Dr. Jon's Wireless Security

Cellular *Networking Perspectives*

Public Key versus Symmetric Key Cryptography

Modern cryptography schemes can largely be classified as either Symmetric Key (also known as Private Key) cryptography or Public Key cryptography. Both methods are applicable to wireless phone networks and TIA/EIA-41 in particular. As previously reported, the decision between symmetric key and public key cryptography will be central for the selection of an ESA (Enhanced Subscriber Authentication) cryptographic algorithm and process.

Wireless Authentication Today: Symmetric Key Encryption using CAVE

In today's TIA/EIA-41 wireless network, authentication is performed using a symmetric key cryptographic process, the CAVE algorithm. The same cryptographic key, the A-Key, is maintained at each mobile phone and at the authentication center for that subscriber. The A-Key must be securely transmitted to both the MS and the authentication center (AC) to provision a new subscriber. Figure 1 illustrates this process.

Technically, CAVE is a method of hashing, not encryption, as the private key

Figure 1: Symmetric (Private Key) Encryption

Home System

1. Home system sends private key to mobile (requires an additional layer of security – OTA, smart card, secure programming equipment, etc.)

1-800-633-5514

AC

2. Messages can be locked and unlocked by anybody with the private key (including eavesdroppers if the key is compromised)

About Dr. Jon's Wireless Security

Price

The stand-alone subscription price for *Dr. Jon's Wireless Security* is 75% of the cost of the corresponding *Cellular Networking Perspectives* subscription (e.g. $225 for a basic subscription).

Current subscribers to *Cellular Networking Perspectives* can extend their subscription to include *Dr. Jon's Wireless Security* for only a 50% premium over their current *Cellular Networking Perspectives* subscription price. For example, subscribers to our standard 10-copy license paying $300 per year for *Cellular Networking Perspectives* would pay only an additional $150 per year for *Dr. Jon's Wireless Security.*

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

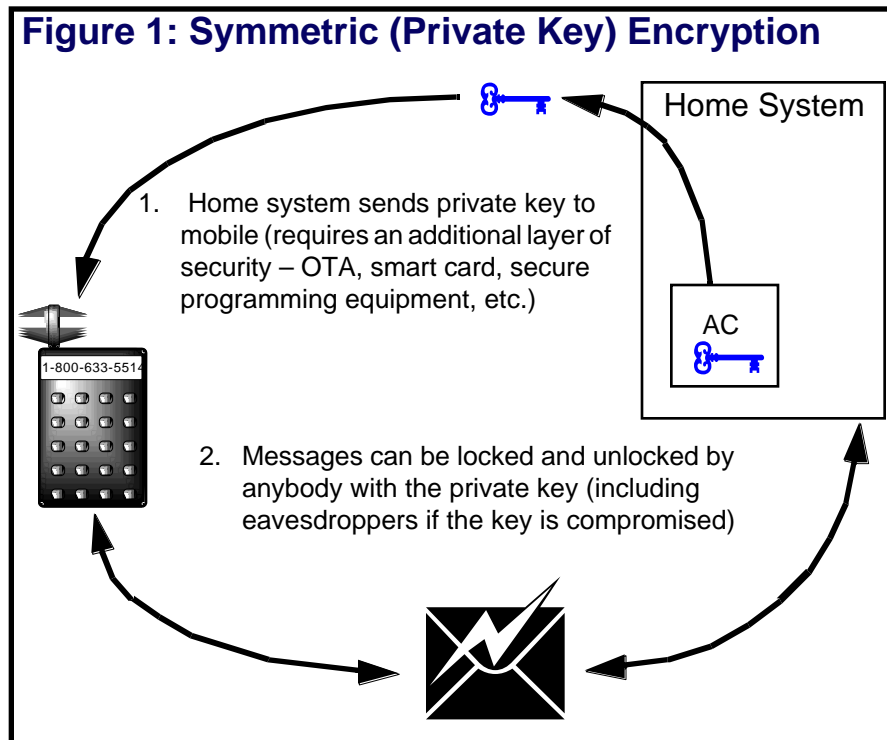cnpaccts@cnp-wireless.com

Next Month's Major Topic

Security of Wireless Cryptographic Procedures.

Next Issue Due…

June 10th, 1999.

Future Topics

Interim CAVE • Global Authentication • UIM • Export Control Laws • Threats to Security Algorithms.

cannot be used to regenerate the plain-text. However, the nature and complexity of this algorithm make it more similar to symmetric encryption than to simple hashing.

Authentication of the mobile station using CAVE is achieved in several steps. The system that performs authentication will be referred to as RAC – the Roamer Authentication Center. This will be the current serving system if the session key (SSD) is shared, or the home AC if it is not shared:

1. The Base Station transmits a random number (rand) to all mobiles within its coverage area.

2. Using the CAVE algorithm the MS computes the following pair: {plain text, cipher text} = {rand, auth}

3. The MS transmits this pair to the RAC over the air (only part of rand is transmitted).

4. The RAC computes its version of auth using the same rand as input to CAVE.

5. The RAC checks the two versions of auth. If they are equal, then authentication is successful. If the two versions of auth are different, then there
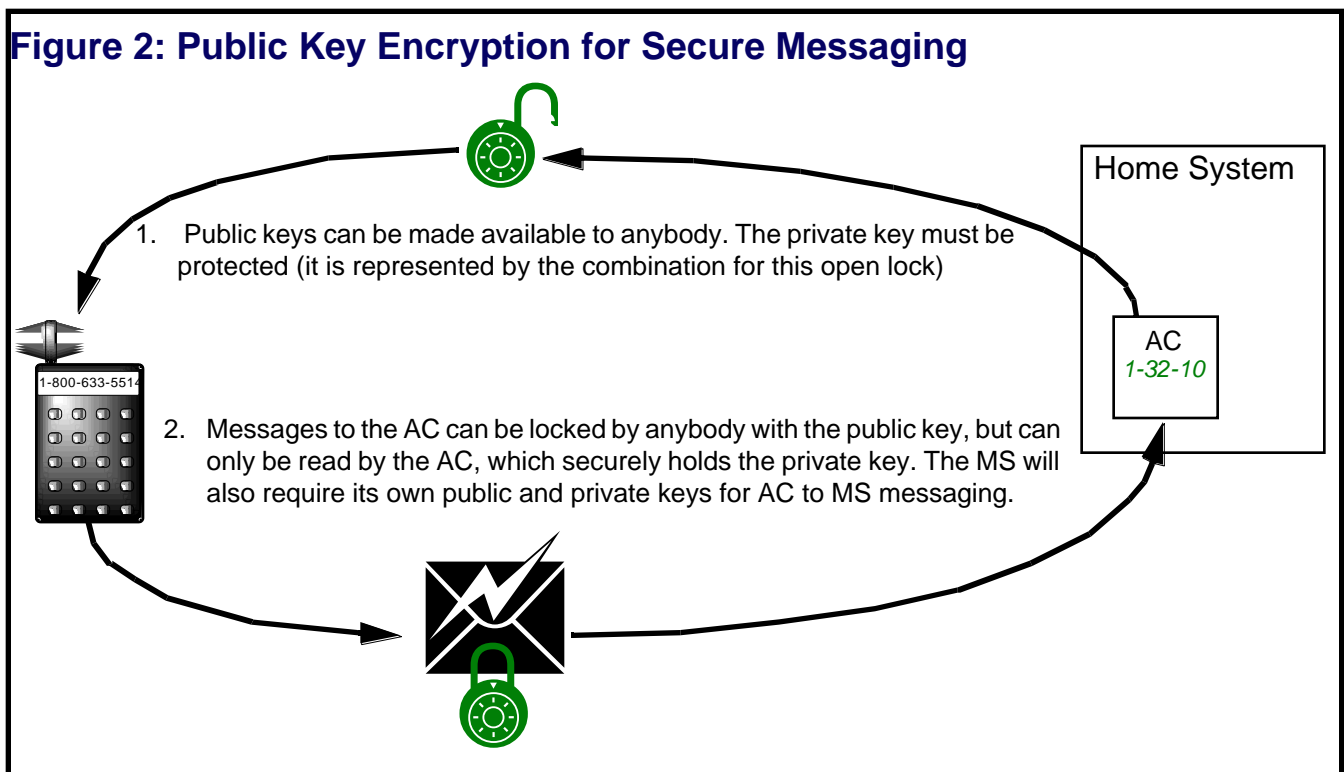
is an authentication failure and the RAC has a variety of local administrative practices to further resolve failures, and to help determine whether it represents a temporary aberration or an invalid mobile attempting to access the system.

The MS does not use the A-Key as an input to the CAVE algorithm for the authentication process, but rather SSD_A, which is a session key derived from the A-Key also using a cryptographic process based on the CAVE algorithm. There are two reasons for using SSD-A. One is to share the processing burden between the AC and the current serving system by sharing SSD, which allows authentication to be performed without intersystem messaging. Secondly, some felt that, because the SSD could periodically be updated, that the security of the A-Key would be strengthened. In a subsequent issue of this report, we will show that this is true only for brute force and other rather unimaginative cryptanalytic attacks against the CAVE algorithm. What is important to note is that the use of SSD and its periodic updating introduces complexity into the authentication process, especially when an authentication failure occurs.

Public Key Cryptography for Wireless Networks.

Figure 2 illustrates the methodology of public key cryptography, where both the sender and the receiver have distinct pairs of cryptographic keys: {public key, private key} — the algorithm is asymmetric. Each public key may be distributed widely and its knowledge by a potential adversary does not affect the strength of the cryptographic process. However, the private key must be held securely because knowledge of it would immediately allow an adversary to decrypt any messages intended for its legitimate owner.

In the TIA/EIA-41 wireless network context, the AC would require both a private key (represented by the closed green combination lock in Figure 2) that must be protected and a public key (represented by the open green combination lock) that can be given to anyone. The MS would have a distinct public and private key. Two way communications therefore requires the use of four different keys (Figure 2 only shows one direction of communication, to simplify the scenario).

Figure 2: Public Key Encryption for Secure Messaging

Home System

1. Public keys can be made available to anybody. The private key must be protected (it is represented by the combination for this open lock)

2. Messages to the AC can be locked by anybody with the public key, but can only be read by the AC, which securely holds the private key. The MS will also require its own public and private keys for AC to MS messaging.

AC
1-32-10

1-800-633-5514

A Lovely Example

Let's see how the public key cryptographic process works. First, Amy and Bob agree upon a cryptographic algorithm — for example RSA. Both Amy and Bob develop (or are provided with) their own distinct pairs of cryptographic keys ({private key$_{bob}$, public key$_{bob}$} and {private key$_{amy}$, public key$_{amy}$}). Then they exchange their public keys. The method of exchange for these public keys can indeed be public because the knowledge of a public key does not benefit an adversary. Now, let us suppose that Amy wants to send Bob a love note which only Bob can read. Amy composes the note (plain text) and then encrypts the note using Bob's public key and the cryptographic algorithm they previously agreed upon. Amy then sends the encrypted note (cipher text) to Bob. Bob eagerly decrypts the message from Amy (cipher text) using the agreed upon cryptographic algorithm and Bob's private key. We note that only Bob can decrypt the note because he is the only person with his private key.

Bob can now compose a winsome reply (plain text) and encrypt it with Amy's public key (cipher text), before securely sending it back to her.

Comparison of Public and Symmetric Key Cryptography

Table 1 summarizes the major issues that are of concern with the choice of an Enhanced Subscriber Authentication (ESA) algorithm.

Table 1: Comparison of Public and Symmetric (Private) Key Cryptography

	Public Key	Symmetric/Private Key
Level of Security Provided	Can be extremely high, assuming an encryption algorithm of adequate strength and proper protection of the private keys.	
Key Provisioning	Minimal security requirements (due to public nature of public keys)	Key exchange must be secure. This security is not provided by the basic private key encryption algorithm.
Key Updates	Simple process with minimal security requirements.	Complex process with high security requirements, including the need for mutual authentication.
Impact on Intersystem Messaging (TIA/EIA-41	For session key exchange, intersystem messaging could be simplified, at the expense of network modifications.	Existing TIA/EIA-41 authentication messaging can be used.
Flexibility for Future Growth	High	Medium
Processor Requirements	Not expected to be a limiting factor with currently available hardware, but will be higher for public key algorithms than for symmetric key.	

International Wireless Security

In April 1999 there was a joint security experts meeting with representatives of North American and Japanese wireless carriers and manufacturers. Significant progress was made in understanding mutual security issues and concerns. It is clear that more meetings of this nature should be held between North American, European and Asian wireless companies to prepare the way for international authentication and secure roaming as the industry moves towards 3G wireless networks.

Dr. Jon's Recommendation

A public key cryptographic algorithm and process should be selected for ESA to enhance flexibility and key management essential to long term growth for TIA/EIA-41 wireless networks.