3GPP TSG SA WG3 Security — S3#16 **S3-000679**

28-30 November, 2000

Sophia Antipolis, France

Source: **Motorola**

Title: **Options for Access Security for IM Domain**

Document for: **Discussion**

Agenda Item: **tbd**

Abstract

The multi-media domain connects together a variety of end-user equipment and services. End-user equipment includes a mixture of both wired devices and wireless devices. Connecting these devices using the Internet should utilize techniques that permit the greatest ease of interoperability between dissimilar equipment types. Provision of end-to-end security and authentication services is becoming an important service differentiator, and interoperability of the techniques for providing wired and wireless access to multimedia content and services is a critical success factor for next generation wireless systems.

1 Introduction

Enormous new markets have emerged as multi-media access and services become available to wireless devices. 3GPP Work Items have been created to facilitate common means of interoperation between dissimilar wireless devices. SA3 is concerned with the need for wireless security when User Equipment (UE) accesses the wireless network. Both known and potential security attacks must be rendered ineffective for the adversary.

In its deliberations to date, SA3 has been primarily concerned with a wireless-centric viewpoint whereby the UE seeks to gain access to the multi-media domain. In the current trust model, SA3 has postulated that the UE shares a secret with its HSS, where the HSS acts as a home register for multi-media access. Under this trust model it seems reasonable that signaling protocols may be established between the UE, various CSCFs, and the HSS to permit entity and message authentication, content integrity, and, where permitted, message privacy.

Several proposals have been offered by both Siemens and Ericsson which reflect this trust model, and these are being considered by SA3.

This trust model ignores a basic property of multi-media access which is that a diverse set of end-users may seek communications with each other, in addition to invoking access to service providers. Some of these end-users will be subscribers to the services of a wireless service provider and others will be subscribers to a wired (Internet) service provider (ISP). 3GPP draft TS 23.228 v1.2.0 illustrates this by means of Figure 4-2 whereby a third party service platform may exist outside of the wireless domain. Similarly, Annex B of draft TS 23.228 v1.2.0 is replete with figures that indicate SIP messages impinging upon, and being sent from, an S-CSCF into the internet void, apparently intended for other SIP servers that are not contained within the wireless network.

Security services for wired Internet devices are being specified in IETF RFC2543. The purpose of this discussion paper is to raise the concern that security services that are invoked to protect multi-mode (wired and wireless) multi-media access may be a concatination of dissimilar methods. Such techniques are often found to offer neither good security nor economy of operation.

2 Approaches to inter-working with Internet based devices

Based on the above discussion, it is recommended that SA3 consider the greater problem of multi-media access both into and out of the wireless domain prior to settling on a scheme that may be limited to protection of intra-wireless communications between wireless end-users and the wireless network.

To this end, three strategies are cited for discussion. Each may achieve multi-media access security that incorporates the wireless domain into the greater scenario that encompasses the entire Internet.

Strategy #1, Use a 3GPP-Specific Solution Throughout the Internet

A possible motivation behind this strategy is that all multi-media access be protected in a manner that becomes standardized by 3GPP. Thus every internet user will need to "belong" to an HSS, and 3GPP signaling will need to be adopted by IETF as the means for multi-media access. Since the number of users on the Internet is a quite large, a symmetric-key solution may be difficult to implement.

Strategy #2, Adopt an IETF-like solution, Modified to Accommodate 3G Wireless

The IETF has already begun its version of standardizing several methods of protecting multi-media users, as defined in RFC2543. SA3 may consider the possibility of adopting and adapting one or more of these methods, and working with IETF to generate a universal security standard for the Internet community at large. The advantage of this strategy is that a CSCF would perform security functions much like a SIP server. The disadvantage may be that undesired computational and signaling loads may be placed upon the wireless network. Hardware acceleration solutions may alleviate this concern.

Strategy #3, Design the P-CSCF as a Protocol Converter between IETF and 3GPP Signaling

3GPP could elect to isolate SIP signaling in the wireless domain from the SIP signaling that exists in the world that uses IETF protocols. Thus the P-CSCF would need to be "dual-ported" such that wireless protocols are executed on the wireless side, and Internet IETF protocols are performed on the wired side. This in turn would force the overall trust model to be transitive, whereby the P-CSCF would internally relay the state of trust between the wireless and wired worlds.

3 Recommendation

Motorola believes that the first strategy is not viable due to current trends in IETF and a large established base of users not currently belonging to an HSS. The third strategy may be possible, but it sets a complexity threshold that will likely inhibit the full potential of wireless multi-media access. Motorola therefore recommends that an investigation into the second strategy cited above be undertaken within SA3.

Agreement to use a particular strategy should occur prior to deliberations related to the development of Stage 2 information flows.