Présentation de l'opération de R&D "Communications sécurisées"

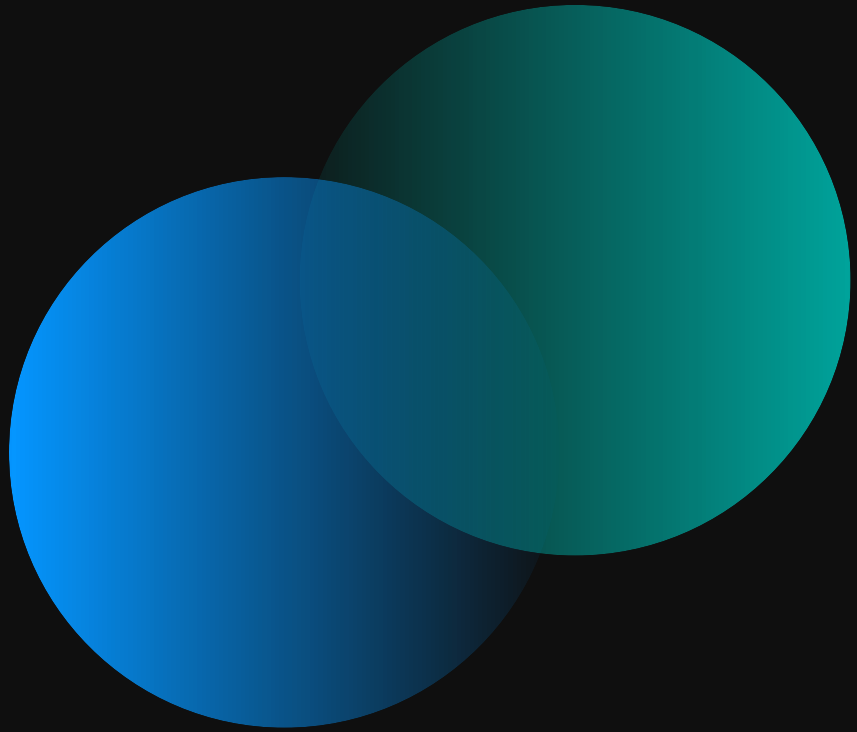
Crédit impôt recherche AVANTIX 2019 2020 2021

Amélie Hennequart
Devices & Infrastructure R&D manager
24/10/2022

Atos

Content overview

01. Objet de l'opération de R&D

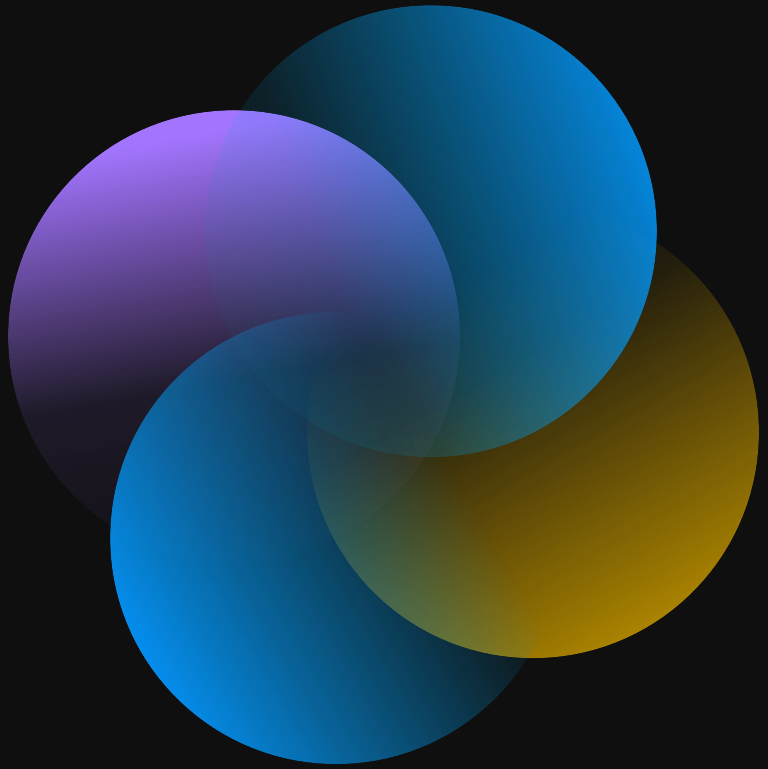


Objet de l'opération de R&D
Communications sécurisées

- Méthodologie de sélection de l'opération de R&D
  - Nos travaux consistent à exploiter les connaissances tirées de la recherche en sécurité des communications ainsi que de l'expérience pratique du Ministère des Armées pour concevoir des systèmes de communication sécurisée. Ils s'inscrivent donc directement dans une démarche de développement expérimental
  - « Le développement expérimental consiste en des travaux systématiques – fondés sur les connaissances tirées de la recherche et l'expérience pratique et produisant de nouvelles connaissances techniques – visant à déboucher sur de nouveaux produits ou procédés ou à améliorer les produits ou procédés existants. »

- Opération de R&D dans le cadre de l'activité de l'entreprise
  - Plateformes de développement de systèmes embarqués critiques faible consommation et durcis
  - Sécurisation des smartphones
  - Sécurisation des communications

02. Etat de l'art



Etat de l'art

Communication dans le domaine militaire

- Longtemps, les militaires ont été cantonnés à l'utilisation de radio militaires ou radio tactiques
  - Systèmes robustes (au niveau physique comme électromagnétique) et sécurisés (souvent CD)
  - Systèmes souvent assez anciens (cycle de développement longs et coûteux), très faible débit
  - Systèmes très coûteux car très souvent conçus spécifiquement pour l'armée (pas d'usage pour un autre marché)
  - Ergonomie et facilité d'utilisation parfois discutables

- Les usages (et les mentalités) ont évolué, ce qui impose la nécessité de modernier les équipements
  - Besoin de débits plus important : permet de nouvaux cas d'utilisation (messages, vidéo, positions amies/ennemies)
  - Compromis nouvelles technologies *vs* sécurité : Il n'y a pas forcément besoin de systèmes CD partout et tout le temps; la sur-sécurité tend à diminuer au profit de niveaux de sécurité mieux adapatés à chaque usage
  - Compromis technologies civiles *vs* coûts de systèmes dédiés
    - l'Etat ne souhaite plus payer 100% d'un développement aux industriels; les entreprises ont plutôt intérêt à travailler sur une base de technologie grand public et à en décliner plusieurs niveaux de sécurité
    - Les technologies civiles évoluent vite, ce qui permet de proposer de nouveaux usages régulièrement et une meilleure adoption par les jeunes recrues

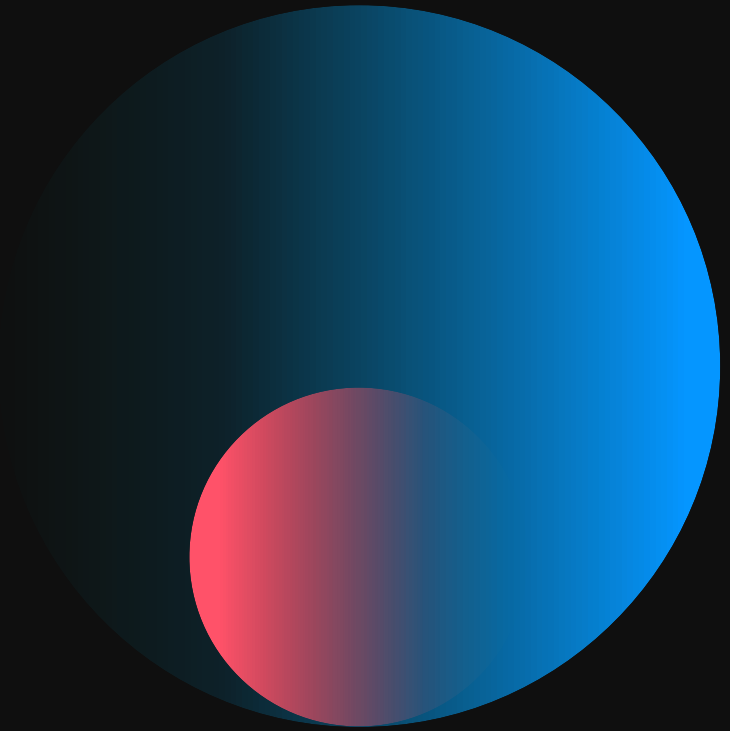
Etat de l'art

Sécurisation des systèmes et des communications

- Failles, vulnérabilités et attaques des terminaux Android
  - Il existe des failles et vulnérabilités à tous les niveaux (e.g. matériel, linux, applications)
  - Elles peuvent être intentionnelles (e.g. portes dérobées) ou la conséquence d'erreurs de codage ou de faiblesses dans l'architecture
  - De nombreux patchs de sécurité sont publiés chaque mois, certaines failles peuvent néanmoins subsister plusieurs années sans être corrigées

- La sécurisation : un renouveau permanent
  - En raison des nouvelles attaques mais aussi des nouvelles versions d'Android ou terminaux mobiles de différentes origines, la recherche de contre mesures est permanente et doit sans cesse être renouvelée
  - Il existe beaucoup de solutions de sécurité purement applicatives dont l'objectif est d'apporter une sécurité partielle au terminal mobile; il s'agit souvent de solution pour des flottes d'entreprise avec une gestion centralisée
  - Il existe aussi des applications permettant de sécuriser les communications mais souvent hébergées par des tiers ne pouvant pas être jugés de confiance notamment quand il y a un besoin de souveraineté (e.g. Whatsapp)
  - Mais il n'existe pas de solution combinant l'ensemble, c'est notre objectif

03. Verrous technologiques



Verrous technologiques

Sécurité des terminaux et des communications

- La sécurité parfaite n'existe pas!
  - Un enjeu clé est de prendre une longueur d'avance par rapport aux attaquants
  - Un autre défi est de mettre en place des mesures de sécurité adaptées aux scénarios d'attaques et à leur probabilité (il ne sert à rien de verrouiller la porte mais laisser la fenêtre ouverte), cela passe par une capacité à analyser finement et hiérarchiser les risques de sécurité
  - Il est nécessaire de respecter les principes de base en sécurité
    - Réduire la surface d'attaque, i.e. supprimer tout ce qui n'est pas nécessaire
    - Mettre en place plusieurs lignes de défense, ainsi si une barrière tombe, il y en aura une derrière et ainsi de suite; le but est de limiter l'impact d'une attaque voire le circonscrire
    - Accorder uniquement les droits et privilèges d'exécution nécessaires
    - Implémenter la sécurité en profondeur, i.e. ne pas se limiter à brider une interface au niveau applicatif mais favoriser la suppression pure et simple du code à plus bas niveau, ainsi pas possible de le réactiver
- Supporter des cas d'usage qui vont à l'encontre de l'utilisation standard (grand public) d'Android
  - Utiliser des produits grand public pour supporter des scénarios d'utilisation militaire impose d'être imaginatif
  - La complexité n'est pas nécessairement dans le développement mais plutôt dans la compréhension du fonctionnement d'Android pour arriver à le détourner pour répondre à nos exigences

Verrous technologiques
Hub

- Architecture matérielle du hub
  - Enjeux de miniaturisation : il n'existe pas de terminal aussi petit (dimensions d'un smartphones, deux fois plus épais) avec autant de fonctionnalités (deux modems LTE, deux chaines radio Device to Device, BT/Wifi, GPS)
  - Dissipation thermique et contraintes environnementales: volume très réduit pour dissiper la température, est utilisé tenu en mains donc ne doit pas être trop chaud (un boitier métallique serait plus facile pour la dissipation)
  - Consommation énergétique et puissance d'émission: un compromis est à définir entre les performances en termes de portée et de débit ainsi que l'autonomie de la batterie

- Architecture et enjeux du Device to Device
  - Les devices sont mobiles et se déplacent de façon non prédictible, ce qui implique que le réseau doit se reconfigurer automatiquement en permanence
  - Compromis entre la portée (le réseau sera plus ou moins étendu) et le débit (suivant que l'on veut passer de la voix de faible qualité ou de très bonne qualité, des messages voire de petits fichiers).
  - Sécurité des communications: ne doit pas impacter les performances

04. Travaux accomplis en 2019

Axes de recherche
Présentation générale

- Axe n°1: Développement d'un dispositif de communication sécurisée adapté au champ de bataille
  - Enjeu majeur: Procédure de sécurisation des terminaux de manière native et/ou applicative
  - Nos travaux nous permettent d'assurer la communication dans un environnement militaire de manière sécurisée

- Axe n°2: Conception d'un dispositif de communication sécurisée pour la défense du territoire national
  - Nos travaux nous ont permis de développer un dispositif de routage performant et adapté aux contraintes opératoires du domaine militaire

Axe n°1 - Introduction

Développement d'un dispositif de communication sécurisée adapté au champ de bataille

- Le SICS est un système d'information et de commandement unique qui équipera les nouvelles plateformes de l'armée de terre. Il permet de partager numériquement, et de manière sécurisée, l'ensemble des informations tactiques disponibles sur le champ de bataille.
- SICS débarqué est l'application du SICS sur le champ de bataille. Nos travaux se sont articulés autour de 3 enjeux :
  - La sécurisation des terminaux SICS débarqué
  - La connectivité de ces terminaux
  - Le développement d'un Outil de Gestion de Flotte (OGF) afin de pouvoir configurer et faciliter la gestion de ces équipements
- L'objectif de ces travaux en terme de sécurité est d'homologuer les terminaux au niveau diffusion restreinte (DR) puis Nato Restricted (NR). Cela implique de respecter des règles et exigences strictes

Axe n°1 - Sécurisation des terminaux SICS Débarqué

Développement d'un dispositif de communication sécurisée adapté au champ de bataille

- Depuis plusieurs années, nous travaillons sur de la sécurisation à très bas niveau, à partir du bootloader (avec modification du code natif); le terminal cible ne permettant pas de faire cela, une étude a été nécessaire pour identifier les mesures à implémenter pour réaliser une sécurité uniquement applicative. C'est un changement total de paradigme pour nos ingénieurs
- Afin d'atteindre un niveau de sécurité suffisant, il est nécessaire de réfléchir à la combinaison de plusieurs solutions - qui seules auraient pu s'avérer trop faibles
- Un cycle de vie du terminal a été défini avec des actions autorisées ou non en fonction des états, ceci étant lié au niveau de sécurité; toute cette logique n'existe absolument pas dans Android
- Ce qui a été mis en place
  - Dès le démarrage du terminal, il fallait éviter que son usage puisse être détourné; ainsi un genre de surcouche a été développée afin de limiter les usages et possibilités au strict nécessaire
  - Mise en place de journaux de sécurité, d'un code de démarrage, d'une politique de sécurité
  - Blocage de tous les ports et périphériques: Bluetooth, Wifi, USB…
  - Mise en place de comptes administrateur et opérateur avec des droits en fonction des états du cycle de vie
  - Effacement d'urgence avec un effacement « à la carte » de certaines données et pas d'autres

Axe n°2 - Connectivité des terminaux

Développement d'un dispositif de communication sécurisée adapté au champ de bataille

- Nous devions assurer la connexion des terminaux avec des équipements extérieurs tels que l'ERR (équipement de raccordement radio) et le MIR (module d'interface radio)
- L'enjeu était d'autoriser la connexion des terminaux uniquement avec ces équipements donc de façon très restreinte afin d'assurer la sécurité du système

- C'est dans ce cadre que nous avons recherché et développé plusieurs services de connexion :
  - Gestion du lien USB sécurisé (MIR/SICSD, ERR/SICSD), pour échange des données liées à l'appairage filaire : ce besoin est couvert par le service « USB IP »
  - Gestion du lien Bluetooth ERR/SICSD : cela concerne uniquement l'appairage, mis en œuvre lors de la connexion USB ERR/SICSD. Ce besoin est couvert par le service « Authentification/appairage ERR »
  - Gestion du lien Wifi Sécurisé (SICSD/SICSD) ; abordé succinctement en 2019, réalisé en 2020

Axe n°1 - Outil de gestion de flotte

Développement d'un dispositif de communication sécurisée adapté au champ de bataille

- L'outil que nous avons développé est le fruit d'un travail de recherche qui consistait à trouver un moyen de contraindre un maximum les opérations de mises à jour, manipulation des données par les terminaux SICS débarqué afin de garantir leur sécurité et restreindre les pouvoirs administratifs sur ces derniers
- L'une des difficultés rencontrées était de parvenir à paralléliser certaines actions pour avoir un gain de performance et simplifier l'utilisation de l'outil. Nous avons déterminé que la parallélisation des processus était bénéfique pour la plupart de nos fonctionnalités à savoir
  - La sauvegarde des journaux de sécurité
  - La sauvegarde des données des terminaux
  - Le chargement des données de configuration
  - L'installation, la désinstallation et la mise à jour des applications Android
- Une difficulté importante concernait l'interruption d'une action en cours (il s'agissait d'éviter que les terminaux se retrouvent dans un état non maitrisé)
  - le choix a été fait de garantir l'intégrité des données et toujours finaliser une tâche même en cas d'annulation au cours de celle-ci

Axe n°2 - Introduction

Conception d'un dispositif de communication sécurisée pour la défense du territoire national

- L'objectif du projet Auxylium est d'équiper les soldats d'un matériel de communication performant et sécurisé dans le cadre de la défense du territoire national, un premier déploiement a eu lieu en 2016
- Nous avons lancé une nouvelle phase de recherche et développement en 2019
- le système Auxylium est basé sur l'association de deux appareils : le terminal avec lequel interagit l'opérateur et le boitier Helium qui est un hub réseau permettant de se connecter de manière sécurisée avec les réseaux 4G publics et privés, avec des radios militaires ou de proposer un réseau D2D

- Le travail effectué porte principalement sur le dispositif réseau qui permet de relier le téléphone sécurisé à l'infrastructure Auxylium nommé Helium. Nos travaux se sont articulés autour de 3 enjeux pour le dispositif Helium
  - Amélioration de l'autonomie
  - Amélioration des caractéristiques mécaniques et thermiques
  - Changement de l'architecture Hardware et conception/développement du logiciel associé

Axe n°2 - Améliorations sur l'autonomie et la robustesse mécanique

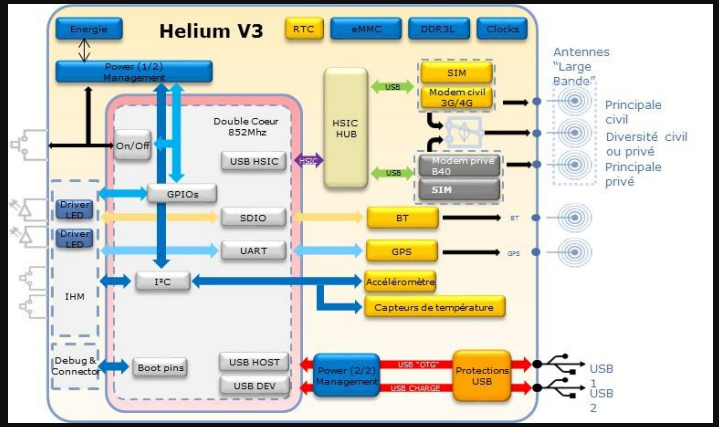
Conception d'un dispositif de communication sécurisée pour la défense du territoire national

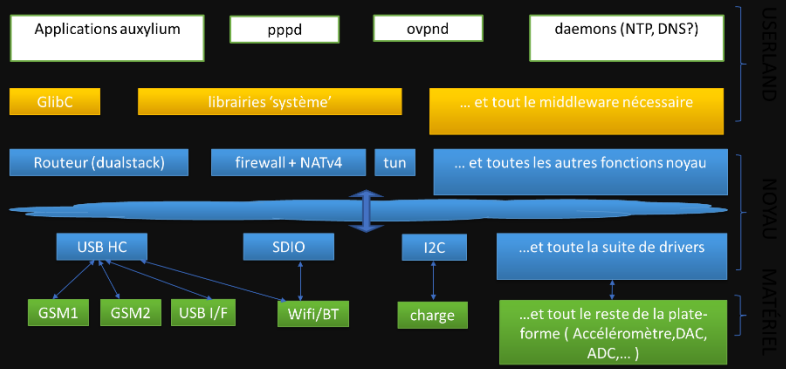
- Amélioration de l'autonomie
  - Désactivation des fonctions inutilisées du CPU (e.g. audio, GPU), blocs mémoires mis en mode low power
  - Ajout de deux fréquence de fonctionnement des cœurs du processeur afin de réduire la puissance consommée: 198MHz et 99MHz correspondant à la moitié et au quart de la fréquence initiale
    - Aucune documentation constructeur n'existait
    - A requis une analyse détaillée de la puissance CPU nécessaire à un bon fonctionnement ainsi qu'une validation intensive
- Amélioration des caractéristiques mécaniques et thermiques
  - Axes sur lesquels il nous est demandé de proposer des solutions par rapport à une précédente version
    - Manque de robustesse mécanique: casse des connecteurs USB et des boutons, pas de support aux chutes, non étanche
    - Montée trop rapide en température rendant l'utilisation inconfortable (présence d'une ceinture métallique)
  - Phase de recherche et choix réalisés
    - Boitier mécanique fait de polycarbonate chargé en fibre de verre à hauteur de 10% recouvert d'un élastomère thermoplastique (TPE); ajout de « silent-blocs » entre le boitier et la carte électronique pour réduire l'impact des chocs. Utilisation de connecteurs militaires. Joint d'étanchéité. Pastille en tissu pour l'équilibre des pressions intérieur/extérieur.
    - Conception d'une plaque d'aluminium recouvrant 61% de la surface. Mise en place de mousse de dissipation thermique entre cette plaque et les capots de blindages présents sur les composants. Il s'agit d'assurer la continuité de la transmission de la chaleur jusqu'à l'extérieur du boitier. Mise en place de sondes de température pour assurer un contrôle en continu

Axe n°2 - Nouvelle architecture du boitier Helium

Conception d'un dispositif de communication sécurisée pour la défense du territoire national

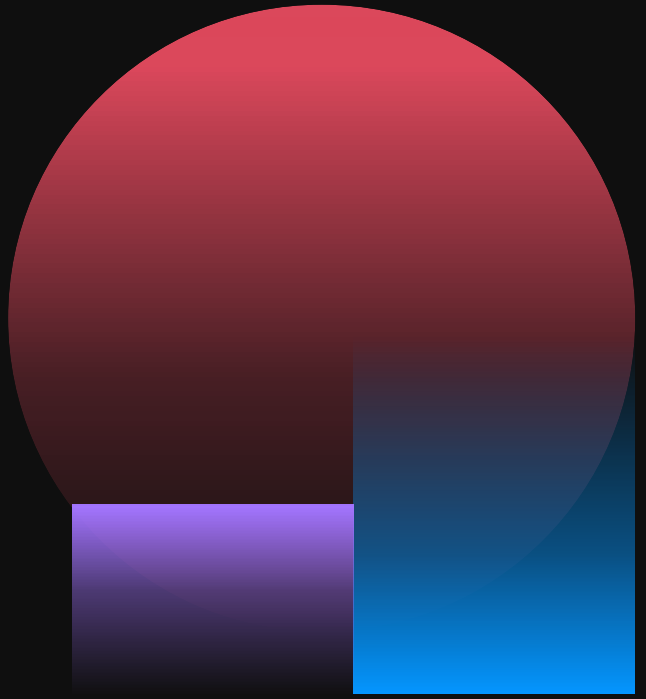
- Conception complète d'un nouvelle carte électronique
  - Contraintes : dimensions, robustesse, pérennité à 10 ans (impose une maitrise de l'ensemble de la carte)
  - Phase d'étude menée pour faire le choix des composants: tableaux de choix, analyse technique
  - Etude particulièrement approfondie sur le processeur, les modems, les mémoires et le Bluetooth





- Nouvelle architecture du logiciel
  - Version précédente sur Android mais peu adapté à un usage de type routeur réseau
  - Choix de concevoir notre logiciel sur une architecture basée sur BuildRoot, tout à fait adapté pour des systèmes embarqués (ayant par définition des contraintes de temps d'exécution et de mémoire)

05. Travaux accomplis en 2020



Axes de recherche
Présentation générale

- Axe n°1: Développement d'un dispositif sécurisé d'échange de fichiers sur le champ de bataille
  - Dans la continuité des travaux de 2019 sur les dispositifs de communication sécurisée adapté au champ de bataille
  - Nos travaux nous permettent donc d'assurer l'échange d'informations stratégiques dans un environnement militaire de manière sécurisée.

- Axe n°2 : Mise en place d'un réseau de communication D2D (Device to Device) avec les boitiers hubs Helium
  - Nos travaux nous ont permis de développer et valider la mise en place d'un réseau D2D dans un environnement opératoire militaire.

Axe n°1 - Dispositif sécurisé d'échange de fichiers par Wifi

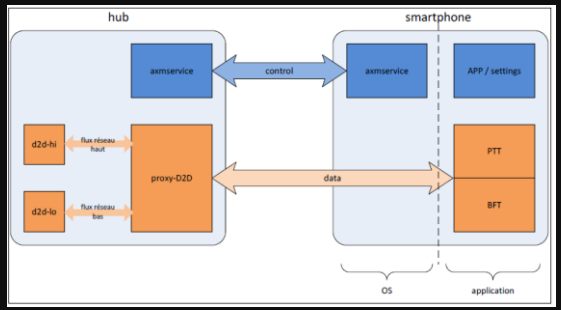
Développement d'un dispositif sécurisé d'échange de fichiers sur le champ de bataille

- Le SICS est un système d'information et de commandement unique qui équipera les nouvelles plateformes de l'armée de terre. Il permet de partager numériquement, et de manière sécurisée, l'ensemble des informations tactiques disponibles sur le champ de bataille.
- SICS débarqué est l'application du SICS sur le champ de bataille
- Nos travaux se sont concentrés sur l'échange de données entre deux terminaux SICS Débarqué en Wifi. Le Wifi est généralement banni quand on parle de sécurité.
  - Une analyse des risques de sécurité a été réalisée afin de hiérarchiser les risques et se concentrer sur les plus importants pour identifier des contre mesures techniques, parfois associées à des mesures opérationnelles
  - Un enjeu non négligeable était aussi de parvenir à implémenter cette solution sans venir à l'encontre des mécanismes de sécurisation mis en place en 2019 (qui – entre autres – interdisaient l'usage du Wifi)
- Solution mise en œuvre
  - Basée sur Wfi Direct (permet de connecter des devices sans passer par un point d'accès) et l'API WifiLocalOnlyHotspot (nécessitant l'échange d'une pre-shared key pour autoriser la connexion)
  - Plusieurs possibilités ont été étudiées pour l'échange transparent de cette pre-shared key dont l'USB; nous nous sommes heurtés aux limites d'Android (sans modification du code natif) et n'avons pu réaliser ce que nous voulions; cet échange est donc finalement réalisé manuellement

Axe n°2 – Contexte et architecture générale

Mise en place d'un réseau de communication D2D (Device to Device)

- Contexte
  - Ce type de réseau est essentiel pour le bon déroulement de certaines missions notamment lorsque les réseaux publics sont coupés ou lorsque leur utilisation est impossible par rapport au terrain d'intervention (e.g. sous-sols)
- Architecture fonctionnelle
  - Groupes de communication organisés de façon hiérarchique (usage militaire en priorité)
  - Deux groupes doivent fonctionner en parallèle (communication avec hiérarchie ou pairs + avec subordonnées)
- Topologie réseau
  - Un groupe de communication peut être vu comme un réseau local IP (LAN), chaque hub ayant une adresse IP
  - Un groupe est caractérisé par un canal radio et une adresse réseau
- La communication est gérée et administrée par le hub Helium et le téléphone selon 2 plans
  - Le plan de contrôle pour contrôler et configurer le réseau D2D
  - Le plan de données pour diriger les flux BFT (blue force tracking) et PTT (push to talk) vers les interfaces radio dédiées



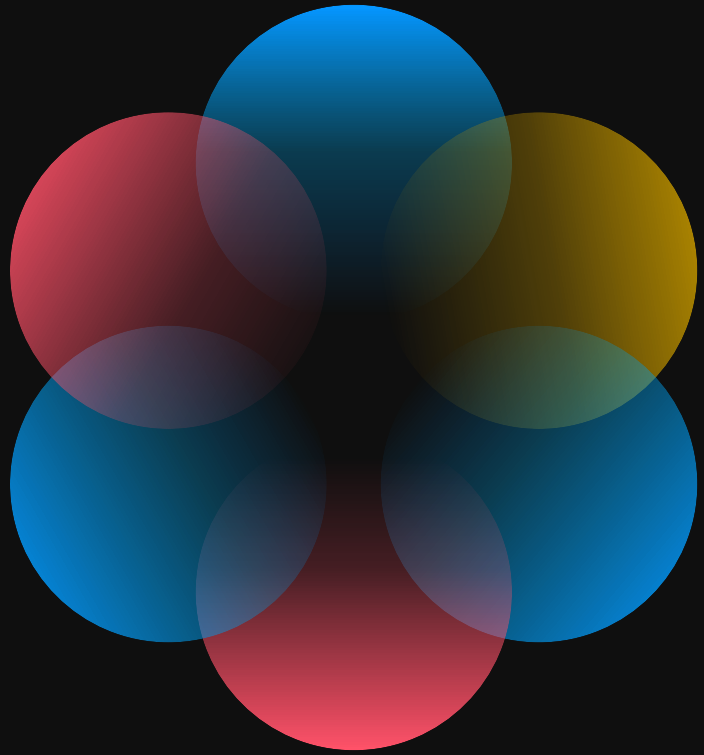
Axe n°2 – Exigences relatives à la conception du bloc radio

Mise en place d'un réseau de communication D2D (Device to Device)

- Exigences pour la conception du bloc radio logiciel (exécution du code au niveau transceiver efr32)
  - Doit pouvoir être paramétré de façon autonome ➔ développement d'une API permettant de régler les paramètres
  - Doit consommer peu de ressources CPU ➔ impacte l'architecture
  - L'adhérence à l'architecture matérielle doit être aussi limitée que possible ➔ impacte l'architecture
  - Performances: portée et débit comparables à des radios militaires
  - Sécurité: les données doivent être protégées en confidentialité (chiffrement) et en intégrité (signature)
- Intégration dans une architecture logicielle existante (exécution du code sur processeur principal)
  - Enrichissement du processus applicatif amxdaemon qui était déjà en place dans le hub
  - Développement d'un nouveau module gérant trois plans : contrôle, données, traces
    - Le sous-module D2D TRACES récupère les payloads des paquets de trace et les envoie directement au logger
    - Le sous-module D2D CTRL manipule les paquets relatifs au plan de configuration en fonction des requêtes entrantes.
    - Le sous-module D2D DATA manipule les paquets relatifs au plan de données
  - Le multiplexage / démultiplexage de ces plans - ainsi que le formatage et la désencapsulation des paquets - est effectué par le sous-système packetizer/depacketizer dont l'essentiel du travail est de manipuler les paquets D2DPKT à la granularité de l'octet

➔Les tests automatiques en simulation comme les tests terrain ont montré de bons résultats

06. Travaux accomplis en 2021



Axes de recherche
Présentation générale

- Axe n°1: Développement, amélioration et sécurisation des communications pour le système Auxylium

- Axe n°2 : Développement d'un système de communication stratégique pour le champ de bataille

- Axe n°3: Sécurisation de terminaux mobiles (MOBS et Hoox)

Axe n°1 – Stabilité et performance du lien Bluetooth

Développement, amélioration et sécurisation des communications pour le système Auxylium

- Des problèmes opérationnels relatifs à la stabilité du lien Bluetooth entre le smartphone et le boitier Helium nous ont contraint à engager des travaux de R&D pour
  - Caractériser les problèmes
  - Proposer des solutions adaptées au contexte d'utilisation
- Caractérisation des problèmes
  - Perte de connexion entre les deux terminaux ➔ provoquée par un crash du composant Bluetooth du boitier
  - Problème de qualité des communications (surtout ressenti avec du Push to Talk et de la video) ➔ lié à des problèmes de latence, débit et pertes de paquets, en partie aussi liés à des interférences entre terminaux
- Identification et mise en place de solutions
  - Travail avec le fournisseur du composant Bluetooth (composant supportant Wifi, Bluetooth et Bluetooth Low Energy). Nous utilisons uniquement le Bluetooth standard et dans un mode particulier (BT-PAN) ➔ des correctifs au niveau du firmware du composant + logiciel du boitier ont permis de résoudre les pb de connexion
  - La qualité de la liaison Bluetooth est améliorée par
    - La diminution de la puissance d'émission du smartphone et un éloignement des deux devices qui peuvent « s'éblouir »
    - La mise en place d'une priorité sur les flux UDP (voix) par rapport aux flux TCP (fichiers) via marquage des paquets + iptables
    - Des optimisations sur chaque file (queue) de la chaine Bluetooth du smartphone pour éviter des engorgements

Axe n°1 – Mise en place du Wifi à la place du Bluetooth

Développement, amélioration et sécurisation des communications pour le système Auxylium

- La série d'optimisations réalisées sur la liaison Bluetooth a été insuffisante pour faire passer de la vidéo dans de bonnes conditions (besoin de débit et faible latence)
- Le choix a donc été fait de remplacer la liaison Bluetooth par une liaison Wifi, avec des contraintes
  - La portée importante du Wifi est en opposition avec notre volonté de créer un lien wifi discret et sécurisé entre le smartphone et le boitier Helium
  - Ce lien de communication s'inscrit dans un système contraint en termes de consommation énergétique
- Ce qui a été réalisé
  - Analyse des risques de sécurité liés à l'utilisation du Wifi
  - Etude des solutions techniques avec compromis sécurité / efficacité / consommation énergétique
  - Développements
    - Mode Access Point sur le boitier Helium avec échange de clés par connexion USB entre les équipements
    - 2,4GHz car 5GHz est trop consommateur
    - Diminution de la puissance d'émission pour ne pas rayonner au-delà de 10 mètres
    - Tests de consommation: courant moyen consommé en Wifi est de 177mA contre 152mA en BT ➔ 16% de conso suppl.
    - Tests en environnement fortement exposés au réseau Wifi ➔ la solution n'est pas perturbée

    ➔ Gain en stabilité et performances, impact sur la consommation énergétique acceptable

Axe n°1 – Amélioration de la sécurité du Wifi par un surchiffrement

Développement, amélioration et sécurisation des communications pour le système Auxylium

- Le Wifi est chiffré en WPA2 par défaut; néanmoins nous avons souhaité apporter une sécurisation supplémentaire dans le cas où des vulnérabilités sur le Wifi seraient exploitées

- Exigences à respecter
  - Limiter l'impact sur le reste du système (i.e. ne pas imposer des développements supplémentaires)
  - Rapidité de mis en œuvre
  - En profiter pour ajouter ce niveau supplémentaire de sécurité sur l'ensemble des liens radio
- Plusieurs solutions ont été étudiées et considérées
  - Passage du chiffrement WPA2 à WPA3
  - Chiffrement applicatif
  - Tunneling SSH
  - Proxyfication TCP
  - Déploiement d'un VPN lien-local ➔ solution choisie; chiffrement à base d'AES-256-CBC

Axe n°1 – Chiffrement des données passant sur le D2D

Développement, amélioration et sécurisation des communications pour le système Auxylium

- Il est nécessaire de mettre en œuvre un moyen cryptographique pour protéger le trafic D2D en confidentialité (sinon n'importe quel ennemi pourrait écouter les échanges)
- Exigences sur le cryptosystème
  - Il ne doit pas impacter le réseau déjà en place (i.e. pas d'overhead sur les paquets)
  - Il reposera sur une clé secrète pré-partagée entre les membres d'une flotte donnée
  - Le chiffrement n'est pas réalisé par le chipset radio (efr), les ressources étant trop limitées
- Ce qui a été réalisé
  - La contrainte de ne pas augmenter la taille des paquets est importante, elle empêche la mise en place d'un canal de contrôle qui permettrait de gérer un état cryptographique complexe (e.g. utilisation de clés éphémères)
  - Développement d'un chiffreur/déchiffreur basé sur AES 256
  - Plusieurs schéma de clé ont été étudiés, celui finalement retenu est CTR qui présente des avantages
    - La compromission d'un bloc ne compromet pas l'ensemble
    - Moins gourmand en temps de calcul que d'autres schémas

➔La radio D2D a été validée par une série de tests de robustesse. La solution est ainsi performante et sécurisée ; néanmoins des optimisations sont toujours à apporter, ce sera l'un des axes 2022

Axe n°2 – Evaluation de l'utilisation d'un nouveau terminal mobile

Développement d'un système de communication stratégique pour le champ de bataille

- Le SICS est un système d'information et de commandement unique qui équipera les nouvelles plateformes de l'armée de terre. Il permet de partager numériquement, et de manière sécurisée, l'ensemble des informations tactiques disponibles sur le champ de bataille.
- SICS débarqué est l'application du SICS sur le champ de bataille

- Echange de fichiers par Wifi
  - Finalisation de l'intégration système du mécanisme de partage de fichiers par Wifi entre deux utilisateurs ; avec comme préoccupation prioritaire de ne pas impacter l'architecture logicielle existante
- Etude d'une nouvelle plateforme (sans accès au code source)
  - Passage de Android 8 à Android 11: importants changements d'architecture au niveau Android
  - Passage d'une tablette Huawei à Samsung: les constructeurs modifient une partie du code, c'est notamment le cas de Samsung qui développe une surcouche complètement propriétaire et intervient aussi sur les couches basses

  ➔Ces deux éléments nous imposent de repenser complètement les développements réalisés jusque là et identifier quelles adaptations voire reprises sont nécessaires; la suite sera réalisée en 2022

Axe n°3 – Des niveaux de sécurité en fonction des usages

Sécurisation de terminaux mobiles (MOBS et Hoox)

- La solution Hoox est une solution de communication sécurisée souveraine avec son propre serveur et ses téléphones Hoox nativement sécurisés
- Les premières briques datent de 2012 et ont été la base dans les années qui ont suivi d'études réalisées dans le cadre de projets comme Auxylium et SICS Débarqué, essentiellement pour la partie « sécurisation du téléphone »

- L'enjeu ici est de réaliser des travaux en vue de développer un téléphone Hoox sur base Android 11 et aussi de tirer profit des études réalisées dans les années précédentes et donc proposer un niveau de sécurité adapté aux besoins
  - Ainsi une sécurité au niveau applicatif (proche de SICS Débarqué) convient dans la majorité des cas de B2B
  - Alors qu'une sécurité à beaucoup plus bas niveau est nécessaire pour une utilisation stratégique; cela correspond à ce qui est étudié dans le cadre du projet MOBS

Axe n°3 – Travaux exploratoires visant un haut niveau de sécurité

Sécurisation de terminaux mobiles (MOBS et Hoox)

- L'exigence principale sur MOBS est d'apporter le niveau de sécurité le meilleur possible sur un téléphone grand public
- L'enjeu sera de déterminer si ce niveau de sécurité est suffisant pour traiter du secret
  - Il s'agit d'éviter de développer des smartphones dédiés à la gestion du secret, cela représente des coûts très conséquents et des délais de plusieurs années (avec des produits quasi obsolètes lors de leur 1er déploiement)
- Les travaux de recherche se sont concentrés sur deux concepts à explorer
  - Nous avons recherché comment imbriquer un second VPN sur la couche de sécurité existante.
  - Nous avons ensuite exploré les possibilités que nous offrait la trust zone du processeur ARM en termes de sécurité.
- Ce qui a été réalisé
  - Etude des travaux de la NSA abordant les surcouches de sécurité de façon conceptuelle, l'idée principale est d'utiliser deux tunnels VPN imbriqués puis essai de faire passer tous nos flux déjà chiffrés (de nos travaux sur le projet Hoox) par un deuxième tunnel VPN basé sur IPsec.
  - Etude de l'architecture du SoC Mediatek ainsi que du moyen de remplacer la TEE (Trusted Exécution Environment) de Mediatek par une TEE maitrisée par Atos; le gain pour la sécurité du système serait très conséquent
  - Etude du preloader et bootloader, des périphériques gérables en TEE, des domaines de sécurité

➔les travaux visant à atteindre une sécurité de très haut niveau seront poursuivis en 2022

Questions

Thank you!

For more information please contact:
M+ 33 6 63 84 29 87
amelie.hennequart@atos.net