AUTHENTICATION

By David Crowe

The Secrets of Authentication

Authentication could be today's newest secret to choking out cloning.

Authentication, as defined for AMPS cellular and digital standards, works using secret keys, encryption algorithms and the concept of "challenges." The secret key should only be known by the mobile and the authentication center and can be used with other data, such as the mobile identification number (MIN) and electronic serial number (ESN) of the mobile and a randomly selected number, to initiate the Telecommunications Industry Association (TIA) cellular authentication and voice encryption (CAVE) algorithm.

SECRET KEYS

When a cellular or PCS system initiates a challenge, it selects a random number and sends it to all mobiles within a cell (for a global challenge) or to a single mobile (for a unique challenge). The mobile then has the information it needs to execute the CAVE algorithm and produce the same response the system already has calculated.

A wannabe cloned handset without the secret key will be unable to produce the correct response to the challenge and will be denied service. This system is infinitely more secure than MIN/ESN or personal identification number (PIN) validation because the secret key is never transmitted over the radio interface.

To make the CAVE algorithm even more secure in situations where a secret key is compromised, two secret keys are used. One, known as the A Key, is known only by the mobile and the authentication center. The second one, known as shared secret data (SSD), is generated by the authentication center and the handset. This second key can be transmitted safely around the IS-41 intersystem operations network and can be changed at any time.

If a potential cloner has the A Key and not the SSD, it will not be able to respond to challenges. Having the SSD and not the A Key will allow calls only until the SSD is regenerated. Even if a cloner has both keys, an automatic SSD update (with manual verification) can eliminate them or, in the most severe cases, a new A Key can be programmed into the phone.

TIME TO MARKET

When authentication was first developed, it was for the IS-54 dual-mode analog/TDMA digital cellular standard. At the time of this standard's development (1989-1992), it was believed that digital could spell the end of analog. However, because of confusion over two competing digital technologies (TDMA and CDMA), concerns over voice quality and lack of a compelling reason for consumers to demand digital, this has not proved to be the case. It was not until 1994 that the first analog standard supported authentication. Another year passed before significant numbers of new analog phones were manufactured with authentication.

Another delaying factor has been the requirement for IS-41 interconnection to make authentication work. Authenticating a roaming carrier requires the ability to perform IS-41 transactions with the authentication center in the home system. This requires the implementation of TSB-51, an addendum to IS-41 Rev. B. Some carriers that are already using IS-41 Rev. A and do not see much added value in Rev. B held out for Rev. C. Unfortunately, IS-41 Rev. C was delayed significantly, not being published in 1995.

However, now most infrastructure vendors are offering an authentication solution, based on either TSB-51 or a subset of IS-41 Rev. C.

Apart from the real difficulties of implementing a new technology, there have been several mental blocks regarding authentication. Some proponents have decried authentication, claiming it can't work because nothing else has yet proved to be the silver bullet. However, authentication is something different and is dramatically more secure than any other available technology.

CONVERTING THE INNOCENT

Another concern has been that there are so many non-authenticating handsets in the field that there is just no point in implementing authentication to protect a small fraction of the subscriber population. Cloners, after all, would just continue to attack the majority of non-authenticating handsets.

This argument was first advanced when there were about 5 million mobiles in the United States. If authentication had been rushed into service then, about 90% of handsets would now be authenticating. Even if the changeover to manufacturing all handsets with authentication capabilities starts this year (as recommended by CTIA), our back-of-the-envelope calculation (using conservative assumptions) shows that it would take only two years for the number of authenticating handsets to equal the number that are non-authenticating, and six years before the 90% authenticating level would be achieved.

Carriers can speed up authentication implementation by targeting their high usage customers, focusing on protecting minutes of airtime and not on the number of subscribers. Carriers should offer incentives to their customers to switch to an authenticating phone; the cost of the program could be subsidized by reductions in cloning losses.

Even the PIN is being used as a tool to encourage the purchase of authentication-capable phones. Carriers are promising customers that they no longer will be required to use their PINs if they obtain an authenticating phone. Implementing authentication for a fraction of subscribers will force cloners to attack a diminishing number of handsets, making their actions more easily detected by other anti-fraud technologies, such as profiling.

At that point, the secret to authentication reaches beyond the secret keys into another secret — the one that will force cloners into another line of business.