3GPP TSG SA WG3 Security **S3-030720**

18th – 21th November, 2003

Munich, Germany

Agenda Item: Presence, GAA

Source: Ericsson

Title: Comparison of authentication proxy solutions

Document for: Discussion/Decision

1. Introduction

Ericsson and Nokia have been driving slightly different versions of authentication proxy in SA3 [S3-020528, S3-030245]. Even tough the solutions are quite similar [see e.g. S3-030391], there are still known differences. This document reviews these solutions, and suggests a way forward.

2. Background

HTTP is probably the most widely deployed application layer protocol today. There are many standardization organizations that are defining extensions related to HTTP applications, e.g. IETF, W3G, OMA and Liberty Alliance. Extensions are easy to define, however, interoperability may become an issue if the extensions requires changes to the UE side implementations.

The Ut interface is not intended for accessing all kinds of HTTP based services. Instead, the primary use of this interface is to access services in the Mobile Operators trust domain [23.002]. This may also include third party service providers that have agreement with the Operator. HTTP and HTTPS may be used outside this interface to access services in other trust domains, e.g. in open Internet.

3. Alternative solutions

3.1 Reverse proxy

Reverse proxy is transparent to the UE, and consequently the UE does not know for fact that the proxy exists in the front of the application server. The UE behaviour is controlled in the network side by configuring DNS, TLS certificate and/or application server name space in appropriate way. The use of the proxy is not mandatory if those application servers that bypass the proxy have some parallel authentication mechanism, or have implemented NAF functionality, i.e. an interface to BSF.

The use of one TLS connection between the UE and the reverse proxy requires the use of some workaround as already pointed out in [S3-030553]. The use of these kinds of workarounds is very common in current Web applications. Since all of the workarounds are transparent to the UE, and they do not require any change to the standard UE side behaviour, 3GPP should not specify which method to use with reverse proxies.

The UE needs to use DNS for each new domain name, which may increase the delay at the beginning of browsing in some configurations. However, some workarounds, such as naming the application servers behind the proxy to match the domain name of the proxy (workaround 3 in S3-030553) lowers the number of DNS queries if compared to deployments without the proxy.

3.2 Forwarding proxy

Forwarding proxy is a fixed access point to some application servers. The UE must somehow know which services are located behind this access point, and consequently some additional configuration mechanism is needed. One alternative

is to re-use the OMA OTA configuration mechanism that uses SMSs for this purpose. Alternatively, OMA Device Management mechanism could be used. The use of OMA Device Management would still require a new object definition for proxy configuration. However, this can be quite easily done if 3GPP requested such extension from OMA. It is also possible that 3GPP defines its own Device Management application because Device Management has been designed to allow such extensions.

Available HTTP clients allow the configuration of one forwarding proxy. All HTTP requests are assumed to be sent to this forwarding proxy except the ones that are for the domains defined in the so-called “exception list”. Exception list may either have domain names or IP-addresses.

The fact that HTTP clients have only “exception list” and not “mandatory list” related to the forwarding proxy set some additional requirements for the solution. If not designed carefully, the solution may reveal the IP-addresses of the application servers behind the forwarding proxy to outsiders. Also, it is not appropriate to define exception list for the “rest of the world”. This may introduce a need for additional proxy in the network side.

If two proxies are needed in the network side, one must either have two separate HTTP applications in the UE, or more enhanced proxy architecture in the network side. One enhanced proxy architecture would be to have one forwarding proxy for all traffic at the edge of the network, and then fork the requests to some additional proxies further down to the network depending on where these requests are directed to, e.g. to the home network or to the open Internet. In this kind of configuration, the use of forwarding proxy minimizes the need for DNS in the UE, however, it requires the use of TLS for all HTTP traffic including normal HTTP browsing. But in general, the client may have to use DNS with every HTTP request depending on the configuration options and the network architecture.

Even though the forwarding proxy is able to minimize the number of parallel TLS connections and consequently the time needed for TLS set-up, these benefits do not come without additional costs. In particular, it is believed that the forwarding proxy requires a specific “agent” in the UE (see Figure 1). It is possible to save resources if the agent keeps the TLS session alive/suspended so when the next session needs to be set up the agent can resume the TLS session. However, this will also consume some unnecessary resources in the ME while the TLS session is not alive. Furthermore, it is not clear if the forwarding proxy solution will save resources compared to the cost to implement this in the UE.

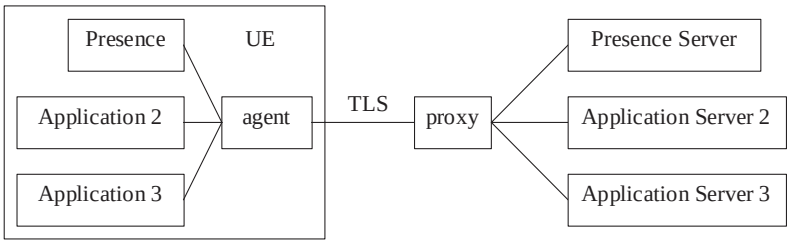

Figure 1: Possible UE side implementation with the forwarding proxy.

4. Conclusions

If the forwarding proxy were standardized in SA3, it would not automatically exclude the use of reverse proxy for the same purpose. Direct UE-to-Application-Server connections are also possible if the identities of these Application Servers are defined in the “exception list”. Both solutions would be open for use because in the end, the Mobile Operator will decide how to configure and build up the network.

Choosing the reverse proxy in SA3, on the other hand, will to some degree exclude the use of forwarding proxy assuming that not all clients have consistent proxy configuration mechanism. However, the use of reverse proxy does not exclude the use of direct UE-to-Application-Server connections (even though it requires the implementation of TLS and some authentication mechanism, such as GBA, in the application server). Note that there is a theoretical possibility of having a “reverse proxy” configured as the “forwarding proxy”. By definition, this configuration will make the “reverse proxy” to be a “forwarding proxy”. However, it is possible that the two proxy models co-exist if some UE’s are configured to use the “forwarding proxy” while others see the same proxy as a “reverse proxy”.

It is believed that the key element of the forwarding proxy, i.e. the configuration mechanism, is useful, and would fulfil the configuration needs related to other potential proxies located in the Operators network. Note that the use of

configuration options is not restricted to any authentication mechanism, such as GBA, and the use of other future applications is still possible in some other contexts in the future.

It is recommended that SA3 would keep the working assumption that the Presence Ut interface would benefit for having an authentication proxy. The working assumption should be that this proxy is of type “reverse proxy”. In this context, the definition of a reverse proxy is: a proxy that is transparent to the UE and consequently the UE does not know for fact that the proxy exists in the front of the application server.

The use of “forwarding proxy” may also be beneficial, however, it should not be made mandatory for the Ut interface. The following issues should be clarified if the forwarding proxy was included as an option for the Presece Ut interface:

- Exception lists; It is not clear how the forwarding proxy can be configured in the way that other HTTP accesses are still possible.
- Configuration mechanism; It is not clear which mechanism is used to configure the forwarding proxy in the UE, and if this mechanism should be mandated in the UE in order to achieve interoperability.
- Complexity of implementation in the UE; The use of the forwarding proxy may require a specific agent in the UE. It is not clear if the forwarding proxy solution saves resources enough compared to the complexity and cost of implementation in the UE side.
- Intensity of use: If the authentication proxy is only used as a management interface to services in the Mobile Operator’s network, the use of this interface may not be very intensive by the end-users. SA3 should consider if it is wise to introduce many 3GPP specific features for such interface.

5. References

[23.002] 3GPP TS 23.002 V6.2.0 Technical Specification Group Services and Systems Aspects; Network architecture (Release 6)

[S3-020528] HTTP Security, contribution from Nokia to SA3#25, Munich, Germany, 8 - 11 October 2002.

[S3-030245] HTTP Security in Mt interface, contribution from Ericsson to SA3#28, Berlin, Germany, 6-9 May, 2003.

[S3-030391] Comparison of different approaches in the Presence/Ut interface, contribution from Nokia and Ericsson to SA3#29, San Francisco, CA, USA, 15–18 July, 2003.

[S3-030553] Difficulties in using one TLS tunnel to access different servers behind an authentication proxy, contribution from Siemens to SA3#30, Povoa do Varzim, Portugal, 6-10 October, 2003.