Proceedings of the 6th WSEAS International Conference on Applied Informatics and Communications, Elounda, Greece, August 18-20, 2006 (pp406-411)

Dual Identity Return Routability for the Security of Mobile Ipv6 Binding Updates within the Distributed Authentication Protocol

ANDREW GEORGIADES,
DR YUAN LUO,
DR ABOUBAKER LASEBAE,
PROF. RICHARD COMLEY
Department of Computing Science
Middlesex University
Hendon campus, The Burroughs, London, NW4 4BT
UNITED KINGDOM
A.georgiades@mdx.ac.uk www.cs.mdx.ac.uk

Abstract: - The future fourth generation 4G networks will provide us with a paradigm shift in how mobile telecommunications will operate. It will be solely based on packet switching using mobile IPv6. However binding update route optimisation is vulnerable to a variety of security attacks. This paper attempts to reduce the security vulnerabilities by creating a new security protocol by first investigating the possible future technologies which may be incorporated into 4G mobile phones. Various technologies such as WI-FI and WiMax will be looked at but one in particular may be of particular interest, sim cards which allow the user to have multiple phone numbers. Using this technology and combining it with the established security protocol return routability, a new enhanced security solution is created called Dual Identity Return Routability. This solution provides an enhanced reachability test and a cheap authentication method, which can be incorporated into the distributed authentication protocol or be used as a stand-alone solution.

Key-Words: - Mobile IPv6, Binding Updates, Security, Authentication, Return Routability, Dual Identity.

1 Introduction

Before a security solution can be designed for a future telecommunication network, it is wise and vital to take a look at the emerging technologies and economical factors, which may impact the very core of the telecommunications industry, as we know it. This paper will present some predictions of which technologies will be incorporated into the Forth Generation of mobile telecommunications, technologies, which may have such a fundamental impact, that it will create a paradigm shift in the way the service is run. Only then can the network architecture be understood and a security solution crafted to adequately take advantage of its environment. This paper attempts to find a solution to prevent binding updates in Mobile Ipv6 from being susceptible to masquerading and impersonation attacks.

2 Problem Definition

Mobile IP has primarily been designed for the ease of mobility of communicating devices. It is the underlining architecture for the fourth generation of mobile phones. Due to the nature of TCP/IP, only static IP addresses are permitted to be used within the network. This causes problems for mobile nodes, which wish to migrate to a new location yet still remain connected to the network. This is because physically moving to another location results in a new attachment to a wireless network node and as a result the IP address would change. Mobile IP solves this issue by employing two addresses [1].

The First address belongs to the home agent, which acts as a proxy for the mobile node and ensures the mobile node remains reachable by having a static address.

The mobile node itself has a dynamic address and this changes every time the node is associated with another point of attachment. Each time the mobile node migrates to a new location, it is assigned a new IP address and the home agent is informed of that new address. A node wishing to contact the mobile node must contact the home agent, which will tunnel the data packets to the current address of the mobile node. Correspondent nodes communicate by sending packets to the

mobile nodes static address, which are then forwarded to the mobile node. This is called triangle routing and can have an impact on communication latency. To avoid latency issues binding updates were introduced to allow the mobile node to communicate directly with the correspondent node by bypassing the home agent, with the use of a binding update. This keeps the home agent and the correspondent node aware of the mobile nodes' current location and allows for direct communication. Binding updates however are susceptible to security attacks such as interception and impersonation. This can be used by an attacker to mount man in the middle, redirection and denial of service attacks [2]. The distributed authentication protocol [3] has been designed to prevent or at least limit this attack from taking place. However can looking at the future technologies which may be implemented and incorporated into 4G technology, allow for improvements in the security design?

3 Emerging technologies

Second generation telecommunications, utilise the circuit switched GSM network to provide a dedicated line for the duration of the call. With the intermediate generational leap to 2.5G, bandwidth speeds have not necessarily increased but support for packet switching of data has been implemented with the use of GPRS. The Third generation systems have been initially designed to provide both circuit switched and packet switched domains for voice and data respectively. However an alternate access network, from 2G systems, needs to be used such as UMTS or CDMA 2000 [4].

Unlike 3G, Fourth Generation systems are based on packet switching only. The method of transmission of voice calls is done with the use of Voice over IP, (VoIP) [5]. This splits voice into data packets, which are sent across the Internet, which are reassembled at the destination address. The advantage is that there is no dedicated line created for the call as packets can take any path they choose, however during some network conditions voice calls can suffer a loss of quality.

4G Mobile devices will use Mobile Ipv6 addresses to identify themselves. This of course does not mean telephone numbers will become obsolete as then can be resolved in the same way a web page address is found in a look up table giving its IP address. This does mean however that mobile phones will operate in a similar way to the infrastructure of broadband Internet in the home. This could possible mean that telecommunication companies in effect become Internet service providers, and as such, instead of paying for a telephone subscription we may have an ISP subscription instead.

Even if companies try to keep the lucrative business models, which they currently enjoy, consumers may find cheaper alternatives such as the Skype service [6, 7], which provides free PC-to-PC calls. As time moves on its highly likely that mobile devices will become comparable in processing power of a PDA or even a low end computer. This means that applications such as Skype will find its way to mobile devices and telecom (ISP) companies will find themselves losing revenue.

ISPs will change their business plan to a more service orientated market and try to generate revenue from killer applications such as premium content music, videos and live streaming television IPTV.

One possible avenue for ISPs to increase revenue will be to acquire as many subscriptions as possible. One way to do this would be to allow multiple subscriptions to the same phone, each for a different number. I.e. a business number and a personal number, all on the same sim card. This would allow the consumer to receive calls from multiple contacts, take advantage of different subscription offers, peak, off peak, and switch off a subscription if they did not want to be contacted and all of this occurring on a single device, Fig 1.
Sim cards are in development, which allow multiple numbers, or identities, on a single sim [8, 9]. It was previously unavailable as different numbers from different companies could not co-exist simultaneously as GSM channels would clash with each other at close range. This issue can be resolved, as an alternative wireless medium will be utilised. Most likely based on WI-FI. It then becomes economically viable for ISP's to provide consumers with more than one phone number for which each needs a subscription. Of course the drawback then is that WI-FI has a limited range in comparison to GSM. The most likely method of wireless transmission is WiMAX, which can cover a large metropolitan area [10]. However it is more likely that this will be used as a backbone for last mile delivery of high-speed broadband to the home. Fortunately it is interoperable with other wireless standards allowing for WI-FI enabled phones/nodes to communicate with each other by interconnecting them.

The WiMax standard utilises a scheduling MAC, which allocates a time slot to the base station

as opposed to Wi-Fi's contention access where all nodes are competing for the base stations attention randomly. This makes WiMax more stable for the purpose of mobile communications. WiMAX also has the potential for mesh networking allowing users to connect to each other by bypassing the infrastructure or allowing nodes to become part of the infrastructure that would otherwise be out of range.

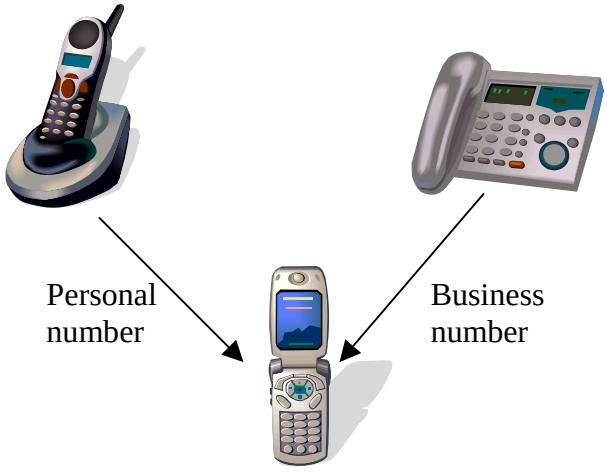

Fig 1. Phone with Dual identity sim

4 Current Security Solutions

Mobille IPv6 Binding updates are vulnerable to attacks such as interception and impersonation. Numerous security solutions have been proposed to protect mobile IPv6 networks and each has 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 [11] that perform authentication by referring to a central authentication database to compare users credentials.

Other security components include hashes [12], digital signatures [13], address based keys [14] and cryptographically generated addresses [15].

More elaborate systems such as IPSEC [16] and RADIUS [17] based on AAA Authentication, authorization and accounting [18], 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 [19] and CAM [20] are good but have flaws. The Trinity protocol [21] 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.

4.1 CGA

Cryptographically generated addresses [15] 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 [22]. 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 [22]. 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.

4.2 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 [23]. 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].

5 Proposed Solution

The distributed authentication protocol was designed to improve the security of binding updates by combining current security with a new authentication method.

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 the address of the user 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.

In addition to the distributed authentication protocol, a new solution in now proposed as a modification to return routability. It will demonstrate that dual identity phones can be used to improve security within 4G networks.

Dual indentity return routability is part of a larger security solution, but could be used as a stand-alone solution. Before the protocol takes place the mobile node sends an intention to communicate with the correspondent node. The mobile node sends the correspondent node its public key MNK+, care of address CoA (actual location dynamic address) and its home address HoA (static address) and the phone number address of its other identity CoA2 and its home agent address HoA2. It is possible for both identities to share the same home agent Fig 2, or use separate home agents Fig 3.

MN ⟶ CN: MNK+, CoA1, HoA1, CoA2, HoA2.

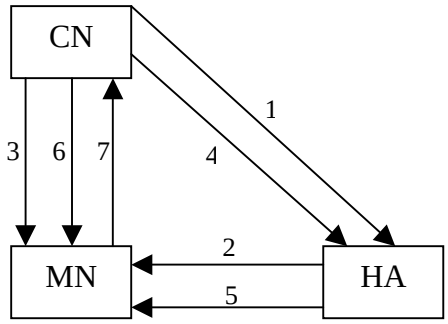

Fig 2, Dual Identity Return Routability with both identities sharing the same home agent.

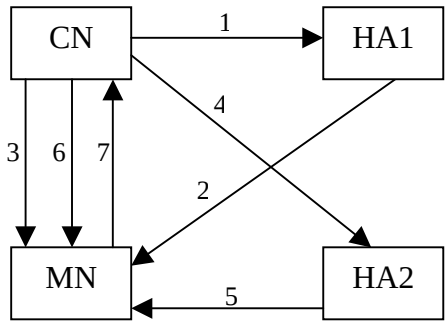

Fig 3, Dual Identity Return Routability with both identities using different home agents.

The Correspondent node (CN) will test to see if the Mobile node MN is reachable at the care of address and also test the other identity address is reachable. The two identities are linked together making spoofing a lot more difficult and proving the user is the owner of the identity.

Message 1

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 token1 = hash (K_{cn} | source address | nonce | 0)

This is then sent to the home agent.

CN ⟶ HA: HoT1.

Message 2
The Home Test packet is then forwarded to the mobile node's care of address.

HA ⟶ MN: HoT1.

Message 3
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 1 and 2, however the token generated is slightly different

Care-of token1 = 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: CoT1.

Message 4
Home token2 = hash (K_{cn} | source address | nonce | 2)

This is then sent to the home agent of the second identity.

CN ⟶ HA: HoT2.

Message 5
The Home Test packet is then forwarded to the mobile node's care of address.

HA ⟶ MN: HoT2.

Message 6
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 4 and 5, again the token generated is slightly different

Care-of token2 = hash (K_{cn} | source address | nonce | 3)

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

CN ⟶ MN: CoT2.

Message 7
The mobile node receives all four tokens from the four test packets sent. It then creates a binding key K_{bm} by hashing the four tokens together.

K_{bm} = hash (home token | care-of token | home token2 | care-of token2)

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 ⟶ CN: K_{bm}(BU)

This protocol proves that the mobile node is reachable at its current address, preventing denial of service attacks and proves that the two identities are associated with each other proving ownership of the phone numbers / IP addresses and providing a cheap method of authentication.

6 Conclusion

This paper aimed to find a security solution for the vulnerabilities of binding updates in mobile IPv6. Binding updates are a route optimisation enhancement to mobile IP, allowing direct communication between nodes and reducing communication latency but are susceptible to impersonation, man in the middle and denial of service attacks. This paper attempted to discover the different types of future technologies in development, which may be incorporated into the 4G fourth Generation mobile network. One technology stood out which allows multiple phone numbers, or identities, to be simultaneously used on a single sim card. Different wireless transmission technologies were also investigated such as W-FI and WiMAX. Taking advantage of these technologies, a new security solution was created based on return routability. Secret tokens are sent to the addresses of the mobile node and the home agent of both identities. This provides reasonable reassurance of two things, 1, the mobile node is indeed in the location it claims to be and 2, proves that mobile node has ownership of both identities providing a cheap authentication solution. Dual Identity Return Routability has been designed to be incorporated with the distributed authentication protocol however could be used as a stand-alone security solution. This may be useful for distributed mesh networks, which could be formed with the use of WiMAX. However, no matter which