Distributed Authentication Protocol for the security of Binding Updates in Mobile IPv6

ANDREW GEORGIADES,
DR YUAN LUO,
DR ABOUBAKER LASEBAE,
PROF. RICHARD COMLEY
Department of Computing Science
Middlesex University
Tottenham campus, White Hart Lane, London, N17 8HR
UNITED KINGDOM
www.cs.mdx.ac.uk

Abstract: - Improvements have been seen with a jump from 2G to 3G in terms of security. Yet security issues persist and will continue to plague mobile communications into the leap to 4G if not addressed. 4G will use an architecture known as mobile IP. One particular security issue involves the route optimisation technique, which deals with binding updates. This paper introduces a distributed authentication protocol. It attempts to solve the security vulnerabilities of binding updates and at the same time over come the short falls of other security solutions by using currently existing technology without introducing any new hardware. The introduction of distributed authentication is aimed at alleviating mobile devices from processor intensive calculations while maintaining a high level of security.

Key-Words: - Mobile IPv6, Binding Updates, Security, Authentication, Location Privacy, Distributed protocol.

1 Introduction

Networking has always been vulnerable to a variety of attacks and the next generation of mobile communications is no different. 4G will be based on the transmission of Internet packets only, using an architecture known as mobile IP. This will feature many advantages however security is still a fundamental issue to be resolved. One particular security issue involves the route optimisation technique, which deals with binding updates [1]. This allows the corresponding node to by-pass the home agent router and communicates directly with the mobile node. The home agent has a static address while the mobile node's address changes every time it moves to a new location with a new point of attachment. The home agent keeps track of the mobile node's current address, so that if a correspondent does not know it, it may send the packets to the home address, which will forward the packets to the mobile node [2]. By bypassing the home address with the binding update route optimisation option, the speed of the delivery of packets increases. There are a variety of security vulnerabilities with binding updates [3].

2 Current Security Solutions

Numerous security solutions have been proposed and each have their advantages and disadvantages. The two main types of security are encryption and authentication. Encryption protects the confidentiality of the data and authentication allows users to verify that they are communicating with validated participants. Different authentication systems exist, such as Kerberos [4] that perform authentication by referring to a central authentication database to compare users credentials.

Other security components include hashes [5], digital signatures [6], address based keys [7] and cryptographically generated addresses [8].

More elaborate systems such as IPSEC [9] and RADIUS [10] based on AAA Authentication, authorization and accounting [11], require the utilization of a central authentication authority. These techniques may not be practical for a mobile environment, and could effectively reduce the users quality of service.

Security protocols, which have been specifically designed for the protection of binding

updates such as, Bake/2 [12] and CAM [13] are good but have flaws. The Trinity protocol [14] introduced a third node to aid in authentication but the addition of new hardware proved to be impractical. However, the two main techniques, which have practically become standardised for binding update security, are: Cryptographically generated addresses and return routability.

2.1 CGA

Cryptographically generated addresses [8] are IPv6 addresses, which are generated by hashing the owner's public key. The address owner uses the corresponding private key to assert address ownership and to sign messages from that address without PKI or some other security infrastructure. 62 bits of the interface identifier can be used to store a cryptographic hash of the public key.

$$(1),\ \text{Host ID} = \text{HASH}_{62}(\text{public key})$$

The CGA binds a users public key to an IPv6 address. The binding between the public key and the address can be verified by re-computing and comparing the hash value of the public key and other parameters sent in the specific message with the interface identifier in the IPv6 address belonging to the owner [15]. A major problem, which should be understood is that, an attacker can always create its own CGA address but will not be able to spoof someone else's address since the message needs to be signed with the corresponding private key, which is only known only by the legitimate owner.

The aim of CGA is to prevent stealing and spoofing of existing IPv6 addresses. CGA assures that the interface identifier part of the address is correct, but does little to ensure that the node is actually reachable at that identifier and prefix [15]. As a result, CGA needs to be used together with a reachability test such as return routability, where redirection denial-of-service attacks are a concern.

2.2 Return routability

Return routability tests whether packets addressed to the two claimed addresses are routed to the mobile node. The Return Routability Procedure gives the correspondent node some reasonable assurance that the mobile node is addressable at its claimed care-of address and its home address. Only with this assurance is the correspondent node able to accept Binding Updates from the mobile node [16]. The return routability test is the most effective way to limit bombing attacks of the mobile's new address. The correspondent only accepts the binding update if the mobile is able to return the hash of a secret value sent in a packet to the new location. This proves that the mobile can receive packets at the address where it claims to be [1].

Some malicious entities on the correspondent's local network may be able to capture a test packet but the number of potential attackers is dramatically reduced. The return routability test is complementary to CGA-based BU authentication, which does not prevent bombing of the home network [1].

3 Proposed Solution: Distributed Authentication Protocol.

The proposed solution attempts to improve to security of binding updates by adding an extra level of authentication. Most authentication systems operate on the premise of a third party is added to the system to provide the authentication requires. In mobile IPv6 for telecommunication devices, however, this is unnecessary. We assume that every mobile node needs to subscribe to a network provider, which in turn will provide the user with a home agent. This is the initial point of contact when an entity wishes to communicate with the mobile device as the home agent is constantly tracking and monitoring its current location.

Using today's mobile communications as a template we know that current systems use a sim card, which contains a sim number and the phone number. The device in use also has an IMEI, which is the hardware serial number. All of these are registered with the service provider. This information will be the basis for the new security solution.

There are three main aspects to the security protocol:

1. Cryptographically Generated Addresses
2. Return Routability
3. Authentication verification

The first two technologies are well-established techniques. Cryptographically Generated Addresses provide a reasonable assurance that that the address of the uses is indeed owned by them and not spoofed. Return Routability provides location authentication proving the communicating device is at the IP address claimed and again combats spoofing.

The third aspect of the security protocol provides solid device authentication and can be expanded to include user authentication in case of device theft.
Adding security features means that there will be an increase in processing power needed by devices. To aid with this burden the protocol proposes using a distributed authentication architecture. The home agent itself will perform part of the processing of the authentication data. This should provide several benefits such as lowering the overall time for the authentication to complete, as different parts of the authentication would occur on the mobile node and at the home agent.
This protocol is designed to be used with either two communicating mobile nodes or a mobile node communicating with a static correspondent. In either case two options are presented:

1. Distributed authentication
2. Standard authentication

The first protocol to be looked at is:

3.1 Standard and distributed authentication in mobile-to-mobile communication.

Firstly all nodes should be using cryptographically generated address, which have been previously created by the function discussed in [17]:

(2), Host ID = $HASH_{62}$(public key)

Message 1.
The mobile node MN attempts to contact the mobile correspondent node CN. It does not know its current location so it first contacts the correspondent's home agent HA2. The mobile node's public key MNK+, care of address CoA and home address HoA are sent to HA2 the correspondent's home agent. Message flows are shown in Fig.1.

MN ⟶ HA2: MNK+, CoA, HoA.

Message 2.
The correspondent's home agent forwards the data to the correspondent

HA2 ⟶ CN: MNK+, CoA, HoA.

Message 3.
The corresponding node compares the mobile node's public key with that of its claimed CGA address and determines if they match. If they do then return routability and device authentication will proceed, otherwise the connection / binding update request is denied.
The next step the correspondent will perform the home address check and the care of address check.
The correspondent will send a home test (HoT) packet, which is assumed that the home agent will tunnel to the mobile node. The HoT packet consists of a home keygen token generated by hashing the secret key K_{cn} only known to the correspondent. A nonce index is also included to allow the CN to find the appropriate nonce easily.

Home token = hash (K_{cn} | source address | nonce | 0)

This is then sent to the home agent.

CN ⟶ HA: HoT.

Message 4.
The Home Test packet is then forwarded to the mobile node's care of address.

HA ⟶ MN: HoT.

Message 5.
The correspondent also performs a care of address test (CoT), which is similar to the home address test and takes place at the same time as message 3, however the token generated is slightly different.

Care-of token = hash (K_{cn} | source address | nonce | 1)

This is then sent directly to the mobile node within a Care of test (CoT) packet.

CN ⟶ MN: CoT.

Message 6.
The mobile node receives both tokens from both the test packets sent. It then creates a binding key K_{bm} by hashing the two tokens together.

K_{bm} = hash (home token | care-of token)
by encapsulating the packets.
The key is used to protect the first and following binding updates. The mobile node then sends a binding update request to the correspondent node, which is protected with the binding key $K_{bm.}$

MN ⟶ HA2: K_{bm}(BU)

Message 7.
The mobile node still sends its packets via the correspondent nodes home address. This is because both nodes are mobile and the MN would have to accept a binding update from the correspondent before being able to communicate directly. For now the correspondents home agent HA2 forwards the packet to the correspondent.

HA2 ⟶ CN: K_{bm}(BU)

Message 8.
This is where traditionally the correspondent would decrypt the data and accept the binding update, however before this begins it must wait for the result of another authentication protocol to complete. This authentication takes place simultaneously with return routability.
The correspondent node sends a request message to the mobile node for its authentication data (RAD).

CN ⟶ MN: RAD

Message 9.
The mobile node replies to the message by sending its authentication data, which includes its current address, its sim number, IMEI number, phone number and even and option for user authentication such as biometric data. This sent to the CN via HA2 encrypted with the binding key $K_{bm.}$

MN ⟶ HA2: K_{bm}(CoA, Sim No, IMEI, Phone No., Biometric)

Message 10.

HA2 ⟶ CN: K_{bm}(CoA, Sim No, IMEI, Phone No., Biometric)

Message 11.
Simultaneously to message 8, the correspondent sends a request for authentication data message to the home agent.

CN ⟶ HA: RAD

Message 12.
The home agent does not have the binding key so sending the authentication data would be a security risk. Instead the home agent hashes the authentication data together and sends that to the correspondent.

HA⟶ HA2: Hash(CoA, Sim No, IMEI, Phone No., Biometric)

Message 13.

HA2 ⟶ CN: Hash(CoA, Sim No, IMEI, Phone No., Biometric)

Message 14.
Now the correspondent will have both the hash of the authentication data and the authentication data encrypted with the binding key. There are now two options:

1. The correspondent performs the authentication comparison by decrypting the binding key and hashing the authentication data received from the mobile node then comparing this to the hash received by the home agent. Skip to Message 16.
2. If the correspondent node is overwhelmed by the current processing of constraints it may opt to send the hash and the decrypted authentication data to the correspondents home agent via a secure tunnel where it will perform the comparison. (Notice the key is not sent as this would be a security vulnerability. The decryption is done by the CN.)

CN ⟶HA2: (Hash(CoA, Sim No, IMEI, Phone No., Biometric), (CoA, Sim No, IMEI, Phone No., Biometric))

Message 15.
The HA2 hashes the authentication data and compares it to the hash. If they match then the authentication is successful and an authorisation ok message is sent to the correspondent node.

CN ⟶ HA2: AOK

Message 16.
If the result of the authentication is successful then the binding update is accepted and a binding acknowledgement BA is sent to the mobile node allowing it to communicate directly with the correspondent.

CN ⟶ MN: BA

As the correspondent is also mobile, the mobile node will have to accept binding updates from it also. The process is the same, only in reverse. Of course less messages will be needed as the mobile node can now communicate directly with the correspondent unless it takes place at the same time.

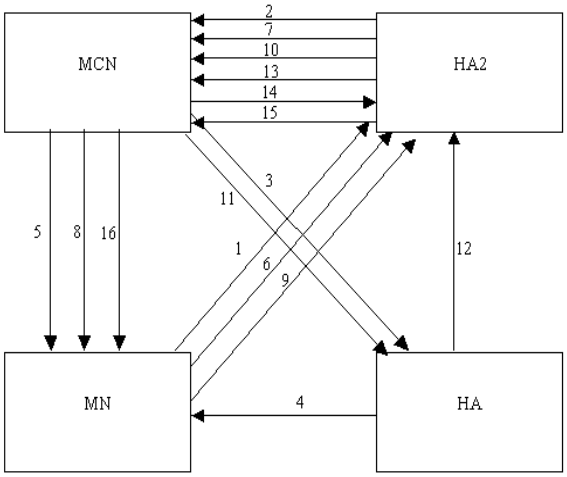

Fig.1, Mobile-to-mobile authentication

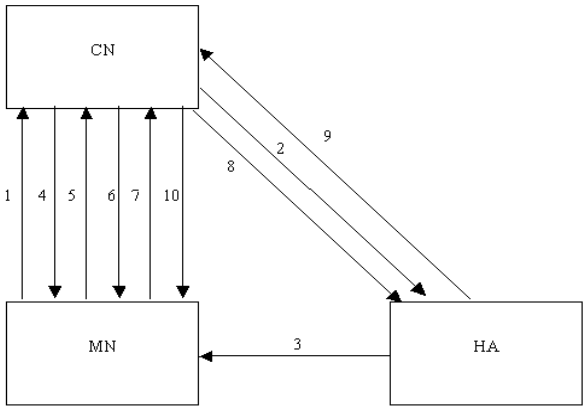

Fig.3, Mobile-to-Static authentication

3.2 Authentication in mobile node to static node communication.

The principle is the same the mobile-to-mobile communication however as the correspondent is static it does not have a home agent and so cannot perform distributed authentication. See Fig.3. However as it is not mobile it is logical to assume it will have a great deal more processing power than a mobile device and so distributed authentication would be unnecessary. All the messages are the same but are far fewer as they do not pass via the correspondent's home agent.

The security protocol uses the same mechanisms, which are already in place, meaning the architecture and headers remain the same, Fig.2, insuring compatibility with any future mobile IP system. The advantages of using a distributed authentication protocol is that there is a predicted increase in processing speed concerning the completion of security techniques which at the same time not over burdening the mobile processor with all the work. The disadvantage is that there is an increase in network traffic, however optimisation to the protocol may be able to reduce this.

Ver.	Traffic Class	Flow label
Payload Length	Next header	Hop limit
128 Bit Source Address		
128 Bit Destination Address		

Fig.2, IPv6 Header

4 Conclusion

The binding update route optimisation protocol suffers from security vulnerabilities, which allow attackers to send false binding updates to redirect data traffic for interception and eavesdropping of packets or the prevention of communication via denial of service attacks.

These problems exist because current security protocols don't effectively authenticate the legitimacy of the users leaving the participants vulnerable to attack. Many of the solutions that currently exist are resource intensive in terms of processing power required, which is unavailable with mobile devices.

The proposed solution will attempt to address these issues by introducing distributed authentication. Its main function is to aid in user and device authentication while providing processing assistance to the mobile device These features will protect the nodes from false binding updates attempting to hijack the session.

The proposed security protocol is designed within the boundaries of the existing architecture and security technologies. The complimentary use for Cryptographically Generated Addresses and return routability limits the options for attackers. It does not however check authentication of the device or user. This has now been introduced and will enhance the security of existing systems. By not modifying any of the standards of mobile IPv6, the security solution should be compatible with any future implementation and at a low cost. The introduction of distributed authentication can have benefits under processor intensive situations but the drawback is that there is an increase in network messages. The option to choose between standard and distributed authentication is a useful choice

however under which circumstances one or the other should be used with have to be tested.

The protocol has addressed many on the security vulnerabilities identified, however it remains to be seen how it holds up in a simulated environment.

The proposed security protocol is designed within the boundaries of the existing architecture and security technologies. The complimentary use for Cryptographically Generated Addresses and return routability limits the options for attackers. It does not however check authentication of the device or user. This has now been introduced and will enhance the security of existing systems. By not modifying any of the standards of mobile IPv6, the security solution should be compatible with any future implementation and at a low cost. The introduction of distributed authentication can have benefits under processor intensive situations but the drawback is that there is an increase in network messages. The option to choose between standard and distributed authentication is a useful choice however under which circumstances one or the other should be used, has to be tested.

The protocol has addressed many on the security vulnerabilities identified, however it remains to be seen how it holds up in a simulated environment.

Glossary: -

MN	Mobile node
CN	Correspondent node
MCN	mobile correspondent node
HA	Home agent
H(m)	A hash of message m
K^+	Public Key
K-	Private Key
MNK^+	Mobile nodes public key

References:

[1] Tuomas Aura, Michael Roe, and Jari Arkko. *Security of internet location management.* In Proc. 18th Annual Computer Security Applications Conference, pages 78-87, Las Vegas, NV USA, December 2002. IEEE Press.

[2] C. Perkins, Mobile IP Design Principles and Practices: Addison Welsey, 1998.

[3] Tuomas Aura. *Mobile IPv6 Security.* In Proc. Security Protocols, 10th International Workshop, Cambridge, UK, April 2002. Springer 2003.

[4] J. Kohl and C. Neuman, The Kerberos Network Authentication Service, RFC 1510, http://www.faqs.org/rfcs/rfc1510.html, September 1993

[5] J. Arkko, P. Nikander, and G. Montenegro. Selection of MIPv6 Security Level Using a Hashed Address Internet Draft draft-arkko-mIPv6-select-hash-00.txt. Work In Progress, IETF, June 2002.

[6] A.S Tanenbaum and M.V Steen, Distributed systems –Principle and paradigms, prentice hall, new jersey, 2002.

[7] James Kempf, Craig Gentry, "Securing IPv6 Neighbor Discovery Using Address Based Keys (ABKs)." (IETF, May 6, 2003)

[8] Tuomas Aura. *Cryptographically Generated Addresses (CGA).* In Proc. 6th Information Security Conference (ISC'03), volume 2851 of LNCS, pages 29-43, Bristol, UK, October 2003. Springer.

[9] J. Arkko, V. Devarapalli, F. Dupont. Using IPSec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents. RFC 3776, IETF, June 2004.

[10] C. Rigney et al, Remote Authentication Dial In User Service (RADIUS, http://www.faqs.org/rfcs/rfc2865.html, RFC 2865, June 2000.

[11] J. Arkko, P. Calhoun, E. Guttman, D. Nelson, and B. Wolff. AAA Solutions. Internet Draft draft-ietf-aaa-solutions-01.txt. Work In Progress, IETF, November, 2000.

[12] M. Roe, G. O'Shea, T. Aura, J. Arkko. Authentication of Mobile IPv6 Binding Updates and Acknowledgments, Internet Draft draft-roe-mobileip-updateauth-02.txt. IETF, February 2002.

[13] Greg O'Shea and Michael Roe, Child-proof authentication for MIPv6 (CAM), ACM Computer Communications Review, 31(2), April 2001.

[14] A.Georgiades et al, Trinity Protocol for the authentication of binding updates in mobile IPv6, WSEAS Transactions on communications, Issue 3, Volume 3, July 2004.

[15] W. Haddad et al, Applying Cryptographically Generated Addresses to Optimize MIPv6, http://www.ietf.org/internet-drafts/draft-haddad-mip6-cga-omipv6-03.txt, October 2004

[16] D. Johnson et al, Mobility Support in IPv6, RFC 3775, http://www.faqs.org/rfcs/rfc3775.html, June 2004

[17] Jari Arkko et al, *Securing IPv6 neighbor discovery and router discovery*. In Proc. 2002 ACM Workshop on Wireless Security (WiSe), pages 77-86, Atlanta, GA USA, September 2002. ACM Press.