Référence : CLB-AOR-2020-11-02-01-v07

Cible de sécurité CSPN - Kakoma

Cailabs – 38 boulevard Albert 1er, 35200 Rennes, FRANCE - www.cailabs.com

Projet / Département	Kakoma		
Résumé	Description du produit Kakoma et de la cible de sécurité pour sa certification CSPN.		
Mots-clés	Fibre multimode, obfuscation, détection d'intrusion		
Confidentialité	☐ Ultra confidentiel	☐ Confidentiel	☒ Public

TABLE DES MATIERES

Cible de sécurité pour une évaluation CSPN, dans le contexte des communications sécurisées sur fibre optique.

1. IDENTIFICATION DU PRODUIT

Société éditrice	Cailabs
Lien vers la société	www.cailabs.com
Nom commercial du produit	Kakoma
Référence du produit évalué	PN : KAKOMA-10G-OM1 (REV 01) Version du logiciel : S6.4.100
Catégorie du produit	Hardware & Embedded Software

La référence du produit est indiquée sur une étiquette en face arrière du rack 1U supérieur :

La version de logiciel embarqué est consultable dans le logiciel lui-même pour chaque châssis (menu « Application » > « Inventory »).

2. ARGUMENTAIRE DU PRODUIT

2.1. Description générale du produit

Le produit Kakoma est un équipement actif de réseau local (LAN) destiné à sécuriser une transmission haut débit sur une fibre optique multimode (MMF) contre une attaque physique d'espionnage sur la fibre.
Les cas d'usage typiques sont la sécurisation d'une fibre déployée sur une base militaire, sur un site industriel ou dans un immeuble de bureaux partagé entre plusieurs entreprises.

Le produit se présente sous la forme d'une paire de châssis insérés respectivement de part et d'autre de la fibre optique multimode du client, directement entre le dernier équipement réseau (typiquement un switch) et l'extrémité de la fibre.
Chaque châssis comporte quatre interfaces :

- une fibre optique multimode (simplex) à épisser sur la fibre terrain,
- un port optique monomode (SMF) duplex (le port « client ») à connecter au switch ou au dernier équipement réseau du client,
- un port RJ45 (le port « mgnt ») permettant d'accéder au logiciel embarqué de contrôle et de supervision du châssis,
- une alimentation secteur.

La transmission sur la fibre optique multimode (simplex) s'effectue de façon bidirectionnelle.

Figure 1 : schéma de déploiement du produit, avec les différentes interfaces des deux châssis et la fibre optique multimode terrain du client.

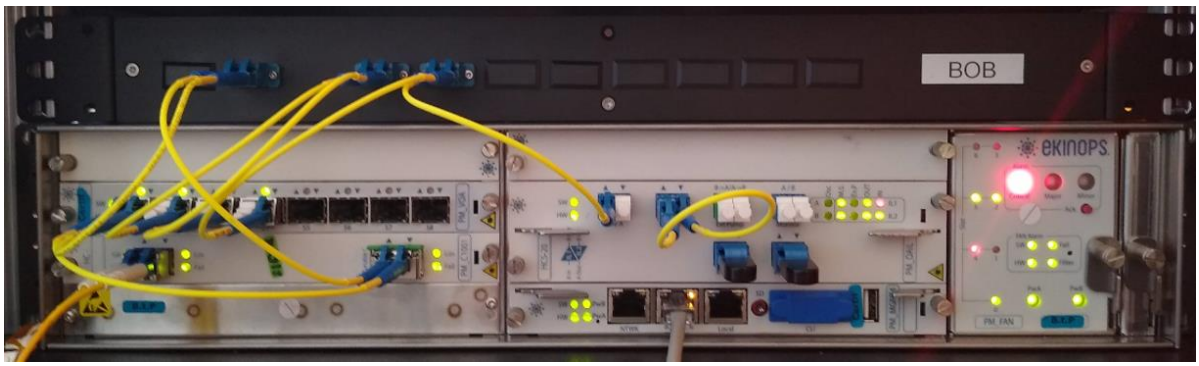

Figure 2 : face avant d'un châssis, constitué d'un rack 1U supérieur et d'un rack 2U inférieur. Le port optique « client » et le port RJ45 « mgnt » sont situés sur le rack 2U inférieur.

Figure 3 : face arrière d'un châssis, constitué d'un rack 1U supérieur et d'un rack 2U inférieur. La fibre optique multimode est située sur le rack 1U supérieur et l'alimentation secteur est située sur le rack 2U inférieur.

Le produit remplit trois fonctions principales :

- Il rend possible une transmission haut débit (10 Gbits/s) sur une fibre optique multimode grâce à l'injection des données sur le mode spatial fondamental de la fibre, ce qui permet de s'affranchir de la dispersion modale qui limite généralement les débits atteignables sur ce type de fibre.
- Il permet d'obfusquer (camoufler) physiquement les données transmises dans la fibre, grâce à l'injection de bruit dans des modes spatiaux d'ordre supérieur de la fibre, appelés « modes boucliers ».
- Il permet de détecter une intrusion physique sur la fibre optique, grâce à la mesure de la puissance optique transmise sur différents modes spatiaux d'ordre supérieur de la fibre, appelés « modes témoins ».

La présente version du produit est compatible avec les fibres optiques multimodes 62.5/125 (OM1), sur des distances typiques comprises entre quelques centaines de mètres et quelques kilomètres. Elle est utilisable à 10 Gbits/s (10G LAN Ethernet, 10GbE).

2.2. Description de la manière d'utiliser le produit

Un manuel d'utilisation est fourni à l'utilisateur.
L'utilisation du produit comporte deux phases : une phase d'installation et une phase d'exploitation.

La phase d'installation comporte les étapes suivantes :

- Un audit est effectué sur la fibre multimode terrain, avec un contrôle visuel renforcé des zones d'épissure et des éventuelles zones douteuses ayant pu être repérées à l'OTDR (si une trace a été mesurée avant l'installation), afin de s'assurer de l'absence de pince optique (dispositif

permettant une petite fuite de lumière par courbure de la fibre), de coupleur fibré (dispositif permettant de rediriger la lumière se propageant dans une fibre vers deux fibres différentes avec un ratio donné) ou de tout autre élément permettant de rediriger une partie de la lumière propagée dans la fibre vers l'extérieur.

- Le câblage des châssis est effectué.
- La fibre optique multimode de chaque châssis est épissée respectivement à chaque extrémité de la fibre optique multimode terrain. Les éventuels connecteurs optiques intermédiaires présents sur la fibre optique multimode terrain sont remplacés par des épissures optiques.
- Une fois les fibres épissées et rangées, les châssis sont mis sous tension et connectés à un ordinateur. Au moyen du logiciel embarqué, une calibration est effectuée sur chacun des deux châssis : il s'agit d'enregistrer une mesure de référence des puissances optiques correspondant aux modes « boucliers » et aux modes « témoins » reçues sur chacun des deux châssis. Lors de cette calibration, on s'assure également que les niveaux de puissance dans les différents modes sont corrects. (Remarque : les valeurs de calibration sont gardées en mémoire sur chaque châssis, même en cas de mise hors tension.)
- Le lien est mis en service.

Le câblage des châssis, l'épissage des fibres optiques multimodes et la calibration doivent être réalisées par une personne de Cailabs (ou formée par Cailabs).

La phase d'utilisation commence immédiatement après la fin de l'installation.

L'utilisateur peut brancher ou débrancher à loisir ses équipements réseaux sur le port optique « client » de chaque châssis, sans incidence sur le fonctionnement du produit ou la sécurité du lien.

Chaque châssis surveille le lien de manière indépendante et déclenche une alarme « intrusion » en cas de suspicion d'intrusion sur la fibre multimode. En cas d'alarme, la transmission des données est automatiquement coupée. L'alarme ne peut être levée qu'après une intervention de l'utilisateur. Celui-ci doit d'abord contrôler le lien (nouvel audit de la fibre) afin de déterminer si l'alarme correspond ou non à une tentative d'espionnage et s'assurer de la disparition de la menace avant de lever l'alarme et de rétablir la transmission.

Un log des événements sur chaque châssis enregistre les actions de l'utilisateur, les apparitions et disparitions d'alarmes, les connexions au châssis, le redémarrage d'une carte, la mise sous tension du châssis, etc.

2.3. Hypothèses sur l'environnement

- **H1** : On suppose que les deux châssis sont installés dans des locaux sécurisés, accessibles uniquement à du personnel habilité et bienveillant, qui ne tentera en aucune manière d'altérer le fonctionnement du produit (notamment par un démontage des châssis ou l'absence de prise en compte d'une alarme) et qui respectera les instructions du manuel utilisateur. Cette hypothèse est valable à la fois lors de la phase d'installation et lors de la phase d'exploitation. On suppose également que les équipements informatiques présents dans les locaux sécurisés et utilisés pour se connecter au port RJ45 des châssis n'altèrent pas le bon fonctionnement des logiciels embarqués.
- **H2** : On suppose que la phase d'installation s'est bien déroulée, audit compris, et en particulier, que les valeurs des puissances dans les différents modes sont correctes, ce qui indique que la fibre et les soudures optiques sont d'une qualité suffisante pour faire fonctionner le produit.
- **H3** : On suppose qu'en cas de mise hors tension des châssis (volontaire ou involontaire), l'utilisateur refera un audit de la fibre avant de reprendre la transmission des données, comme indiqué dans le manuel utilisateur.

2.4. Description des utilisateurs du produit

Les utilisateurs du produit sont typiquement les administrateurs réseau et les personnes chargées de la sécurité du réseau.

La phase d'installation nécessite aussi l'intervention d'une personne de Cailabs ou formée par Cailabs (pour effectuer le câblage, les épissures des fibres optiques et la calibration).

2.5. Définition du périmètre de l'évaluation

L'évaluation concerne une paire de châssis installée sur une fibre OM1, pour une transmission à 10 Gbit/s (10G LAN Ethernet, 10GbE).
Sont incluses dans l'évaluation les deux fonctions de sécurité suivantes :

- **FS1** : fonction d'obfuscation (camouflage) des données dans la fibre.
- **FS2** : fonction de détection d'intrusion sur la fibre.

3. BIENS SENSIBLES PROTEGES

Les biens sensibles protégés par le produit sont les données transmises sur le mode fondamental de la fibre optique multimode : un attaquant ne doit pas pouvoir extraire de façon exploitable des données sans que sa présence ne soit détectée.

4. DESCRIPTION DES MENACES

4.1. Profil des attaquants

Les attaquants potentiels (espions) sont toutes les personnes, internes ou externes au site, ayant accès à la fibre optique multimode sur laquelle sont transmises les données.

Ne sont pas considérées comme attaquants potentiels les personnes ayant accès aux locaux sécurisés dans lesquels se trouvent les châssis, ni en phase d'installation, ni en phase d'exploitation.

4.2. Types de menaces

Les menaces considérées dans la présente évaluation sont :

- **M1** : Un espion pose une pince optique (commerciale ou améliorée) sur la fibre. La pince induit une faible perturbation sur la fibre. L'espion n'est pas détecté et parvient à extraire des données exploitables malgré l'obfuscation de celles-ci.
- **M2** : Un espion pose une pince optique (commerciale ou améliorée) sur la fibre. La pince induit une forte perturbation sur la fibre. L'espion est détecté mais parvient à extraire des données exploitables malgré l'obfuscation de celles-ci, juste avant que la transmission ne soit coupée suite à la détection d'intrusion.
- **M3** : Un espion coupe la fibre puis installe un coupleur optique entre les deux portions de la fibre, afin d'extraire une partie du signal. Il n'est pas détecté et parvient à extraire des données exploitables malgré l'obfuscation de celles-ci.

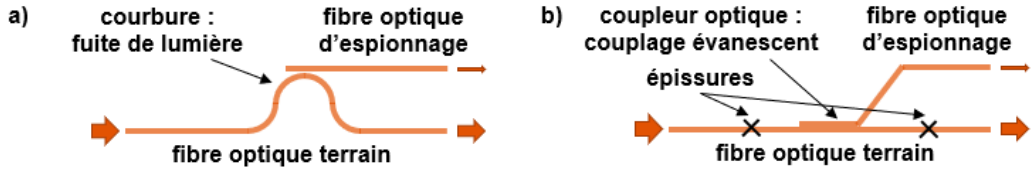

Figure 4 : schéma de principe a) d'une pince optique utilisant une courbure sur la fibre (M1 ou M2) et b) d'un coupleur optique, inséré par épissure sur la fibre (M3).

5. DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

Les deux fonctions de sécurité considérées dans l'évaluation sont :

- **FS1** : fonction d'obfuscation (camouflage) des données dans la fibre.
- **FS2** : fonction de détection d'intrusion sur la fibre.

FS1 - Fonction d'obfuscation (camouflage) :

A chaque extrémité de la fibre, à l'émission, les données d'entrée du port optique « client » sont injectées optiquement sur le mode spatial fondamental de la fibre optique multimode, et multiplexées spatialement avec un bruit optique large bande sur plusieurs modes spatiaux d'ordre supérieur de la fibre (les modes « boucliers »). A chaque extrémité de la fibre, à la réception, les différents modes spatiaux sont démultiplexés et les données sont extraites vers le port optique « client ».

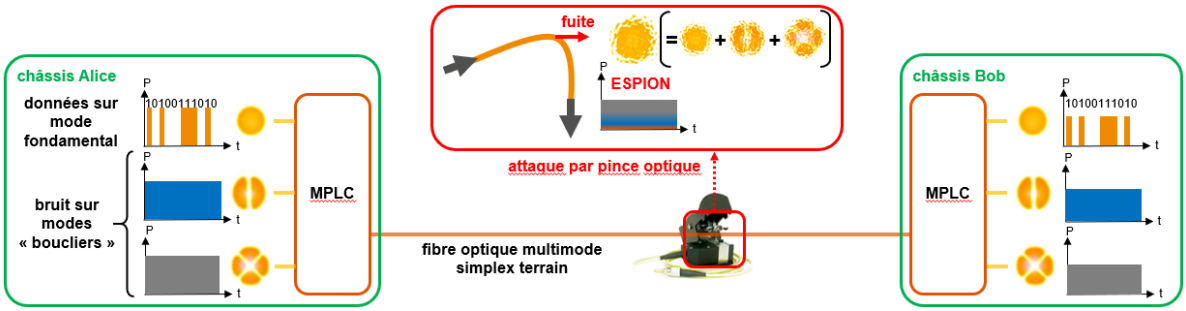

Figure 5 : schéma de principe de la fonction obfuscation (camouflage). Les MPLC sont des multiplexeurs/démultiplexeurs de modes spatiaux. Les modes d'ordre supérieur sur le schéma ne sont donnés qu'à titre d'exemple.

- Si un espion tente de récupérer une partie de la lumière transmise sur la fibre optique au moyen d'une pince optique (**M1** ou **M2**), il extrait par courbure un mélange des différents modes spatiaux : dans la part de lumière qui fuit de la fibre, les données sont noyées dans le bruit. L'espion peut tenter d'utiliser lui-même un démultiplexeur de modes spatiaux sur la fuite de lumière mais son rapport signal-à-bruit n'en sera pas significativement amélioré car un fort couplage des différents modes a lieu lors de la fuite.
- La fonction d'obfuscation seule n'est en revanche pas totalement efficace contre une attaque par insertion d'un coupleur optique entre deux portions de la fibre (**M3**) et utilisation par l'espion d'un démultiplexeur de modes spatiaux sur son port de sortie du coupleur. Seuls l'audit de la fibre lors de la phase d'installation (**H2**) et la fonction de détection d'intrusion (**FS2**) permettent de se prémunir contre cette attaque.

FS2 - Fonction de détection d'intrusion :

A chaque extrémité de la fibre, à l'émission, les données et les modes « boucliers » sont également multiplexés avec plusieurs modes spatiaux d'ordre supérieur de la fibre (les modes « témoins »). A chaque extrémité de la fibre, à la réception, les modes « témoins » sont démultiplexés et leurs puissances optiques sont mesurées.

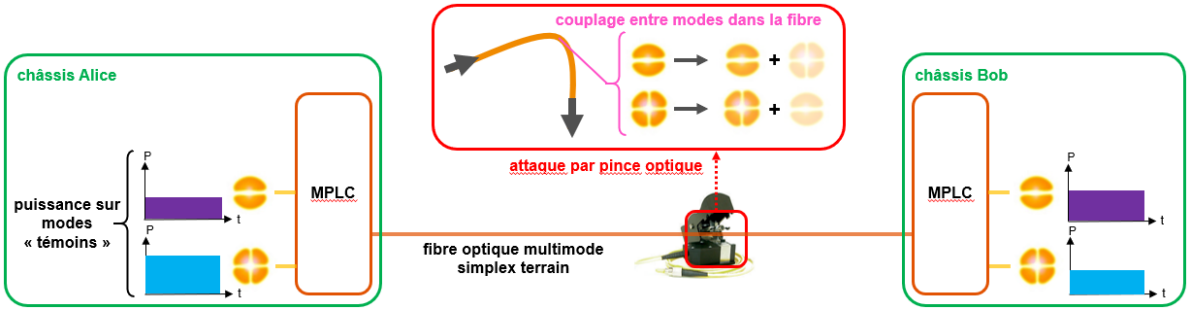

Figure 6 : schéma de principe de la fonction détection d'intrusion. Les MPLC sont des multiplexeurs/démultiplexeurs de modes spatiaux. Les modes d'ordre supérieur sur le schéma ne sont donnés qu'à titre d'exemple.

- Si un espion tente de poser une pince optique (**M1** ou **M2**), il induit un couplage entre les différents modes spatiaux se propageant dans la fibre. Ceci induit une variation significative de la puissance et des rapports de puissance des différents modes « témoins ». La comparaison de ces puissances avec le seuil de détection calibré à l'installation du produit, permet de détecter l'attaque de l'espion (**M2**). Si la perturbation induite par la pince est trop faible, l'intrusion n'est pas détectée (**M1**) mais le signal récupéré par l'espion est aussi plus faible et la fonction d'obfuscation (**FS1**) protège les données.
- Si un espion tente d'installer un coupleur optique (**M3**), il devra couper la fibre pendant quelques minutes (le temps de réaliser deux épissures). La puissance dans les modes « témoins » sera donc nulle ou très fortement diminuée pendant cette période et l'attaque de l'espion sera ainsi détectée.

Protection contre les différentes menaces par les fonctions de sécurité :

	FS1 : obfuscation	**FS2 : détection d'intrusion**
M1 : pose de pince (faible perturbation)	OUI	NON
M2 : pose de pince (forte perturbation)	OUI	OUI
M3 : coupure de la fibre et pose de coupleur	NON	OUI