorised access to HLR could result in activating subscribers not seen by the billing system, thus not chargeable. Services may also be activated or deactivated for each subscriber, thus allowing unauthorised access to services or denial of service attacks. In certain circumstances it is possible to use Man-Machine (MM) commands to monitor other HLR user's action - this would also often allow for unauthorised access to data.

An operator should not rely on the fact that an intruder's knowledge on particular vendor's MM language will be limited. Those attacks can be performed both by external intruders and by operator's employees.

Access control to HLRs should be based on user profiles, using at least a unique username and a password as authentication data. Remote access to HLR should be protected from eavesdropping, source and destination spoofing and session hijacking. An operator may therefore wish to limit the range of protocols available for communication with HLR.

8.1.2 Authentication Centre - AuC

An intruder who gains direct access to an AuC can effectively clone all subscribers whose data he had access to.

Number of employees having physical and logical access to AuC should be limited. From security point of view it is then reasonable to use an AuC which is not integrated with HLR.

Operators should carefully consider the need for encryption of AuC data. Some vendors use default encryption, the algorithm being proprietary and confidential. It should be noted that strength of such encryption could be questionable.

If decided to use an add-on ciphering facility, attention should be paid to cryptographic key management. Careless use of such equipment could even lower AuC security.

Authentication triplets can be obtained from AuC by masquerading as another system entity (namely HLR). The threat is present when HLR and AuC are physically separated.

8.1.3 Mobile Switching Centre - MSC

An MSC is one of the most important nodes of any 3GPP network. It handles all calls incoming to, or originating from subscribers visiting the given switch area. Unauthorised, local or remote, access to an MSC would likely result in the loss of confidentiality of user data, unauthorised access to services or denial of service for large numbers of subscribers.

It is strongly recommended that access to MSCs is restricted, both in terms of physical and logical access. It is also recommended that their physical location is not made public.

When co-located, several MSC should be independent (i.e. separated power, transmission,) in order to limit the impacts from accidents on one particular MSC (e.g. fire).

8.1.4 3GPP network interfaces

An intruder gaining access to 3GPP network interfaces would primary gain access to information sent on the interface targeted. However, playing denial-of-service attacks would also be feasible - dependent on how the interface is technically realised (e.g. cable or wireless).

Telecommunication networks are usually designed with necessary redundancy, allowing for reconfiguration in case of loss of a link or links. From security point of view it is particularly important to foresee alternate connection paths where links vulnerable to denial-of-service attacks (e.g., microwave links susceptible to jamming) are in use.

8.1.5 Billing system / Customer Care system

Billing/customer care systems are critical for maintaining the business continuity of a 3GPP Operator.

Unauthorised access to the billing or customer care system could result in:

- loss of revenue due to manipulated CDRs (on the mediation device/billing system level);

- unauthorised applying of service discounts (customer care system level), unauthorised access to services (false subscriptions);

- and even denial of service - by repeated launching of resource - consuming system jobs.

Attention should be paid to the fact that access rights to the billing/customer care system are often granted to temporary employees.

As 3GPP network operators should introduce proper access control mechanisms, coherent with the Operator's general security policy. In particular, it would be advisable to:

- Control the access to the billing data on the database level;

- All users of the billing system should be authenticated by the billing database and access rights should be granted by the database upon successful authentication. Relaying on the application-to-database authentication leaves the database open for a skilled attacker;

- Review the activation process.

The same employee should not carry out both tasks; data verification should involve a trusted employee. Activation should be made only upon confirmation of the person verifying the data entered.

9 *User Module and Smart Card*

If a 3GPP SIM is integrated on a multi-application smart card, there should be sufficient guarantees that the Ki cannot be read or used by any application other than the 3GPP application. Also there should be clear and secure procedures for placing applications and information on the smart card, ensuring that 3GPP information cannot be changed in an unauthorised way. There should be clear responsibilities and procedures for dealing with stolen or malfunctioning cards.

The importance of secure management of Ki's is already detailed above. In addition it is important that SIM status lists are kept up to date and that operators define measures to detect and investigate the misuse of SIMs. There should be procedures to replace SIMs, for example at the end of their validity period, and to deal with stolen SIMs. It is particularly important that individual operators devise and operate secure SIM management processes with their SIM suppliers and throughout the SIM distribution channel.

10 Algorithms

10.1 Authentication algorithm

3GPP has defined a standard authentication algorithm called MILENAGE, but also allows operators to choose their own versions, which comply with the published standards.. The authentication algorithm is contained within the smart card.

The individual key for each IMSI must be chosen to be **random**, and must be protected in order to prevent the user from being duplicated. Throughout the security process Ki should be protected.

10.2 Confidentiality algorithm

3GPP defines a standard confidentiality algorithm called KASUMI, which is contained within all mobiles, and protects user data from the mobile to the serving node. This is not only over the radio path as in GSM, but also continues back over the links to the serving node.

11 Services

There are many value-added services within the 3G standards, which when wrongly implemented or interpreted, can be used for fraud.

For example, call forwarding can be set which will then allow calls made to a mobile to be sent to expensive destination numbers. This could be done, for example, by ringing a mobile customer and getting them to put in a call forward number themselves by persuading them that they are testing the mobile.

Many other similar problems exist, such as follow-me services, voicemail, and explicit call transfer. It is to expected that as the services offered by 3GPP become more complex (and include for example Internet connectivity, packet data services as well as MExE which runs code on the mobile, and Java multi application smart cards) then the problem can only become worse.

Operators should ensure that they look carefully at every new network feature and service product to ensure that such problems will not occur in their networks.

11.1 Location services

The location service feature in 3GPP depends on the accuracy of the mechanism used within the mobile equipment. It cannot be though of as accurate, as the mobile software can be modified, or the GPS (Global Positioning System by Satellite) could be displaced by a differential input. There are, of course, personal privacy issues that must be taken into account of location based services, as well as designing the system to provide data to those to which the customer agrees.

11.2 Mobile Execution Environment - MExE

The ability to remotely modify remote and run code on a mobile clearly introduces a security risk. In the case of MExE it is up to the user to determine if a possible security risk is introduced, and stop the action from taking place. It is to be expected that a smart attacker will be able to introduce code that will fool a user into setting up services or connection that will compromise them or result them in losing money.

12 Lawful interception

The standards include lawful interception functions for 3GPP, so that where required by national requirements, this facility is built into equipment.

Annex A:
Security policy

This is an example Security Policy that could be used by and operator. You should also take advice from ISO/IEC 17799 [14].

A.1 Example Policy

A.1.1 Access control policy

Access control policy with respect to 3GPP network elements should be consistent with general access control policy as defined in the particular operator's security policy. As a basis, the following rules should apply:

In granting users access rights to 3GPP networks elements or supporting IT systems the following principles should be followed:

- every employee should only have access to those resources necessary for the completion of the work-related tasks set;
- the "positive access control" principle should be applied, meaning it shall be assumed that an employee is authorised to carry out only those operations for which he has obtained authority;
- The right of access to resources should be granted only at the moment when it is actually necessary and should be rescinded when no longer necessary for the completion of work-related tasks.

Operator's employees should be made responsible for the secure storing and use of access control executive components entrusted to them (badges, cards). Access control executive components should not be stored together with a computer used to access the network element or IT system.

Every user of a given system should be provided with an identification (log-in name, account name) that is unique within the framework or the Company. The following principles apply:

- a user's identification on its own should not be sufficient for granting access authority;
- an identification should not give any indication of the user's authority within the system;
- The use of forms of group identification should only be admissible in exceptional circumstances.

Granting of full or very wide rights of access to resources should be limited and strictly controlled.

A.2 Secure network elements interconnection

3GPP network elements must provide means for remote management, maintenance and communication with IT systems (e.g. the billing system). Often an operator's corporate computer network is used for this purpose. This considerably lower infrastructure costs but poses significant security threats for 3GPP system entities. If no security is applied, usually each user of corporate network can try to access remotely a 3GPP network element, provided its network address is known.

As a principle, 3GPP network elements should be separated, at least logically, from an operator's corporate computer network. A unique username and password should identify each employee who is authorised to access to network element. Proper application and system logs should be maintained, reviewed and protected.

Remote access to network entities should be, subject to the operator's security policy, protected from eavesdropping and session hijacking.

Physical access to 3GPP network elements should be controlled by appropriate physical security measures. It is advisable that physical location of network elements be treated as protected information.

A.3 Communications node security

To countermeasure the threats described in this document an operator should define and implement proper security measures. The following section specifies the desirable security features that any 3GPP Network Element (NE), Network System (NS), Operations System (OS) or Data Communications Network (DCN) should provide in order to reduce the risk of potentially service affecting security compromises. The term "3GPP node" in the following section is used to imply a NE, NS, OS, or a DCN and its nodes.

A.3.1 Connection

The connection between the O&M person's screen and the physical 3GPP node should be considered insecure. The manufacturer should provide facilities to ensure the security of this connection. The following options are available.

A.3.1.1 Direct physical connection

This connection should be provided for the installation and major upgrade of equipment. It is as secure as the operators physical access procedures. The node should still require that the user of this connection be authenticated in the same manner as all other users. The only exception to this rule is the allowance of a limited set of commands to the node in order to "boot" the system into an operating state.

A.3.1.2 Direct modem connection

This should be regarded as a highly insecure connection. Equipment manufacturers often propose these sorts of connection in order to provide remote support for their equipment. There are several facilities that should be enabled on these connections to improve the security.

The connection should be able to be disabled and enabled remotely by the network operator. The operator would enable the port on escalation of a fault to the manufacturer, and disabled it again afterwards.

If the authentication system is a username password scheme the modem should be configured for dial back. This means that the connection can only be used from a limited set of locations.

Manufacturers using this type of connection would be strongly advised to support an Authentication Server interface so operators could use Secure-ID or other verification techniques.

The system should provide no information on what the node is before the user has been authenticated. The system should provide a warning explicitly explaining that unauthorised access is prohibited and will be prosecuted to the full extent of the law. This message should be configurable by the operator according to the requirements of the law of the country involved.

A.3.1.3 TELNET network connection

This connection should be regarded as somewhat insecure. It can be assumed that the operator has an internal Intranet data network that is connected to the Internet via adequate firewall protection. This type of connection however transmits all of the session data, including usernames and passwords, in plaintext.

Manufacturers should seriously consider using Kerberos services, or other similar encryption products to ensure the integrity of the network connection.

A.3.1.4 Web browser network connection

Many manufacturers are adopting the use of web browser interfaces to provide O&M access to their systems. Careful attention should be made to the design of these systems to ensure the security of the interface. These interfaces should use the Secure Sockets Layer (SSL) to provide an encrypted connection.

A.3.2 Identification

Each operations related process running in the 3GPP node should be associated with the corresponding user-ID (so that an audit trail can be established if there is a need).

The 3GPP node should disable a user-ID if it has remained inactive (i.e., never used) over a specified time period.

A.3.3 Authentication

All Operations, Administration, Maintenance and Provisioning (OAM&P) input ports of the 3GPP node (including direct, dial-up and network access) should require authentication of a session requester, without any provision for a bypass mechanism.

A.3.3.1 Direct authentication of users

Communication nodes that perform their own authentication of access requests must provide at least a minimum set of features to ensure that operators can effectively operate the equipment in a secure manner.

A single stored password entry (e.g., in a password file) should not be allowed to be shared by multiple user-IDs. However, the 3GPP node should not prevent a user from choosing (unknowingly) a password that is already being used by some other user. Nor should the 3GPP node volunteer this information to either user.

Passwords should be stored in a one-way encrypted form, and should not be retrievable by any user including managers or administrators (of system and security). Also, there should be no clear text display (on a device such as a screen, typewriter, or printer) of a password at any time (e.g., login, file dump, etc.).

The 3GPP node should allow passwords to be user changeable (requiring re-authentication), and should require that the user change it the first time he/she establishes a session with the password assigned to him/her. The default should be non-trivial in nature, ideally random.

The password should have an “ageing” feature, and it should have a complexity requirement to make it not easily guessed. The 3GPP node should not accept common words or names as valid passwords. Also, it should not allow a recently obsolete password to be readily reselected by the said user.

Manufacturers should consider how the authentication system can be extended to allow for other systems of identification of the user, such as biometrics (fingerprint scanner, retina scan, voice print, etc) to be used.

A.3.3.2 Use of a remote Authentication Server

Manufacturers should consider the use of a Remote Authentication Server. The node then only has to implement the server client part of the authentication, all of the password management is removed from the node. The node will still have to have a username entry for every user so as to implement the access controls on the node.

This would simplify the implementation and allow a centralised access server that stores all authentication information. Extensions like adding authentication with Secure-ID would be supported without any extra changes. Auditing would be simplified. Add on products for log evaluation from third party vendors could also be used.

This approach greatly assists operators in the administration of user identities and passwords, especially in larger networks, which may consist of thousands of Network Elements or nodes, and hundreds of users who require access to them.

A.3.3.2.1 The RADUS authentication protocol

“Remote Authentication Dial in User Service” (RADIUS) Internet standards RFC 2138 and RFC 2139.

This is a very simple protocol and has been widely implemented. It is primarily aimed at authenticating users after dialling into a remote access device. The user is challenged for a username and password, this is then sent to the RADIUS server for verification and the result transmitted back to the requestor.

All of the passwords are transmitted across the network in plain text, and the equipment node does all of the interfacing with the user.

A.3.3.2.2 The KERBEROS authentication protocol

Kerberos was created at the Massachusetts Institute of Technology in the early 1980s. (Cerberus is the name of the three-headed dog that guards Hades, which makes it an apt name for a security service, MIT Project Athena chose to use the Greek spelling and pronunciation).

The current version, Kerberos version 5, has been published by the IETF (Internet Engineering Task Force) as RFC 1510.

This is a much more comprehensive protocol. It allows a user to enter their password once and then be validated automatically on each system or service they connect to. This would require more effort from the network operator to set up the Authentication Server and some extra effort on behalf of the manufacturer to "Kerberize" the application. All of the software for the Kerberos system is available under an Open Source licence.

A.3.4 System Access Control

The 3GPP node should not allow access to any session requester unless identified and authenticated. There should be no default mechanism to circumvent it.

The 3GPP node should not allow any session to be established via a port that is not authorised to accept input commands. For example, if an output port receives a login request, the 3GPP node should not respond.

The entire login procedure should be allowed to be completed without interruption, even if incorrect parameters (such as an incorrect user-ID or an incorrect password) are entered, and no "help message" should be transmitted to the session requester as to which part of the authentication is incorrect. The only information to be conveyed at the end of the login attempt is that the login is invalid.

After a specified number of incorrect login attempts carried out in succession, the 3GPP node should lock out the channel and raise an alarm in real time for the administrator.

Before the session begins, the 3GPP node should provide a warning message explicitly alerting the user of the consequences of unauthorised access and use.

At the beginning of the session, the 3GPP node should display the date and time of the user's last successful access and the number of unsuccessful attempts, if any, that have been made to establish a session since the last successful access.

There should be a "time-out" feature - i.e., the 3GPP node should disconnect or re-authenticated users after a specified time interval during which no messages were exchanged. Also, there should be a mechanism for user-initiated keyboard locking.

The 3GPP node should provide a mechanism to end a session through a secure logoff procedure. If a session gets interrupted due to reasons such as time-out, power failure, link disconnection, etc., the port should be dropped immediately.

For dial-up access over untrusted channels, authentication involving one time passwords should be required (e.g., smart card, etc.).

A.3.5 Resource Access Control

Access to resources should be controlled on the basis of "privilege" (i.e., access permission) associated with user-ID and channel. It should not be based on a "password" associated with the access function, because that password will have to be necessarily shared among all users requiring such access. Neither should encryption be used as a primary access control mechanism (though encryption may be used to enhance it).

The granularity of resource access control should be such that for each resource it should be possible to grant (or deny) access privilege to any single user (or a prescribed group of users). For example, the control should be adequately fine-grained so that user access and channel access can be restricted on the basis of commands, database views (i.e., objects), records (i.e., object instances), and fields (i.e., attributes).

If external entities - e.g., customers, are allowed access to the resources, each 3GPP node's resource (e.g., proprietary data) should be protected from access by unauthorised persons.

Executable/loadable/fetchable software should be access controlled for overwrite, update, and execution rights.

A.3.6 Accountability and Audit

The 3GPP node should generate a security log containing information sufficient for after-the-fact investigation of loss or impropriety.

The security log should be protected from unauthorised access. No user should be allowed to modify or delete a security log. There should be no mechanism to disable the security log. There should be an alarm in real time if the security log does not function properly.

The security log should, as a minimum, record events such as:

- all sessions established;
- invalid user authentication attempts;
- unauthorised attempts to access resources (including data and transactions);
- changes in users' security profiles and attributes;
- changes in access rights to resources;
- changes in the 3GPP node security configuration;
- And modification of 3GPP node software.

For each such event, the record should, as a minimum, include date and time of event, initiator of the event such as: user-ID, terminal, port, network address, etc., names of resources accessed, and success or failure of the event.

Actual or attempted passwords should not be recorded in the security log.

There should be audit tools to produce exception reports, summary reports, and detailed reports on specifiable data items, users, or communication facilities.

A.3.7 Security Administration

The 3GPP node should support functions for the "management" of security related data (e.g., security parameters such as user-IDs, passwords, privileges, etc.) as "separate" from other user functions. Security administration should be reserved only for an appropriate administrator.

The administrator should be able to display all currently logged-in users as well as a list of all authorised user-IDs.

The administrator should be able to independently and selectively monitor, in real time, the actions of any one or more users based on respective user-IDs, terminals, ports, or network addresses.

The administrator should be able to identify all resources owned by or accessible to any specific user along with the associated access privileges.

The administrator should be able to enter, edit, delete or retrieve all attributes of a user-ID (except for a password, which should not be retrievable).

The administrator should limit the use of a "null password" during system login on a per user or per port basis (i.e. during new release installation).

The administrator should be able to save the security log for safe storage, so that it is not written over when the buffer is full.

All security parameters (e.g., password-ageing interval, time-out interval, and various alarm conditions) should be specifiable and adjustable by the administrator. This implies that the 3GPP node should not have any security parameters hard coded.

A.3.8 Documentation

Any 3GPP node supplier/vendor should provide documentation on security considerations for administrators, operators, and users. They can be stand-alone documents or sections incorporated in appropriate vendor manuals.

- The administrator's guide should contain items such as:
- functions and privileges that need to be controlled to secure the facility;
- proper usage of security audit tools, procedures for examining and maintaining audit files, procedures for periodic saving and backup of security logs;
- recommendations on setting the minimum access permissions on all files;
- directories, and databases;
- guidelines on security assessment techniques.

The operator's guide should contain procedures necessary to initially start the 3GPP node in a secure manner and to resume secure operation after any lapse that may have occurred.

The user's guide should describe the protection mechanisms that are non-transparent to the user, should explain their purpose, and provide guidelines on their use. It should not contain any information that could jeopardise the security of the 3GPP node if made public.

Passwords should be stored in a one-way encrypted form, and should not be retrievable by any user including managers or administrators (of system and security). Also, there should be no clear text display (on a device such as a screen, typewriter, or printer) of a password at any time (e.g., login, file dump, etc.).

The 3GPP node should allow passwords to be user changeable (requiring reauthentication), and should require that the user change it the first time he/she establishes a session with the password assigned to him/her. The default should be non-trivial in nature, ideally random.

Annex B:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
10-1999	-	-	-	-	Publication as first draft to 3GPP TSG SA WG3 Security	-	0.0
11-1999	-	-	-	-	Presented at SA3#06 for information	0.0	1.0
01-2000	-	-	-	-	Presented at SA3#10 for comment	1.0	2.0
02-2000	-	-	-	-	Editing meeting at DTI 16/02/2000. For presentation at SA3#11	2.0	3.0
07-2001	-	-	-	-	Updated to include comments received: - S3-000571 DoS attacks - S3-000228 Authentication and Network Security	3.0	4.0
10-2001	-	-	-	-	Formatted into 3GPP style by MCC (Auto section numbering removed, sections re-numbered). NOTE: Updated versions in this table from 1.x.0 to x.0 as not yet at version 1.x.y. (MCC)	4.0	0.4.1