November 2011, Vol. 49, No. 11

IEEE Communications MAGAZINE

www.comsoc.org

Free ComSoc Articles
RF Amplifier Technology
See Page 9

- The Internet of Things
- Automotive Networking
- Consumer Communications
- Toward Next-Generation PONs

IEEE COMMUNICATIONS SOCIETY
A Publication of the IEEE Communications Society

IEEE Communications MAGAZINE

November 2011, Vol. 49, No. 11

www.comsoc.org/~ci

THE INTERNET OF THINGS

GUEST EDITORS: JUN ZHENG, DAVID SIMPLOT-RYL, CHATSCHIK BISDIKIAN, AND HUSSEIN T. MOUFTAH

PASSIVE OPTICAL NETWORKS (PONS): TOWARD NEXT-GENERATION PONS

SERIES EDITORS: OSMAN S. GEBIZLIOGLU, HIDEO KUWAHARA, VIJAY JAIN, AND JOHN SPENCER

IEEE COMMUNICATIONS MAGAZINE (ISSN 0163-6804) is published monthly by The Institute of Electrical and Electronics Engineers, Inc. Headquarters address: IEEE, 3 Park Avenue, 17th Floor, New York, NY 10016-5997, USA; tel: +1-212-705-8900; http://www.comsoc.org/ci. Responsibility for the contents rests upon authors of signed articles and not the IEEE or its members. Unless otherwise specified, the IEEE neither endorses nor sanctions any positions or actions espoused in *IEEE Communications Magazine*.

ANNUAL SUBSCRIPTION: $27 per year print subscription. $16 per year digital subscription. Non-member print subscription: $400. Single copy price is $25.

EDITORIAL CORRESPONDENCE: Address to: Editor-in-Chief, Steve Gorshe, PMC-Sierra, Inc., 10565 S.W. Nimbus Avenue, Portland, OR 97223; tel: +(503) 431-7440, e-mail: steve_gorshe@pmc-sierra.com.

POSTMASTER: Send address changes to *IEEE Communications Magazine*, IEEE, 445 Hoes Lane, Piscataway, NJ 08855-1331. GST Registration No. 125634188. Printed in USA. Periodicals postage paid at New York, NY and at additional mailing offices. Canadian Post International Publications Mail (Canadian Distribution) Sales Agreement No. 40030962. Return undeliverable Canadian addresses to: Frontier, PO Box 1051, 1031 Helena Street, Fort Eire, ON L2A 6C7

SUBSCRIPTIONS, orders, address changes — IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855-1331, USA; tel: +1-732-981-0060; e-mail: address.change@ieee.org.

ADVERTISING: Advertising is accepted at the discretion of the publisher. Address correspondence to: Advertising Manager, *IEEE Communications Magazine*, 3 Park Avenue, 17th Floor, New York, NY 10016.

SUBMISSIONS: The magazine welcomes tutorial or survey articles that span the breadth of communications. Submissions will normally be approximately 4500 words, with few mathematical formulas, accompanied by up to six figures and/or tables, with up to 10 carefully selected references. Electronic submissions are preferred, and should be sumitted through Manuscript Central http://mc.manuscriptcentral.com/commag-ieee. Instructions can be found at the following: http://dl.comsoc.org/livepubs/ci1/info/sub_guidelines.html. For further information contact Sean Moore, Associate Editor-in-Chief (smoore-phd@ieee.org). All submissions will be peer reviewed.

BPA WORLDWIDE

TOPICS IN AUTOMOTIVE NETWORKING

SERIES EDITORS: FALKO DRESSLER, OZAN K. TONGUZ, WAI CHEN, LUCA DELGROSSI, TIMO KOSCH, AND TADAO SAITO

CONSUMER COMMUNICATION APPLICATIONS DRIVE NETWORK INTEGRATION

SERIES EDITORS: ALI C. BEGEN, MARIO KOLBERG, MADJID MERABTI, AND STAN MOYER

SERIES EDITORIAL

CONSUMER COMMUNICATION APPLICATIONS DRIVE NETWORK INTEGRATION

Ali C. Begen *Mario Kolberg* *Madjid Merabti* *Stan Moyer*

This theme is strongly reflected in the four articles we have selected for this edition of the Consumer Communications and Networking series. The theme includes the integration of network features as well as new application and network integration. The first article in this edition, by Stuart Jacobs, focuses on the authentication mechanisms in WiMAX-based metropolitan networks. It discusses how digital certificates are handled and highlights the lack of multiple certificate authority support as an issue that prevents the interoperability of WiMAX devices from different manufacturers.

The second article, by Sye Loong Keoh, presents the Marlin initiative as a way of offering seamless content sharing and digital rights management functionality. The article gives particular emphasis to the Octopus and NEMO frameworks within Marlin to achieve this. The article includes examples of industrial adoption of Marlin.

The third article, by Antonio Aragues *et al.*, looks at integration activities in e-health communications. The article argues that due to the increasing introduction of wireless transport technologies in this market, a number of novel technologies have been proposed that can be used in different e-health use cases which can be further extended by device interoperability. The article provides an overview of emerging technologies in this space.

The final article in this issue, by Jose Saldana *et al.*, focuses on whether smarter networks can save bandwidth without adversely affecting online games and thus annoying the gamers. The article uses the example of first-person shooter type online games. The article tests an approach called tunneling, compressing, and multiplexing (TCM) as a technique that enables more players to share the same network links.

Finally, this series has enjoyed enormous success in recent years, with ever increasing submission numbers of high-quality papers. In pushing this series and offering his wealth of experience, Stan Moyer has played a major part in the success of this series. After many years for service to the magazine, Stan has decided to leave this series to concentrate on new opportunities and challenges. We would like to thank Stan for all his work for *IEEE Communications Magazine* and wish him every success in the future. Stan's place on the editorial team will be taken by Ali C. Begen of Cisco. Ali has extensive experience in multimedia networking and communications systems. His contributions and industrial perspective will ensure the series will continue to flourish and serve the magazine readership.

In closing, we would like to remind you that January is again IEEE CCNC time. The Consumer Communications and Networking Conference will be running for the ninth time January 14–17, 2012 in Las Vegas, Nevada. IEEE CCNC 2012 will provide a forum to discuss consumer communications issues mentioned in this edition and many more. See http://www.ieee-ccnc.org for details. As in past years, CCNC will run around the same time as the Consumer Electronics Show (CES), giving you two opportunities to learn more about and see consumer communications in action. We hope to see you in Las Vegas in January!

BIOGRAPHIES

ALI C. BEGEN [M] (abegen@cisco.com) is with the Video and Content Platforms Research and Advanced Development Group at Cisco. His interests include networked entertainment, Internet multimedia, transport protocols, and content distribution. He is currently working on architectures for next-generation video transport and distribution over IP networks, and he is an active contributor in the Internet Engineering Task Force (IETF) in these areas. He holds a Ph.D. degree in electrical and computer engineering from Georgia Tech. He received the Best Student-Paper Award at IEEE ICIP 2003 and the Most-cited Paper Award from Elsevier *Signal Processing: Image Communication* in 2008. Recently, he was general co-chair for the ACM Multimedia Systems Conference 2011. Currently, he is organizing a special session on IPTV and related technologies for Packet Video Workshop 2012. Further information on his projects, publications, and presentations can be found at http://ali.begen.net.

MARIO KOLBERG [SM] is a senior lecturer within the Institute of Computing Science and Mathematics at the University of Stirling. His research interests include peer-to-peer overlay networks, home automation, and IP telephony. He led a project funded by Panasonic (USA) investigating efficiency gains in

SERIES EDITORIAL

structured peer-to-peer overlays. He was the academic supervisor in a Knowledge Transfer Partnership focusing on developing a peer-to-peer overlay for mobile handsets. He is working in the ESRC project Interlife where he is working on using peer-to-peer networks with 3D virtual worlds in an educational context. He is also involved in the MATCH project, focusing on integrating different network technologies for care in the home. He is on the editorial board of the Springer journal *Peer-to-Peer Networking and Applications*, and has a long standing involvement with IEEE CCNC. He served as its TPC Chair for the January 2011 running. He is TPC co-chair of the 5th International Conference on Internet Multimedia Systems Architecture and Applications (IMSAA-11) to be held in December 2011 in Bangalore, India. He has published more than 50 papers in leading journals and conferences. He is a member of a number of international conferences' program committees on networking and communications. He holds a Ph.D. from the University of Strathclyde, United Kingdom.

MADJID MERABTI [M] (M.Merabti@ljmu.ac.uk) is a professor of networked systems and director of the School of Computing and Mathematical Sciences at Liverpool John Moores University, United Kingdom. He holds a Ph.D. from Lancaster University, United Kingdom. He has over 20 years' experience in conducting research and teaching in the areas of computer networks (fixed and wireless), mobile computing, and computer network security. He is widely published, with over 150 publications in these areas, and leads the Distributed Multimedia Systems and Security Research Group. He is principal investigator on a number of current projects: Mobile Networks Security and Privacy Architectures and Protocols, Secure Component Composition in Ubiquitous Personal Networks, Networked Appliances, Mobile and Ad Hoc Computing Environments, Sensor Networks, and computer games technology. He was Guest Editor for the Special issue on Research Developments in Consumer Communications and Networking of *Multimedia Tools and Applications: An International Journal* (Kluwer, September 2005). He is a member of the Steering Committee for IEEE CCNC. He has acted as TPC chair for a number of international conferences, including the 5th IEEE Workshop on Networked Appliances, Liverpool, October 2002. He is a member of a number of international conferences program committees on networking, security, and computer entertainment

STAN MOYER [SM] (smoyer@inventures.com) currently vice president and executive director at Global Inventures. At Inventures, he is responsible for managing technology alliances and collaborations like the SD Card Association, Open Visual Communications Consortium, and Universal PV Interface Alliance. Prior to that he was executive director and strategic research program manager in the Applied Research area of Telcordia, where he worked from 1990 to 2011. He is also past-president of the OSGi™ Alliance, an industry consortium creating specifications for the managed delivery of networked services. He is a member of the Board and Director of Marketing & Industry Relations for the IEEE Communications Society, Vice-Chair of the IEEE CCNC steering committee, and a member of the IEEE GLOBECOM 2012 organizing committee.

WiMAX Subscriber and Mobile Station Authentication Challenges

Stuart Jacobs, Boston University

ABSTRACT

This article examines the subject of authentication within WiMAX (IEEE 802.16-2009) based wireless metropolitan networks. The two WiMAX authentication mechanisms (PKM versions 1 and 2) are discussed and a number of aspects affecting their authentication capabilities presented. Of particular note is the handling of digital certificates and the lack of multiple certificate authority support. This lack essentially prevents the interoperability of WiMAX devices produced by different manufactures. Proposed recommendations are presented that should improve how WiMAX authentication operates and allow for mixed manufacturer device interoperability.

INTRODUCTION

The IEEE 802.16 (WiMAX) specification [1] defines a wireless network technology that telecommunications service providers (TSPs) can use when constructing TSP local and metropolitan access networks. The WiMAX specification primarily focuses on the physical and data link layers, in what is considered medium access control (MAC); yet it does include some network aspects dealing with mobility and management. The MAC functionality is further decomposed into three sublayers:

- A service-specific convergence sublayer (CS) provides any transformation or mapping of external network data.
- A common part sublayer (CPS) provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance.
- A security sublayer provides authentication, secure key exchange, and encryption.

The security sublayer is the primary focus of this article as therein resides responsibility for authentication of fixed and mobile stations which are the devices that rely on WiMAX-based network access. Figure 1 depicts the overall architecture model and scope of the WiMAX security sublayer.

The primary devices within a WiMAX infrastructure include subscriber stations (SSs), mobile stations (MSs), and base stations (BSs). A network control and management system (NCMS) abstraction is also discussed in the specification as a "black box" so that WiMAX physical and MAC layers can be specified independent of overall network architecture (backbone and transport network, and the protocols used at the backend). The NCMS functionality exists within each BS and SS/MS, termed NCMS(BS) and NCMS(SS/MS) as a layer-independent management or control function for coordinating SS/MS and MS access activities with BSs as well as any necessary inter-BS coordination. Herein, the author provides an analysis of how authentication is provided and identifies a number of problems with the specified authentication mechanisms within the IEEE standard.

WiMAX AUTHENTICATION

The WiMAX security sublayer provides SSs with authentication and confidentiality across the WiMAX wireless network by applying cryptographic transforms to MAC protocol data units (PDUs) communicated between the SS/MS and BS. The security sublayer employs an authenticated client/server key management protocol in which the BS, the server, controls distribution of keying material to SS/MS clients. The basic security mechanisms are strengthened by adding digital-certificate-based SS/MS device authentication to the key management protocol. A key management protocol (PKM) is used for authentication, authorization, and distribution of keying data from the BS to the SS/MS.

The security sublayer security components, shown in Fig. 2, include:

- PKM control management: This function controls all other security components.
- Traffic data encryption/authentication processing: This function encrypts or decrypts traffic data.
- Control message processing: This function processes various PKM-related MAC messages.
- Message authentication processing: This function provides data-origin message authentication function.
- RSA-based authentication: This function performs the Rivest, Shamir, and Adleman

0163-6804/11/$25.00 © 2011 IEEE

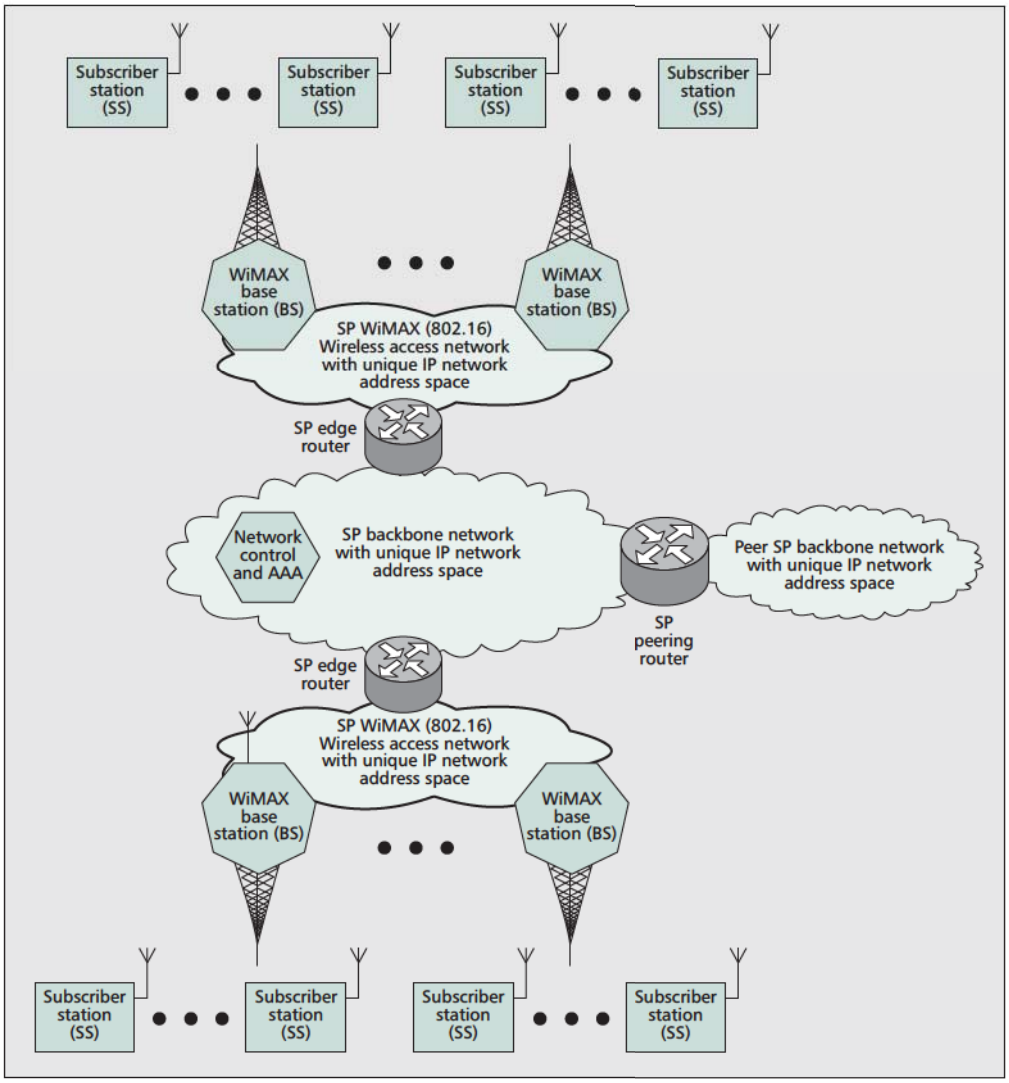

Figure 1. *Overall architecture of the WiMAX security sublayer.*

The WiMAX security sub-layer provides subscriber stations with authentication and confidentiality across the WiMAX wireless network by applying cryptographic transforms to MAC PDUs communicated between the SS/MS and BS.

(RSA)-based authentication function using the SS/MS X.509 digital certificate and the BS's X.509 digital certificate when RSA-based authorization is selected as the authentication approach between an SS/MS and a BS.

- EAP encapsulation/decapsulation: This function provides the interface with the Extensible Authentication Protocol (EAP) method-independent function, when EAP-based authentication is selected between an SS/MS and a BS.
- Authorization/SA control: This function controls the authorization state machine and traffic encryption key state machine.
- EAP method-independent and EAP method-specific entity authentication functionality: These are considered outside of the scope of the WiMAX standard.

There are two versions (PKMv1 and PKMv2) of the PKM protocol, which allow both mutual authentication and/or unilateral authentication (e.g., where the BS authenticates the SS/MS, but not vice versa). In both versions, SS/MS authentication is considered part of the process of SS/MS authorization.

PKM Version 1

PKM version 1 authentication relies on the use of RSA asymmetric encryption, via RSA private/public key pairs, and International Telecommunication Union — Telecommunication Sector (ITU-T) X.509 version 3 (X.509v3) digital certificates, via explicit reference to Internet Engineering Task Force (IETF) Request for Comments (RFC) 3280. An SS/MS begins authorization by sending to a BS an authentication information (Auth Info) message containing the SS/MS manufacturer's certificate authority (CA) X.509 certificate, issued by either the manufacturer's CA itself or an external public key infrastructure (PKI) CA. The Auth Info message is strictly informative, and if the BS chooses to ignore it, the BS internal NCMS function must already possess a copy of the manufacturer CA certificate or reply to the SS/MS that authentication has failed. The SS/MS then sends an autho-

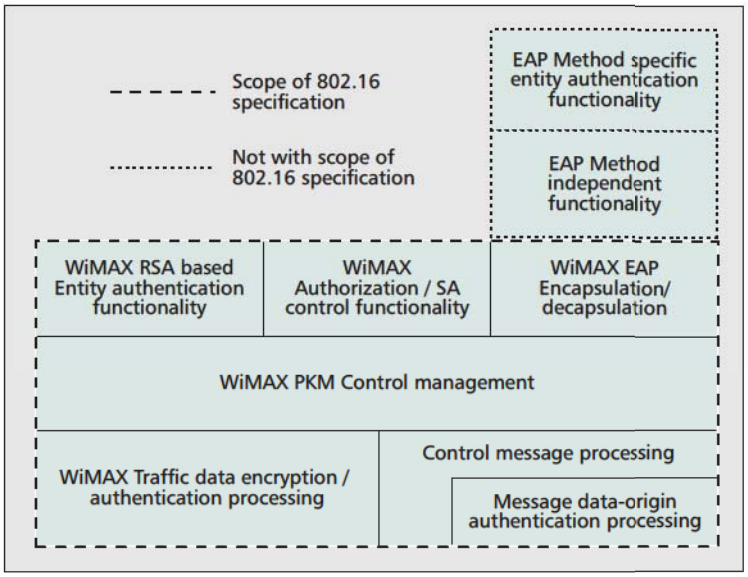

Figure 2. *Security components of the WiMAX security sublayer.*

rization request (Auth Request) message to its BS that includes, among other data items, the X.509v3 digital certificate a manufacturer CA issued to the SS/MS, which contains a verifiable copy of the SS/MS public key.

In response to an Auth Request message, a BS validates the requesting SS/MS identity by comparing the MAC address within the Auth Request message against the common name within the SS/MS certificate contained within the Auth Request message. Since MAC addresses can be "spoofed," this checking for MAC address against common name does not constitute strong authentication of the SS/MS. The BS verifies the SS's certificate by:

- Performing the normal not-before and not-after date checks
- Verifying the digital signature protecting the SS/MS certificate that was created using the public key of the manufacturer CA that issued the SS/MS certificate
- Checking whether the SS/MS certificate is currently valid via a query to an Online Certificate Status Protocol (OCSP) server as specified in RFC 2560

By implication 802.16 appears to require WiMAX implementations to follow RFC 3280 beyond just the format of X.509v3 certificates. RFC 3280 clearly states in section 3.2:

"In general, a chain of multiple certificates may be needed, comprising a certificate of the public key owner (the end entity) signed by one CA, and zero or more additional certificates of CAs signed by other CAs. Such chains, called certification paths, are required because a public key user is only initialized with a limited number of assured CA public keys."

802.16 makes no allowance for processing certification paths; actually 802.16 specifically requires that all SS/MS certificates for a specific brand of SS/MS equipment be issued by a single manufacturer CA. When [2] reported that just five months ago vendors shipped 294.9 million cell phones in the first quarter of 2010, it is reasonable to expect the volume of WiMAX devices to exceed 100 million over a 10-year period, which represents less than 1 percent of the projected volume of cell phones annualized over a 10-year period. Assuming there are 10 WiMAX equipment manufacturers, each producing 1 million units per year, 802.16 would require the CA of each manufacturer to issue over 1 million SS/MS certificates in that period. Common industry practice is for a single CA to issue no more than about 100,000 user/device certificates, thereby limiting CA compromise exposure and enhancing CA performance, which would necessitate a WiMAX manufacturer to use at least a two-tier CA hierarchy.

802.16 does not accommodate real-world CA/public key infrastructure (PKI) deployments regarding certification path processing. Another aspect of 802.16 that deviates from RFC 3280 is how certificate revocation is checked. RFC 3280 specifically discusses the use of certificate revocation lists (CRLs) as the primary mechanism for certificate revocation. Although 802.16 calls for the use of OCSP, defined by RFC 2560, nowhere is RFC 2560 specifically referenced as a formal standard should do.

Another problem with PKMv1 is the lack of mutual authentication, which [3] considered a critical capability in future large-scale wireless metropolitan networks. Reference [4] in their analysis of security issues in [5], which introduced WiMAX mobile stations, concurred with by stating:

"A certificate sent by SS/MS allows BS to authenticate a legitimate SS. On the other hand, SS/MS also needs to authenticate BS to keep away from malicious ones. That is because through the open air interface, SS/MS has no other way to differentiate legitimate BS from malicious adversaries."

802.16 mandates RSA authentication in PKMv1, although it is optional in PKMv2 so PKMv1 continues to include the lack of mutual authentication and the vulnerability this represents. Reference [6] has noted the possibility of denial of service (DoS) attacks, and [7] further noted that:

"Failure to implement proper security procedures can allow malicious nodes to masquerade as legitimate hosts and carry out DoS attacks."

Reference [8] notes the lack of mutual authentication as a problem by stating:

"If X.509-based authentication is used, the likelihood for a user (a MS) to be the victim of BS masquerading is possible because of the asymmetry of the mechanism. For a system, it is unlikely. The impact for a user is high because it can lead to loss of service for long periods of time. The impact for a system is medium, because it can lead to limited financial loss (due to theft of air time). In the case of a user, the risk is critical and countermeasures are needed. For a system, the risk is minor and there is no need for countermeasures."

The above point further emphasizes the need for mutual authentication, especially when MSs are involved.

Another observation regarding PKMv1 focuses on SS/MS authentication. Consumer wireless devices (cell phones) have been routinely illegally copied ("cloning"), which also copies consumer/subscriber authentication credentials stored in the device for the purpose of stealing network services. It is reasonable to anticipate the cloning of WiMAX devices in time where the MAC address within such devices is manipulated by the "cloner" to match the common name of a device's internally stored certificate. Given the likelihood of cloned WiMAX devices, how a WiMAX device stores and protects its RSA private key becomes critical. Currently, devices that contain/store asymmetric private keys store these private keys in a cipher text form that requires decrypting back to a clear text form prior to private key usage. Furthermore, "smart cards" containing asymmetric private keys are designed to resist any economical form of physical and electronic tampering that would divulge the private key in either cipher or clear text form. Unfortunately, 802.16 fails to address private key storage, which implies that private key protection is left to manufacturers, which could easily become a vulnerability.

Assuming the SS/MS sent Auth Request message passes authentication and other checks, the BS sends back to the SS/MS an authorization reply (Auth Reply) message containing a number of data items including an authorization key (AK) which is asymmetrically encrypted using the public key of the SS/MS contained within its certificate. The fact that the Auth Reply message includes material encrypted using the public key of the SS/MS ensures that only the SS/MS possessing the corresponding private key will be able to decrypt the material, thus ensuring confidentiality, but unfortunately not providing any form of BS authentication.

PKM Version 2

PKMv2 provides mutual authentication between an SS/MA and a BS in either of two modes of operation. In the first mode, mutual authentication is provided by PKMv2, which added:

- An SS/MS private-key-based digital signature within the PKMv2 RSA-Request and PKMv2 RSA-Acknowledgment messages
- A BS private-key-based digital signature within the PKMv2 RSA-Reply and PKMv2 RSA-Reject messages

These changes provide strong peer-entity authentication and non-repudiation of these four PKMv2 messages. PKMv2 RSA-based authentication still suffers from the problems associated with PKMv1 relative to the lack of certificate path processing in support of multi-CA organized PKIs, support of CRLs, and an undefined use of OCSP.

PKMv2 was introduced in 802.16-2009 and added a second mode of authentication via EAP, specified in RFC 3748, support in addition to RSA-based authentication. In this second mode, the PKMv2 RSA-based mutual authentication just discussed is followed by EAP authentication allowing PKMv2 RSA-based mutual authentication to be performed only for initial network entry and EAP authentication to be performed for network reentry.

While PKMv2 is a major improvement over PKMv1, it introduced new problems. Within PKMv2, an EAP exchange occurs between the SS/MS and the BS using an operator-selected EAP method (e.g., EAP-TLS specified in RFC 2716) and the credentials appropriate for the EAP method employed, such as an X.509 certificate in the case of EAP-TLS or a subscriber identification module in the case of EAP-SIM. 802.16 considers the particular credentials and EAP methods used as outside the scope of 802.16, but specifies that the EAP method selected should fulfill the mandatory criteria listed in Section 2.2 of RFC 4017 so as to avoid security vulnerabilities.

RFC 4017 states that mutual authentication support is a mandatory requirement and that the current mandatory-to-implement EAP authentication method EAP-MD5-Challenge (RFC 3748 section 5.4), along with the one-time password (RFC 3748 Section 5.5) and generic token card (RFC 3748 Section 5.6) are methods that do not support any of the mandatory requirements defined in Section 2.2 of RFC 4017 regarding mutual authentication. Furthermore, these methods do not support any of the recommended features defined in RFC 4017 Section 2.3 or any of the optional features defined in RFC 4017 Section 2.4.

As EAP-TLS is the only EAP method specifically discussed by 802.16, it deserves further examination. RFC 2716, when discussing fragmentation in Section 3.3, makes the point that a single TLS record may be up to 16,384 octets in length, a TLS message may span multiple TLS records, and a TLS certificate message could be as long as 16 million octets. 802.16 does support fragmentation of the secondary management channel, which would be used for EAP-TLS carrying PKMv2 messages. Since 802.16 specifies a MAC header length field of 11 bits, which restricts MAC PDUs to a maximum length of 2047 octets, one can safely assume that all EAP-TLS records will require fragmentation. A worst case EAP-TLS certificate message of 16 million octets would have to be fragmented into some 7800 MAC PDUs. Thus, it is a serious oversight that 802.16 does not discuss the likely need for fragmentation of EAP-TLS messages.

Another aspect of EAP-TLS is how it performs identity verification (as covered in RFC 2716 Section 3.4), based on matching a server or supplicant/peer claimed identity against the name in a presented digital certificate, yet RFC 2716 does not identify whether the match is against the digital certificate Certificate.subject distinguished name field (see the table of fields in RFC 2716) or the common name of an identifier within a certificate alternative name extension. This lack of specificity within RFC 2716 is problematic at best and will likely cause interoperability issues. Another EAP-TLS deficiency in identity verification is that EAP-TLS does not make use of digital signatures, as is done in TLS and specified in RFC 5246. Certificate authenticity and revocation are also problematic in EAP-

The fact that the Auth Reply message includes material encrypted using the public key of the SS/MS ensures that only the SS/MS possessing the corresponding private key will be able to decrypt the material, thus ensuring confidentiality, but unfortunately not providing any form of BS authentication.

Digital certificates are a primary component of RSA authentication in both PKM versions 1 and 2. 802.16 clause 7.6.1 deserves further consideration as this clause describes the X.509 Version 3 certificate format used in WiMAX-compliant devices.

X.509 v3 field	Description
Certificate.version	Indicates the X.509 certificate version and always set to v3
Certificate.serialNumber	Unique integer the issuing CA assigns to the certificate
Certificate.signature	Defines the algorithm used to sign the certificate
Certificate.issuer	Distinguished Name of the CA that issued the certificate
Certificate.validity	Specifies when the certificate becomes active and when it expires
Certificate.subject	Distinguished Name identifying the entity whose public key is certified in the Certificatesubjectpublic key information field
Certificate.subjectPublicKeyInfo	Contains the public key, parameters and key usage algorithm identifier
signatureValue	Digital signature spanning all other certificate fields

Table 1. *X.509 Version 3 digital certificate primary fields.*

TLS. RFC 2716 notes in section 6.1 that the EAP server, as it has existing Internet access, is able to perform certificate path processing and CRL checks; yet the supplicant/peer will not likely have Internet access and will be unable to perform either activity.

A final concern with WiMAX use of EAP-TLS is that the supplicant/peer/client (SS/MS) negotiates a cipher suite with the EAP-TLS server, not with the EAP-TLS authenticator (the BS) when EAP server and authenticator functions are not collocated within the BS. When the EAP server and authenticator reside in separate devices:

- There needs to be some mechanism by which the negotiated cipher suite is communicated to the authenticator (BA) by the EAP server, which RFC 2716 considers out of scope.
- The SS/MS is unable to authenticate the BS.

802.16 states that each BS is required to perform certificate path processing, yet fails to identify the manner in which this processing is to occur. However, this point is not discussed within the descriptions of either PKM versions 1 and 2; nor do the state machines for these protocols include certificate path processing as states or transition initiators between states.

Keys and Certificates Used by WiMAX

One important area worth considering is effective RSA key length since 802.16 specifies the use of either 1024- or 2048-bit RSA keys. Reference [9, Table 2] proposes that an RSA key of 1024 only provides 80 bits of security and an RSA key of 2048 only provides 112 bits of security due to attacks on the RSA algorithm. These attacks leverage the computational resources now available with the advent of micro supercomputers, based on products like the NVIDIA Tesla C1060, which provides 933,000 MIPS (MFlops), available since 2008 with a list price under $10,000.

Digital certificates are a primary component of RSA authentication in both PKM versions 1 and 2. 802.16 clause 7.6.1 deserves further consideration as this clause describes the X.509 Version 3 certificate format used in WiMAX-compliant devices. Table 1 identifies the primary fields of an X.509 Version 3 certificate.

There are a number of certificate fields used by WiMAX in either a non-standard manner or will cause problems. These fields are:

Certificate.signature specifies use of the RSA signature algorithm using SHA-1. However, the RSA private keys used to sign these certificates are required by 802.16 to use key lengths that are rapidly becoming considered insufficient.

Certificate.issuer of SS/MS and BS certificates contains the Distinguished name of the issuing manufacturer CA.

Certificate.issuer of manufacturer CA certificates contain either the Distinguished name of the issuing manufacturer CA or the distinguished name of an external PKI CA

signatureValue of SS/MS and BS certificates contains the RSA-SHA-1 signature computed over the ASN.1 DER encoded Certificate using the manufacturer CA's private key. However the RSA private keys used to sign these certificates are required by 802.16 to use key lengths that are rapidly becoming considered as insufficient.

Certificate.validity.notBefore and **Certificate.validity.notAfter** have a validity period greater than the likely operational lifetime of the SS/MS, with a validity period beginning with the date of generation of the device's certificate and extending out to at least 10 years after that manufacturing date. Requiring SS/MS certificates to have a lifetime up to 10 years is not the norm for retail devices (VeriSign only issues certificates with one-year lifetimes, and most private PKIs stipulate an end device certificate lifetime of about five years).

Certificate.subject of SS/MS certificates contain the distinguished name of the SS/MS

with the common name part set to the device's MAC address set to six pairs of hexadecimal digits separated by colons, which is a non-standard form of common name.

Certificate.subject of BS certificates contain the distinguished name of the BS with the common name part set to the device's BS identifier (BSID) where the BSID field is operator-defined and set to six pairs of hexadecimal digits separated by colons, which is a non-standard form of common name.

Some additional observations about the above certificate fields and their usage are worth noting:

- As already noted earlier in this article, the certificate profile used in WiMAX does not allow for a multiple-CA hierarchy.
- It is assumed that the same manufacturer CA issues certificates to all SS/MSs and BSs of a TSP, which will cause problems when SS/MS devices are not manufactured by the same provider of BSs since cross-CA certification is not considered within 802.16.
- No details are provided regarding CAs that are part of a PKI not directly operated by a WiMAX equipment manufacturer.

When discussing the storage and processing of certificates, 802.16 expects manufacturer issued SS/MS certificates to be loaded into SS/MA permanent write once memory along with a manufacturer installed RSA private key. 802.16 does not discuss any protection mechanisms for these private keys. For any SS/MS device that internally generates its own RSA key pair some undefined mechanism is to be used for securely requesting the creation of a digital certificate or private key secure storage considered.

802.16 requires that manufacturer CA certificates are to be embedded into the SS/MS software, unlike most other systems that store all certificates internal within a common certificate storage area. Even where a manufacturer issues SS/MS certificates by multiple manufacturer CAs, the certificates of all these manufacturer CAs are expected to be embedded with the SS/MS software. This embedding of certificates directly into SS/MS software complicates certificate replacement by necessitating complete software replacement/reloading rather than the more straightforward replacement of just stored certificates.

Concluding Remarks

Generally, RSA asymmetric encryption, when coupled with a PKI, provides highly reliable peer-entity authentication and non-repudiation. These security services are the result of a recipient of a message digitally signed by the sender's private key:

- Having high assurance that the sender's private key has not been stolen or lost, or is still valid for use by the signer.
- The message recipient possesses an authentic copy of the sender's public key.

The first point is achieved by the recipient being able to verify that the certificate associated with the sender's private key has not been revoked prior to the certificate's notAfter date. The second point is achieved by the recipient being able to establish a chain of digital signatures on certificates starting from the sender's certificate to the certificate of the CA that issued the sender's certificate and continuing up a chain of CA certificates until a CA is identified that is within the hierarchy of CAs leading down to the CA that issued the recipient's certificate.

The primary EAP method 802.16 discussed is EAP TLS; however, there are a number of EAP methods that may be as, if not more, appropriate. For example, EAP-TTLS (RFC 5281) and EAP-IKEv2 (RFC 5106) methods should be considered for inclusion in PKMv2 as part of a future version of IEEE 802.16.

The lack of specificity within 802.16 for:

- Certificate path processing
- Secure storage of RSA private keys
- Usage of OCSP (or alternatively CRL retrieval and checks)
- Secure generation of requests for CA issuance of certificates by those SS/MS devices that internally generate their own RSA key pairs

are points for concern that a future version of IEEE 802.16 should address. Such a future version of 802.16 should also include support for:

- RSA key lengths greater than 2048
- Multiple CA hierarchies
- Cross CA certification

For an SS/MS initially entering a WiMAX network, using OCSP or CRLs for certificate revocation is a problem as the SS/MS does not yet possess Internet access. However, this can be overcome by having the SS/MS perform such checks once it does obtain Internet access but prior to using said access for communicating non-management traffic/information. Such an approach has been described in [10, Section 8], which proposes a delayed check for certificate revocation. Another aspect of [10] is the distribution of complete certificate chains whenever an end device certificate is shared, which allows for both single rooted certificate hierarchies and cross-CA certified hierarchies.

This embedding of certificates directly into SS/MS software complicates certificate replacement by necessitating complete software replacement/ reloading rather than the more straightforward replacement of just stored certificates.

References

[1] R. Marks *et al.*, "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air interface for Broadband Wireless Access Systems," May 29, 2009; http://standards.ieee.org/getieee802/802.16.html

[2] IDC, "Mobile Phone Recovery Continues with Nearly 22 percent Growth in First Quarter, According to IDC," Apr. 2010; http://www.idc.com/getdoc.jsp?containerId=prUS22322210

[3] Y. Zhang and Y. Fang, "A Secure Authentication and Billing Architecture for Wireless Mesh Networks," *Wireless Networks*, vol. 13, no. 5, 2007, pp. 663–78; http://portal.acm.org.ezproxylocal.library.nova.edu/citation.cfm?id=1295219.1295226&coll=ACM&dl=ACM&CFID=100594914&CFTOKEN=46300227

[4] S. Xu, M. Matthews, and C. Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16," *Proc. 44th annual Southeast Regional Conf.*, 2006, Melbourne, FL, pp. 113–18.

[5] B. Kiernan *et al.*, "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1," May 2005;

http://standards.ieee.org/getieee802/download/802.16e-2005.pdf

[6] S. Maru and T. X. Brown, "Denial of Service Vulnerabilities in the 802.16 Protocol," *Proc. 4th Annual Int'l. Conf. Wireless Internet*, Maui, HI, 2008; http://portal.acm.org.ezproxylocal.library.nova.edu/citation.cfm?id=1554126.1554172&coll=ACM&dl=ACM&CFID=100594914&CFTOKEN=46300227

[7] K. Sethom, H. Afifi, and G. Pujolle, "A Distributed and Secured Architecture to Enhance Smooth Handoffs in Wide Area Wireless IP Infrastructures," *SIGMOBILE Mob. Comp. Commun. Rev.*, 2006, vol. 10, no. 3, pp. 46–57.

[8] M. Barbeau, "WiMax/802.16 Threat Analysis," *Proc. 1st ACM Int'l. Wksp. Quality of Service & Security in Wireless and Mobile Networks*, 2005, Montreal, Quebec, Canada, pp. 8–15.

[9] E. Barker *et al.*, "Recommendation for Key Management – Part 1: General (Revised)," NIST Special Pub. 800-57, Mar. 2007; http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

[10] S. Jacobs and S. Belgard, "Mobile IP Public Key Based Authentication," draft-jacobs-mobileip-pki-auth-03.txt, July 2001, IETF expired Internet draft; http://tools.ietf.org/id/draft-jacobs-mobileip-pki-auth-03.txt.

BIOGRAPHY

STUART JACOBS [M] (sjjacobs@bu.edu) is a lecturer in Boston University's Metropolitan College Computer Science Department with responsibilities for teaching graduate courses on enterprise information security, network security, and network forensics along with advising on security curricula issues and new security course development. He is an Industry Security Subject Matter Expert for the Alliance for the Telecommunications Industry Solutions (ATIS) and served as Technical Editor of the ATIS Technical Report, "Information & Communications Security for NGN Converged Services IP Networks and Infrastructure" and as the Technical Editor of ITU-T M.3410, "Guidelines and Requirements for Security Management Systems". He is currently working on a doctoral degree at Nova Southeastern University in information systems security. He retired from Verizon Corporation in 2007, after 40 years in industrial engineering, where he was a Principal Member of Technical Staff with responsibility for security architecture development, security requirements analysis, and standards development activities. As a Verizon lead security architect, he was the lead engineer for security on numerous Verizon network equipment RFPs and provided security consulting on wireless and wired networks, SS7, CALEA/LI, vulnerability analysis, intrusion detection, and systems engineering methodologies. Additionally, he served as Verizon's security subject matter expert for ANSI-ATIS, ITU-T, TMF, OIF, MSF, OMG, and IETF activities. He holds an M.Sc. degree and CISSP Certification, and is a member of the Association for Computing Machinery (ACM), International Information Systems Security Certification Consortium (ISC2); and Information Systems Security Association (ISSA). His research interests include NGN and IMS architecture security issues, management of security in NGNs as well as MANET and Mobile IP security. His book *Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance* is part of the IEEE Press Series on Information and Communication Networks Security.