Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

The Modeling Of An Identity Catching Attack On The Universal Mobile Telecommunication System (UMTS) Using Attack Tree Methodology

by

EZEUDE, Kingsley Anayo

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: December 2009

Research advisors:

Dr. Dale Lindskog, Assistant Professor, MISSM

Ron Ruhl, Director and Assistant Professor, MISSM

Dr. Pavol Zavarsky, Director of Research and Associate Professor, MISSM

The Modeling Of An Identity Catching Attack On The Universal Mobile Telecommunication System (UMTS) Using Attack Tree Methodology

by

EZEUDE, Kingsley Anayo

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Associate Professor, MISSM

Reviews Committee:

Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

Concordia University College of Alberta
Information Systems Security Management
7128 Ada Boulevard, Edmonton, AB
Canada T5B 4E4

The Modeling Of An Identity Catching Attack On The Universal Mobile Telecommunication System (UMTS) Using Attack Tree Methodology

By

Kingsley Anayo Ezeude

A research paper submitted in partial fulfillment of the requirements for for the degree of
Master of Information Systems Security Management

Research advisors:
Pavol Zavarsky, Ron Ruhl, and Dale Lindskog

September 2009

The Modeling Of An Identity Catching Attack On The Universal Mobile Telecommunication System (UMTS) Using Attack Tree Methodology

Kingsley Anayo Ezeude
Pavol Zavarsky (research advisor)
Ron Ruhl (research advisor)
Dale Lindskog (research advisor)

Information Systems Security Management
Concordia University College of Alberta
7128 Ada Boulevard, Edmonton, Alberta, Canada T5B 4E4
http://infosec.concordia.ab.ca

Abstract

This research focuses on the modeling of an Identity Catching attacks in the Universal Mobile Telecommunication System (UMTS) using attack tree methodology. The possible ways an intruder could launch an identity catching attacks on the UMTS are identified and modeled using attack tree methodology. While the use of the Temporal Mobile Subscriber Identity (TMSI) was designed to thwart identity catching attacks (which attempt to track the subscribers location), this paper will show that this measure is weak in protecting the IMSI (location). Even though the subscriber number is at risk, there is no reason this risk needs to escalate further (beyond initial location tracking) if properly configured UMTS only networks are accessed.

I. INTRODUCTION

Universal Mobile Telecommunication System (UMTS) is regarded as an evolution of the Global System for Mobile communication (GSM) system. “It was built within the common frame work defined by the ITU (International Telecommunication Union) in 1998” [1]. It is also one of the third generation mobile networks. The core third generation network consists of the circuit-switched (CS) domain, the packet-switched (PS) domain, and the Internet Protocol (IP) multimedia subsystem [2], [3].

The principal goal of the third-generation mobile telecommunication system project was stated by Dan Fox, in “Testing UMTS”, 2008, [4]. The principal goal “was to try to identify a band of radio spectrum that could be used in as many regions of the world as possible, to promote the concept of a truly global system”. UMTS is compatible with GSM (second generation) since it was constructed from existing GSM technology [5],[6],[7].

The main security objectives of the UMTS are to ensure data and user confidentiality, integrity, and entity authentication [8],[9],[10]. The identities in UMTS are; International Mobile Equipment Identity (IMEI), Temporal Mobile Subscriber Identity (TMSI) and International Mobile Subscriber Identity (IMSI). IMEI is a unique number used to identify a valid device in the network. The TMSI is a temporary identity designed in UMTS to protect user’s identity in radio access path. The IMSI is the permanent identity used to uniquely identify a user in UMTS, and an identity catching attack is aimed at obtaining the IMSI of a user.

The Universal Mobile Telecommunication System (UMTS) is used for many commercial applications such as in E-commerce, mobile online banking and other mobile financial transactions [11], [12], in addition to its application to the Combined Mobile Information System [13],[14], in the health care industry. The high use of UMTS requires an increasing level of security and privacy measures. The security and privacy of UMTS user information is very important due to the sensitive nature of the communication data for the above stated applications [15].

Attack tree methodology is used to model the UMTS; showing the possible ways an attacker could launch an identity catching attack in UMTS. The attack tree methodology is a tree structure with the attacker’s objective at the root node and the possible ways to achieve the objective placed in the sub nodes [16], [17].

The rest of the paper is organized as follows: Section 1.1 gives an explanation of an attack tree methodology. Section 2.0 shows possible ways an identity catching attack could be launched on the UMTS, using attack tree methodology/counter measures. Section 2.1 explains the likelihood paths that could easily be compromised by an attacker. Finally, section 3.0 concludes the paper and gives some suggestions about future work.

1.1 The explanation of an Attack Tree Methodology

The attacker's objective placed in the root node of the tree model represents the general attack on the system. The various sub goals necessary to reach the objective are called leaf nodes. The attack tree also forms a convenient way to systematically categorize the different ways in which a system can be attacked [18], [19]. Then, the overall attack goal is further refined in the tree structure using AND and OR logical connections. By using the AND logical connection, an arc is used to connect lines, between a node to its sub nodes. AND logical connections indicate that both conditions of sister sub nodes must be met to continue in the attack vector. An OR logical connection is used to represent an OR node, a node without an arc between the lines of that node. OR logical connections indicate that either condition of the sub node can be met, without any additional condition, to continue the attack vector. Each level of the tree breaks the steps into more details until a realistic map on how an attacker can exploit a system is achieved [20], [21], [16], and [18]. An attack tree can also be represented with text, which communicates the same information as the graphical version, although sometimes textual descriptions are not easy to visualize. The attack tree methodology as is used in this research work to model attacks and will be used here to model an identity catching attack, one of the identified possible attacks against a user on the UMTS. The identity catching attack is a violation of user identity location confidentiality and traceability. Figure 1. shows a graphical representation of an attack tree model on possible ways an intruder could launch an identity catching attack, against a UMTS user.

1.2 Possible ways an Identity Catching Attacks could be launched on UMTS using an Attack Tree Methodology/counter measures

A. ***Passive Identity Catching***

The attacker waits passively for a new registration or a database crash to obtain a user's unencrypted International Mobile Subscriber Identity (IMSI) which is sent during the first rrcConnection request. This attack is possible because the Visitor Location Register/ Serving GPRS Support Node (VLR/SGSN) requires the Mobile Subscriber (MS) to send its identity in clear text during the initial rrcConnection request [22], [23], [24], [25] in order to identify the location of the subscriber to bill for services (making appropriate adjustments for location). In UMTS, a user (MS) is authenticated when registering for the first time with the network or when roaming to a network which is not a part of its home network. During that process, the VLR/SGSN requests a user to send its IMSI in clear text so that the subscriber will be identified and then authenticated by its Home Environment/Authentication Center (HE/AUC) enabling location tracking and smooth handoffs during roaming calls by the MS user. A simple radio listening device can record the IMSI number passively.

After identifying the subscriber (through the clear text IMSI number), the next step in enabling network access is to authenticate the subscriber and then negotiate ciphering and integrity capabilities of the MS. In order to do this the HE/AUC uses its copy of the secret key (K_i) to create a authentication token (AUTH) which only the MS can decrypt. When the MS receives this token (by way of the VLR/SGSN) the secret key (K_i) in the phone is used to decrypt several components of the AUTH which first authenticate the HE/AUC server and then authenticates the MS and enable an encrypted circuit for the MS traffic. A TSMI is then substituted for the IMSI by the VLR/SGSN to hide the subscriber location from others except for the VLR/SGSN [34][35] that maintains a mapping. The TMSI protects the user identity unless the MS roams to another service providers' area and thus is requested to send the IMSI in clear text again.

Passive identity catching in UMTS can be further minimized by using two temporal mobile subscriber identities. This mechanism allows a user to be identified on the radio access interface by the second TSMI that is chosen by HE and sent to the mobile station during the previous authentication of the MS by HE/AUC. This mechanism does not completely stop an attacker from launching passive identity catching attack because there are still chances of malfunctioning of the HE/AUC. Therefore, an IMSI will be resent and could be passively obtained by an attacker [22].

Regardless of the passive methods used to obtain the IMSI, if the subscriber identify is obtained this has little value to an attacker (other than initial user location traceability) since the location will be hidden when a TMSI is implemented. Moreover, if the phone and HE/AUC is configured to only roam within UMTS networks (and not in GSM networks) the risk is minimal. In UMTS networks, mutual authentication is implemented along with sequence numbers which are synchronized between the MS and the HE/AUC [34], [35], and [36]. These are used by the HE/AUC to create an encrypted authentication token (AUTH) that only the cell phone of the subscriber can decrypt (with their copy of the secret key, K_i). This effectively thwarts man-in-the-middle attacks and false base station attacks [34],[35],[36],[29]. In decrypting the AUTH the MS authenticates the server sending the AUTH and only then sends a message requesting encrypted access based on the Kasumi cipher (which is very resistant to cipher attacks with a time requirement of 2^{76} Kasumi encryptions using 2^{54} chosen plain texts)[37].

On the other hand, if the MS and HE/AUC are configured to allow roaming in non-EAP-SIM (Extensible Authentication Protocol) GSM networks, then depending on the capabilities of the roaming stations, situations may be created where the MS enables no GSM encryption (i.e. A5/0) or weak encryption (i.e. A5/1 and A5/2) rather than the A5/3 or Kasumi cipher. In these cases, several man-in-the-middle attacks are possible [29] if active methods are then used. In all these cases, such a passive attack could be used to launch an active attack on the phone using some of the attack methods discussed later in this paper.

Under the above conditions, allowing non-EAP-SIM GSM roaming in UMTS networks poses significant risk to the otherwise secure UMTS mutual authentication and subsequent implementation of Kasumi symmetric encryption and a TMSI. To mitigate these passive attacks in areas where there may be risk, turning the phone off until it is used minimizes the frequency of authentication to roaming stations (and subsequent sending of IMSI in clear text). If this is not an alternative, turning the phone off during transit mitigates multiple hand-offs to base stations during transit. Once at the new location the TMSI mitigates the IMSI exposure after the first activation of the phone at the new target destination.

B. Active Identity Catching

It is a form of Identity Catching attack which could be launched by an attacker through camping on false base station (1.2.1.1) or IMSI catching (1.2.1.2) or compromise of authentication data itself (1.2.1.3).

1. Camping on false base station: Camping on false base station attacks on pure UMTS networks and users are extremely difficult to launch as integrity protection of signaling messages and authentication of the serving networks avoids the attack [12]. This has been discussed earlier under passive attacks which escalate into active attacks. In pure UMTS networks, only the server in the home IP based network can construct the AUTH token (with knowledge of current sequence number and K_i) and only the same key in the subscribers cell phone can decrypt the token. One exception to this is unscrupulous sellers of cell phones who obtain the key during the process of selling and activating (the USIM) the phone.

UMTS also combines authentication token validity with integrity protection of signaling messages on the air interface between the MS and the network to thwart camping on false base station attacks [29]. A station pretending to be a base station simply cannot create the messages that a MS can authenticate and subsequently the MS will not request network service from false stations. While an active attack can obtain the IMSI (and thus initial location) an escalation of the active attack is prevented in pure UMTS networks.

The authentication token inhibits the replay of authentication data and also ensures the origin of authentication challenge. The integrity of the signaling messages protects the MS and the network from being fooled by an attacker not to use encryption in their communication [29].

When roaming in GSM networks the SGSN determines the GSM encryption used and computes keys derived from the UMTS keys it has. These derived keys are then forwarded to the GSM base station for use with the MS/GSM base station exchanges. Since there is no integrity and no encrypted secret that can authenticate the server (i.e. an AUTH token), a roaming MS cell phone is susceptible to a man-in-the middle attack in such GSM networks. Furthermore, if the traffic is encrypted with A5/1 or A5/2 then it can be compromised with no further effort on the part of the attacker [29] to obtain the data (the call) transmitted.

Given that most providers of network services want to maximize the sale of services, they will undoubtedly enable GSM roaming when not in a UMTS service area. This poses the same risk discussed earlier in passive attacks which escalate. While the user can take measures themselves (limiting the use of the phone) changes in GSM could also be made (such as changing the UMTS standard to enforce a more robust cipher mode command and integrity check. Without this enhancement to UMTS, a UMTS phone will be at risk whenever out of range of a home base UMTS system or a roaming UMTS base station (both of which force the MS to use UMTS authentication methods preventing man-in-the-middle attacks)[29].

UMTS users roaming in GSM network are vulnerable to false base station attacks. GSM networks do subscriber authentication and encryption of the radio of the radio interface between the MS and the network [29]. But an attacker with a valid authentication token from a real (UMTS) network, can use it to impersonate a GSM network to the user [29]. Apart from capturing the IMSI of the user, an attacker can launch a man-in-the-middle attack and also eavesdrop on the user’s communication. Due to the limited coverage area of UMTS, it is impossible for UMTS users to not to roam in GSM network. The statistic of global mobile coverage on wireless intelligence is shown in Table 1. It is taken directly form Global Mobile Market Share by Technology, 4Q08.

Table 1: Global Mobile Coverage statistic [31]

	CDMA (Family)	GSM	WCDMA (Family)	Other	%Global Connections
Africa	2.36%	96.12%	1.52%	0.00%	9.40%
America	9.32%	88.28%	0.91%	1.49%	11.33%
Asia Pacific	11.56%	80.39%	7.67%	0.38%	42.75%
Europe Western	0.01%	74.75%	25.24%	0.00%	12.62%
Europe Eastern	0.62%	95.11%	4.26%	0.01%	11.11%
Middle East	1.96%	94.79%	2.85%	0.40%	5.52%
USA & Canada	53.54%	33.45%	7.79%	5.22%	7.25%
Others	10.28%	81.08%	7.90%	0.74%	

The effective counter measure to camping on false base station attack is to disable UMTS users from roaming in GSM networks.

2. Active IMSI Catching : It has a sub node 1.2.1.2.1 that is UMTS debugging and testing tools as shown in figure 1. UMTS debugging and test tools such as UMTS Air Protocol Analyzer and UMTS Protocol Tester are applied to the air interface between User Equipment (UE) and Base Transceiver Station (BTS) in UMTS network. These tools are used by cellular manufacturers, network operations, developer and secret services around the world [32]. Since these tools are capable to obtain the IMSI and the equipment identity of the user, it can also be used in passive identity catching. An access control which will be strictly based the organization's polices should be put in place as a control measure. Also the staff with good reputations and trustworthiness should be assigned to the tools.

3. Compromise Authentication Data; In UMTS, the user's permanent identity is stored in the home environment/authentication center (HE/AUC). The HE/AUC does the authentication of the user for VLR/SGSN during rrcConnectionRequest and also when (a) the VLR/SGSN cannot identify the user when the user is roaming in a network apart from its own network, (b) a VLR database crash occurs, or (c) there is a malfunction in the VLR. The UE and the network are authenticated simultaneously during authentication and key agreement procedure (AKA) and this depends on the personal identity information and K_i on the IP based HE/AUC server.

Since UMTS (AUC) is an IP based network, adequate security measures should be in place to avoid unauthorized physical or logical access to the HE/AUC . The server(s) that house(s) the database should both physically and logically protected [33]. All the system and database patches should be installed and updated regularly: the systems should be hardened and highly resistant to attacks from IP based systems. Center for Internet Security (CIS) tools should be run against the HE/AUC to ascertain how secured it is. Only minimum privileges required completing a task should be given to the administrators that connect to the database. Access to the database should be controlled with access control list based on the organization's policies. Lastly, a firewall should implemented to protecting the HE/AUC. The above mechanisms provide an overview of security methods for server protection but the purpose of this paper is not to discuss them in depth.

II. THE LIKELIHOOD PATHS THAT COULD BE EASILY COMPROMISED BY AN ATTACKER

In figure 2, the shaded lines and attack tree components are used to show the likely paths that could be easily compromised by an attacker to launch an identity catching attack against UMTS users . From figure 2 passive identity catching may be more likely to occur through sub nodes 1.1.1 - 1.1.1.1 than 1.1.1.2, because the "IMSI is sent in clear during the first rrcConnection request, VLR database crash or VLR's inability to identify the TMSI"[12]. If an attacker was able to obtain both sub nodes 1.1.1.1.1 and 1.1.1.1.2, then the sub node 1.1.1.1 is already compromised. Sub node 1.1.1.2 might not be easily compromise, since an attacker must wait for the unlikely events of 1.1.1.2.1 or 1.1.1.2.2 to occur since servers holding the database normally have redundant systems to ensure their continual availability.

Active identity catching may most likely occur through (1.2.1.2) or when authentication data is compromised (1.2.1.3). The sub node 1.2.1.1, which is camping on false base station, might not be a likely path to be easily compromised because it is very difficult for an attacker to achieve. This attack node (1.2.1.1) is based on compromising the security mechanisms in the design of the UMTS (i.e. the validity of an authentication token, AUTH, and the integrity protection of the signaling messages) [29],[30]. If UMTS is properly implemented, it will be very difficult for an attacker to achieve 1.2.1.1. because they will not be able to decrypt the AUTH token. This inability will prevent authentication of the server, and thus will end the authentication attempt and as a result the

IMSI will (in these cases) not be sent (in pure UMTS networks). The sub node 1.2.1.2. is likely to be easily compromised since the sub nodes 1.2.1.2.1.1 and 1.2.1.2.1.2 are available in the market [12]. . As pointed out in Section 2.0, this tracking will be of limited use in pure UMTS networks as elevated attacks will be very difficult to achieve unless the MS roams in GSM networks.

Sub node 1.2.1.3.1 is entirely dependent on how secure the IP server which holds the database is protected by network architecture, firewalls and hardening of related server systems. Given that the data is on an IP network a wide variety of attacks are possible including many logical attacks, physical attacks and social engineering attacks.

The purpose of this paper is not to enumerate and discuss exploits to servers in IP networks as these exploits are discussed elsewhere. On the other hand, this research must enumerate this as a path and avenue of attack to the UMTS system.

III. CONCLUSION AND FUTURE WORK

The possible ways a UMTS user's initial identity confidentiality could be compromised by an intruder using identity catching attack is presented using an attack tree methodology despite the implementation of using TMSI to identify the user after the rrcConnection request. The likely paths that could be easily compromised by an attacker to launch an identity catching attack on UMTS users are highlighted and explained. All of the attacks to the initial IMSI can be elevated if the phone/network service is configured to allow roaming connections to non-UMTS networks where various attacks discussed in this research have proven successful. For a UMTS MS to roam in a GSM network can present real and substantial risk.

The following areas are suggested for future work on the UMTS in order to mitigate against the threat of identity catching attack. A mechanism should be implemented on the UE so that it can be able to authenticate messages received over the radio interface when roaming in the non-EAP-SIM GSM network (i.e. to authenticate the GSM server). In addition, the integrity protection mechanism should be modified to prevent an attacker from launching an identity catching attack on UMTS users roaming on GSM network by enticing them to camp on false base station. To avoid identity catching attacks the user identity (IMSI) should never be transmitted in cleartext by considering a PKI mechanism using the public key of the base station network provider to hide the IMSI and subsequent request for service from the initial request for service sent to the nearest VLR. A further enhancement to the above would be an enforcement of GSM A5/3 encryption bringing the required encryption of traffic to the same level as a UMTS provider (in cases where GSM roaming is configured).

Finally, the attack tree methodology has been successfully used to map the process of identity catching attack against a UMTS user. The explanation of the possible ways the attack can be launched, gives an insight on the measures that might be taken to thwart the attack from occurring. This paper has shown that UMTS phones roaming in GSM networks have several risks which pure UMTS networks do not have and these risks should be assessed in relation to the value of information transmitted by the MS.

REFERENCES

[1] Pierre Betouin, "UMTS Security" ESIEA- TOWARDS 3G NETWORKS, http://securitech.homeunix.org, June 20, 2006

[2] C.K Dimitriadis, "Improving Mobile Core Network Security with Honeynets"; published by IEEE Computer society, 2007 IEEE

[3] Network Architecture, TS 23.002, Third Generation Partnership Project, 2006; www.3gpp.org

[4] D. Fox, "Testing UMTS : assuring conformance and quality of UMTS user equipment" , Chichester,England; Hoboken,NJ: John Wiley, 2008

[5] J. Oudelaar, "Evolution Towards UMTS" IEEE 2002

[6] A. R. Mishra, " Advanced Cellular Network Planning and Optimization", Wiley, 2007

[7] M. Rahnema, " UMTS Network Planning, Optimization, and Inter-operation with GSM" WILEY, 2008

[8] 3GPP TS 33.120 (4.0.0), "3G Security; Security Principles and Objective", Release 4, March 2001

[9] 3G TSPP 33.102 version 3.7.0, "Security Architecture", Release 1999

[10] T. Flanagan, T. Coffery, R. Dojen "Radio Access Link Security for Universal Mobile Telecommunication System (UMTS)" department of Electronics and Computer Engineering, University of Limerick, Ireland, 2001

[11] Deutsche Bank Research. E –Banking Snapshot http://www.dbresearch.com, Dec. 2007

[12] M. Khan, A. Ahmed, A.R Cheema "Vulnerabilities of UMTS Access Domain Security Architecture" Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/ Distributed Computing, IEEE Computer society, 2008 IEEE

[13] A. Mustafa, K. Ramesh “Reviewing Security and Privacy Aspects in Combined Mobile Information System (CMIS) for health care system”, master thesis, department of Software Engineering and Computer science, school of Engineering , Blekinge Institute of Technology, Sweden. Thesis number : MCS 2007:13, June 2007

[14] O. Morger, U. Nitsche, S. Teufel, “Security Concerns for Mobile Information System in Health Care”, IEEE 1997

[15] C. Tang, D. Oliver Wu, “ Mobile Privacy in Wireless Networks – Revisited”, IEEE 2008

[16] ISSM 525 “Securing an E-commerce Infrastructure” http://course.concordia.ab.ca ; “Threat Modeling”; http://msdn.microsoft.com/en-us/security/aa570411.aspx

[17] T. Olzak “A practical A PracticalApproach to Threat Modeling”; http://adventuresinsecurity.com, March 2006.

[18] B. Schneier “Attack Trees” Modeling security threats, Dr. Dobb’s Journal, page 21-29, December 1999

[19] S. Mauw, M.Oostdijk “Foundations of Attack Trees”, Eindhoven University of Technology; Radboud University, Nijmegan, http://www.sti.uniurb.it/events/fosad05/attacktrees.pdf, 2006

[20] A. Aijaz, B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh and T. Leinmuller “Attack on Inter Vehicle Communication System – an Analysis” http://www.network-on-wheels.de/downloads/NOW_TechReport_Attacks_on_Inter_Vehicle_Communications.pdf

[21] M. Bauer “Practical Threat Analysis and Risk Management”,2002; http://www.linuxjournal.com/article/5567

[22] USECA final technical report, “UMTS Security Architecture”, June, 2001

[23] 3G TS 21.133 version 3.1.0, “Security Threats and Requirements”, December 1999

[24] A. Bais, W. T. Penzhorn, P. Palensky “Evaluation of UMTS Security Architecture and Services”, IEEE 2006

[25] 3G TR 33.900 v1.2.0 “A Guide to 3rd Generation Security”, January,2000

[26] http://news.bbc.co.uk/2/hi/technology/4738219.stm, January 2008

[27] M. Lei, H. Bi, Z. Feng, “Security Architecture and Mechanism of Third Generation Mobile Communication”, IEEE 2002.

[28] 3GPP TS 33.102, version 8.0.0 “3G Security; Security Architecture”, June, 2008

[29] U. Meyer, S. Wetzel “A Man-In- The Middle Attack on UMTS”, Computer – Communication Network; wireless communication, Philadelphia, Pennsylvania, USA, Wise’ 04, October,2004

[30] I. Pooters “ An Approach To Full User Data Integrity Protection In UMTS Access Network” 4th Twente Student Conference on IT, Enschede, January, 2006

[31] “Wireless Intelligence”, www.irelessintelligence.com, 5 March,2009.

[32] “Pioneering 3G Mobile Testing Solution”, www.prmti.com/products/ap6000.htm

[33] “Financial Information Security News” http://searchfinancialsecurity.techtarget.com/news/interview/0,289202,sid185_gci1293647,00.html,Jan 2008

[34] “UMTS Authentication and Key Agreement - A comprehensive illustration of AKA procedures within the UMTS system”, Graduate Thesis, Sivilingeniør Degree Information and Communication Technology, Jon Robert Dohmen & Lars Sømo Olaussen Grimstad 2001.

[35] “Evaluation of UMTS security architecture and services”, Abdul Bais Walter T. Penzhorn Peter Palensky, 2006.

[36] “UMTS security”, by K. Boman, G. Horn, P. Howard and V. Niemi 2002.

[37] A Related-Key Rectangle Attack on the Full Kasumi, Eli Biham, Orr Dunkelman and Nathan Keller, Technical Computer Science Department Technical Report, 2005.

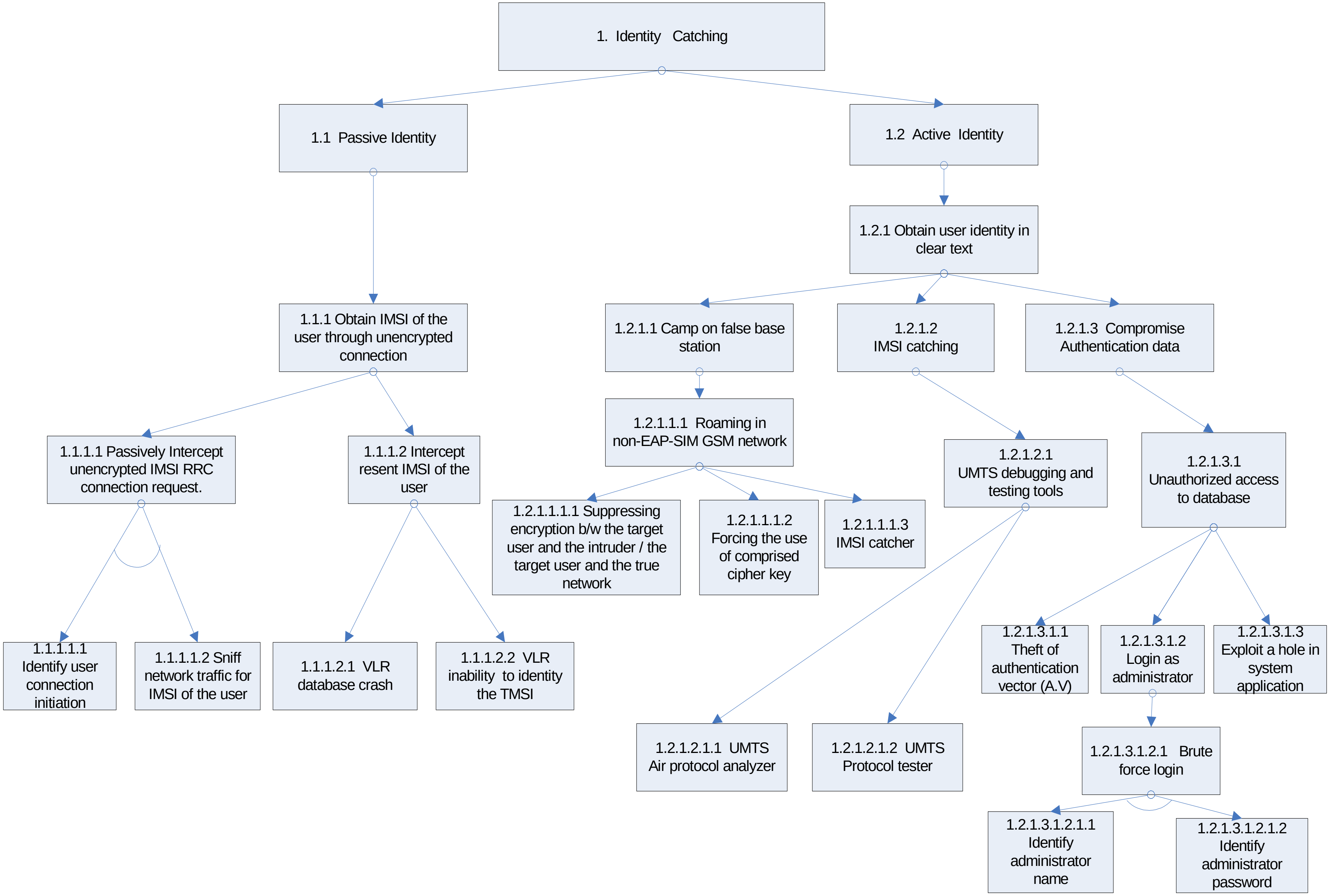
1. Identity Catching
1.1 Passive Identity
1.2 Active Identity
1.1.1 Obtain IMSI of the user through unencrypted connection
1.2.1 Obtain user identity in clear text
1.2.1.1 Camp on false base station
1.2.1.2 IMSI catching
1.2.1.3 Compromise Authentication data
1.2.1.1.1 Roaming in non-EAP-SIM GSM network
1.1.1.1 Passively Intercept unencrypted IMSI RRC connection request.
1.1.1.2 Intercept resent IMSI of the user
1.2.1.2.1 UMTS debugging and testing tools
1.2.1.3.1 Unauthorized access to database
1.2.1.1.1.1 Suppressing encryption b/w the target user and the intruder / the target user and the true network
1.2.1.1.1.2 Forcing the use of comprised cipher key
1.2.1.1.1.3 IMSI catcher
1.2.1.3.1.1 Theft of authentication vector (A.V)
1.2.1.3.1.2 Login as administrator
1.2.1.3.1.3 Exploit a hole in system application
1.1.1.1.1 Identify user connection initiation
1.1.1.1.2 Sniff network traffic for IMSI of the user
1.1.1.2.1 VLR database crash
1.1.1.2.2 VLR inability to identity the TMSI
1.2.1.2.1.1 UMTS Air protocol analyzer
1.2.1.2.1.2 UMTS Protocol tester
1.2.1.3.1.2.1 Brute force login
1.2.1.3.1.2.1.1 Identify administrator name
1.2.1.3.1.2.1.2 Identify administrator password

Figure 1. Identity Catching Attack Tree Model

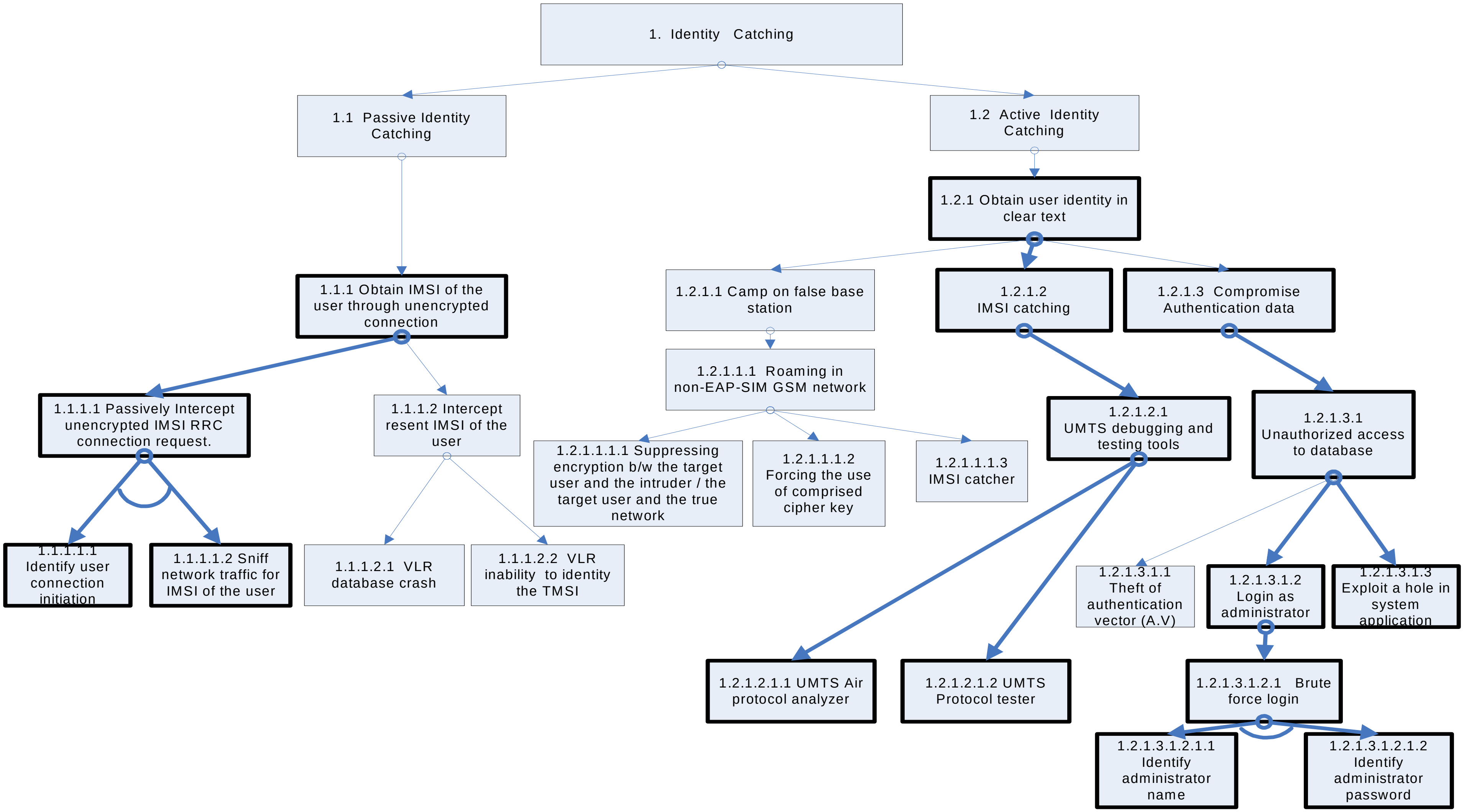
1. Identity Catching
1.1 Passive Identity Catching
1.2 Active Identity Catching
1.2.1 Obtain user identity in clear text
1.1.1 Obtain IMSI of the user through unencrypted connection
1.2.1.1 Camp on false base station
1.2.1.2 IMSI catching
1.2.1.3 Compromise Authentication data
1.2.1.1.1 Roaming in non-EAP-SIM GSM network
1.1.1.1 Passively Intercept unencrypted IMSI RRC connection request.
1.1.1.2 Intercept resent IMSI of the user
1.2.1.2.1 UMTS debugging and testing tools
1.2.1.3.1 Unauthorized access to database
1.2.1.1.1.1 Suppressing encryption b/w the target user and the intruder / the target user and the true network
1.2.1.1.1.2 Forcing the use of comprised cipher key
1.2.1.1.1.3 IMSI catcher
1.1.1.1.1 Identify user connection initiation
1.1.1.1.2 Sniff network traffic for IMSI of the user
1.1.1.2.1 VLR database crash
1.1.1.2.2 VLR inability to identity the TMSI
1.2.1.3.1.1 Theft of authentication vector (A.V)
1.2.1.3.1.2 Login as administrator
1.2.1.3.1.3 Exploit a hole in system application
1.2.1.2.1.1 UMTS Air protocol analyzer
1.2.1.2.1.2 UMTS Protocol tester
1.2.1.3.1.2.1 Brute force login
1.2.1.3.1.2.1.1 Identify administrator name
1.2.1.3.1.2.1.2 Identify administrator password

Figure 2. Identity Catching attack tree model emphasized likelihood paths that could be easily compromised by an attacker