3GPP TSG SA WG3 (Security) –S3 #33 **S3-040284**
10-14 May 2004
Beijing, China

Agenda Item: **6.10 – WLAN Interworking**

Source: **Nortel Networks**

Title: **Use of IKE in End-to-end tunneling**

Document for: **Discussion and Decision**

1. Introduction

In the latest version of WLAN Interworking Security TS 33.234 v6.0.0 (approved in SA#23), the working assumption of SA3 is to use IKEv2 with IPSec ESP for security in establishing end-to-end tunnels to the HPLMN for accessing home network services by the WLAN UE's. In annex E, the TS also mentions two alternative mechanisms for the set up of UE-initiated tunnels (Scenario 3):

- IKEv1 with Subscriber certificates
- IKEv2 with Subscriber certificates

In this contribution, we analyze some practical difficulties or issues in mandating only IKEv2 in the specification and recommend that 3GPP allow the use of IKEv1 with subscriber certificates for establishing UE-initiated tunnels when an operator has the infrastructure to issue subscriber certificates. Furthermore, we also request SA3, to allow the use of IKEv2 with subscriber certificates in order to enable the migration of any installed base of users who are using IKE with subscriber certificates. Allowing these two options in the specification is also beneficial in scenarios where the service provider already has PKI infrastructure available in their network.

2. IKEv2 Specification

According to [IKEv2]:

"This version of the IKE specification combines the contents of what were previously separate documents, including ISAKMP (RFC 2408), IKE (RFC 2409), the Internet DOI (RFC 2407), NAT Traversal, Legacy authentication, and remote address acquisition.

Version 2 of IKE does not interoperate with version 1, but it has enough of the header format in common that both versions can unambiguously run over the same UDP port."

Some other key features of IKEv2 are:

- preserves most of the functions of IKEv1
- re-designs the protocol for efficiency, security, flexibility and robustness
- Supports EAP in order to re-use legacy authentications
- Support for NAT traversal (using UDP encapsulation with ESP SPI value of zero)

3. IKEv2 IETF Status

The IKEv2 draft is currently at revision 13. On April 7, 2004, on the IETF IKEv2 mailing list the following conversation took place between Cisco and the editor of IKEv2 (http://www.vpnc.org/ietf-ipsec/mail-archive/msg03199.html):

> *To: "Kevin Li", <ipsec@xxxxxxxxxxxxxxxxx>*
> *Subject: RE: IKEv2 Standardization*
> *From: "Charlie Kaufman" <charliek@xxxxxxxxxxxxx>*
> *Date: Wed, 7 Apr 2004 17:05:11 -0700*
>
> *The only analogy I can think of is being pecked to death by ducks. IKEv2 has been on final drafts for over a year, and was pretty much done a year before that. It will never be the case that there is nothing anyone can think of to 'improve'. I don't know how to make it stop.*
>
> *>Will it take another half a year or more?*
>
> *I would confidently say 'certainly not' except I've said that so many times that I'm no longer credible even to myself.*
>
> *--Charlie*
>
> *-----Original Message-----*
>
> *From: Kevin Li [mailto:kli@xxxxxxxxx]*
> *Sent: Wednesday, April 07, 2004 4:41 PM*
> *To: Charlie Kaufman; ipsec@xxxxxxxxxxxxxxxxx*
> *Subject: IKEv2 Standardization*
>
> *Hi Charlie and IKEv2 folks,*
>
> *I am separating this question from another email thread to be more specific.*
>
> *We like the simplicity, efficiency and clarity of IKEv2, and have projects implementing it on various Cisco products. However, I am a little bit concerned that our implementation based on current IKEv2 spec won't interoperate with products from other vendors based on the standard IKEv2 (future).*
>
> *There have been some update activities on IKEv2 protocol spec, the latest version now is IKEv2-13. I am wondering how far away IKEv2 spec is from standardization? Will it take another half a year or more?*
>
> *It would definitely help if we could get some sense of how mature the IKEv2-13 is from the IKEv2 experts' point of view.*
>
> *Thank you very much.*
>
> *Kevin Li*
> *Cisco Systems*

The IKEv2 draft is currently in IETF last call and the expectation is that it will move to Proposed Standard RFC status in a few weeks or months. However, The Internet Standards Process (RFC 2026), section 4.1.1 states that:

"…

A Proposed Standard specification is generally stable, has resolved known design choices, is believed to be well-understood, has received significant community review, and appears to enjoy enough community interest to be considered valuable. ***However, further experience might result in a change or even retraction of the specification before it advances***

…"

Even if the IKEv2 draft moves to RFC status, it does not imply that the products implementing IKEv2 will be commercially available, due to the reasons provided in the next section (Section 4).

4. IKEv2 Product Implementation status

The two well-known consortiums that perform interoperability testing and certify IPSec implementations are ICSA Labs IPSec Product Consortium and the VPN Consortium.

ICSA Labs IPSec Product Consortium (www.icsalabs.com) whose mission is to "To promote consumer confidence in the use of IPSec products and to facilitate interoperability". Its test plans are driven by vendor interest and product capabilities and according to their roadmap (in http://www.icsalabs.com/html/communities/ipsec/membership/IPSec_Mtg_Sum021903.pdf), they are still awaiting IKEv2 to become RFC, before even developing a test plan. Furthermore, they also released a program paper on IKEv2 titled "IKEv2 - If They build it, Will they come?". Some relevant extracts from this paper are given here:

> "*"The consensus of the Consortium was that specific testing points were NOT what needed to be discussed, instead, what WAS more important was communication regarding the broader business justification for even contemplating developing and exerting resources to meet IKEv2 requirements."*
>
> *"…whether anyone was going to expend time, energy & resources into developing IKEv2 before there was evidence of a need for it from the industry…"*
>
> *"What would push accelerated adoption of IKEv2 standards would be an exploitable vulnerability in IKEv1, of which none of a severe nature has been identified."*
>
> *"Will a simplified IKEv2 by itself justify the development by the manufacturers and implementations by existing extranets consisting of disparate VPN equipment?"*

Another organization, VPN Consortium (www.vpnc.org), conducts interoperability testing. It is focused on gateway-to-gateway testing using pre-shared secrets and certificates (using IKEv1) only. Advanced testing includes support of AES with 128-bit keys. According to a recent (April 20, 2004) private communication with the Director of the VPN Consortium, Paul Hoffman, indicated the following:

> *"No one has announced any IKEv2 implementations yet because the spec is still not finished. I doubt you'll see any final implementations this year."*

To date, there is no known IKEv2 implementation, test plan or interoperability testing event.

5. Other Issues with 3GPP use of EAP-AKA/SIM with IKEv2

According to the "HSS-Related design guidelines for a Security Architecture" agreed in SA3#29 (refer to the SA2#29 meeting report), it is desirable to use a solution which does not consume (or at least keep it to a minimum) the authentication vectors (AVs) and/or avoid having interface to the HSS. The use of AVs for scenario 3, in addition to other authentication domains (e.g., GSM CSD, GPRS CSD, UMTS CSD and PSD, IMS, GBA and WLAN access) only exacerbates synchronization failure problem. It should be noted that GBA may have to have multiple authentication domains within it, depending on whether key separation is provided for different application servers in GBA domain (refer to TS 33.220). The practical implications of using AVs across so many authentications domains (and some may consume AVs more frequently) is not yet proven to be viable approach in the longer-term. In our view, this is also a significant concern that warrants that future solutions (such as WLAN scenario 3) should offer alternative mechanisms for end-to-end tunnel authentications.

6. Possible options

I. Allow only IKEv2 with EAP-SIM/AKA: Although this option appears the most elegant from theoretical point of view, it will not get implemented if operators want to provide WLAN scenario 3 services before the commercial availability of IKEv2 based VPN gateways. Furthermore, if the operators have subscriber certificates implemented in their networks, it does not allow them to use it for scenario 3 security purposes. Therefore, in our view, it is desirable to specify other options in the standards so that any early deployments as well as future deployments with subscriber certificates will be standards compliant.

II. Allow only use of IKEv1 with subscriber certificates: This option requires that all operators wishing to offer scenario 3 have PKI implemented in order to be standards compliant.

III. Allow only use of IKEv2 with subscriber certificates: same problem as in option 2, in addition to the availability of IKEv2 compliant VPN gateways

IV. Allow use of IKEv1 with subscriber certificates, in addition to Option 1: This is desirable as it offers standards compliant solution to at least some operators who have support for subscriber certificates before IKEv2 VPN gateways are available.

V. Allow use of IKE and IKEv2 with subscriber certificates, in addition to Option 1. This is most desirable from standards perspective, as it offers operators standards-compliant solution before IKEv2 based IPSec is available and allows them to migrate to IKEv2 with subscriber certificates when IKEv2 becomes available. Also, depending on when IKEv2 based solutions are available, 3GPP may study in a future release the migration issues and provide recommendations on how to migrate from IKEv1 implementations.

Other architectural options are possible and some were discussed by SA3 in earlier meetings and eliminated (for example, S3-030550). Therefore, we do not consider them further in this contribution.

7. Roaming

As both WLAN access clients for scenario 3 and the PDGs are under the control of HPLMN, we do not foresee any interworking problems for the various WLAN roaming scenarios.

8. Conclusion

In this paper we provided information with respect to the expected commercial availability of IKEv2 in product implementations. Our view is that availability of IKEv2 VPN gateways is uncertain and therefore we propose that:

Proposal 1: SA3 agree to include the alternative solutions for WLAN scenario 3 end-to end tunnel security in the WLAN TS

Proposal 2: If the proposal 1 is agreed, then we further propose that the option V (i.e., allow the use of IKE and IKEv2 with subscriber certificates, in addition to IKEv2 with EAP-SIM/AKA) is included in the main body of WLAN TS (although, option VI is also acceptable to us).

Due to the uncertaintcommercial availability of VPN gateways with IKEv2 we believe that allowing more than one option for establishing IPSec tunnel for WLAN scenario 3 is justified as an exceptional case.

A CR to TS 33.234 implementing proposal 2 (with option V) is also presented to this meeting in a separate contribution.