

A Taxonomy of Cyber Attacks on 3G Networks

Kameswari Kotapati, Peng Liu, Yan Sun, Thomas F. LaPorta
kotapati@cse.psu.edu, pliu@ist.psu.edu, yasun@cse.psu.edu, tlp@cse.psu.edu
The Pennsylvania State University, University Park, PA 16802 USA

Abstract

Cross Network Services are a new breed of services that have spawned from the merger of the Internet and the previously isolated wireless telecommunication network. These services act as a launching pad for a new type of security threat - the Cross Infrastructure Cyber Attack. This paper is the first to propose attack taxonomy for 3G networks. The uniqueness of this taxonomy is the inclusion of Cross Infrastructure Cyber Attacks in addition to the standard Single Infrastructure attacks. This paper also proposes an abstract model of the 3G network entities. This abstract model has been a vehicle in the development of the attack taxonomy, detection of vulnerable points in the network and validating 3G network vulnerability assessment tools. This paper examines the threats and vulnerabilities in a 3G network with special examination of the security threats and vulnerabilities introduced by the merger of the 3G and the Internet. The abstract model aids this comprehensive study of security threats and vulnerabilities on 3G networks.

1. Introduction

Early first and second generation (1G & 2G, respectively) wireless telecommunication networks were controlled by exchanging signaling messages on closed SS7 based networks. These networks were isolated because they did not provide connectivity to any public networks to which end subscribers had direct access. The vulnerabilities of these networks were few and well assessed. The vision of the next generation 3G wireless telecommunication network is to use IP technologies. 3G networks will provide IP connectivity to its subscribers with the help of its IP Multimedia Subsystem. The IP Multimedia Subsystem will use IP to transport information, and Session Initiation Protocol (SIP) and Mobile IP for session control and mobility management.

The introduction of IP technologies into traditional wireless telecommunication networks has opened up a new generation of IP-based services that must interwork with the 3G wireless telecommunication networks. These services are called *Cross Network Services*. *Cross Network Services* will use a combination of Internet-based data and data from the wireless telecommunication network to provide services to the wireless subscriber. They will be multi-vendor, multi-domain, and will cater to a wide variety of needs.

A security risk is introduced by providing Internet connectivity to 3G networks in that certain attacks can be easily enforced on the wireless telecommunication network indirectly from the IP networks. These *Cross Infrastructure Cyber Attacks* are simple to execute and yet have serious effects.

The threats and vulnerabilities introduced by merging these networks have not been studied or assessed. In this paper we present a unique attack taxonomy, in which we consider the *Cross Infrastructure Cyber* attacks in addition to the standard *Single Infrastructure* attacks, some of which have already been studied. To develop the attack taxonomy we derived an abstract model of the 3G network infrastructure. Other applications of this abstract model include detection of vulnerable points in the network and validation of 3G vulnerability assessment tools. In this paper the *abstract model* is used to study the *Cross Infrastructure Cyber Attacks* and illustrate the taxonomy.

Existing literature identifies security threats, security scenarios, security problems and security requirements of the standalone wireless telecommunication network. There is no available literature on *Cross Infrastructure Cyber* attacks and attack taxonomy. This paper expects to bridge the gap. Section 2 gives an overview of the 3G network, background and literature survey. Section 3 explains the abstract model and Section 4 explains how these attacks are enabled. Section 5 explains the taxonomy of attacks and Section 6 concludes. In the body of this paper we focus on the interaction of circuit-based 3G wireless networks and IP-based services. In Appendix B we discuss pure all-IP based networks.

2. Background

3G networks are designed to provide multimedia capabilities and high speed *packet data service*. The architecture of the 3G Network is illustrated in Figure 2.1. The core 3G network may be accessed through a *Radio Access network* (also called the Air Interface) with 3G-enabled technology such as CDMA 2000 and WCDMA. The Core 3G network is connected to the Internet and the PSTN (Public Switched Telephone Network). Internet connectivity enables 3G users to receive data services, such as weather reports, stock reports, sports information, chat, electronic mail; *Cross Network Services* such as Call Forwarding Services, Client Billing Service and Location Based Instant Messaging; Location Based Services such as navigation, restaurant information, etc. In 2G systems network access is provided either to the PSTN or the Internet, so *Cross Network Services* are unavailable.

The core 3G network is further divided into the *Circuit Switched (CS)* domain, the *Packet Switched (PS)* domain and the *IP Multimedia Subsystem (IMS)* based on the functional viewpoint. Deployment of the IP Multimedia Subsystem requires the deployment of the PS domain [2].

The *Circuit Switched* domain comprises of a set of all core network entities offering circuit switched type of connections for user traffic and related signaling. The CS Domain is used to access the PSTN. The CS domain entities are described in Section 2.1.

The *Packet Switched* domain comprises of a set of all core network entities offering packet switched type of connection for user traffic and related signaling. The PS domain is used to access the Internet. The CS and PS domain may have some entities in common [3].

The *IP Multimedia Subsystem* comprises of a set of all core network entities for provision of multimedia services. The IMS enables the mobile network operators to offer their subscriber's multimedia services based on and built upon Internet applications, services and protocols. The IMS entities are described in Appendix B.1. The SIP (Session Initiation Protocol) protocol may be used for multimedia session control in the IMS [2]. The IMS is the ultimate goal to provide IP Services to its subscribers.

In this paper we describe access of IP based services to wireless telecommunication subscribers through interaction with the CS domain of the 3G network. This interaction will provide a migration path for CS networks to IMS and it will likely be used for several decades as CS networks remain in existence. It is the combination of IP services and CS networks that enables the *Cross Network Services* and *Cross Infrastructure Cyber Attacks*. Readers interested in IP based services interacting with the IP Multimedia subsystem may read Appendix B.

In the next two subsections we will discuss 3G network entities, Cross Network Services and Cross Infrastructure Cyber attacks.

2.1 Core 3G Network

Subscribers may be affiliated with two networks in a 3G system: a *home network* and a *serving network*. Every subscriber is permanently assigned to the *home network*. The responsibilities of the home network include provision of services to the subscriber, management and maintenance of subscriber profiles, billing and authenticating the subscriber to receive service. The serving network changes as the user location changes. It provides radio resources, mobility management, routing and handling services for the subscribers. The Serving Network capabilities are provided to the subscribers on behalf of the home environment, with which the serving network has an appropriate agreement [13]. There are four main entities in the CS domain and are described below.

All subscribers are permanently assigned to a fixed Home Location Register (HLR). The HLR is said to be in the home network. The HLR stores permanent subscriber profile data and relevant temporary data such as current subscriber location (pointer to VLR) [5].

Visitor Location Register's (VLR) are assigned to a specific administrative area and associated with one or more MSC's. The VLR acts as a temporary repository and stores data of all mobile stations (user handset) that are currently roaming in its assigned area. The VLR obtains this data from the HLR assigned to the mobile station [5].

The Mobile Switching Center (MSC) acts as an interface between the radio system and the fixed network. It is assigned to a fixed administrative area. It performs all necessary functions in order to handle the circuit switched services to and from the mobile stations roaming into its area. The MSC is in-charge of functions related to registration, mobility management, paging, handover etc. The VLR and MSC could be either in the home network, if the subscriber is located in the home network, or the serving network if the subscriber roams into another location area [5].

If a network delivering a call to the mobile network cannot interrogate the HLR, the call is routed to an MSC. This MSC will interrogate the appropriate HLR and then route the call to the MSC where the mobile station is located. The MSC in charge of routing the call to the actual location of the mobile station is called the Gateway MSC (GMSC). The GMSC's are available to pass voice traffic between the PSTN network and the 3G network [5]. For description of the IMS entities refer to Appendix B.1.

For the 3G networks to provide service to the subscriber some of the above-mentioned entities must perform certain functions. These functions may be triggered by the arrival of signaling messages. Hence it can be said that the 3G network provides the subscriber service through the exchange of *signaling messages* among its entities. Signal 1 in Fig 4.1 is an example of a signaling message. Some of the 3G entities have data stores associated with them. These data stores maintain the data used by the 3G entities. The entity manages the data store by sending database queries to the data store. Database queries 2a, 2b in Fig 4.1 are examples of a database queries.

2.2 Cross Network Services and Attacks

We define *Cross Network Service* as a new generation of IP-based services that must interwork with the 3G wireless telecommunication networks. *Cross Network Services* will use data from the IP network and data from the wireless telecommunication network to provide services to the wireless subscriber. We describe three examples of Cross Network Services below.

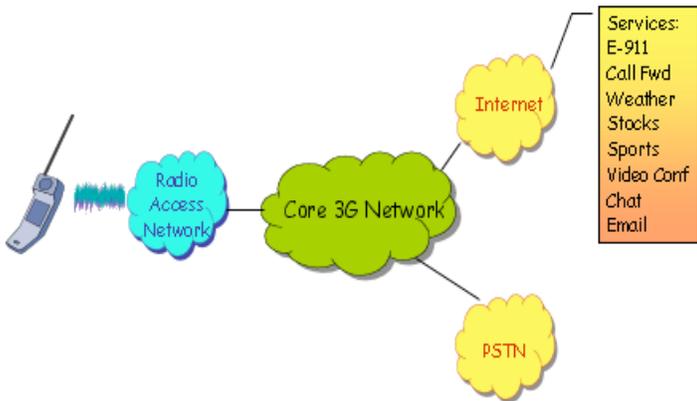


Figure 2.1: Architecture of a 3G network

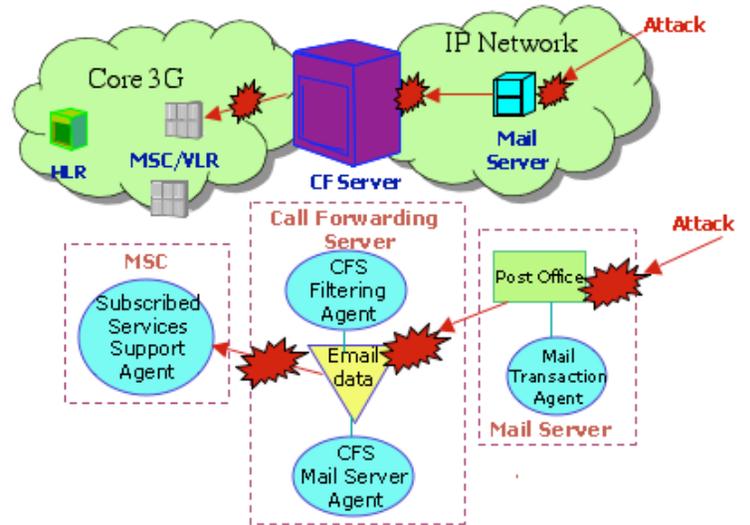


Figure 2.2: Attack Propagation in CFS with simplified abstract model

In the Email Based Call Forwarding Service (CFS) the status of the subscriber's email inbox is used to trigger call forwarding in the wireless telecommunication network. E.g. calls from a certain peer group that have emails pending in the called party's inbox for longer than a certain period of time are delivered to voice mail; calls from a second peer group are immediately delivered to the cell phone. Call delivery is via the 3G network.

In the Client Billing Service (CBS) the caller id of an incoming call is used to trigger a client billing system, which will forward the call and bill the client appropriately. Lawyers or Agents in an Insurance Agency may use such a Client Billing Service to bill clients for the telephone advice or services offered.

In the Location Based Instant Messaging System (LB-IM), a location track request from a buddy triggers the core 3G network to locate the subscriber. This location is revealed only if the buddy belongs in a location visibility group and a time visibility group. After the location is known the requestor can begin instant messaging. An example of the *Location Visibility Group* is that a supervisor may locate colleagues at work. An example of the *Time Visibility Group* is that colleagues and supervisors at a work place can view location between 9 am and 5 pm on weekdays.

Single Infrastructure Attacks are attacks on a domain from the same network domain, e.g., the attacker has gained access into a core 3G network entity and attacks other 3G network entities.

Cross Infrastructure Cyber Attacks may be defined as attacks on the wireless telecommunication network from the IP domain. These attacks use *Cross Network Services* as an entry point into the wireless telecommunication network. We will now illustrate such an attack with the help of the abstract model and a simplified version of the Email Based Call Forwarding Service. In the following discussion, we refer to the abstract model detailed in Section 3.

The simplified version of the CFS works by forwarding a call to the voice mail if there is no email from the caller; otherwise the call is forwarded to the subscriber's cellular phone. Every one-hour the *CFS Mail Server Agent* in the CF Server will fetch emails stored in the *Post Office* data source of the Mail Server. This data is stored in *Email data* cache of the CFS. When there is an incoming call for the CF subscriber, the *Subscribed Services Support Agent* in the MSC will query the CF Server on how to forward the call. The *CFS Filtering Agent* will check its *Email data* cache, and if there is an email from the caller, the call is forwarded to the subscriber's cellular phone.

The propagation of the attack from the Mail Server to the CF Server and finally the 3G network entity is illustrated in Fig 2.2. Using any standard Mail Server vulnerabilities the attacker may compromise the Mail Server and corrupt the *Post Office* data source by deleting emails from certain people from whom the victim is expecting calls. The *CFS Mail Server Agent* queries the *Mail Transaction Agent* for emails from *Post Office* data source and the *Mail Transaction Agent* will pass on the corrupted email data to the *CFS Mail Server Agent*. The *CFS Mail Server Agent* will cache the email data in its *Email data* cache. The *Email data* cache will be corrupted and the effect of the attack on the Mail Server has propagated to the CF Server. When the *Subscribed Services Support Agent* in the MSC entity of the 3G network sends out a 'how to forward the call' query to the CF Server, the CF Server will check its corrupt *Email data* cache and find that there are no emails from the caller. The CF Server will reply to the *Subscribed Services Support Agent* to forward the call to the voice mail when in reality the call should be forwarded to the cellular phone. Thus the effect of the attack on the Mail Server has propagated to the 3G network. This is a classic example of a Dimension: I-Level V Cross Infrastructure Cyber Attack, where the attacker gains access to the *Cross Network Server* and attacks by modifying data in the data source of the *Cross Network Server*. Detailed information of the various Dimensions and Levels may be found in Section 5.

2.3 Literature Survey

Telecommunication standards [13,14,15] specify 3G security and identify certain security threats. They including eavesdropping, masquerading, traffic analysis, browsing, compromising authentication vectors, manipulation of messages, disturbing or misusing network services, denial of service, resource exhaustion, misuse of privileges and abuse of services. Such papers [11,12,17,19,25] have identified single infrastructure threats or attack scenarios on 3G networks while trying to prove the inadequacy of current security schemes or presenting a new architecture or guidelines for 3G security. The attack scenarios identified in these papers include masquerade, unauthorized notification of resources, line-tap attacks, eavesdropping, man in the middle, guessing attack, replay attacks, interleaving attack and they have been included in our taxonomy.

Threats, vulnerabilities and attack scenarios on the SS7 domain are identified in [9,10,24]. An attack taxonomy for SS7 network entities is defined in [9]. The classification in [9] groups attacks based on the SS7 entity (Service Switching Points, Signal Transfer Point and Service Control Point) under attack. The need for security is motivated in [21]. The security features available in current 3G networks are discussed in [22,23,26]. In conclusion of this survey, we find that attacks on the SS7 networks are well studied and documented with an attack taxonomy. Some attacks on the core 3G networks are well studied but there is no existing attack taxonomy. We define an attack taxonomy to fill this void. The uniqueness of this taxonomy is the inclusion of *Cross Infrastructure Cyber Attacks*.

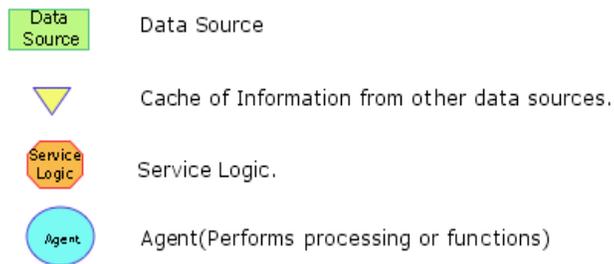


Fig 3.1: Elements used in the abstract model

3. Abstract Model

We have defined an abstract model to better understand and classify the attacks that may be possible on the 3G network. The abstract model has been constructed for relevant 3G network entities. Every network entity performs a number of sophisticated functions that have been divided into a number of basic, simple atomic functions. Each network entity has been divided into atomic functional units called Agents. Each of these basic, simple atomic functions is assigned to an Agent. Network entities manage some data. This data may be permanent or temporarily cached from another network entity. Every network entity also has Service Logic. The Service Logic coordinates interactions between the different Agents and data inside the network entities. Fig 3.1 shows the schematic representation of abstract model elements.

Fig 3.2 shows the abstract model of the entities in the CS domain. Table 3.1 describes the agents used in CS Domain abstract model. Fig 3.3 shows the abstract model of the CF Service; it includes the CF Server and the Mail Server. Table 3.2 describes the agents used in the Mail Server. Table 3.3 describes the agents used in the CF Server. Fig 3.4 shows the abstract model of the LB-IM Service. Table 3.4 describes agents in LB-IM Server. Fig 3.5 shows abstract model of the CBS Service. Table 3.5 describes agents in CBS Server.

With the help of the abstract model, it is straightforward to pinpoint security threats, vulnerabilities and attacks at specific points in 3G infrastructures. For example, if outgoing links from the HLR are compromised and if the caller id in the signaling message 8 of Figure 4.1 is changed, then calls to a subscriber may not be routed to the appropriate CF Server. If the caller is an important person, he may be very unhappy to get the voice mail and the victim subscriber may suffer financial losses as a result of not receiving the call.

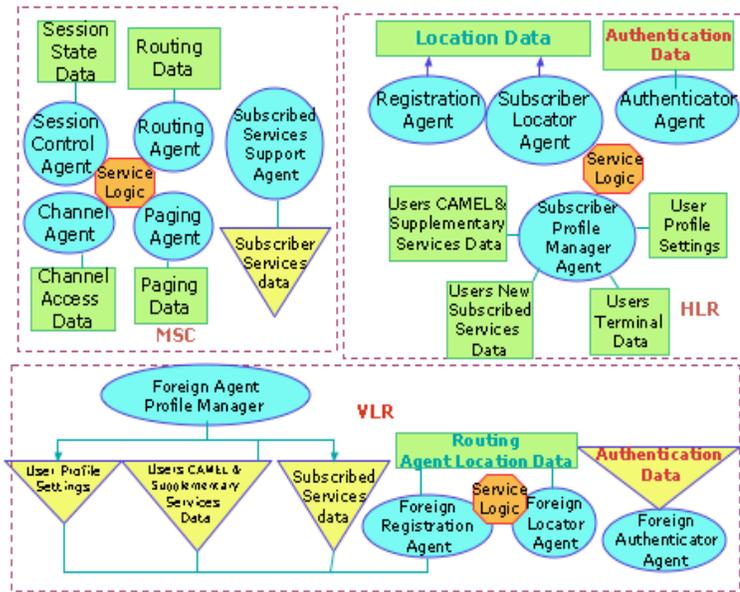


Fig 3.2: Abstract Model of Entities in the CS Domain

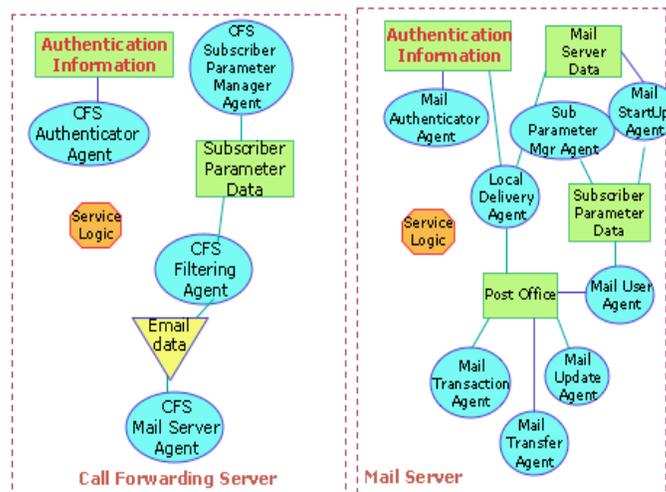


Fig 3.3: Abstract Model of the CF Service

Entity	Name of Agent	Description
MSC	Session Control	Manages calls, sessions or handles sessions, calls on behalf of the user. Maintains Session State.
	Routing	Provides Routing Information (Routing Numbers) to route the call up to the user (MSC).
	Channel	Establishes contact between the mobile station and the network
	Paging	Maintains Paging Lists and Pages the Base Stations to locate the user.
VLR	Foreign Agent Profile Manager	Has access to subscriber's profile, services data source in order to support CAMEL, supplementary and new subscribed services such as call forwarding, location based IM, etc.
	Foreign Locator	Maintains Information on all mobile stations visiting its location area. It is the point of contact for the subscriber locator Agent.
	Foreign Registration	Handles Registration Messages from all mobile stations visiting its location area. This agent will invoke the Foreign Authenticator Agent, which will authenticate the subscriber using AKA.
	Foreign Authenticator	Fetches the required keys from the Home Registration Agent and will authenticate the subscriber using AKA. It maintains the all of the Keys in the Authentication Data cache.
HLR	Registration	Manages downloading authentication, profile and subscribed service data into its new visitor data source and cancels the subscriber information in its old visitor data source when a user enters a new location area.
	Authenticator	Retrieves keys from the authentication data source and generates authentication material for all users subscribing to its network.
	Subscriber Locator	Tracks the location of all the users to which it is assigned. It stores the subscriber's location Information in location data.
	Subscriber Profile Manager	Manages Subscriber Profile (Access Policy, Roaming Agreements), Terminal Data, CAMEL & Supplementary Services and New Subscribed Services.

Table 3.1 Entities in CS Domain

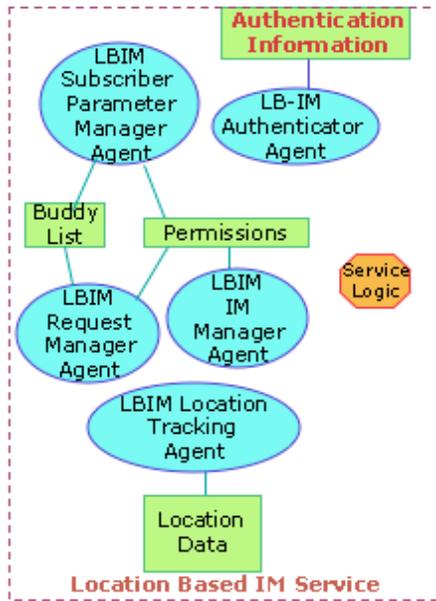


Fig 3.4: Abstract Model of the LB-IM Service

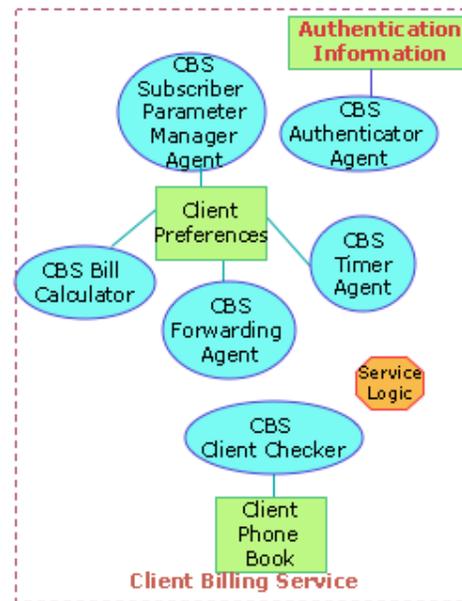


Fig 3.5: Abstract Model of the CBS Service

Name of Agent	Description
Subscriber Parameter Manager Agent	Manages all of the parameters set by the subscriber.
Mail Starting	Retrieves Subscribers Parameter Settings & Mail Server Data and Invoke Mail Transfer Agent when a subscriber starts the Mail Service.
Local Delivery	Takes care of mail that is to be delivered to a local user
Mail Transaction Agent	Allow queries to the incoming mail storage (Post Office) and retrieves the result
Mail User Agent	Allows the user to compose and read e-mail messages. This agent acts as an interface between the user and the Mail Transfer Agent.
Mail Update Agent	Manages the state of the incoming mail storage in the Post Office.
Mail Transfer Agent	Transfers e-mail messages from one computer to another. This agent is responsible for delivering outgoing mail and receiving incoming mail.
Authenticator	Responsible for authenticating subscribers wanting to access the Mail Server and all other servers that contact the Mail Server with a request .

Table 3.2 Entities in Mail Server

Name of Agent	Description
Subscriber Parameter Manager Agent	Manages all of the parameters set by the subscriber
Filtering	Filters data retrieved by the Mail Server Agent/ Phone Book Agent based on parameters set by a subscriber and instructs the Mail Server Agent/ Phone Book Agent to retrieve more information.
Mail Server Agent	Interfaces Mail Server with Call Forwarding Server. It will query Mail Server based on subscriber parameters and retrieve information
Authenticator	Maintains Subscriber Authentication Data and will know the address of the 3 rd party used to authenticate the subscriber.

Table 3.3 Entities in CF Server

Name of Agent	Description
Subscriber Parameter Manager Agent	Manages all of the parameters set by the subscriber.
Request Manager Agent	Receives Requests to view subscriber location and services them.
IM Manager Agent	In charge of sending out location track requests to members on the buddy list
Location Tracking Agent	Responsible for tracking the location of the user by querying the 3G network and it maintains current location data of the subscriber
Authenticator	Responsible for authenticating subscribers /networks wanting to access the LB-IM Server and all other servers that contact the LB-IM with a request.

Table 3.4 Entities in LB-IM Server

Name of Agent	Description
Subscriber Parameter Manager Agent	Manages all of the parameters set by the subscriber
Time Agent	Times the call and saves in as a part of the clients account
Forwarding	Forward the call to the appropriate party
Bill Calculator	Calculates the bill, based on Time logged and other constraints
Mail Server Agent	Interfaces Mail Server with Call Forwarding Server. It will query Mail Server based on subscriber parameters and retrieve information
Authenticator	Maintains Subscriber Authentication Data and will know the address of the 3 rd party used to authenticate the subscriber.

Table 3.5 Entities in CBS Server

For the abstract model of the IMS, refer to Appendix B.2. Appendix B.2 also has Table B.1 with a description of the IMS entities.

4. Attack Overview

4.1 What makes attacks possible on the 3G Network?

Early 1G and 2G wireless telecommunication networks and the PSTN networks were closed as signaling messages were exchanged on private isolated SS7 based networks. These isolated networks were not connected to any public networks and hence malicious hackers could not gain easy access into the wireless telecommunication network. The attacks that were possible on these isolated networks were well studied and have been considered in our taxonomy. An example of what makes these attacks possible is the easy availability of standard inexpensive “off-the-shelf” mobile radio test equipment. This equipment could be used to impersonate parts of the network. Other threats are disgruntled employees and terrorists who can gain access into central offices and into 3G core network entities.

With the integration of the core 3G networks, the PSTN and the Internet, the networks have opened up additional vulnerabilities and provided malicious attackers easy access through the *Cross Network Servers*. The Internet is open and accessible to one and all with simple equipment. It is also very easy for malicious attackers to break into Internet servers due to many vulnerabilities [27]. Breaking into an Internet server providing *Cross Network Service* opens up possibilities for the attacker to invade the 3G core and PSTN networks. The *Cross Infrastructure Cyber Attack* is easy to execute and may be serious enough to cause the breakdown of the telecommunication network. Some examples of *Cross Network Services* that act as a launching pad for the Cross Infrastructure Cyber Attacks are the Call Forwarding Service (CFS), the Location Based-Instant Messaging (LB-IM) and the Client Billing Services (CBS). In the following discussion, we refer to the agents at data sources summarized in Tables 3.1-3.5.

The CFS and CBS Services are triggered when a signaling message arrives at the *Subscriber Locator Agent (HLR)* assigned to the subscriber. The *Subscriber Locator Agent* will send a database query to its *User Terminal* data source and find the terminals registered for the user, and will subsequently query the *Location Data Source* and find the *Foreign Location Agent (VLR)* where the subscriber is registered. The *Foreign Locator Agent* will invoke the *Routing Agent (MSC)* to provide a *routing number* to route the call to the *Session Control Agent (MSC)* where the subscriber is currently roaming. The *routing number* is returned to the *Subscriber Locator Agent (HLR)*. The call is routed to the *Session Control Agent (MSC)*. The *Session Control Agent (MSC)* will invoke the *Subscriber Services Support Manager (MSC)* to check if there

CBS Bill Calculator will calculate the billing amount. Fig 4.4 shows the signaling flows for the above process. In the CBS Cross Network Service, the Cross Infrastructure Cyber Attacks can occur at the CB Server.

The LB-IM is triggered when a location track request arrives at the LB-IM Request Manager. The LB-IM Request Manager will check if the requestor belongs in the location and time visibility group by checking the Permissions data store. If the requestor satisfies the constraints, the LB-IM Location Tracking Agent fetches the location of the subscriber by querying the 3G network entities.

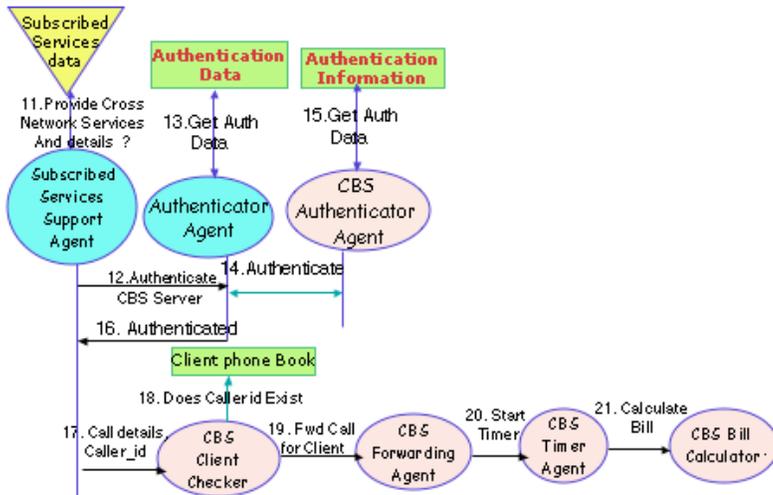


Fig 4.4: Signal Flows: Provide CBS for Incoming Call

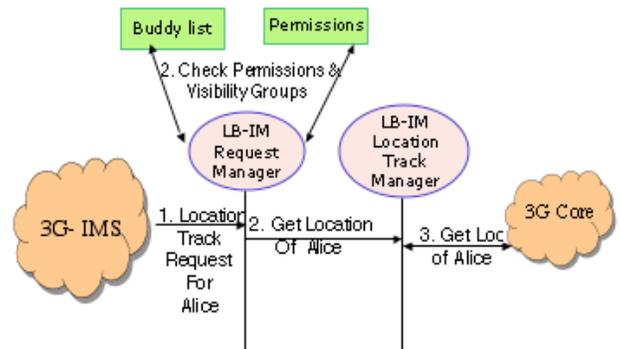


Fig 4.5: Signal Flows: Handling LB-IM request

4.2 How do attacks on 3G networks occur?

Attacks may occur from various points in the network. Broadly attacks may be divided into *Single Infrastructure* and *Cross Infrastructure Cyber Attacks*.

Most *Single Infrastructure Attacks* will be launched from the air interface of the 3G networks. These may be originated using standard inexpensive “off-the-shelf” mobile radio test equipment to impersonate parts of the network [11]. The intruder can analyze traffic, eavesdrop, intercept signaling messages, modify signaling messages and jam the radio interface.

If an attacker breaks into a 3G core network entity itself, the attacker can insert, modify and destroy data sources so that malicious subscribers may commit subscription fraud, collect confidential information from other entities and modify service logic to disrupt the network operation, thereby denying service. However, it is very difficult to break into a core 3G network entity.

Breaking into an Internet Server providing a *Cross Network Service* opens up possibilities for the attacker to execute *Cross Infrastructure Cyber Attacks*. We will now consider how attacks can happen using the above *Cross Network Services* examples.

With CFS attacks can occur at the Mail Server or CF Server. Attacks at the Mail Server enabled, using vulnerabilities at the *Mail Transfer Agent* such as a badly configured sendmail daemon. The attacker can send emails with a fake source id to the victim; the CF Server will assume that it is checking the correct constraints, but in reality the victim may receive unwanted calls and have important calls sent to voice mail.

Other attacks may be launched if the attacker gains privileges to modify the service logic. Modification of time and other settings in the service logic would result in the *Mail Transaction Agent* replying to queries from *CFS Mail Server Agent* with zero emails, when in reality there may be a number of emails.

Attacks at the CF server include, sending spoofed messages to the *CFS Subscriber Parameter Manager Agent* requesting a change in parameters, or by gaining privileges to modify the email cache and subscriber preferences and causing a denial of service by flooding the *CFS Authentication Agent*.

With the CBS, attacks can occur at the CB Server. Attacks include a denial of service on the *CBS Authentication Agent*, or obtaining privileges to modify the *Timer Agents*, *Bill Calculator Agents* and *Forwarding Agents*. Such attacks may result in the victims receiving large bills and unable to receive service on time.

With the LB-IM service, spoofed messages may be sent to the *LB-IM Subscriber Parameter Manager Agent* requesting a change in permissions resulting in invasion of the victim’s privacy and disturbance from unwanted parties.

5. Attack Taxonomy

In the following subsections we present a formal taxonomy of attacks on 3G Networks.

5.1 Taxonomy of Attacks on 3G Networks

In order to devise a taxonomy of attacks on the 3G Network, we consider the attacker's physical access to the network, the type of attack categories and the means used to cause the attack. We classify the attacks into three dimensions: Dimension I: Physical Access to the Network, Dimension II: Attack Categories and Dimension III: Attack Means.

5.1 Dimension I: Physical Access to the Network

In this dimension, attacks are classified based on the level of physical access the attacker has to the 3G wireless telecommunication network. Dimension I may be further classified as Single Infrastructure Attack (Level I-III) and Cross Infrastructure Cyber Attack (Level IV-V):

Level I: Access to air interface with physical device: The attacker has access to standard inexpensive "off-the-shelf" equipment that could be used to impersonate parts of the network [11]. The attacker may put up a false base station. Victims camping on the false base station are subject to false base station attacks. Attackers may also use modified mobile stations to broadcast at a high frequency, eavesdrop and cause a man in the middle attack.

Level II: Access to Cables connecting Central Offices (3G core network entities): The central offices house the 3G core network entities. Typically authorized personnel only may access these central offices. If the attacker has access to cables connecting these central offices. They may cause damage by disrupting normal transmission of signaling messages.

Level III: Access to 3G core network entities in the Central Office: In this case the attacker may be a disgruntled employee or a terrorist who has managed to gain access into the central office. Here the attacker can cause damage by editing the service logic or modifying subscriber data (profile, security and services) stored in the network entity.

Level IV: Access to Links connecting the Internet and the 3G core network: This is a *Cross Infrastructure Cyber Attack*. The attacker has access to links connecting the 3G-core network and the Internet based *Cross Network Services*. In this case the attacker can cause damage by disrupting normal transmission of signaling messages traversing the link and inserting signaling messages into the link between the two networks. *Level IV* may be sub divided based on the interworking approaches used to connect the 3G core network and the Internet. Appendix A details the various interworking approaches and attacks.

Level V: Access to Internet Servers or Cross Network Servers (provides multimedia or other services to mobile subscribers) connected to the 3G networks: This is a *Cross Infrastructure Cyber Attack*. In this case the attacker can cause damage by editing the service logic, modifying subscriber data (profile, security and services) stored in the *Cross Network Servers*. This level of attack is easier to achieve *Level II* and *Level III*.

5.1.1 Dimension II: Attack Categories

In this dimension, attacks are classified based on type of attack. The attack categories are based on [30].

Interception: The attacker intercepts information e.g., reads signaling messages on a cable (Level II), but does not modify or delete them. This is a passive attack. This affects the privacy of the subscriber and the network operator. The attacker may use the data obtained from *interception* to analyze traffic and eliminate the competition provided by the network operator.

Fabrication/Replay: In this case the attacker may insert spurious objects into the system. These objects depend on the level of the attackers physical access to the system. E.g.: In a Level II, the attacker may insert fake signaling messages, in a Level III, the attacker may insert fake service logic or fake subscriber data into this system. The effects could result in the attacker masquerading as an authority figure.

Modification of Resources: The attacker causes damage by modifying system resources. E.g.: In a Level II, the attacker may modify signaling messages in and out of the cable. In a Level III, the attacker may modify service logic or modify subscriber data in the entity.

Denial Of Service: The attacker causes an overload or a disruption in the system such that network functions in an abnormal manner. The abnormal behavior could be legitimate subscribers not receiving service, illegitimate subscribers receiving service or the entire network may be disabled as a result of the attack.

Interruption: The attacker caused an Interruption by destroying resources. E.g.: In a Level II, the attacker may delete signaling messages in and out of the cable. In a Level III, the attacker may delete a subscriber data in the entity such as an HLR and the attacker may not receive service.

5.1.2 Dimension III: Attack Means

In this dimension, attacks are classified based on what means are used to cause the attack. The attack means are as follows.

Data: The attacker attacks the data stored in the system. Damage is inflicted by modifying, inserting and deleting the data stored in the system.

Messages: The attacker attacks the system through the signaling messages. The attacker may insert, modify, delete and replay signaling messages going in and out of the network.

Service Logic: The attacker inflicts damage by attacking the service logic running in the various 3G core network entities. E.g.: Interruption attack on service logic would be to completely delete the logic running on an entity such as the MSC.

5.2 Attacks

In this section we will use the classification detailed in Section 5.1 to group attacks. The attacks are tabulated as *CASE 1: Dimension I-Physical Access Vs Dimension II-Attack Categories* and *CASE 2: Dimension II-Attack Categories Vs Dimension III-Attack Means*. Note that the *Dimension I vs. Dimension III CASE* can be transitively inferred from *CASE 1 and CASE 2*.

We tabulate a list of possible attacks on the CS Domain. Table 5.1 shows the *CASE 1* tabulation of possible *Single Infrastructure attacks* on the CS domain. Table 5.2 shows the *CASE I* tabulation of possible *Cross Infrastructure Cyber attacks*. Table 5.3 shows attacks classified by *CASE II*. Interested readers may view Appendix B.4 for attacks on the IP Multimedia Subsystem.

A *Cross Infrastructure Cyber Attack* can be comprised of a single stage or multiple stages. In a multistage *Cross Infrastructure Cyber Attack* each stage can belong to different *attack categories* (Dimension II) and can use different *attack means* (Dimension II). Cross Network Servers offer services in multiple phases. Each service phase may be subject to a *Cross Infrastructure Cyber Attack* stage. The effects caused by an attack on a single phase of this service can have direct or indirect effects on the next service phase and can result in a multi stage attack. A number of these single stage attacks when executed in sequence can form a multi stage *Cross Infrastructure Cyber Attack*. We now present some examples of single stage *Cross Infrastructure Cyber Attacks* outlined in Table 5.2.

Call forwarding Service (CFS): Level IV attacks on the CF Service may be enumerated as follows. In **Interception attacks**, the attacker may view caller-id's of calls to a victim and sell this information. The attacker may also view the call forward number and track the whereabouts of the victim. The attacker may view the authentication messages and use it for a replay attack later on. The attacker may also view emails fetched by the CF Server from the Mail Server and gain access to the victim's personal information.

In the **Insertion/Fabrication attack**, the attacker can bombard the CF server with *Call Forward requests* and can cause a denial of service. The attacker can send a large number of authentication requests to the CF and Mail Servers and cause a denial of service attack. The attacker may also request email messages from the Mail Server with the help of the authentication messages captured early on.

In the **Modification attack**, the attacker can modify parameters in the messages, e.g. caller id so that the calls are forwarded incorrectly, modify the call forward number, change the authentication challenge response to incorrect value so the CF and Mail servers are never authenticated. In the **Interruption attack**, the attacker may delete all messages on the link arriving to the CF Server or Mail Server giving an impression that these servers are not functional.

Level V attacks on the CF Service may be enumerated as follows. In the **Interception attack** the attacker may steal personal information of subscribers stored in the *Subscriber Parameter* data store of the CF or Mail Server. In the **Insertion/Fabrication attack**, subscribers not paying for the service may be inserted into the *CF Subscriber Parameter* data sources. At the CF Server fake email data may be inserted into the *Email* data cache through the CFS Mail Server Agent. In the **Modification attack**, the attacker may also have the capability to modify call forward numbers for subscriber at the *Subscriber Parameter* data store, change the time stamps of cached *Email* data, replace service logic in the *CFS Filtering Agent* and the *CFS Mail Server Agent*.

Denial of Service may be caused by the changing the CF number since the victim does not gain access to the voice message or the call itself. Sending two or three call forward numbers to the *Session Control Agent* at the MSC may cause confusion and the call may not be handled properly. In the **Interruption attack**, the attacker may delete certain target subscriber profiles in the data sources so that they may not receive CF service. At the Mail server, the emails in the *Post office* data store may be deleted. Service logic of certain entities may be completely deleted such as the *CFS Filtering Agent* so that they may be unable to provide any service.

Client Billing Service (CBS): Level IV attacks on the CB service may be enumerated as follows. In **Interception attacks**, the attacker may view caller id's of calls to a victim and sell this information. The attacker may view the authentication messages and use it for a replay attack later on. In the **Insertion/Fabrication attack** the attacker can

bombard the CB server with *Bill Client Requests* and can possibly cause a denial of service. The attacker can send a large number of authentication requests to the CB Server and cause a denial of service attack.

In the **Modification attack**, the attacker can modify parameters in the messages, e.g. caller id so that the calls are forwarded incorrectly, change the authentication challenge response to incorrect value, the CB servers are never authenticated. In the **Interruption attack**, the attacker may delete all messages on the link arriving to the CB Server giving an impression that these servers are not functional.

Level V attacks on the CB Service may be enumerated as follows. In the **Interception attack** the attacker may steal personal information of subscribers stored in the client preferences data source in CB Server. In the **Insertion/Fabrication attack**, subscribers not paying for the service may be inserted into the CB data source or fake charged may be inserted into a victim's bill.

In the **Modification attack**, the attacker may also have the capability to modify the forward numbers for subscriber or corrupt logic in *CBS Timer Agent* and *CBS Bill Calculator*; this results in the victim receiving exorbitant bills. Attack the *CBS Client Checker Agent*; change the bill amount or the time log of the client's consultation. **Denial of Service** may be caused by changing the CF number or simply removing the victims name from the client phone book. In the **Interruption attack**, the attacker may corrupt the phone book and delete victims from the *Client Phone Book* data source so that they may not receive CF service.

Location Based Instant Message System (LB-IM): Level IV attacks on the LB-IM Service may be enumerated as follows. In **Interception attacks**, the attacker may view location track requests and location in the location track responses violating privacy. The attacker may view the authentication messages and use it for a replay attack later on. In the **Insertion/Fabrication attack** the attacker can bombard the LB-IM server with *location track requests* and can possibly cause a denial of service.

The attacker can send a large number of authentication requests to the LB-IM Server and cause a denial of service attack. In the **Modification attack**, the attacker can modify parameters in the messages, e.g. name of buddy in the location track request and the location where the buddy is located or change the authentication challenge response to incorrect value so the LB-IM server is never authenticated. In the **Interruption attack**, the attacker may delete all messages on the link arriving to the LB-IM Server giving the impression that this server is not functional.

Level V attacks on the LB-IM Service may be enumerated as follows. In the **Interception attack** the attacker may steal personal information of subscribers stored in the *Permissions* and *Buddy list* data store of the LB-IM. In the **Insertion/Fabrication attack**, subscribers not paying for the service may be inserted into the LB-IM permissions and buddy list data sources. At the LB-IM server authentication information may be inserted to authenticate fake core network entities.

In the **Modification attack**, the attacker may also have the capability to modify permissions and buddy list data stores, E.g. the victim's boss may be able to view the victim's weekend locations. The service logic in the LB-IM request manager may be modified so that the requests are not properly checked. Changing the Buddy list and permissions so that legitimate members of the list cannot locate the subscriber thereby cause **Denial of Service**. In the **Interruption attack**, the attacker may delete certain target subscriber profiles in the data sources so that they may not receive LB-IM service. Service logic of certain agents may be completely deleted.

6. Conclusion

This paper has defined a unique attack taxonomy for 3G networks, which includes the *Cross Infrastructure Cyber attack*. As more vulnerabilities are discovered, the taxonomy may be expanded to support newer attacks. The abstract model defined in this paper has been instrumental in the development of the 3G attack taxonomy. We have demonstrated that with the help of the abstract model, it is straightforward to pinpoint security threats, vulnerabilities and attacks at specific points in 3G the infrastructure. In the future it can be shown that the abstract model may be used to validate 3G vulnerability assessment tools.

	Interception	Fabrication/ Insertion	Modification Of Resources	Denial Of Service	Interruption
Level I	<ul style="list-style-type: none"> -Observe time, rate, length, source and destination of victim's locations. -With modified MS, eavesdrop on victim. 	<ul style="list-style-type: none"> - When target camps at false base station, calls made by the victim may be hijacked and used to make fraud calls, while the victim is charged. 	<ul style="list-style-type: none"> - With modified base station and modified mobile station, the intruder can come between the target and the network 	<ul style="list-style-type: none"> - When victims camp at false base stations, then victims are out of reach of signals from the serving network and can no longer receive calls and other network related services. 	<ul style="list-style-type: none"> -Jam victims traffic channels so the victim cannot access the channel. -Broadcast at a higher intensity than allowed hogging bandwidth
Level II	<ul style="list-style-type: none"> -Analyze traffic patterns, gather subscriber/company data -Eavesdrop on calls and voice signaling messages -Capture AV's sent from HLR to VLR and use in replay attacks. 	<ul style="list-style-type: none"> - Send a large number of routing requests to the Routing Agent (MSC): exhaust RN's, so the MSC cannot support more call requests. - Send Registration / Location Update messages to Registration Agent (HLR) to cause incorrect call routing, shutting down of the mobile station's - Send profile change messages to: Subscriber Profile Manager Agent At HLR: Subscriber may not receive services. - Request AV's from HLR: Authenticator Agent and use for replay attacks 	<ul style="list-style-type: none"> - Change called party number in call request messages and the call is sent to incorrect party. -Change the routing numbers in routing responses, so MSC under attack does not receive incoming calls. - Change the AV's sent to authenticate the MS, so that the MS is never authenticated. 	<ul style="list-style-type: none"> - Send IAM to switch /MSC: exhaust RN's : Overload Switch - Large number of auth request to authenticator Agent At HLR slow down HLR and surrounding links. - Send spoofed Location Update message to HLR : Registration Agent cause incorrect call routing, shutting down MN -Changing Profile Settings: Subscriber Profile Manager Agent at HLR 	<ul style="list-style-type: none"> -Delete Registration / Loc Update Messages at Registration Agent (HLR) results in incorrect call routing - Delete Call Requests - Delete Send authentication Information Requests
Level III	<ul style="list-style-type: none"> -Analyze traffic patterns, gather subscriber/company data arriving at the compromising entity -Gather data stored in HLR and sell it to competition -At MSC, track the subscriber's activities, calls and their services they access. 	<ul style="list-style-type: none"> Access to HLR: Add new subscribers to the Profile Setting, Terminal Data, Subscribed Services and CAMEL & Supplementary Services Data stores and not the billing data store, this way the fraud subscribers can access the services without paying. - Insert new service logic to the compromised entity so that it is disabled at a particular time. 	<ul style="list-style-type: none"> -Change Subscriber Profile, Authentication data, location data at the HLR. -Change the mapping at HLR: Location data: Registration Agent -Modify the routing numbers in the Routing Agents. Calls cannot be routed to the Session Control Agents. 	<ul style="list-style-type: none"> -Modify a parameter in the Authentication Vector calculating algorithm so that none of the MS's may be authenticated and hence do not get service. 	<ul style="list-style-type: none"> - Delete subscriber preferences - At Authenticator Agent HLR, delete Ciphering algorithm and replace with another one, fail to authenticate all MN.

*AV: Authentication vector

Table 5.1: Single Infrastructure attacks on the CS domain classified by *CASE I*.

	Interception	Fabrication/ Insertion	Modification of Resources	Denial Of Service	Interruption
Level IV	<ul style="list-style-type: none"> -Analyze traffic patterns, gather subscriber/company data - View details of messages between the Cross Network Servers and 3G core network entity. 	<ul style="list-style-type: none"> - Send profile change messages to Cross Network Servers: Subscriber Profile Manager Agent - Send a large number of authentication requests to the Cross Network Servers. -Bombard the Cross Network Servers with requests. 	<ul style="list-style-type: none"> -Modify messages passing on the link : Change the challenge response to incorrect value: device is never authenticated. : Change replies to queries to incorrect values. : Modify parameters in the signaling messages. 	<ul style="list-style-type: none"> - Send the MSC: Session Control Agent/ Subscribed Services Support Agent a large number of replies for a particular query or spoof it to be queries for different subscribers. - Send the Cross Network Servers large number of Authentication Requests and slow them down 	<ul style="list-style-type: none"> - Delete all messages arriving and leaving the Cross Network Servers
Level V	<ul style="list-style-type: none"> -Analyze traffic patterns, gather subscriber/ company data - Steal personal information of subscribers registered. Service Logic at the Cross Network Servers. 	<ul style="list-style-type: none"> - Insert subscribers not subscribed for service into the Cross Network Servers, they receive service but are not charged. - Insert fake data into the data stores of the Cross Network Servers. 	<ul style="list-style-type: none"> -Modify Service Logic and data sources in the Cross Network Servers. 	<ul style="list-style-type: none"> - Caused by editing the data sources. 	<ul style="list-style-type: none"> - Delete data sources and service logic in the Cross Network servers.

Table 5.2: Cross Infrastructure Cyber attacks classified by CASE I

Attack Categories	Data	Messages	Service Logic
Interception	- Gather customer information by reading data stored in database. At the Cross Network Servers invoke Subscriber Parameter manager Agent	-Analyze traffic patterns, gather subscriber/company data	- Gather system information by observing/reading operations in the system -At the Cross Network Servers invoke read the service logic
Insertion/ Fabrication	-Add users to the database that are not subscribed/ paying for the service. -At the Cross Network Servers invoke Subscriber Parameter manager Agent to insert into the Subscriber Parameter Data Store	- Send a large number of routing requests to the Routing Agent (MSC): exhaust RN's, so the MSC cannot support more call requests. - Send Registration / Location Update messages to Registration Agent (HLR) to cause incorrect call routing, shutting down of the mobile station's - Send profile change messages to Subscriber Profile Manager at HLR - Request AV's from Authenticator Agent at HLR	-Insert new service logic to the compromised entity so that it is disabled at a particular time.
Modification of Resources	- Modify Subscriber profile Information so that the subscriber receives services he is not paying for. (E.g.: Receive National wide service when subscribed for local service.) -Remove subscribers name from database. (E.g.: Deny Service for those already registered)	-Modify messages passing on the link : Change the challenge response to incorrect value: device is never authenticated. : Change replies to queries to incorrect values.	-Modify Service Logic : Fwd Calls to wrong Location : Change Call Forwarding Logic : Show Wrong Buddies subscriber Location Information: Service Logic in request IM : Change E-mail Time Stamps: Service Logic Mail Server : Client Phone Book: Client Checker Agent
Denial of Services	-Deny Service for those already registered by removing subscribers name from database: Invoke the Registration Agent	- Send Multiple Challenges to Authenticator Agent at HLR requesting authentication for multiple users. This could clog the HLR. - Send the MSC: Session Control Agent a large number of replies for a particular query or spoof it to be queries for different subscribers	- Modify Service Logic : Fwd Calls to wrong Location : Change Call Forwarding Logic
Deletion / Interruption	- Delete subscriber data / Subscriber preferences stored in the Cross Network Server : Mail Data : Phone Book Data : CF Data : Buddy List	- Delete all messages arriving at the Cross Network Server : CF messages -Delete all messages leaving the Cross Network : Challenges to HLR : Response to queries (MSC)	- Delete service logic Cross Network Server : CF rules set by the subscriber: CFS Subscriber Parameter Manager agent. : CBS service logic : Permissions and Buddy list LB-IM Subscriber Parameter Manager agent.

Table 5.3: Attacks classified by CASE II

7. References

- [1] Andrew P. Snow, Upkar Varshney, Alisha D. Malloy, "Reliability and Survivability of Wireless and Mobile Networks", IEEE Computer, July 2000, p. 49-55.
- [2] 3GPP TS 23.221, "Architectural requirements", V6.3.0 (2004-06).
- [3] 3GPP TS 23.002 V3.3.0 (2000-03), Network architecture (Release 1999).
- [4] 3GPP TS 23.228 V6.7.0 (2004-09), IP Multimedia Subsystem (IMS); Stage 2 (Release 6)
- [5] Eberspacher, Vogel, "GSM Switching, Services and Protocols", John Wiley & Sons, Copyright 1999.
- [6] 3GPP TS 23.008 V3.3.0 (2000-03), Organization of subscriber data (Release 99)
- [7] C. W. Blanchard, "Wireless Security", BT Technology Journal, v.19 n.3, p.67-75, July 2001
- [8] 3GPP TS 23.018 V 3.4.0 (2000-03), Basic Call Handling (Release 99)
- [9] G. Lorenz, T. Moore, G. Manes, J. Hale, S. Sheno, "Securing SS7 Telecommunications Networks", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, June 2001
- [10] T. Moore, T. Kosloff, J.Keller, G. Manes, S. Sheno, "Signaling System 7 (SS7) Network Security," Proceedings of the IEEE 45th Midwest Symposium on Circuits and Systems, Tulsa, OK, August 4-7, 2002.
- [11] Howard, P. Walker, M. Wright, T., "Towards a coherent approach to third generation system security", Second International Conference, 3G Mobile Communication Technologies, 2001. on (Conf. Publ. No. 477)
- [12] El-Fishway, Nawal A.; Nofal, Mostafa A.; Tadros, Albert M., "An Improvement on Secure Communication in PCS", Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International , 9-11 April 2003
- [13] 3G TS 21.133 V3.1.0 (1999-12) 3G Security; Security Threats and Requirements version 3.1.0
- [14] 3G TR 33.900 V1.2.0 (2000-01), A Guide to 3rd Generation Security
- [15] 3G TS 33.120 V3.0.0 (1999-05) 3G Security; Security Principles and Objectives version 3.0.0
- [16] J.Rao, P. Rohatgi, H. Scherzer, S. Tinguely, "Partitioning Attack: Or How to Rapidly Clone Some GSM Cards", IEEE Symposium on Security and Privacy, May 2002.
- [17] CC Lo and YJ Chen, "Secure communication mechanisms for GSM networks," IEEE Transactions on Consumer Electronics, Vol. 45, No. 4, pp..
- [18] A. Chakrabarti and G. Manimaran, "Internet Infrastructure Security: A Taxonomy," IEEE Network, vol.16, no.6, pp.13-21, Nov/Dec. 2002.
- [19] Donald Welch ,Scott Lathrop, "Wireless Security Threat Taxonomy", June 2003 IEEE Workshop on Information Assurance.
- [20] C. W. Blanchard, "Wireless Security", BT Technology Journal, v.19 n.3, p.67-75, July 2001
- [21] Brookson, C.B., "Security in current systems", Security in Networks (Digest No. 1995/024), IEE Colloquium on , 3 Feb. 1995, Pages:3/1 - 3/6.
- [22] Mitchell, C.J.; "Security in Networks", (Digest No. 1995/024), IEE Colloquium on , 3 Feb. 1995 ,Pages:2/1 - 2/6.
- [23] Boman K, Horn G, Howard P, Niemi V, "UMTS security", Electronics & Communication Engineering Journal, Volume: 14 , Issue: 5 , Oct. 2002, Pages:191 - 204
- [24] Kluepfel, H.M., "Securing a global village and its resources: Baseline security for interconnected Signaling System #7 telecommunications networks" Security Technology, 1993. Security Technology, Proceedings. IEEE 1993 International Carnahan Conference on , 13-15 Oct. 1993, Pages:171 - 188.
- [25] Clissmann, C., Patel, A., "Security for mobile users of telecommunication services", Universal Personal Communications, 1994. Record., 1994 Third Annual International Conference on , 27 Sept.-1 Oct. 1994, Pages:350 - 353.
- [26] V. Bharghavan, C.V. Ramamoorthy, "Security Issues in Mobile Communications", Autonomous Decentralized Systems, 1995. Proceedings. ISADS 95., Second International Symposium on , 25-27 April 1995.
- [27] <http://www.kb.cert.org/vuls/id/125235>
- [28] CERT Advisory CA-97.05: "MIME Conversion Buffer Overflow in Sendmail Versions 8.8.3 and 8.8.4" at: <http://www.cert.org/advisories/CA-97.05.sendmail.html>
- [29] Sendmail Consortium: "Sendmail FAQ" <http://www.sendmail.org/faq>
- [30] Stallings, "Cryptography and Network Security: Principles and Practice", Second Edition, Copyright 2000.
- [31] K. Murakami, O. Haase, J. Shin, T. F. LaPorta. Mobility Management Alternatives for the Migration to Mobile Internet Session-based Services. In IEEE Journal on Selected Areas in Communications (J-SAC), special issue on Mobile Internet, Vol. 22, No. 5, Jun 2004.
- [32] Amit P. Sheth , James A. Larson, " Federated database systems for managing distributed, heterogeneous, and autonomous databases", ACM Computing Surveys, Vol. 22, No. 3, pp. 183-236, Sep. 1990.

Appendix A - Interworking Approaches

In this section we identify attack scenarios in the methods used to interwork the 3G core network and the Internet. Based on the interworking approaches we will modify the attack taxonomy and group the attacks.

A.1 Background

In this section we discuss the three approaches for interworking the core 3G networks and the Internet. Protocol Gateway Approach, Federated Approach and the Unified Approach are the three basic approaches and they are described in detail below [31].

Protocol Gateways: Protocol Gateways are components used to connect disparate networks by passing traffic between the two networks. The Protocol Gateway performs the protocol conversion and routes traffic; every network receives traffic in the protocol it understands. E.g. In Fig A.1, the Protocol Gateway converts 3G Traffic to IP Traffic and vice versa.

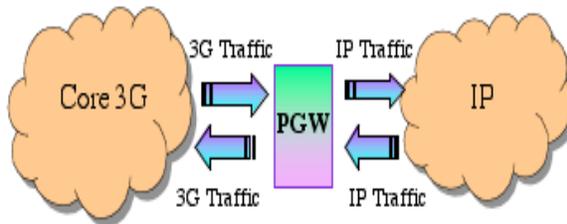


Fig A.1: Protocol Gateway connecting the core 3G and IP Networks.

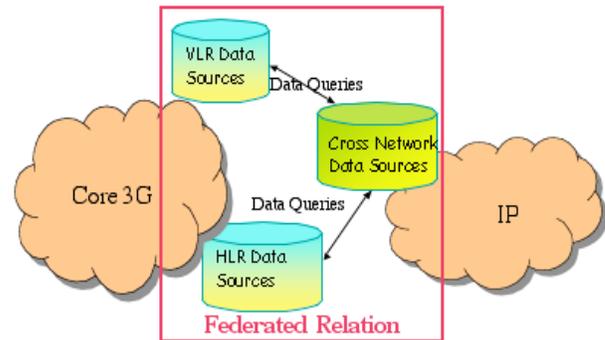


Fig A.2: Core 3G and IP Network entities in a Federated Relation

Federated Approach: In the Federated Approach, entities in the core 3G and the IP networks communicate through their data sources. Entities in the federated approach share their data sources with other entities while maintaining some measure of local control. Component data sources can operate independently, but can also give up their autonomy to participate in the federation. Entities in a federated relationship communicate by exchanging queries between data sources instead of signaling messages between the entities. These database queries will traverse the links connecting the two networks. Fig A.2 displays the federated relationship. E.g. In Fig 4.2 the “Authenticate” signal message 14 exchanged between the *Authenticator Agent (HLR)* and *CFS Authenticator Agent* may be replaced by an exchange between the *HLR-Authentication Data* and *CFS-Authentication Information* data sources in the Federated Approach. Cross Network signaling messages are replaced by Cross Network data source queries [32].

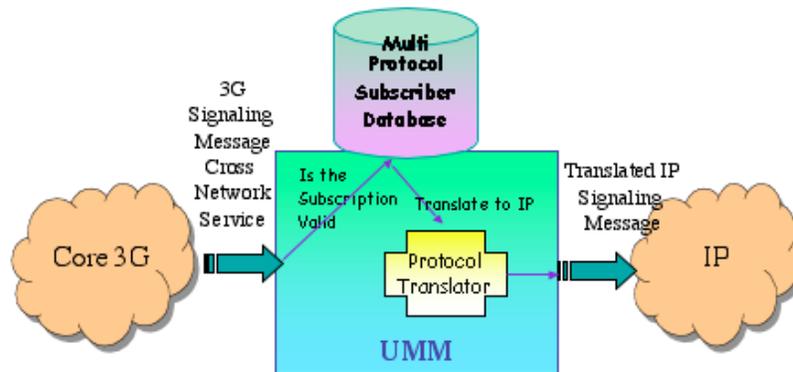


Fig A.3: Interworking Core 3G and IP Network entities with UMM

Unified Approach: The unified approach introduces a network element called the *Unified Mobility Manager* (UMM). The UMM contains a multiprotocol subscriber database which maintains the subscriber profile information for all services and all network types to which the user subscribes. The UMM also has an internal protocol translator which translates from one protocol to another [31]. E.g. UMM multiprotocol subscriber database stores data from HLR; Cross Network services such CF services, LB-IM services etc. Figure A.3 shows the interworking using the UMM approach. Cross Network signaling queries are sent to the UMM, which looks up its multiprotocol subscriber database to check if the query is valid. If this query is valid the signaling messages goes through the protocol translator and is sent to the other network.

A.2 Attack Taxonomy and Attacks

This section examines the changes in attack taxonomy and groups attacks in the three interworking approaches.

A.2.1 Protocol Gateways

In this Approach, Dimension I-Level IV may be further divided into Level IV a and Level IV b. In Level IV a the attacker has *Access to Links connecting the Internet and the 3G core network*, it is the same as Level IV in Section 5.1.1. and in Level IV b the attacker has *Access to Protocol Gateway*.

Level IV b : *Access to Protocol Gateway*: When the attacker has access to the Protocol Gateway the attacker may view the messages passing through the links, insert messages into the links and corrupt the protocol translator or service logic.

We will use the above classification to detail attacks. The attacks are tabulated as *CASE 1: Dimension I: Physical Access Vs Dimension II: Attack Categories*. Table A.1 shows the CASE 1 tabulation of possible attacks with the introduction of the protocol gateways. In Table A.1 we will consider the effect of Dimension I-Level III access on the Protocol Gateway, effect of Level IV b access and the effect of Dimension I-Level V access on the Protocol Gateway.

	Interception	Fabrication/ Insertion	Modification Of Resources	Denial Of Service	Interruption
Level III	-Analyze traffic patterns, gather data around PGW.	- Insert large number of messages requesting Cross Network Services and Hence Protocol conversion: Overload Gateway.	- By causing a buffer overflow attack modify the contents/service Logic of Protocol Gateway	- Repeated Requests for Cross Network Services.	-By causing a buffer overflow attack delete the contents/service Logic of Protocol Gateway
Level IV b	-View Messages arriving at the gateway	-Insert messages into the link requesting for Cross Network Services and 3G-core services	-Modify routing tables so that the converted traffic is routed to the Intruder's network -Modify parameters in the protocol conversion logic, the converted traffic is garbled : Service is not provided	-Deletion/Do not provide responses of Requests that arrive at the PGW.	-Insert Large number of messages on the link.
Level V	-Analyze Traffic Patterns	- Insert large number of messages requesting 3G core services	-Remote access the Protocol Gateway causing a buffer overflow	- Repeated Requests for 3G Services.	-By causing a buffer overflow attack delete the contents/service Logic of Protocol Gateway

Table A.1: Attacks classified by CASE 1 Protocol Gateway Approach.

A.2.2 Federated Approach

In this Approach, Dimension I-Level IV definition remains the same when compared to the other interworking cases. In this case database queries traverse the links instead of signaling messages. The attacker can cause damage by disrupting normal transmission of database queries traversing the link and inserting database queries into the link between the two networks.

We will use the above classification to detail attacks. The attacks are tabulated as *CASE 1: Dimension I: Physical Access Vs Dimension II: Attack Categories*. Table A.2 shows the CASE 1 tabulation of possible attacks with the Federated

approach. In Table A.2 we will consider the effect of Dimension I-Level III access on Federated relation, effect of Level IV access and the effect of Dimension I-Level V access on Federated relation.

	Interception	Fabrication/ Insertion	Modification Of Resources	Denial Of Service	Interruption
Level III	-Analyze traffic patterns, gather data. -Eavesdrop on messages	- Send a large number of data queries to Cross Network entities. -Insert fake data into the database such that it is disseminated to other entities. -Send messages to other entities and gather sensitive data from their databases.	- Modify Subscriber Information. - Modify access rules in the federated relation so that valid queries are denied access. -Modify data conversion rules	- Modify Port addresses so the entity may not be reached by other entities in the federated relation. - Send a large number of messages and clog the database port. -Modify mapping between subscriber profile and settings (preferences, authentication); valid queries are denied. -Open up ports in 3G entities, making it vulnerable to other attacks.	- Delete the contents of the database. -Deny data access to other valid entities in the federated relation.
Level IV	-Analyze traffic patterns, gather data. -Eavesdrop on messages	- Insert spoofed Request /Response type of database queries to the databases to gather sensitive information.	- Modify all database queries on the link. -Modify source, destination address, query, response.	- Direct database ports of entities in the federation with Service requests and clog the ports and the links.	-Deleting signaling queries on link. - Send Spoofed Messages to cancel service. -By deleting database responses, the source will continue to query and overload the destination.
Level V	-Analyze traffic patterns, gather data. -Eavesdrop on messages	- Send fake response message (Just respond and not process the messages). - Send Spoofed Messages to 3G entities like HLR, VLR requesting a specific service such as process an incoming call.	-Modify parameter used for protocol conversion in wrappers. -Modify Requests. - Modify Service Logic so that multiple responses are sent instead of a single one.	- Repeated Requests for IP Services. -Change authentication information at the Cross Network Servers , so that certain people are never authenticated and never receive any service. -Open up ports in Cross Network Servers, making it vulnerable to other attacks.	-Modify service logic so that the IP Service Server only responds to every 2 nd or 3 rd message

Table A.2 : Attacks classified by CASE 1 Federated Approach.

A.2.3 Unified Approach

In this Approach, Dimension I-Level IV may be further divided into Level IV a and Level IV b. In Level IV a the attacker has *Access to Links connecting the Internet and the 3G core network*, it is the same as Level IV and Level IV b is *Access to Unified Mobility Manager*.

Level IV b : *Access to Unified Mobility Manager*: When the attacker has access to the *Unified Mobility Manager* attacker may view the messages passing arriving at the UMM, access the data in the multiprotocol subscriber database, access the protocol translator logic. The attacker may insert messages into the links and corrupt the multiprotocol subscriber database, protocol translator or service logic.

We will use the above classification to detail attacks. The attacks are tabulated as *CASE 1: Dimension I: Physical Access Vs Dimension II: Attack Categories*. Table A.3 shows the CASE 1 tabulation of possible attacks with the introduction of the *Unified Mobility Manager*. In Table A.3 we will consider the effect of Dimension I-Level III access on the *Unified Mobility Manager*, effect of Level IV b access and the effect of Dimension I-Level V access on the *Unified Mobility Manager*.

	Interception	Fabrication/ Insertion	Modification Of Resources	Denial Of Service	Interruption
Level III	-Analyze traffic patterns, gather data. -Eavesdrop on messages arriving at the entities.	- Send large number of messages to the Cross Network Servers, so that the UMM is overloaded.	- Send messages to the UMM requesting for change in a 3G subscriber's profile in the multiprotocol Subscriber database.	- Repeated Requests for IP Services to the UMM.	-Delete 3G subscriber profile data in the multiprotocol subscriber database.
Level IV b	-Analyze traffic patterns, gather data. -Eavesdrop on messages arriving at the UMM	-Insert invalid subscriber profile into the multiprotocol Subscriber database. -Insert fake messages on the links.	- Modify multiprotocol subscriber database, query does not go through - Modify protocol translator such that signaling messages are not translated right. -Modify the Cross Network signaling messages passing through the UMM	-Delete subscriber profile from the multiprotocol Subscriber database attached to the UMM; this way legitimate subscribers do not receive cross network service.	-Delete Messages arriving at the UMM. -Delete data in the multiprotocol subscriber database. -Delete the protocol translation logic so that signal messages are not translated.
Level V	-Analyze traffic patterns, gather data. -Eavesdrop on messages arriving at the entities.	- Send large number of messages to the Cross Network Servers, so that the UMM is overloaded.	- Send messages to the UMM requesting for change in a Cross Network subscriber's profile in the multiprotocol Subscriber database.	- Repeated Requests for 3G Core Services to the UMM.	-Delete Cross Network Service subscriber profile data in the multiprotocol subscriber database.

Table A.3: Attacks classified by CASE 1 UMM Approach.

Appendix B: IP Multimedia Subsystem

B.1. Background

In this section we discuss the four main core network entities used in the IP multimedia subsystem.

Every network operator assigns in its administrative areas one or more P-CSCF's (Proxy-Call Session Control Function). The P-CSCF is the first point of contact for a mobile station into the IMS network. The P-CSCF accepts requests from the mobile station and either services them or forwards them on. It will locate the subscriber's home network and is in charge of QOS reservation based on local network conditions and capabilities [4,7].

Every network operator has one or more I-CSCF(Interrogating-Call Session Control Function) assigned to its network. All messages in and out of the network must pass through the I-CSCF. This entity acts as a firewall and will hide the network's configuration, capacity and topology from the outside. The I-CSCF is the first point of contact into the network from the outside world for incoming messages (Requests from subscribers roaming in other networks). All messages exiting the network must pass through the I-CSCF [4,7].

The S-CSCF (Serving-Call Session Control Function) is located in the home network of the subscriber and is assigned at the time of registration depending on the needs of the subscriber. At the time of registration the subscriber service profile is downloaded from the HSS to the S-CSCF. It maintains the session state information as needed by the network operator to support services [4,7].

The subscriber's IMS service settings, profile data, authentication data is defined and maintained in the HSS (Home Subscriber Server). The HSS also maintains information of all S-CSCF's in its domain.

The Session Initiation Protocol Uniform Resource Identifier (SIP:URI) is the generic form of address of a Internet based user (E.g., SIP User) or Internet resource. URI' includes URL's and Email Address.

B.2. Abstract Model for IP Multimedia Subsystem

Fig B.1 shows the abstract model of the entities in the PS domain. The abstract model for the IMS shows the abstract model for the User Agent. The User Agent is a part of the mobile station. The User Agent contains data needed by the core network and agents that interact with the network to provide service to the subscriber. Table B.1 describes the agents used in IP Multimedia System Abstract Model.

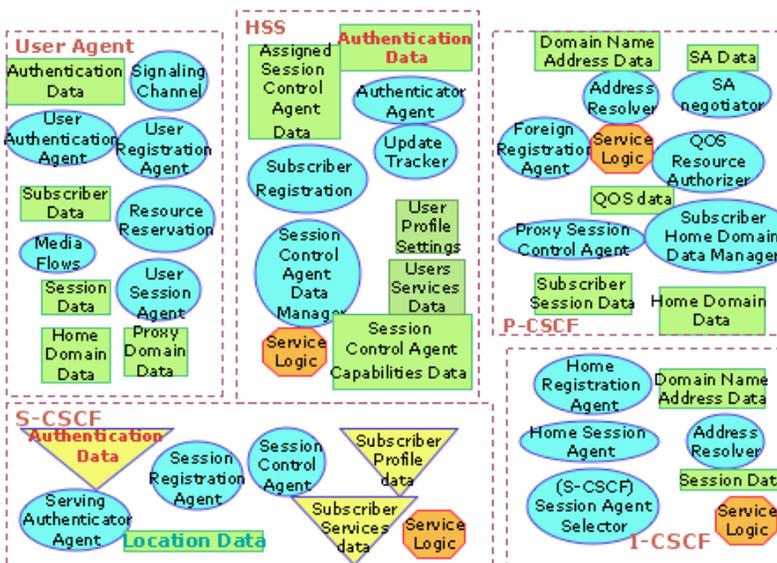


Fig B.1: Abstract Model of Entities in the IP Multimedia Subsystem

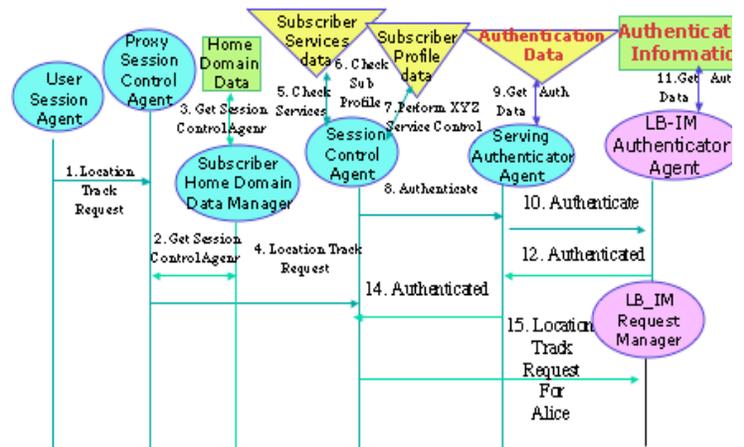


Fig B.2: Signal Flows IMS requesting LB-IM service

B.3 Attack Overview

In this section we will use the abstract model to study the initiation of the LB-IM service by the IP Multimedia Subsystem and discuss the attack possibilities on the IP Multimedia Subsystem. The LB-IM is triggered when a location track request arrives at the *LB-IM Request Manager*. Fig B.2 shows the IMS signal flows requesting for LB-IM Service. This is an expansion of the 3G IMS cloud in Fig 4.5. In Fig B.2 the User Session Agent in the *User Agent* sends a *Location Track Request* into the serving network *Proxy Session Control Agent(P-CSCF)*. The serving network *Subscriber home domain Data Manager(P-CSCF)* stores the address of the *Session Control Agent(S-CSCF)*, which is assigned at the time of registration. The *Session Control Agent (S-CSCF)* remains the same for the length of the registration. The *Subscriber Home Domain Data Manager (P-CSCF)* looks into its *Home Domain Data Source* to find the address of the *Session Control Agent (S-CSCF)*. Once the *Proxy Session Control Agent (P-CSCF)* gets the address of the *Session Control Agent (S-CSCF)* it forwards the *Location Track Request* to the *Session Control Agent*. The *Session Control Agent (S-CSCF)* looks into its cached *Subscriber Services data* source and *Subscriber Profile data* source to check the subscriber's profile and the subscriber's services data. If the *Session Control Agent (S-CSCF)* finds the request to be valid, it will request the *Serving Authentication Agent (S-CSCF)* to authenticate with the *LB-IM Authentication Agent*. Once authenticated the *Session Control Agent (S-CSCF)* forwards the *Location Track* request to the *LB-IM Request Manager* and the request will be serviced.

In the LB-IM Service spoofed messages may be sent to the *LB-IM Subscriber Parameter Manager* as mentioned in Section 4.1. Other possible attacks include corrupting the Home Domain data source so that the Session Control Agent may not be located, corrupting the Subscriber Services data source and Subscriber Profile data sources. Section B.4 provides more information on these attacks.

B.4 Attacks

We tabulate a list of possible attacks on the IMS Domain. Table B.1 shows attacks on IMS Subsystem classified by *CASE 1*. Level I of Attacks on the IMS Subsystem is the same as Level I of Attacks on the CS Domain (Table 5.1) hence we are omitting it from Table B.1. In IMS Subsystem, Dimension I-Level III may be further divided into Level III a and Level III b. In Level III a the attacker has *Remote access to IMS entities* and Level III b the attacker has *Direct access to IMS entities*. Level III b it is the same as Level III in the CS Domain. *Cross Infrastructure Cyber Attacks* of Level VI and V are similar to the CS domain shown in Table 5.2.

Entity	Name of Agent	Description
User Agent	User Authenticator	Manages Authentication data (secret key, algorithm etc) stored in the mobile node.
	Resource Reservation	Based on incoming/outgoing session descriptors and its own terminal capabilities it will decide the resources needed for the session.
	Signaling Channel	Establishes contact between the mobile station and the network
	Media Flows	Will start/initiate media flows for a session based on terminal capabilities
	User Session	Will Initiate/Handle Incoming Sessions on behalf of the User.
	User Registration	It is invoked when a mobile node powers up or enters/exits a new area. This invokes the registration at the visiting network.
P-CSCF	SA Negotiator	Negotiates Security Association with the User Agent.
	Address Resolver	Resolves URI's to IP Addresses
	QOS Resource Authorizer	It will approve/authorized the QOS resource reservation request based on current network load and radio link capacity.
	Proxy Session Control Agent	Handles Incoming & Outgoing Sessions for a Users currently registered with the visiting network.
	Subscriber Home Domain Data Manager	Will save address of the visiting subscriber's assigned session control agent for that registration.
	Foreign Registration	It is the Registration Agent in the Visiting Network and is invoked by the user registration agent
I-CSCF	Home Registration	Receives registration messages at the entry point into the home network.
	Address Resolver	Resolves URI's to IP Addresses
	Home Session	It will handle sessions for a user and forward messages between session control agent and proxy session control agent.
	S-SCSF/Session Agent Selector	It will select session control agent for the registered subscriber based on subscriber's requirements and session control agent capabilities.
S-CSCF	Serving Authenticator	Manages authentication data cached from the home network and performs the 3-way AKA.
	Session Registration	Handles subscriber registration by caching user profile data, services data from home domain and stores home domain address locally and provide home domain the address of the assigned session control agent.
	Session Control	Handles Sessions for the user in the Home network. Performs Service Control based on subscriber's profile & subscribed services data.
HSS	Authenticator	Is in charge of retrieving keys from the authentication data source and generating authentication material for all users subscribing to its network and also other services the user may be subscribed to. It may be invoked to authenticate the subscriber
	Subscriber Registration Agent	Handles all registration messages, checks if the user is already registered, if the user is allowed to register in the Visiting Network and will contact the Authenticator to authenticate the user.
	Session Control Agent Data Manager	Manages data of all the S-CSCF/Session Control Agent in the network.
	Update Tracker	Will inform the assigned Session Control Agent if the user profile settings or services data.

Table B.1: Description of Agents used in IMS Abstract Model

Physical Access	Interception	Fabrication/ Insertion	Modification of Resources	Denial Of Service	Interruption
Level II Links Connecting IMS Entities	<ul style="list-style-type: none"> -Analyze traffic patterns, gather subscriber/company data -Eavesdrop on calls and voice messages -Capture AV's sent from Authenticator Agent (HSS) to S-CSCF (Serving Authenticator Agent) and use in replay attacks. 	<ul style="list-style-type: none"> - Send repeated INVITE messages to S-CSCF (Session Control Agent): overload Home Network, this way it cannot service valid incoming requests and generate outgoing requests. - Send Registration / Location Update messaged to Subscriber Registration Agent (HSS): cause incorrect call routing, shutting down MN - Send profile change messages to HSS (Session Control Agent Data Manager) - Request AV's from Authenticator Agent (HSS) 	<ul style="list-style-type: none"> -Change the SIP:URI [Uniform resource identifier] (IMS User Address) in Registration signaling message so that the subscriber cannot be registered. -Change the other party's SIP:URI address in outgoing INVITE service request signaling messages and the request is sent to incorrect party. -Change the SIP:URI addresses in the Incoming Session Invite Messages; message does not reach the subscriber -Change the AV's sent to authenticate the User Agent, so that the User Agent is never authenticated. 	<ul style="list-style-type: none"> - Send repeated INVITE messages to S-CSCF (Session Control Agent): overload Home Network. - Large number of auth request to Authenticator Agent (HSS) slow down Authenticator Agent and surrounding links. - Send repeated Registration / Location Update messaged to Subscriber Registration Agent (HSS): cause incorrect call routing, shutting down MN - Send profile change messages to HSS (Session Control Agent Data Manager). 	<ul style="list-style-type: none"> -Delete Registration / Location Update messaged to Subscriber Registration Agent (HSS): incorrect call routing - Delete Call Invite Requests - Delete AV's sent from Authenticator Agent (HSS) to S-CSCF (Serving Authenticator Agent) Send authentication -Delete Ringing Messages
Level III a Remote Connection To IMS Entities	<ul style="list-style-type: none"> -Analyze traffic patterns, gather subscriber/company data arriving at the compromising entity 	<ul style="list-style-type: none"> - Insert new service logic to the compromised entity so that it directs all traffic to the Intruders service location. 	<ul style="list-style-type: none"> - Buffer overflow attacks cause execution of malicious code and hence modification of Service Logic. 	<ul style="list-style-type: none"> -Buffer overflow could also cause a denial of Service at the IMS Entity. 	<ul style="list-style-type: none"> -Delete data sources in the entities.
Level III b Direct Connection To IMS Entities	<ul style="list-style-type: none"> -Gather data stored in entity and sell it to competition -Track a particular subscribers activities at the Session Control Agent and Data sources in the HSS 	<ul style="list-style-type: none"> - Insert new service logic to the compromised entity so that it is disabled at a particular time. -Access to HSS : Add new subscribers to the Profile Setting, Subscribed Data stores and not the billing data store, this way the fraud subscribers can access the services without paying. 	<ul style="list-style-type: none"> -Modify destination of Session Invite Messages. -Modify Session Descriptors -Change Subscriber Profile, AV, location mapping at S-CSCF & HSS data sources - Modify the session handling capabilities at the Session Control Agent and Proxy Session Control Agent. -Modify Service Logic in Subscriber Home Domain Manager so that User Session Control Agent mapping is corrupted and the users requests may not be serviced. 	<ul style="list-style-type: none"> -Modify a parameter in the Authentication Vector calculating algorithm so that none of the MS's may be authenticated and hence do not get service. 	<ul style="list-style-type: none"> - Delete subscriber preferences - At Authenticator Agent (HSS), delete Ciphering algorithm and replace with another one, fail to authenticate all MN. - Delete subscriber preferences

Table B.1: Attacks on IMS Subsystem classified by CASE 1