3GPP TSG SA WG3 Security — S3#16 **S3-000663**

28-30 November, 2000

Sophia Antipolis, France

Source: **Telenor**

Title: **Simplifying assumption for the use of IPsec in UMTS**

Document for: **Discussion/decision**

Agenda Item: **tbd**

Abstract

IPsec was designed to meet requirements from a wide selection of user environments and needs. It has a fairly complete set of features and can be adapted to many different needs. The UMTS core network is a highly homogenous network and from a UMTS core network perspective, a number of the options really aren't required. With this as a starting point it is suggested that some of the IPsec options is considered not to be part of the requirements for UMTS. By removing options one can have simpler and more stable SA negotiations, more straightforward interworking in addition to a generally less complex network to operate.

1 Simplifying assumption for the use of IPsec in UMTS

The simplification presented here draws on suggestions and contributions sent to the IPsec mailing list (ipsec@lists.tislabs.com). That being said, this contribution should be viewed in the context of security needs foreseen for the UMTS core network and more specific the UMTS core network control plane.

The suggested simplifications for the use of IPsec within the UMTS core network control plane are:

- Disallow/discourage use of IP payload compression together with IPsec
- Disallow/discourage use of transport-mode
- Disallow/discourage use of AH
- Disallow/discourage use of nested tunnels (only use chained-tunnels)

1.1 Disallowing/discourage use of IPsec compression together with IPsec

In this section it is argued that IPsec compression is not necessary or needed on the UMTS control plane. The basic reason for this is that IPsec compression is stateless and is consequently limited to work on only one IP packet at a time and that control plane packets are generally too small for compression to be effective. This seriously limits the compression rate and the gain probably cannot be justified when one also takes into account the processing overhead as well as the header overhead in the IP packet.

There is a standard way of compressing IP payload, which is defined in RFC-2393 "IP Payload Compression Protocol" (IPComp, PCP). PCP is, by necessity, a stateless protocol operating on one packet at a time. This means that compression algorithms that build dynamic dictionaries etc are of limited utility here. This is the case since the size of the packets is generally so small that the benefit of the dictionary is quite limited. Furthermore, the dictionaries must be rebuilt for every IP packet.

PCP, like AH and ESP, also requires an SA to be established. For PCP this SA is called an IP Compression Association (IPCA). The SA required by PCP is minimal since no keys or parameter need to be negotiated. The only issue that must be resolved is the compression algorithm to be used. The currently defined algorithms are LZS and Deflate.

PCP operates differently from AH and ESP in the sense that PCP need not be used for all IP packets even when it has been negotiated. This means that a compressed packet can be discarded if the compression isn't effective, and one can have policies to only compress when the size of the payload is above a certain threshold value[1].

1.2 Disallow/discourage use of transport-mode

*In this section it is advocated that only **tunnel mode** should be used for UMTS. This does not necessarily mean that **transport mode** need to be disallowed in UMTS, but simply that one can do without it and that is should not be used for control plane interworking between operators.*

Most communication between operators will take place between SEGs or other well-defined border gateways[2]. Since IPsec mandates use of tunnel mode when passing security gateways, an obvious simplification is to only mandate support for tunnel mode in UMTS. As for traffic internally in an operators network it is really for the operator to decide if transport mode or tunnel mode should be used, but we should recommend that only tunnel mode is used.

It must be noted that for case where both transport mode and tunnel mode are valid choices, there is some overhead in using tunnel mode. This overhead is due to the inclusion of an extra IP header. In terms of capacity, this overhead is insignificant in the core network. On the other side, only tunnel mode can provide confidentiality to the header part of the original packet.

1.3 Disallow/discourage use of AH

*In this section it is advocated that only **ESP** should be used for UMTS interoperability. This does not necessarily mean that **AH** need to be disallowed in UMTS, but simply that one can do without it and that is should not be used for control plane interworking between operators.*

IPsec provides two different methods of protecting the payload data. These are:

- **Authentication Header (AH)**

  AH provides the following security services: data origin authentication, data integrity and anti-replay. AH does not provide confidentiality.

- **Encapsulating Security Payload (ESP)**

  ESP provides all that AH provides in addition to selectively provide confidentiality and limited traffic analysis protection.

Considering this it may seem strange that AH is an option since the services that it provides are all found in ESP. However, AH do actually have broader coverage of its services since it also covers parts of the (outer) IP-header. Specifically, AH cover the immutable parts of the (outer) header in addition to the payload while ESP do not cover the (outer) IP header. The payload (DATA) is always considered immutable (which is one reason why NATs don't go well with IPsec).

---

[1] One suggested value here is 128 bytes.

[2] A BG will likely have some security functionality (FW etc) and will likely have to be treated as a security gateways from an IPsec perspective.

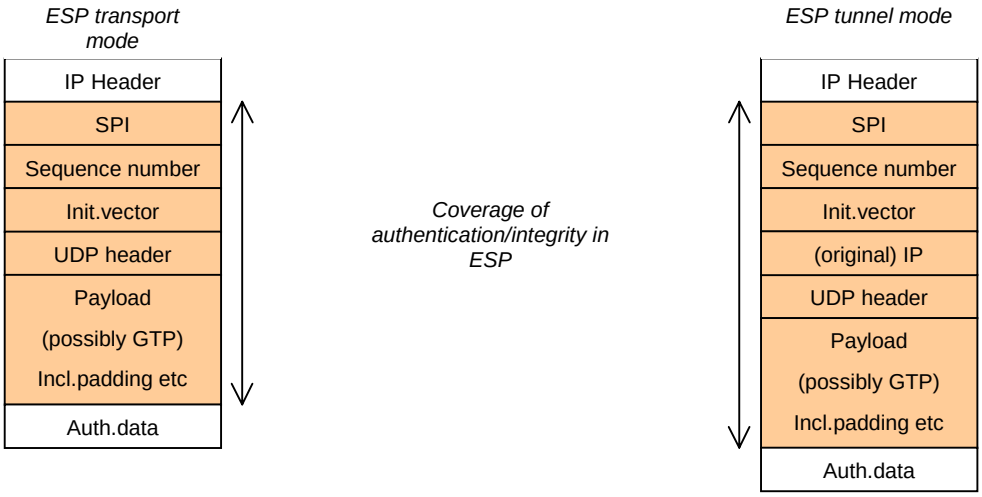

Figure-1: Coverage of authentication/integrity in ESP

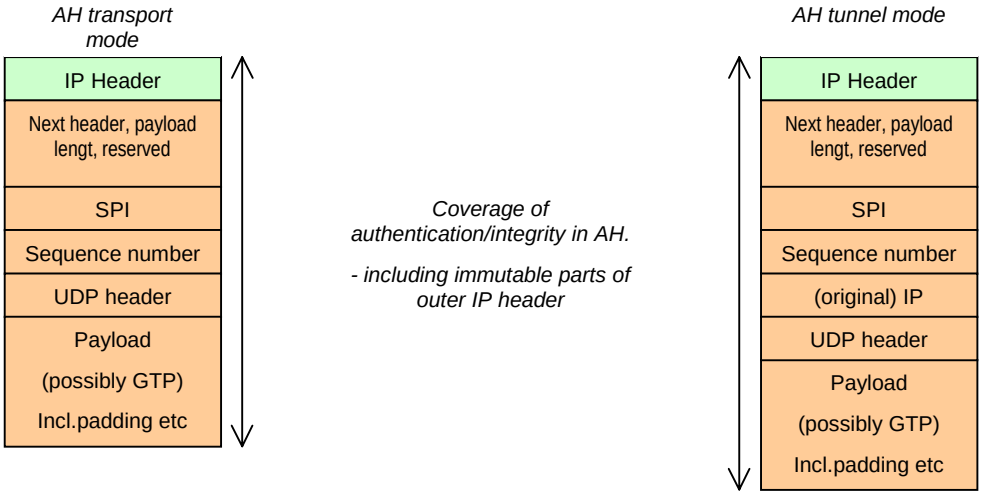

Figure-2: Coverage of authentication/integrity in AH

Version	Payload length	Type of service	Total length
Identification		flag	Fragment offset
Time to live	IP protocol	Header checksum	
Source IP address			
Destination IP address			

Figure-3: Mutable (yellow shade) and immutable fields of an IPv4 header

When it comes to the actual AH provided protection to the (outer) IP header, it covers all the immutable parts (figure-3) of the header.

For the UMTS case we must then try to identify the requirements for having authentication to cover the IP header. How important is it to provide data origin authentication to the (outer) IP header?

Since we for the control plane are dealing with the lower IP layer, we are in effect inside an intranet. This is also the case for interoperator traffic, which will be sent over GRX network(s)[3]. So the question is whether or not it is important to integrity protect the outer IP header. This question would to some extent depend on whether transport mode or tunnel mode is used. If tunnel mode is used, all of the original IP header (mutable and immutable) will be protected by ESP authentication. For transport mode, the original IP header is the only IP header and it will not be covered by ESP authentication.

It ought to be noted that the combination of AH and ESP (with encryption and without authentication) will provide the best protection from a security point of view. However, such a combination incurs some overhead in the IP packet as well as it will require separate SAs for AH and ESP.

The additional overhead can in all probability be justified since the penalty of some additional bytes to the packet in the core network is unlikely to affect the performance in any significant way.

It is noted that there are discussions within the IPsec community concerning the possible removal of AH, and that it has been suggested to propose an option pruned IPsec light specification where AH would be one of the candidates for omission.

1.4 Disallow/discourage use of nested tunnels (only use chained-tunnels)

In this section it argued that nested tunnels and complicated SA-bundle scenarios can be avoided. The provisions for avoiding nested tunnels and complicated SA-bundle scenarios are basically that we only specify use of chained ESP-only tunnels.

If the proposal for disallowing AH and transport-mode is accepted then the SA-bundle scenarios will be very much simpler. The only remaining alternative would then be nested ESP tunnels. There really is no strong incentive to use nested ESP tunnels in UMTS, and unless a positive case for nested ESP tunnels can be found we should disallow/discourage nested ESP tunnels.

For the UMTS core network control plane we do not normally need fine grained control over the way various protocols are protected. This allows for "permanent" and coarse-grained tunnels to be used. These permanent tunnels are usually termed *chained-tunnels* or *hub-and-spoke* type of tunnels depending on network topology. Use of *chained tunnels* also fits nicely with our need for SEGs to be able to process the original IP packet in clear.

[3] Note that operators are not strictly required to use the GRXs. However, the operators that choose not to use GRXs are likely to provide similar features as does the GRXs.

2 Conclusion

SA3 is asked to evaluate the following proposals:

- ***Disallow/discourage use of IP payload compression together with IPsec***

  Given that PCP is not likely to be very effective in terms of achieved compression rate and that bandwidth isn't particularly scarce in the core network, there really is no strong justification for deploying PCP. Consequently, it is suggested that PCP shall not be part of the requirements for TS 33.200 Network Domain Security. There is no need to explicitly forbid the use of PCP inside an operators UMTS core network, but it is suggested that PCP **shall not** be used for inter-operator traffic in the basic profile and that use PCP together with IPsec should be discouraged in general. This decision does not have an impact on security except from the possible benefit that management/complexity would be simpler.

- ***Disallow/discourage use of transport-mode***

  Only tunnel mode should be required to be supported in an UMTS network. The use of tunnel mode for inter-operator communication should be made mandatory. There is no explicit need to disallow transport mode. It is suggested that only tunnel mode is part of the basic profile. This decision has minimal security impact – the only effect is positive as confidentiality can be applied to the entire original IP packet including the header information.

- ***Disallow/discourage use of AH***

  For authentication/integrity protection in the UMTS core network control plane AH does not provide significant additional protection compared to ESP. We can therefore safely conclude that AH is needed in our case. Since ESP is required when passing security gateways and since only ESP can provide confidentiality, the logical conclusion seems to be that only ESP is needed. Given that, it would simplify matters quite a lot if AH could be disallowed/discouraged. For the inter-PLMN interworking case AH should simply be disallowed to ensure smooth interoperability. SA3 should perhaps not explicitly disallow use of AH within one operators network, but we should nevertheless recommend that only ESP be used.

- ***Disallow/discourage use of nested tunnels (only use chained-tunnels)***

  The NDS architecture will be greatly simplified if only ESP in tunnel mode is allowed. A further simplification is to disallow/discourage the use of nested tunnels. Provided that no significant case for nested tunnels is presented, we should at least disallow nested tunnels for the inter-PLMN case. We should never recommend use of nested tunnels unless a convincing case is brought forward. The net effect of the above proposals is that we should build our NDS architecture around chained ESP tunnels.

3 References

RFC 2393 IP Payload Compression Protocol (IPComp)
A. Shacham, R. Monsour, R. Pereira, M. Thomas; December 1998

RFC 2401 Security Architecture for the Internet Protocol
S. Kent, R. Atkinson; November 1998

RFC 2402 IP Authentication Header
S. Kent, R. Atkinson; November 1998

RFC-2406: IP Encapsulating Security Payload
S. Kent, R. Atkinson; November 1998