3GPP TSG SA WG3 Security — S3#14 **S3-000436**

1-4 August, 2000.

Oslo.

Source: ~~Motorola~~BT

Title: **Notes on security related issues from MExE Meeting 27th-29th June 2000**

~~**A method to retain the IPsec full security services in the three layer network domain security architecture**~~

Document for: **Discussion**

Agenda Item: **tbd**

The following Notes on security related issues from the MExE meeting 27th-29th June 2000. A formal report is available on the 3GPP MExE Server.

CLDC Presentation

SUN Microsystems gave a presentation on Connected Limited Device Configuration (CLDC). This is open specification with no licence fee payable to SUN. It considers all devices to be portals to services. And provides open standards between clients across industries – Digital TV / Automotive / Telephony.

Two security mechanisms are supported

- Two-pass classfile verifier (This generates a stack map at build time and downloads /verifies in the target device)
- Sandbox. Note that CLDC has no fine grain security and all Java apps/MIDP Applications (MIDlets) can access the same functions (the API is the sandbox and new capability can be added to the API if required)

It was noted that applications inside a sandbox are not trusted and that it is not possible to have a trusted application in the sandbox, adding that pjava 1.1 does not explicitly support fine-grained security, but it may be able to support multiple domains (the reference to pjava 1.1 is incorrect), but there may be an implementation to make pjava 1.1 deliver multiple domain support (by hard coding a number of domains and the access required for each, but this would not allow changes after implementation). Pjava 1.2 does allow fine grained security with flexibility. jdk 1.1 does not have fine grained security, but does have certificates. Therefore pjava 1.1 may not have a variable sandbox. Pjava 1.1 was upgraded to 1.2 to specifically include fine grained security (for running multiple domains).

In addition CLDC has a test suite to test applications against. Therefore an independent party can check the application before allowing download to a device.

MIDP Presentation

Mark Cataldo gave a presentation on Mobile Information Device Profile (MIDP).
MIDP is the first of many profiles to be defined in the Java Community Process (JCP) and is expected to be run on top of CLDC. Its objective is to create a common application development environment for 2 way communication devices.

Goals: small footprint 128k ROM / 32k RAM / efficient device (processor/ heap/ garbage collector) / short time to market.

New specifications for MExE

A new version of the MExE specification is now available (23.057v3.2.0)

USIM CR 31.102 approved regarding Support of root public keys. A change request has also been raised against the USIM to allow support of root public keys.

Storage of User Private Data in the user profile in the network

It was confirmed that new services may make use of user private data stored in the network, but only with user permission.

Journalling (Auditing)

There was a discussion on journalling in the handsets and whether journalling should have a default to 'ON', currently there is no default requirement.
It was pointed out that this will not overload the memory as earlier events will be overwritten.
It was pointed out that journalling all chargeable events would be appropriate. However it was also pointed out that the phone does not know which are chargeable events. Concern that logging everything will create an unusable record for the user. Anna Zhuang noted that journalling is already mandatory, the number of events is manufacturer dependent.
Because of these issues and on the concerns for the performance of the handset the discussion on the default was deferred to the next meeting.

Application\Activity Icon

An issue was raised with respect to supporting an icon for untrusted applications and network related activity. This was identified as a requirement of the terminal and not the application, that discussions had been raised on this subject before and rejected. It was recommended that a stronger case should be presented for change before resubmitting the CR.

User Profiles

Discussion on support user profiles MExE are required to identify the elements in the user profile and SWG 2 will then implement it. A draft LS will be produced to identify the information required for the user profile, emphasising the need to be internet minded and to standardise only the minimum amount of information elements.

Security

S3 will track MExE work and make recommendations through LS's where necessary. MExE members should have an informal meeting 3 times per year with S3 and that MExE should keep S3 informed of security during the year. Andrew Myers (BT) to be MExE/S3 liaison person, and to identify when items should be communicated to S3.

MExE will provide S3 with a briefing on proposed MExE R00 (See attached presentation)

Classmark 3 Security

Relies on the capabilities that CLDC and MIDP provide within the untrusted domain otherwise known as the Sandbox. CLDC/MIDP includes the Sandbox as an additional security domain to the Operator Domain, the Handset Maunfacturers Domain and the 3rd Party Domain. Security for the sandbox will be treated in the same way as that for Classmarks 1 & 2. Classmark 3 takes into account the special characteristics of CLDC.

References to 'sandbox' raised some confusion. The definition of the Java Sandbox may be technically different from the MExE use of sandbox. In addition the terms Sandbox and Domain caused a certain amount of confusion.

Call initiation and termination

There is no mention of a mechanism to allow user termination of an application however a user can terminate MExE application any time (maybe with another menu)

CLDC does not allow a MIDP application to call the functionality of the phone. Assuming that the underlying application/ user is allowed to set up a call the MIDP could use the http connection method to establish a link to a server. If the ability to set up a call did exist it would be in MIDP and could be quick. Concerns were raised that once MExE introduce this functionality, then any application could call on MIDP and so make a call.