SECURITE DES INFORMATIONS

DANS LES COMMUNICATIONS VIA SATELLITE

Bruno VO VAN,

Mise à jour : Juin 2006

SOMMAIRE

1 PREAMBULE

La facilité de recevoir des signaux satellite en tout endroit et sur une couverture qui peut être intercontinentale donne une image vulnérable quant' à la sécurité des informations transmises.

Beaucoup d'opérateurs historiques ont entretenu ces craintes. Les réseaux d'entreprises utilisant comme vecteur principal un satellite ne tiennent pas compte des frontières. Ils étaient alors considérés comme un levier à une dérégulation rapide du marché des télécommunications.
Durant la période de dérégulation (1999-2002) de ce marché des télécommunications, la longueur de fibres optiques posées augmentait sur une vitesse journalière à plus de deux fois la vitesse du son pendant trois années. C'était un investissement considéré assez important pour mentir par omission.

L'utilisateur potentiel comprenait, de façon erronée, qu'une meilleure protection existerait sur un réseau terrestre mondial en fibre optique.

Une des conclusions était de prétendre que seul un chiffrage, de plus haut niveau, des communications au niveau du transport mais aussi des contenus des données pouvait assurer un parfaite invulnérabilité à des intrusions illégales.

Ce document montre que les technologies utilisées en liaisons satellite, et en particulier celles d'accès multiple au segment spatial, sont très fermées à toute intrusion. Elles sont souvent le choix privilégié de réseaux militaires car elles peuvent constituer un réseau parfaitement indépendant de tout accès et d'un accès technologique extrêmement difficile.
Les progrès en matière de communications numériques par voie hertzienne et des techniques d'optimisation de l'usage des segments spatiaux donnent une multitude de protocoles d'accès multiple. Les intrusions ne peuvent pas utiliser des méthodes génériques qui définiraient à notre avis un constat de faiblesse en matière de sécurité des données.

Il décrit la technologie choisie par LCDC SA dans ses offres d'intégration de réseaux satellite d'entreprises.

2 ABBREVIATIONS

ATU	: Automatic Tuning Unit (Unité d'adaptation d'antenne)
BER	: Bit Error Rate (taux d'erreur d'une liaison)
BURST	: Implusion de transmission d'une station dans une trame TDMA
CENELEC	: European Committee for Electro Technical Standardisation
CIR	: Committed Information Rate
FM	: Frequency Modulation
FRAD	: Frame Relay Access Device
IEEE	: Institute of Electrical and Electronics Engineers
ITU	: International Telecommunication Union
kbps	: Kilo bits per second
kHz	: Kilo Hertz
KSA	: Kingdom of Saudi Arabia
LAN	: Local Area Network
MHz	: Mega Hertz
NMS	: Network Management System
PC	: Personal Computer
RTT	: Round Trip Time

RX : Receive
SCADA : Supervisory Control And Data Acquisition
SES : Satellite Earth Station
TDMA : Time Division Multiple Access
TX : Transmit
UHF : Ultra High Frequency
VHF : Very High Frequency
VSAT : Very Small Aperture Terminal

3 PROTOCOLE D'ACCES MULTIPLE AU SEGMENT SPATIAL.

Chaque constructeur propose alors un équipement orienté selon son analyse marketing. Le modem qu'il proposera sera développé selon des fonctionnalités qu'il aura jugées le plus opportunes pour répondre aux segments du marché choisis.

En favorisant, par exemple, une dépendance du client vis-à-vis des opérateurs de Téléport : gestion centralisée, réseau étoilé, intelligence centralisée,... En proposant un prix de terminal le plus bas possible pour l'utilisateur et un hub très couteux au niveau des opérateurs de Téléport: exemple hub DBV-RCS ou hubs des constructeurs VIASAT ou I-Direct.

- Il néglige de fait une vraie optimisation de la consommation des segments spatiaux. Le coût des segments spatiaux étant un coût opératoire pour l'usager.
- Il placerait le niveau de sécurité des informations en critères mineurs. Les orientations ci-dessus ne peuvent pas être considérées pour la constitution de réseaux sécurisés.

Il paraît évident que pour réaliser un réseau réellement sécurisé, il soit nécessaire d'avoir au minimum les orientations suivantes :

- La possibilité d'indépendance de l'utilisateur, vis-à-vis d'un téléport
- Un segment spatial exclusivement dédié
- Un coût opératoire minimisé par des stations pouvant travailler sans Hub, et possédant assez d'intelligence pour travailler seules.

Certains constructeurs dont NDSATCom possèdent une série de modems ayant ces fonctionnalités. C'est le choix de LCDC SA pour offrir une intégration de réseaux VSAT parfaitement sécurisés pour les Entreprises.

Ces modems utilisent le protocole AMRT (TDMA), à saut de fréquences et allocation dynamique de bande passante par variations de l'intervalle de temps attribuée à la transmission par impulsion d'une station. A ce protocole est associé des fonctionnalités qui optimisent ses performances en matière de Qualité de Services et d'économie de bandes passantes spatiales.
LCDC SA le qualifie comme un système sans noyau central essentiel et à intelligence répartie : il est ''Hubless''. Il permet de créer des réseaux VSAT parfaitement isolés.

4 NIVEAUX D'INTRUSION

4.1 ECOUTE SUR LA COUCHE DE TRANSPORT

Chaque modem génère sa propre séquence de transmission et produit des caractéristiques de signal uniques en ce qui concerne l'ordre des stations qui émettent en séquences, la durée et la séparation d'impulsions.

En raison de ce côté propriétaire, il n'est pas possible de décoder ou produire le signal de la porteuse avec un modem d'un autre constructeur disponible sur le marché.

De plus, la structure des trames d'émissions diffère entre les réseaux même en utilisant un modem identique: ex., ceux-ci peuvent travaillent simultanément sur plusieurs porteuses pour transporter la même information.

Une intrusion illégale sur un réseau de ce type nécessite des achats d'équipements nombreux de réception pour l'écoute d'une seule station pour une collecte des signaux.

La station intruse doit alors d'être à proximité de la station à écouter car chaque station du réseau ajuste sa fenêtre d'écoute selon la durée de propagation entre et le satellite (RTT). L'argument d'une écoute au niveau international ou même régionale s'avère faux:
L'évaluation d'informations reçues exige la synchronisation appropriée, qui ne peut pas être considérée comme acquise naturellement dans le système, parce que le temps d'aller et retour vers le satellite différera de la station originale. L'adaptation d'un RTT automatique exigerait que clone transmette, ce qui mènerait à sa découverte. L'information obtenue serait de plus encodée.

La station intruse ne peut que collecter (et enregistrer) qu' fil de l'eau, et ne décoder que de façon binaire sur la base de la connaissance du type de modulation (QPSK, QAM8, 16), de la valeur de la correction d'erreur (FEC), des codages et algorithmes économisant la bande passante : Viterbi, Turbo Code, Reed Solomon, pour les modulations ; G723, 729, etc. pour les compressions de phonie.

Pour décoder des signaux de réception au niveau de la couche de transport, l'intrus devra alors connaitre les paramètres qui sont spécifiques à la station qu'il espionne. Cette collecte de l'écoute sera inutile sans corrélations et connaissance d'autres données liées directement à la connaissance des divers types de flux en temps réel de toutes les stations du réseau.

4.2 ACCES AUX COUCHES DE DONNEES ET DE RESEAUX.

Une partie de ces données complémentaires sont alors à trouver au niveau de couches de données et réseaux.

Le protocole propriétaire assigne à chaque station de s'identifier à intervalles définies et assignées de façon totalement dynamique. Ces intervalles sont ''aléatoires'' car elles suivent les flux à transmettre en temps réel (phonie), respectent les priorités des applicatifs du client, etc.. Il n'existe donc pas de trames répétitives identiques qui permettraient de constitueraient des trappes à analyser.

Chaque station a une adresse unique et doit être enregistrée. L'information qu'elle transporte ne peut être identifiée que par un décodage complet du contenu du contenu du ''burst'' de transmission.

L'émission et la réception ne sont seulement possibles pour des stations enregistrées et possédant une identification validée. Toutes autres demandes de transmissions d'une adresse inconnue sont rejetées et aucune donnée ne lui est envoyée. Il y aurait en outre une alerte au niveau de la supervision du réseau.

4.3 ACCES AUX DONNEES DES APPLICATIONS

Les données reçues par une station sont extraites du conteneur de données dans le ''burst'' de la trame TDMA. Ces données sont amenées sur la carte de l'unité centrale puis traitées plus loin dans le FRAD interne au modem ou dans le pont Ethernet selon l'adressage.
Seules les données adressées dans le nœud de réseau seront disponibles aux ports Frame Relay ou Ethernet.

Il n'y a aucun accès à d'autres données que ceux destinées pour la station.

Il n'existe donc pas d'accès aux autres données que celles destinées à la station considérée.

5 EFFICACITE DES CES INTRUSIONS ILLEGALES

S'immiscer dans ce type de réseau demandera dans tous les cas de moyens matériels très importants ainsi qu'une connaissance détaillée des types de flux des utilisateurs. D'autres formes d'intrusions seraient certainement moins onéreuses et plus efficaces, en particulier sur les supports terrestres.
L'efficacité des différentes manières de s'immiscer dans un réseau de ce type est alors sujette à de forts doutes de résultat.

6 MALVEILLANCE

6.1 INTEGRITE DES DONNEES

Il n'y a aucune possibilité pour des personnes non autorisées de changer, modifier, supprimer ou ajouter des données pendant la transmission sur un réseau de ce type, simplement parce que pour des stations terriennes non enregistrées, il n'est pas possible de transmettre.

Toute tentative de clone d'une station légitime provoquera immédiatement du conflit causant immédiatement un conflit d'adressage et un disfonctionnement et une alarme au niveau de la gestion du réseau.

Dans le doute, l'utilisateur de réseau aura la possibilité d'exclure cette station ou la station clonée du réseau.

Il est généralement possible d'empêcher un réseau de ce type par un brouillage approprié sur les fréquences des porteuses.
Un délit si évident mettrait en fait hors de service toutes sortes de communications satellites : C'est le cas très improbable sauf par malveillance ou en temps de guerre.

D'autre part, la capacité d'utiliser des porteuses multiples sur une très large bande couvrant toute la bande C ou Ku rend difficile un brouillage complet difficile.

6.2 CONFIDENTIALITE DES DONNEES

Comme expliqué ci-dessus, l'intrus illégal se doit d'acheter un modem identique au réseau à introduire et d'être capable de structurer et décoder les données transportées l'obligeant d'avoir la connaissance de tous les paramètres spécifiques du réseau.

La station clonée ne peut seulement obtenir l'accès aux informations qui ''lui'' sont adressées.
Reconstituer les données complémentaires des autres stations du réseau nécessiterait des modifications en profondeur des systèmes opératoires propriétaires du modem lui-même.

7 VULNERABILITES A L'ECOUTE

Les activités de communications de stations satellites à partir du sol, sont moins faciles de détecter et localiser et analyser que sur des réseaux radioélectriques (HF, VHF, UHF etc...) ou terrestre par cuivre ou par fibres.
Le signal transmis est émis dans un angle très étroit (typiquement 1 degré) dans la direction au satellite. En raison de la radiation très concentrée il n'y a aucune énergie considérable

voyageant le long de la surface de la terre, qui pourrait être détectée et évaluée dans une certaine distance.

Les écoutes des communications dépendent principalement de l'écoute des transmissions du satellite. Les stations émettrices ne peuvent pas être identifiées sans décodage complet du contenu de données dans chaque impulsion des trames TDMA.
Seule une station clonée seraient capable de déchiffrer avec beaucoup de conditions réunies : porteuses identiques, flux entrants uniquement, mais aucune corrélation avec le trafic qui permettrait un décodage ''rapide'' ne serait obtenue pour entreprendre la prochaine étape de déchiffrage.

8 CONCLUSIONS

Les barrières pour un intrus sont extrêmement hautes dans des réseaux satellite utilisant un protocole d'accès multiple TDMA à allocation dynamique de bande passante, à allocation dynamique de l'intervalle de temps de transmission, à porteuse multiples.
En particulier lorsqu'elles sont associées à des fonctionnalités d'optimisation de bande passante par remplissage de containers de paquets vides de phonie par des bits de données qui rend le protocole de base TDMA propriétaire.

Le gain possible à l'obtention d'information par des moyens d'écoute est très faible en comparaison de l'effort exigé et aux risques d'échec en étant découvert.
Le résultat d'une comparaison entre les risques de confidentialité divers montrerait que c'est beaucoup plus facile pour un intrus potentiel d'obtenir les informations autrement. Par exemples en interceptant des données sur les secteurs terrestres ou par les agents de l'utilisateur, la forteresse étant mieux protégée par ses habitants que par ses murs.

Si, malgré le risque extrêmement bas pour la perte de confidentialité, il y a une nécessité supérieure (réseaux gouvernementaux) d'augmenter la sûreté de l'information et sa sécurité, on peut considérer le chiffrage de données d'utilisateur.
Ce sujet fait l'objet d'un autre document sur le respect de la QoS dans un réseau crypté