Pervasive Service Access with SIM-based VPN

Do van Thanh – Telenor & NTNU, Norway – thanh-van.do@telenor.com
Ivar Jørstad – Ubisafe, Norway – ivar@ubisafe.no
Tor Anders Johansen– Ubisafe, Norway – tor.anders.johansen@ubisafe.no
Elias Bakken – Ubisafe, Norway – elias.bakken@ubisafe.no
Do van Thuan – Linus, Norway – t.do@linus.no

Abstract – **Mobile users need to have access to internal resources on their enterprise or home network from remote locations in an efficient but secure way. Currently, such a secured access is realised with Virtual Private Network (VPN) connections. Although operational, the current VPN solutions suffer of severe limitations. Most of the VPN solutions are not sufficiently secured since they are using weak authentication. The more secured ones are quite often expensive and require the usage of security tokens that demand administration from the service provider. On the user's side there is a need for additional care and attention since he/she has to carry an extra device. This paper presents a VPN solution that remedies the mentioned limitations by re-using an existing device, namely the mobile phone and its SIM card as a security token. Another ingenuity of the solution lies on the separation of the authentication phase from the rest of the VPN establishment process making possible the usage of the same security token for multiple VPNs. The solution is hence secured, affordable and practical for the users.**

Keywords: VPN, Virtual Private Networks, SIM, mobile phone authentication, SIM authentication

I. INTRODUCTION

With its ubiquitous presence the Internet has brought universal connectivity to mobile users and enabling them to be "always-on". However, it is completely useless to be always connected if access to services and contents is not allowed. Unfortunately, the increase in frauds and attacks on the Internet have forced every Internet player from enterprises, banks, governmental offices to even private home networks to barricade themselves behind firewalls, which ultimate goal is to limit access to services and contents. To re-enable controlled access to internal resources, virtual private networks (VPNs) are then introduced establishing "virtual" connections routed through the Internet from the player's private network to the mobile users. Although operational, current VPN solutions suffer of severe limitations. Indeed, many of them are not sufficiently secured since weak authentications, e.g. passwords, are often used. The more secured VPN solutions are quite often expensive and require the usage of security tokens that demand administration from the service provider. Furthermore additional care and attention are required from the user since he/she has to carry an extra device.

This paper presents a VPN solution that remedies the mentioned limitations by re-using an existing device, namely the mobile phone and its SIM card as a security token. Another ingenuity of the solution lies on the separation of the authentication phase from the rest of the VPN establishment process making possible the usage of the same security token for multiple VPNs. The solution is hence secured, affordable and practical for the users. A proof-of-concept prototype has been successfully implemented within the framework the EUREKA Mobicome project[1]. The paper starts with a brief introduction to VPNs. Next, the limitations of the state-of the art VPNs are clearly explained. The high level requirements of an ideal VPN are then specified. The SIM-based VPN is described thoroughly. To illustrate the simplicity of usage, the establishment of the SIM-based VPN is depicted.

II. BRIEFLY ABOUT VIRTUAL PRIVATE NETWORKS

A. Architecture

The goal of a VPN solution is to establish a secure communication channel between different networks, or between a user and a specific network (e.g. the enterprise network), from remote locations. The secure channel is typically established across a public network, usually the Internet. After the establishment of a VPN connection, hosts on one of the networks will perceive hosts on the other network as part of the same Local Area Network (LAN), and users are thus able to access services as if they were local. A special configuration often referred to as "road-warrior" is commonly used by employees to remotely

[1] The EUREKA Mobicome project with the participation of Telenor, Telefonica, Ericsson, Linus, Ubisafe, Oslo University, Polytechnic University of Madrid, Blekinge Institute of Technology, HiQ, is aiming at providing Fixed-Mobile Convergent IMS environment.

978-1-4244-5113-5/09/$25.00 ©2009 IEEE

access their enterprise network, and their computer (e.g. laptop) will become part of the same sub-network as the enterprise network upon successful connection, i.e., the computer will get a local address.

To summarise, there are two major VPN types:

Network-to-network (site-to-site) – Usually used to unify geographically distributed network sites of an enterprise (e.g. its branch offices) (See Figure 1).

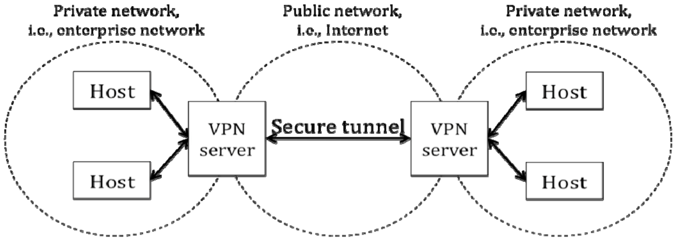

Figure 1 Typical network-to-network VPN architecture

Road-warrior (remote access) – Usually used for employees to connect to their enterprise network from remote locations, e.g., from home (see Figure 2).

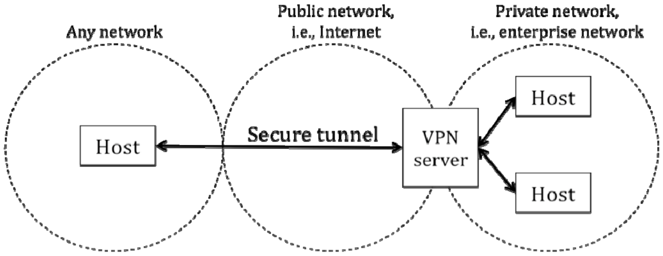

Figure 2 Typical road-warrior VPN architecture

B. VPN security functions

Every VPN solution must at least include two security functions:

- ***Authentication*** – In order to grant access to network resources from remote locations across a public network, a VPN solution must include proper authentication mechanisms, i.e., the determination of a valid user and his/her access rights.

  Typical authentication mechanisms for VPNs include:

  - Username and password
  - Pre-shared keys
  - Smart Card with PKI
  - One Time Password (OTP) with code generator
  - One Time Password (OTP) with Short Message Service (SMS)
  - Other methods supported through RADIUS/DIAMETER

  Brief descriptions of some common protocols for authentication in VPNs are now provided.

  IKE [1] [12][13] – IPSEC VPN tunnels can be configured statically or established dynamically using messages defined by the Internet Key Exchange (IKE) standard. IKE lets two VPN gateways authenticate each other, negotiate security parameters, and generate keys for data encryption and integrity. IKE uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived. Public key techniques or, alternatively, a pre-shared key, are used to mutually authenticate the communicating parties.

  XAUTH [2] – The authentication methods supported by IKE are a good fit for site-to-site VPNs, but IKE does not support asymmetric user authentication methods like passwords, challenge/response exchanges and two-factor tokens, which are commonly used for remote access. To overcome this, many vendors implement non-standard enhancements like XAUTH (Extended Authentication). XAUTH is an Internet Draft that supports asymmetric authentication by inserting a new message exchange after Main/Aggressive Mode (IKE Phase 1) and before IPSEC parameter negotiation (IKE Phase 2). VPN gateways that use XAUTH can prompt remote users for a secondary login. If user login succeeds, IPSEC setup continues; otherwise, setup is abandoned. XAUTH – and an improvement called Hybrid – are widely implemented in VPN solutions to enable user authentication with "legacy" credentials like Windows logins or SecurID tokens.

  PAM [3]– Pluggable Authentication Module (PAM) is a mechanism to integrate multiple low-level authentication schemes into a high-level API. It allows programs that rely on authentication to be written independently of the underlying authentication scheme.

- ***Encryption*** – Since communication typically travels across an unsecured, public network, it is necessary to use encryption of user data travelling between the two sites (e.g. between the user and the enterprise network), in order to provide confidentiality and prohibit eavesdroppers any access to the potentially sensitive information sent between the sites.

  Typical protocols for VPNs include:

  IPSEC [4][5] – Internet Protocol Security (IPSEC) is a protocol suite for securing IP communications by authenticating and encrypting the IP data stream.

IPSEC also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPSEC can be used to protect data flows site-to-site or remote access to enterprise network.

SSL/TLS [6]– Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security and data integrity for IP based communications. SSL and TLS encrypt the segments of network connections at the Transport Layer end-to-end. The TLS protocol is designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography.

Utility of TLS – There has been substantial development since the late 1990s in utilizing TLS outside of the browser to enable support for client/server applications. For instance TLS can be used to tunnel an entire network stack to create a VPN, as is the case with OpenVPN.

OpenVPN – OpenVPN is a free and open source VPN system. It is capable of establishing direct links between computers across network address translators (NATs) and firewalls. OpenVPN offers pre-shared secret key, certificate-based, and username/password-based authentication. Preshared secret key is the easiest, with certificate based being the most robust and feature-rich. Username/password is a new feature (v2.0) that can be used with or without a client certificate (the server still needs a certificate).

When compared with traditional IPSEC VPN technologies, TLS has some inherent advantages in firewall and NAT traversal that make it easier to administer for large remote-access populations.

III. LIMITATIONS OF STATE-OF THE ART VPNs

Security weaknesses of VPN solutions have been studied in depth in the literature. In [7], several common VPN security flaws are described. One major limitation of current VPN solutions lies on its first security function, namely the authentication of users. A strong authentication is often both expensive and complex to the users whiled affordable and user friendly authentications tend to be weak. The challenge is to incorporate a solution that is secure, cost-efficient and user-friendly. The current authentication mechanisms for VPNs suffer of limitations as follows:

- ***Username and password*** – Username password authentication is usually not sufficiently secure, since a security breach would allow illegitimate users access to an enterprise's often highly confidential resources. Username and passwords are subject to plain guessing attacks, brute force-attacks and dictionary attacks etc., and are too dependent on the users being careful in the selection of passwords. For an enterprise that takes security seriously, the responsibility of security should not primarily be left with the users, since they often have a misconception of what constitutes a secure password and what does not.

- ***Pre-shared keys*** – Pre-shared keys may be secure, but the administrative procedures for deployment may be time-consuming and costly. It is crucial that the transport of a pre-shared key between two locations is performed in a security-conscious manner, i.e., not sent by unencrypted mail or stored in transit in various locations.

- ***Smart Card with PKI*** – These solutions are highly secure, but the major drawback is the cost of establishment and maintenance. Users need an additional card reader, as well as a Smart Card with their certificates and private keys installed.

- ***OTP with code generator*** – Another option is to use One-Time-Passwords (OTP) based on code generators (physical, electronic devices typically capable of generating 4-6 digit codes). However, these solutions have some of the drawbacks as Smart Card-based solutions; they are costly in deployment and maintenance due to the added device. However, the security may be quite good.

- ***OTP with SMS*** – There are solutions that allow users to receive OTP through the Short Message Service (SMS) on their mobile phones. These are quite secure (it requires substantial resources to be able to eavesdrop on GSM communication), but may be costly due to the added cost of sending an SMS for each authentication. Depending on the volume of authentication transactions in an enterprise, this may become a relatively large expense.

IV. VPN HIGH LEVEL REQUIREMENTS

Based on the observations collected from the previous sections the following high level requirements on VPN can be derived:

1. ***Provide adequate protection of local resources*** – This is definitely the number one requirement of any VPN solution. If adequate protection of shared resources is not possible, VPN should not be introduced into an organisation as a means for allowing employees to perform work remotely.

2. ***Enable easy sharing of resources from remote locations*** – After the previous requirement, this is the most important requirement of a VPN, and it is also the reason for introducing a VPN in the first place.

3. ***Provide adequate protection of the user*** – The VPN should preserve privacy and prohibit identity theft.

4. ***Offer simpler usage and care from the user*** – Although making use of strong authentication the VPN should offer very user-friendly user interface and no additional care should be required from the user.

5. ***Provide simple and cost-efficient administration for network owners*** – The VPN should enable network owners (i.e., enterprises, home users, etc.) to easily and cost-efficiently administrate the users of the VPN.

V. THE SIM-BASED VPN SOLUTION

The functional architecture of the SIM-based VPN solution is depicted in Figure 3.

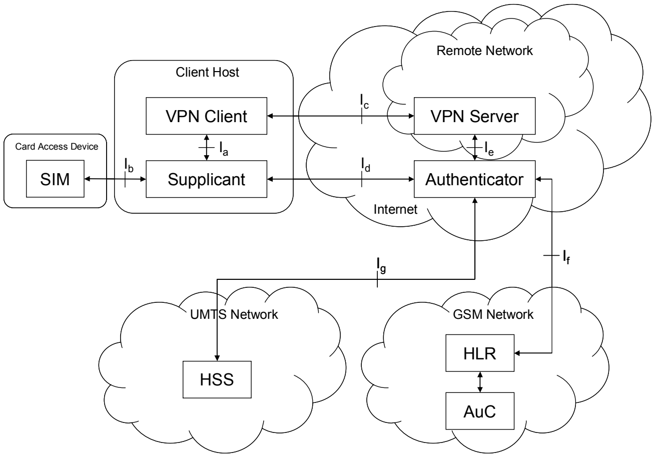

Figure 3 The SIM-based VPN functional architecture

A. Strong and simple authentication with SIM card

To satisfy the requirement 3 concerning adequate protection of the user the proposed VPN solution must employ strong authentication. Although there are other alternatives the most popular authentication is two factor authentication which combines one first factor characterised by "something you know" and a second one characterised by "something you have". Consequently, two factor authentication requires the usage of an additional device, which demands administration from the network owner and extra care from the user.

To avoid introducing extra device which could be inconvenient to the user, our SIM-based VPN solution proposes to re-use an already in-use device, namely the mobile phone. Indeed, the mobile phone is today the most popular mobile device and a vast majority of mobile users carrying a laptop is equipped with mobile phone. The mobile phone hosts a SIM (Subscriber Identity Module) card which is a tamper-resistant smart card. Originally, the SIM card is intended for the authentication and authorisation of the mobile phone to the mobile network but there are recently a few proposals to extend the usage for other services and applications [8][9]. We propose now to extend the usage of the GSM authentication and the SIM card to the VPN authentication. The authentication is a strong two factor authentication with the mobile phone as "something you have" and the PIN code as "something you know". The user will benefit from the fact that he/she has one PIN code less to remember. The requirement 4 regarding simpler usage and care is hence satisfied.
As shown in Figure 3 the VPN authentication is assumed by the SIM card, the Supplicant on the client and the Authenticator on the network.

The ***SIM card*** is an ordinary GSM Subscriber Identity Module (SIM) or UMTS USIM etc. There are no modifications to the card, i.e. no installation of additional software on the card is required. This is important to ensure that any mobile operator can support the service model without modifying their subscribers' modules. The SIM is accessed across the Ib interface by the Supplicant, and this interface supports the Smart Card APDU according to [10][11]. The physical bearer can be either USB as in the case of a USB dongle carrying a SIM and plugged onto the USB port of the PC or Bluetooth in the case of a mobile phone connected to the PC via Bluetooth.

The **Supplicant** is a software component located on the user's device and is acting as mediator between the authentication device, i.e., SIM, and the authentication server referred to as the Authenticator in this architecture.

The **Authenticator** is the counterpart of the Supplicant, and is the mediator towards the mobile telecommunication network components (i.e. Home Location Register (HLR) with Authentication Centre (AuC) in GSM network or Home Subscriber Service (HSS).

B. Delegation of authentication to third party

The biggest obstacles of VPN solutions are the high costs at deployment and most importantly the high operational expenses (OPEX) related to the usage of strong authentication. By removing the authentication from the VPN solution, the proposed solution becomes much more cost efficient and hence satisfying the requirement 5 concerning cost-efficiency. Indeed, the authentication performed by the Supplicant and the Authenticator can be administered in a more efficient way by a third party, which can be the mobile operator or an identity provider.

As shown in Figure 3, two interfaces *Ia* and *Ib* have been introduced to allow the initiation and accomplishment of the authentication by the VPN as follows:

The **VPN client** is an ordinary VPN client, e.g. supporting either IPSEC or SSL/TLS for establishing secure tunnels with a VPN server, that is modified to communicate directly with the Supplicant across the *Interface Ia* (e.g. by utilising the clients plug-in architecture, sockets or any other inter-process-communication mechanism.), or indirectly using shared memory.

The **VPN server** is an ordinary VPN server, which is modified to communicate directly with the Authenticator, or indirectly using shared memory. *Interface Ic* corresponds to the VPN protocols supported by the VPN solution.

C. Generation of encryption key with GSM ciphering key

To protect resources and satisfying the requirement 1 and 2 encryption must be used to establish a secure channel between the VPN client and VPN server. The proposed solution provides a simple method for generating the encryption key needed the encryption of data and a safe method for the exchange of encryption keys.

Upon successful authentication, the Authenticator sends n new challenges to the Supplicant. The Supplicant then invokes the A8 GSM algorithm on the SIM card n times for the generation of n cipher keys [Kc1, Kcn]. A string K of n*64 bits can be obtained by the concatenation of the n ciper keys as follows:

K = (Kc1 | ... | Kcn) of length n*64 bits.

The encryption K can be then passed to the VPN client by the Supplicant. The Authenticator can perform the similar operation on its side to generate the same encryption K and transfer it to the VPN server. The encryption K can now be used to set up an encrypted connection between the VPN client and server. K can be of any length to fit to the encryption algorithm used.

VI. AN ILLUSTRATING USE CASE

To elucidate the proposed SIM-based VPN solution a use case is given in

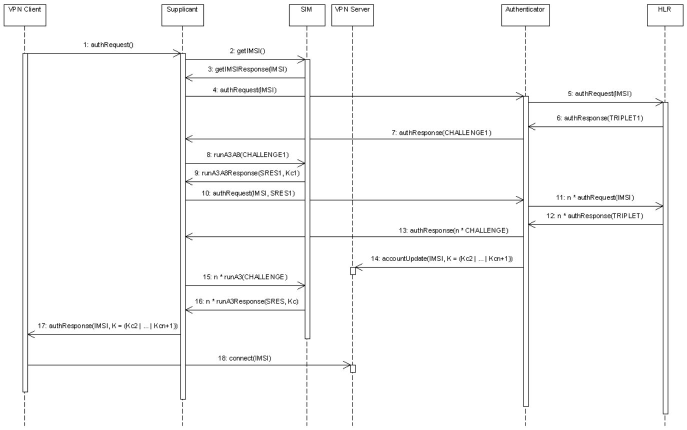
VPN Client
Supplicant
SIM
VPN Server
Authenticator
HLR
1: authRequest()
2: getIMSI()
3: getIMSIResponse(IMSI)
4: authRequest(IMSI)
5: authRequest(IMSI)
6: authResponse(TRIPLET1)
7: authResponse(CHALLENGE1)
8: runA3A8(CHALLENGE1)
9: runA3A8Response(SRES1, Kc1)
10: authRequest(IMSI, SRES1)
11: n * authRequest(IMSI)
12: n * authResponse(TRIPLET)
13: authResponse(n * CHALLENGE)
14: accountUpdate(IMSI, K = (Kc2 | ... | Kcn+1))
15: n * runA3(CHALLENGE)
16: n * runA3Response(SRES, Kc)
17: authResponse(IMSI, K = (Kc2 | ... | Kcn+1))
18: connect(IMSI)

Figure 4 Sequence diagram for SIM-based VPN

1. The user decides to connect to the VPN, and the VPN Client sends an authentication request to the Supplicant.

2. The Supplicant requests the IMSI (International Mobile Subscriber Identity from the user's SIM card.

3. The Supplicant receives the IMSI from the user's SIM card.

4. The Supplicant sends an authentication request to the Authenticator with the IMSI as input parameter.

5. The Authenticator sends an authentication request to the HLR in the GSM network with the IMSI as input parameter.

6. The Authenticator receives a triplet (TRIPLET1) from the HLR, which includes a challenge, the expected result from running the GSM A3 algorithm on this challenge (XRES1) and an encryption key (Kc1) generated by the A8 algorithm.

7. The Supplicant receives the challenge from the Authenticator.

8. The Supplicant initiates the execution of A3 algorithm on the SIM card, using the received challenge as input.

9. The Supplicant receives the signed response (SRES1) and an encryption key (Kc1) from the SIM, which are the results from running the A3 and A8 algorithms.

10. The Supplicant issues a new authentication request towards the Authenticator, carrying the user identity (IMSI) and the signed response (SRES1). This authentication request should/could be carried across an encrypted connection set up with Kc1 as the encryption key.
The Authenticator verifies that SRES1 matches with XRES1. If there is no match, the Authenticator returns an error message to the Supplicant that forwards it to the VPN Client. Upon match the Authenticator proceeds with step 11.

11. The Authenticator issues n additional authentication requests towards the HLR in the GSM network in order to generate a sufficiently long encryption key for the VPN connection.

12. n triplets carrying n ciphering key Kc are returned by the GSM network.

13. The Authenticator sends back to the Supplicant a response carrying n challenges from the triplets received by the Authenticator from the GSM network.

14. The Authenticator sends to the VPN server a message to request an update of the encryption key with the new one K = (Kc1 | … | Kcn)

15. The Supplicant sends n challenges to the SIM card that runs the A3/A8 algorithm n times.

16. The SIM card returns a message carrying n SRES and Kc.

17. The Supplicant returns now to the VPN server a message containing an encryption key K = (Kc1 | … | Kcn) to be used.

18. The VPN client can now send to the VPN server a connection request containing the subscriber identity IMSI and the connection is encrypted using the encryption key K.

VII. CONCLUSION

This paper presents an innovative VPN solution that combines the best technologies from the telecommunication world and the computing world to the benefits of the users and the service providers. By separating the authentication from the establishment of the VPN and delegating to a third party, which can the mobile operator or an identity provider, a user-friendly and secure VPN solution is achieved. The re-use of the SIM card and the GSM authentication adopted in the solution will relieve the user of the burden of carrying an extra device and remembering an additional PIN code at the same time as the cost for deployment and administration can be reduced dramatically thanks to the sharing of cost. A proof-of-concept prototype has been successfully implemented within the framework of the EUREKA Mobicome project. However, only GSM authentication has been implemented and the next step will be to implement the UMTS AKA authentication for the SIM-based VPN solution.

REFERENCES

[1] Harkins, D. & Carrel, D., RFC-2409: The Internet Key Exchange (IKE), IETF, Network Working Group, November 1998, online: http://www.ietf.org/rfc/rfc2409.txt

[2] Pereira, R. & Beaulieu, S., Extended Authentication within ISAKMP/Oakley (XAUTH), IETF, online: http://tools.ietf.org/id/draft-ietf-ipsec-isakmp-xauth-06.txt

[3] Samar, V. & Schemers, R., Unified Login with Pluggable Authentication Module (PAM), Open Software Foundation, October 1995, online: http://www.opengroup.org

[4] Kent, S. & Seo, K., RFC-4301: Security Architecture for the Internet Protocol, IETF, Network Working Group, December 2005, online: http://www.ietf.org/rfc/rfc4301.txt

[5] Phifer, L., Understanding IPSec identity and authentication options, SearchSecurity.com, June 2006, online: http://searchsecurity.techtarget.com

[6] Dierks, T. & Rescorla, E., The Transport Layer Security (TLS) Protocol Version 1.1, IETF, NetworkWorking Group, April 2006, online: http://www.ietf.org/rfc/rfc4346.txt

[7] Hills, R., Common VPN Security Flaws, NTA Monitor Ltd., January 2005, online: http://www.nta-monitor.com/posts/2005/01/VPN-Flaws-Whitepaper.pdf

[8] Do Van Thanh, Tore Jønvik, Do Van Thuan & Ivar Jørstad: Enhancing Internet service security using GSM SIM authentication, Proceedings of the IEEE Globecom 2006 conference – ISBN 1-4244-0357-X – San Francisco, USA, Nov 27 - Dec 1, 2006

[9] Ivar Jørstad, Do Van Thuan, Tore Jønvik and Do Van Thanh: Bridging CardSpace and Liberty Alliance with SIM authentication, Proceedings of the 10th International Conference on Intelligence in Next Generation Networks (ICIN 2007), published by ADERA – B.P 196 – 33608 PESSAC Cedex – France, Bordeaux , France, Oct 8-11, 2007

[10] International Organization for Standardization (ISO), ISO-7816-1/4

[11] 3GPP/ETSI, Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface (3GPP TS 11.11 version 8.14.0 Release 1999) TS 11.11

[12] Pliam, J., Authentication Vulnerabilities in IKE and XAuth with Weak Pre-Shared Secrets, online: http://www.vpnc.org/ietf-ipsec/99.ipsec/msg01451.html

[13] 4. Thumann, M. & Rey, E., PSK Cracking using IKE Aggressive Mode, online: http://www.ernw.de/download/pskattack.pdf