Mutual Biometric Authentication

Mostafa El-Said
Grand Valley State University, USA

INTRODUCTION

Cell phone fraud accounts for more than a billion dollars in lost revenue in North America (Rose, 1999; Wingert & Naidu, 2002). Therefore, one of the largest problems in cellular communication systems is the security of cellular phones and the authenticity of cell phone base stations. Caller authentication and voice encryption (CAVE) is the currently used algorithm in cellular systems for authentication and data integrity (Cryptome, 1997; Korzeniowski, 2005; Cellular Technologies, 2006). It was developed by Committee TR45.3 of TIA/EIA under the auspices of the NSA. Gauravaram and Millan (2004) presented two crypto methods to exploit the security vulnerabilities in the CAVE algorithm, and proposed two attack methods that demonstrated that the CAVE is insecure. Another attempt to crack the CAVE is conducted by a research team at the University of California at Berkeley. David Wagner, a member of this research team, announced the CAVE algorithm can be cracked in a matter of minutes or at most hours (Monitoring Times, 1997).

Other attacks on the cellular systems can take place through the RF interface or through the interconnecting wireline networks, including the radio network controller switch and the PSTN network. The RF interface attack is the most severe attack on the cellular systems. Several well-known RF attacks are recognized by the cell phone industry including:

- **Cell Phone Cloning:** The cell phone cloning problem is created because illegal users can capture a cell phone's pair of uniquely assigned numbers—ESN (Electronic Serial Number) and MIN (Mobile Identification Number)—when sending the information to the tower. Then, those illegal users can bill time to a user's account. The cell phone industry solved this problem by encrypting the cell phone number and the pair of ESN and MIN when sending the information to the tower (Hai-Ping Ko, 1996; Landmark Communications, 1996).
- **SMS Messages Flood Attack:** The SMS messages flood attack was a direct result of the shortcoming of 3G cell phone design where the same control channel is used for both call setup and sending SMS messages. An attacker can exploit this vulnerability and use free SMS Web sites to send a large number of anonymous text messages to a cellular phone tower. This could eventually jam up the cellular tower, block any new telephone calls from going through, and result in a denial of service (DoS) attack on the cellular system. The SMS message attack problem was discovered by accident, and some of the European networks have already been jammed when the volume of SMS messaging reached an unexpectedly high level. This problem is still under research (McMillan, 2005).
- **Hash Function Attack:** Gauravaram, McCullagh, and Dawson (2006) investigated several legal and practical implications of attacks against various 128-bit hash functions, and in particular MD5 due to its wide usage. They claim that MD5 can be a single point of failure in various applications. Also, they suggested that new hashing algorithms should be developed in order to avoid new attacks in the future (Gauravaram, Millan, & May, 2004).

This article addresses another severe threat affecting the security of cellular systems, called *pilot aliasing attack.* This problem occurred due to pilot code reuse among different cellular carriers.

In the forward link direction, the base station transmits a dense pack of codes which assists the mobile terminal in performing vital operations such as system synchronization, system acquisition, cell search, and monitoring strong pilots in its serving zone. In general, the CDMA cellular systems have a total of $(2^{18} - 1)$ scrambling codes available in the downlink path. These codes are arranged into blocks of 512 coding sets, which are sufficient for a cellular carrier to start deploying a new service. Each cellular tower is allocated one and only one scrambling code, which serves as a unique identifier for the tower and used for cell separation.

These code sets can be reused over and over again within the same carrier's network, and in different carrier networks provided that they will interfere with each other as little as possible (Calhoun, 2003). All 512 cells have the same pilot waveform (same code). They can be differentiated from one another by their pilot signal phase offset. The pilot phase offset is always assigned to the base stations in a multiple of $(2^6=64$ chips), such as that shown in Figure 1.

Due to the carriers' interoperability nature of the cellular networks, the cell phone may receive two identical pilot signal phase offsets (PN offsets) from two distinct carrier networks at any moment in time. This phenomenon is even worse in the presence of non-homogeneous geography and high-dynamic RF multi-path environments. The mobile

Figure 1. Base stations pilot code phase offset

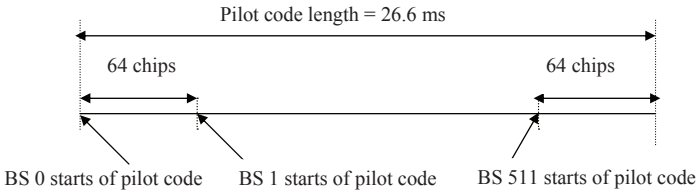
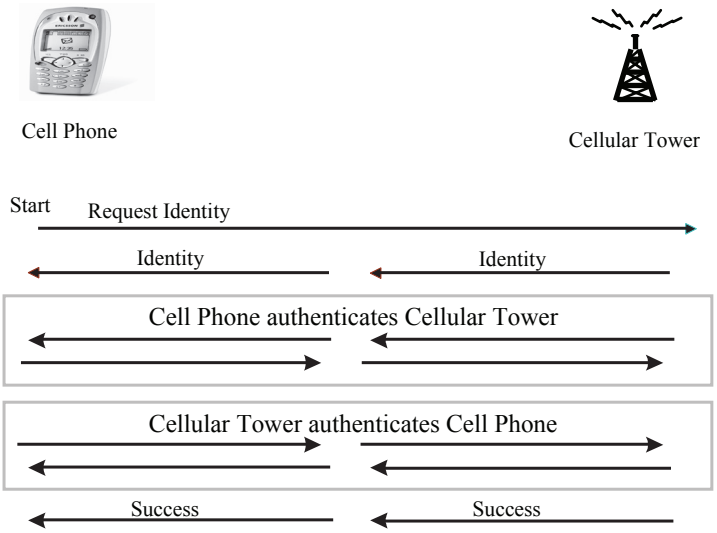


Figure 2. MBA interaction algorithm



receiver became confused and cannot distinguish between the two pilots. One of the pilot signals may be sent from a fake malicious tower that hunts for cell users, which results in *pilot aliasing attack.*

In this article, I use a mutual biometric authentication (MBA-) based solution to allow the cell phone device to authenticate the cellular phone tower before using it as a serving base station. This solution allows the cell phone to detect the existence of pilot aliasing attack. The proposed solution stems from authenticating the cellular tower based on a combined key that consists of the TowerID and the CarrierID's fingerprint. This is a significant step towards creating a robust mutual biometric authentication technique in the cellular system.

PROPOSED SOLUTION

The proposed MBA solution relies on having the tower and the cell phone devices passing each one's credentials before engaging in a communication scenario, such as that described in Figure 2.

The following section describes the proposed MBA interaction algorithm.

MBA Algorithm Assumptions

- The cell phone's Electronic Serial Numb: ESN
- The cell phone's Mobile Identification Number: MIN
- The cell phone's public Number: PPN
- The cellular tower has an ID: TowerID
- The cellular tower Broadcast its PilotID: PilotID
- The CarrierID is kept at the tower and at the cell phone station and acts as a shared secret key between the cell phone and the carrier tower. (See Diagram 1.)

PERFORMANCE MEASUREMENTS AND KEY FINDINGS

To test the applicability of the proposed MBA solution, I use and compare the two hashing algorithms, called MDS and SHA1. To do that, the simulation experiments are carried out 10,000 times. I computed the time that the cell phone