Sécurité des appareils mobiles, des applis et de l'IdO

Protéger les données et les appareils dans le monde entier

Face à la montée en flèche des cyberattaques soutenues par certains États et autres acteurs malveillants en ligne, nous pensons que la sûreté de nos produits et services devient tout aussi importante que leur utilité. Chez Google, nous sommes plus que jamais mobilisés pour protéger les personnes, les entreprises et les gouvernements en partageant notre expertise, en donnant à la société les moyens de faire face aux cyberrisques en constante évolution et nous efforçant de faire progresser les pratiques de pointe en matière de cybersécurité afin de construire un monde plus sûr pour tous.

Il est crucial de garder une longueur d'avance et de faire évoluer en permanence nos solutions de sécurité dans un contexte de menace croissante. Cela nous permettra de sécuriser tous les appareils connectés et toutes les applis, et d'offrir aux consommateurs un environnement sûr dans lequel ils pourront choisir en toute connaissance de cause les appareils qu'ils utilisent.

Le défi

La connectivité a un prix

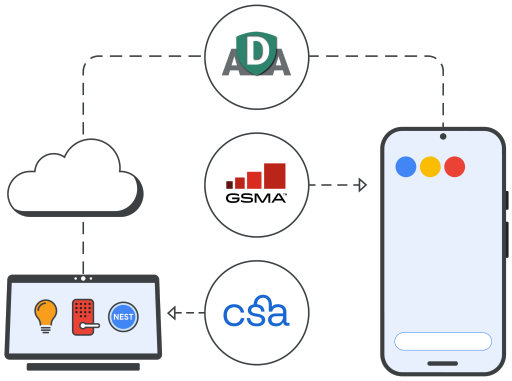
Une part importante de notre vie quotidienne est gérée à partir de nos téléphones intelligents, de nos applis et de nos appareils IdO. Nous passons de plus en plus de temps en ligne et nous partageons toujours plus de données précieuses, telles que des informations bancaires ou relatives à la santé. C'est pourquoi les cybercriminels aux techniques sophistiquées ciblent plus que jamais ces appareils pour obtenir des informations sensibles.

Qui dit plus d'appareils et de données dit plus de menaces

On estime aujourd'hui à 17 milliards le nombre d'appareils faisant partie de l'IdO dans le monde, des imprimantes aux dispositifs d'ouverture à distance des portes de garage, tous équipés d'un logiciel (dont des logiciels ouverts) pouvant être facilement piraté[1]. Parmi eux, le nombre d'appareils vulnérables et exploités de l'IdO a presque doublé en 2020[2].

- Alors que nous sommes de plus en plus connectés grâce aux appareils faisant partie de l'IdO, l'absence de normes mondiales permettant de mesurer l'ampleur de la vulnérabilité de ces appareils empêche les consommateurs de prendre des décisions éclairées en matière de sécurité des appareils.
- Tout comme ils ont accès à la composition des aliments ou des produits de nettoyage qu'ils achètent, les consommateurs devraient avoir le droit à davantage de transparence concernant leurs produits numériques.
- Les appareils mobiles ne sont que l'un des vecteurs pour d'autres surfaces d'attaque, et l'interconnectivité des appareils accroît de manière très importante le besoin de transparence en matière de sécurité. C'est pourquoi la sécurité de l'écosystème des appareils connectés est tout aussi importante que la sécurité des réseaux et des systèmes.

Notre collaboration avec des organisations du secteur des télécommunications



Notre solution

Chez Google, nous améliorons la sécurité et la transparence de nos appareils connectés grâce à la sécurité des appareils mobiles, des applis et de l'IdO :

Sécurité des appareils mobiles

Android, notre système d'exploitation ouvert, s'appuie sur une approche de sécurité multicouche pour assurer la sécurité des appareils mobiles :

- Sécurité multi-niveaux
  - La technologie Verified Boot, la protection anti-retour et la protection contre la réinitialisation d'usine garantissent l'utilisation de la version la plus récente et la plus sûre d'Android.
  - L'authentification biométrique et par code NIP assure une protection contre les intrusions extérieures.
  - La fonction « Trouver mon appareil » permet de localiser l'appareil ou de le vider de ses données en cas de vol ou de perte.
- Protection de l'identité et du mot de passe
  - La vérification en 2 étapes, l'utilisation du téléphone comme clé de sécurité et le gestionnaire de mots de passe protègent votre compte Google contre les intrusions extérieures.
  - Le vérification de la sécurité et la protection avancée en option permettent à l'appareil de fonctionner en toute sécurité et de manière fluide.
- Protection contre l'hameçonnage
  - Les applis Téléphone Google et Messages par Google permettent de détecter et de prévenir les escroqueries ainsi que les attaques par hameçonnage.
  - La navigation sécurisée Google protège plus de 5 milliards d'appareils dans le monde.

Sécurité des applis

Un logiciel de lutte contre les maliciels prêt à l'emploi permet d'écarter les applis malveillantes alors qu'un système d'informations sur la sécurité des données offre une transparence aux utilisateurs lorsqu'ils téléchargent des applis.

- Google Play Store : Des outils de détection alimentés par l'apprentissage automatique, ainsi que des analystes humains, examinent toutes les applis avant qu'elles ne soient disponibles en téléchargement. La section Sécurité des données donne des informations sur le type de données collectées par les applis et sur l'usage qui en est fait.
- Google Play Protect : Analyse chaque jour plus de 125 milliards d'applis et notifie, supprime ou désactive celles qui présentent des risques de sécurité.
- App Defense Alliance (ADA) : Google a collaboré avec les principaux partenaires du domaine des menaces contre les appareils mobiles pour fonder l'App Defense Alliance (ADA). Cet organisme a pour mission de protéger les utilisateurs Android contre les applis potentiellement nuisibles (APN) grâce au partage d'informations et à la coordination de processus de détection.

Sécurité de l'IdO

Les étiquettes de sécurité de l'IdO indiquent clairement les pratiques en matière de confidentialité et de sécurité d'un appareil, comme le type de données collectées.

- Nous défendons un système basé sur cinq principes fondamentaux pour les schémas d'étiquetage de la sécurité de l'IdO : étiquetage « en direct », schémas d'évaluation, niveaux minimum de sécurité de référence couplés à une certaine flexibilité, transparence à grande échelle et incitations à l'adoption.
- Nous travaillons avec la Connectivity Standards Alliance (CSA) et la GSM Alliance (GSMA) pour normaliser un programme de certification à l'échelle du secteur qui réponde aux exigences réglementaires actuelles et futures.

Nos principes

Chez Google, nous appliquons 3 principes fondamentaux pour la sécurité et la transparence de nos appareils connectés :

Protection en profondeur : Nous utilisons une architecture à plusieurs niveaux de sécurité qui fonctionnent ensemble pour une protection solide, fluide et efficace.

Ouverture et transparence : La transparence est au cœur de notre philosophie. Nous sommes persuadés qu'un écosystème de code source ouvert peut se révéler plus sûr qu'un écosystème fermé, c'est pourquoi nous tenons informés les utilisateurs de notre plateforme et nous partageons nos connaissances pour renforcer nos systèmes de protection.

Le meilleur de Google et de notre écosystème : Nous travaillons en partenariat avec des équipes spécialisées internes à Google et issues du secteur, pour protéger des milliards d'utilisateurs.

Applis

Étiquettes de sécurité pour l'IdO : placer le consommateur en situation de contrôle

En l'absence d'étiquettes de sécurité pour l'IdO, les fabricants d'appareils ne sont pas tenus de respecter des normes mondiales. De leur côté, les utilisateurs n'ont aucune visibilité sur la manière dont leurs appareils protègent leurs données. Le secteur doit unir ses efforts pour faire progresser la sécurité de l'IdO et redonner le contrôle aux consommateurs. Nous travaillons à la mise en place d'un système d'étiquetage de la sécurité de l'IdO via nos processus et nos partenariats.

Tout d'abord, nous investissons dans la recherche sur la cybersécurité dans le but d'identifier les éventuelles vulnérabilités (Google Nest participe au programme de récompense des vulnérabilités de Google et offre des récompenses aux chercheurs en cybersécurité qui, en dehors de Google, traquent et trouvent des vulnérabilités).

Tous nos appareils développés en 2019 et au-delà utilisent Verified Boot pour garantir que le bon logiciel fonctionne et que l'accès est protégé. C'est notamment le cas de nos appareils Google Nest qui sont validés sur la base de normes de sécurité tierces reconnues par le secteur, telles que celles produites par les organismes de normalisation NIST, ETSI et ISO.

Ces normes, ainsi que notre cycle de vie sécurisé pour le développement des logiciels (SDLC), réduisent la probabilité que les consommateurs soient exposés à de mauvaises pratiques en matière de sécurité et préparent le terrain à un Internet ouvert et plus sûr.

Nos investissements dans le secteur et étapes clés

2007 Mise en place de la navigation sécurisée pour alerter de manière proactive les utilisateurs lorsqu'ils visitent des sites Web dangereux; elle protège aujourd'hui plus de 5 milliards d'appareils.

2010 Publication du rapport sur la transparence de Google qui explique comment les règles et les actions des organismes gouvernementaux et des entreprises affectent la confidentialité, la sécurité et l'accès à l'information en ligne. En 2018, nous avons ajouté un rapport sur la transparence spécifique à Android.

2017 Lancement de Google Play Protect, le logiciel de lutte contre les maliciels le plus largement déployé à ce jour, qui analyse tous les jours plus de 125 milliards d'applis installées sur plus de 3 milliards d'appareils.

2019 Mise sur le marché de la clé de sécurité, une fonctionnalité intégrée à Android dans un premier temps, puis à l'iPhone en 2020.

2022 Lancement, sur Google Play, d'une section sur la sécurité des données qui informe les utilisateurs sur la manière dont les applis collectent, partagent et sécurisent leurs données, et mise en place du premier système de badge pour toute appli ayant fait l'objet d'un examen de sécurité indépendant par l'App Defense Alliance.

2023 La clé d'accès, pour un avenir sans mot de passe, est en cours de déploiement avec une prise en charge étendue après une décennie de normes ouvertes avec l'alliance FIDO et les géants de la technologie du monde entier.

Notre approche

Mobilisés pour un monde numérique ouvert et sûr

Avec l'augmentation du nombre de données sur un plus grand nombre d'appareils connectés à différents réseaux, les questions de sécurité se font de plus en plus pressantes. Nous contribuons à faire progresser l'avenir de la sécurité des appareils connectés grâce au développement de nos produits, à nos critères de transparence et à nos partenariats avec les entreprises du secteur.

La sécurisation par défaut de tous nos produits est au centre de notre stratégie. La navigation sécurisée, Google Play Protect et les clés de sécurité intégrées protègent les appareils mobiles et les applis tout en assurant le niveau de sécurité le plus élevé de nos produits.

En faisant preuve d'ouverture et de transparence sur la façon dont nous traitons les failles et en partageant nos connaissances en matière de sécurité des appareils connectés, nous contribuons à la démocratisation de la sécurité opérationnelle. Nous sommes persuadés qu'un écosystème de code source ouvert peut se révéler plus sûr qu'un écosystème fermé grâce à notre approche multicouche de la sécurité.

En collaborant avec des organismes tels que la CSA, l'ADA et la GSMA, nous mettons tout en œuvre pour faire progresser les pratiques de pointe en matière de cybersécurité, tout en ouvrant la voie à un Internet et à un avenir plus sûrs pour tous.

Nous sommes déterminés à relever le niveau de sécurité des appareils connectés et à mettre en place des normes garantissant un environnement en ligne plus sûr pour tous et partout. Pour en savoir plus sur les progrès de Google en matière de sécurité des appareils connectés : g.co/connecteddevicesafety

Sources : [1] CNBC Cyber Report, 9 janvier 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security, 20 juillet 2021