points, along with mobile devices such as tablets and cell phones, and the threat to have information and data stolen or corrupted increases. A lost handheld device which set to access internal data and services can be a very serious security risk. Providing high levels of security is crucial within a provider's network. Applications traditionally supported in the desktop environment are penetrating the market for mobility. All sorts of mobile devices now use software just as commonly as any other fixed device. The growth rate is extremely fast. Many steps should be taken to ensure communication remains secure as new features, networks, and devices are added to the conglomerate. From 2010 to 2019 the worldwide shipments of laptops, tablets and desktop PCs (in million units) as shown in figure 1 [1]. Users are consuming more data every year, and as the reliance on the Internet continue to grow, so too will the demands for higher data capacity. The tremendous data demand by mobile consumers and operators commitment to provide quality of services and user experience have been the main driving forces of deployment of multiple cellualr networks augmented with small cells and wifi to cope with capcity increase demand and to provide relaible coverage throughout the service area. Mobile users should not worry about dealing with a comlicated procedure to access wireless networks seamlessly and securly.

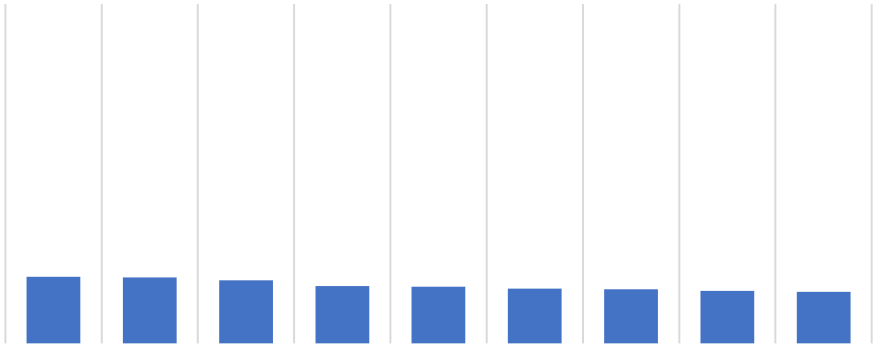

Figure 1) Number of Desktop-PCs (blue) versus Laptops (Black) versus Tablets (Grey)

Commercial:

Consumers are more demanding for services and applications. They depend on providers to handle the security component of their service just as much as the service itself. Recently, the number of security breaches from other industry segments have done harm to some organizations. A record of a security breach with leaked consumer information is devastating to operations and eventually, the bottom line. No organization wants to have a botched name from such an event. Are Mobile Network Operators (MNOs) taking the right approach? Taking a proactive stance to ensure infrastructure meets and exceeds the industry standard for security should be the ultimate goal. Other organizations who have taken a reactive approach to security threats suffered some serious losses. In some cases the damage may be irreversible. I will identify some problem areas in mobile network operations and some

approaches providers can take to optimize security to protect the ones who keep the lights on, the consumer.

A. Google

Industry giant, Google, captures a wide range of data in the form of online behaviour. In the development of their location-based service Google Maps, a fleet of vehicles (bicycles and cars) collected data in the form of photographs from the street level and uploaded images to a database that creates a virtual 360 degree street view. People, automobiles, and private residences were captured as well as payload data (personal email, passwords, and passwords) collected from unsecured wireless networks [2].

B. Social Media

Each social media platform establishes its own dynamic privacy policy and terms and conditions of use. There are various privacy threats that common users of social media are exposed to whether they are cautious of information broadcast in status updates or not.

1) Facebook: Of the estimated 7.2 billion people in the world [3], Facebook reports, as of September 30, 2014, an average of 1.35 billion monthly active users and 1.12 billion mobile monthly active users, collecting both personal and usage data [4]. The personal data (demographics, status, email, location, media, etc.) users willing disclose can be used maliciously to determine personal and private information. Third-party companies, allowed access to personal and usage data by Facebook and users, predict personality and actions then use this information to manipulate decision-making and influence behaviour such as purchases through targeted advertisements.

2) The Virtual Market*:*

availability of end users to see my emails, applications I use, or anything else is horrifying. Such software should be banned in the consumer market.

The United States of America, founded on the principles of a government for the people by the people, has strayed in its founding vision of a promised land in which citizens hold this government accountable for its actions. When addressing the nation, US Secretary of State, Hillary Clinton stated, "We stand for a single internet where all of humanity has equal access to knowledge and ideas." Clinton further states that it is "our responsibility to help ensure the free exchange of ideas goes back to the birth of our republic. The words of the First Amendment to our Constitution are carved in 50 tons of Tennessee marble on the front of this building. And every generation of Americans has worked to protect the values etched in that stone." Those words, although they promote equality in information exchange over a single internet, do not reflect the actions of the federal government, nor do those civil liberties protect people that exchange information regarding government interference in civilian privacy over this free internet for enlightenment [5].

A. NSA

Edward Snowden, during contractual work at National Security Agency (NSA) facilities, collected tens of thousands of classified documents pertaining to various government surveillance programs and leaked them to the public in piecemeal fashion in June of 2013. The NSA surveillance programs target different aspects and different areas of the Internet. The surveillance project, upstream, uses fiber-optic cables to collect communications. Another NSA surveillance project, MUSCULAR, processes data collected from the internal cables that link the data centers for Google and Yahoo.

1) Boundless Informant: Used as a data mining tool, Boundless Informant has "the ability to

Several organizations, including Verizon Business customers the ACLU (American Civil Liberties Union), filed lawsuits in federal court against the federal government on the grounds that the NSA used the Patriot Act to violate the freedom Americans are constitutionally guaranteed security from unwarranted search and seizures from the federal government in June of 2013. The ACLU has also filed a Freedom of Information Act lawsuit, which demands the government provide information about the use of Executive Order 12333 to intercept and collect the communications of Americans.

7) Piecemeal: Used as a data mining tool, Boundless Informant has "the ability to dynamically describe GAO's [Global Access Operations] collection capabilities (through metadata record counts) with no human intervention and graphically display the information in map view, bar chart or simple table [8]."

platforms. The IEEE 802.11 wireless networks have recently become so popular in the industry due to their ability to provide mobility, flexibility and security in the access to information and information resources. This report provides a detailed description and elaboration of the IEEE 802.11 Wireless LAN's security mechanisms and begins by providing an introduction to wireless networks, their vulnerabilities and how the IEEE 802.11 architecture can be used to employ security to the wireless networks. In this section, it is

during the association request between the client and the access point and hence an attacker may intercept the transmission and gain access to the SSID.

Attackers may also gain easy access to a default SSID, this happens when the client or

users to connect to the Internet through a wireless network, or connect to a user's mobile or

the establishment, maintenance and release of the bearers. In connection management, which is used for the establishment of the security and connection between the network and UE.

The access network

LTE access network, E-UTRAN comprises of network of eNodeBs, where there is no controller in E-UTRAN for normal user traffic. Hence the architecture of the E-UTRAN is flat, it is shown in figure [18].

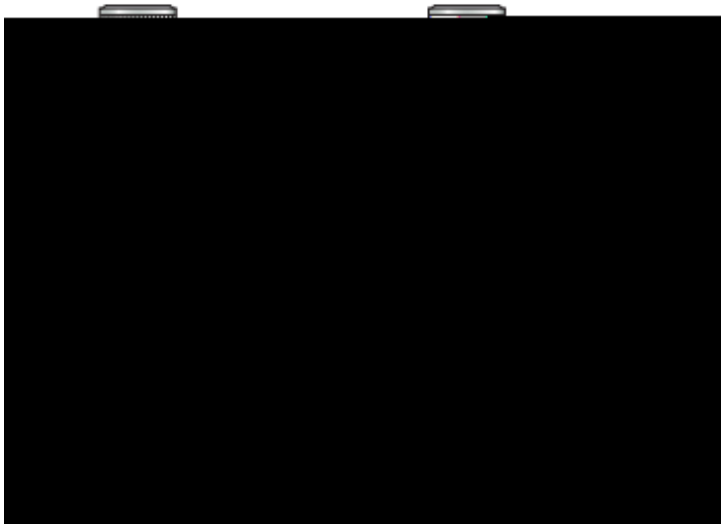

Figure 3) E-UTRAN architecture

From the above figure the eNodeBs are interconnected through the X2 interface and to the EPC by S1 interface- more accurately connected to the MME through the S1-MME interface and to the S-GW through the S1-U interface. The Access Stratum (AS) protocols are function between the eNodeBs and the UE.

All radio related functions are managed by the E-UTRAN in the LTE network, such as Radio Resource Management (RRM), security, header compression and network to the EPC. Radio Resource Management (RRM), which extends all the functions identified with the radio bearers including radio admission control, radio mobility control, radio bearer control, scheduling and dynamic allocation of resources to UEs in both uplink and downlink. Header compression, which is used to reduce the overhead of the IP packets by compressing headers of the IP packet. Security, which is encryption of the data that sent over the radio interface. All of the network functions are reside in the eNodeBs, these functions are responsible for managing multiple cells and all the radio control function incorporated into an eNodeB [18].

Security technology for SAE/LTE

The architecture design of LTE is different to an extraordinary degree from the scheme utilized by the existing 3G network. That distinction between the architecture design brings with it need to adjust and enhance the security function. The most essential necessity is that level of security in 3G network must be ensured in LTE [18]. The necessity additions and changes are made to fulfill security in LTE are listed below.

-

LTE security architecture

The complete overview of the LTE security architecture is shown in figure 4 [21]. The stratums in the network are identified and each stratums addressing the isolated category of the security threats in the LTE system.

Figure 4) Overview of the Security architecture

From the above figure there are five security feature groups in the LTE security architecture.

(I) Network access security: Network access

- It requires IMSI and IMEI should be protected confidentially.
- Authentication between the user and USIM, PIN is used to authenticate the user to access the USIM.
- Authentication between the USIM and terminal, this is used for SIM locked mobiles. In SIM locked mobile devices are stored the IMSI of the USIM.

(IV) Application domain security: It enables the UE applications and exchanging messages between the USIM and the network in a secure manner.

(V) Visibility and configurability of security: Which allows the user to know about the feature of the security is in operation or not and whether the services utilize and provision should depend on the security feature. This security provides following security functions:

- Access network encryption indication
- Security level indication
- User-USIM authentication enabling or disabling
- Accepting or rejecting incoming non-ciphered calls

Vulnerabilities in system architecture

There is an increase with the security risks in the 3GPP LTE networks because of its flat IP-based architecture. A directed path to the base station is provided by the all-IP network for the malicious attackers because of the various eNBs in the flat architecture are managed by an MME. Along with these security risks there is also an existing security risk because of the mobility of UE from an eNB/HeNB to a HeNB/eNB. Bandwidth consumption as well as signaling overhead authentication among the HN and the SN will arise due to the SN requests authentication vectors set from the HN when the UE remains in the SN for a long time and consumes its authentication vectors set for the authentication [39].

Security in a LTE Cellular System

In a LTE cellular security, the important scheme is the mutual authentication between the user entity (UE) and the evolved packet core (EPC). The mutual authentication between the UE and the EPC is achieved by using the Authentication and Key Agreement (AKA) procedure and it shown in figure 5 [21].

Figure 5) Authentication and Key Agreement

In Authentication and Key Agreement (AKA) procedure the authentication data generated by Home Subscriber Server (HSS) provided to the Mobility Management Entity (MME). Different session keys are used for the encryption and the integrity protection, which are derived by the integrity key (IK) and ciphering key (CK) that are generated in the AKA procedure.

In the LTE system, when UE interfaces with the EPC over the E-UTRAN, the MME represents the EPCPCoce(ov)1Nthe E

Figure

Figure 7) Hierarchical keys and method for key generation between entities in LTE

The USIM and Authentication Centre (AuC) in the key hierarchical system share secret information (key k) in advance similarly as the key shared in the 3G network.

- Mutual authentication between the network and user executed by using Authentication and Key Management (AKA), keys are generated for integrity protection (key IK) and encryption (key CK) and respectively keys are passed from USIM to mobile equipment (ME) and AuC to HSS.
- Key generation function used to generate K_{ASME} by ME and HSS from the key pair CK, IK based on the ID of the visited network. HSS in the network side ensures that K_{ASME} can be used by the visited network by building the correspondence of K_{ASME} key. To serve as essential data on the key hierarchy K_{ASME} is exchanged from the HSS to MME of the visited network.
- Keys K_{NASenc} and K_{NASint} for NAS protocol encryption and integrity protection between the MME and the UE are generated from K_{ASME}.
- MME generates K_{eNB} key when the UE is associated to the network and passes key to the eNB. The K_{UPsec} key for user plane encryption, the K_{RRCenc} and K_{RRCint} keys for

eNB for UEs in idle mode. Because NAS messages are transferred with idle mode UEs, NAS security associations are laid down between the UE and the MME.

After completion of UE authentication, K_{ASME} key is retained by the MME, which is the highest priority key of the key hierarchy in the visited network. By using K_{NASenc} and K_{NASint} keys the NAS security command manages the encryption and integrity protection algorithms for NAS communication between UE and the MME. Right now, the MME must find from which UE the authentication request message arrived so as to discover the right key to use for decryption and to verify data integrity. Nevertheless, a temporary ID called the GUTI (Global Unique Temporary Identity) introduced in LTE network to identify the UE instead of using the IMSI because the UE ID should be protected in the radio link. It is not possible to trace which GUTI the UE is using because of this GUTI changed periodically.

When UE enters92 reW*nBT/F4 10.56 Tf1 0 0 1 108.02 576.22 Tm0 g0 G[(t)5(he 1 108.02isdQq( )] TJETQq47(N

foom he mS urity asgorithms

- Inter-RAT handover: This handover occurs when the UE moves from E-UTRAN to different RAT

X2 Handover

This Handover occurs when User Entity (UE) moves from source eNB to the target eNB, where eNBs connected to the same MME. In this case a new key is provided to the target eNB in the core network and unknown key in the source eNB, these keys are used after handover. Next Hop (NH) parameter is the arbitrary value at the UE and eNB, this parameter is sent to the target eNB by the MME. If the source eNB is compromised by attacker have the ability to effect the services of the given UE at the target eNB however UE services will be secured from the following handover onwards by assuming the target eNB is not compromised. X2 handover mechanism shown in below figure 8 [24].

Intra E-

Security in IMS (IP Multimedia Subsystem)

There are three different types of attackers to attack IP Multimedia Subsystem (IMS). First type of attackers are script kiddies, they are curious but they don't ability to write advanced hacking programs on their own and their attacks are simple and initiated on the proposed security problems. Second type of attackers are well educated and their goal is to attack on financial issues. Third type of attackers have good knowledge but their attacks on the modern secret activities. The potential dangerous attackers are the IMS employees because they possess incredible knowledge of the system [27].

Security threats to IMS

The scope of the amount of data transformation, data links and problems with security are increasing in number because of the increase in IMS users, mobile subscription and web users. The security threats to IMS are categorized as follows.

External threats: Because of continuous growth in the mobile wireless technology IMS posed security threats are becoming increasingly critical. There are number of groups to support hacking in the IMS. The motivation behind this hacking is not only limited to the profit based but some of the organizations take hacking as prestige. These security threats largely on the databases of the corporate customers by listening through the network, and completed by destroying the material of communication system [27].

Internal threats: internal attacks are more dangerous than the external attacks. These attacks are posed by the employees, consultants, contractors and service providers inside an organization i.e. the information security is breaches by the insiders. These are range from the administrative mistakes and careless behavior

2. A security association and a secure connection between the UE and a Proxy Call Session Control Function (P-CSCF) is established by network access (Gm) for the Gm reference point protection.
3. The network domain security is allowed for the network domain (Cx) between HSS and Interrogating Call Session Control Function (I-CSCF) and between HSS and S-CSCF for Cx interface protection. TS 33.210 cover this security association.
4. Security between distinctive networks is provided by network domain (Mw) for Session Initiation Protocol (SIP) capable nodes. This security association is provided by TS 33.210 and applicable only when the P-CSCF resides in the Visited Network.
5. Security is provided within the network internally by network domain (Mw) among the SIP capable nodes. This security association enforces when the P-CSCF resides in the home network.

IMS access security-IMS AKA

The purpose of access security in IMS is to address the security between the IMS network and the UE. IMS access security provides following features [30].

Access security in the IMS is allowing the network to authenticate with the user and it provides authentication of network and the subscriber.

Access security provides IMS signaling confidentiality and integrity protection.

Access security provides policy control system, which is used to control the traffic to and from the UE by allowing the network.

The mutual authentication between the UE and the home network is provided by using the IMS AKA procedure. The UMTS AKA procedure concepts and principles are used as same in the IMS AKA procedure. The figure 13 [30] shows the IMS AKA procedure for an unregistered IMS user. The UE register with the IMS CN by sending SIP messages to the IMS CN, Then IMS CN is routed to the S-CSCF.

- Unauthenticated traffic on the links among the core network and the HeNB shall be filtered out.
- New users should be called for to confirm their acceptance ahead being joined to a HeNB.
- Authentication credentials at HeNB shall be stored inside a secure domain.

Security threats mitigation of HeNB

- Strong authentication algorithms might be used for authentication, confidentiality protection and integrity protection.
- Before securing association with the core network the integrity of HeNB must be validated.
- HeNB software and configuration updates must be in a secure wayay612 792 reW*n27.106.07 644.62 Tm0 g0 G

- Allowing MTC devices for very low energy consumption for data transmission to ensure long battery life for MTC applications [30].
- Allowing MTC devices for very low cost and they should have low complexity.
- Providing better coverage for MTC devices in challenging locations.
- Covering a very large number of MTC devices per cell [34

A3. MTC security communication among the MTC device and MTC interworking function for 3GPP access and between the MTC device and ePDG for non-3GPP access.

B. MTC security communication between the 3GPP network and MTC server/MTC user, MTC application can be further separated to:
   B1. Communication security among the MTC server and 3GPP network and it is further divided based on the MTC server, whether it is outside the 3GPP network and within the 3GPP network for the security aspects in MTC communication.
   B2. MTC security communication between the MTC application and 3GPP network.

C. MTC security communication between the entity outside 3GPP network i.e. MTC device/ MTC server device, MTC application and 3GPP network can be further divided to:
   C1. MTC security between the MTC server and MTC device.
   C2. MTC security between the MTC user, MTC application and MTC device [36].

Security issues in MTC

- The key issue in the MTC security is device triggering, which has three possibilities for the indication of the device triggering i.e. triggering indication when MTC device in detached state, MTC device in attached state and the device has a no connection to the PDN and MTC device in attached state. device as g0 0 612 C1e:nd as g0 0 612 C1e:nd v3 C1e:nd8

needs through the use of a single rechargeable battery power, without running for a long time. Because of the false network triggering in the network waste the power of the MTC device by awaking it when in detached state. So the false network threat is serious to the MTC devices compared to non-MTC communication [37].

Tamper attack: In this type of threat, the trigger indication which contain IP or TCP application port server that the MTC device should contact. If the IP or TCP application port server is tampered by the attacker, then MTC device may be rejected by the MTC server or establish PDN connection

Ensure that a MTC device can only communicate with the MTC servers of its subscriber and it is not possible to communicate with any other entities.

- The first point of entry into a secure operator network is MTC security GW could be used between the MTC server and core network.
- The use of USIM in the network must be restricted to the specific MEs/MTC devices.

Vulnerability in MTC security

- Security schemes for the communication among the MTC device and the ePDG and for non-3GPP access, which among the MTC applications and the MTC devices and among the MTC applications and for the 3GPP networks are lacks in the Machine-Type Communication (MTC).
- The MTC devices are vulnerable to various attacks such as protocol attacks, physical attacks, credentials compromise and the attacks to the core network.
- Signaling overhead incur between an HSS and the MME when a number of MTC devices are authenticate simultaneously [39].

Conclusion

Rapid growth in telecommunications and development of new technologies did not allow for proper growth and development of new privacy laws to protect users. In the US, there is currently no standard curriculum or program implemented in the public education system to formally teach and train users of the Internet and web enabled devices or promote safe and secure use of telecommunications systems and technology. Until a remarkable advancement in education and privacy laws protecting the essential liberties of civilians are implemented, telecommunications will continue to diminish privacy.

References

[1] Statista, “Forecast for global shipments of tablets, laptops and desktop PCs from 2010 to 2019 (in million units),” 2015.
[2] Dwyer, “Privacy in the Age of Google and Facebook," Technology and Society Magazine, IEEE, vol.30, no.3, pp.58-63, fall 2011.
[3] US Census Bureau. (2014) International Data Base World Population Summary. [Online]. Available: https://www.census.gov/population/international/data/idb/worldpopinfo.php
[4] Facebook. (2014) Statistics. [Online]. Available: http://newsroom.fb.com/company-info/
[5] Boundless Informant: NSA explainer – full document text, Guardian, June 8, 2013. [Online] Available: http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text
[6] S. Landau. "Highlights from Making Sense of Snowden, Part II: What's Significant in

[20] Alf Zugenmaier, Hiroshi Aono, “Security Technology for SAE/LTE”, NTT DOCOMO Technical Journal, Vol. 11 No. 3, PP 27-30.
[21] 3GPP TS 33.102 version 8.2.0 Release 8, “Universal Mobile Telecommu l ڎ d، m yn #