Security of USMobile (www.USMobile.me) Scrambl3

Professor Dr. Yuliang Zheng

To address security issues in pervasive mobile communications, NSA's Information Assurance Directorate (IAD) initiated the Mobility Program (also known as the "Fishbowl Project") in December 2012. This program uses well-established, standard cryptographic primitives to protect US Government classified mobile communications up to the "Top Secret" level. Fishbowl is designed to protect communications by double-encryption. Its architecture can be summarized as follows:

- Each user's mobile device is required to establish a VPN connection to a corporate gateway prior to the start of a communication. No communication outside of the VPN tunnel is allowed.
- Users then communicate among themselves using a second encryption tunnel that is embedded inside the VPN tunnel.

As an example, when two users Alice and Bob wish to make a secure phone call, they establish a VPN tunnel to their corporate network first. Afterwards Alice and Bob create a point to point encrypted tunnel for their phone call inside the VPN tunnel. These two nested, encrypted tunnels implement one of the most fundamental security principles: defense in depth.

The National Institute of Standards and Technology (NIST) has developed comprehensive cryptographic standards to protect US Federal Agencies' classified information. Based on standards developed by NIST, NSA IAD published Suite B Cryptography standards which can be used to protect Federal Agencies SECRET and TOP SECRET information. The Suite B Cryptography standards recommend AES-128 and ECDH/ECDSA/SHA for the protection of Federal SECRET information, and AES-256 and ECDH/ECDSA/SHA for TOP SECRET information. The recommendation is summarized in the following table.

SECRET	**TOP SECRET**
AES-128, Curve P-256 based ECDH/ECDSA, and SHA-256	AES-256, Curve P-384 based ECDH/ECDSA, and SHA-384

USMobile's Scrambl3 communication system employs AES-256 and Curve P-384 based elliptic curve Suite B cryptographic techniques. Cryptographic techniques with these security parameters are intended for the protection of information that is required be secure within the next 50 years.

Compared to existing secure VoIP techniques, Scrambl3 has the following unique characteristics.

1. Double layer encryption. No existing VoIP system is known to employ this principle to achieve the goal of defense in depth. In a typical SDP based

SRTP VoIP deployment, end users exchange key information in a signaling protocol (with or without TLS protection) and actual phone calls are then encrypted in a parallel channel. Likewise, ZRTP based VoIP systems offer one layer of encryption only.

2. Cryptographic techniques employed in Scrambl3 afford a security level of 192-bits. This is more favorable than most existing VoIP deployments that use outdated security techniques such as Triple DES to protect communication contents. Though T-DES has 112 bits in a key, its effective security level is 80 bits only under chosen-plaintext or known-plaintext attacks (for details see NIST SP800-57). Back in 2005 NIST recommended that the 80-bit security level should not be used beyond 2010.
3. Scrambl3 employs PKI based key management that is generally more robust than key management techniques used by existing secure VoIP deployments.
4. Scrambl3 is based on widely deployed, mature technologies such as VPN and TLS. In comparison, ZRTP based VoIP systems rely on out-of-band human voice based authentication to counter man-in-the-middle attacks, which requires further examinations with regard to its security.

USMobile’s Scrambl3 has implemented the most salient security features of NSA’s “Fishbowl Project” secure VOIP architecture. It does deviate from NSA’s “Fishbowl project” in one aspect, namely security policies for the management of mobile devices. The original “Fishbowl project” requires the use of custom-built mobile devices that are configured by a central device management server. To add flexibility to a deployment, Scrambl3 leaves device management to a third party Mobile Device Management (MDM) application which is offered by such vendors as IBM (MaaS360) and others.

Brief Biography of Yuliang Zheng.
Dr. Yuliang Zheng is Chair of the Department of Computer and Information Sciences at the University of Alabama at Birmingham. He is best known for inventing the Signcryption cryptographic primitive that combines digital signature and encryption operations into one single step. Signcryption has been standardized by ISO and IEEE for industry use. He also invented the HAVAL hash function, SPEED cipher, and STRANDOM pseudo-random number generator.