Compte-rendu
Atelier Smart cities – Safe cities

Animateur

Christian AGHROUM
Président de SoCoA, Vice-président de CyAN

Participants

Patrick CHAMBET
CESIN

Fabien GERMAIN
ENGIE INEO DEFENSE

Patrick CHAMBET
CESIN

M. Chambet rappelle que les objectifs de la Smart city sont de générer des services innovants et économes au territoire, développer et susciter une croissance économique locale, diffuser les principes de la Smart city aux populations (collecte des déchets ou usages des applications mobiles), avoir une plateforme collaborative. Il s'agit de gagner en efficience et en qualité environnementale.

Les capteurs urbains se rapprochant de l'IoT (Internet Of Things) utilisés soulèvent différents questionnements, relativement :

- Aux moyens de collecte mis en œuvre (bluetooth, radio, NtoN), ainsi que le stockage des données dans les *datacenters* ;
- L'usage fait de ces données collectées ;
- L'*hypervision urbaine* (par la création d'alertes et une cartographie) et son application pour les citoyens.

En parallèle de cela, il existe une notion d'*open datas* qui sont disponibles et accessibles à tous sur la plateforme.

« Les objectifs de la Smart city sont de générer des services innovants et économes au territoire, développer et susciter une croissance économique locale. Il s'agit de gagner en efficience et en qualité environnementale. »

Pour comprendre la Smart city, il faut comprendre la multiplicité des capteurs, par exemple pour les place de parking, le trafic routier, des lampadaires pour moduler l'éclairage en fonction des présences humaines, des capteurs de qualité de l'air sur les véhicules de la mairie...
Plusieurs domaines sont touchés : assainissement, Gestion Technique des Bâtiments (GTB), circulation, signification des citoyens sur des problèmes pouvant être résolus par la mairie (objets cassés), données météos, des données du tourisme (chambres réservées)...
Tout cela alimente l'hyperviseur (une cartographie géographique avec des alertes et différents calques), et l'IOC (*Intelligent Operation Center*) qui s'occupe de tout cela.

Concernant la sécurité, c'est la rencontre de nombreux dispositifs. Il faut arriver à faire dialoguer les acteurs afin de parvenir à la sécurité, car sans sécurité des informations échangées et stockées, il ne peut y avoir de Smart cities. Cela implique des contraintes, les capteurs devant toujours être disponibles, ainsi que leurs systèmes de gestion et de pilotage. La sous-traitance sur ces sujets engendre parfois un scepticisme. Chaque capteur a une ID unique pour éviter les capteurs pirates, afin d'instaurer et d'assurer la confiance dans les données remontées, certaines données étant en effet assez sensibles (même s'il y a assez peu de données nominatives). Il existe néanmoins des appartements pilotes dont les propriétaires sont volontaires et dont les données sont anonymisées.

Par exemple, un capteur routier a une batterie intégrée de 8 à 10 heures d'autonomie. Cette autonomie limitée implique pour le capteur de faire le minimum, donc peu d'opérations, dont aucun chiffrement. Autre exemple, Nice a une benne intelligente, qui émet une alerte dès qu'elle atteint ses 100% de capacité, pour venir être collectée. Cela rentre dans ce que l'on appelle le Monitoring Urbain Environnemental. Nice s'attache à pouvoir favoriser les interconnections et le chiffrement des protocoles (via les protocoles LoRa et Sigfox notamment). On utilise des serveurs d'accueil pour les prestataires. Il existe aussi des applications web à protéger afin d'éviter la fuite de données.

« Ce qu'il faut comprendre, c'est que la cybersécurité ne doit pas gêner la circulation des données, mais bien accroître la confiance. »

La protection des équipements est importante en raison de leur pluralité physique ou technologique : les mots de passe par défaut sont bien sûr à proscrire (certaines caméras ont déjà été hackées). L'anonymisation des données a lieu dès que cela est possible.

Il y a un débat sur le Cloud dans l'administration : la note d'information d'avril 2016 est une note administrative décrétant illégal le stockage d'informations de la part de toute administration dans un Cloud qui ne serait pas souverain. Pour l'être, il faut un *datacenter* en France, avec du personnel français, et ce dernier doit être accrédité par l'ANSSI. Il faut préparer également la gestion de crise de la Smart city, car pour le moment celle-ci reste traditionnelle. Il faut aussi sensibiliser les partenaires à la sécurité (Schneider Electric, les fabricants d'IoT, etc.). Les dernières versions de produits comprennent des paramètres de sécurité.

« Il faut arriver à faire dialoguer les acteurs afin de parvenir à la sécurité, car sans sécurité des informations échangées et stockées, il ne peut y avoir de Smart cities. »

Ce qu'il faut comprendre, c'est que la cybersécurité ne doit pas gêner la circulation des données, mais bien accroître la confiance.

Fabien GERMAIN
ENGIE INEO DEFENSE

Evolution de la menace sur la Smart city. La vie personnelle quotidienne (ou la vie au travail) repose sur un/des réseau(x) de services. Ce sont ces réseaux de service qu'il faut améliorer, pour permettre de développer l'attractivité. La massification des réseaux augmente la surface pouvant être la cible d'attaque avec des ricochets, la menace devient ainsi plus globale.

« La centralisation des données permet d'appréhender une attaque globale, et permet une certaine efficacité. Il s'agit par là de ne pas passer outre divers signaux faibles, afin de coordonner les actions. »

Il y a une convergence technologique qui s'opère, ce qui permet un développement des services ; mais cette convergence permet aussi une multiplication et une forte diversification des attaques. Face à ce risque, Engie préconise une forte sensibilisation. Des exemples de menace qui pourrait être critique pour une ville : une attaque contre les services d'assainissements ; ou encore une attaque contre les panneaux d'une ville, pour détruire sa réputation. On peut aller jusqu'à une entreprise faisant de l'énergie locale, une entreprise sous domination étrangère pouvant, par exemple, en cas de conflits entre un pays tiers et la France (si l'on prend l'exemple de la France par exemple), couper la production et l'accès à l'énergie.
Un autre problème est la diversité des données qui entraînent des législations différentes.

Christian AGHROUM
SoCoA

La Gouvernance de la Smart city est aussi une autre problématique. La gouvernance est-elle globale ? Et est-elle légitime ?
Il faut comprendre que la centralisation des données permet d'appréhender une attaque globale, et permet une certaine efficacité. Il s'agit par là de ne pas passer outre divers signaux faibles, afin de coordonner les actions.

« La massification des réseaux augmente la surface pouvant être la cible d'attaque avec des ricochets, la menace devient ainsi plus globale. »

Se pose aussi la question des intérêts qu'auraient des criminels à hacker une Smart city. Cette dernière pourrait servir à indiquer la présence d'individus à certains endroits (donc à repérer un cambriolage en cours) ; on peut envisager une stratégie de rançonnage sur les *datacenters*.
Ce que recouvre le concept de la « Safe city » ne s'applique pour le moment qu'à la sécurité des données recueillies, pas encore à la Smart city en tant que telle (sécurité des capteurs composant la Smart city). Pour comprendre tous les enjeux de la Smart city, lire le magazine *Smart city mag.*

CE QU'IL FAUT RETENIR

⧫ Les objectifs de la Smart city sont de générer des services innovants et économes au territoire, développer et susciter une croissance économique locale. Il s'agit de gagner en efficience et en qualité environnementale.

⧫ Il faut arriver à faire dialoguer les acteurs afin de parvenir à la sécurité, car sans sécurité des informations échangées et stockées, il ne peut y avoir de Smart cities.

⧫ Ce qu'il faut comprendre, c'est que la cybersécurité ne doit pas gêner la circulation des données, mais bien accroître la confiance.

⧫ La massification des réseaux augmente la surface pouvant être la cible d'attaque avec des ricochets, la menace devient ainsi plus globale.

⧫ La centralisation des données permet d'appréhender une attaque globale, et permet une certaine efficacité. Il s'agit par là de ne pas passer outre divers signaux faibles, afin de coordonner les actions.