PLA-MIH: A Secure IEEE802.21 Signaling Scheme

Sumanta Saha
Department of Computer Science and Engineering
Helsinki University of Technology TKK
Espoo, Finland
sumanta.saha@tkk.fi

Dmitrij Lagutin
Helsinki Institute for Information Technology HIIT
Helsinki University of Technology TKK
Espoo, Finland
dmitrij.lagutin@hiit.fi

I. Copyright notice

II. Introduction

This presentation proposes a novel solution to secure the MIH signaling from various threats by using a network layer protocol named PLA. PLA aims to provide availability and accountability on the network layer and it is based on per-packet cryptographic signatures.

The paper is organized as follows. Chapter III briefly describes the Packet Level Authentication (PLA) protocol. The transport architecture for MIH is shown in Chapter IV. The security properties of the proposed solution are described in Section V, which is followed by evaluation of the scheme and conclusion in Chapters VI and VII.

III. Packet Level Authentication

Packet Level Authentication (PLA) [1] is a novel way to provide availability and protect the network infrastructure from several kinds of attacks, like denial-of-service (DoS) attacks, on the network layer. PLA is based on the assumption that per packet public key cryptographic operations are possible at wire speed in high speed networks due to new cryptographic algorithms and advances in semiconductor technology.

PLA aims to detect and stop malicious traffic as quickly as possible freeing resources to the benevolent traffic. A good analogy to the principle of PLA is a paper currency. Anyone can independently verify whether the bill is authentic simply by checking the security measures inside the bill like a watermark and hologram. There is no need to contact the bank that has issued the bill. Similarly, PLA gives every node a possibility to check whether the packet has been modified, duplicated or delayed without a previously established trust relation with the sender of the packet. Such packets can discarded immediately by any node in the network.

The PLA relies on IP header extension techniques to add an own header to the packet. The PLA header contains following fields. The trusted third party certificate corroborates the binding between the sender's identity and its public key. It also guarantees that the sender is a valid entity within the network. To reduce computational and bandwidth overhead, PLA utilizes identity-based implicitly-certified keys [2], where the sender's public key is calculated from the TTP certificate.

The PLA header also includes timestamp and sequence number fields that make possible to detect delayed and duplicated packets, which can be a sign of a replay attack. Finally, there is a cryptographic signature over the whole packet ignoring some IP header fields like hop limit, since these change during the lifetime of the packet. The signature protects the integrity of packet and together with sender's public key it offers non-reputability; the sender cannot deny sending the packet.

Since PLA includes signatures and public keys in every packet, it is not feasible to use traditional cryptographic solutions like RSA. To reduce the bandwidth overhead, PLA uses elliptic curve cryptography (ECC) [3]. A 163-bit EEC key used with PLA offers the same cryptographic strength as a 1024-bit RSA key [4]. An FPGA-based hardware accelerator has been developed for PLA [5]. According to simulations, an ASIC based on Altera's harcopy [6] technology built on 90 nm manufacturing process would achieve 850,000 signature verifications per second with a power consumption of just 22.4 W.

IV. PLA-MIH Architecture

The proposed solution utilizes PLA to transport MIH signal. PoAs and users are authorized by operators through cryptographic certificates. Such certificates contain a validity time

and rights field, which in this case are used to distinguish infrastructure nodes from MNs. PLA's signature over the packet provides integrity protection, therefore the receiver of the packet can verify that it is authentic and has originated from a trusted sender, e.g., from the PoA of a known operator.

Typical MIH signaling for handover decision comprises of two sets of messages. First set of messages corresponds to the information exchange between the mobile node and the information server of the MIH infrastructure. This information is required by the MN to make a decision about possible handover scenarios. After making a decision, further information exchange is possible for gathering more fine-grained information about the selected network. Then the second batch of message passing is started between the MN and the target network. In this phase, information collected form the previous phase is used to communicate and negotiate with the target network to make a network entry.

To make this handover scenario realistic, signaling among the MIH nodes needs to be secure so that no malicious attacker can tamper with the signaling. By using PLA as a network layer protocol for MIH signaling, it is possible to ensure secured communication inherently without any explicit AAA related roundtrip. As per the previous discussion about PLA, it is possible for the infrastructure nodes to have their own certificates issued by the network operator. The MNs can also receive a certificate from the operator. These certificates have different rights to indicate the difference in their role. By inspecting the certificates and the signatures in the messages packets, it will be possible for the nodes to verify the authenticity as well as the integrity of the message. The security architecture is based on the fact that the per-hop security feature of PLA ensures the authenticity of the sender of the packet as well as the integrity of the information using built-in certificates in each packet. The only overhead is the verification of the certificates and occasional contact with the TTP to verify the validity of the certificates. In the proposed architecture the certificate hierarchy is created in such a way that the communication to third party TTP is minimum. This decision is realized by a special Certificate Authority (CA) structure and collateral agreement among network operators.

A. Trust relationships

The proposal assumes following trust relationships in the system, which are described in Figure 1. Operators, in this case operator A and B, have their own certificate authorities (CAs). All operator's PoAs and users have a trust relationship with the operator's CA. In the example user is authorized to use the operator's A network, and therefore there is trust relationship between the user and the operator's CA. In order for the multiple operators to co-operate, they would need for form trust relationships between themselves. However, trust relationships do not necessarily need to be direct. Considering that the number of major operators is relatively small, the overhead for forming and maintaining trust relationships will not be significant.

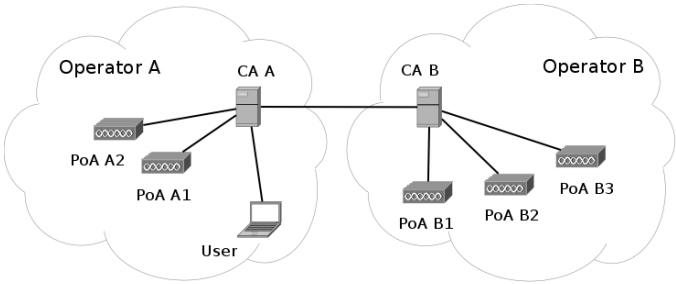

Fig. 1. Trust relationships in the proposed system

B. Bootstrapping

To make the certificate management for the user more flexible, two kinds of certificates are used. The user will receive a long-term certificate from its operator during, e.g., the creation of the contract. Such a certificate will have validity time of months or years and will be used to retrieve short-term certificates, e.g., through the operator's online service. These short-term certificates will have validity time of days or hours and will be used during the mobile node authentication.

If the short-term is lost or expired or lost, a new one can retrieved in an automated way using the long-term certificate. The same principles can be used to renew long-term certificate before its expiration. In an unlikely event that the long-term certificate has been expired or lost, the user should contact the operator off-line to retrieve a valid long-term certificate.

From the operator's point of view, the bootstrapping problem for infrastructure nodes is simpler. The operator will just grant certificates to its new access points, and configure access points to automatically trust the operator's CA.

C. MIH signaling over PLA

As discussed, all the PoAs and MNs of a single operator have certificates issued by that particular operator's CA. In the scenario where a single operator is managing several types of wireless networks and uses MIH to allow its clients to receive a seamless experience across the networks, the MIH signaling overhead can be kept at a minimum using PLA, since PoAs naturally trust in their own CA.

As illustrated in Figure 2, both IS informational signals as well as ES/CS notifications can be readily verified to be coming from the authorized source using the embedded certificate and the packet's signature. The figure is self explanatory and the certificates are verified by checking whether the issuer of the certificate is a trusted CA. The integrity is protected by the packet's signature, which covers all the fixed fields of IP and PLA header as well as the payload. In case of further confidentiality is required, it is possible to establish a Diffie-Hellman (DH) shared secret in the first few PLA packets.

On the other hand, the situation of MIH signaling across different operators offers additional challenges. Due to the fact that both MN and new PoA may not recognize each other's CAs, verification is necessary before trusting each other. The new PoA, to which the MN has decided to make a handover, is an infrastructure node and has an unlimited access to the

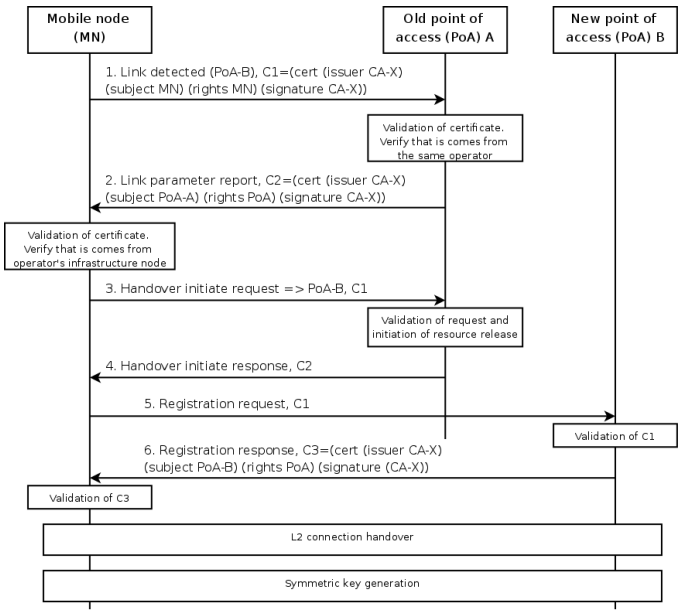

Fig. 2. MIH signaling using PLA: Single operator scenario

Internet. Therefore, it can verify authenticity of MN's CA by contacting its own CA. Whereas in case of the MN, it can notify the old PoA about the probable new PoAs and the old PoA can deliver the necessary credentials to verify the certificates of new PoA using IS messages. This scenario is illustrated in Figure 3. In the figure, the MN is about to perform a handover from PoA-X (old PoA) to PoA-Y (new PoA). The MN already have a trust relationship with PoA-X. When the MN decides to perform the handover, it notifies PoA-X and PoA-X in return delivers the necessary credentials of PoA-Y to the MN. After received the credentials, the MN can verify the authenticity of the packets from PoA-Y. On the other hand, PoA-Y can also verify the authenticity of the MN by contacting its own CA, unless it already knows that CA-X can be trusted.

In real-life scenarios there may not be many operators present in a particular area, therefore PoAs can store cryptographic identities of all major CAs. In that case, no inter-operator signaling is required for verifying the issuer of MN certificate. For additional security, PoA-Y may contact CA-X to verify whether the MNs certificate has been revoked. Since validity time of MNs short-term certificates used in the handover process is limited, revocation check is usually not necessary.

V. Security Analysis

The security threat and their solutions will be listed according to the affected node in the MIH system.

A. Threats to MN

In the signaling process there are several threats to the MN. These threats are listed here according to the analysis done in the IEEE WG for security analysis of MIH. Alleviations of those threats by using PLA are described alongside.

- **Identity Spoofing:** The identity of any MIHF of the infrastructure nodes such as IS can be spoofed by an attacker.
  - *Severity and possibility:* The severity of this type of attack is high as it will be possible to deviate the MN to handover to a potentially high cost and risky network by providing wrong information. Possibility of this type of attack is moderate because the attacker needs to have inside information about the network infrastructure. However, necessary authentication mechanism should be there to authenticate the information provider from MNs.
  - *Solution:* While using PLA as a network layer protocol for exchanging information, identity spoofing is not possible. PLA header and TTP certificate is enough to verify the identity of the sender as long as both parties trust the same TTP, which is the network operator's CA in this case.
- **Tampering by MITM attack:** Information sent by the IS can be tampered in the middle of the path by an attacker. This attack will result in malformed unreliable information and possibly denial of service.
  - *Severity and possibility:* Severity of attack is high as this attack can potentially deny the total service but the possibility of this type of breach in system is quite low because of the link layer security system involved in wireless communication. Nevertheless, inherent integrity protection is required for the messages.
  - *Solution:* Using PLA it is possible to verify the integrity of the message using the signature in PLA header and thus malicious packets can be blocked in the network layer without processing the contents of it.
- **Unauthorized information disclosure:** An MN can get access to unauthorized information from IS and use it for further attack to the infrastructure.
  - *Severity and possibility:* In case of no access control or authorization mechanism, the severity and frequency of this kind of attack is high. Possibility of using this information for other attacks makes this even more severe.
  - *Solution:* Access control and authorization mechanism is required to limit the access to information residing in IS. With PLA header this can be easily accomplished by using the "rights" field of the certificate to indicate access rights of a particular MN or IS.

B. Threats to IS

Possible threats to the IS involves all the threats similar to MS, such as identity spoofing, tampering and information disclosure and they can be alleviated in the same way as described above. There is also the possibility of flooding attack by several rogue MNs or botnets.

- **DoS attack by flooding:** An attacker can start a DoS attack on an IS by flooding it with numerous requests.

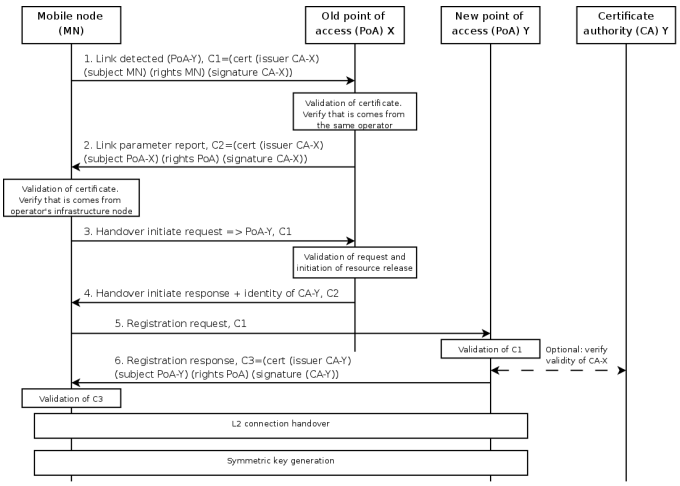

Fig. 3. MIH signaling using PLA: Multiple operator scenario

It can also be done with botnets built from a number of compromised MNs. In which case, it is even worse due to the fact that the MNs involved are also suffering.

- *Severity and possibility:* Severity of this attack is high. However, it would be quite difficult to arrange such an attack as it requires detailed knowledge of the network.
- *Solution:* As the IS is bound to process all requests from valid subscribers, it would not be possible cryptographically to thwart valid subscribers from a botnet from flooding the IS with requests. However, after identifying malicious behavior from a certain MN, the IS can report the MN's cryptographic identity to the CA which ultimately invalidate the certificate of the MN. On the other hand, to reduce attacks from MNs with self-signed certificates, the operator can impose a rule on the IS not to process any request without a valid certificate issued by the operator CA.

C. Threats to ES/CS

Alongside similar threats as defined in case of MN, ES/CS also bears the possibility of discloser of different type of information. Due to the fact that ES/CS are used for notifying events and commanding to perform handover, it is possible for attackers to monitor the ES/CS signaling and thus track any MN. This opens a serious breach to privacy.

- **Tracking information disclosure:** By monitoring the events and commands exchanged between the MN and the MIH nodes, an attacker can predict and profile a user's movement and activity.
  - *Severity and possibility:* Severity of this attack is medium. Most of the time the profiling of a user's full activity requires too much information than it is possible to capture. Moreover, to profile such information a continuous access to the signaling is necessary.
  - *Solution:* To prevent this kind of attack, confidentiality of signaling is necessary. However, PLA does not provide confidentiality as is. Nevertheless, it is possible to create a set of symmetric key in the network attachment phase of MIH with the new network using DH. Thus, later all the events and commands can be exchanged encrypted using the symmetric key.

VI. Evaluation

Utilizing PLA to secure media independent handover signaling offers a strong security and reduces the latency of the authentication phase. PLA-MIH relies on certificates issued and signed by operators, therefore the user or a malicious access points is not able to forge the certificate information.

Remote Authentication Dial In User Service (RADIUS) [7] is a widely used method for authenticating users in various networks. In RADIUS the user sends a request to the network access server (NAS) that in turn forwards the request to the RADIUS server, which grants or rejects the access. The user's password is encrypted using shared secret.

In PLA-MIH the mutual authentication can be performed simply by verifying the PLA certificate present in signaling messages. Communication with a centralized server, in this case with a certificate authority, is necessary only if the issuer of the certificate is not known. Therefore the latency of the authentication is reduced. In many cases the mobile node can determine trustworthiness of access points directly from their advertisement messages. Additionally, a certificate mechanism offers a better security and flexibility than a shared secret based solution.

In the proposed scheme access points may be attacked by flooding a large amount of PLA protected signaling packets. Since we assume that access points do not have a dedicated hardware for cryptographic operations, they would not able to verify the signature of every packet. This problem can be mitigated by allowing only a limited amount of handover request from the single user for a specific time frame.

A. Real-life deployment of PLA-MIH

The computational overhead of PLA-MIH is not significant, since the cryptographic signatures are only used for the signaling traffic. Therefore it is enough for PoAs to perform just few signature verifications or generations per second. The bandwidth overhead of PLA-MIH is also small, since the size of the PLA header is only about 1000 bits.

A proof of concept PLA implementation is available under GPL and BSD licenses [8] and it can be easily modified to support proposed PLA-MIH scheme. Additionally, a trust management system where operators certify their users and access points, needs to be created for PLA-MIH to work at its fullest extent.

VII. Conclusions and Future Work

We believe that utilizing existing PLA offers a good and flexible solution for MIH framework. In comparison with a

similar solutions like RADIUS, PLA-MIH reduces the latency during the MIH signaling. Furthermore, since the trust mechanism is embedded into PLA rather than using another application layer protocol to ensure security, use of PLA ensures a very simple and robust architecture. All the security threats to MIH as identified by IEEE802.21a workgroup can be alleviated successfully using PLA.

Additionally, using PLA for every payload packet in the network would add more security, and would allow operators to implement per-packet or per-bandwidth billing in a secure and flexible way. However, it would require dedicated hardware for accelerating cryptographic operations. Although this work theoretically proved the validity of the scheme and analyzed the security features of it, a detailed simulation of the scenarios is in order and the authors intend to perform to do it in future.

REFERENCES

[1] D. Lagutin, "Redesigning internet - the packet level authentication architecture," Licentiate's Thesis in Computer Science, Helsinki University of Technology, Espoo, Finland, 2008.

[2] B. B. Brumley and K. Nyberg, "Differential properties of elliptic curves and blind signatures," in *ISC '07: Proceedings of 10th International Conference on Information Security*, ser. Lecture Notes in Computer Science, vol. 4779. Springer-Verlag, 2007, pp. 376–389.

[3] V. S. Miller, "Use of elliptic curves in cryptography," in *CRYPTO '85: Proceedings of the Advances in Cryptology*, August 1985.

[4] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management - part 1: General, nist special publication 800-57," National Institute of Standards and Technology, Tech. Rep., March 2007.

[5] J. Forsten, K. Järvinen, and J. Skyttä, "Packet level authentication: Hardware subtask final report," Helsinki University of Technology, Tech. Rep., 2008. [Online]. Available: http://www.tcs.hut.fi/Software/PLA/new/doc/PLA_HW_final_report.pdf

[6] Altera, "Hardcopy structured asics: technology for business," 2008. [Online]. Available: http://www.altera.com/products/devices/hardcopy/hrd-index.html

[7] C. Rigney, S. W. Livingston, A. R. Merit, and W. S. Daydreamer, "Remote authentication dial in user service (radius)," RFC 2865 (Informational), June 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2865.txt

[8] "Packet level authentication (pla) library." [Online]. Available: http://www.psirp.org/publications