IUT de Lannion–Département Informatique

PPP–Projet de S1

OBJETS CONNECTÉS LA SÉCURITÉ, LA CONFIDENTIALITÉ

Romain BUNEL
Moussa MAHAMAT ADJI
Groupe H2

Table des matières

I. Outils utilisés

1. Phase de documentation / de veille

Les principaux moteurs de recherches que nous avons été amenés à utiliser sont les suivants:

- Google France
- Bing
- DuckDuckGo
- Qwant

Nous avons également utilisé un agrégateur de flux RSS: Feedly. Celui-ci nous a permis de regrouper nombreux articles concernant les objets connectés. Ceux-ci sont listés dans la partie Référence/Sources, à la fin du rapport.

2. Phase de réalisation

Nous avons utilisé les outils proposés par Google Drive tels que Google Doc ,Google Drawing(pour le rapport), Ninja Mock(pour le maquettage), kobra.io(pour codage html/css en ligne) afin de réaliser nos différents travaux collaboratifs.

3. Mots clés

Les principaux mots clés auxquels nous avons eu recours sont les suivants:

- Objets connectés
- Objets connectés danger
- Sécurité objets connectés
- Objets connectés fiables ou vulnérables
- Objets connectés cryptographie

Nous avons utilisés les opérateurs logiques afin de raffiner nos recherches.

4. Répartition des tâches

Avant d'entreprendre ce projet, nous avons réparti les tâches en fonction de nos compétences personnelles et de nos envies, afin de pouvoir assurer la meilleure des coordinations dans notre travail.

Sachant que nous ne sommes que deux dans notre sous équipe pour la réalisation de ce projet, nous n'aurions pas à nommer un chef de projet, ainsi nous nous sommes basés sur

une répartition équitable et l'autonomie de chacun de nous. Par contre un compte rendu se fait automatiquement pour l'avancé du travail.

5. Objectifs du projet

Plusieurs objectifs sont à remplir:

- Définir ce qui est les objets connectés dans notre vie ;
- Voir sous quel angle les objets connectés nous font exposer ;
- Quelles sont manières de protéger ces informations.

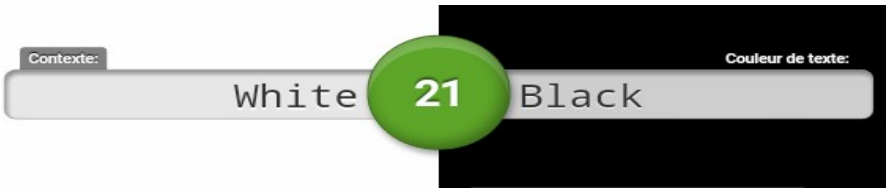
6. La charte graphique

Pour la réalisation de notre page web nous étions amenés à faire des choix de police, de taille de police et aussi de couleur.

Le choix de la police était crucial pour la page car il faut en tout premier lieu séduire l'internaute (l'utilisateur). Et donc nous y avons pensé à une police pas trop fantaisiste, facile à lire, et aussi pas trop droite afin d'attirer l'attention. Ainsi nous avons retenu deux polices pour le premier filtre qui sont Times New Roman et Adamina. Adamina est une police initialement de grande taille face à Times New Roman qui elle est de petite taille, ces deux polices sont très ressemblante. Comme le choix de la police est pour une page web donc il faut harmoniser et c'est ainsi que nous avons retenu Times New Roman.

Pour la couleur nous nous sommes directement orientés vers les nuances foncés du rouge, car le rouge est la couleur de la force extérieure, de même que les objets connectés s'intègrent dans notre quotidien de plus en plus. De plus après une simulation de contraste de la couleur blanche sur fond rouge nuancé réalisé sur le site web [contrast-ratio] on a obtenu 9 point ce qui est clairement parfait.

Et en ce qui concerne le texte, nous nous sommes proposé le texte en noir sur fond blanc et la simulation de ce contraste est la plus excellente avec 21 point.



On ne s'est pas arrêté là comme lors de la conception de la page nous voudrions un menu actif de couleur autre pour marquer la différence. Nous avions retenu la couleur verte claire sur un fond rouge nuancé est le résultat était parfait tel que la simulation donne 6,7 point.

Le choix des tailles de police est aussi crucial, il faut alterner entre un utilisateur mal voyant et les autres donc pas une grande taille, ni une petite. Alors, nous sommes entendus que la taille des textes sera de 14 pour la version Desktop et 12 pour la version mobile, exemple : Les objets connectés sont la troisième révolution numérique.

Le titre principal sera en 60 sur la version Desktop et 48 sur la version mobile.

7. L'arborescence

Nous nous sommes proposé l'arborescence de sorte qu'on ait à l'accueil une introduction sur les objets connectés afin de ramener l'utilisateur dans le contexte des objets connectés et l'objet visé de la page web. La page sécurité va montrer à l'utilisateur la sécurité au niveau de son appareil et de l'hébergeur des données appelé le Data Center. Puis la page confidentialité qui permettra à l'utilisateur de savoir réellement quel type de confidentialité est associé à son objet connecté le Privacy by Design ou le Privacy by Default. Une page solution proposant des possibilités au niveau d'utilisateur avec des mots de passe et aussi fabriquant avec la cryptographie. Et tout au bout la page contact qui fera office de liaison entre l'internaute et le propriétaire du site.

II. Introduction

2.1 Qu'est-ce qu'un "Objet Connecté" ?

Un objet connecté est un appareil électronique qui peut envoyer des informations en temps réel à un ordinateur, un Smartphone ou une tablette.

Il existe deux grandes différence d'objets connectés : Les "Portés" (Montres, Lunettes, Bracelet …) et les "Indépendants" (Station météo, Caméra de surveillance, Voiture …)

Même si tous les domaines sont touchés par l'activité des Objet connectés, on distingue quelques grandes familles :

- Le bien-être et la santé (Montres, Brosse à dent ….)
- Le sport et les loisirs (Chaussures, Montres de sport, Raquettes …)
- L'habitat (Thermostat, Electroménager, Ampoules …)
- Les transports (Voiture connectée...)
- L'entreprise (Badges, …)

Quelques chiffres : (Etude GFK 2014*)

En 2014, il s'est vendu en France:

- 190 000 montres intelligentes
- 250 000 montres "sport" dotées de GPS
- 200 000 bracelets suivis d'activités
- 100 000 drones de loisirs
- 50 000 produit de santé (balance, tensiomètres connectés, brosse à dent …)
- 20 000 thermostats

Après le web qui a révolutionné notre façon de communiquer et de consommer, et la mobilité (téléphone portable, ordinateur…) qui a permis d'y avoir accès partout ou presque : les objets connectés sont la troisième révolution numérique.

Les objets connectés vont avoir un impact dans tous les domaines, ils vont modifier notre façon de vivre : en médecine avec les implants, dans la maison avec la domotique, les voitures automatiques (exemple de Renault Zoé), dans nos habitudes (cartes bancaires numériques, le sport)…Ils sont de plus en plus présent dans notre vie et nous nous en approchons de plus pour se faciliter la vie. De même, nos données confidentielles et professionnelles y sont stockées, véhiculées à travers ces derniers. Ainsi, nous nous interrogeons : Les objets connectés nous sont-ils fiables? Que deviennent nos données traitées? Véhiculent elles juste en nos appareils (Objets connectés)? Et sont-elles supprimées à la demande sans laisser de traces?

C’est à cet effet que nous nous sommes proposé les objets connectés comme thème du groupe et orienté la sécurité, la confidentialité comme projet du sous-groupe.

Alors pour mener à bien ce projet, nous traiterons de manière explicite ce qui est : La sécurité, la confidentialité des Objets connectés, tout au long de ce dossier.

III. Développement

Comme vu plus haut avec les chiffres de l'Étude GFK 2014, les objets connectés sont de plus en plus présent dans la vie de tous les jours. De plus, ils utilisent pour certains nos données personnelles, tel que la position GPS, le son enregistré avec le microphone, ou encore la caméra de surveillance ! Et si toutes ces données étaient piratées ? Et si quelqu'un avait accès à toutes ces données ? Et si quelqu'un avait en permanence accès au camera de sécurité de chez vous ?

Nous allons voir comment les développeurs de ces objets réagissent face à toutes ces contraintes.

10. La Sécurité

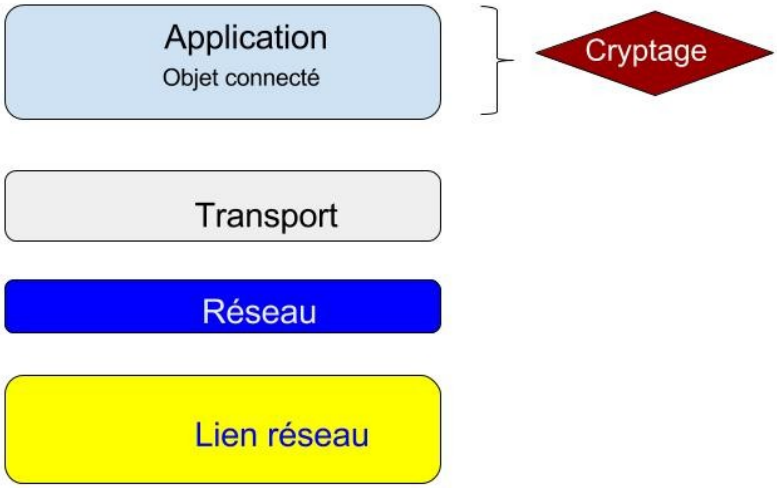
Il faut avant tout savoir qu'il n'existe pas de sécurité parfaite, tout produit qui n'est pas mis à jour régulièrement, fera apparaître de nouveau hacker prêt à tout pour recueillir la moindre donnée personnelle. Ces mise-à-jours sont appelés : OTA, autrement dit Over The Air. Ce sont des mises à jour automatiques de l'appareil qui peuvent modifier les parties systèmes d'un Smartphone ou d'un objet connecté. Y compris les protections contre les piratages ou autres intrusions informatique.

Pour une bonne sécurité, nous avons aussi besoins d'un bon chiffrement dans le transfert de données, d'une vérification cryptographique de chaque code configuration et d'une analyse de sécurité externe par de professionnels du cyber sécurité. Les objets connectés doivent être fiables dès leurs sorties d'usine.

4. Les applications (Programmes) installés sur les objets connectés

Pour cette partie de la sécurité, nous allons faire un peu de réseau. Bref un schéma des couches réseau en modèle TCP/IP permet d'illustrer cela.

Modèle TCP/IP



Les aspects sécurité sont portés dans ce modèle TCP/IP. Les capacités de sécurité au niveau de la couche application : l'autorisation, l'authentification, la confidentialité des données d'application et la protection de leur intégrité, la protection de la sphère privée, les audits de sécurité.

Dans une étude réalisée en 2014 réalisée par Fortify, la division d'HP dédiée au cyber sécurité. On a pu constater que sur 10 objets connectés audités:

- 70 % ne cryptent pas les données échangées avec le réseau
- Ce manque de cryptage laisse le champ libre aux pirates informatiques, d'où problème de sécurité.
- 80 % ne nécessitent pas de mot de passe suffisamment complexe;
- 60% n'offrent pas une interface Web suffisamment sécurisée.

Donc nous allons basés au niveau de la couche application afin de voir le chiffrement des données personnelles avant les transports sur le réseau.

Le cryptage de l'information se fait par l'intermédiaire de la cryptographie symétrique ou asymétrique qui va permettre le chiffrement des données de l'utilisateur pour la circulation sur le réseau afin d'éviter le piratage de données, donc assurer la sécurité de l'information.

Or en réalité peu des objets connectés sont dotés de cette fonction de cryptage de données comme l'affirme l'étude sur le cyber sécurité précédente.

Mais tout de fois même si les données sont moins sécurisées au niveau de l'utilisateur, il est d'une grande importance pour l'hébergeur des données, le Data Center.

5. Data Center

La deuxième partie de la sécurité est lié au Data center.

Le data center (centre de traitement des données en français) est l'un des éléments nécessaires au traitement et stockage des données numériques. Indispensable à Internet, il a connu un fort développement avec l'essor du cloud computing. Concrètement, il s'agit d'un lieu physique contenant les serveurs informatiques qui stockent les données numériques.

Normes ISO/CEI 27001:2005 et 27001:2013 - Systèmes de gestion de la sécurité de l'information. La sécurité est d'une importance capitale pour les Datacenter et ses clients. La norme ISO 27001 constitue la certification la plus largement reconnue en matière de sécurité physique, de sécurité des informations et de continuité de services. L'ISO 27001 garantit que :

- les risques et les menaces pour l'entreprise sont évalués et gérés ;
- les procédures de sécurité physique, tel que l'accès restreint/nominatif, sont appliquées en permanence ;
- des audits sont effectués régulièrement sur chaque site, et comprennent des tests de sécurité ainsi que la programmation et le suivi de la vidéosurveillance.

11. La Confidentialité

Une étude commanditée par Intel Security montre que 81% des Français craignent que les données collectées par leurs objets connectés soient utilisées à des fins marketings. Avec la montée en puissance de l'Internet des objets, et leur diversification dans la quasi-totalité des secteurs d'activité économique (de la santé au tourisme, de la maîtrise de l'environnement aux loisirs…) de nouvelles questions sont désormais posées aux concepteurs de ces objets pour répondre aux attentes de leurs usagers, en particulier en matière de protection des informations personnelles.

Les objets connectés diffèrent en effet des objets industriels traditionnels en ce qu'ils conservent, durant l'ensemble de leur cycle de vie, un lien avec l'Internet mais aussi et surtout avec l'entreprise qui les a produits. Leur conception même (leur design) doit donc désormais intégrer ces préoccupations pour que les usagers puissent garder la maîtrise de leurs données. La protection de la vie privée des utilisateurs des objets connectés devient ainsi une préoccupation majeure de l'ensemble des acteurs industriels

Il existe une réglementation européenne sur la protection des données qui introduit deux notions fondamentales à prendre en compte: celles du "privacy by design" et du "privacy by default".

6. Privacy by design

La notion de "privacy by design" suppose que les questions de respect de la confidentialité et de protection des données soient intégrées dès la conception d'un objet ou d'un service connecté. Le risque avec cette réglementation est celle de l'accessibilité aux informations personnelles par l'entreprise, le fabricant. Ce qui fait ressortir l'aspect de la surveillance généralisée lié aux objets connectés et encore plus pire la vente des données personnelles.

Par contre une forme de réglementation existe c'est la "privacy by default".

7. Privacy by default

La notion de "privacy by default" signifie que, par défaut, ledit service doit être "réglé" sur le niveau le plus protecteur pour le consommateur. En d'autres termes, que ce dernier soit obligé de partager le minimum d'informations nécessaires.

12. Les Solutions

De façon générale, on utilise un mot de passe de sorte à protéger ses comptes ou bien un appareil pour garder hors de vue les fichiers personnels ou autre informations propre à soi-même. Les mots de passe sont (la plupart du temps) en lien avec la vie de l'utilisateur, par exemple la ville avec le numéro de département de l'utilisateur, une date marquante, le nom d'un proche important…. Donc de ce fait, il n'est pas impossible de trouver le mot de passe de quelqu'un si on le connaît un petit peu. C'est pour cela que des solution existe pour complexifier le mot de passe comme alterner entre majuscule et minuscule, ajouter des caractères spéciaux, ou même changer complètement le mot de passe (qui n'est donc pas en lien avec la vie privée) en utilisant un générateur de mot de passe tel que : https://www.generateurdemotdepasse.com/

De plus pour une meilleure protection, l'objet connecté doit bien être à jour, les développeurs améliore en permanence leur système de protection sur les objets connecté, les mises à jour sont donc très utiles pour contrer la plupart des attaques.

La solution la plus probable est la cryptographie, avec les nouvelles tendances de l'intégration de fonctions cryptologique directement dans le silicium de composants (au niveau du fabriquant de l'objet connecté) qui offrira au microprocesseur de l'appareil des performances élevées de chiffrement de données intégrée. Ainsi un extrait d'algorithme de générateur de nombre aléatoire permettant de chiffrer les données de l'utilisateur:

```
void setup() {
  Serial.begin(9600);
  pmc_enable_periph_clk(ID_TRNG);
  trng_enable(TRNG);

  NVIC_DisableIRQ(TRNG_IRQn);
  NVIC_ClearPendingIRQ(TRNG_IRQn);
  NVIC_SetPriority(TRNG_IRQn, 0);
  NVIC_EnableIRQ(TRNG_IRQn);
  trng_enable_interrupt(TRNG);
}

void TRNG_Handler(void) {
  uint32_t stat = trng_get_interrupt_status(TRNG);

  if ((stat & TRNG_ISR_DATRDY) == TRNG_ISR_DATRDY) {
    int r = trng_read_output_data(TRNG);
    Serial.println(r);
  }
}

void loop() {
}
```

Donc les fabricants doivent produire des appareils (objets connectés) dotés de mémoire possible (2GB, 4GB ou plus) capables d'effectuer des puissants calculs.

IV. Conclusion

En somme, aujourd'hui les objets connectés nous paraissent douteux, peu fiable par contre la technologie de ces appareils ne cessent de s'améliorer depuis ces dernières années. Ainsi, on passe d'un nombre d'utilisateur réduit à un effectif considérable de nos jours. Le développement de normes, sur le modèle de celles mises en place par l'ISO, qui permettra d'identifier les services qui sont exemplaires du point de vue de la protection des données personnelles et du respect de la confidentialité. La conformité à ces normes donnerait confiance au consommateur, de plus en plus préoccupé par ces questions de sécurité et de confidentialité. Il est probable que ces normes se développent dans les prochaines années.

V. Références/Sources

Voici une liste des articles et autres documents que nous avons utilisés.

- Le lien entre Langage Cryptographique et Objet connecté
- Exemple de Datacenter pour la Sécurité
- La fiabilité des objets connectés dès leur sortie d'usine
- Remise en question de la sécurité après une attaque aux Etats Unis
- Comparaison rumeur / réalité
- Les normes pour lutter le piratage de données personnelles
- Réseau des objets connectés
- Qu'est ce que l'ISO
- L'exemple de l'ISO concernant le Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002
- Le modèle TCP/IP pour les objets connectés
- Privacy by design