Wireless network security

There is a growing need to find lasting solutions on how to deal with security issues involving with wireless networks, in order to make them as secure as possible. The growth of the Internet has been an explosive since inception, and this has lead to a great increase in the number of portable/mobile computing and communication devices such as notebook computers and mobile phones, in recent years. As manufacturers constantly improve on the features, and general capabilities of mobile devices, the Internet also continues to get bigger and to improve, even at a faster rate than these mobile devices. In fact, the market for mobile computing and telecommunications is likely to overtake the market for fixed (conventional) computing and telecommunications, in the near future. This is because there has been a consistent growth in the demand for mobile devices for computing and telecommunications. [1]

Without a doubt, wireless technology was has been a very relevant and vital breakthrough in the computer and telecommunications world, and the Wireless third generation (3G) network is proving to be increasingly beneficial to many users of various networks. The main advantages of the 3G networks are that they provide a lot more interconnectivity and, a better and wider reach.

Wireless Local Area Network (WLAN) has also been advantageous. Some of the advantages of WLAN include the use of Broadband service with low costs and wide-reaching technology. Therefore, integrating 3G wireless networks with wireless local area network was invented, naturally, so as to get the best of both words of3G wireless network and WLAN.

[1] http://csrc. nist. gov/publications/nistpubs/800-48/NIST_SP_800-48. pdf

Background.

WLAN and 3G are two key mobile/wireless technologies, which have been identified to have great potential in terms of value to the customer. While 3G is a standard that defines technology that can provide high bandwidth wireless access over a large area and supports various services such as roaming, WLAN is a disruptive technology that provides higher bandwidth within small areas.

With WLAN getting integrated to 3G networks, there are several security threats that need to be considered. These are threats that are unique to such an integrated network as well as threats due to the vulnerabilities inherent in each network.

The 3 rd Generation Partnership Program (3GPP) has defined the standards for the integrated WLAN-3G network. The organisation takes into consideration several security issues, as part of its standardisation efforts. However, there are still some gaps in the security that can adversely affect service delivery and vulnerability.

From the security point of view, the network architectures are defined for both Roaming and Non-Roaming inter-working scenario. Additional components are specified to the 3GPP network architecture to facilitate inter-working such as Packet Data Gateway (PDG) and WLAN Access Gateway (WAG). The inter-working is based on UMTS Authentication and Key Agreement (AKA) authentication method. This requires a user equipment to run the USIM application. This means that WLAN user equipment is equipped with capability to use UICC smart cards.

The inter-working mechanism enables a 3G mobile network subscriber to access WLAN networks operated by different service providers. This also supports roaming scenarios.

Wireless local area network (WLAN) and 3-G devices enable users to carry their computers and communication devices around within their offices and homes, without having to handle any wires and without having to disconnect from the network when moving around. There is greater flexibility with these devices, due to less wiring, thereby increasing overall efficiency, and also reduced wiring costs. For instance, networks that use Bluetooth technology can be used for synchronization of data with network systems, and enable the sharing between of computer applications between devices. With Bluetooth functionality, there is no need for printer cables and some other connection equipment for peripheral devices.

3G network based security threats.

The key threats for 3G networks in perspective of integration of networks are:

- Wireless LAN customer who does not have access to 3G networks get access to 3G services without subscription.
- WLAN user gains access to 3G network and creates issues such as Denial of Service

- WLAN user gains access to 3G network and uses impersonation for using the service but charging other customers.
- Manipulation of charging when services like calls are transferred from one network to another.

Application and Data related threats.

- Collection of login details and personal details that are transmitted over the network by using sniffing tools and mechanisms, especially when sufficient transport security is not set.
- Manipulation of information used for user authentication or service access to gain access to unauthorised services or manipulation of billing.
- Extracts personal information that are used at other places such as credit card information.
- Obtain information about user such as permanent identity in the network.
- Virus attacks from WLAN devices to other devices in the network
- Trojans and malicious software passed from one end-device to another.
- For volume based charging model, a rogue partner can flood the user with garbage packets to increase the invoiced amount.
- Malicious programs on the user terminal that increases the traffic to certain sites or content to illegally increase the traffic.

Security Considerations for 3G-WLAN Integrated Networks.

The security framework for 3G-WLAN integrated networks consists of various layers. Each security layer is independent of the other layers. However, there needs to be an overall security scheme that connects all the security requirements together. Also, since some of the vulnerabilities can happen at multiple layers, a holistic approach and framework is required to address all the risks of the special network.

Authentication security at the user terminal.

The authentication scheme in the case of 3G-WLAN should be based on a challenge response protocol similar to the existing mobile communication authentication scheme. This requires that the authentication details in the user terminal to be stored securely on UICC or SIM card. This should support mutual authentication and security mechanisms such EAP.

Signalling and User Data Security.

The subscriber needs to have the same level of security as the mobile access that is specified for the 3G networks. This means that the WLAN authentication and re-authentication mechanisms must be at the same levels as for 3G USIM based access. It needs to support the maintaining session key verification and maintenance. Also the 3G systems should provide the required keys with sufficient length and levels of entropy that are required by the WLAN subsystem.

WLAN key agreement, distribution and authentication mechanism should be secure against any attacks by middlemen. The WLAN access technology between the user equipment and the access point/ network should be able to utilise the generated session keying material to ensure the integrity of the connection for authentication.

Privacy of User Identity.

The keys used by 3G AAA function that are used for the generation of temporary identities that is used for the communication between the network element and the user terminal should not be possible to recover. If it is possible to retrieve the keys, the permanent identity can be derived from any of the temporary identities. Also it should be possible to mask the different temporary identities corresponding to the permanent identity.

Security of the access interface.

The access interface between the user equipment and the network element should be protected against eavesdropping and all attacks on the security-relevant information. Sufficient cryptographic mechanisms should be employed to ensure adequate security, and at least 128 bit encryption keys should be used for the security system.

The interaction between the different endpoints of the local interface should be properly authenticated and authorised. Also the keys used for the security should not be shared across the local interface links and each interface should use unique keys.

Access of the user terminal and SIM remotely should be monitored such that the user can choose to allow or disallow the connection. Displaying of the information should be provided to the user to enable the user to take the decision.

Further, the USIM information should be secured when it is transferred across different networks such as 3G core network, WLAN network or any other networks involved.

Link Level Security.

Wireless link can be classified as the most vulnerable interface among all the interfaces in the 3G-WLAN integrated network. The link layer security provided by the WLAN network should be used for ensuring security at this layer. At this layer, the confidentiality and integrity of user data should be protected. In addition, any signalling information between the user equipment and the access point should also be secured. Another area of vulnerability is the key distribution, key validation, key freshness and key ageing.

Security of any Tunnelling.

UE can tunnel information to other devices in the Visited PLMN or the Home PLMN. When such tunnelling is employed, the data origin should be authenticated and integrity checks should be supported. Also the confidentiality mechanisms should be in place between the systems. As the 3G systems have defined security roles in tunnelling, the decision on allowing tunnelling is a function of the 3G network. It is essential to implement the right decision parameters such as level of trust in the WLAN access network or the Visited PLMN involved, capabilities supported in the WLAN user equipment in terms of security in tunnelling and whether the user is authorised for such services.

Privacy of User Identity.

User identity privacy ensures that none of the permanent subscriber identification information is send across the network in clear. This is based on temporary identities such as pseudonyms or re-authentication identities. Sufficient security procedures should be followed in generating, distributing, using and updating these identities. Also the period of maintaining a temporary identity is also important to prevent tracing of the identity. Various scenarios need to be considered for design of such a system such as:

- WLAN UE receiving more than one temporary identity from the AAA server
- Tunnel establishment
- If the identity privacy support is not activated by the home network

Confidentiality Protection.

The confidentiality protection should consider different scenarios and network access options. The key scenarios are:

- In WLAN direct IP access: Here the function is implemented using the WLAN access network link layer.
- In WLAN 3GPP IP access: Here the integrity of IP packets that is sent through the tunnel between the user equipment and the network should be protected.

Research Points.

Authentication, Authorisation and Accounting are the most important factors in ensuring network security. There are various techniques available in various types of

network available for AAA. One example is UMTS-AKA in 3G network and EPA in wireless networks. Each of these techniques are suitable for the respective types of networks and considering the security requirements.

With the integration of networks, the characteristics expected of the integrated network are a combination of both networks. The integrated network is expected to work with the same simplicity and efficiency as a WLAN network but with the security implementations of a 3G network. However a 3G-network security introduces overhead on the network resources that are not desirable in the integrated network. Also when there is an access from one network to another, the overall security profile of the integrated network is that of the weaker part of the network, in this case, the WLAN network.

There is a need for the use of the AAA method, which is simple in operation in terms of the message handshakes required and delay introduced and at the same time secure enough to match the 3G network security requirements.

The objective of this research is to:

- Evaluate the current AAA mechanisms available in terms of its capability,

- Recommend the best option for WLAN-3G network in terms of the efficiency and the security effectiveness.

Methodology

The methodology for identification of suitable AAA function involves the following:

- Evaluation of the currently selected methodologies used – UMTA-AKA, WLAN-EAP

These protocols are evaluated in terms of the

- overhead required to handle the mechanism and
- strength of the method
- infrastructure required to support the system in terms of network elements.
- Identification of other methodologies used in other technologies and networks
- Profiling of the different technologies in terms of the capabilities, limitations and characteristics
- Establishment of minimum requirements of 3G-WLAN network
- Comparison of profile to the minimum requirements established and selection of methodologies
- Recommendation of modifications required in the methodologies to suit to WLAN-3G environment.

Research Tools.

Various tools and resources will be employed during the course of this research, including:

- Reference implementations of AAA functions.
- Simulation software for evaluation of the robustness and strength of the AAA functions.
- Standardisation documents that provide evaluation of the AAA methodologies.
- Commercial products that employ AAA functions; such as WLAN access points and WLAN user equipments.
- Software protocol analysers for checking the message flow and function.

Expected Results.

This research will aim at providing guidance to operators and vendors, on the use of AAA functions for 3G-WLAN networks. Specifically, the following results expected at the end of this research:

- Identification of suitable AAA function for use in integrated WLAN-3G networks
- Recommendations of modifications required for the current implementation of the AAA function.

References.

A Guide to Wireless Network Security: White Paper.

http://techlibrary. networkcomputing. com/rlist/920045790_12/sort_by/doc_type/IP-

Networks. html

Wireless Networks Evolution, Vijay Garg, 2002, Prentice Hall.

http://www. cs. columbia. edu/~charles/publication/ft-concept. pdf

http://fiddle. visc. vt. edu/courses/ecpe6504-wireless/projects_spring2000/report_sathyamoorthy. pdf

http://csrc. nist. gov/publications/nistpubs/800-48/NIST_SP_800-48. pdf

http://compnetworking. about. com/od/wirelesssecurity/tp/wifisecurity. htm

http://www. pcstats. com/articleview. cfm? articleID= 1489

http://www. practicallynetworked. com/support/wireless_secure. htm

http://www. windowsecurity. com/articles/Wireless-Network-Security-Home. html

http://computer. howstuffworks. com/wireless-network. htm

http://netsecurity. about. com/od/hackertools/a/aa072004b. htm

http://netsecurity. about. com/cs/wireless/a/aa112203_2. htm

http://www. networkworld. com/topics/wireless-security. html

Home

3GPP TSG Services and System Aspects, 3G Security: Wireless Local Area Network

(WLAN) Interworking Security (release 6), Technical Report, 3GPP TS 33. 234

V6. 5. 1, (2005-6), December 2005.

3GPP TSG Services and System Aspects, 3G Security: Security Architecture (release 6),

Technical Report, 3GPP TS 33. 102 V7. 0. 0, December 2005.

3G and WLAN Interworking Security: Current Status and Key Issues, International

Journal of Network Security, Jan 20063GPP TSG Service and System Aspects,

Feasibility Study on 3GPP System to Wireless Local Area (WLAN) Interworking

(release 6), Technical Report, 3G TS 22. 934 v. 6. 2. 0 (2003-09), Sept. 2003.