3GPP TSG SA WG3 Security — S3#23 **S3-020244**

14 - 17 May 2002

Victoria, Canada

Source: Ericsson

Title: The use of IPv6 addressing privacy within IMS

Agenda item: ~~? IMS~~

Document for: Information

1 Scope and objectives

This document describes the IPv6 addressing privacy ~~addressing~~ feature and its implications in the IMS context.

2 Privacy Addressing Overview

RFC 3041 [RFC 3041] describes a form of privacy in how IPv6 addresses can be used.

~~Nodes~~ Hosts use IPv6 stateless address auto-configuration to generate addresses without any additional servers (except for a router). In 3GPP, a similar stateless approach is employed between the terminal and the GGSN. In 3GPP, ~~N and~~ each terminal is allocated~~s~~ a unique prefix that it may use for generating a whole range of addresses within that prefix.

Combining a ~~64 bit~~64-bit network prefix with a ~~64 bit~~64-bit interface identifier forms a ~~128 bit~~128-bit IPv6 address. On interfaces that contain embedded IEEE Identifiers, the interface identifier is typically derived from it. RFC 3041 describes how ~~nodes~~ hosts can generate global-scope addresses that change over time. This is done through a random generation of interface identifiers. Multiple addresses may be in use at any one time.

Changing the interface identifier (and the global-scope addresses generated from it) over time makes it more difficult for eavesdroppers and other information collectors to identify ~~when~~ whether different addresses used in different transactions actually correspond to the same ~~node~~host. RFC 3041 can of course be only used when stateless address auto-configuration is being used as well.

Many types of equipment such as laptops support RFC 3041.
It is expected that 3GPP terminals compliant to IPv6 protocol suite ~~will~~would also be able to also support RFC 3041 ~~in case ofwhere~~if they so desire. ~~stateless address auto-configuration is being used.~~

3 IMS Integrity Protection

IMS employs IPsec ESP for integrity protection between the terminal and the P-CSCF.

For the protection of IMS SIP traffic ~~between~~ with a specific terminal, two Security Associations are needed. The IP Security Architecture specification [RFC 2401] states, “A security association is uniquely identified by a triple consisting of a Security Parameter Index (SPI), an IP Destination Address, and a security protocol (AH or ESP) identifier.”

4 Privacy Addressing and IMS

IPv6 is employed in the IMS, as is SIP, and ESP-based integrity protection.

The addressing privacy function interacts with ~~and~~ the identification of SAs through addresses ~~interact. I: I~~f the terminal switches to a new IPv6 address while an SA from the P-CSCF is still active, the responses from the P-CSCF can not use the new address. Also, any communication from the terminal towards the P-CSCF can not use the new IP address to communicate with the P-CSCF having an active SA. If the terminal~~they did~~ uses a

new address according to the scenarios above, a RFC 2401 compliant IPsec implementation would not find the SA since the destination address would be different from what was agreed earlier. Furthermore, the P-CSCF needs to check the IP addresses and port numbers for the ~~in~~ traffic that is incoming to it destined to this terminal, and these checks would fail if new IP addresses were used. In IKE-based security associations these problems do~~es~~ not exist, because security associations can be renegotiated without the involvement of the application layer.

In outgoing calls, a SIP client implementation in general is allowed to use IP addresses and port numbers different from its currently registered contact address. Proxies and servers are expected to answer to the same address a particular request has been sent from. Incoming calls could still be accepted on the originally used IP address.

Due to the problems ~~related with changing IP addresses~~caused to the used security mechanism, the above general SIP behaviour ~~is can not~~should not be allowed within IMS.

5 Solutions

~~Instead, it~~It is suggested that IMS clients must ~~re-register and re-establish~~re-establish the security associations when they change IP addresses within a prefix.
Currently in 23.228, ~~it~~this is reflected as follows:

> "4.3.1 Address management
> The issues of general IP address management are discussed in TS 23.221 [7].
> According to the procedures defined in TS 23.060 [23], when a UE is assigned an IPv6 prefix, it can change the global IPv6 address it is currently using via the mechanism defined in RFC 3041 [16a], or similar means. When a UE is registered in the IM CN Subsystem, any change to the IP address that is used to access the IM CN subsystem shall trigger automatic registration in order to update the UE's IP address.
> ~~The ability of the User plane and the Control Plane for a single session being able to pass through different GGSNs is not defined in this release.~~
> "

How will this automatic registration then, in detail, take place? What IP addresses should be used in the re-registration procedure itself? How should the UE inform the IMS that it no longer wishes to use the old addresses? What are the implications for ongoing sessions?

The re-registration should take place as soon as the UE wishes to use the new address for IMS communications.

The first message pair in the re-registration should use the old IP addresses, due to the security being bound to them. The second message pair in the re-registration should use the new IP addresses.

A SIP REGISTER request contains contact information. There may be multiple contacts, and the contacts can be assigned expiry times. SIP registrars ~~in~~ maintain multiple contacts for each user, and a new REGISTER request does not in general override old ones, unless explicitly indicated in the message. In order to indicate to IMS that the old addresses should be deleted from the currently stored contacts list, clients must include the old contact information in the re-registration request in addition to the new one, and set the expiry time of the old contact information to 0.

Furthermore, it is suggested that UEs shall not start to use a new address while a session is in progress. Given that specific QoS may have been reserved for a particular flow and that these flows are identified by IP-level filters at the GGSN, changing the addresses in these packets is not possible.

~~5~~6 Conclusions

SA3 would agree to ~~this~~the principle in SA2 and in addition clarify in ~~Access Security spec~~TS 33.203 ~~t~~the following:

- IMS clients must re-register and re-establish the security associations when they change addresses.
- IMS clients must not use new addresses with old SAs when performing a re-registration procedure.
- IMS clients must use new addresses with new SAs when performing a re-registration procedure.
- IMS clients must include the old contact information in the re-registration request in addition to the new one, and set the expiry time of the old contact information to 0.

- The current model of maximum one SA pair and IP address being active for one user at a time should be kept. The purpose of the re-registration procedure is to change the address, not add a new one.
- IMS clients must not start to use a new address in ongoing sessions.

A liaison statement should be sent to ~~hat:~~
~~IMS clients must re-register and re-establish the security associations when they change addresses.~~CN1 in order to add rules to 24.229 for taking care of these issues.

6 References

[RFC 2401] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, November 1998.

[RFC 3041] T. Narten and R. Draves, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, RFC 3041, January 2001.