SÉCURITÉ SUR SONET/SDH

Cet article a été composé avec vim et fop.
JJ. Puig, thésard à l'INT.
Janvier 2002.

SOMMAIRE

INTRODUCTION

Peu d'informations sont disponibles au sujet de la sécurité sur SONET ou SDH; il est vrai que ce domaine est des plus spécifiques.

Cependant, au moins une fois l'an, la question est posée sur le forum comp.dcom.sdh-sonet [9]. La reconnaissance du problème est sans doute une étape indispensable à la constitution d'une solution de sécurité.

Cet article fera le point sur les avis et technologies de sécurité disponibles à l'heure actuelle pour SONET et SDH. Les sources d'informations traitant de ce sujet sur Internet sont rares, et certaines sont payantes; on a donc choisi, parmi les contributions gratuites, les plus significatives. Ces dernières apportent des réponses en terme de normes ou de recommandations à l'accès et à la confidentialité sur SONET et SDH. Des *datasheets* de produits donnent par ailleurs la réalité des faits par rapport à ces normes ou recommandations.

CONTRÔLE D'ACCÈS ET SÉCURITÉ D'ADMINISTRATION DES ÉQUIPEMENTS

Le *Network and Services Integration Forum* (NSIF [7]) émet des recommandations concernant le déploiement des technologies SONET et SDH; notamment en ce qui concerne l'intégration, l'interopérabilité et la mise en place de services. Plusieurs documents ont été émis par le NSIF, mais tous ne sont plus accessibles. Parmi les contributions ayant trait à la sécurité, on remarque trois documents [13], [14], [17].

COMMON APPLICATIONS REQUIREMENTS FOR SONET NE SECURITY SYSTEM

Les documents [13] et [14] ont été rédigés par le même auteur, en 1999 et en 2000 respectivement. La version de 1999 constitue le draft, tandis que celle de 2000 est un document approuvé par le forum. Substantiellement, le draft se propose d'établir une recommandation en vue de sécuriser les accès aux *Network Elements* (NE) de SONET. Un *NE* est en fait tout type d'équipement télécom qui fournit un support ou un service à l'utilisateur ([22]). Il présente le processus opératoire au moment de la rédaction et les besoins ressentis par les ISP afin d'administrer leur réseau. De là plusieurs solutions sont présentées, dont une seule est choisie et développée en détail.

Un problème de sécurité se posait au moment de la rédaction du draft : il fallait un couple (*login / password*) par NE. D'une part, cela handicapait les utilisateurs qui agissaient en différents points du réseau, puisqu'ils devaient retenir un mot de passe par NE, d'autre part, cela nécessitait de la part des NE de conserver chacun de nombreuses informations sur les utilisateurs (plusieurs centaines d'utilisateurs par NE), ce qui posait des problèmes de capacités des NE et surtout ne permettait pas d'administration centralisée de la sécurité.

Le draft identifie en conséquence un ensemble de besoins :

- Définir un système centralisé de sécurité
- Permettre la gestion des utilisateurs
- Permettre la gestion des droits des utilisateurs selon les ressources, les dates, les points d'entrées dans le réseau
- Permettre la traçabilité par utilisateur
- Distinguer la connexion distante, via un OS, de la connexion locale au NE, afin de mettre en place des mécanismes de sécurité adaptés à chacun de ces cas

Ces impératifs sont classiques dans de nombreux domaines, notamment les systèmes d'exploitation interconnectés en réseaux locaux; les solutions proposées par le draft sont d'ailleurs toutes aussi classiques.

Il semble exclu (pour l'auteur) de concevoir des "super-NE" capables de gérer de nombreux utilisateurs : même si cela est techniquement possible, le coût et la difficulté d'utilisation (réplication des données du système de sécurité centralisé) rendent ce choix inadapté.

De même, un simple système centralisé de gestion de mots de passe est trop limité (pas de vue d'ensemble sur la gestion des droits des utilisateurs).

Par conséquent, il convient d'établir un système centralisé de gestion des utilisateurs. Ce dernier devra, sur demande de la part des NE, analyser les requêtes de connexions aux NE et y accorder l'accès le cas échéant. Les fonctions de sécurité présentées sont :

- L'identification (unique, de 7 caractères et plus...)
- L'authentification (avec un chiffrement unidirectionnel du password, de 6 caractères et plus...)
- Contrôle d'accès au niveau système (sans *BACK-DOOR*)
- Contrôle d'accès au niveau ressource (avec profils de groupes dotés d'une granularité suffisante : utilisation, développement, support, maintenance, administration...)
- Outils d'administration de la sécurité
- Traçabilité (des utilisateurs, de l'activité système, des alarmes...)

Ces fonctions étaient celles présentées dans le document original (le draft). Le document final a vu l'ajout de nouvelles fonctions :

- Confidentialité des données gérées et stockées par le système
- Intégrité du système et des données (redondance, réplication, limitation des risques en cas d'intrusion)

Remarque: Notons que de telles fonctions ne peuvent être mises en place que si les NE actuels et les NE futurs sont susceptibles de les supporter.

Toutes ces fonctions sont particulièrement bien détaillées dans les deux documents (taille des champs login, password, les fonctions de hachage, durée de vie des informations...) aussi ne seront-elles pas plus développées ici. Il convient cependant de préciser que le cas des accès distants, par exemple via ISDN, wireless ou Internet, s'il est évoqué par endroits, n'a pas fait l'objet d'une analyse en profondeur. De plus, aucune description générale de l'architecture n'est effectuée.

Enfin, l'auteur du document traite aussi de deux autres points :

- La sûreté de fonctionnement : en énonçant la nécessité d'utiliser des protocoles assurant la détection et/ou la correction d'erreurs (ce qui n'est pas réellement une problématique de sécurité, même si cela peut l'affecter).
- La sécurité juridique : il propose d'afficher une licence d'utilisation lorsqu'une session est ouverte, pour prévenir contre les conséquences juridiques d'une utilisation délictueuse du système.

En guise de conclusion sur ce document, on peut, d'une part, souligner l'absence de précisions sur les protocoles à mettre en place. Ce document définit en profondeur les besoins, mais n'aborde en aucun cas les solutions. D'autre part, s'il présente des problématiques classiques, il en précise les détails relatifs à ce contexte particulier.

*** * ***

SECURITY REQUIREMENTS FOR OPERATIONS INTERFACES IN A MULTI-TECHNOLOGY NETWORK

Le document [17] se veut plus général que les précédents en présentant des besoins de sécurité pour différentes infrastructures de réseaux de télécommunication (notamment DWDM et SONET). Le fort développement de l'interconnexion de LAN privés aux réseaux d'opérateurs a rendu cette approche nécessaire. Les objectifs des opérateurs sont :

- Réduire les coûts d'administration
- Réduire les coûts d'infrastructure de sécurité
- Augmenter le niveau d'interopérabilité
- Accélérer le déploiement de solutions de sécurité

Afin de mieux cerner ces problématiques, le point de vue a été situé au niveau de la gestion de réseau d'opérateur, c'est-à-dire au niveau du *Telecommunication Management Network* (TMN). A l'intérieur du plan TMN, le NSIF s'est focalisé sur les accès f et q aux trois couches basses :

- *Network Element Layer* (NEL)
- *Element Management Layer* (EML)
- *Network Management Layer* (NML)

Remarque: pour rappel, q est le point de référence représentant les interfaces entre les blocs *Operations System Function* (OSF) et les *Network Elements* (NE) et f est le point de référence représentant les interfaces entre les blocs *Operations System Function* (OSF) et les *Workstation Function* (WSF).

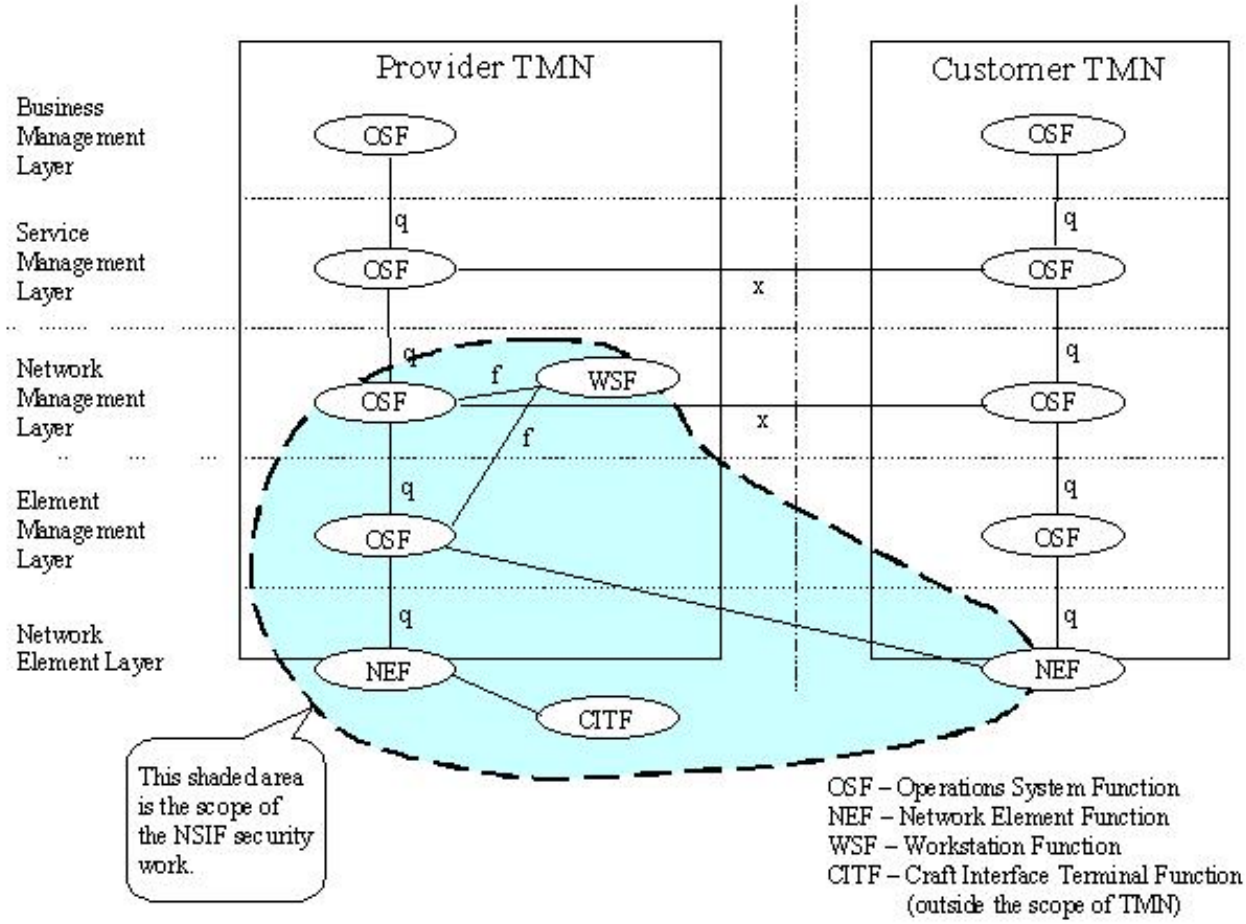


Figure extraite de [17] (Fig. 1).

Afin d'assurer les fonctions de sécurité désirées, le *Craft Interface Terminal Function* (CITF) est une fonction ajoutée à TMN. Pour déterminer les processus de sécurité à mettre en oeuvre au cours d'opérations d'interconnexion, le document présente les huits scénarii envisageables par un provider :

- 1. Service client au dessus d'un anneau métropolitain DWDM ou SONET géré par un provider
- 2. Location par un client de ressources d'un anneau métropolitain DWDM ou SONET géré par un provider
- 3. Accès local d'un *Craft Interface Terminal* (CIT) à un anneau DWDM ou SONET
- 4. Location par un client de ressources d'un anneau métropolitain DWDM ou SONET géré directement par le client
- 5. Location par un client de ressources d'un anneau métropolitain DWDM ou SONET géré indirectement par le client (via une interface X entre OSF provider et client)
- 6. Location par un client de ressources d'un anneau métropolitain DWDM ou SONET géré indirectement par le client via un accès à une *Workstation Function* du provider
- 7. *Network Elements* du client gérés indirectement par un provider via DCC/OSC (*Data Communications Channel/Optical Supervisory Channel* - voir ci-après)

· 8. *Network Elements* du client gérés par un accès du provider au travers de l'OSF

Tous ces scénarii n'entrent pas dans les prérogatives du NSIF, celui-ci se focalisant sur les trois couches basses de TMN. Notamment, les cinquième et sixième scénarii sont hors sujet, et le quatrième scénario est interdit (pour des raisons évidentes de sécurité). Enfin, le septième scénario est déconseillé (les protocoles DCC/OSC ne sont pas sûrs).

En terme de fonctions de sécurité, les besoins sont l'**identification**, l'**authentification** mutuelle et l'**intégrité**. L'**autorisation**, qui se fait généralement par le biais d'*Access Control List* (ACL), n'entre pas dans les attributions du document, au même titre que l'**audit** et les **alarmes**. La **confidentialité** et la **non-répudiation** y sont définies comme optionelles, car elles ne devraient pas être nécessaires pour les types d'interfaces étudiées. D'ailleurs le document n'en parle pas non plus.

Tout ce qui précède a permi d'établir un ensemble de contraintes, de scénarii; bref, de reconnaître des besoins. Il convient de faire des choix pour la mise en oeuvre, au niveau du système de clefs et de certificats, au niveau du protocole entre les interfaces, et au niveau applicatif.

Pour la gestion des clefs et des certificats, la recommandation est l'infrastructure à clefs publiques (PKI), donc avec une autorité de certification et des autorités d'enregistrement (RA) qui vérifient l'identité des destinataires des certificats. Tout cela est détaillé de façon claire avec un schéma dans le document [17], et s'appuie sur des recommandations de l'ANSI concernant l'utilisation de PKI dans le contexte des réseaux télécoms, et notamment avec TMN ([18], [19]).

La couche de sécurité suggérée par le document [17] pour le protocole entre interfaces (gestion du réseau) est SSLv3 (obligatoire) ou TLSv1 [21] (optionnel). SSLv3 répond aux trois besoins de fonctions de sécurité mentionnées ci-dessus : **Identification**, **authentification** et **intégrité**. Le hash recommandé pour l'intégrité est SHA-1. SSLv3 est alors requis sur tout OS ou NE disposant d'une pile TCP/IP pour l'administration. Les suites cryptographiques suivantes pour SSL devront être supportées :

· SSL_RSA_WITH_NULL_SHA

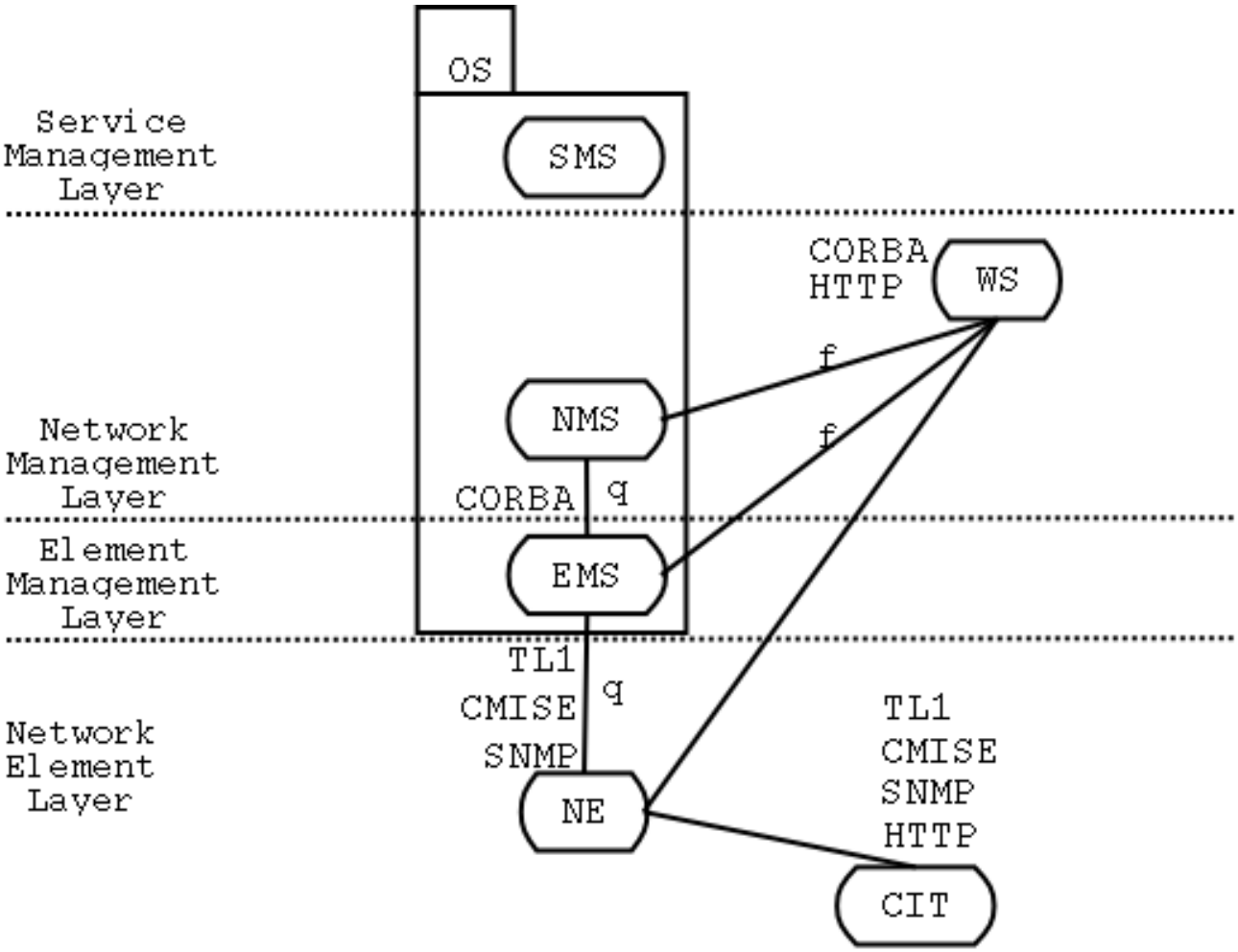
· SSL_RSA_WITH_DES_CBC_SHA

Remarque: Le document [20], en cours de rédaction, fait le point sur les services et méthodes de sécurité utilisés pour TMN.

Le choix de SSLv3 est cohérent dans la mesure où une pile TCP/IP est disponible. Cependant, d'une part ce prédicat n'est pas toujours vrai; d'autre part l'implantation de SSLv3 n'est pas forcément évidente au cas par cas. Pour ces deux raisons, des solutions alternatives sont présentées (avec des références vers les recommandations correspondantes) pour les interfaces WSF/NEF, OSF/NEF utilisées avec le protocole TL1, pour les interfaces q utilisées avec le protocole CMIP, mais aussi pour CORBA, SNMP, HTTP et FTP lorsque SSLv3 et TLS ne sont pas supportés ou en phase transitoire (en attendant une définition/implémentation de SSLv3 pour le contexte).

Au niveau applicatif, les protocoles de gestion sont ceux déjà cités ci-dessus :

- *Transaction Language 1* (TL1)
- *Common Management Information Protocol* (CMIP)
- *File Transfer, Access and Management* (FTAM)
- *Common Object Request Broker Architecture* (CORBA)
- *Simple Network Management Protocol* (SNMP)
- *Hypertext Transport Protocol* (HTTP)
- *File Transfer Protocol* (FTP)



Puisque ces protocoles ont pour but la gestion du réseau et s'appuient sur d'autres protocoles (SSL, TLS...) pour obtenir une couche de sécurité, on n'en parlera pas plus ici.

En conclusion, ce document pose de façon claire une démarche pour décrire une infrastructure de sécurité sur un réseau opérateur, en prenant fortement en considération l'aspect inévitable de l'interopérabilité avec les réseaux clients. Un fait est cependant surprenant: la confidentialité est d'emblée rejetée dans l'analyse, alors même qu'elle pourrait être proposée de façon optionnelle. Ce service peut en effet s'avérer nécessaire dans des circonstances qui n'ont pas été envisagées par le document. C'est d'autant plus troublant que les piles SSL ou TLS existantes proposent déjà de tels services, via les

algorithmes DES et 3DES.

*** * ***

Les documents du NSIF apportent des réponses (souvent incomplètes) en terme de sécurité du point de vue du provider. Gageons que cet effort continuera à l'avenir pour aboutir à des recommandations plus complètes.

PROTECTION CRYPTOGRAPHIQUE DES LIENS

Nous avons vu que plusieurs solutions existaient pour sécuriser les accès (administratifs et utilisateurs) aux niveau des NE. Cependant, la sécurité des liens a été mise de côté. Afin de protéger les données qui transitent sur ces liens, il convient d'utiliser des méthodes cryptographiques, notamment de chiffrer, mais aussi de garantir l'intégrité. Deux difficultés se présentent alors :

- La vitesse de chiffrement
- Les problèmes de synchronisation

Les constructeurs doivent donc faire face à ces deux contraintes. Aussi les *datasheets* des équipements comporte-t'elles des précisions importantes concernant les débits et les latences de fonctionnement sur différents types d'interfaces ([24]).

S'il existe quelques produits commerciaux et une certaine recherche en la matière ([23], [27]), il ne semble cependant pas y avoir de consensus quand aux protocoles utilisés, ce qui pourrait compromettre l'interopérabilité entre deux réseaux appartenant à des entités qui se fourniraient chez des constructeurs différents. Par ailleurs, il n'y a actuellement qu'un constructeur sur le marché, ce qui tue le débat.

Cet unique constructeur, Motorola, a choisi des méthodes cryptographiques recommandées par la NSA. Il est d'ailleurs tout a fait plausible que la NSA soit le client principal de Motorola pour cette branche d'activité :

- *Electronic Key Management System* (EKMS) est un protocole d'échange de clefs.
- FIREFLY est un algorithme à clef publique qui permet d'établir les clefs de sessions.

Remarque: Le chiffreur effectue un raffraichissement périodique des clefs. Il est possible de définir manuellement les clefs.

Ces chiffreurs ont été développés en coopération avec Northen Telecom (Nortel). Ces appareils ont été adoptés par la NSA ([28]):

- *SONET OC-3 (155 Mbps) KG-189 HW encryption using TYPE I*
- *SONET OC-12 (622 Mbps) KG-189 HW encryption using TYPE I*

Remarque: TYPE I signifie que tout traffic sortant de l'équipement sera chiffré. Les données en clair sont totalement interdites.

Les informations relatives à ces produits datent du 2 Avril 1998. Des versions supérieures (OC-48, ie 2,488 Gbps) de ces équipements étaient annoncées dès 1998, mais aucune information à ce sujet n'a été diffusée depuis 28 Juin 2001.

PROBLÈMES DE SÉCURITÉ CONNUS

PPP AU DESSUS DE SONET/SDH

En 1994, le groupe de travail PPP de l'IETF a édité un RFC concernant l'encapsulation des trames PPP dans les trames SONET ou SDH [25]. La section *Security Considerations* portait la mention : *Security issues are not discussed in this memo*.

Par ailleurs la section 2 - *Physical Layer Requirements* - précise : *"No scrambling is needed during insertion into the SPE"*. C'est-à-dire qu'un brouillage n'est pas nécessaire avant l'insertion de la trame PPP dans le *Synchronous Payload Enveloppe* (SPE), c'est-à-dire le containeur de données des trames SDH ou SONET, alors que cette opération était effectuée pour l'ATM. Ce point constitue la raison pour laquelle ce RFC a été revu et corrigé par [26].

Le RFC 2615 [26] explique l'origine du problème dans sa section *Security Considerations* : *RFC 1619 was operationally found to permit malicious users to generate packets with bit patterns that could create SONET/SDH-layer low-transition-density synchronization problems, emulation of the SDH set-reset scrambler pattern, and replication of the STM-N frame alignment word* . Autrement dit, l'absence de brouillage permettait d'injecter des trames pouvant causer des pertes d'alignement, de synchronisation ou leurrer des équipements.

En réalité, ces risques sont inhérents à la technologie *Packet Over Sonet* (POS) (voir p.619-620 [2]). Les équipements SONET/SDH doivent travailler de façon synchrone. Aussi, quand un problème survient, ces équipements essaient de rétablir d'eux-mêmes la synchronisation (on dit qu'ils sont "autoreconfigurables"). Pour cela, ils effectuent une analyse du signal sur le lien pour repérer des motifs de synchronisation (il existe à l'heure actuelle plusieurs manières de coder ces motifs). Si les données utilisateurs répètent ces motifs, cela peut faire échouer la reconfiguration.

Ce problème a été résolu par un brouillage des trames PPP avant leur insertion dans le SPE SDH ou SONET. Comme le brouillage se fait en mode chaîné et que le vecteur d'initialisation (sur 43 bits) contient des données qui ne sont pas facilement prévisibles par un attaquant, la probabilité de réussite d'une telle attaque est fortement réduite (à 9e-16 d'après le RFC). De plus, indépendamment de toute considération sur les vélléités de malveillances des utilisateurs, ce brouillage facilite une dispersion statistique des valeurs des bits, ce qui diminue les risques d'erreurs.

Le brouilleur proposé utilise en fait exactement le même algorithme que pour ATM over SONET/SDH. La conclusion de ces considérations est qu'un brouillage doit être systématique. Le principe des couches permet d'interdire à l'utilisateur la connaissance de la façon suivant laquelle ses données transitent dans le réseau, chaque couche se comportant à la manière d'une "boîte noire". L'utilisation d'un brouillage à l'intérieur d'une

couche permet de renforcer l'opacité du traitement à l'intérieur de cette boîte, ce qui complique les attaques basées sur ce traitement depuis les couches supérieures.

Un autre problème de sécurité est évoqué dans ce RFC : la présence de *flags* ou de séquences d'échappements dans les données transmises permettent de réduire la bande passante (cela double la bande passante nécessaire pour transmettre un même volume de données). Un protocole synchrone est relativement fragile face à l'insertion massive de ce genre de *flags* ou de séquences. De telles fonctionnalités doivent en effet exister pour garantir la synchronisation dans certains cas, par exemple quand le buffer d'arrivée des données sur l'interface est vide (*buffer under-run*), il faut signaler que le reste des données sera disponible dans un prochain conteneur. Par conséquent, on ne peut qu'essayer de limiter les effets d'une attaque par caractères d'échappement. D'ailleurs les conséquences n'en sont pas nécessairement très graves pour le réseau.

*** * ***

CONSIDÉRATIONS TECHNIQUES SUR UNE ATTAQUE PHYSIQUE EN COEUR DE RÉSEAU

Une attaque physique en coeur de réseau SDH ou SONET peut être menée à trois niveaux :

- Sur les noeuds : switchs et terminaux
- Sur les liens électriques
- Sur les liens optiques

Concernant les noeuds, les risques sont : les *backdoors*, un contrôle d'accès défaillant, les attaques par *buffer overflow* ou *stack overflow*... Ces attaques relèvent de la sécurité des systèmes d'exploitation et des programmes et non de la sécurité des protocoles.

Concernant les liens électriques, il convient de rappeler que SONET, comme son nom ne l'indique pas, est aussi utilisé sur des câbles électriques (type coax CATV 75 ohms pour être plus précis). Par conséquent, une connexion sur un tel lien avec un T d'adaptation d'impédance permet l'espionnage et les attaques actives. Une parade est de vérifier que l'impédance du lien n'enregistre pas de variations suspectes et que l'atténuation du signal le long du lien reste relativement constante. De telles vérifications permettent aussi d'anticiper des défaillances matérielles.

Concernant les liens optiques, une connexion nécessite un appareil volumineux, cher et rare, et aucun actuellement ne permet de faire des attaques actives. Ils récupèrent et amplifient l'énergie des ondes evanescentes qui traversent la gaine de la fibre afin de permettre l'espionnage. Les organisations pouvant disposer d'un tel matériel ont normalement des moyens plus simples pour parvenir à leurs objectifs. Par ailleurs, les répéteurs sur les fibres sont des points relativement vulnérables.

*** * ***

CONCLUSION

Nous avons pu voir au cours de cet article les différentes techniques qui, à l'heure actuelle, peuvent sécuriser l'utilisation de SONET/SDH; ces techniques sont principalement le contrôle d'accès et le chiffrement, des solutions classiques. Contre les attaques de format par l'insertion de données spécifiquement construites, le brouillage s'avère être une excellente technique, au moins sur le plan théorique.

Cependant, SONET et SDH n'en restent pas moins sensibles à quelques utilisations biaisées, comme l'insertion de séquences d'échappement. A priori, ces limites ne constituent pas réellement des problèmes de sécurité majeurs : elles ne peuvent causer de dénis de service sur le réseau, et la dégradation de la prestation ne devrait pas être significative (cela dépend, en réalité, du type de connexion dont dispose l'attaquant).

En conclusion de cette étude, on peut affirmer qu'utiliser SDH et SONET en toute sécurité est réaliste, la complexité des attaques à mettre en oeuvre étant très élevée.

ANNEXE A - DISCUSSION SUR LE DEVENIR DE SONET/SDH

Le 22 Décembre 2000 s'est tenue sur le groupe comp.dcom.sdh-sonet [9] une discussion ayant pour sujet *SONET/SDH Becoming Obsolete?*. Certains messages dans cette discussion touchent à la sécurité; ces derniers sont retranscrits ici.

FROM : BEYERM @MY-DEJA.COM

Question: Will SONET/SDH become obsolete in the near future? With technologies like IP over DWDM and Gigabit Ethernet becoming more widely deployed is an interoperable standard like SONET/SDH really necessary? If SONET/SDH is on the way out, when will this happen?

I'm looking for some views on this subject for publication, so any help you can give will be appreciated

* * *

FROM : "CONDUCTOR " <RIGHT @THE.BUS.STOP.COM>

I think in the short to medium term SONET/SDH will survive but I can see now some providers moving away from SDH toward Lambda net for ATM switches etc. which of-course still utilise SDH/SONET interfaces. The SDH network is less complex, simpler to fault diagnose, administer and easily re-routable, ***I also believe some customers prefer the additional layered security (leased STM-N) inherent in SDH.*** *We will continue to use switched voice/fax calls and RAS connexions and it will take many years for IP based solutions to eliminate this need, we can look at FDM here in the UK where some customers (very few) still have Megastream over FDM basically as they state it is working and never failed so don't fix it.*

My guess is SDH will be around for the next 10 years and then begin to decline with an increase in purely IP solutions (or whatever comes next). This is how I feel but would be interested in other peoples theories.

* * *

FROM : "BYRAUTOR " <BYRAUTOR @WANADOO .FR>

In what is going to follow Sonet and SDH are considered identical. The debate general by present door on the opposition that between the transmissions by circuits (establish) as SDH and the transmissions by datagram, independent and isolated packets. ONE

perceives, with MPLS in Internet, that the rebirth of virtual circuits as in X25, ATM, relay of plot and SDH and SONET is under way.

For my part ([5]) I am partisan of the SDH model, independent and that himself support on a technology rather cabled that software; ***in SDH it is the position of the bit in relation to a scorer of plot (framing bytes in Sonet, bytes A1, A2 in SDH G.707 ITU) that indicates its function; there is not to analyze the value of a byte or a set of bytes;*** *this technology should be always the fastest.*

Sonet and SDH have again of beautiful days before them; for several reasons:

- *1) first the quantity of SDH facilities installed and the quantity of facilities to install again requires an interview and a constant management therefore a lot of work for a lot of people and for a long time because when its functions there is anything to make that to supervise; there are a lot of SDH facilities that get settled again, by Alcatel exemple installs in That land 10 000 km of optic fibers with SDH facilities.*
- *2)* ***SDH and Sonets are very definite, very robust products and that possess devices of very sure auto-repair; so an user of SDH is assured of a guarantee to 99,99% of availability*** *(less than one hour per year of service stop; NDLA: voir [24] à ce sujet); all big enterprises use some SDH channels in their important links and secured.*
- *3) it is necessary to remember that the SDH is a transparent technology to the protocols that it transports;* ***completely independent of the elated data****; it can transport all sets of bits provided (on condition) that the clocks are: or in foreseen tolerances; or taken on the SDH equipment (as provides the 114 in V24 or the DB binds 15 in RS 232 or the ST. in RS 449: (clock modem pprovide to the issuing terminal).*
- ***4) it is necessary to know that SDH doesn't possess orders of sorting and mailing (routage, routers) it resists the piracy (hackers) thus perfectly because to spy on a lign off SDH it is necessary to work also on the network of surveillance (monitoring) that is a different network. The boredom, for the user (and the supplier) it is that 2 interfaces and 2 different protocols are necessary; one of connexion demand generally owner and the other of very very definite transportation. I think that all protocol of transportation that also transports the information of sorting and mailing (routage , routers) (among others) is a fragile protocol; one sees the complexity that arrives in the devices of cryptages that it is necessary to use now to protect its data in Internet; with SDH channels it is not useful.***
- *5) the WDM, the DWDM and SWDM are a supplementary layer that widens the possibilities of the SDH considerably; one can, or one will be able to, to make pass some packets directly on these optic channels but it will be necessary, of a manner or the other to take the devices of signaling of the SDH to achieve all functions of surveillance necessary to the knowledge of the transportation qualities and to the setting in service of the emergency devices. It is besides in progress to the ITU (Geneva) but when one will want smaller channels (2,048 Mb/ses for example, one will come back in SDH).*

SDH assures a transmission regularity without equal, if you send 4 x STM-1 with each 63 VC-12 of 2,048 Mb/s each (of any protocol) you will have, in receipt 4 x 63 = 252

streams of data that will be presented very simultaneously; each with its own clock of (emission) broadcast; every clock of emission (broadcas)t will fully be restored.

The SDH is a little as what is a motor diesel in relation to a motor to gas; difficult to construct but very robust. The problem with the other protocols it is that there is interference between the protocol and its transmission; one says that the SDH, as the WDM is transparent.

The worse disadvantage of the SDH is its need to work in double sense (direction) on every channel; so if the data only pass in a sense (direction) , the other sense is vacant; it cannot be lent to another user, alas. Some societies prepare a solution to this defect, as the Dynarc society to http://www.dynarc.se /. I could tell of it to you more but I would need more of time to translate because I write in French. Are not angry at me if you find difficulties of reading.

*** * ***

SDH et SONET sont donc plutôt sécurisés, d'un point de vue intrinsèque, puisque les données et les informations concernant leur acheminement sont gérées par des réseaux logiques différents. Une attaque active de type *man in the middle* ou même *spoofing* nécessite d'agir sur les deux réseaux, à des débits qui peuvent être très importants, et de façon synchrone !

Cependant, cette séparation données / informations de routage rend le système plus complexe, et notamment plus sensible à tout un ensemble d'incidents, par exemple la perte de synchronisation. Il résulte de cette considération que des attaques ayant pour cible le réseau et non ses extrèmités peuvent être menées: dégradation du service ou carrément *denial of service*. Il convient alors de faire en sorte que les interfaces entre sdh et d'autres technologies soient suffisamment rigides pour empêcher les abus. Cela n'est pas toujours évident, comme l'a montré l'évolution du RFC 1619 [25].

RÉFÉRENCES :

1 INTERCARRIER INTERFACE RECOMMENDATIONS
Date: Juin 1998
Status: SIF Approved Document SIF-010-1998
Auteur: Cypryan (Kip) T. Klish, II
Organisation: ATIS-NSIF
Ce document définit les problématiques d'implémentation pour les interfaces entre providers ou entre provider et client.

2 LES RÉSEAUX
Date: 3 Mars 2000
Status: Livre
Auteur: Guy Pujolle
Editeur: Eyrolles
Référence française sur les technologies réseaux. Le chapitre 22 traite plus particulièrement de SDH et de SONET.

3 SONET HOME PAGE
Status: Site Web
Organisation: sonet.com
Ensemble de liens sur la technologie SONET.

4 UNDERSTANDING SONET/SDH STANDARDS AND APPLICATIONS
Date: Décembre 1995
Status: Livre
Auteur: Ming-Chwan Chow

5 THE NETWORKS SYNCHRONOUS EXTENDED PDH AND SDH
Status: Livre
Auteur: G. Bouyer
Editeur: HERMES
Un livre sur SDH d'un auteur français. Notons que l'auteur est intervenu dans des discussions concernant la sécurité sur comp.dcom.sdh-sonet.

6 SONET
Date: 1 Juillet 2000
Status: Livre
Auteur: Walter J. Goralski
Editeur: McGRAW-HILL

7 NETWORK AND SERVICES INTEGRATION FORUM
Status: Organisation
Organisation: ATIS
Responsable: Catrina Akers
Le NSIF est un groupe industriel qui a été mis en place afin de définir et de résoudre les problématiques d'implémentation sur SONET.

8 NSIF REFERENCE ARCHITECTURE
Date: 2 Mai 2000
Status: NSIF Approved Document NSIF-GN-0003-015-R1
Auteur: Andy Walsh
Organisation: ATIS-NSIF
Ce document décrit le vocabulaire, les concepts et les architectures de référence sur lesquels se basent les travaux du NSIF.

9 COMP.DCOM.SDH-SONET
Status: Groupe de discussion
Organisation: Usenet
Groupe de discussion sur les technologies SDH et SONET.

10 SHEDDING LIGHT ON SONET
Date: 20 Mars 2000
Status: Article
Auteur: Darrin Woods
Cet article présente l'état de l'art sur SONET et SDH. La question de la sécurité n'y est cependant pas abordée.

11 SONET: COMMON GENERIC CRITERIA
Date: Decembre 1997
Status: GR-253-CORE
Organisation: Bellcore
Ce document définit des critères de tests sur les implémentations SDH/SONET.

12 NSIF SECURITY
Status: Organisation
Organisation: ATIS-NSIF
Responsable: Catrina Akers
Ce groupe définit les besoins des architectures de sécurité, des interfaces et de gestion de la sécurité qui permettent d'améliorer la sécurité des opérations sur un réseau et qui demeurent consistantes dans un réseau hétérogène.

13 COMMON APPLICATIONS REQUIREMENTS FOR SONET NE SECURITY SYSTEM
Date: 9 Novembre 1999
Status: Draft NSIF-CA-9910-110
Auteur: Ron Roman
Organisation: ATIS-NSIF-NSIF Security

14 COMMON APPLICATIONS REQUIREMENTS FOR SONET NE SECURITY SYSTEM
Date: 13 Avril 2000
Status: NSIF Approved Document NSIF-037-2000
Auteur: Ron Roman
Organisation: ATIS-NSIF-NSIF Security
Ce document, approuvé par le NSIF, identifie les besoins pour un serveur de sécurité et spécifie les besoins pour la gestion des utilisateurs d'un tel serveur; un futur document du NSIF décrira une solution pour l'implémentation de ce serveur.

15 GENERIC REQUIREMENTS FOR NETWORK ELEMENT /NETWORK SYSTEM (NE/NS) SECURITY
Date: Novembre 1997
Status: GR-815-CORE
Organisation: Bellcore
Ce document définit les besoins de sécurité des NE et NS.

16 SONET: COMMON GENERIC CRITERIA
Date: Decembre 1997
Status: GR-253-CORE
Organisation: Bellcore
Ce document définit des critères de tests sur les implémentations SDH/SONET.

17 SECURITY REQUIREMENTS FOR OPERATIONS INTERFACES IN A MULTI-TECHNOLOGY NETWORK
Date: 23 Août 2001
Status: NSIF Approved Document NSIF-040-2001
Auteur: Connie Hunt
Organisation: ATIS-NSIF-NSIF Security
Ce document décrit les procédures de sécurité qu'il convient de mettre en place par un

provider de réseau télécom. Différents cas sont analysés, certains trouvent une solution, d'autres sont rejetés, et les restants contituent des situations déconseillées.

18 TMN PKI - Digital Certificates and Certificate Revocation List Profiles
Date: 2000
Status: Document ANSI T1.268 - 2000
Organisation: ANSI
Ce standard décrit l'interopérabilité des éléments TMN avec l'infrastructure à clefs publiques en vue de supporter des fonctions de sécurité.

19 PKI Practices and Policy Framework
Date: 2000
Status: Document ANSI X9.79 - 2000
Organisation: ANSI
Ce document définit les composants d'une infrastructure à clefs publiques et établit son cadre d'utilisation et ses besoins en terme de politiques de sécurité.

20 Security Services and Algorithms for TMN
Date: 2000
Status: Draft T1M1.5/2000-154
Organisation: ANSI
Ce draft permet de référencer les services de sécurité, les algorithmes et leur cadre d'application pour TMN.

21 The TLS Protocol - Version 1.0
Date: Janvier 1999
Status: Request for Comments: 2246
Auteur: T. Dierks, C. Allen
Organisation: IETF-TLS
Responsable: Win Treese
Ce rfc décrit le protocole TLS.

22 network element (NE)
Date: Août 1996
Status: Glossaire Télécom
Organisation: Institute of Telecommunications Sciences
Ce site donne les définitions des différents acronymes et termes liés à TMN.

23 Systèmes de chiffrement pour SDH/SONET
Status: Laboratoire
Organisation: Institute for Data Communications Systems
Responsable: Oliver Jung
Cet institut développe des chiffreurs pour SDH/SONET, à des débits de 155 Mbit/s et 622 Mbit/s. La vitesse de chiffrement et l'aptitude à se synchroniser d'un tel équipement étant primordiales, une attention particulière est apportée sur la conception et la production de nouveaux processus opératoires de chiffrement.

24 KG-189
Status: Produit
Organisation: Motorola
Il s'agit "du" chiffreur SONET, adopté par la NSA.

25 PPP over SONET/SDH
Date: Mai 1994
Status: Request for Comments: 1619
Auteur: W. Simpson
Organisation: IETF-PPP Working Group
Responsable: Russ Hobby, Drew Perkins
Ce RFC décrit l'encapsulation de PPP dans SDH ou SONET.

26 PPP over SONET/SDH

Date: Juin 1999
Status: Request for Comments: 2615
Auteur: A.Malis, W. Simpson
Organisation: IETF-PPP Working Group
Responsable: Russ Hobby, Drew Perkins
Ce RFC décrit l'encapsulation de PPP dans SDH ou SONET. Il rend obsolete le RFC 1619 pour des raisons de sécurité.

27 XILINX, PMC TEAM ON 10-GBIT/S PACKET-OVER-SONET
Date: Mars 2001
Status: Article
Auteur: Anthony Cataldo
Organisation: EETimes
Cet article présente des FPGA produits par Xilinx, lesquels peuvent être utilisés pour du chiffrement sur SONET (voir fin de l'article).

28 THE FUTURE OF NETWORKING -- CAN SECURITY KEEP UP ?
Date: 1999
Status: Notes
Organisation: National Security Agency (NSA)
Responsable: Jeff Ingle
Notes d'orientations des travaux de la NSA sur la sécurité des réseaux.
