Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 9, September 2013, pg.70 – 79

RESEARCH ARTICLE

Safety Measures in Wireless Information Networks

K.V.N.R. Sai Krishna[1], CH. Krishnamohan[2]

[1]Department of Computer science, S.V.R.M.College, Nagaram, INDIA
[2]Department of Computer science, P.B.Siddhartha College of Arts and Science, Vijayawada INDIA

[1] kvnrsaikrishna@gmail.com, [2] km.mohan3@gmail.com

ABSTRACT

Both security and wireless communication will remain an interesting subject for years to come. They represent the need of ease of use and flexibility of communications in the computer world without jeopardizing the communicated content. This paper illustrates the key concepts of security, wireless networks, and security over wireless networks. Wireless security is demonstrated by explaining the main specifications of the common security standards like 802.11 WEP, WMAN, 802.11 WPA and WPA2. Moreover, it explains the concept of (Wireless Metropolitan Access Network) and its security specifications. Finally, it sums up with thoughts and suggestions about wireless security, along with a chosen example of the current proposals in wireless security.

KEYWORDS: *PANA; Wireless LAN; EAPO; RADIUS; Basic Service Set*

I INTRODUCTION

Security in computer world determines the ability of the system to manage, protect and distribute sensitive information. Data Security was found many years before the advent of wireless communication due to the mankind's need to send information (in war or in peace time) without exposing its content to others. The first and most known machine (Enigma) was used in WWII by the German military to encrypt their messages. The machine was something similar to a simple typing machine with a scrambler unit to obfuscate the content of the messages [Enigma] [NIST98]. From that time till now, many solutions to security threats have been introduced, and most of them were abandoned or replaced by better security standards. These ongoing changes promoted the security field to be a permanent hot topic.

This paper aims to give a better understanding of security measures and protocols available in the market, along with a brief analysis of each security scheme's weaknesses and points of strength. This paper starts with an introduction to security and wireless worlds to give the right background for understanding the evolution of security standards. A brief description about security standards in wireless LANs. WMAN 802.16 protocol and the current security schemes used with it. Since security in wireless networks is still a working progress, discusses one of the recent proposals to enhance current security standards, a protocol called PANA (Protocol for carrying Authentication for Network Access).

2. SECURITY AND WIRELESS OVERVIEW

An overview of security and wireless communications is presented in this section. Although this introduction will not cover all the aspects of both worlds, it will give a descent amount of information that allows the reader to go through the paper without the necessity of referring to other books or papers. A crash course in security for both wired and wireless worlds. The current wireless systems and infrastructures. Finally, a list of the common security threats and attacks are discussed

2.1 INTRODUCTION TO SECURITY

This section outlines some of the basic conceptions in the security world. It starts by defining the goals behind implementing security in the computer world. Then it discuss encryption and decryption concept, the implementation of both block and stream ciphers , and finally a brief description of the most common encryption standards.

2.1.1 SECURITY GOALS

Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories [Earle2005][Imai2006]:

Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

Secrecy or Confidentiality: Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) content and no one else.

Integrity: Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.

Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the quality of service they expect.

Block Cipher

In this method data is encrypted and decrypted if from of blocks. In its simplest mode, you divide the plain text into blocks which are then fed into the cipher system to produce blocks of cipher text. There are many variances of block cipher, where different techniques are used to strengthen the security of the system. The most common methods are: ECB (Electronic Codebook Mode), CBC (Chain Block Chaining Mode), and OFB (Output Feedback Mode). ECB is the basic form of clock cipher where data blocks are encrypted directly to generate its correspondent ciphered blocks (shown in Fig. 1). CBC mode uses the cipher block from the previous step of encryption in the current one, which forms a chain-like encryption process. OFB operates on plain text in away similar to stream cipher that will be described below, where the encryption key used in every step depends on the encryption key from the previous step[Chandra2005] [Edney2003] .

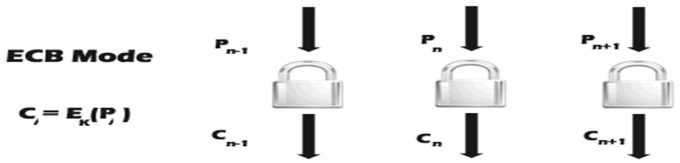

Fig.1 Block Cipher : ECB MODE

The other mode is called Self-Synchronizing Stream Cipher. In this mode, the state of Key Stream Generator (the Key Used for that instant of time) depends on the previous states of cipher text bits. The previous states number is fixed and defined by the algorithm. Self-Synchronizing method is more secure than the previous mode, but it is slower. Fig 2 below shows the process undertaken by self-synch stream cipher to encrypt/decrypt data.

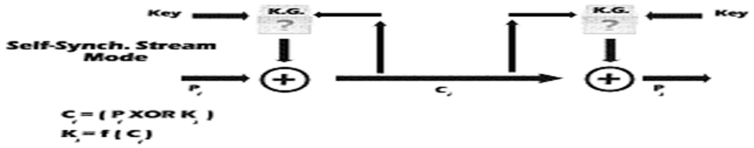

Fig.2 Stream Cipher : Self-Synch. Mode

Stream cipher has a well known advantage over block cipher because of its speed and simplicity of analysis. But in the same time it is a known fact that stream cipher is less secure than block cipher. That's why most of the recommendation of today's standards recommends using block cipher techniques over stream cipher ones [Chandra2005] .

2.1.2 WIRELESS LAN (WLAN)

Wireless LAN is simply trying to imitate the structure of the wired LANs, using another medium to transfer data rather than cables. This medium is electromagnetic waves which are mainly either radio frequency (RF) or infrared frequency (IR).

Wireless LANs consist mainly of two entities: clients or end-user devices and Access Points (AP). Clients' are equipped with devices that allow the user to use the RF medium to communicate with other wireless devices. AP functions like a regular switch or router in wired network for the wireless devices. Moreover, it represents a gateway between the wireless devices and a wired network. The basic structure

of a Wireless LAN is called BSS (Basic Service Set) shown in Fig. 3, in which the network consists of an AP and several wireless devices. When these devices try to communicate among themselves they propagate their data through the AP device. In order to form the network, AP keeps broadcasting its SSID (Service Set Identifier) to allow others to join the network.

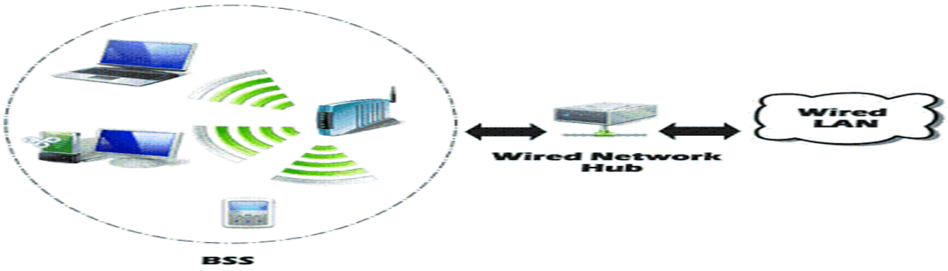

Fig.3 WLAN : BSS Structure

2.2 SECURITY ATTACKS

As mentioned before, the main difference between wired and wireless networks is the medium it transfers its data through. This difference made the burden of securing the network heavier. The broadcast nature of wireless networks makes it easy for everyone to attack the network if not secured, due to the absence of physical barriers, where the range of wireless transmission ranges from 300 ft to half a mile [Arbaugh2003] . The exponential growth of wireless networks add another obstacle on enhancing the network security. People tend to keep things the way they are instead of doing what is right. Also such enhancement of security is expensive in terms of time, money and effort that many users do not have or wish not to spend. Below is a list of the most common attack types known in both wired and wireless networks. Most of the security attacks and threats are listed under the following categories:

Traffic Analysis

In this type of attacks the attacker uses the statistics of network connectivity and activity to find information about the attacked network. Information includes: AP location, AP SSID and the type of protocol used by the analysis of size and types of packets[Welch2003] .

Passive Eavesdropping

Attackers in this type set themselves in sniffing mode, where they listen to all the network traffic hoping to extract information from it. This type of attack is only useful with unencrypted networks and stream cipher encrypted ones.

Active Eavesdropping

Similar to passive eavesdropping but the attacker tries to change the data on the packet, or to inject a complete packet in the stream of data.

Unauthorized Access

This type of attack is also known by many other names, such as war driving, war walking, and war flying[Earle2005] . This is the most common attack type where the attacker tries to get access to a

network that she is not authorized to access. Mainly the reason behind such attacks is just to get Internet access for free[Potter2003] .

Man-in-the-middle Attacks

In this attack, the attacker gets the packets before the intended receiver does. This allows her to change the content of the message. One of the most known subset of this attack is called ARP (Address Resolution Protocol) attacks, where the attacker redirects network traffic to pass through her device[Welch2003] .

DoS Attacks

DoS (Denial of Service) attacks are the hardest type of attacks to overcome. Attackers use frequency devices to send continuous noise on a specific channel to ruin network connectivity. It is known in the wireless world as RF Jamming [Welch2003] .

3. 802.1X : EAP OVER LAN (EAPOL)

The 802.1x standard was designed for port base authentication for 802 networks. 802.1x does not care what encryption techniques is used, it is only used to authenticate users. EAP (Extensible authentication Protocol) was designed to support multiple authentication methods over point to point connections without requiring IP [RFC3748] . EAP allows any of the encryption schemes to be implemented on top of it, adding flexibility to the security design module. EAPOL (EAP over LAN) is EAP's implementation for LANs[EAPOL] .

The 802.1x framework defines three ports or entities: Supplicant (client want to be authenticated), Authenticator (AP that connect the supplicant to the wired network), and Authentication Server (abbreviated AS which performs the authentication process from the supplicant based on their credentials). [Hardjono2005] [Earle2005] [EAPOL] The authentication server in the 802.1x framework uses RADIUS (Remote Authentication Dial-In User Service) protocol to provide AAA (Authentication, Authorization and Accounting) service for network clients [RADIUS][Imai2006] . The protocol creates an encrypted tunnel between the AS (Authentication Server) and the Authenticator (AP). Authentication messages are exchanged inside the tunnel to determine if the client has access to the network or not. Fig.4below shows the network layout.

Fig.4 802.1x Authentication

4. SECURITY IN WMAN 802.16

As mentioned before, the WMAN or WiMAX was proposed to solve the "last mile" problem. The 802.16 standard was released in Dec 2001. That gave the designers the time to learn from the mistakes made in 802.11 WEP security protocol. In the following sections the architecture of 802.16 will be discussed along with pointing out the security threats found in it.

4.1 THE 802.16 PROTOCOL LAYERS

802.16 protocol consists of four layers (Shown in Fig. 5):

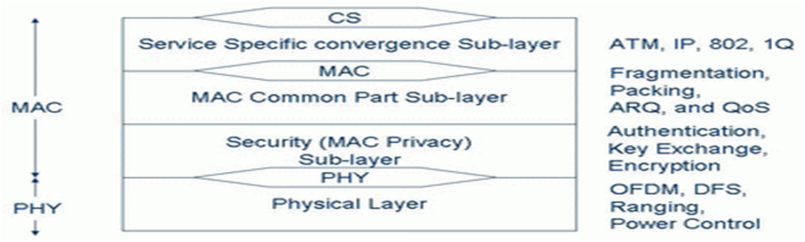

Fig.5 802.16 Layers

Physical layer:
802.16 protocol operates in three major frequency bands:

1. 10 to 66 GHz (licensed bands)
2. 2 to 11 GHz (licensed bands)
3. 2 to 11 GHz (unlicensed bands)

To support these three bands, the protocol specifies multiple physical layers.
Security sub-layer or MAC sub-layer:
This layer focuses on the security functions in the MAC layer. It consists of two component protocols:
1. Encapsulation protocol: This component describes how the authentication is processed and the types of algorithms to be used in encrypting packets between the BS (Base Station) and the SS (Subscriber Station).
2. Key Management protocol: This component describes how to distribute and manage connection keys. The default protocol used here is PKM (Privacy Key Management).
Each connection between the BS and SS or MS (Mobile Station) has a unique CID (Connection ID).
MAC common part sub-layer:
It is a connection oriented sub-layer, and it includes the mechanisms to request bandwidth. Authentication and registration is also a part of this layer functionality.
MAC convergence sub-layer (service specific convergence sub-layer):
Dividing the MAC layer into two sub-layers aims to solve the problem of having different protocols, where the common part sub-layer provides common functionality units to the above layer (MAC convergence sub-layer). The MAC convergence sub-layer implements different services on top of the common part sub-layer. It is also responsible about bandwidth allocation and QoS.[Cohen2003]

The security model in 802.16 ensures that specific requirements are supported. The first requirement is the ability of BS to identify the MS to allow it to access the network. Once done a master session key (MSK) is transferred securely between BS and MS. Secondly, WiMAX support a multicast and broadcast

service (MBS) that allows the BS to distribute data to a certain group of registered users. The system must be able to control access to the distributed content by using a per-group secret key. Finally, WMAN security system provides per-MPDU (MAC Packet Data Unit) integrity protection and reply protection.

After we have briefed about WiMAX (WMAN) architecture, and explaining the main functionalities of each layer and summarized the security techniques used to keep the traffic secure, in the next section we summarize the security threats found in 802.16 security system.

5. VIEW ON WIRELESS SECURITY

5.1 BEST PRACTICES

WEP has many flaws in its security system, but this is not the main reason why most of the wireless networks are attacked. Less than half of wireless networks are well configured and running correctly. In addition to that most APs default settings do not implement any type of encryption or authentication.[Manley2005] One of the best practices in home networks is to change the WEP key on a regular basis; this will weaken the chances of getting attacked. One of the most common techniques to test your network security is to use what attackers use to hack your network. There are many tools online that you can use, and they are available for different operating systems [WarDrive] .

5.2 SECURITY POLICY

Such techniques are not feasible for companies where many computers are attached to the network. In this situation a security policy must be described and written down to allow managers as well as technicians to react correctly to undesired circumstances [Manley2005] . It is not surprising that the main reason for security breaches is the human error factor or what is known as social engineering. APs can also be configured to stop broadcasting its SSID which will make it harder for the attacker to forge a rouge AP.

6. PROPOSALS

This Section discusses one of the recent proposals working to enhance wireless security mechanisms. The chosen protocols is PANA . PANA (Protocol for Carrying Authentication for Network Access) target is to improve the authorization between WLAN clients and AAA servers.

6.1 PANA

PANA is a new method to authenticate WLAN users over IP based networks. The goal of this proposal is to identify a link-layer protocol to allow host and network to authenticate each other for network access. The protocol runs between PaC (PANA Client) and PAA (PANA Authentication Agent). The purpose of this protocol is to provide the carrier for the existed security protocols. This protocol design is limited only to defining a messaging protocol that will allow authentication payload to be carried between the host/client (PaC) and an agent/server (PAA) in the access network for authentication and authorization purposes regardless of the AAA infrastructure that may (or may not) reside on the network[RFC4058] . As a network-layer protocol, it will be independent of the underlying access technologies and applicable to any network topology.PANA is intended to be used in situations where no prior trust between PAA and PaC exists. PANA defines four integral parts : PaC, EP (Enforcement Point) the physical point where inbound and outbound traffic filters are applied, and PAA which represent the access authority on the network.

In this if the client wishes to gain access to the network it has to go through a specific scenario. PaC must first discover the IP address of PAA, after that it starts sending authentication messages to authenticate itself on the network. Authentication can be granted from AAA server or from the local PAA depending on the network authentication infrastructure. Once the client is authenticated, PANA SA is created in both PAA and PaC. Furthermore, information filters are installed on the EP. Even after the client is authenticated, there might be other authentication messages exchanged between PaC and PAA during the connection session. Fig.6 below shows the authentication process in PANA.

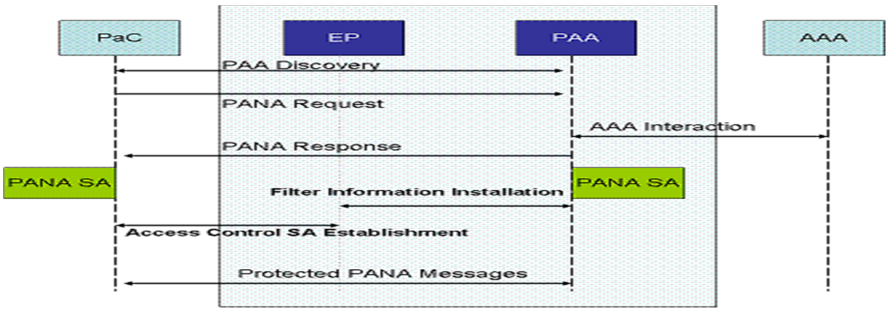

Fig.6 PANA Framework

It also provides a mechanism to prevent DoS attacks by using ISN (Initial Sequence Number), and cookie based authentication between PAA and PaC. It also works as a carrier to carry EAP packets..[RFC4058] [RFC4016] [Foresberg2005] PANA is still being developed and there are many discussion about its strength and flexibility. These ongoing discussions are aiming to provide a very reliable substitute to the 802.1x/EAP authentication scheme.

7. CONCLUSION

In this paper we reviewed how security in wireless data networks has evolved over the last years. We have discussed also how the difference in the data transfer medium between wired and wireless networks plays a key role in exposing the system to more possible attacks. Security hazards will always be around, they can only be avoided if the correct policies and standards are used. The 802.1 protocol promises to fix most of the security holes found in its predecessor WEP, but since the standard is relatively new, it did not have the proper period of time to be tested thoroughly. Only the future can tell us if the current standards are secure as they promise. Moreover, we mentioned some of the ways that can be utilized to improve the security of the wireless networks. PANA the new protocol proposed to work as a messaging protocol between network clients and network access authority was discussed . Security still evolves and it will remain a hot topic as long as there are ways to threaten data security.

REFERENCES

1. [Chandra2005]," BULLETPROOF WIRELESS SECURITY : GSM, UMTS, 802.11, and Ad Hoc Security (Communications Engineering) ,". Newnes 2005
2. [Imai2006]," Wireless Communications Security ,". Artech House Publishers 2006
3. [Welch2003] "Wireless security threat taxonomy,". Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society 18-20 June 2003 Page(s):76 - 83
4. [Edney2003]," Real 802.11 Security: Wi-Fi Protected Access and 802.11i ,". Addison Wesley 2003
5. [Earle2005] "Wireless Security Handbook,". Auerbach Publications 2005
6. [Hardjono2005]," Security In Wireless LANS And MANS ,". Artech House Publishers 2005

7. [Rittinghouse2004]," Wireless Operational Security ,". Digital Press 2004
8. [Prasad2005]," 802.11 WLANs and IP Networking: Security, QoS, and Mobility ,". Artech House Publishers 2005
9. [Manley2005] "Wireless security policy development for sensitive organizations,".Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE 15-17 June 2005 Page(s):150 - 157.
10. [Arbaugh2003] "Wireless security is different,". Computer Volume 36, Issue 8, Aug. 2003 Page(s):99 - 101
11. [Potter2003] "Wireless security's future,". Security & Privacy Magazine, IEEE Volume 1, Issue 4, July-Aug. 2003 Page(s):68 - 72
12. [Osorio2005] "Measuring energy-security tradeoffs in wireless networks,". Performance,Computing, and Communications Conference, 2005. IPCCC 2005. 24th IEEE International 7-9 April 2005 Page(s):293 - 302
13. [Chen2005] "Wireless LAN security and IEEE 802.11i,". Wireless Communications, IEEE Volume 12, Issue 1, Feb. 2005 Page(s):27 - 36
14. [Brown2003] "802.11: the security differences between b and i ,". " Potentials, IEEE Volume 22, Issue 4, Oct-Nov 2003 Page(s):23 - 27"
15. [Barbeau2005] "WiMax/802.16 threat analysis,". International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems
16. [WirelessLAN]; Wireless LAN ," http://cnscenter.future.co.kr/hot- topic/wlan.html [This page sums up all the organizations, papers, resources, … etc related to WLAN]
17. [Unofficial802.11]" The Unofficial 802.11 Security Web Page ," http://www.drizzle.com/~aboba/IEEE/ [This page tries to gather relevant papers and standards to 802.11 Security in a single place.]
18. [CITA]" CTIA : Wireless Internet Caucus: Standards & Tech ," http://www.wirelessenterpriseinfo.org/wic/standardsandtech.htm [Links to all groups that have been involved in the identification and development of standards and requirements for mobile data solutions]
19. [WiFiPlanet] " Wi-Fi Planet ," http://www.wi-fiplanet.com/ [The Source for Wi-Fi Business and Technology]
20. [ITtoolbox]" ITtoolbox Security Knowledge Base ," http://security.ittoolbox.com/ [ITtoolbox Security Knowledge Base provides the latest community-generated content from the IT market. Share knowledge with your peers and work together to form experience-based decisions.]
21. [Enigma]. "Enigma Machine", http://homepages.tesco.net/~andycarlson/enigma/about_enigma.html [Description about Enigma Machine and how it works]
22. [NIST98] "Security History", http://csrc.nist.gov/publications/history/ [Group of papers that explain security history in computer world]
23. [Sabc] "Glossary Terms", http://www.sabc.co.za/manual/ibm/9agloss.htm [Definition of security]
24. [TropSoft] "DES Overview", http://www.tropsoft.com/strongenc/des.htm [Explains how DES works in details, features and weaknesses]
25. [Cohen2003] "802.16 Tutorial" http://www.wi-fiplanet.com/tutorials/article.php/3068551 [Tutorial about 802.16 standard and about its security features]
26. [WarDrive] "War Driving Tools", http://www.wardrive.net/wardriving/tools/ [War driving tools to hack/test wireless networks for different OSes]
27. [bbwexchange] "WPA2 Routers List". http://www.bbwexchange.com/publications/newswires/page546-1160883.asp [contains a list of the WPA2 routers from different companies]

28. [Wireless80211] "802.11 standards" , http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm [Describe briefly 802.11 standards and their specifications]
29. [startawisp] " Shared vs Open authentication method", http://www.startawisp.com/index2.php?option=com_content&do_pdf=1&id=147 [Explains why shared Authentication is considered less secure than open authentication]
30. [RFC3748] "Extensible Authentication Protocol (EAP)", http://www.ietf.org/rfc/rfc3748.txt [RFC draft for EAP]
31. [EAPOL] "EEE 802.1X: EAP over LAN (EAPOL) for LAN/WLAN Authentication&Key Management",http://www.javvin.com/protocol8021X.html [Explanation of 802.1x, EAPOL]
32. [RADIUS],"RADIUS - Wikipedia, the free encyclopedia",http://en.wikipedia.org/wiki/RADIUS [Wikipedia definition and related resources about RADIUS]
33. [WPA],"Wi-Fi Protected Access - Wikipedia,", http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access. [Wikipedia definition and related resources about WPA]
34. [TKIP],"TKIP - Wikipedia", http://en.wikipedia.org/wiki/TKIP . [Wikipedia definition and related resources about TKIP]
35. [Microsoft-WPA] "Overview of the WPA wireless security update in Windows XP", http://support.microsoft.com/?kbid=815485 [Explains the security features in WPA]
36. [Tech-FAQ] "What is MIC ?", http://www.tech-faq.com/mic-message-integrity-check.shtml [Short definition for MIC and how it works]
37. [Tech-FAQ2] "What is WRAP ?",http://www.tech-faq.com/wrap-wireless-robust-authenticated-protocol.shtml , [Explaining why WRAP is not the recommended data transfer encryption standard for 802.11i]
38. [RFC4058],[Yegin, et al.] ,Protocol for Carrying Authentication for Network Access (PANA) Requirements
39. [RFC4016],[Parthasarathy], PANA Threat Analysis and Security Requirments.
40. [Foresberg2005] [Foresberg, et al.]. "PANA", http://people.nokia.net/~patil/IETF56/PANA/PANA_Solution_Slides_7.pdf

