Lightweight Authentication and Key Management on 802.11 Wireless Networks

Konstantinos Georgantas, Andrei Gurtov†
Helsinki Institute for Information Technology
Aalto University, Helsinki, Finland
† Centre for Wireless Communication, University of Oulu, Finland
Email: {Konstantinos.Georgantas, Gurtov}@hiit.fi

***Abstract*—Wireless Local Area Networks (WLANs) have experienced a significant growth during the last years because of the ever emerging and resource demanding applications. One of these applications is Voice over IP (VoIP), which is characterized by its time sensitivity. The current 802.11 standard addresses the most security vulnerabilities observed in WLANs but introduces a more cumbersome Link layer together with a significant signalling overhead. Thus the current standard poses constraints in such applications as far as mobility support is concerned. More specifically, the current authentication methods of 802.11 networks demand quite a lot of time comparing to what VoIP and other real-time applications can tolerate. In this paper, we propose the *Diet EXchange (DEX)* version of the *Host Identity Protocol (HIP)* which intends to provide the necessary IP layer elevated security mechanisms in order to face the challenge of *fast authentication* in WLANs. HIP introduces a radically new way of authenticating hosts in WLANs in only two message exchanges and therefore saves time during authentication. Two roundtrips are quite less than the eleven ones consumed by the 802.1X/EAP authentication framework. Furthermore, we propose a different hierarchy of the network components by slightly redefining the roles of the devices that take part into the entire link establishment process.**

I. Introduction

The technology advances of the last decade have contributed the most to the development of portable mobile devices. IEEE 802.11 standard is the major reason that these devices are used so broadly in every aspect of our life. Its main purpose is to provide WLAN connectivity and introduce mobility of devices. At the same time *Voice over IP (VoIP)* is gaining acceptance due to the cost effective communication it provides especially when compared with cellular billing services. Moreover cellular networks are bandwidth limited; thus VoIP poses a significant constraint when used over them. 802.11 networks are attractive to VoIP because of the high data rates they can provide and hence the uninterrupted services they can support.

However the above statement is not true in mobile environments in which mobile *STAtions (STAs)* are moving from one *Basic Service Set (BSS)* to another; especially when they experience a short dwell time within an *Access Point's (AP)* coverage area. It is also not true when a large amount of users closely (in time scale) enters for the first time an *Extended Service Set (ESS)*.

More specifically, host mobility introduces four serious problems [1]:

TABLE I
Network layer hierarchy before and after HIP

Application	Application
Transport	Transport
Network	HIP
	Network
Link	Link
Physical	Physical

- **Addressing** When a host attaches to a new AP it finds out that it has a topologically invalid address.
- **Location management** Changing the IP address to solve the above issue creates additional overhead as the mobile STA must also inform its peering nodes.
- **Session maintenance** Changing an IP address may also tear down active connections. IP addresses are often used as part of the connection identifier. Higher layers are sensitive to disconnections.
- **Security Handover** means also reauthentication and often reassociation.

Moreover network architectures in the name of backward compatibility and incremental upgrades supported from the beginning a multi-layered design. Thus the fact that wireless networks are by themselves insecure, due to the media they use, imposed to each and every network layer to perform similar authentication and authorization security mechanisms [2], [3]. In pure mobility cases the above implementation is simply inefficient.

In this paper we concentrate on the overhead that the current initial authentication process introduces to a mobile STA when the latter enters an ESS for the first time as well as the whole link establishment process. Fast authentication is what mobile stations need in order to experience real mobile services. We also present the use of a centralized authentication mechanism which could possibly allow for faster mobility during BSS handovers. Additionally, HIP can help in this direction as it presents a new cryptographic namespace which identifies hosts and therefore allows the Network layer to be decoupled from upper layers, as shown in Table I with security in scope. That means that the dual purpose of IP addresses as both host identifiers and locators is not present any more. Therefore, HIP gives solutions to problems like multi-homing, mobility

and security.

The rest of this paper is structured as follows: Section II describes the current authentication methods of *Robust Security Networks (RSNs)*. Section III describes the basic principles of HIP and introduces its two versions; *Base EXchange (BEX)* and DEX. Further on, Section IV explains the basic aims of FIA, presents some of the already proposed solutions in Section IV-A and describes the way that DEX could be utilized in the context of FIA in Section IV-B. Finally, Section V concludes the paper.

II. 802.1X/EAP AUTHENTICATION

As security is a major concern in wireless networks, in this paper we will consider only the use of RSNs as described in IEEE 802.11-2007 standard [4]. RSNs rely entirely on the *802.1X* authorization framework and the *Extensible Authentication Protocol (EAP)*. 802.1X is a port based network access control standard which provides the means for authentication and authorization of network devices [5]. The standard defines a set of entities such as the *Authenticator*, the *Supplicant* and the *Authentication Server*. More specifically:

- Supplicant is an entity that requests network access and needs to be authenticated according to its credentials.
- Authenticator is an entity that holds two authentication ports; the uncontrolled one that allows EAP authentication traffic to pass by and the controlled one that blocks any traffic until the Supplicant gets authenticated.
- Authentication Server (AS) is responsible for validating the Supplicant's identity and further informing the Authenticator about it.

EAP is a Layer 2 authentication protocol. There are quite different versions of it either proprietary or standardized. Some support one-way authentication and others mutual (that is authentication of the AS side) [6]. In an EAP exchange the two main parts that take part in it are the Supplicant and the AS. The Authenticator acts more like a relay between them, however note that it controls the controlled and uncontrolled ports. 802.1X/EAP procedure starts directly after the Open System authentication and Association. A generic (not version specific) EAP exchange includes the following steps:

1) The Supplicant passes the Open System authentication and Association phases. However the controlled and uncontrolled ports on the Authenticator are blocked.
2) The Supplicant initiates the EAP process by sending an EAPOL-Start frame to the Authenticator.
3) The Authenticator then sends an EAP-Request asking the Supplicant for its identity.
4) The Supplicant replies with an EAP-Response and provides the Authenticator with its identity in clear text. The uncontrolled port unblocks.
5) The Authenticator encapsulates the EAP-Response into an Access Request packet and sends it to the AS.
6) The AS checks the Supplicant's identity in its database and sends to the Supplicant an Access Challenge packet.
7) The Authenticator acts as a relay and sends the EAP-Access Challenge to the Supplicant in an EAP frame.
8) The Supplicant hashes the received challenge and sends an EAP-Access Response back to the AS.
9) The Authenticator forwards the response to the AS.
10) The AS compares the hashed supplicant version of the challenge with the proper one and responses with an Access Response.
11) The Authenticator forwards an EAP-Access Response frame and the supplicant is authenticated if every previous step was completed successfully.
12) A 4-way Handshake takes place between the Supplicant and the Authenticator in order to derive the dynamic encryption key that will be used during the data exchange.
13) When every step has been completed the controlled port is unblocked and the Supplicant can obtain an IP by DHCP and start using the network resources.

The above 802.1X/EAP scheme is currently proposed by the 802.11-2007 standard yet without specifying which EAP version to be used. As it can be seen there are quite a lot of message exchanges until the Supplicant finally authenticates itself to the server and creates the appropriate session keys. The main drawback is that quite a lot of time is consumed in Authentication processes [7].

III. HOST IDENTITY PROTOCOL

The Host Identity Protocol (HIP) was introduced by Robert Moskowitz. Its main purpose is to separate the identifier and locator roles of IP addresses [8]. It is generally designed so that it provides end-to-end authentication and key establishment. HIP introduces a new namespace where only Host Identities exist. A Host's Identity can be represented by either a Host Identifier (HI) or a Host Identity Tag (HIT). HI is the public key of an asymmetric key-pair. However HI is not suitable to serve as a packet identifier because public keys' length varies. Thus the HIT is a 128-bit hashed representation of the HI. Its length as you may notice was chosen deliberately in order to make HIP compatible with IPv6 applications.

HIP traffic is using IPsec in Encapsulated Security Payload (ESP) transport mode. Therefore HIP provides end-host to end-host encryption by establishing a pair of IPsec ESP Security Associations (SAs), one for each direction. Note that the established SAs are bound to HITs therefore enabling dynamic change of IP addresses. SAs are identified by the Secure Parameter Index (SPI). There is also no HIP specific data packet format and traffic is transported as previously in IPsec ESP mode without introducing any HIP overhead [8].

A. The HIP Base EXchange (BEX)

The HIP BEX is a cryptographic protocol that uses a SIGMA-compliant *4-way handshake* in order to establish a *Diffie-Hellman (DH)* key exchange and a pair of *IPsec ESP Security Associations (SAs)* between two entities; the Initiator and the Responder [9].

As shown in Figure 1 the I1 packet initiates the 4-way handshake. The I1 packet contains the HIT of the Initiator and optionally the HIT of the Responder. The Responder replies with an R1 packet which contains a cryptographic challenge

that the Initiator is supposed to solve. The main purpose of this challenge is to make the protocol resilient to Denial of Service (DoS) attacks. The R1 packet also initiates the DH key exchange by attaching the Responder's public key and the DH key to the R1 packet. R1 includes a signature. This lets the Initiator to authenticate the Responder and at the same time allows the use of precomputed challenges. Then the Initiator also computes the DH session key and creates a HIP association with the derived keying material. The solution of the challenge is attached in the I2 packet together with the Initiator's DH key and its public authentication key. The Responder then verifies the solution of the challenge, computes the DH session key by using the Initiator's DH key, creates a HIP association and finally authenticates the Initiator. At the end it informs the Initiator about receiving the I2 packet by sending an R2 packet. After that the traffic starts flowing between the two entities [10] and the data traffic is encrypted by ESP as the two hosts exchanged *Security Parameter Index (SPI)* values in the I2 and R2 messages and established the appropriate SAs [11].

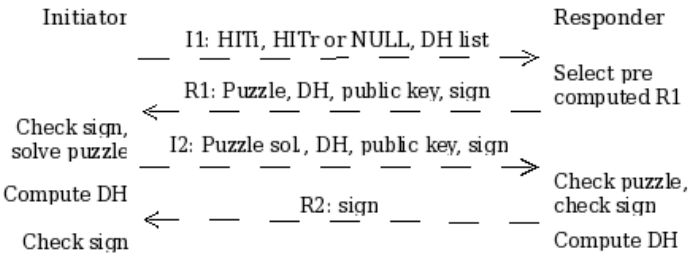

Fig. 1. HIP Basic EXchange

B. The HIP Diet EXchange (DEX)

HIP BEX can introduce some overhead in memory and processor constrained devices. Thus HIP DEX intends to provide the same level of security as BEX but with the use of as few as possible cryptographic primitives [12]. DEX is a cryptographic protocol similar in philosophy to BEX but with minor changes. The basic differences are summarized below:

- The DH key exchange is replaced by Elliptic Curve DH (ECDH) key exchange. RSA/DSA are also replaced by ECDSA [13].
- DEX makes use of AES-CBC encryption algorithm for providing CMAC instead of HMAC.
- The HIT in DEX is also 128 bits as in BEX but the way it is derived is different. DEX does not apply any cryptographic hash on the HI. Instead it uses the left 96-bit of an Elliptic Curve HI, the 4 bits of the HIT suite and the HIP IPv6 prefix that is also used by BEX.
- DEX does not provide anonymity.
- DEX cannot provide perfect forward secrecy.
- DEX was designed to operate in environments with high packet loss. Therefore it supports an aggressive retransmission practice for the messages sent by the Initiator. I1 and I2 messages should be sent every delta msec until the Initiator receives R1 or R2 packets respectively.

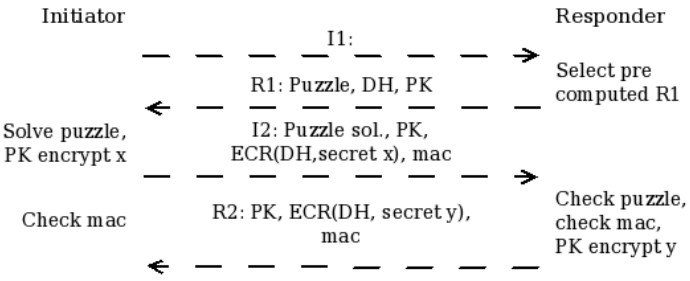

Fig. 2. HIP Diet EXchange

As shown in Figure 2, the first packet I1 initiates the HIP exchange as in BEX. The Responder replies with an R1 packet in which it attaches a cryptographic challenge and states the cryptographic algorithms it supports. In the next packet the Initiator presents the solution of the challenge and attaches also a DH key wrapper that carries a key for the Responder. This key is half of the final session key. At this point if there is a password based configured authentication the Initiator performs the appropriate actions in order to attach an authentication response to the I2 message. The I2 packet is MACed by the Initiator. The R2 packet contains a DH key wrapper for the Initiator which contains the other half of the final session key.

Note that there is no signature available in the above packets as with BEX. For HIP packet authentication purposes there is one DEX parameter in I2 and R2 packets which is a CMAC based message authentication code.

As stated in [12] DEX procedure is equivalent to 802.11-2007 Master and Pair-wise Transient Key (PTK) generation but in DEX it is handled in a single exchange. HIP DEX establishes two SAs. The first one for the DH derived key (Master key equivalent) and the other for the session key (PTK equivalent). The DH derived key is used to secure DEX parameters as well as authenticate the HIP packets [12]. The session key is used for traffic security and authentication.

Robert Moskowitz suggested that HIP and especially the DEX version has all the appropriate characteristics in order to be used as a key exchange mechanism in a MAC layer security protocol [12]. The contribution of this paper is the detailed design of the architecture.

HIP is also proposed to act as a mobility management protocol and seems to provide better results than MIPv6 [14] but this kind of HIP capabilities are beyond the scope of this paper which focuses mainly on the Authentication process.

IV. Fast Initial Authentication

FIA aims in three basic amendments of the IEEE 802.11 standard [15]:

1) Support of high number of simultaneously entering mobile STAs in an ESS.
2) Support of small dwell time (because of high velocity and small cell areas) within an Extended Service Area (ESA).
3) Secure initial authentication.

FIA's scope is only within the Authentication and Association processes, neither the AP Discovery nor the upper layer link setup such as DHCP. According to [16], eleven out of sixteen of the message exchanges during link setup are consumed on Authentication and two out of sixteen on Association processes. This makes a rough total of 80% of the message exchanges. Thus the reduction of the total roundtrips depends mostly on the Authentication process.

A. FIA proposed solutions

There are already some proposed solutions that could possibly face the above challenge [17]. The most of them rely on the existing authentication mechanisms and try to reduce the exchanged packets by modifying the 802.1X/EAP Authentication process. More specifically there is a lot of doubt about the existence of the Open System authentication which is considered to be a pre-RSNA Authentication process not acceptable anymore in contemporary wireless networks. The solution of piggybacking authentication information onto Association Request/Response messages is also proposed. Finally another proposal is introducing upper layer information on Association Request/Response messages in order to speed up the process of link establishment.

In our opinion the first solution is a reasonable one and more or less should be incorporated in the next standard. The only reason that Open System authentication still exists is the maintenance of backward compatibility with the IEEE 802.11 state machine [4]. The second solution seems capable of improving the whole Authentication process but it does not seem to provide a fine grained and performance acceptable solution towards a more effective authentication. Finally, the third solution does not really improve the Authentication process itself, rather it is an intermediate way to accelerate the link establishment procedure. But the most time-consuming process is *Authentication and Key Management (AKM)*. The main focus should be over AKM and ways to improve it.

B. HIP Diet EXchange based Authentication and Key Management

Having described all the background of the concepts involved in a HIP based Authentication process, it should be clear by now that there can be direct application of DEX in IEEE 802.11 standard for entity authentication and key generation. What remains to be defined is *how* HIP can be integrated in the current standard and act as a *Key Management System (KMS)*. Note that HIP's BEX version has been already tested in 802.11 networks but does not seem to achieve the desired results [3].

One of the main advantages of HIP (both BEX and DEX) is that it fits directly into the key model that 802.11 standard has introduced (MK, PTK, GTK). The first thoughts about integrating HIP into such a process is to let HIP datagrams run over 802.11 Authentication frames [18]. The MK and PTK keys would be delivered as already mentioned in Section III-B. The GTK could be delivered on an Association Response frame as a reply to an Association Request frame that contains a HIP UPDATE datagram. The HIP UPDATE can generally act as a rekeying mechanism when needed.

Hereby, we should mention that terms like mobile STA, Supplicant and Initiator may be used interchangeably from now on and depending to the context. The same applies for Authenticator and Responder terms.

A suitable deployment could consider a central wireless controller to act as a HIP Responder and its assigned APs as relays of traffic between the HIP Initiator and the HIP Responder [3]. The APs may introduce a Port based Network Access Control as the one in use by 802.1X framework for ensuring that only authorized Supplicants may have access to the network. By adding a new Information Element to the beacon and Authentication frames we can firstly announce the HIP capabilities of the network [3] and secondly distinguish HIP traffic. In this way only HIP traffic will be allowed to flow between the Initiator and the Responder until the Supplicant gets authenticated.

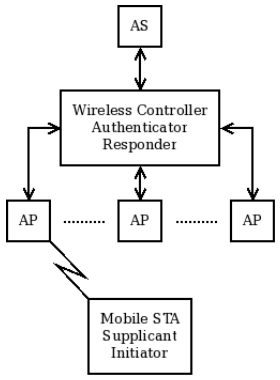

Fig. 3. HIP DEX authentication network architecture

The above scheme introduces a much simpler architecture and seamless handovers within the same ESS. More specifically the established HIP DEX SAs are preserved during handovers within the same ESS as the SA establishment is valid between the mobile STAs and the wireless controller. Thus the controller and only the controller, which has the appropriate level of trust by the AS, should be responsible for communicating with the AS. Hereby we assume that the Initiator and the Responder share long lived SAs and credentials with the AS and create SAs between them according to the described protocol. The SA between the Initiator and the AS is used for mutual authentication purposes. Figure 3 shows how this entities could possibly interact according to their roles.

The procedure should be rather simple. According to Figure 4 the basic steps are:

1) The APs transmits beacon frames that advertise the HIP capabilities of the network as well as the Responder's address (alternatively the mobile STA could perform active scanning and begin a HIP message exchange to Responder's link-local address or pre-defined multicast address [3]).
2) The Initiator performs Open System authentication and

Association. Both ports of the AP are blocked in the beginning.

3) The Initiator (acts as Supplicant) starts a DEX exchange with the Responder (acts as Authenticator) where the AP act as relay of traffic. The uncontrolled Port unblocks in order to let HIP traffic flow to the Responder.
4) The Responder after the reception of the I2 message communicates with AS in order to authenticate the Initiator and replies accordingly back.
5) Setup of ESP SAs.
6) Flow of ESP protected traffic (no HIP overhead).

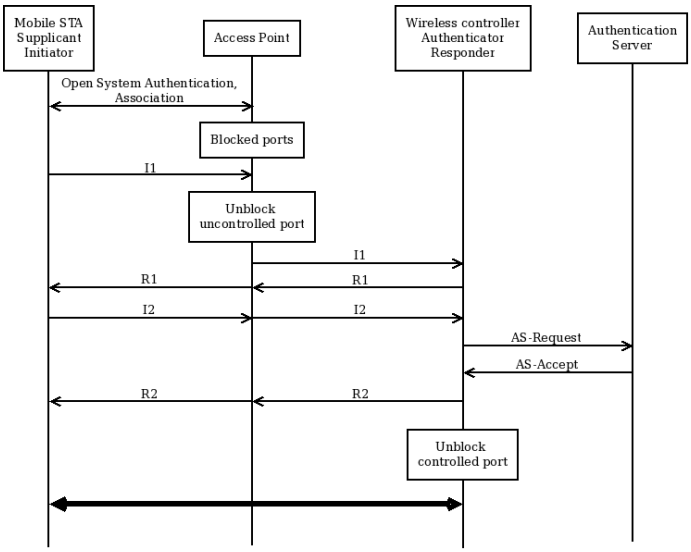

Fig. 4. HIP Fast Initial Authentication

The wireless controller could support tens of APs. However, in the case of ESS transition (that is translated to wireless controller transition) there should also be defined a HIP based mobility solution. Mobility could either include rekeying or not and should use the HIP UPDATE message in order to inform peers about the change of address.

In this way DEX certainly promises the reduction of the Authentication process messages, not to mention the fast transitions during ESS handovers. As shown in Figure 4, the Authentication process roundtrips are reduced to two and this is the reason we believe that DEX can provide delays that can be tolerated by most of the time sensitive applications.

V. Conclusion

In this paper we presented an alternative AKM system based on HIP DEX. By introducing the described network architecture there are a lot of benefits as far as the mobility process is concerned. We believe that intra-network handovers (BSS transitions) can be much faster and the inter-network ones (ESS transitions) are quite "cheap" in cost as DEX allows for a light AKM overhead. More specifically, the Authentication process can be up to five times faster as the authentication message exchanges can be reduced from eleven to two. Therefore the above concept could be utilized in cases where time sensitive applications demand a fast Authentication process. However, there are some security considerations that should be reviewed like the strength of the derived keys and the lack of perfect forward secrecy. Additionally the authentication of the Initiator is done by an externally configured password.

As part of the future work we plan to implement and test the above concept and compare it with other proposed solutions. We also intend to make the Authentication process more secure without changing its existing lightweight character.

Acknowledgment

This work was supported in part by TEKES as part of the Future Internet program of the ICT cluster of the Finnish Strategic Centers for Science, Technology and Innovation.

References

[1] T. Henderson, J. Ahrenholz, and J. Kim, "Experience with the Host Identity Protocol for Secure Host Mobility and Multihoming," *IEEE Wireless Communications and Networking, 2003*, pp. 2120–2125, 2003.

[2] J. Arkko, P. Eronen, and H. Tschofenig, "Quick NAP–Secure and Efficient Network Access Protocol," in *Proc. 6th International Workshop on Applications and Services in Wireless Networks*, pp. 163–170, 2006.

[3] J. Korhonen, A. Mkela, and T. Rinta-aho, "HIP Based Network Access Protocol in Operator Network Deployments," in *First Ambient Networks Workshop on Mobility, Multiaccess, and Network Management*, 2007.

[4] "IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," tech. rep., Dec. 2007.

[5] "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control," tech. rep., May 2010.

[6] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, Internet Engineering Task Force, 2004.

[7] H. Mano, "Fast Initial Authentication." [Online], Available at: https://mentor.ieee.org/802.11/dcn/10/11-10-0371-03-0000-fast-initial-a%uthentication.ppt, 2010.

[8] A. Gurtov, *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. WILEY, 2008.

[9] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423, Internet Engineering Task Force, 2006.

[10] R. Moskowitz, P. Jokela, T. Henderson, and T. Heer, "Host Identity Protocol draft-ietf-hip-rfc5201-bis-04," 2011. Status: Work in progress.

[11] P. Jokela, R. Moskowitz, and P. Nikander, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)," RFC 5202, Internet Engineering Task Force, 2008.

[12] R. Moskowitz, "HIP Diet EXchange (DEX) draft-moskowitz-hip-rg-dex-04," 2011. Status: Work in progress.

[13] R. Moskowitz, "Key Negotiation using DIET HIP." [Online], Available at: https://mentor.ieee.org/802.15/dcn/10/15-10-0412-06-wng0-key-negotiatio%n-using-diet-hip.ppt, 2010.

[14] P. Jokela, T. Rinta-aho, T. Jokikyyny, J. Wall, M. Kuparinen, H. Mahkonen, T. Kauppinen, and J. Korhonen, "Handover Performance with HIP and MIPv6," *1st International Symposium on Wireless Communication Systems*, pp. 324–328, 2004.

[15] H. Morioka, "Feasibility Study of FIA." [Online], Available at: https://mentor.ieee.org/802.11/dcn/10/11-10-0836-01-0fia-feasibility-st%udy-of-fia.ppt, 2010.

[16] H. Nakano, "Effectiveness of Reduction of Message Exchanges." [Online], Available at: https://mentor.ieee.org/802.11/dcn/10/11-10-0873-00-0fia-effectiveness-%of-reduction-of-message-exchanges.ppt, 2010.

[17] H. Nakano, "Fast Initial Authentication." [Online], Available at: https://mentor.ieee.org/802.11/dcn/10/11-10-0361-01-0000-fast-initial-a%uthentication.ppt, 2010.

[18] R. Moskowitz, "Summary and Comments, FIA Security Analysis." [Online], Available at: https://mentor.ieee.org/802.11/dcn/10/11-10-0980-00-0fia-fia-security-a%nalysis-bobm.pptx, 2010.