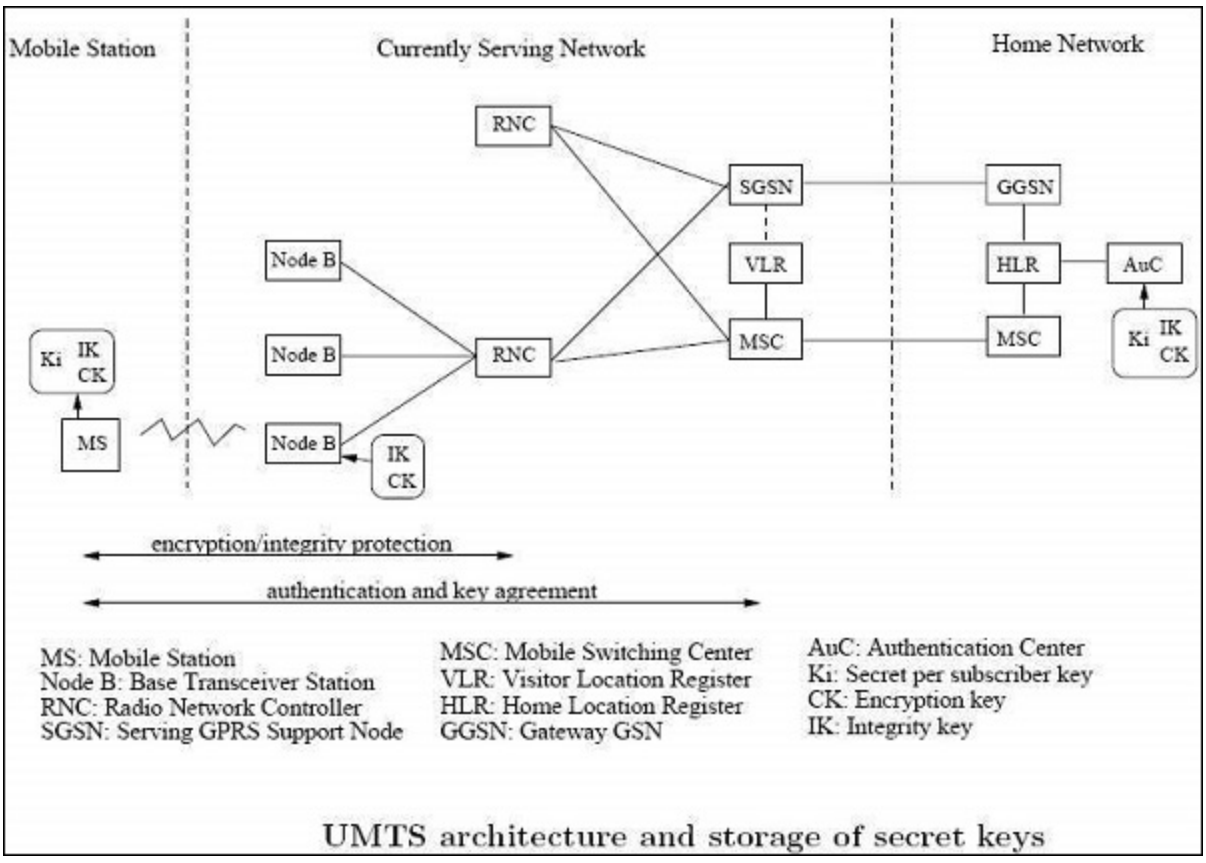
UMTS – Security and Privacy

Visitor Location Register (VLR) and SNB are used to keep track of all the mobile stations that are currently connected to the network. Each subscriber can be identified by its International Mobile Subscriber Identity (IMSI). To protect against profiling attacks, the permanent identifier is sent over the air interface as infrequently as possible. Instead, local identities Temporary Mobile Subscriber force (TMSI) is used to identify a subscriber whenever possible. Each UMTS subscriber has a dedicated home network with which it shares a secret key K_i long term.

The Home Location Register (HLR) keeps track of the current location of all the home network subscribers. Mutual authentication between a mobile station and a visited network is carried out with the support of the current GSN (SGSN) and the MSC / VLR, respectively. UMTS supports encryption of the radio interface and the integrity protection of signaling messages.

UMTS is designed to interoperate with GSM networks. To protect GSM networks against man-in-middle attacks, 3GPP is considering to add a structure RAND authentication challenge.



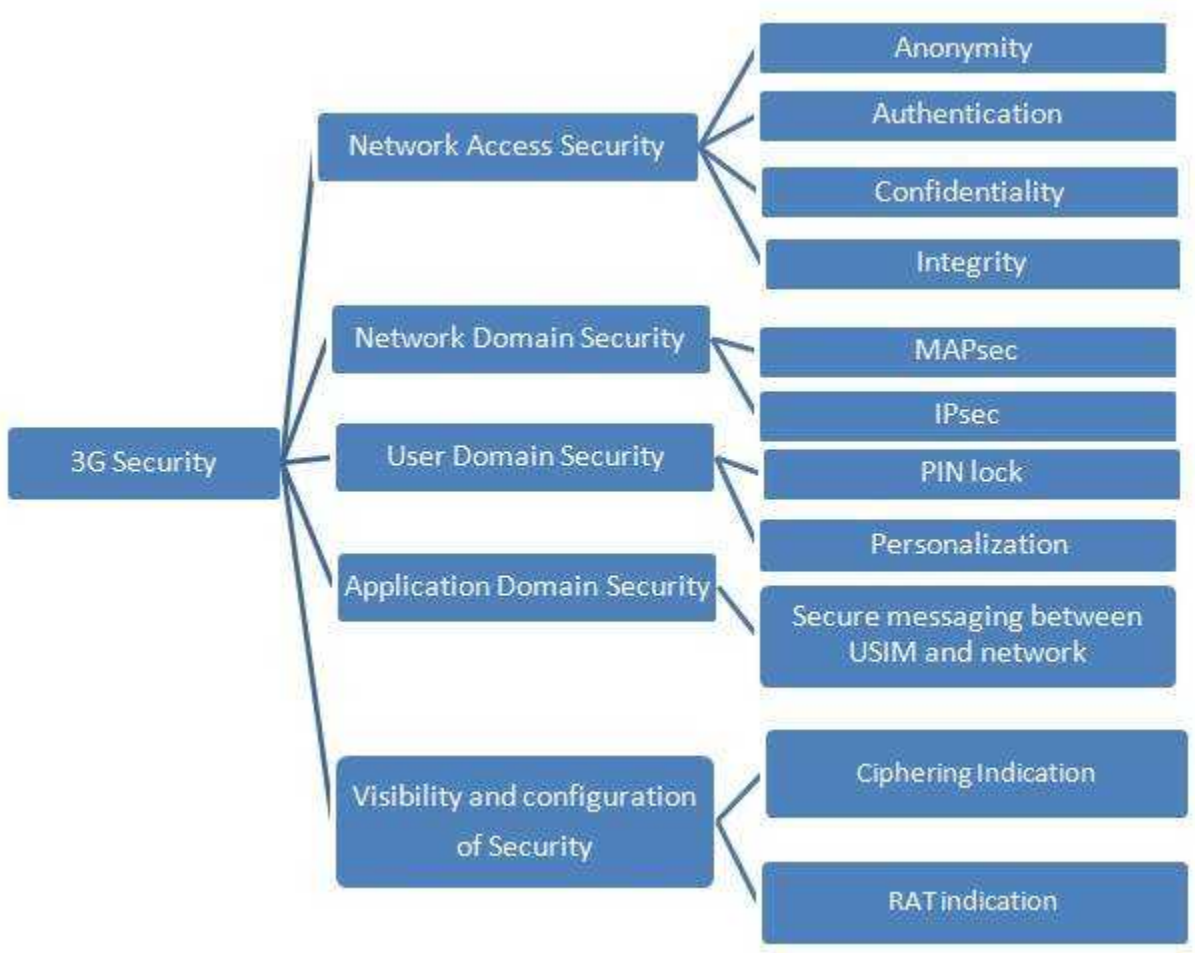
UMTS architecture and storage of secret keys

UMTS security is also referred as **3G security**. Five security groups exist in 3G networks as shown in the figure. Network Access Security helps protect air interface and also provide 3g

subscribers to access the 3g network securely. In UMTS authentication, key 'K' is shared between network and UE.

Five security groups exist in 3G networks as shown in the figure.

- Network Access Security
- Network domain security
- User domain security
- Application domain security
- visibility, configurability of security



Network Access Security helps protect air interface and also provide 3g subscribers to access the 3g network securely. In UMTS authentication, key 'K' is shared between network and UE. The network transmits random generated number 'RAND' and 'AUTN' in the message authentication challenge to the UE. AUTN makes it possible for UE to authenticate the 3g network. USIM generates response back to the network with ciphering and integrity keys. This helps network authenticate the UE. The major difference between gsm security and **3g security** is that network authentication was not possible with gsm compliant UE. This is possible in UMTS compliant UE.

What are the risks to your wireless network?

- Piggybacking. If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can use your connection. ...
- Wardriving. ...
- Evil Twin Attacks. ...
- Wireless Sniffing. ...
- Unauthorized Computer Access. ...
- Shoulder Surfing. ...
- Theft of Mobile Devices.

Wireless networks are subject to both passive and active attacks. A passive attack is one in which an attacker just captures signals, whereas an active attack is one in which an attacker sends signals, too. Passive attacks are exceedingly easy to carry out with wireless antennae and are undetectable. Any good security mechanism must start with the assumption that an attacker can see everything.

Open Authentication

- Open authentication allows any device network access.
- If no encryption is enabled on the network, any device that knows the SSID of the access point can gain access to the network.
- With WEP encryption enabled on an access point, the WEP key itself becomes a means of access control.

802.11 client authentication process

- 1. Client broadcasts a probe request frame on every channel
- 2. Access points within range respond with a probe response frame
- 3. The client decides which access point (AP) is the best for access and sends an authentication request
- 4. The access point will send an authentication reply
- 5. Upon successful authentication, the client will send an association request frame to the access point
- 6. The access point will reply with an association response
- 7. The client is now able to pass traffic to the access point

Open Authentication Vulnerabilities

- No way for the access point to determine whether a client is valid.
- A major security vulnerability if WEP or better encryption is not implemented
- Cisco does not recommend deploying wireless LANs without WEP encryption.
- When WEP encryption is not needed or is not feasible to deploy - such as public WLAN

deployments
- Higher-layer authentication can be provided by implementing a Service Selection Gateway (SSG).

Phishing

Phishing email messages, websites, and phone calls are designed to steal money or sensitive information. Cybercriminals can do this by installing malicious software on your computer, tricking you into giving them sensitive information, or outright stealing personal information off of your computer.

Types of phishing

Social Engineering - On your Facebook profile or LinkedIn profile, you can find: Name, Date of Birth, Location, Workplace, Interests, Hobbies, Skills, your Relationship Status, Telephone Number, Email Address and Favorite Food. This is everything a Cybercriminal needs in order to fool you into thinking that the message or email is legitimate.

Link Manipulation - Most methods of phishing use some form of deception designed to make a link in an email appear to belong to the spoofed organization or person. Misspelled URLs or the use of subdomains are common tricks used by phishers. Many email clients or web browsers will show previews of where a link will take the user in the bottom left of the screen or while hovering the mouse cursor over a link.

Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information (social engineering) about their targets to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.

Clone phishing - A type of phishing attack whereby a legitimate, and previously delivered email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender.

Voice Phishing - Voice phishing is the criminal practice of using social engineering over the telephone system to gain access to personal and financial information from the public for the purpose of financial reward. Sometimes referred to as 'vishing', Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Buffer Overflow

The Buffer Overflow Problem

- Buffer is a contiguous block of memory, of a fixed size
- Buffer overflow is a spill, fill over the top, or bounds.
- Buffers can be over flown with too much data, if not checked
- This can be exploited by malicious program to change the flow of control to the malicious code

Contiguous Memory
Flow of Execution
Bad Pointer
Bad Code
Over flown
Buffer

In and Out of The Stack!

- Stack is a contiguous block of memory
- Stack Pointer (SP)
- Bottom of stack is a fixed address
- PUSH and POP operations defined on stack
- Stack consists of logical stack frames
- Frame Pointer (FP)

Changing the Flow of Control

- Step 1 Injecting attack code into process memory of the vulnerable process
- Step 2 Overflowing a buffer in stack, that writes to memory of process to alter data that controls the execution flow

Changing the Flow of Control Attack Targets

- The return address, allocated on the Stack
- The old base pointer, also on Stack
- Function pointers, allocated on Heap, in the BSS, or Data segment, or on Stack either as local variable or as a parameter
- int (func_ptr) (char)
- Longjmp buffers, on Heap, in the BSS, or on Data segment, or on the Stack either as local variable or as a parameter
- Not going through the chain of return addresses

example1.c

- void function(int a, int b, int c)char

buffer1 5char buffer210

- int main()function(5, 1, 7)return(1)

example2.c

- void function(char str)char buffer 16strcpy(buffer, str)
- int main()char large_strlarge_str calloc(256, A)
- function(large_str)return(1)

Segmentation fault!!! Why?

Previous Work Static Analysis or Static Intrusion Prevention

- Looks for security bugs in source code ITS4
- Scans source code for known dangerous library calls
- Checks arguments to function calls and reports severity of threat
- Checks for other potential problems and race conditions
- Integer range analysis to locate potential buffer overflows
- Tracks allocated memory and possible length of strings
- This method is imprecise
- Someone has to keep an updated database of programming flaws to test for
- Examines program execution to determine whether buffer overflow occur during execution
- Compilers can add code to check bounds, or to arrange data structures in memory to cause hardware faults if bounds exceeds
- Purify detects memory errors, out-of-bound errors
- Does its own memory bookkeeping
- Fuzz tests programs
- Provides programs with large, random streams of characters
- Property based testing program satisfy certain properties
- Main Problem Need of test data that causes overflow
- Tries to solve known security problems

Prevention

- Non-executable stack
- Static source code analysis.
- Run time checking: StackGuard, Libsafe, SafeC, (Purify).
- Randomization.
- Type safe languages (Java, ML).
- Detection deviation of program behavior
- Sandboxing
- Access control …