

Tallinn, Estonia, 7-9 September 2010

Title: LI of MIKEY-IBAKE, a UK perspective

Document for: Discussion

Date:

Source:

Background

Various schemes have been discussed for inclusion in IMS Media Plane Security; MIKEY-IBAKE is currently being considered. There is some concern about the Lawful Interception solution proposed for this scheme, which may prevent its deployment in some jurisdictions.

Recent events have highlighted the difficulties that can arise when appropriate LI mechanisms are not engineered into systems at an early stage.

MIKEY-IBAKE and LI Requirements

To perform Lawful Interception on MIKEY-IBAKE communications, a LEMF would be required to perform a Man-in-the-Middle attack during session establishment (or re-key), and continue to decrypt and re-encrypt communications for the duration of the session. This appears to prohibit several of the requirements agreed in Section 5.7 of 3GPP TS 33.106. The requirements are considered in turn here.

1. When an encryption service is provided by the PLMN, lawful interception shall take place as for a non encrypted communications.
 - a. In addition encrypted communications shall be decrypted, or the decryption keys and any required associated information (e.g. roll over counters) shall be provided to the LEMF.
 - b. For the specific case where a key server based solution is used, it is a national option for the operator to make keys and any associated information (e.g. roll over counters) directly available to the LEMF for the decryption of communications.

It appears that MIKEY-IBAKE satisfies this requirement.

2. Interception shall be performed in such a manner as to avoid detectability by the Target or others. In particular:
 - a. There shall be no significant difference in latency during call setup or during communications compared to a non intercepted communications.

Due to the timing and interaction required to perform the Man-in-the-Middle attack during call setup, there will be additional latency in call setup. This will be especially pronounced when large numbers of Surveillance Subjects are active in one region or one switch. Computationally intensive elliptic curve calculations will need to be performed for every call setup under surveillance, so a slot to perform these

calculations is required before the call can commence. It appears that MIKEY-IBAKE does not satisfy this requirement.

- b. Interception of a Target shall not prevent the use of key exchange applications which provide a user key confirmation mechanism.

NOTE: Key confirmation mechanisms such as an authentication string to be exchanged verbally are commonly used to provide additional assurance of authentication.

The Man-in-the-Middle attack required for LI in MIKEY-IBAKE results in different keys being derived by each MS/UE when surveillance is taking place. This prohibits the use of such key confirmation mechanisms which some users may expect, and may be included in implementations of the standard. It appears that MIKEY-IBAKE does not satisfy this requirement.

- c. Should interception fail during a call (or during call setup), the call shall be unaffected.

Should a MIKEY-IBAKE LI implementation fail, all calls subject to interception will immediately fail. This is because the LI implementation needs to decrypt and re-encrypt (with a different key) all data it intercepts. Such an event may raise awareness of a Surveillance Subject to interception. It should be noted that multiple Surveillance Subjects' calls would be simultaneously terminated (and other users in the same location would not); this may indicate which users are under surveillance. It appears that MIKEY-IBAKE does not satisfy this requirement.

3. Where the PLMN operator provides decryption of the communication, it is the operator's choice where in the network this decryption is performed. However, following decryption, all IRI and CC shall be provided to the LEMF using handover mechanisms as per a non encrypted communication.

Operators have little choice in the positioning of the decryption function when performing LI on MIKEY-IBAKE. The communications must be decrypted and re-encrypted en-route, in the core network, as the communicating parties of a MIKEY-IBAKE call under surveillance have different keys. Note that this approach also causes difficulties in performing LI when Local Routing is employed. It appears that MIKEY-IBAKE does not satisfy this requirement.

4. An encryption solution shall not prohibit commencement of Interception and decryption of an existing communication.

By allowing for session rekeys, it may be possible for MIKEY-IBAKE to satisfy this requirement. However, if rekeying of sessions is not commonly configured by users, the use of a session rekey to facilitate Lawful Interception will be detectable by Surveillance Subjects. It is unclear whether MIKEY-IBAKE can satisfy this requirement.

5. If key material and any associated information are available, it shall be possible to retrospectively decrypt encrypted communications.

A Man-in-the-Middle attack is an *active* attack, which must be performed at the time of call setup. Therefore in MIKEY-IBAKE, if this attack has not been performed, any surveillance is impossible, whether during or after the call. In order to retrospectively

decrypt communications the Man-in-the-Middle attack must have been performed on all subscribers. It appears that MIKEY-IBAKE does not satisfy this requirement.

It is possible to employ Identity Based Encryption whilst allowing for the possibility of Lawful Interception. In light of these requirements, UK government has developed a similar scheme, MIKEY-SAKKE, which supports 3GPP SA3 LI requirements and has additional benefits such as low latency. Full details of this scheme can be found in the MIKEY-SAKKE Internet Draft.

An additional concern in the UK is that performing an active attack, such as the Man-in-the-Middle attack proposed in the Lawful Interception solution for MIKEY-IBAKE may be illegal. The UK Computer Misuse Act 1990 provides legislative protection against unauthorised access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material. A Man-in-the-Middle attack causes modification to computer data and will impact the reliability of the data. As a result, it is likely that LEMFs and PLMNs would be unable to perform LI on MIKEY-IBAKE within the current legal constraints. Furthermore, the fact that communications are modified en-route by an active attack would render any intercepted data unacceptable for evidential use.

For these reasons there must be significant doubt regarding deployment of MIKEY-IBAKE in the UK or in other countries with similar legal frameworks or where evidential LI is required.

References

These requirements relate to IMS Media Security and to Lawful Interception.

3GPP TS 33.106: "Lawful interception requirements"

3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security"

3GPP TR 33.828: "IP Multimedia Subsystem (IMS) media plane security"

Specification for MIKEY-SAKKE:

IETF Internet Draft draft-groves-mikey-sakke-00, MIKEY-SAKKE: Sakai-Kasahara Key Exchange in Multimedia Internet KEYing (work in progress)

Recommendation

SA3-LI members are requested to discuss the concerns herein regarding Lawful Interception of MIKEY-IBAKE.