Comparison of Airlink Encryptions

With the growing use of wireless data, the need to provide secure communications is paramount. The key to a secure network is to provide an end-to-end security solution. Having only portions of a communications link encrypted, compromises the overall security. For example, the wireline side of the link can easily be breached or data packets can be intercepted on the Internet. Widely tested and accepted security protocols like VPN, IPSec, PPTP and SSL can be used for a complete end-to-end security solution. Most data users today employ these protocols to protect proprietary or financial information. However airlink security is available, if the operator desires to use it.

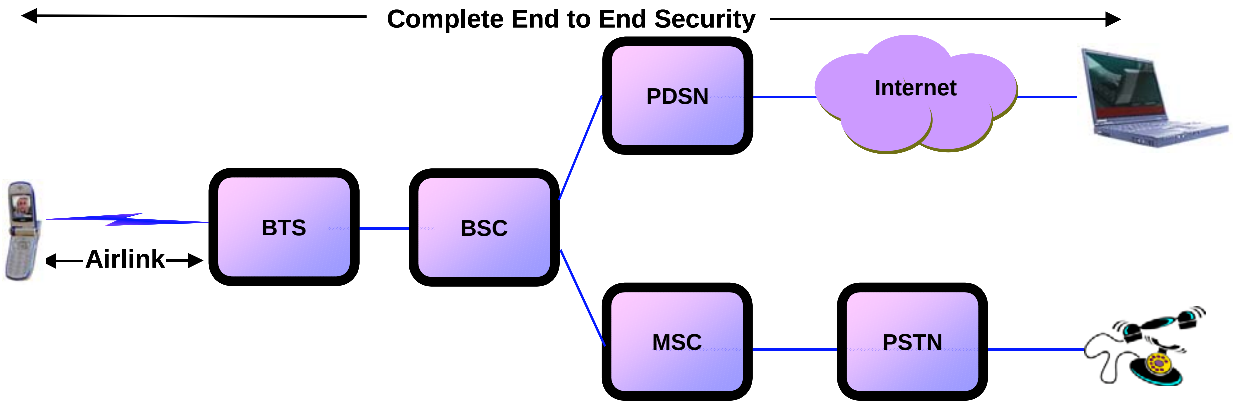

Figure 1 Complete End-to-End Security in Cellular Communications

Security and privacy in cellular communications systems are composed of three main components: authentication, message integrity and encryption. Authentication verifies that the device and network are who they say they are. Message integrity ensures that the signaling information has not been modified in transit between the sender and the receiver. This is usually accomplished with a Message Authentication Code (similar to a hash function with a secret key). Encryption ensures the privacy of the signaling or data transmitted. The focus of this paper will be the comparison of airlink encryptions on various widely used technologies.

Main Security Components

Two main components should be considered when evaluating the security level of an airlink encryption method. The first is the algorithm itself and the second is the length of the key used by the algorithm to encrypt the signaling and data. In order for an unauthorized person to get access to the encrypted data or signaling messages, the algorithm has to be broken or the secret key determined.

An encryption algorithm takes as input unencrypted data and a key to generate encrypted data. Only authorized people who have the key can decrypt the data and view it. A variety of encryption algorithms exist and new ones are continuously being developed. One way to prevent the algorithm from being broken is to keep it secret and only to allow legitimate manufacturers to know how to implement it. However, this has proven to be a very difficult task and most algorithms have been reverse engineered and openly published. A better way is to openly publish the algorithm and depend on the secrecy of the key used for encryption to protect the data. Openly publishing the algorithm also has a secondary benefit of having the cryptologic community widely testing it. If an algorithm can pass such scrutiny, there is greater confidence in its security.

The second component to security is the length of the key used to encrypt the data. As a simple example a key that is only two bits long can be easily broken as there are only 4 possible key values. However, a key that is 32 bits long has 2^32 (more than 4.2 billion) possible values. The time needed to search through all possible key values increases, as the key length gets longer. A longer key length is thus more secure. In order for this to be true, the key being used should be truly random. If there is any similarity or pattern in the bits in the key that can be exploited, the effectiveness of the key will be reduced. For example, creating a 64-bit key by concatenating a 32-bit key with itself does not make a true 64-bit key. It only generates an effective 32-bit key in terms of key strength. Additionally, vulnerabilities in the algorithm can also be exploited to reduce the effective key length. Even though data might be encrypted with a truly random 64-bit key, vulnerabilities in the algorithm might be exploited to make this seem like a 40-bit key.

CDMA 2000 1X

CDMA 2000 1X has security and encryption described as part of layer 3 in the IS-2000 standard. In 1X Revision 0, Enhanced Cellular Message Encryption Algorithm (ECMEA) can be used with a 64-bit CMEA key to encrypt signaling messages. ORYX (a linear feedback shift register stream cipher) can be used with a 32-bit data key to encrypt data traffic. Both ECMEA and ORYX are published algorithms, although subject to export control. The security protocols for 1X rely on the 64-bit authentication key (A Key) and the Electronic Serial Number (ESN) of the user device. These are both provisioned into the device at the factory or point of sale. The 64-bit CMEA key and the 32-bit data key are derived from these using the Cellular Authentication and Voice Encryption (CAVE) algorithm.

From 1X Revision A onwards, AES (also known as Rijndael) encryption algorithm can be used to encrypt individual channels or all channels (access and traffic channels). The AES algorithm has been widely published and tested and proven to be a very secure algorithm. Though the AES algorithm in 1X Revision A uses a 128-bit key, this key is derived from duplication of the 64-bit CMEA key used in 1X Revision 0. Thus the true effective key length is 64 bits.

From 1X Revision C onwards, a true 128-bit key generated by AKA protocol can be used. This provides one of the highest levels of security in airlink encryptions. Again, individual channels or all channels can be encrypted.

CDMA 2000 1xEV-DO

1xEV-DO, standardized as IS-856, has the capability to add encryption to the airlink. This encryption capability is defined in the IS-925 standard. IS-925 encryption uses the AES encryption algorithm. It uses a true 128-bit key that is derived from a Diffie-Hellman key exchange algorithm during authentication between the device and the base station that generates either a 768-bit key or a 1024-bit shared secret, which is hashed to create the 128-bit key. A hash function takes a variable length input and generates a fixed length output. Knowing the output does not compromise the input values. IS-925 allows individual channels or all channels to be encrypted. The true 128-bit key provides a very high level of security.

GSM / GPRS

In GSM/GPRS networks, the security in the user device is maintained in the SIM card and the device itself. The SIM card contains the 128-bit authentication key, similar to the 64-bit A-key in CDMA systems. The SIM card also has the A8 algorithm which is used to generate the 64-bit cipher key that is used by the device to encrypt data and signaling over the air.

Original GSM/GPRS supports 3 levels of security for airlink encryption: unencrypted, A5/2 and A5/1 in increasing security order. The A5 encryption algorithm resides on the device and was kept secret and not openly published. However, it was reverse engineered and leaked on the Internet some years ago. The A5 algorithm uses the 64-bit cipher key derived from the 128-bit authentication key by the A8 algorithm in the SIM card to perform the encryption. However, most implementations have artificially weakened the key to 54-bits by zeroing out the top 10 bits. Using a brute force attack on A5/1 reduces the key to an equivalent 40-bit key, and even more powerful attacks have been published. A5/2 was designed to be weaker for export reasons and can be broken in less than a second using a standard PC.

In response to the weak nature of the encryption algorithms and the short effective key lengths, A5/3 encryption algorithm was introduced in 2002 and it is expected to be stronger. It is based on the widely published Kasumi algorithm. Though A5/3 uses a 128-bit key, this key is derived from duplicating the 64-bit cipher key described before. Thus the effective key length is still only 64-bits. There are currently no deployed versions of A5/3.

One fundamental issue with the A5 series of algorithms is that they all use the same 64-bit cipher key. Most devices support all versions of the A5 algorithm to ensure backward compatibility and roaming across legacy networks. However, this flexibility can be exploited to circumvent the higher level of security provided by A5/3. A device can be forced into thinking that the network only supports the weak A5/2. Any messages sent can then be easily broken to get the 64-bit cipher key. As this is the same key used by A5/1 and A5/3, the security is thus also compromised for those algorithms as well. The key can be easily broken with A5/2 and thus security is also broken for both A5/1 and A5/3.

WCDMA

WCDMA systems use an encryption algorithm based on the widely published Kasumi algorithm. It is a 64-bit block cipher using a true 128-bit key. A true 128-bit key Kasumi implementation is not exactly equivalent to 128-bit AES implementation: even though the key strength is the same, a 64-bit block cipher would theoretically be vulnerable to a 2^{64} lookup-table attack, while AES would require a table of size 2^{128}.

Conclusion

Table 1 below summarizes the comparison of the different airlink encryption mechanisms.

	CDMA 2000 1X Rev 0	CDMA 2000 1X Rev A	CDMA 2000 1X Rev C, D	CDMA 2000 1xEV-DO	GSM A5/1 and A5/2	GSM A5/3	WCDMA
Encryption Algorithm	ECMEA,ORYX	AES	AES	AES	A5	Based on Kasumi	Based on Kasumi
Algorithm public? (Better tested)	Yes, Yes	Yes	Yes	Yes	No	Yes	Yes
Key Length / Effective key length	64,32 / 64,32	128 / 64	128 / 128	128 / 128	64 / 54	128 / 64	128 / 128

Table 1 Airlink Encryption Comparison[1]

Airlink security is best implemented with algorithms that are published and can be tested widely by the cryptologic community. The strength of the keys used in these algorithms is also of paramount importance. The AES algorithm is published and well tested. It relies on the security of the key rather than keeping the algorithm secret. A5 algorithm was a secret but it was reverse engineered and there are a number of attacks. The effective key length or strength of the key for A5 is much less than AES implementations. User data is best secured with a well tested end-to-end solution like VPN regardless of the airlink encryption. However airlink encryption might be desired for marketing reasons or to protect airlink usage.

[1] Note that the effective key lengths for ORYX and A5/2 are even shorter than the best case shown in the table. A5/3 has not been implemented to determine the true effective key length.

Glossary

1xEV-DO – CDMA2000 1x Evolution Data Optimized

AES – Advanced Encryption Standard, also known as Rijndael

AKA – Authentication and Key Agreement

BTS – Base Transceiver Subsystem

BSC – Base Station Controller

CAVE – Cellular Authentication and Voice Encryption

CDMA – Code Division Multiple Access

CMEA – Cellular Message Encryption Algorithm

ECMEA – Enhanced CMEA

ESN – Electronic Serial Number

GSM – Global System for Mobile communications

GPRS – General Packet Radio Service

IPsec – IP Security Protocol

L2TP – Layer 2 Tunneling Protocol

LFSR – Linear Feedback Shift Register

MSC – Mobile Switching Center

ORYX – LFSR Stream cipher

PDSN – Packet Data Serving Node

PSTN – Public Switched Telephone Network

SIM – Subscriber Identity Module

SSL – Secure Sockets Layer

VPN – Virtual Private Network

WCDMA – Wideband Code Division Multiple Access