Le LiFi et les environnements hautement sécurisés

En 2014, j'ai rédigé l'article 'Sécurité et LiFi". Depuis, le développement du LiFi a pris un essor considérable. À une époque où les communications sans fil occupent une place centrale dans notre vie quotidienne, le LiFi (Light Fidelity) introduit une approche innovante en transmettant des données par la lumière. Au lieu d'ondes radio utilisées par le WiFi traditionnel, le LiFi utilise des ondes lumineuses visibles, infrarouges ou ultraviolettes, offrant des vitesses élevées et une transmission de données potentiellement plus sécurisée. Le présent article explore la technologie sous-jacente au LiFi et la manière dont elle contribue à la sécurité de l'information et pointe ses avantages, ses défis et ses perspectives d'avenir.

Qu'est-ce que le LiFi?

Le LiFi est une technologie qui utilise des lampes LED pour transmettre des données par la lumière. Les lampes forment la base du LiFi car elles peuvent s'allumer et s'éteindre des milliards de fois par seconde, de manière invisible à l'œil humain, pour transmettre de l'information digitale sous forme binaire. Un photodétecteur, comme une photodiode, reçoit les signaux lumineux et les convertit en signaux électriques que les appareils peuvent traiter. La vitesse du LiFi varie selon la situation. Lors de tests en laboratoire, des vitesses allant jusqu'à 224 gigabits par seconde (Gbps) ont été atteintes, tandis que les applications pratiques offrent généralement des vitesses plus faibles, autour de 3,5 Gbps ou 30 Mbit/s pour les systèmes commerciaux. Le LiFi fonctionne dans le spectre de la lumière visible et nécessite une ligne de visée directe entre l'émetteur (la lampe LED) et le récepteur. La lumière ne peut donc pas traverser les murs, ce qui constitue à la fois une limitation et un avantage, notamment en matière de sécurité de l'information.

Sécurité de l'information et LiFi

L'un des grands avantages du LiFi pour la sécurité de l'information réside dans la limitation physique de la lumière. Comme les signaux lumineux ne peuvent pas traverser les murs ou les objets opaques, il est plus difficile pour des personnes non autorisées d'accéder au réseau depuis l'extérieur. Cela contraste avec le WiFi où les ondes radio peuvent être captées sur de longues distances et à travers des barrières physiques, augmentant le risque d'écoute clandestine.

Le LiFi assure une isolation naturelle du réseau. Dans un environnement de bureau, par exemple, chaque pièce peut disposer de son propre réseau LiFi, sans interférence ni chevauchement avec d'autres espaces. Cela réduit le risque d'accès non autorisé aux données sensibles. En outre, le LiFi peut être associé à des techniques de cryptage telles que l'AES (Advanced Encryption Standard)

pour sécuriser davantage la transmission des données, ce qui en fait une solution robuste pour les environnements où la sécurité est essentielle, tels que les banques, la défense et les institutions gouvernementales. Depuis cette année, les produits LiFi sont disponibles sur le marché avec la certification FIPS 140-3, rendant le LiFi plus adapté aux applications de haute sécurité.

Défis en matière de sécurité

Le piratage du LiFi est un sujet relativement nouveau et complexe, dû en partie à la nature unique de la technologie. Comme le LiFi transmet des données par des signaux lumineux, le piratage nécessite une ligne de visée directe vers la source lumineuse, ce qui le rend plus difficile qu'avec le WiFi. Cependant, des vulnérabilités potentielles existent, comme l'interception de signaux à l'aide d'équipements optiques sophistiqués si l'émetteur n'est pas correctement protégé. La manipulation de lampes LED, de photodétecteurs ou de connexions réseau pourrait également, en théorie, permettre l'accès au réseau. Le cryptage, comme l'AES, et la sécurité physique de l'infrastructure sont essentiels pour minimiser les risques. À ce jour, peu de cas de piratages LiFi réussis ont été signalés, mais la recherche reste nécessaire à mesure que la technologie se développe. Un autre défi réside dans l'intégration du LiFi aux infrastructures réseau existantes. De nombreuses organisations s'appuient sur une combinaison de réseaux filaires et sans fil, et l'implémentation du LiFi nécessite des investissements dans du nouveau hardware comme les lampes LED et des photodétecteurs. En outre, les organisations doivent s'assurer que les logiciels et les protocoles supportant les réseaux LiFi répondent à des normes de sécurité strictes pour minimiser les vulnérabilités.

Perspectives d'avenir

Le LiFi est actuellement opérationnel, principalement dans les secteurs où la sécurité de l'information est primordiale. Les chercheurs travaillent sur des innovations telles que l'utilisation de plusieurs sources lumineuses pour augmenter la couverture et réduire la dépendance à une ligne de visée directe, en accordant une attention particulière à l'itinérance entre les différents réseaux LiFi. Les utilisateurs veulent pouvoir se déplacer de leur chambre à un autre espace en passant par le couloir sans perdre la connexion. La localisation fait également l'objet de recherches. Dans les bâtiments LiFi, les lampes LED peuvent déterminer votre position grâce à la ligne de visée, ce qui évite aux lampes hors de portée d'émettre ou de recevoir des signaux. Des systèmes hybrides intégrant le LiFi et le WiFi sont à l'étude afin d'améliorer la vitesse et la sécurité. Enfin, le LiFi est déjà utilisé dans des environnements où les ondes radio sont indésirables et où les interférences électromagnétiques peuvent poser un problème, et peut représenter une solution.

Le LiFi implique des changements organisationnels

L'introduction du LiFi va entraîner des changements organisationnels importants. Il existe déjà des luminaires compatibles avec le LiFi sur le marché, ce qui ajoute une nouvelle dimension à l'infrastructure des bureaux et autres postes de travail. Cela soulève la question suivante: le service IT va-t-il également devenir responsable de l'éclairage ? L'intégration de l'éclairage et de la technologie internet peut entraîner une redéfinition des tâches au sein des organisations. Cela signifie que les collaborateurs IT pourraient avoir besoin d'une formation pour exploiter ces systèmes hybrides. Dans le même temps, cela pourrait renforcer la collaboration entre des services tels que le facility management et l'IT. Il s'agit d'un développement qui demande une planification et une adaptation minutieuses pour se dérouler sans heurts.

Conclusie

en matière de sécurité de l'information. Les limitations physiques des signaux lumineux en font une alternative plus sûre au WiFi dans les environnements où la protection des données est cruciale. Malgré les défis, comme la dépendance à une ligne de visée directe et le coût de mise en œuvre, les vitesses élevées et les avantages inhérents en sécurité font du LiFi une technologie prometteuse pour l'avenir. À mesure que la technologie continue de se développer, le LiFi est susceptible de jouer un rôle important dans la conception de réseaux de communication sûrs, rapides et efficaces.

Ronald Eygendaal rédige depuis 1990 des articles sur la sécurité de l'information, la sécurité dans l'automatisation industrielle et la sécurité électronique et technique pour des revues spécialisées en Belgique et aux Pays-Bas.

Source: Ronald Eygendaal

Photo: Ronald Eygendaal