INSA Lyon – Département Télécommunications
Année universitaire : 2025 – 2026

Appareil de diffusion vidéo non intrusif
Analyse des surfaces d'attaque

Encadrant :
Stéphane Frenot - Damien Reimert

Réalisé par :

- Orhon Gabriel
- Chkoundali Yasmine
- Mohammi Islam
- Abidi Jean
- Adjami Axel

Modifications

Version	Date	Auteur	Modifications
v0	19/12/2025	Gabriel	**Création initiale :** Analyse basée sur les impacts Qualité de service / Confidentialité. Identification des risques de Hijack, DoS, et VP-Spoofing.
v1	09/01/2026	Axel	– **Restructuration :** Adoption d'un plan par zones d'attaque Serveur / Matériel / Réseau qui remplace le plan par impacts. – **Ajouts :** Partie 2 dédiée risques liés Raspberry Pi Section 1.1 sur le détournement de relais Section 1.3 sur la manipulation de signalisation (Man-in-the-Middle) et solution WSS. Modification de la solution contre le VP-Spoofing – **Suppressions :** Section dédiée au Hijack du flux

Abstract

Ce document présente une analyse de la surface d'attaque d'un dispositif de diffusion vidéo par Web Real-Time Communication (WebRTC) déployé au sein des salles de cours de l'INSA de Lyon. L'objectif est d'évaluer si cette solution résiste aux tentatives de piratage. L'analyse met en lumière trois zones de risque majeures : le détournement possible des serveurs centraux pour masquer des activités illégales, la fragilité des boîtiers Raspberry Pi laissés sans surveillance, et les tentatives d'usurpation d'identité sur le réseau.

Ce document classe ces menaces de façon arbitraire et liste les protections plausibles à activer pour garantir que ce service ne devienne pas une porte d'entrée pour attaquer le réseau de l'école.

Sommaire

Introduction

Lors d'une présentation, un flux vidéo n'est pas forcément une donnée sensible. Cependant, pour certaines présentations telles que des rapports de stage ou les rapports de période entreprise pour les alternants, les utilisateurs sont amenés à partager des données confidentielles. La fuite de ces données vers des acteurs malveillants est donc un risque important à prendre en compte.

L'intégration de dispositifs connectés IoT dans des environnements ouverts comme les salles d'enseignement génère de nouvelles portes d'entrée pour des acteurs malveillants. Ce projet introduit par sa nature même des composants critiques au cœur du système d'information : un serveur de relais ouvert sur le réseau départemental et des micro-ordinateurs Raspberry Pi disséminés dans les espaces publics. Dans un contexte où la menace ne provient pas uniquement de l'extérieur mais également d'utilisateurs légitimes du réseau disposant d'accès physiques et logiques, une approche de sécurité périmétrique classique est insuffisante.

Il devient judicieux d'adopter une posture de "Zero Trust". Ce rapport a pour objectif d'auditer la sécurité globale de cette solution. Nous présentons successivement les trois couches exposées : l'infrastructure serveur et ses risques de détournement, le matériel terminal et sa sensibilité aux attaques physiques, et enfin le canal de communication Eduroam.

1. Analyse de l'Infrastructure Serveur

La centralisation des services sur le réseau tc-net offre une facilité de gestion mais crée un point de défaillance unique dont la compromission affecterait l'ensemble du département.

1.1. Détournement de relais et risques juridiques

Le protocole WebRTC favorise les connexions directes en pair à pair. Cependant, les configurations réseau restrictives et les pare-feux nécessitent fréquemment l'usage d'un serveur intermédiaire TURN, pour relayer le trafic média.

Mécanisme de l'attaque : Un serveur TURN configuré par défaut opère souvent en mode relais ouvert (Open Relay). Il accepte sans discrimination les requêtes d'allocation de ressources provenant de n'importe quelle adresse IP. Un attaquant externe identifie ce serveur et configure ses propres applications pour transiter par ce relais. Le serveur de l'INSA devient alors un proxy anonyme gratuit pour l'attaquant.

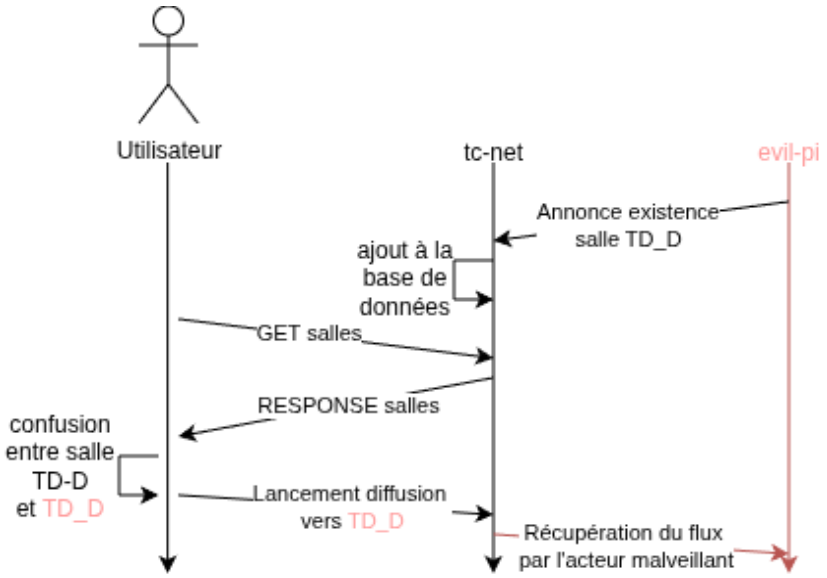
Conséquences : L'infrastructure de l'école sert de couverture pour des activités illicites telles que le partage de fichiers illégaux ou le lancement de cyberattaques. Aux yeux des autorités et des opérateurs, le trafic émane légitimement des adresses IP de l'INSA. Cette situation engage la responsabilité juridique de l'établissement et expose son réseau à un risque de blocage ou de mise sur liste noire par les fournisseurs d'accès Internet. De plus, l'utilisation de serveurs publics externes est proscrite car elle offre des métadonnées critiques à des tiers et induit une latence préjudiciable.

Mécanisme de défense : On pourrait utiliser un mot de passe fixe, mais il finira sûrement par fuiter vu le nombre d'acteurs qui seront impliqués. La solution peut être alors d'utiliser le mécanisme "Long-Term Credential". Concrètement : Avant chaque appel, le serveur Web génère un "ticket d'entrée" temporaire, un token chiffré valable seulement quelques minutes. Le serveur TURN vérifie ce ticket. Pas de ticket valide = pas de relais.

1.2. Intégrité du parc et usurpation d'équipement

La facilité de déploiement suggère une procédure d'auto-déclaration des équipements où chaque Raspberry Pi annonce sa présence au serveur central pour être ajouté à l'annuaire des salles disponibles.

Mécanisme de l'attaque : Cette approche expose le système au VP-Spoofing. En l'absence de vérification d'identité, un attaquant connecte un dispositif pirate, nommé *evil-pi*, sur le réseau et envoie une requête d'annonce au serveur. Il utilise une technique de typo-squatting en nommant sa fausse salle de manière trompeuse, par exemple `TD_D` au lieu de la salle officielle `TD-D`.



Fonctionnement de l'attaque en l'absence de mécanisme de sécurité

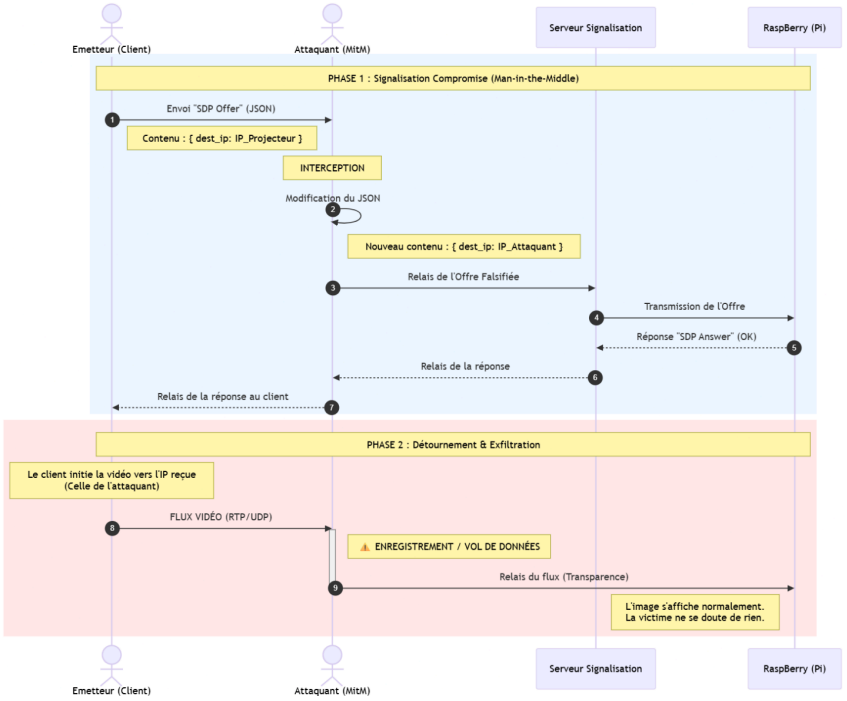
Conséquences : L'utilisateur final, trompé par la similarité des noms, sélectionne le dispositif pirate dans son interface. Le flux vidéo confidentiel est alors transmis directement à l'attaquant qui peut l'enregistrer ou le rediffuser. Cette confusion perturbe également le déroulement des cours, l'utilisateur ne comprenant pas pourquoi sa diffusion n'apparaît pas sur le vidéoprojecteur légitime.

Mécanisme de défense : Contrôle d'accès par Liste Blanche (Whitelisting). L'architecture privilégie une approche déterministe via un contrôle d'accès strict côté serveur. Le serveur central maintient une liste statique recensant exhaustivement les identifiants uniques et les adresses MAC des Raspberry Pi officiellement déployés dans l'établissement. Lors d'une phase d'annonce, le serveur confronte l'identité de l'émetteur à cette liste blanche déclarée manuellement. Toute requête provenant d'un dispositif non répertorié est silencieusement ignorée par le serveur, rendant impossible l'insertion d'un équipement pirate dans l'annuaire de découverte, même si l'attaquant est présent sur le réseau.

1.3. Manipulation de la signalisation et interception

L'établissement de la connexion multimédia repose sur l'échange de paramètres techniques via le protocole Session Description Protocol (SDP), formaté en JavaScript Object Notation (JSON).

Mécanisme de l'attaque : Ces messages transitent par le serveur de signalisation. Si ce canal n'est pas sécurisé, un attaquant positionné en Man-in-the-Middle intercepte les messages JSON en transit. Il modifie les champs spécifiant l'adresse IP et le port de destination média pour y insérer ses propres coordonnées réseau avant de relayer le message.



Fonctionnement de l'attaque Man-In-The-Middle

Conséquences : Le client émetteur reçoit une réponse falsifiée qu'il croit légitime. Il établit la connexion vidéo vers la machine de l'attaquant au lieu du vidéoprojecteur. L'attaque est totalement transparente : si l'attaquant relaye ensuite le flux vers le vrai projecteur, l'utilisateur ne se rend compte de rien et continue sa présentation normalement pendant que ses données sont exfiltrées à son insu.

Mécanisme de défense : Pour la confidentialité et l'intégrité des échanges on utilise le protocole WebSocket Secure, ou WSS. Ce protocole encapsule les échanges dans un tunnel chiffré Transport Layer Security, ou TLS, rendant toute modification à la volée impossible. En complément, le serveur applicatif doit implémenter une validation rigoureuse des schémas JSON entrants via une bibliothèque comme Joi. Cette validation s'assure que les adresses IP fournies appartiennent exclusivement aux plages d'adresses du réseau local autorisé.

2. Analyse du Boîtier d'Affichage Raspberry Pi

Le boîtier Raspberry Pi constitue le maillon le plus vulnérable de la chaîne de sécurité car il est physiquement accessible dans les salles de cours sans surveillance permanente.

2.1. Vulnérabilité des interfaces physiques

Les ports USB du Raspberry Pi sont exposés et actifs par défaut. Les systèmes d'exploitation modernes font implicitement confiance aux périphériques de saisie.

Mécanisme de l'attaque : Un attaquant utilise un dispositif malveillant de type BadUSB. Ce matériel se présente électroniquement comme un clavier standard lors de sa connexion. Une fois accepté par le système, il injecte une séquence de touches préprogrammée à une vitesse surhumaine.

Conséquences : Le faux clavier ouvre un terminal, saisit des commandes complexes pour télécharger des charges virales, créer des portes dérobées ou exfiltrer des données, le tout en quelques secondes. La compromission est quasi instantanée et indétectable visuellement.

Mécanisme de défense : Le déploiement du démon logiciel USBGuard. Ce service applique une politique de liste blanche stricte. Il bloque systématiquement tout nouveau périphérique connecté et n'autorise que les équipements dont les identifiants matériels sont explicitement reconnus, tels que le clavier et la souris officiels de la salle. Toute tentative de connexion d'une clé inconnue est refusée au niveau du noyau du boîtier.

2.2. Persistance des données et vol de matériel

Le Raspberry Pi utilise une carte MicroSD pour stocker son système d'exploitation et ses fichiers de configuration. Ce support de stockage est rarement chiffré pour préserver les performances du processeur.

Mécanisme de l'attaque : Les permissions Linux tel que mot de passe root, droits d'accès aux fichiers ne sont valables que quand le système tourne. Si quelqu'un retire la carte SD et la lit sur son propre PC, il peut tout voir. Il est "administrateur" de la carte puisqu'elle est chez lui.

Conséquences : L'attaquant accède à l'intégralité des données sans restriction de droits. Il récupère les clés de chiffrement, les certificats SSL, les journaux de connexion et les scripts de configuration. Ces informations lui permettent de compromettre ultérieurement le serveur central ou de déchiffrer des échanges passés.

Mécanisme de défense : La solution réside dans la configuration du système de fichiers en mode lecture seule (Read-Only). Le système d'exploitation traite la carte SD comme un support immuable. Toutes les écritures nécessaires au fonctionnement, comme les fichiers temporaires ou les logs, sont redirigées vers une couche virtuelle en mémoire vive, ou RAM Overlay. Lors d'un redémarrage ou d'une coupure électrique, le contenu de la mémoire vive

s'efface instantanément. Le système repart toujours d'un état sain et aucune donnée sensible ne persiste sur le support physique.

2.3. Contournement de l'interface graphique

Le Raspberry Pi est censé n'afficher que le navigateur web en plein écran. Mais derrière, il y a tout un système d'exploitation.

Mécanisme de l'attaque : Si le navigateur crash ou si l'utilisateur connaît les raccourcis système comme Ctrl+Alt+F1 ou Alt+Tab, il peut faire disparaître le navigateur et accéder au bureau Linux ou à une invite de commande classique.

Conséquences : La fermeture de l'interface kiosque révèle le bureau du système d'exploitation sous-jacent. L'attaquant obtient un accès à l'environnement Linux, peut lancer un terminal et tenter d'élever ses privilèges pour prendre le contrôle total de la machine.

Mécanisme de défense : L'utilisation d'un gestionnaire de fenêtres minimaliste dépourvu de barre des tâches et de menu contextuel est judicieux. Les raccourcis clavier sont désactivés au niveau du serveur d'affichage. Un script de surveillance de type Watchdog contrôle en permanence l'exécution du processus navigateur. En cas de fermeture, accidentelle ou malveillante, le script relance immédiatement l'application, empêchant l'accès au système sous-jacent.

3. Analyse du Réseau de Transport Eduroam

Le réseau Wi-Fi Eduroam est sécurisé pour l'authentification, mais il reste un milieu partagé : les données circulent sous forme d'ondes radio que tout le monde peut capter. Cela expose le système à deux faiblesses majeures qui ne dépendent pas du code de l'application, mais de la nature même du Wi-Fi..

Sabotage actif : La déconnexion forcée

C'est une attaque de "Déni de Service" (DoS) très efficace sur le Wi-Fi, qui permet de couper la connexion d'un appareil sans même être connecté au réseau.

Mécanisme de l’attaque: Le protocole Wi-Fi utilise des commandes de gestion pour dire à un appareil "Déconnecte-toi". Sur beaucoup de réseaux, ces commandes administratives ne sont pas chiffrées. Un attaquant peut se faire passer pour l'antenne Wi-Fi (usurpation d'identité) et ordonner au Raspberry Pi de se déconnecter. Le Pi, croyant obéir à l'infrastructure officielle, coupe la connexion.

Conséquences : Un individu malveillant utilise un petit boîtier électronique facilement trouvable dans le commerce, caché dans l'amphi. Il le programme pour envoyer l'ordre

"Déconnexion" en boucle au vidéoprojecteur. L'image se fige et la connexion saute toutes les 10 secondes. Le cours devient impossible à assurer.

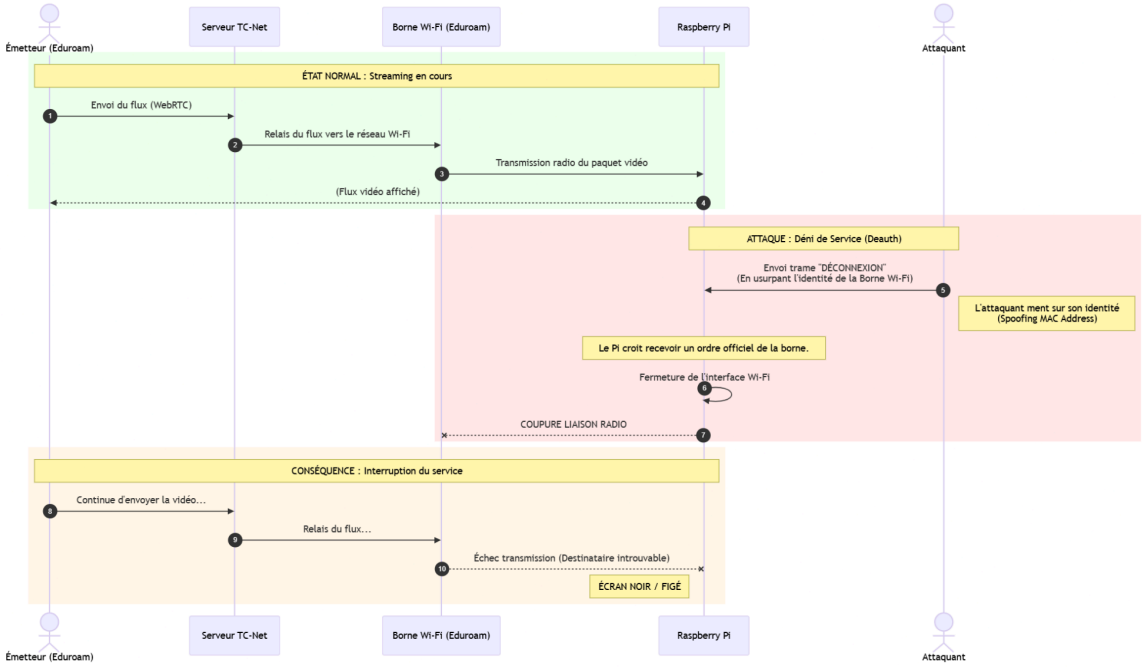


Diagramme de séquence du fonctionnement de l'attaque

Solution : On garantit la disponibilité du service dans les grands amphithéâtres en reliant le Raspberry Pi par un câble Ethernet, insensible à ces perturbations radio.

Note sur la protection native (802.11w) : Bien que la norme 802.11w (Protected Management Frames) permette théoriquement de contrer cette attaque en signant les ordres de déconnexion, son activation stricte sur le réseau Eduroam n'est pas garantie. Pour des raisons de rétrocompatibilité avec les anciens terminaux (Legacy Support), cette protection est souvent configurée en mode Optionnel ou désactivée. Par conséquent, le projet ne peut pas se reposer sur la configuration de l'infrastructure pour assurer sa disponibilité et doit envisager le pire scénario.

Conclusion

Cette analyse met en évidence la nécessité de compromis entre sécurité, simplicité d'usage et contraintes matérielles. L'analyse des vulnérabilités menée sur le système de diffusion vidéo montre que la robustesse du protocole WebRTC ne suffit pas à elle seule à garantir la sécurité d'un service déployé sur une infrastructure campus. Les vecteurs d'attaque les plus critiques se situent en périphérie du flux chiffré.

L'audit identifie deux failles majeures nécessitant une action prioritaire : l'exposition du serveur TURN qui transforme l'infrastructure en proxy ouvert sans authentification stricte et la vulnérabilité physique des boîtiers Raspberry Pi. Les risques de fuite de données liés à l'auto-déclaration des équipements mettent en évidence l'importance de maîtriser tous les éléments de la chaîne de diffusion en vérifiant l'identité de tous les appareils embarqués.

La mise en place du système ne pourra être validée qu'après l'application des mesures de durcissement préconisées : authentification par tokens éphémères sur les relais, chiffrement des supports de stockage et surveillance active des métadonnées réseau. Plutôt que de viser une sécurité absolue difficilement atteignable, les solutions proposées réduisent les attaques opportunistes tout en garantissant une expérience utilisateur fluide