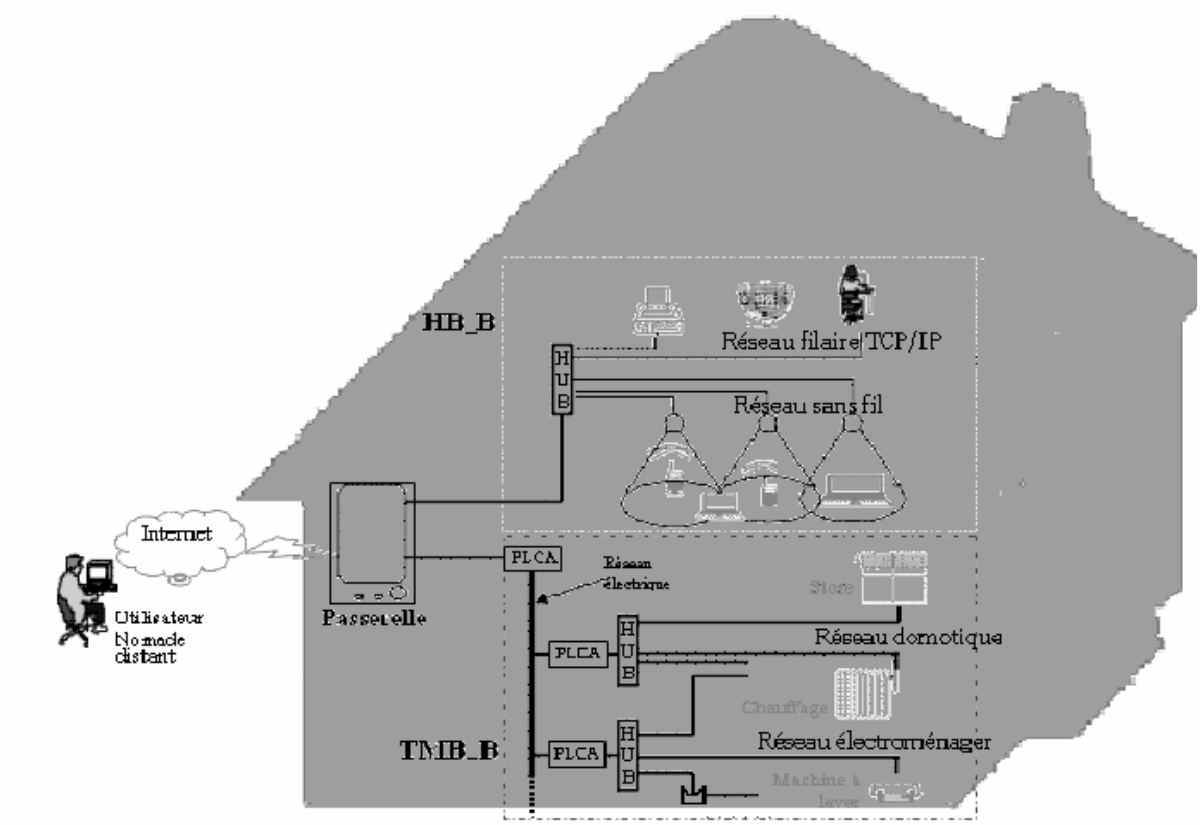
Intégration du protocole IPsec dans un réseau domestique pour sécuriser le bloc des sous-réseaux FAN



Ali Larab (ali.larab@etu.univ-tours.fr)
Pierre Gaucher (pierre.gaucher@univ-tours.fr)
Patrick Martineau (patrick.martineau@univ-tours.fr)
Laboratoire Informatique de L'Université de Tours. UPRES EA n° 2101
Département Informatique de Polytech'Tours
64 Avenue Jean Portalis, 37200, Tours, France.
Tél. :02 47 36 14 14

Sommaire

Liste des figures :

Liste des tableaux :

I Introduction

La domotique, ou l'automatisation des tâches domestiques, n'a connu d'essor qu'après l'avènement de l'ordinateur et de l'informatique au sein de l'habitat. Elle prend de plus en plus d'ampleur, surtout dans les pays développés [Produ_02]. L'utilisation croissante des PCs au sein des réseaux domestiques est due à l'attirance croissante des gens pour Internet et le multimédia. Aux USA, par exemple, qui est l'un des pays les plus avancés dans ce domaine, plus de 95% des maisons utilisent le câble, avec un taux de croissance régulier de 32% [MontP_03]. Actuellement, on ne parle plus de maison domotisée mais plutôt de maison connectée. Connecter son habitat à l'extérieur, en particulier à Internet, permet d'améliorer les services rendus par son réseau domestique, d'être en contact avec l'extérieur et d'être en contact avec l'intérieur quand on est à l'extérieur. Les communications entre les services internes de l'habitat et ses habitants quand ils sont à l'extérieur (utilisateurs nomades) s'accompagnent d'un fort besoin de sécurité. Dans ce document, nous nous intéressons à la sécurité du réseau domestique, en particulier à celle d'un de ses sous-réseaux appelé le sous-réseau FAN (Field Area Network). Nous décrirons, dans la section II, la structure du réseau domestique. Dans la section III, nous verrons pourquoi il faut sécuriser ce réseau et quels sont les services de sécurité qu'il faut offrir au sous-réseau FAN. La section IV est dédiée à la description du protocole de sécurité choisi pour sécuriser les communications domestiques. Les solutions proposées pour pallier les problèmes de sécurité que peut rencontrer le sous-réseau FAN sont présentées dans la section V. Nous terminons ce document par une conclusion et quelques perspectives.

II Réseau domestique

II.1 Définition

La domotique a pour objectif l'automatisation, au sein d'un habitat, de toute fonction ou tâche possible. Cette automatisation s'effectue en commandant par programmation certaines fonctions telles que la gestion de l'éclairage et de l'énergie électrique, la gestion du chauffage ou de la climatisation, la détection des fuites de gaz et d'eau, l'ouverture des portes, des fenêtres et des stores et la mise sous alarme de la maison. Un habitat domotisé est donc un habitat qui essaye de tirer le meilleur parti des nouvelles technologies afin d'améliorer le confort et le bien-être de ses résidents. Pour atteindre cet objectif, il est plus intéressant de relier par un réseau les différents actionneurs aux ordinateurs de gestion. Par exemple un détecteur de présence ou de fuite doit être relié à un actionneur lequel, à son tour, doit être relié au système de commande et de réglage des alarmes. Pour que la gestion de l'ensemble des services offerts par un habitat domotisé soit globale, pour que cet habitat offre le maximum de services, et afin d'augmenter la valeur du style de vie numérique (manipulation et échange de données numériques), les appareils domestiques doivent donc être reliés par un réseau. Ce réseau est appelé « **réseau domestique** » ou **HLN**, pour Home Local Network.

II.2 Structure

A cause de l'hétérogénéité des appareils utilisés dans l'habitat, le HLN (Home Local Network) peut être vu comme un ensemble de sous-réseaux utilisant des protocoles et des media différents. Sa structure actuelle n'est pas encore figée [MontP_03]. Parmi les éléments qui influent sur la structure de ce réseau, on trouve :

sur le module de sécurité ; il s'adaptera automatiquement puisqu'il est doté de la version IPsec qu'il faut (IPsec NAT-T).
Le module doit être configuré (création de 2 ou plusieurs SA) de façon à ce qu'il n'accepte de messages que d'un appareil (un autre module ou le serveur) dont il a connaissance. De même, il ne doit envoyer de messages qu'aux appareils avec lesquels il a le droit de communiquer. Tous les autres messages qu'il reçoit doivent être rejetés (Drop).

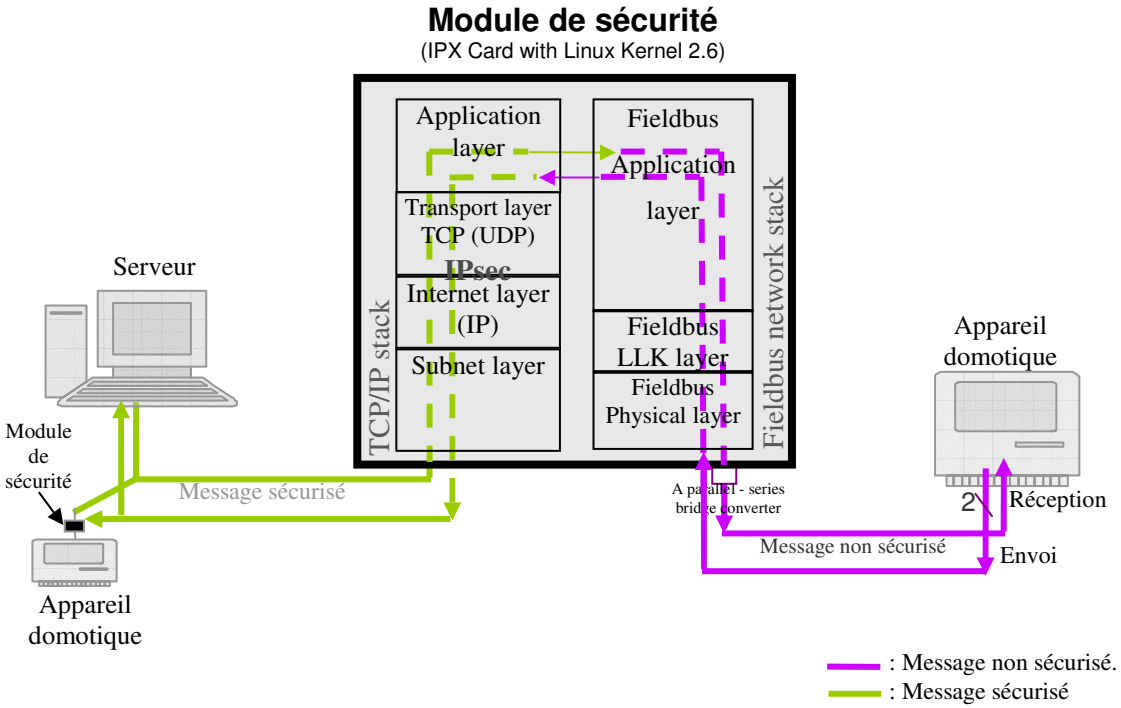


Figure 19 : Structure logique du module de sécurité IPsec.

VI Conclusion et perspectives

Dans ce rapport, nous avons donné la définition d'un réseau domestique ainsi que sa structure. On a montré pourquoi il est nécessaire de le relier à l'extérieur, en occurrence à Internet, et pourquoi il faut le sécuriser. Nous avons montré aussi qu'il n'est pas suffisant de sécuriser seulement la passerelle qui relie le réseau à l'extérieur mais il faut aussi sécuriser les autres sous-réseaux. Parmi les services de sécurité, nous avons montré que le service d'intégrité, le service d'authentification des utilisateurs et des machines ainsi que le service de confidentialité sont les services les plus intéressants dont a besoin le sous-réseau FAN (Field Area Network). Après étude des différents protocoles de sécurité existants, pour sécuriser le sous-réseau FAN, notre choix s'est porté sur IPsec (IP Security Protocol). Toute la section IV est dédiée à décrire ce protocole et son principe de fonctionnement. Ceci nous a aidé à comprendre quelles sont les configurations (modes, variantes, protocoles) qu'il faut choisir pour que IPsec s'adapte au sous-réseau domestique FAN et pour qu'il réponde à nos besoins de sécurité. A l'issu de cette étude, nous avons choisi de créer un module de sécurité qui

utilisera IPsec avec son mode transport AH et ESP pour sécuriser les communications au sein du sous réseau FAN. IPsec est utilisé aussi pour sécuriser les communications entre le serveur Web domestique et un utilisateur nomade externe. La solution proposée ici est une solution à base de modules. D'après [MontP_03] cette approche est favorisée pour ce genre de structure car elle aide à surmonter le problème de limitation d'appareils utilisés en domotique et pousse les limites de ces appareils. Utiliser un protocole basé sur IP pour sécuriser le sous-réseau FAN permet d'unifier le protocole d'échange de données entre les différents sous-réseaux domestiques. Ce qui permet de faciliter les échanges entre les différents sous-réseaux sans faire appel à une passerelle (pont ou routeur). IPsec, tel quel, ne peut pas répondre à tous nos besoins, nous avons rencontré certains problèmes avec son intégration dans le sous-réseau FAN, tels que la traversée du NAT et l'authentification des utilisateurs. Il nous a fallu alors proposer certaines solutions complémentaires pour améliorer les services rendus par IPsec. A la fin de cette section, nous avons donné la structure, logique, du module de sécurité qui sert à sécuriser les communications entre un appareil domotique et d'autres appareils domotiques ou entre un appareil domotique et la machine d'un utilisateur distant.
La solution que nous proposons dans ce rapport est dédiée au sous-réseau FAN. Elle s'adresse particulièrement aux appareils domotiques sédentaires tels que les appareils électroménagers (produits blancs). Mais elle peut être généralisée à tous les appareils qui n'utilisent pas le protocole TCP/IP et qui n'intègrent pas de fonctions de sécurité. Dans le cas où on généralise cette solution aux autres appareils ou aux autres sous-réseaux, on rencontre un autre problème : on ne peut pas doter tous ces appareils d'un module de sécurité car, il y en a beaucoup et surtout parce qu'ils utilisent des protocoles différents et propriétaires. Le problème dans ce cas est la cohabitation entre les appareils qui sont dotés d'un module de sécurité avec ceux qui ne le sont pas. La solution telle que nous la voyons actuellement est de faire du module de sécurité un appareil qui peut comprendre plusieurs formats de messages (protocoles TCP/IP, protocoles bus de terrains…). Il doit être capable de reconnaître et de faire la différence entre les messages qui sont sécurisés (utilisation d'IPsec) et ceux qui ne le sont pas (utilisation seulement d'un protocole bus de terrain). Ce module doit donc être capable de recevoir et de traiter des messages sécurisés mais aussi des messages simples venant d'appareils domestiques qui n'intègrent pas de fonctions de sécurité.

VII Bibliographie

Références des articles, livres et des RFC (Request For Comments)

[Doras_99] Naganand Doraswamy and Dan Harkins « IPsec: The New Security Standard for the Inter- net, Intranets, and Virtual Private Networks », Hardcover edition Prentice Hall PTR, 1999. ISBN: 013-011898-2.

[Kivin_04] T. Kivinen, A. Huttunen, B. Swander and V. « Volpe, Negotiation of NAT-Traversal in the IKE », IP Security Protocol Working Group, Internet-Draft SafeNet, 2004/02/10, http://mirrors.sec.informatik.tu-darmstadt.de/ftp.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-08.txt

[Larab_03] Ali Larab, Patrick Martineau, Pierre Gaucher. « Synthèse sur la sécurité des réseaux domotiques orientés Gestion Technique du Bâtiment », les nouvelles technologies dans la cité. Rennes, décembre 2003, pp 135-144.

[Larab_03_a] A. LARAB, J. LELOUP, P. GAUCHER, P. MARTINEAU, « Description des conséquences du développement des TIC dans l'habitat », Laboratoire

Informatique de l'Université de Tours, Rapport Interne n° 265x 45p, mars 2003.

[Mahal_03] N. P. Mahalik, « Fieldbus Technology: Industrial Network Standards for Real-Time Distributed Control », Springer-Verlag edition, September 2003. ISBN: 3540401830.

[MontP_03] Marie-José Montpetit, David Starobinski, « Small and home networks », Computer Networks, Elsevier Sciences, 2003, pp 1-5.

[Nikol_02] NIKOLOUTSOS E., PRAYATI A., KALOGEROS A., KAPSALIS V. and PAPADOPOULOS G., « Integrating IP Trafic into Fieldbus Networks », IEEE, 2002, pp 67-72.

[Ruixi_01] Ruixi Yuan, Timothy W. Strayer, « Virtual Private Networks: Technologies and Solutions", Addison-Wesley Professional, avril 2001, ISBN: 0201702096.

[Saute_02] Sauter T. and Schwaiger C., « Achievement of secure Internet access to fieldbus systems », Microprocessors and Microsystems, Volume 26, 10 Septembre 2002, pp 331-339

[Shea_99] Richard Shea, "L2TP: Implementation and Operation", The Addison-Wesley Networking Basics Series, Addison Wesley, September 1999. ISBN: 0-201-60448-5.

[Stass_02] Keith Strassberg, Gary Rollie, Richard Gondek « Firewalls: The Complete Reference », 2002, Edition: Paperback, ISBN: 0-07-2195673.

[White_03] Ollie Whitehouse, Security Advisory, Nokia 6210 DoS SMS Issue, 2003/02/25, http://www.atstake.com/research/advisories/2003/a022503-1.txt .

[Windo_02] Robert Cowart and Brian Knittel, « Microsoft Windows XP, édition professionnelle », Compus Press, 2002. ISBN: 2-7440-1349-8.

Références des RFC (Request For Comments)

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", 1995/10, http://www.ietf.org/rfc/rfc1847.txt

[RFC2341] A. Valencia, M. Littlewood, T. Kolar, "Cisco Layer Two Forwarding (Protocol) "L2F"", Cisco Systems, 1998/05, http://www.faqs.org/rfcs/rfc2341.html .

[RFC2401] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", 1998/11, http://www.faqs.org/rfcs/rfc2401.html .

[RFC2402] S. Kent, R. Atkinson, "IP Authentication Header", 1998/11, http://www.faqs.org/rfcs/rfc2402.html.

[RFC2406] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", 1998/11, http://www.faqs.org/rfcs/rfc2406.html .

[RFC2407] D. Piper, "RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP", Network Alchemy, 1998/11, http://www.faqs.org/rfcs/rfc2407.html

[RFC2408] D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", 1998/11, http://www.faqs.org/rfcs/rfc2408.html.

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter, « Layer Two Tunneling Protocol "L2TP" », 1999/08, http://www.faqs.org/rfcs/rfc2661.html .

[RFC3715] B. Aboba and W. Dixon, « IPsec-Network Address Translation (NAT) compatibility Requirements », 2004/03, http://asg.web.cmu.edu/rfc/rfc3715.html.

Références des Revues

[Bedin_02] François Bedin, « RPV : relier en mode privé les sites distants », revue '01Net' Décision Micro, août 2002.

[Echos_03] Les échos, « voyage au cœur de Microsoft, demain tous connectés partout », enquête du 05.02.2003, p46-47.

[Produ_02] Centre d'information du Ministère de l'économie des finances et de l'industrie, "L'industrie française des technologies de l'information et de la communication', Production industrielle (hors série), 2002, http://www.industrie.gouv.fr/sessi.

[Sagot_01] F.Sagot, C.Ferrero et E.Sorlet, "Comment rendre la maison communicante'', le Moniteur, 29 juin 2001. pp 56-60.

Autres références Web (sans RFC)

[ADAE_04] ADAE (Agence pour le Développement de l'Administration Electronique), « Réseau et Sécurité avec IPSEC », http://www.adae.gouv.fr/article.php3?id_article=110, Lien valide le: 10.09.2004

[Allie_97] Marc ALLIER, Olivier DEBAISIEUX, « Les réseaux locaux industriels (R.L.I.) », ENIC telecom (groupe des Ecoles de télécommunications), Université de Lille1, 1997/10, http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio1997/ResIndus/RliAd.htm , Lien valide le: 30.06.2004.

[Benefic] Microsoft, « Les bénéfices de Windows 2000 Server pour les entreprises », http://www.microsoft.com/france/windows/2000/server/decouvrez/benefices.asp, Lien valide le: 15.06.2004.

[Davis_02] Chris Davis and Aaron Higbee, DC. Phone Home, BlackHat Conference, 2002, http://www.blackhat.com/html/bh-usa-02/bh-usa-02-speakers.html#Davis Higbee, Lien valide le: 01.07.2004.

[Ghisl_00] Ghislaine Labouret, « IPSEC : Présentation technique », Hervé Schauer Consultants (HSC), http://www.hsc.fr/ , 16 juin 2000. Lien valide le: 20.06.2004.

[GuyMS_02] The Cable Guy of Microsoft, « IPsec NAT Traversal Overview », 08/2002, www. Lien valide le: 30.06.2004. http://www.microsoft.com/technet/community/columns/cableguy/cg0802.mspx .

[HelpWin] Help de Windows XP.

[L2TP] Site officiel de L2TP, http://www.L2tpd.org , Lien valide le:30.09.2004.

[MicroL2TP] « The Microsoft L2TP/IPsec VPN Client », http://infocenter.cramsession.com/articles/files/the-microsoft-l2tpIPsec-v-9172003-1414.asp?show_qod=yes&, Lien valide le: 20.06.2004.

[Montarn] Nicolas Montarnal, « Mise en place d'un réseau privé virtuel VPN sous protocole PPTP (PPTP et le tunneling) » http://www.minet.net/spip/IMG/txt/pptp-vpn.txt, Lien valide le: 15.06.2004.

[Secinfo] Sécurité info.com, « IPsec », http://www.securiteinfo.com/crypto/IPsec.shtml , Lien valide le: 15.06.2004.

[SET] "Secure Electronic Transaction: a market survey and a test implementation of SET technology", http://www.wolrath.com/set.html, Lien valide le: 30.09.2004.

[SSL] Site de SSL, http://www.ssl.com, Lien valide le: 30.09.2004.

VIII Annexe

VIII.1 Sigles et acronymes

AH	Authentication Header
DES	Data Encryption Standard
DoS	Denial of Service (Déni de Service)
ESP	Encapsulating Security Payload
HLN	Home Local Network
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security protocol
IPv4	IP version 4
IPv6	IP version 6
ISAKMP	Internet Security Association and Key Management Protocol
OSGI	Open Service Gateway Initiative
OSI	Open System Interconnection
RFC	Request For Comments
RSA	Algorithme de chiffrement de Rivest, Shamir, Adleman
SA	Security Association
SAD	Security Association Database
SHA1	Secure Hash Algorithm 1
SPD	Security Policy Database
SPI	Security Parameter Index
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
VPN	Virtual Private Network

Tableau 2 : Sigles et acronymes.