Security Implications and Considerations for Femtocells

Jing Chen and Marcus Wong

Huawei Technologies, 400 Crossings Blvd, 2FL Bridgewater, NJ 08807, USA;
e-mail: eric.chenjing, mwong@huawei.com

Abstract

A Femto system is able to provide new services with higher data rate at relatively lower cost than traditional cellular system. Operators have already indicated their interest in this area and the number of deployments is ever increasing. Security is a critical part of Femto in all aspects of the operation of Femto services. In this paper, we analyze the security of Femto based on 3GPP system architecture. In addition, we will look into the details of other security aspects of Femto system, including security requirement and security mechanism.

Keywords: 3GPP, cellular, femtocells, security.

1 Introduction

Femto system is able to provide new services with higher data rate at relatively lower cost than traditional cellular systems allowing wireless service providers to rapidly extend coverage and expand user base. With the first deployment of commercial femtocells in a major operator network in 2007

Journal of Cyber Security and Mobility, 21–35.

that was based on CDMA technology, other major operators throughout the world have followed with similar femtocells that are based on UMTS technology, including that of the Vodafone's networks of femtocell deployments in Greece, Spain, and UK using femtocells developed and manufactured by Huawei Technologies. Recent studies indicated that worldwide deployments of femtocells could reach 49 million by 2014. A femtocell, also called a Femto Access Point (FAP), is located in customer premise and will access the operator's core network via an IP link that an operator generally does not trust. As a result, the security risks to operator's core network will be increased when FAPs are introduced into an operator's cellular network which has been traditionally been considered a closed network. In addition, since FAPs are to be deployed in the customer premise, such as a home environment or a small enterprise setting, the FAP is vulnerable various threats and attacks (e.g. tamper the FAP, compromise or clone of FAP authentication credential, etc).

Since security is a critical aspect of Femto, we will analyze the security issues related to various aspects of a Femto system.

In this paper, we will introduce the security system architecture of Femto in Section 2; discuss some recent attacks on femtocells and introduce the security requirements of Femto AP in Section 3; and explore the security mechanisms to satisfy the security requirements in Section 4. Note that security architecture of Femto AP is very suitable for UMTS networks and more advanced Long Term Evolution (LTE) networks.

2 Femto System Architecture

The Femto System Architecture is shown in Figure 1 largely based on the work of 3GPP working group SA3 which is responsible for the overall security of all 3GPP systems.

The system architecture is described as having the following features:

- The backhaul link, being unsecure through the Internet, is connected from the Femto AP (FAP) to the operator's core network via a SeGW (Security Gateway).
- SeGW represents operator's core network to perform mutual authentication with FAP.
- An AAA server authenticates the hosting party module, a SIM-card based mechanism that is optionally deployed in the Femto architecture to help the operators effectively managing the FAP.

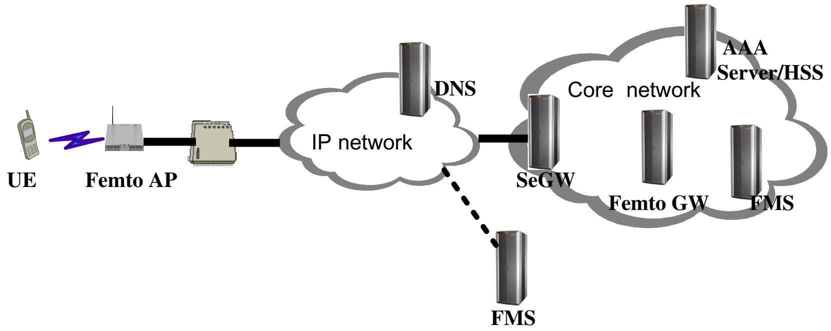

Figure 1 Femto system security architecture [1].

- Security tunnel is established between FAP and SeGW to protect information transmitted in backhaul link.
- Femto AP Management System (FMS) can configure the FAP according to the operator's policy (e.g. spectrum reuse policy, location policy, etc.). FMS is also capable of installing software updates on the FAP. The FMS server may be located inside the operator's core network (accessible on the Mobile Network Operator's Intranet) or outside of it (accessible on the public Internet), depending on operator's model or preference. However, secure communication is required between FAP and FMS (e.g. TLS or IPsec).
- A Femto GW and/or FAP perform(s) the access control in case non-CSG (Closed Subscriber Group) capable UEs or non-CSG capable FAPs are deployed depending on the level of equipment deployed. Femto is capable of being deployed in various scenarios to accommodate equipment from different releases of 3GPP specifications thus achieving backward compatibilities.
- FMS and/or Femto GW perform location verification of FAP to ensure that the FAPs operate in an area where the operator has licensed spectrum to operate.

In a traditional cellular network, a macro base station (the equivalent of a Femto Access Point) connects to the operator core network using dedicated links. However, the same dedicated links do not exist for Femto systems. Instead, a public Internet is used. As a result, special security consideration is needed in order to guarantee the same level of security into the operator's core network as with a traditional macro base station. Regardless of the type of cells, an user is able to initiate and receive calls using a handset that is compliant with whichever the technology the user has subscribed to (e.g. 3G UMTS, 3G CDMS, 2G GSM, etc.)

3 Security Requirements

When an important component of wireless system is located at a customer premise, such as the Femto Access Point, the convenience of the equipment location is tempting enough to attract attackers and hackers both occasional and professional. Due to the fact that a number of Femto systems had been developed and deployed as a result of speedy need to reach market quickly, these systems were based on some of the older security assumptions and technologies and therefore experienced the most scrutiny from the hacker community. Notably, there were two such attacks. These attacks and other common threats make it imperative that such a Femto system is designed with stringent security requirements from the very beginning.

3.1 Attack on the Vodafone Femtocells

The attacks on the femtocells in the Vodafone's network were made known in July of 2011 by a group known as The Hacker's Choice (THC) [2]. The attack seemed simply enough. Though the serial port of the FAP had been sealed off, the attackers were able to figure out the pin connection and made some soldering to connect to the serial console of the FAP. Once inside the console, the attacker was able to guess the root password and gain access as a root user. From that point, the attack has total control of the FAP and was able to disable the firewall, change the internal configurations and other settings. Once the configurations had been modified to the hacker's desire, the privacy of any user that was accessing his or her wireless services through the FAP was at the mercy of the attacker. Vodafone has since upgraded the older versions of the femtocells that were used in these attacks and patched the security hole.

3.2 Attack on SFR's Femtocells

In yet another attack on SFR's Femtocells as demonstrated in Blackhat 2011 [3], the attacker was able to take advantage of system's recovery procedure by connecting to an unauthenticated server, install his own software, firmware image and configurations, and turn the Femto into his playground. The description of the may be overly simplifying, but the attack was real. As a result, the attacker was able mount a number of attacks and compromising both system security and user privacy. Though the attack was focused on some of the older version of the femtocells, the holes have since been plugged. As we can see, the threats and security issues are real. A set of security requirements needs to be defined to ensure that the above mentioned attacks and other attacks are not to be repeated.

3.3 Operation Requirements

The Femto, being part of the operator's network, need to adhere to a set of operation requirements that have been well established for other components of the system and in addition to any other Femto specific requirements, namely:

(1) Only algorithms of adequate cryptographic strength will be used for authentication and protection of confidentiality and integrity.
(2) Modifications of Hosting Party controlled information by the operator will only be allowed with the permission of the Hosting Party.
(3) The extent of Hosting Party controllable information will be controlled by the operator.
(4) IMSIs of users connected to FAP will not be revealed to the Hosting Party of the Femto AP.

Note that the term Hosting Party refers to a person or entity where the femtocell is deployed. Due to the fact that the Femto is still considered a part of the operator network, even though a Hosting Party may have purchased the Femto, but only the operator has the ultimate legal authority to operate it.

3.4 Requirements on FAP

As the FAP is likely to be located in a physical environment that is out of the control and monitoring of the operator, the requirement of the FAP are enhancements from that of the traditional base stations to further protect it from hackers and outside threats:

(1) The integrity of the FAP will be validated before any connection into the core network is established.
(2) The FAP will be authenticated by the SeGW based on a globally unique and permanent FAP identity. The authentication will be performed using a certificate provided by the operator, manufacturer or vendor of the FAP.
(3) The FAP will authenticate the SeGW. The authentication will take place based on a SeGW certificate.
(4) Optionally when deployed, the hosting party of the FAP may be authenticated based on EAP-AKA [4].
(5) The Femto AP will authenticate the FMS, if the FMS is accessed on the public Internet.
(6) The Femto AP will be authenticated by the FMS using the same identity as for authentication to the SeGW, if the FMS is accessed on the public Internet.
(7) The configuration and the software of the Femto AP will only be updated securely, i.e. the integrity of the configuration data including the licensed radio parameters and the integrity of the software updates must be verified.
(8) Sensitive data including cryptographic keys, authentication credentials, user information, user plane data and control plane data will not be accessible at the Femto AP in plaintext to unauthorized access.
(9) The time base of the Femto AP will be synchronized to the core network.
(10) The location of the Femto AP will be reliably transferred to the network.
(11) Any unauthenticated traffic received from the access network will be filtered out by the FAP.

3.5 Requirements on SeGW

As a single point of entry into operator network, the security gateway plays one of the most important roles in terms of access. The requirements are equally stringent:

(1) The SeGW will be authenticated by the Femto AP using a SeGW certificate. The SeGW certificate will be signed by a certificate authority trusted by the operator.
(2) The SeGW will authenticate the Femto AP based on Femto AP certificate.
(3) The SeGW may authenticate the hosting party of the Femto AP in cooperation with the AAA server using EAP-AKA.
(4) The SeGW will allow the FAP access to the core network only after successful completion of all required authentications.

3.6 Requirements on FMS

As we have seen in one of the attacks where the attacker was able to connect a FAP to an unauthenticated server, it is essential such access is not given. Following the requirements below prevents above mentioned attacks and other similar attacks:

(1) The FMS will be authenticated by the FAP using a FMS certificate. The FMS certificate will be provided by the mobile network operator (MNO).
(2) The FMS will authenticate the identity of the Femto AP using a FAP certificate. This identity will be the same as used during backhaul link establishment
(3) If the FMS is accessible on the MNO Intranet, the mutual authentication between FMS and Femto AP may be replaced by the authentication between SeGW and Femto AP. In this case only the identity of Femto AP has to be transferred over the FMS link.

3.7 Requirements on Backhaul Link

As the backhaul link now travels through the public Internet, the likelihood of attacks and attempts to break into the operator network increases. The requirements are designed to deal specifically with these threats:

(1) The establishment of the secure backhaul link will be based on IKEv2 [5].

(2) The backhaul link will provide integrity protection of the transmitted data. It may provide confidentiality protection of the transmitted data, depending on operator requirements and/or policies.
(3) The security solution for the backhaul link will be based on IPsec ESP tunnel mode.
(4) Any connection between the FAP and the core network will be tunnelled through the backhaul link.
(5) The security solution for the backhaul link will be compatible with common network address and port translation variations and support firewall traversal.

4 Security Mechanism

Once we have established a good set of security requirements, we also need to design a good set of security mechanisms to fulfill these requirements. We now describe the security mechanisms based on the following area of protection:

- FAP Physical Security
- FAP and Core Network mutual authentication and IPSec tunnel establishment
- Location Verification
- Access Control
- Protection of FMS traffic between FMS and FAP
- Measures for Clock Protection

4.1 Femto AP Physical Security

4.1.1 Trusted Environment (TrE)

To provide FAP physical security, the logical entity of Trusted Environment (TrE) is defined and used based on an irremovable, hardware-based root of trust by way of a secure boot process, which will occur whenever a FAP is turned on or goes through a hard reset. An example implementation of such a TrE may be realized in the form of existing technology, such as a trusted platform module (TPM) commonly found in today's high end personal computers. It is important that the root of trust is physically bound to the FAP and that a secure boot process is used that includes checking the integrity of every loaded or started component of the TrE and only allow components to be loaded or started upon successful integrity validation.

4.1.2 Device Integrity Check

The Femto AP and TrE will perform a device integrity check upon booting and before connecting to the core network and/or to the FMS. The device integrity check is based on one or more trusted reference value(s) and the TrE:

- The integrity of a component is verified by comparing the result of a measurement (typically a cryptographic hash) of the component to the trusted reference value. If these values agree, the component is successfully verified and can be loaded and/or started.
- The integrity of the device is verified if all components necessary for trusted operation of the device are verified.

4.1.3 Femto AP Validation

The FAP supports a device validation method where the device implicitly indicates its validity to the SeGW or FMS by successful execution of device authentication. But various validation techniques are possible:

1. Autonomous validation
2. Remote validation
3. Semi-autonomous validation
4. Hybrid validation

In an autonomous validation, FAP's validity is assessed internally within the FAP itself without depending on external network entities.

In a remote validation, an external platform validation entity assesses the validity of the FAP after it receives comprehensive evidence for the validation generated by the Femto AP's TrE

In a semi-autonomous validation, the FAP's validity is first assessed internally by the TrE without depending on external entities. After the TrE makes such an assessment, the assessment and any additional required evidence are sent securely to an external platform validation entity that subsequently makes its own decisions based on whether to grant access.

In a Hybrid validation, a FAP powering up will execute a secure start-up procedure to bring it to a determined and trustworthy state. Additionally, FAP will gradually bring the rest of the system, modules, and other components to a trustworthy state.

4.2 Femto AP and CN mutual authentication and IPsec tunnel establishment

Since there may be two trusted entities (e.g. FAP itself and the hosting party module) in the FAP, the FAP supports the following authentication:

a) Device authentication: Mutual authentication of Femto AP device and the operator's network is mandatory performed when Femto AP access to the network.
b) Hosting Party Authentication: Authentication of the hosting party by the operator's network is based on credentials contained in a separate Hosting Party Module (HPM) in FAP. This authentication maybe optional depending on an operator's network configuration.
c) A combined authentication is also possible to maximize efficiency without sacrificing security

4.2.1 Device Authentication Procedure

Device authentication of FAP is based on device certificate for FAP and network certificate for the core network with the TrE securely protecting the FAP's credentials and critical security functions, including the authentication function. Device authentication is based on IKEv2 with public key signature based authentication with certificates, as specified in RFC 4306 [5]. An example of certificate-based device Authentication Call-flow is shown in Figure 2.

4.2.2 Hosting Party Authentication

When a hosting party module is present, device authentication may be followed with an EAP-AKA-based hosting party authentication exchange using extended IKEv2's multiple authentication procedure as defined in IETF RFC 4739 [6]. The authentication of the hosting party is based on an AKA credentials contained in a separate Hosting Party Module (HPM) in FAP. The

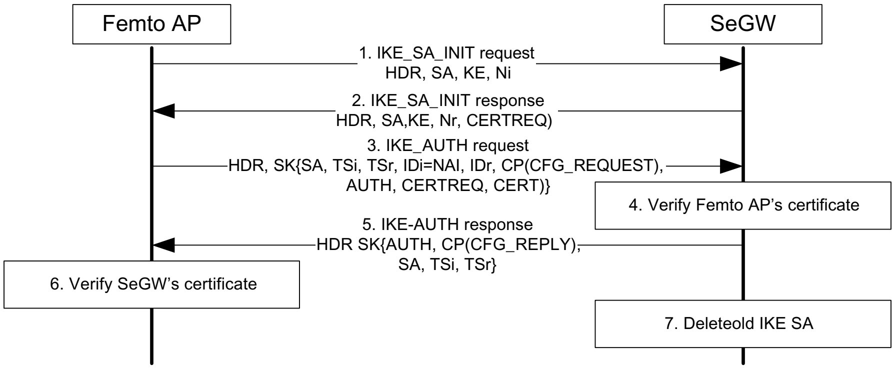

Figure 2 Certificate-based authentication.

SeGW acts as an EAP authenticator and forwards the EAP protocol messages to the AAA server to retrieve an authentication vector from the operator's authentication center via HSS/HLR. An example call flow between the Femto AP, SeGW and AAA server is shown in Figure 3. This example illustrates a certificate based mutual authentication between the Femto AP and the core network, followed by an EAP-AKA-based HP authentication exchange between the FAP/HPM and the AAA server.

4.2.3 IPsec Tunnel Establishment

After the device authentication, HPM authentication or combined authentication, IPsec tunnel is established between the FAP and the SeGW setting up a pair of unidirectional security associations. After that point onward, all signalling, user, and management plane traffic over the interface between FAP and SeGW will be sent through that tunnel operating in IPsec ESP tunnel mode(with NAT-T UDP encapsulation as necessary).

4.3 Location Verification

Operators require assurance of the FAP location to satisfy various security, regulatory and operational requirements due to the fact that the FAP, being a network component, requires the use of licensed spectrum which the operator has acquired for specific geographical location or region. The FMS and/or Femto GW may act as the verifying node to perform location verification. The

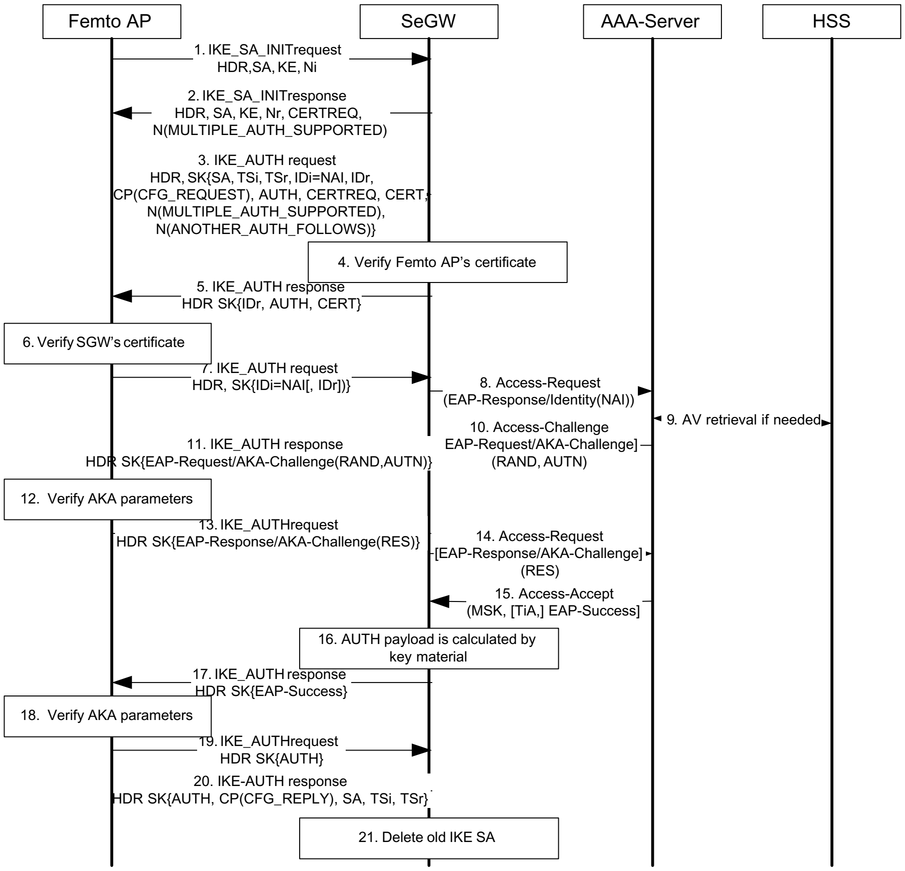
Femto AP
SeGW
AAA-Server
HSS
1. IKE_SA_INITrequest
HDR,SA, KE, Ni
2. IKE_SA_INITresponse
HDR, SA, KE, Nr, CERTREQ,
N(MULTIPLE_AUTH_SUPPORTED)
3. IKE_AUTH request
HDR, SK{SA, TSi, TSr, IDi=NAI, IDr,
CP(CFG_REQUEST), AUTH, CERTREQ, CERT,
N(MULTIPLE_AUTH_SUPPORTED),
N(ANOTHER_AUTH_FOLLOWS)}
4. Verify Femto AP's certificate
5. IKE_AUTH response
HDR SK{IDr, AUTH, CERT}
6. Verify SGW's certificate
7. IKE_AUTH request
HDR, SK{IDi=NAI[, IDr]}}
8. Access-Request
(EAP-Response/Identity(NAI))
9. AV retrieval if needed
10. Access-Challenge
EAP-Request/AKA-Challenge]
(RAND, AUTN)
11. IKE_AUTH response
HDR SK{EAP-Request/AKA-Challenge(RAND,AUTN)}
12. Verify AKA parameters
13. IKE_AUTHrequest
HDR SK{EAP-Response/AKA-Challenge(RES)}
14. Access-Request
[EAP-Response/AKA-Challenge]
(RES)
15. Access-Accept
(MSK, [TiA,] EAP-Success]
16. AUTH payload is calculated by
key material
17. IKE_AUTH response
HDR SK{EAP-Success}
18. Verify AKA parameters
19. IKE_AUTHrequest
HDR SK{AUTH}
20. IKE-AUTH response
HDR SK{AUTH, CP(CFG_REPLY), SA, TSi, TSr}
21. Delete old IKE SA

Figure 3 Combined certificate and EAP-AKA-based authentication.

verifying node needs one or more of the following information elements to perform location verification:

(1) the public IP address of the broadband access device provided by the FAP
(2) the IP address and/or access line location identifier provided by broadband access provider
(3) information of macro-cells surrounding the FAP provided by the FAP
(4) geo-coordinates provided by a global navigation system satellite receiver embedded into the FAP

Different deployment scenarios and FAP configurations will influence the availability, accuracy and reliability of these types of location information and determine the best solution for an operator.

4.4 Access Control

To prevent unauthorized access, only the authorized user can be allowed to access a Femto AP. An authorized user may be the FAP purchaser's friends and family but not his neighbor. To set up such an access control, the user may need to enter a list of cell phone numbers that are allowed to be connected to the FAP in a access control list, either through his how phone or through a web interface provided by the operator. Due to the capabilities of the user's mobile equipment, it is necessary to consider the cases when the mobile is non-CSG capable and when the mobile is CSG capable.

4.4.1 Non-CSG Method

Older equipment that does not support CSG can be either a non-CSG capable mobile or a non-CSG capable FAP. In this case, Femto GW and/or FAP will perform the optional access control based on the access control list stored in Femto GW and FAP.

4.4.2 CSG Method

For newer equipment that are CSG capable (mobiles or FAPs), other network elements in operator's core network (e.g. mobility management entity) will perform access control for UE for accessing Femto AP.

4.5 Protection of FMS traffic between FMS and Femto AP

4.5.1 Connection to FMS Accessible on MNO Intranet

When FMS is accessible on within the operator's network, FMS traffic will be protected through the support of one of the three security mechanisms determined by the Network Operator's Security Policies:

(1) Hop-by-hop where FMS traffic is protected between FAP and SeGW in one security association and then between SeGW and

FMS in yet another security association. Network security mechanisms will be used to protect FMS traffic between SeGW and FMS when the path from SeGW to FMS is considered as insecure.

(2) End-to-end where FMS TLS tunnel is established between Femto AP and FMS.

(3) End-to-end within IPsec between FAP and SeGW where the end-to-end TLS tunnel may be ignorant of the existence of an already established IPsec tunnelled between FAP and SeGW.

4.5.2 Connection to FMS accessible on public Internet

When the FMS is accessible on the public Internet (in case the FMS is managed by a third party other than the operator), the FMS is exposed to attackers located in insecure network. FMS traffic will be protected by TLS tunnel established between Femto AP and FMS. In this case, mutual authentication between Femto AP and FMS will be based on device certificate for the Femto AP and network certificate for the FMS.

4.6 Measures for Clock Protection

For Femto that does not rely on strict chip-level synchronization, an internal clock may be considered as extraneous. However, the availability of the correct current time is important for certificate validation and thus for the establishment of secure links (IKEv2 and/or TLS). In addition, the internal clock and the network clock should be synchronized upon establishing a secure connection to the core network. To ensure the security of the current time, the last time at which the Femto AP was active before the current power-up should be recorded and saved in the TrE.

5 Conclusion

In this paper, we have looked at the security Femto system architecture in detail. In addition, we have also analyzed the security requirements of Femto AP and explored the security mechanisms based on the security requirements as developed in 3GPP. Though still developing and emerging, we believe that the security requirements and security mechanisms currently developed will provide reasonable and practical security for the current and foreseeable generations of Femcocells.

References

[1] 3GPP TS 33.320 v0.2.0: “3GPP Security Aspect of Home NodeB and Home eNodeB; Release 9”.

[2] The Hacker’s Choice, http://wiki.thc.org/vodafone.

[3] Ravishankar Borgaonkar, Nico Golde, Kévin Redon: “Femtocells: a Poisonous Needle in the Operator’s Hay Stack”, August, 2011

[4] IETF RFC 4187: “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”.

[5] IETF RFC 4306: “Internet Key Exchange (IKEv2) Protocol”.

[6] IETF RFC 4739: “Multiple Authentication Exchanges in the Internet Key Exchange”, November 2006.

Biography

Jing Chen is a member of the senior research in the wireless security group in Huawei’s Shanghai Research Center. He received Master in Xi’dian University, Xi’an, China. After a brief stay in ZTE Corporation, he has since been with Huawei Technologies for about 8 years. He has worked in wireless security area since the early 2000’s. His current research interests include security of wireless system, IP transport security, trusted computing, etc. He has extensive involvement in various standardization activities in both CCSA TC8 and 3GPP SA3. He currently is the serving vice-chairman of WG2 (Wireless Security Working group) within TC8 of CCSA.

Marcus Wong is in the Wireless Advanced Research & Standards organization of Huawei North America R&D center. He joined Huawei in 2007 and has been focusing on various aspects of research and standardization in 3GPP and WiMAX Forum security area. Marcus is also active in the Wireless World Research Forum, contributing to various projects within WWRF.

Before joining Huawei, Marcus had spent 15 years in the telecommunication industry with both Bell Laboratories and Samsung’s

Advanced Institute of Technology covering many aspects of the security in wireless systems, including that of 2G/3G cellular networks, Personal Area Networks, and satellite communication systems.

He was previously the vice-chairman of 3GPP SA3 (Security Group) from November 2009 to December 2011 and is currently the serving vice-chairman of WWRF WG7 (Security & Trust Working group), a position he has held since 2007.