Dr. Jon's Wireless Security

Cellular Networking Perspectives

Editor: David Crowe

Vol. 1, No. 6 August, 1999

AHAG Update

The meeting to allow proponents of various ESA (Enhanced Subscriber Authentication) proponents to present their proposals to members of the AHAG and others will be held on August 30th, 1999 and not on August 29th, as we reported in the July issue. The location is still Toronto, Ontario, Canada. Contact the chairman of AHAG, Chris Carroll of GTE if you wish to attend:

ccarroll@gte.com

The AHAG is considering the impact of the *Twinkle* and related attacks on wireless systems. This attack is named after the flashing LED's in Professor Adi Shamir's (so far) theoretical encryption machine. Although the attack is directed toward RSA, it would also work on many other cryptographic systems, including some being considered for next generation wireless security algorithms. For more information on this attack, consult:

www.jya.com/twinkle.htm

and

www.rsa.com/rsalabs/html/twinkle.html

Thanks to David Ott of Qualcomm for bringing this information to our attention.

New Writer, New Name

We are pleased to announce that Les Owens has been appointed as the lead writer for Dr. Jon's Wireless Security starting in September. For obvious reasons, we will need a new name for this bulletin, and invite your submissions. The winner will receive a free *Cellular Networking Perspectives* golf shirt plus a 6 month free subscription to *Dr. Jon's Wireless Security* (or whatever it is then called!). If you already have a subscription, we will extend it by 6 months.

Basics of Wireless Authentication

Operating a wireless telecommunications website (www.cnp-wireless.com) gives us the dubious privilege of receiving many questions like "Can a mobile phone be made to operate on any other identity and how? What are the tools needed for it?" Perhaps we are overly cynical, but we assume that these people are looking for instructions to clone cellular phones.

We have asked the mysterious Crypto-Answer-Man to address this issue.

Cloning is the unauthorized use of a legitimate MIN/ESN combination in a wireless phone.It was easy to perpetrate until authentication came along. This vulnerability occurred because, as Figure 1 illustrates, the MIN and ESN of cellular phones are transmitted in the clear on every phone call, whenever a mobile registers and during some other transactions as well. The transmission of the MIN and ESN is needed so that the base station can identify the phone that is requesting a service.

The MIN, assigned by the mobile telephone's carrier, typically can be changed

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

Enhanced Subscriber Authentication (ESA).

Next Issue Due…

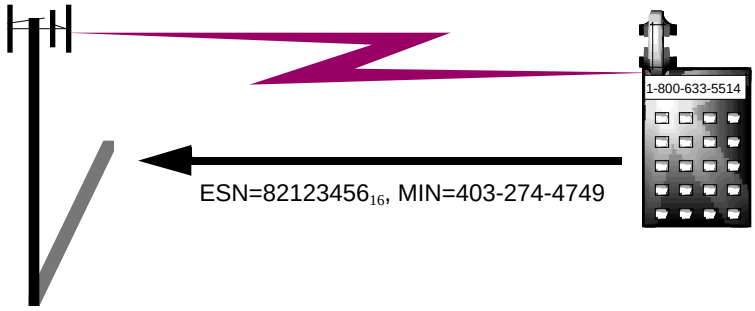
Sept. 15th, 1999.

Future Topics

Voice over Packet security • Public Key & Wireless • GSM Security

Dr. Jon's Wireless Security is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary AB, T2N 3W1, Canada.
Contact Information: Phone: 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http:/www.cnp-wireless.com/djws.html.
Subscriptions: $150 for current *Cellular Networking Perspectives* subscribers for delivery in the USA or Canada, US$200 elsewhere. Non-subscribers pay $225/yr. for delivery in the USA or Canada, US$300/yr. elsewhere. Payment is accepted by cheque, bank transfer, American Express, MasterCard or Visa. **Delivery:** Email or 1st class mail.
Back Issues: Available individually for $20 in the US and Canada and US$25 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

Figure 1: Transmission of the ESN and MIN in the AMPS/TDMA/CDMA Environment



through the user interface of a wireless phone or through its data interface, just as other NAM (Number Assignment Module) parameters can be changed. On the other hand, the ESN, a 32-bit pattern that is 'burned' (i.e. securely stored) in the phone, is not intended to be readily modified, and is intended to permanently identify the mobile hardware rather than the subscription (which is the purpose of the MIN, or its alternate, IMSI). FCC guidelines require that the ESN be stored obscurely ('security through obscurity') in the handset to prevent tampering. Now the ESN is usually stored in a memory device (e.g. EPROM, EEPROM, flash memory) it is possible to subvert the design and change it, or to change the software that reads it from memory before transmitting it. Building a truly tamper-proof device (that can still make calls) is difficult, if not impossible!

Crypto-Answer-Man Notable Note 1

It is illegal in the US and in some other countries to change the ESN of a mobile telephone once it is programmed by the manufacturer.

The cloning fraud problem, caused by interlopers masquerading as legitimate customers for anonymity or financial reasons, began in the US around 1992. The major US operators began to implement the Telecommunications Industry Association's (TIA) cryptographic authentication scheme known as CAVE in the 1995 time frame after they realized that the cloning fraud problem was not going to magically go away. Eventually, they concluded that CAVE authentication was the best fraud-prevention scheme available. The other schemes, such as PIN validation and clone-detection-and-shutdown-systems, were easily defeated or were inadequate. CAVE is a simple 'challenge-response' system that is used to validate the identity of a wireless phone. It does this by verifying cryptographically that the telephone is the one claimed. Although not perfect, the network provides a high level of confidence that the telephone contains a secret that is shared with the network but unknown to others.

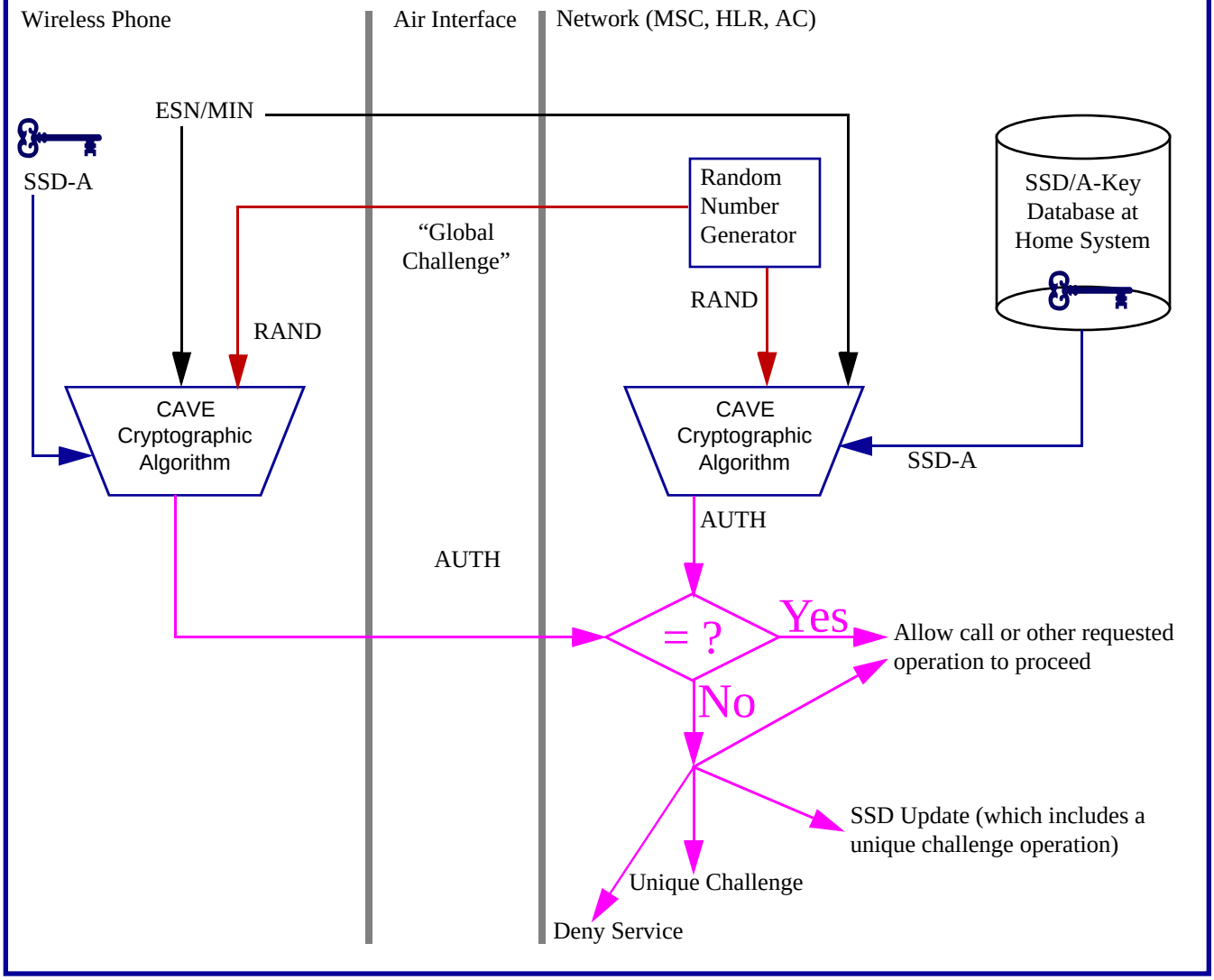
Crypto-Answer-Man Notable Note 2

In 1995, the losses due to cellular telephone fraud problem amounted to over $600 Million in the US according to the CTIA. Because of authentication, those losses have been reduced dramatically.

The basic steps of the authentication process for the North American cellular system is illustrated in Figure 2 and described below:

1. The telephone identifies itself to the network with the ESN and the MIN upon power-up and during other call processing activities.
2. The network transmits a 32-bit random number to the telephone (RAND). This transmission, like all other communications with the network, is performed over the wireless network or radio path.
3. The telephone performs a cryptographic operation on the ESN, MIN and random number and returns an 18-bit authentication response to the network (AUTH). The computation is done using the CAVE (Cellular Authentication and Voice Encryption) algorithm with the SSD-A cryptographic key as secret input. SSD-A (Share Secret Data - A) is a 64-bit value that is in turn derived from the 64-bit A-key (authentication key) also using CAVE. Both the SSD-A (and its counterpart the SSD-B) and the A-key are stored in the telephone and are never transmitted over the radiopath, although they may be derived indirectly using radio communications.
4. The network performs the same computation using the CAVE algorithm and the shared information: the secret SSD-A assigned to that mobile telephone.
5. If the authentication response, AUTH, from the mobile telephone equals that produced by the network, the mobile telephone is provided service. Otherwise, the operator has the choice of providing service anyway, denying service or performing further authentication operations. The most likely is a Unique Challenge operation. Because this is based on a unique random number (and not a globally broadcast one) it is more secure. Alternatively, an attempt can be made to update the SSD key if it is believed that the mobile no longer has a valid key.

Figure 2: Simplified View of TIA *Challenge-Response* Authentication



Crypto-Answer-Man Notable Note 3

Not all operators in the US (and certainly not those in other countries) have implemented this strong security tool for fraud prevention. Because of the high integrity of the Crypto-Answer Man and his desire not to perpetuate the fraud problem, he will not divulge specific means to modify ESN's nor means by which authentication can be defeated. ;-)

Further Reading

To learn more about fraud control and authentication, obtain the TIA air-interface and interoperability standards (e.g. TIA/EIA-41-D, IS-54B, IS-91A, TIA/EIA-95-B, TIA/EIA-136-B, IS-2000), or search for the following United States patents. Note that some information is export-controlled and is only available after signing an agreement with the TIA:

1. Patent # 5,668,875, Brown, et al.; September 16, 1997
2. Patent # 5,551,073, Sammarco; August 27, 1996
3. Patent # 5,282,250, Dent, et al.; January 25, 1994
4. Patent # 5,241,598, Raith; August 31, 1993
5. Patent # 5,237,612, Raith; August 17, 1993
6. Patent # 5,204,902, Reeds, III, et al.; April 20, 1993
7. Patent # 5,172,414, Reeds, III, et al.; December 15, 1992
8. Patent # 5,159,634, Reeds, III; October 27, 1992
9. Patent # 5,153,919, Reeds, III, et al.; October 6, 1992
10. Patent # 5,060,265, Finkelstein; October 22, 1991

Alternatively, you may hire a friendly consultant through *Cellular Networking Perspectives Ltd.* ;-)