AN AUTHENTICATION PROTOCOL FOR MOBILE CELLULAR NETWORK

L. A. Mohammed, Abdul Rahman Ramli, Mohamed Daud*, and V. Prakash
Department of Computer and Communications System Engineering
*Department of Biological and Agricultural Engineering
43400, UPM Serdang, Selangor, Malaysia
Tel. : 012-6589205
email : gs00607@stud.upm.edu.my

ABSTRACT

Current cellular telephone system is vulnerable to various attacks. With more complicated equipments, it is possible to receive the ESN and PIN of legal user and use them to commit cellular telephone frauds. Generally, the frauds can be classified into three: subscription fraud, technical fraud, and internal fraud. This paper analyses the frauds in cellular mobile communication and provides an efficient authentication protocol that can be taken to protect the current system.

Keywords: ***Cellular telephone fraud, Key management, Authentication protocol***

1.0 INTRODUCTION

The main objective of security in cellular mobile communication systems is to secure the conversations and signaling data from interception as well as preventing the system from other frauds such as *cloning* and the like. With the older analog-based cellular telephone system such as *Advance Mobile Phone System* (AMPS), it is relatively simple matter to intercept cellular telephone conversation with a police scanner. Cellular companies lose a substantial amount of money per year to cellular fraud. One cause of this fraud is cloning of cellular telephones. Federal Communications Commission (FCC) estimated that the cellular industry loses more than $650 million per year to fraud [1]. As a result of this, the *Wireless Telephone Protection Act* (Public Law 105-172) was signed into law on April 24, 1998 in the USA, expanding the prior law to criminalise the use, possession, manufacture or sale of cloning hardware or software.

This paper is organised as follows: The next section explains how a phone call is made in a mobile telephone system. Security issues are discussed in Section 3, it gives a brief explanation of mobile phone cloning and a survey of some authentication protocols (we gave an overview of GSM authentication protocol as an example) and Beller-Chang-Yacobi protocol that form a foundation of our analysis. Then, in Section 4 we design a better method that can be implemented. Finally, in Section 5 we conclude with an analysis of the new scheme.

2.0 MAKING CELLULAR RADIO CALLS

A wireless network is typically organised into geographical region called cells. Before a mobile user can communicate with other user(s) in the network, a connection must usually be established between the users. The establishment and maintenance of a connection in a cell is the responsibility of the *base station* (BS). If a mobile user wants to make a call, the mobile handset scans the predetermined channels to determine the strongest control channel, and monitors it to receive network status and availability information. When the telephone number of the destination has been dialed by the customer and the *send key* has been pressed, the mobile handset finds a free control channel and broadcast a request for a user channel. On the receipt of such a request by any *base station* (a transmitter which emit and receive radio signals from mobile station), a message is sent to the nearest *mobile switching center* (MSC), indicating both the desire of the mobile station to place a call and the strength of the radio signal received from the mobile. The MSC determines which base station has received the greatest signal strength, and, based on this, decide which cell the mobile is in. It then requests the mobile handset to identify itself with an authorisation number that can be used for call charging. Following authorisation of an outgoing call, a free radio channel is allocated in the appropriate cell for the carriage of the call itself, and the call is extended to its destination on the public switching telephone network. At the end of the call, the mobile station generates an *end of call* signal which causes release of the radio channel, and reverts handset back to monitoring the control and paging channel.

3.0 SECURITY ISSUES

Fraud in cellular communication system can be categorised into three:

1. Internal fraud - this involves an insider who is working in the cellular company. He/she may register fake subscriber so as to gain the financial benefit from the company.
2. Subscribers fraud – subscribers giving fake addresses and identities during registration so that the bills cannot sent to them (they cannot be charged).
3. Cloning – Using legitimate subscribers line to make calls (details is given in Section 3.1). The main objective of this paper is to develop an authentication and integrity scheme that can be used to authenticate a legitimate user. Authentication is simply making sure users are who they say they are. Integrity is knowing that the data sent has not been altered along the way. Message integrity is maintained with digital signatures. A digital signature is a block of data at the end of a message that attests to the authenticity of the file. If any change is made to the file, the signature will not verify. Digital signatures perform both an authentication and message integrity function.

3.1 Cloning

Cloning in cellular telephone is a process of reprogramming a mobile phone to transmit the electronic serial number (ESN) and telephone number (MIN) belonging to a legitimate user. Unscrupulous persons obtain valid ESN/MIN combination by illegally monitoring the transmissions from the cellular telephones of legitimate subscribers. As a result of this, the cellular system cannot distinguish the cloned cellular from the legitimate one. A clone cellular phone can then be used to make calls that will be billed to the legitimate subscriber. According to [2], within telecommunications, energy and cable sector, the wireless phone industry is particularly hard-hit. The cloning/roaming fraud of the past has become subscription/application fraud of today. The mobility of the telephone, the resale value of the instrument and the high value of telecommunication services make this sector a tempting target for fraud. It was mentioned that credit application fraud is estimated to cost more than US$35 billion annually.

3.2 Authentication Protocols

The general idea of identification involves a claimant A and a verifier B. The verifier presented with, or presumes beforehand, the purported identity of the claimant. The goal is to corroborate that the identity of the claimant is indeed A (i.e. to provide entity authentication). Entity authentication plays an important role in ensuring data secrecy and authenticity because of its goals of allowing any pair of communicating parties to mutually verify each other's identity. We can therefore define entity authentication as the process whereby one party is assured of the identity of the second party involved in a protocol, and that the second party actually participated (is active at, or immediately prior to, the time the evidence is acquired.

The objectives of authentication protocol include the following:

- A is able to successfully authenticate itself to B.
- Transferability – B cannot reuse an identification exchange with A so as to successfully impersonate A to a third party C.
- The probability of impersonation should be negligible.
- The system should be able to detect some well-known attacks such as: *replay*, *interleaving*, *reflection*, *chosen-text*, *forced delay, stealth of information,* etc.

Some identification protocols are summarised below:
Zero-knowledge protocols – Generally, A identify itself to B by showing that he/she knows some secret *S* corresponding to some public number *x*, without revealing any computational knowledge about *S*. It should be very hard for some one not knowing *S* to claim he knows it. However, as indicated in [3] it is possible while A is proving he is *A* to *B*, *B* helps *C*, in real-time, to prove to D the false claim that *C* is *A*. Solutions to avoid this drawback have been proposed in [3, 4]. Detail of such protocol is given in [5]. Further survey is given in [6, 7, 8].

Challenge-response protocols – the idea here is that the claimant proves its identity to the verifier by demonstrating knowledge of certain secret known to be associated with that entity, without revealing the secret itself to the verifier during the protocol. However, in some situations, the secret is known to the verifier, and is used to verify the response, whereas in other situations, the verifier does not need to know the secret. This can be achieved by providing a response to a time-variant challenge, where the response depends on both the entity's secret and the challenge. Challenge response operations is a popular approach for ensuring freshness in entity authentication, it can be implemented based on symmetric-key or asymmetric-key techniques. Details can be found in [9] and [10]. However, a potential drawback with the use of random number challenge was identified in [11].

Password – This is considered to be a weak authentication protocol. It associates with each user a string of characters that the user and the server can share in order to identify a legal user. In some schemes *userid* and password are used together in which *userid* is a claim of identity, and password is the evidence supporting the claim. There are many types of password schemes, for example, personal identification number (PINs) is considered to be part of time-variant passwords. Though generally speaking passwords are classified as weak authentication techniques, however, there are many ways of making it a little bit harder to break.

3.3 Key Distribution Protocols

There are two types of key distribution protocols namely centralised key distribution protocol and public key distribution protocol. The centralised key distribution protocols like [12] assumes that a network has a centralised key distribution facility which distributes a session key to the requesting terminals. The session key is encrypted by the terminal's encryption key. If classical key cryptographic method is employed for the key encryption, then the central facility should manage each user's private key. If a public key cryptographic method is employed for the key encryption, then the management problem is reduced. Decryption at a hardware limited user terminal may, however, take an impractically long time.

Public key distribution protocol, invented by Diffie and Hellman [13], enables direct key distribution between two user terminals in a system and eliminates the key management problem at a network center. This protocol requires computation in a finite field. For the scheme to be secure, the order of the finite field should be very large, making realization of this scheme impractical without using special hardware or high-speed digital signal processors (DSP's).

3.4 GSM Authentication Protocol

The GSM security consists of subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. The subscriber is uniquely identified by the International Mobile Subscriber Identity (IMSI). The MS identifies itself by means of a Temporary Mobile Subscriber Identity (TMSI), which is issued by the network and may be changed periodically during handover for additional security. The security design is in such a way that the information will never be transmitted over the radio channel. The authentication protocol is carried out through a challenge response mechanism which consists of asking the subscriber so that only the right user equipment *Subscriber Identity Module* (SIM) can answer. The feedback computed internally in the SIM card will then be compared in the authentication center [14, 15,16, 17]. In practice, a 128-bit random number (RAND) is sent to the MS and the signed result (32-bit) or SRES (expected answer) is returned. This is generated locally and by *Home Location Register/Authentication Center* (HLR/AC) and then combined with the user's secret key K_i through the authentication algorithm (A3) to get the SRES. The AC is responsible for generating the sets of RAND, SRES, and K_c which are stored in the HLR and *Visitor Location Register* (VLR) for subsequent use in the authentication processes. If the received SRES agrees with the calculated value, the *Mobile Station* (MS) has been successfully authenticated and may be given access. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS. Each time a mobile station is authenticated, the network and the MS has to compute the ciphering key K_c (using A8 algorithm) which is used for encrypting and decrypting the transmitted data. *Equipment Identity Register (*EIR) is a database that contains a list of valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The mobile station is continuously listening to the location area identity (LAI) being transmitted on the broadcast channel, comparing the new LAI received with the last LAI (stored in the SIM). Whenever the received LAI is different from the old LAI stored in its SIM card the MS proceed with a new registration. The registration starts first with getting access to the *Stand-alone Dedicated Control Channel* (SDCCH) over which the *Base Transceiver Station* (BTS) and the MS communicates with each other. Detail is available in GSM Recommendations 02.09 [18]. Fig. 1 below shows the architecture of GSM. All radio-related functions are performed in the *Base Station Subsystem* (BSS), which consist of *Base Station Controllers* (BSC) and the base station transceivers (BTSs). The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in base transceiver stations. A number of BSCs are served by an MSC. The BTS handles the radio interface to the mobile station. The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network.

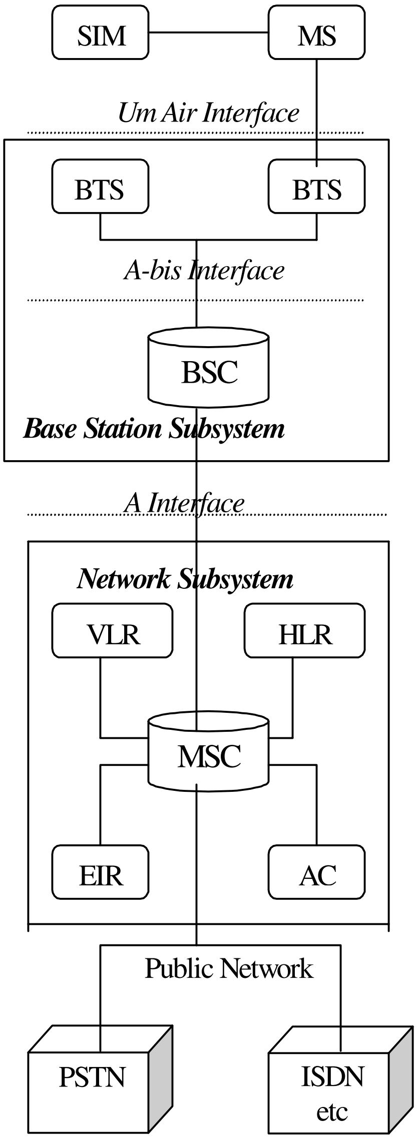

Fig. 1: Architecture of GSM system

A group of BTSs are controlled by a BSC. *The Public Switched Telephone Network* (PSTN) is made of local networks, the exchange area networks, and the long-haul network that interconnect telephones and other communication devices on a worldwide basis.

4.0 THE PROPOSED PROTOCOL

First, the Beller-Chang-Yacobi's protocol [14] is briefly reviewed here. We will then show how it can be implemented in a mobile network system, followed by the main drawback of the protocol and some counter measures against the drawback.

Beller-Chang-Yacobi protocol is partially based on the Diffie-Hellman key distribution scheme [13]. We briefly review the protocol as follows: Let N be a large prime and α be a primitive element of the Galois field *GF(N)*, both N and α are public. Each user μ selects his/her own secret key S_μ in *GF(N)*, and calculate the public key $P_\mu, \equiv \alpha^{S\mu}$ *(mod N)*. Two users μ_i and μ_j can compute a common secret key K_{ij} by

$$K_{ij} \equiv (P_i)^{Sj} \ (mod\ N) \equiv \alpha^{SiSj} \ (mod\ N) \equiv (P_j)^{Si} \ (mod\ N)$$

Beller-Chang-Yacobi considered a more general case where N can be obtained from two large primes. The protocol can be used in a mobile cellular system as follows:

Let (U) be the set of all users (i.e. $\forall$ Mobile Station (MS) $\exists\ \mu \in U$), Base Station (B), and Mobile Switching center (MSC). Then for every user $\mu\ \exists$ a pair of public and secret keys (P_μ, S_μ). B also has a pair of (P_B, S_B), Where $P_B \equiv \alpha^{SB}$ *(mod N).* We assume that MSC is also the certification authority or *CA*. *CA* issues certificate for each user and each base station as well as P_μ and P_B. We define the certificate as follows:

$$Sig_{CA}\ (\mu) \equiv (h\ (\mu, P_\mu))^{1/2}\ (Mod\ N_{CA})$$
$$Sig_{CA}(B) \equiv (h\ (B, N_B, P_B))^{1/2}\ (Mod\ N_{CA})$$

Where h is a one-way hash function known to the public. N_B is the product of two large primes associated with B. Similarly N_{CA}. N_B and N_{CA} are made public (their prime factors must be kept secret). Lastly, we can use any secret key encryption algorithm such as IDEA, DES, or Rijndael.

Summary of the steps:

1. $\mu \Rightarrow B$ *(request for service)*
2. $\mu \Leftarrow B\ (B, N_B, P_B, Sig_{CA}(B))$
3. μ *checks if* $(h\ (B, N_B, P_B)) \equiv Sig^2_{CA}(B)\ (mod\ N_{CA})$
4. $\mu \Rightarrow B\ (e_2, e_3)$
5. *B extracts x from* e_2 *and use it to decrypt* e_3 *and check if* $h(\mu, P_\mu) \equiv Sig^2_{CA}(\mu)\ (mod\ N_{CA})$
6. $\mu \Leftrightarrow B$ *(using session key sk)*

Note that the numbers e_2, e_3 are defined as:

$$e_2 = x^2\ (mod\ N_B)$$
$$e_3 = encrypt\ x\ (\mu, P_\mu, Sig_{CA}(\mu))$$

x is a random number between 1 and $N_B - 1$. B extracts x from e_2 as and uses e_3 as follows:

$$x \equiv (e_2)^{1/2}\ (mod\ N_B)$$
$$(\mu, P_\mu, Sig_{CA}(\mu)) = decryptx\ (e_3)$$

It is easy to see that μ and B can respectively calculate:

$$\Re \equiv P_B^{S\mu}\ (mod\ N),\ \ sk = encrypt\Re\ (x)$$
$$\Re \equiv P_\mu^{SB}\ (mod\ N),\ sk = encrypt\Re\ (x)$$

sk is now the session key for μ and B.

5.0 ANALYSIS AND CONCLUSION

The major problem with Beller et. al. scheme is concern with *replay* attacks. For instance, an attacker T can obtain the public key and the digital signature of μ i.e. $(\mu, P_\mu, Sig_{CA}(\mu))$. T can then impersonate μ and initiate the protocol with B. Next we show how this can be prevented in three different ways:

Method 1 (Using nonce):
Recall that ⊕ denotes bit-wise exclusive-or operation, and *CA* is a mediator between B and μ, we consider the following steps:

1. $\mu \Rightarrow CA$: $\{AI_\mu, I_B\}P_{CA}$
2. $CA \Rightarrow \mu$: $\{AI_\mu, I_B, (n_{CA})\}K_\mu$
3. $\mu \Rightarrow B$: $\{AI_\mu, I_B, \mu n_1, \mu n_2\ (n_{CA})\ K_\mu\}P_{CA}$
4. $B \Rightarrow CA$: $(\{AI_\mu, I_B, \mu n_1, \mu n_2\ (n_{CA})\ K_\mu\}K_B)\ P_{CA}$
5. $CA \Rightarrow B$: $\{AI_\mu, I_B, (n_{CA})\}K_B$
6. $B \Rightarrow CA$: $\{I_B, AI_\mu,, Bn_1, Bn_2\ (n_{CA})K_B\}P_{CA}$

7. $CA \Rightarrow B: \{\mu n_1, K_{\mu B} \oplus \mu n_2\}K_{\mu}, \{Bn_1, K_{\mu B} \oplus Bn_2\}K_B$
8. $B \Rightarrow \mu: \{\mu n_1, K_{\mu B} \oplus \mu n_2\}K_{\mu}, \{f_1(r\mu), rB\}K_{\mu B}$
9. $B \Leftarrow \mu \{f_2(rB)\}K_{\mu B}$

Where
K_{μ}, K_B, $K_{\mu B}$ denote a session key between *CA* and μ, *CA* and *B*, and μ and *B* respectively. n_{CA} denote a nonce issued by *CA*. P_{CA} denotes *CA's* public key. AI_{μ}, and I_B denote anonymity ID of μ, and ID of *B* respectively. μn_1, μn_2, Bn_1, Bn_2 are random numbers generated by μ and *B*. $(r\mu)$ is a challenge and $f(r\mu)$ is the response encrypted using the session key $K_{\mu B}$. Note that AI_{μ} is the anonymity of user μ, it should contain some secret information only known and can only be used by *CA* alone.

Method 2 (one-time signature)
One-time signature can be used instead of normal signature as shown in Section 5. There are many options here [19, 20], etc, we will give example based on Shimon et. al [21] method: We assume that μ has stored a pre-computed signature *Sig* (using the pair of one-time $(P_{\mu}*, S_{\mu}*)$ keys), *Sig* can be defined as $S_{S\mu*}(P_{\mu}*)$. To sign a message *M*, μ uses *Sig* and $(P_{\mu}*, S_{\mu}*)$, then uses a hash function *h* i.e. *h(M)* and then computes the one-time signature:

$$\Upsilon = S_{S\mu*}(h(M))$$

The signature of *M* consists of the concatenation of $P_{\mu}*$, *Sig*, and Υ. *CA* can then verify $P_{\mu}*$, *Sig*, and Υ with respect to P_{μ} using a verification algorithm *V*. First, *CA* uses *V* and P_{μ} to check whether *Sig* is a signature of P_{μ}, *CA* then computes $f = h(M)$ to check whether Υ is a signature of with respect to $P_{\mu}*$. The verification can be written as:

- $V1\ P_{\mu}\ (P_{\mu}*,Sig)$
- $V2P_{\mu}*,(h(M), \Upsilon)$

Note that the hash function is also a one-way hash function. Therefore, even if an attacker attempt to replay an old $P\mu*$ and forge Υ for a new $M*$, this will amount to either attacking the one-time signature, i.e. $h(M*)$ which is different from all previously hashed values or finding a new $M*$ such that $h(M) = h(M*)$. Since h is one-time this implies $h(M)$ will never be equal to $h(M*)$. The reader can refer to [21] for the proof of the theoretical result.

Method 3 (timestamp)
The main drawback of method 1 and 2 is time consuming. Therefore in some situations whereby charges are considered to be less, a timestamp approach can be used (e.g. for local calls). This can be achieved as follows:

$$\mu \Rightarrow CA: (\tau s\ ||r\mu)^e\ (mod\ N)$$

Where τs is timestamp, $||$ denotes concatenation, rμ is the random number generated by μ and *e* is the encryption exponent. In this case, *CA* should have the means of checking the timeless of the timestamp. Note that τs may include date, time, expiring date etc.

We have shown that by modifying Beller's et. al. scheme it will be good enough to ensure authentication and identification in a mobile cellular network system. Our proposed scheme ensures confidence to the communicating parties that at the time of request, an entity cannot masquerade as another and cannot mount a replay attack as both *U* and *B* rely on the authentication server *CA*, since *CA* can reliably verify the identity of both *U* and *B*. Moreover, our scheme is not vulnerable to attack from eavesdroppers. This is achieved by establishing a session key between *U* and *CA*, *U*, *CA*, and *B*, and finally between *U* and *B*. In some situations users might wish to keep their IDs secret. AI_{μ} (anonymity ID of U) can be used to hide the real ID of users, so that only *CA* knows the mapping between AI_{μ} and *real* I_{μ}.

REFERENCES

[1] FCC - Federal Communications Commission, "Cellular Fraud": *http://www.fcc.gov/wtb/cellular/cellfrd*.html (Visited on 10/7/2001).

[2] L. Porter, "Application Fraud: An Old Problem Receives New Medicine". *Global Communication Interactive*, 2000, pp. 64-66.

[3] S. Bengio, et. al., "Secure Implementations of Identification Systems". *J. of Cryptology,* 4, 1991, pp. 175-183.

[4] T. Beth and Y. Desmedt, "Identification Tokens-Or: Solving the Chess Grandmaster Problem", in *Advances in Cryptology- Crypto'90, Proceedings (Lecture Notes in Computer Science 537)*, A. J. Menezes and S. A. Vanstone Eds. Springer-Verlag pp. 1991, 69-176.

[5] S. Goldwasser et. al., "The Knowledge Complexity of Interactive Proof Systems". *Siam J. Comput. Systems.* 1, 1989, pp. 186-208.

[6] A. Mitopoulos and H. Meijer, "Zero Knowledge Proofs – A Survey". *Technical Report No. 90-IR-05*, Queen's University, Ontario, Canada, 1990.

[7] O. Goldreich and Y. Oren, "Definitions and Properties of Zero-Knowledge Proof Systems". *J. of Cryptology,* 7, 1994, pp. 1-32.

[8] G. Brassard, D. Chaum, and C. Crefeau, "Minimum Discloser Proofs of Knowledge". *J. of Comput. and System Sciences*, 37, 1988, pp. 156-189.

[9] K. Y. Lam and D. Gollman, "Freshness Assurance of Authentication Protocols". *Euro. Symposium on Research in Computer Security*, Toulouse, France, Nov. 1992.

[10] K. Y. Lam and T. Beth, "Timely Authentication in Distributed Systems". Deswarte G., et. al. Eds. *Second European Symposium on Research in Computer Security – ESORICS'92 (LNCS 648),* Springer-Verlag, 1992. pp. 293-303.

[11] C. J. Mitchell and A. Thomas, "Standardizing Authentication Protocols Based on Public Key Techniques". *J. of Comput. Security,* Vol. 20, No. 1, 1993.

[12] D. E. Denning, *Cryptography and Data Security*. Addison-Wesley, 1983.

[13] W. Diffie and M. Hellman, "New Directions in Cryptography". *IEEE Trans. On Info. Theory,* Vol. IT-22, No. 6, 1976, pp. 644-654.

[14] J. M. Beller et. al., "Privacy and Authentication on a Portable Communications System". *IEEE Journal on Selected Areas in Communications*, Vol. 11, No. 6, Aug. 1993, pp. 821-829.

[15] D. Brown, "Techniques for Privacy and Authentication in Personal Communication Systems". *IEEE Personal Communications*, Vol. 2, No. 4, Aug. 1995, pp. 6-10.

[16] S. Mohan, "Privacy and Authentication Protocols for PCS". *IEEE Personal Communications*, Oct. 1996, pp. 34-38.

[17] R. Molva et. al., "Authentication of Mobile Users". *IEEE Network*, Oct. 1996, pp. 26-34.

[18] European Telecommunications Standards Institute, *Recommendation GSM 02.09. Security Aspects.*

[19] M. O. Rabin, "Digital Signature", *in Foundation of Secure Communication*, R. A. DeMillo, et. al., (eds). Academic press, 1978, pp. 155-168.

[20] R. C. Merkle, “A Digital Signature Based on Conventional Encryption Function”. *Advances in Cryptology-CRYPTO’87,* Pomerance (ed), Lecture Notes in Computer Sc., Vol. 293, Springer-Verlag, 1988, pp. 369-378.

[21] E. Shimon et. al., “On-line/Off-Line Digital Signature”. *Advances in Cryptology- CRYPTO’89,* G. Goos and J. Hartmanis (Eds), Lecture Notes in Computer Sc., Springer- Verlag, 1990, pp. 263-275.

BIOGRAPHY

Lawan Ahmed Mohammed is currently a PhD student at the Department of Computer and Communication Systems Engineering, University Putra Malaysia (UPM). He obtained his first degree (BSc Ed. Mathematics) in 1995 from Ahmed Bello University Zaria, Nigeria and MSc degree in Operations Research from University Putra Malaysia in 1999. His research interests include smart security, cryptography, and mathematical programming.

Abdul Rahman Ramli is currently the head of Multimedia and Imaging System Research Group at Department of Computer and Communication System, Faculty of Engineering, University Putra Malaysia. He holds a Bachelor’s degree in Electronics from University Kebangsaan Malaysia (UKM), an MSc in Information Technology Systems from the Strathclyde University (UK) and a PhD in Image Processing from the Bradford University (UK). His research interests include image processing and imaging system, instrumentation, PC applications, multimedia systems, microprocessor/embedded system, remote sensing, remote monitoring and control, Internet computing, smart card applications, computer telephony integration, and artificial intelligent applications.

Mohamed Daud is an Associate Professor at the Department of Biological and Agricultural Engineering, Faculty of Engineering, University Putra Malaysia (UPM). He obtained his Bachelor degree in Engineering from U. C. Davis (USA), an M.S. Degree in Agricultural Engineering from Pennsylvania State (USA), an MBA in Finance from UPM and PhD degree in Knowledge Engineering from UPM. He is a Registered Professional Engineer by the Board of Engineer Malaysia, a Fellow Member of Institution of Engineers Malaysia, and a Licensed Company Secretary of Malaysia (LS), by Registrar of Companies Malaysia. His research interests include Expert System, Environmental Impact Assessment, and Irrigation Management.

Veeraraghavan Prakash is a senior lecturer at the Department of Computer and Communication System Engineering University Putra Malaysia (UPM). His research interests include computer and Internet security.