ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

UIT-T X.1454 (09/2023)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

Applications et services sécurisés (2) – Sécurité des applications (2)

Mesures de sécurité pour les services de bureau intelligent fondés sur la localisation

RECOMMANDATIONS UIT-T DE LA SÉRIE X

Réseaux de données, communication entre systèmes ouverts et sécurité

RÉSEAUX PUBLICS DE DONNÉES	X.1-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	X.850-X.899
TRAITEMENT RÉPARTI OUVERT	X.900-X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	X.1000-X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	X.1100-X.1199
SÉCURITÉ DU CYBERESPACE	X.1200-X.1299
APPLICATIONS ET SERVICES SÉCURISÉS (2)	X.1300-X.1499
Communications d'urgence	X.1300-X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310-X.1319
Sécurité des réseaux électriques intelligents	X.1330-X.1339
Courrier certifié	X.1340-X.1349
Sécurité de l'Internet des objets (IoT)	X.1350-X.1369
Sécurité des systèmes de transport intelligents	X.1370-X.1399
Sécurité de la technologie des registres distribués (DLT)	X.1400-X.1429
Sécurité des applications (2)	**X.1450-X.1459**
Sécurité de la toile (2)	X.1470-X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	X.1500-X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	X.1600-X.1699
COMMUNICATIONS QUANTIQUES	X.1700-X.1729
SÉCURITÉ DES DONNÉES	X.1750-X.1799
SÉCURITÉ DES IMT-2020	X.1800-X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1454

Mesures de sécurité pour les services de bureau intelligent fondés sur la localisation

Résumé

Les services de bureau intelligent, qui combinent plusieurs applications intelligentes, visent à améliorer la qualité des activités de bureau et à améliorer la gestion de l'efficacité. Les technologies de l'information et de la communication (TIC) servant de base aux technologies utilisées dans les services de bureau intelligent, l'opérateur de télécommunication joue un rôle important parmi les parties prenantes de ces services.

Les services de bureau intelligent types comprennent le stationnement intelligent, la conduite intelligente, le magasin de vente au détail intelligent, le bureau intelligent, la gestion des salles de réunion intelligentes, la gestion de l'eau intelligente et la gestion de la consommation d'énergie intelligente. Parmi ces services de bureau intelligent types, les données de localisation fournies par l'opérateur constituent l'un des éléments clés de la plupart des mises en œuvre des services de bureau intelligent.

Afin de garantir la sécurité des services de bureau intelligent fondés sur la localisation, il est nécessaire d'analyser les menaces pour la sécurité et les exigences de sécurité pertinentes propres aux services fondés sur la localisation et d'établir des mesures globales en matière de sécurité.

La Recommandation UIT-T X.1454 analyse les scénarios d'application types des services de bureau intelligent fondés sur la localisation, spécifie les menaces et les exigences en matière de sécurité et établit des mesures de sécurité pour l'opérateur et les principales parties prenantes d'un bureau intelligent afin de protéger les services fondés sur la localisation.

Historique*

Édition	Recommandation	Approbation	Commission d'études	ID unique
1.0	UIT-T X.1454	08-09-2023	17	11.1002/1000/15111

Mots clés

Localisation, mesures de sécurité, services de bureau intelligent.

* Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1454

Mesures de sécurité pour les services de bureau intelligent fondés sur la localisation

1 Domaine d'application

La présente Recommandation analyse les scénarios d'application types des services de bureau intelligent fondés sur la localisation, présente les menaces et les exigences en matière de sécurité propres aux services fondés sur la localisation, et établit ainsi les mesures de sécurité pour l'opérateur et les principales parties prenantes d'un bureau intelligent afin de protéger les services fondés sur la localisation.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

Néant.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 service de bureau intelligent: un service combinant plusieurs applications intelligentes (par exemple, le stationnement intelligent, la gestion de l'eau intelligente ou le magasin de vente au détail intelligent) qui vise à servir et à soutenir les tâches d'une activité de bureau, à améliorer la qualité de cette activité et l'efficacité de sa gestion, et à créer un environnement de bureau adapté pour les personnes.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

DDoS déni de service réparti (*distributed denial of service*)

GNSS système mondial de navigation par satellite (*global navigation satellite system*)

SEM surveillance intelligente de l'environnement (*smart environmental monitoring*)

SRNS système de radionavigation par satellite

TIC technologies de l'information et de la communication

UWB ultra-large bande (*ultra-wide band*)

WiFi fidélité sans fil (*wireless fidelity*)

5 Conventions

L'expression "**il est exigé**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

6 Aperçu des services de bureau intelligent fondés sur la localisation

Selon la vision des villes intelligentes et durables, qui utilise les technologies de l'information et de la communication (TIC) et d'autres moyens pour améliorer la qualité de vie, l'efficacité de la gestion urbaine et des services urbains ainsi que la compétitivité, le service de bureau intelligent devient une application type dans une ville intelligente et durable.

Le service de bureau intelligent combinant plusieurs applications intelligentes (par exemple, le stationnement intelligent, la gestion de l'eau intelligente ou le magasin de vente au détail intelligent) vise à améliorer la qualité des offres d'une activité de bureau et l'efficacité de sa gestion.

Les services de bureau intelligent combinent plusieurs applications intelligentes et les principales parties prenantes sont diverses. Étant donné que les TIC servent de base aux technologies utilisées dans les services de bureau intelligent, parmi les services de bureau intelligent types, les données de localisation fournies par l'opérateur constituent l'un des éléments clés de la plupart des mises en œuvre de ces services.

Les principales parties prenantes dans le domaine des systèmes de bureau intelligent fondés sur la localisation sont les suivantes:

– le fournisseur de services de bureau intelligent;

– le fournisseur de données et de calculs;

– le fournisseur de capteurs et d'infrastructure;

– l'utilisateur.

NOTE – Ces parties prenantes essentielles dans le domaine des systèmes de bureau intelligent fondés sur la localisation, à savoir le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure, pourraient être des fournisseurs indépendants ou un fournisseur de services intégrés.

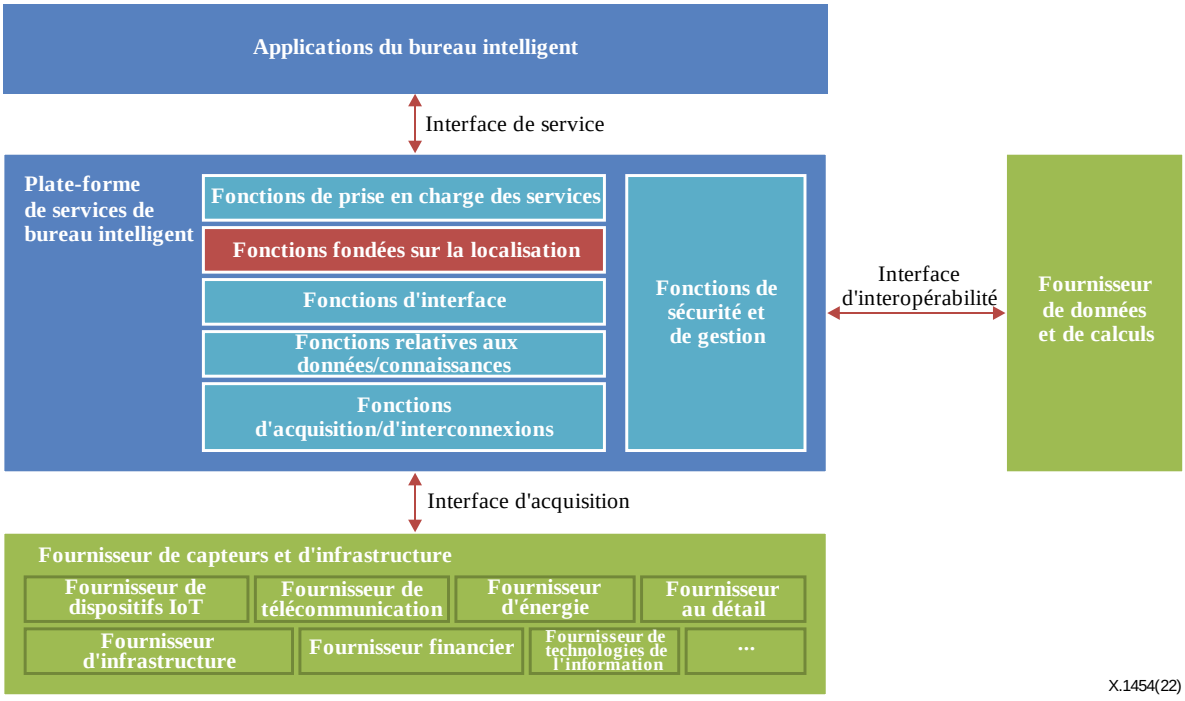

Figure 1 – Aperçu d'un système de bureau intelligent fondé sur la localisation

Le système de bureau intelligent fondé sur la localisation assure les fonctions suivantes:

– **Fonctions d'acquisition/d'interconnexion**: fournissent des mécanismes de saisies de données à partir de différentes sources de systèmes de collecte de données.

– **Fonctions relatives aux données/connaissances**: prennent en charge le traitement des données, en ajoutant de la valeur et en transformant les informations en connaissances.

– **Fonctions d'interface**: permettent l'accès à l'information à différents niveaux.

– **Fonctions fondées sur la localisation**: fournissent des données de localisation à partir du système de l'opérateur.

– **Fonctions de prise en charge des services**: coordonnent tous les services possibles impliqués dans chaque action pour assurer les fonctions d'interopérabilité.

– **Fonctions de sécurité et de gestion**: fournissent des fonctionnalités horizontales comme les audits, le contrôle et la sécurité.

Les interfaces permettent la communication entre les fonctions:

– **Interface d'acquisition**: permet la collecte d'informations à partir des éléments extérieurs.

– **Interface d'interopérabilité**: permet la communication avec les fournisseurs de données externes et les systèmes de calcul tiers.

– **Interface de service**: permet l'accès d'application à application pour la prise en charge de fonctions fournies par la plate-forme de services de bureau intelligent.

7 Scénarios d'application types des services de bureau intelligent fondés sur la localisation

7.1 Stationnement intelligent

Le stationnement intelligent permet une intégration efficace des ressources de stationnement dans un parking de bureau et coordonne les installations de stationnement avec d'autres systèmes (par exemple, un système de paiement extérieur ou un système de stationnement basé sur un site web ou une application).

Le stationnement intelligent peut notamment comprendre les fonctions types suivantes: guidage de stationnement, réservation de place de stationnement, recherche inversée de véhicule, contrôle d'accès automatique au véhicule et paiement en libre-service. Les fonctions de stationnement intelligent fondées sur la localisation sont les suivantes:

– **Guidage de stationnement**: les informations de localisation relatives aux places de stationnement inoccupées appuient la publication d'informations sur le guidage de stationnement.

– **Réservation de place de stationnement**: les informations de localisation peuvent être une aide pour la recherche d'informations sur les places de stationnement disponibles et la réservation de places de stationnement à l'avance.

– **Recherche inversée de véhicule**: les informations de localisation pourraient aider les conducteurs de véhicules à retrouver l'emplacement de leur véhicule au cas où ils oublieraient où ils l'ont laissé.

7.2 Surveillance intelligente de l'environnement

En tant qu'application d'autosurveillance et d'autoprotection de l'environnement, la surveillance intelligente de l'environnement (SEM) peut connaître la situation environnementale actuelle.

La SEM peut comprendre les entités fonctionnelles de plates-formes SEM, les dispositifs SEM et le réseau. Les fonctions de surveillance intelligente de l'environnement fondées sur la localisation sont les suivantes:

– **Gestion du paramétrage des mesures**: l'emplacement d'un dispositif constitue l'information nécessaire pour paramétrer les mesures selon les facteurs environnementaux.
– **Présentation des données**: les données brutes à chaque emplacement donné (d'un ou plusieurs dispositifs de surveillance intelligente de l'environnement) constituent les informations facultatives pour la présentation de la qualité de l'environnement.

7.3 Livraison intelligente

La livraison intelligente tire parti de l'application de véhicules sans conducteur et de robots dans un scénario de bureau intelligent, et peut livrer automatiquement les colis, les fichiers, les fournitures de bureau, etc.

Les fonctions de livraison intelligente fondées sur la localisation sont les suivantes:

– Assister la conduite autonome en offrant une fonction de localisation avec une précision de l'ordre du centimètre.
– Améliorer l'efficacité de la livraison par le véhicule/robot en faisant le lien entre l'ordre de livraison et l'emplacement du dispositif.
– Optimiser le routage de livraison et contrôler le processus de livraison en suivant la localisation et le trajet du véhicule/robot en temps réel.

8 Menaces de sécurité pour les services de bureau intelligent fondés sur la localisation

8.1 Menaces de sécurité pour les données

8.1.1 Écoute illicite des données de localisation

Les données de localisation dans les services de bureau intelligent pouvant être fondées sur le réseau sans fil ouvert, l'auteur d'une attaque peut écouter clandestinement les données de localisation en surveillant le canal hertzien.

8.1.2 Altération des données de localisation

L'auteur d'une attaque peut obtenir le paquet de données au sein des données de localisation transmises depuis le réseau et modifier à des fins malveillantes ou falsifier les données de localisation pour lancer d'autres attaques. Dans certains scénarios, les données de localisation modifiées ou falsifiées peuvent engendrer des problèmes de sécurité, par exemple en ce qui concerne le stationnement intelligent, la conduite intelligente et les secours d'urgence.

8.1.3 Interception de la communication des données de localisation

L'auteur d'une attaque peut s'emparer des dispositifs IoT ou les altérer en refusant de communiquer les données de localisation des dispositifs IoT au réseau ou à la plate-forme de services de bureau intelligent.

8.1.4 Invocation de données de localisation non autorisée

En l'absence du mécanisme d'authentification entre les applications et la plate-forme de services de bureau intelligent, les données de localisation peuvent être invoquées sans autorisation par l'auteur d'une attaque.

8.1.5 Données non disponibles

Le format de données non unifié peut conduire à l'indisponibilité d'une application dans un bureau intelligent; par exemple, le format non unifié de données de localisation en intérieur (y compris les données relatives à l'étage, à la salle, au bureau) peut induire en erreur le robot lorsqu'il livre le colis au destinataire.

8.1.6 Divulgation d'informations en matière de comportement

Cette menace peut survenir lorsqu'une plate-forme de bureau intelligent subit une altération volontaire ou que l'auteur d'une attaque usurpe l'identité d'une personne morale pour avoir la possibilité d'obtenir des informations sur le comportement des utilisateurs (par exemple, les préférences concernant la planification d'un itinéraire) à des fins malveillantes, comme leur revente à profit.

8.1.7 Localisation sans le consentement de l'utilisateur

Cette menace survient lorsque l'entité de la fonction de localisation collecte les données de localisation de l'utilisateur et analyse les données connexes sans le consentement de l'utilisateur, y compris en ce qui concerne le champ d'application, l'intention, la méthode, les résultats et leur utilisation.

8.2 Menaces pour la sécurité du dispositif

8.2.1 Vulnérabilité du matériel et des logiciels

Il est possible que le processus de développement des dispositifs de localisation présente des vulnérabilités et des menaces pour la sécurité, avec par exemple, des ports de débogage mal protégés, l'utilisation d'algorithmes de chiffrement faibles, et possiblement l'échec de la mise à jour d'éléments matériels et de logiciels, et l'absence de contrôles d'intégrité réguliers.

8.2.2 Manipulation du dispositif de localisation

L'auteur d'une attaque peut manipuler un dispositif de localisation en altérant les systèmes de capteurs et l'infrastructure, ce qui peut donner lieu à un résultat de localisation inexact.

8.3 Menaces pour la sécurité des interfaces

8.3.1 Interface d'acquisition

L'interface entre le fournisseur de capteurs et d'infrastructure et la plate-forme de services de bureau intelligent est vulnérable face aux menaces suivantes:

– **Reniflage de données**: en l'absence de mécanismes d'authentification et d'autorisation entre la plate-forme de services de bureau intelligent et le fournisseur de capteurs et d'infrastructure, l'auteur d'une attaque peut se faire passer pour la plate-forme de services de bureau intelligent pour collecter des données de détection et d'infrastructure.

– **Déni de service**: l'auteur d'une attaque peut lancer des attaques par déni de service réparti (DDoS) en modifiant la politique de collecte des données (par exemple, en collectant fréquemment les données de détection et d'infrastructure en un laps de temps très court).

– **Fuite d'informations**: les dispositifs mobiles envoient régulièrement des données de service, en particulier des données de localisation, via l'interface d'acquisition, à une plate-forme de services de bureau intelligent. L'auteur d'une attaque peut identifier les habitudes quotidiennes de l'utilisateur s'il peut renifler les données de service et de localisation.

8.3.2 Interface d'interopérabilité

L'interface entre la plate-forme de services de bureau intelligent et le fournisseur de données et de calculs est vulnérable face aux menaces suivantes:

– **Accès non autorisé aux données**: en l'absence de mécanismes d'authentification et d'autorisation entre la plate-forme de services de bureau intelligent et le fournisseur de données et de calculs, l'auteur d'une attaque peut altérer l'interface d'interopérabilité pour accéder aux données de service, aux données de localisation et aux données de profil.

– **Falsification des données**: en l'absence de mécanismes d'authentification et d'autorisation entre la plate-forme de services de bureau intelligent et le fournisseur de données et de calculs, l'auteur d'une attaque peut altérer l'interface d'interopérabilité pour falsifier les données de service, les données de localisation et les données de profil. Cette menace pourrait engendrer une fuite d'informations, un dysfonctionnement de la plate-forme et une facturation erronée du fournisseur de données et de calculs.

8.3.3 Interface de service

L'interface entre la plate-forme de services de bureau intelligent et les applications du bureau intelligent est vulnérable face aux menaces suivantes:

– **Accès non autorisé aux données**: en l'absence de mécanismes d'authentification et d'autorisation entre la plate-forme de services de bureau intelligent et les applications du bureau intelligent, l'auteur d'une attaque peut altérer l'interface de service pour accéder aux données de service, aux données de localisation et aux données de profil.

– **Falsification des données**: en l'absence de mécanismes d'authentification et d'autorisation entre la plate-forme de services de bureau intelligent et les applications du bureau intelligent, l'auteur d'une attaque peut altérer l'interface de service pour falsifier les données de service, les données de localisation et les données de profil. Cette menace peut engendrer une facturation erronée des clients.

8.4 Menaces pour la sécurité de la plate-forme

8.4.1 Vulnérabilité des technologies de localisation hybrides

La fonction de localisation est l'une des entités fonctionnelles de base de la couche de la plate-forme. En tant que telle, elle peut nécessiter une agrégation des technologies de localisation hybrides fondées sur les différents systèmes hertziens, comme le système mondial de navigation par satellite (GNSS), le service de radionavigation par satellite (SRNS), la technologie Bluetooth, le WiFi, les réseaux cellulaires et la bande ultralarge (UWB). La mise en œuvre de ces technologies de localisation hybrides nécessite l'extraction d'informations, le calcul de position et le filtrage. La vulnérabilité du processus d'agrégation et l'algorithme peuvent produire un résultat de localisation inexact.

8.4.2 Exposition des capacités

Une plate-forme de bureau intelligent expose le service de localisation ainsi que d'autres capacités de service aux applications intelligentes. Une entité non autorisée peut par conséquent insérer, modifier ou supprimer les privilèges relatifs à l'utilisation des capacités. Cette entité non autorisée peut être une personne, un programme ou un dispositif. Ces attaques surviennent lorsqu'une entité ajoute des données à une connexion existante avec la capacité de service utilisée en détournant ou en transmettant des données de configuration à des fins malveillantes. Il peut en résulter une attaque par déni de service et la possibilité d'accéder aux données du service.

8.5 Menaces pour la sécurité des applications intelligentes

8.5.1 Utilisation non autorisée

Cette menace survient lorsqu'une application intelligente non autorisée profite des capacités de service offertes par une plate-forme de bureau intelligent en se faisant passer pour une entité autorisée.

8.5.2 Injection de chevaux de Troie et de virus

Cela se produit lorsque l'auteur d'une attaque usurpe l'identité d'une application intelligente licite et injecte un cheval de Troie ou un virus dans l'application intelligente, portant ainsi préjudice à la plate-forme de bureau intelligent et pouvant permettre le lancement d'autres attaques à son encontre.

8.6 Relations entre les menaces de sécurité et les principales parties prenantes

Les relations entre les menaces de sécurité et les principales parties prenantes qui utilisent des services de bureau intelligent fondés sur la localisation sont indiquées dans le Tableau 1.

Dans le Tableau 1, la mention "Oui" est inscrite dans une case pour indiquer que la partie prenante principale est concernée par la menace de sécurité en question.

Tableau 1 – Relations entre les menaces de sécurité et les entités

Principales partie prenantes / Menaces	Fournisseur de services de bureau intelligent	Fournisseur de données et de calculs	Fournisseur de capteurs et d'infrastructures	Utilisateur
Divulgation d'informations en matière de comportement	Oui	Oui	Oui	Oui
Localisation sans le consentement de l'utilisateur	Oui		Oui	Oui
Reniflage de données	Oui		Oui	Oui
Déni de service	Oui		Oui	
Fuite d'informations	Oui		Oui	Oui
Accès non autorisé à des données	Oui	Oui	Oui	Oui
Falsification de données	Oui	Oui	Oui	Oui
Vulnérabilité des technologies de localisation hybrides			Oui	
Exposition des capacités	Oui			
Vulnérabilité du matériel et des logiciels			Oui	
Manipulation du dispositif de localisation			Oui	
Utilisation non autorisée	Oui			
Injection de chevaux de Troie et de virus	Oui			

9 Exigences de sécurité pour les services de bureau intelligent fondés sur la localisation

9.1 Exigences de sécurité relatives aux données

– E-01: il est exigé que le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure prévoient une fonctionnalité permettant de garantir la confidentialité des données, en particulier des données de localisation.

– E-02: il est exigé que le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure prévoient une fonctionnalité permettant de garantir l'intégrité des données, en particulier des données de localisation.

– E-03: il est exigé que le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure garantissent que seuls les utilisateurs ou dispositifs autorisés puissent accéder aux données, en particulier aux données de localisation.

– E-04: il est exigé que le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure confirment les identités des entités et empêchent les auteurs d'attaques de tenter d'usurper l'identité d'une entité autorisée.

– E-05: il est exigé que le fournisseur de services de bureau intelligent prévoie une fonctionnalité permettant de garantir que seuls les dispositifs ou applications autorisés puissent accéder à l'environnement du bureau.

– E-06: il est exigé que le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure mettent en place un mécanisme de collaboration pour unifier le format des données.

– E-07: il est exigé que le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure ne soient autorisés à recueillir les données personnelles de l'utilisateur, en particulier les données de localisation, qu'après avoir obtenu le consentement de celui-ci. Cela implique de rappeler, présenter et expliquer brièvement à l'utilisateur comment ses données personnelles sont recueillies.

Pour ce qui concerne les données d'un service de bureau intelligent fondé sur la localisation, les exigences de sécurité découlant des menaces de sécurité correspondantes sont indiquées dans le Tableau 2.

Tableau 2 – Exigences de sécurité relatives aux données en fonction des menaces de sécurité

Menaces de sécurité	**Exigences de sécurité**
Écoute illicite des données de localisation	E-01, E-02, E-03, E-04
Altération des données de localisation	E-03, E-04
Interception de la communication des données de localisation	E-03, E-04
Invocation de données de localisation non autorisée	E-03, E-04, E-05
Données non disponibles	E-06
Divulgation d'informations en matière de comportement	E-01, E-03, E-04
Localisation sans le consentement de l'utilisateur	E-07

9.2 Exigences de sécurité relatives aux dispositifs

– E-08: il est exigé que le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure mettent en place un processus de réponse en cas d'incident relatif à la détection d'un logiciel malveillant, déploient au préalable des mécanismes de sécurité pour réagir à une attaque et y répondent temps.

– E-09: il est exigé que le fournisseur de capteurs et d'infrastructure fasse en sorte que l'auteur d'une attaque ne puisse pas accéder aux données, même en cas de détournement du matériel, notamment:

  • en vérifiant l'authenticité et l'intégrité des logiciels dans le cas d'un dispositif utilisant des signatures numériques générées de manière cryptographique [b-ISO/CEI 9796-3];

- en contrôlant le trafic dont le point de terminaison est le dispositif au moyen d'un pare-feu, d'un mécanisme de détection des intrusions et d'un système de protection contre les intrusions.

– E-10: il est exigé que le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure utilisent des algorithmes de chiffrement appropriés pour garantir la confidentialité des données, en particulier des données de localisation.

– E-11: il est exigé que le fournisseur de capteurs et d'infrastructure prévoie une fonctionnalité permettant de confirmer les identités des entités et d'empêcher les auteurs d'attaques de tenter d'usurper l'identité d'une entité autorisée.

Pour ce qui concerne un dispositif de services de bureau intelligent fondés sur la localisation, les exigences de sécurité qui découlent des menaces de sécurité correspondantes sont présentées dans le Tableau 3.

Tableau 3 – Exigences de sécurité relatives à un dispositif en fonction des menaces de sécurité

Menaces de sécurité	**Exigences de sécurité**
Vulnérabilité du matériel et des logiciels	E-08, E-09, E-10
Manipulation du dispositif de localisation	E-09, E-11

9.3 Exigences de sécurité relatives aux interfaces

– E-12: il est exigé que le fournisseur de services de bureau intelligent, le fournisseur de données et de calculs et le fournisseur de capteurs et d'infrastructure prévoient une fonctionnalité permettant de garantir que seuls les utilisateurs ou dispositifs autorisés puissent avoir accès aux données de détection et d'infrastructure par l'intermédiaire des interfaces.

– E-13: il est exigé que le fournisseur de services de bureau intelligent et le fournisseur de capteurs et d'infrastructure prévoient une fonctionnalité permettant de confirmer les identités des entités et d'empêcher l'auteur d'une attaque de tenter d'usurper l'identité d'une entité autorisée.

– E-14: il est exigé que le fournisseur de services de bureau intelligent et le fournisseur de capteurs et d'infrastructure prévoient une fonctionnalité permettant de garantir la confidentialité des données, en particulier des données de localisation.

– E-15: il est exigé que le fournisseur de services de bureau intelligent et le fournisseur de données et de calculs prévoient une fonctionnalité permettant de garantir que seuls les utilisateurs autorisés puissent avoir accès aux données, en particulier aux données de localisation et de profil.

– E-16: il est exigé que le fournisseur de services de bureau intelligent et le fournisseur de données et de calculs prévoient une fonctionnalité permettant de confirmer les identités des entités et d'empêcher l'auteur d'une attaque de tenter d'usurper l'identité d'une entité autorisée.

– E-17: il est exigé que le fournisseur de services de bureau intelligent et le fournisseur de données et de calculs prévoient une fonctionnalité permettant de garantir l'intégrité des données de service, des données de localisation et des données de profil.

Pour ce qui concerne l'interface des services de bureau intelligent fondés sur la localisation, les exigences de sécurité qui découlent des menaces de sécurité correspondantes sont présentées dans le Tableau 4.

Tableau 4 – Exigences de sécurité relatives aux interfaces en fonction des menaces de sécurité

Menaces de sécurité	Exigences de sécurité
Reniflage de données	E-12, E-13
Déni de service	E-13
Fuite d'informations	E-13, E-14
Accès non autorisé aux données	E-15, E-16
Falsification des données	E-17

9.4 Exigences de sécurité relatives à la plate-forme

– E-18: il est exigé que le fournisseur de capteurs et d'infrastructure prévoie une fonctionnalité permettant de vérifier l'exactitude et l'intégrité de l'algorithme ou des algorithmes de localisation hybride(s).

– E-19: il est exigé que le fournisseur de services de bureau intelligent prévoie une fonctionnalité permettant de garantir que seuls les dispositifs ou applications autorisés puissent accéder aux services de bureau intelligent fondés sur la localisation.

– E-20: il est exigé que le fournisseur de services de bureau intelligent prévoie une fonctionnalité permettant de confirmer les identités des entités et d'empêcher l'auteur d'une attaque de tenter d'usurper l'identité d'une entité autorisée.

Pour ce qui concerne l'interface des services de bureau intelligent fondés sur la localisation, les exigences de sécurité qui découlent des menaces de sécurité correspondantes sont présentées dans le Tableau 5.

Tableau 5 – Exigences de sécurité relatives à la plate-forme en fonction des menaces de sécurité

Menaces de sécurité	Exigences de sécurité
Vulnérabilité des technologies de localisation hybrides	E-18
Exposition des capacités	E-19, E-20

9.5 Exigences de sécurité relatives aux applications intelligentes

– E-21: il est exigé que le fournisseur de services de bureau intelligent prévoie une fonctionnalité permettant de garantir que seuls les utilisateurs ou dispositifs autorisés puissent accéder aux données, en particulier aux données de localisation.

– E-22: il est exigé que le fournisseur de services de bureau intelligent prévoie une fonctionnalité permettant de garantir que seuls les dispositifs ou applications autorisés puissent accéder aux services de bureau intelligent.

– E-23: il est exigé que le fournisseur de services de bureau intelligent prévoie une fonctionnalité permettant de garantir que seuls les utilisateurs ou dispositifs autorisés puissent accéder aux services de bureau intelligent fondés sur la localisation.

– E-24: il est exigé que le fournisseur de services de bureau intelligent prévoie une fonctionnalité permettant de mettre en place un processus de réponse en cas d'incident relatif à la détection d'un logiciel malveillant, de déployer au préalable des mécanismes de sécurité pour réagir à une attaque et d'y faire face à temps.

Pour ce qui concerne les applications intelligentes des services de bureau intelligent fondés sur la localisation, les exigences de sécurité qui découlent des menaces de sécurité correspondantes sont présentées dans le Tableau 6.

Tableau 6 – Exigences de sécurité des applications intelligentes en fonction des menaces de sécurité

Menaces de sécurité	Exigences de sécurité
Utilisation non autorisée	E-21, E-22
Injection de chevaux de Troie et de virus	E-23, E-24

10 Fonctions de sécurité

Pour satisfaire aux exigences de sécurité applicables aux services de bureau intelligent fondés sur la localisation, plusieurs fonctions de sécurité sont possibles, notamment les suivantes:

– chiffrement des données et gestion des clés;
– gestion des identités et contrôle d'accès;
– vérification de l'intégrité;
– surveillance de la sécurité et réponse en cas d'événement lié à la sécurité;
– rappel à l'utilisateur.

10.1 Chiffrement des données et gestion des clés

Le chiffrement et la gestion des clés sont des mécanismes essentiels pour protéger la confidentialité des données dans les services de bureau intelligent. Le chiffrement fournit une approche fondée sur la protection des ressources, tandis que la gestion des clés assure le contrôle des clés de chiffrement.

Le chiffrement doit être conforme aux normes industrielles et nationales pertinentes. Cela inclut notamment les éléments suivants:

– chiffrement des données dynamiques dans les processus du service;
– chiffrement des données statiques dans la base de données;
– chiffrement des données dans le fichier de sauvegarde.

La gestion des clés comprend la génération, la distribution, le partage, le renouvellement et la révocation de clés de chiffrement pour la confidentialité et l'authentification des données. La gestion constitue le fondement de la sécurité du service et comprend notamment les éléments suivants:

– **Protection des informations concernant les clés**: les informations concernant les clés doivent être protégées en tant que données sensibles et le niveau de sécurité qui leur est attribué doit être plus haut que les autres.
– **Sauvegarde et récupération**: étant donné qu'un incident éventuel peut causer la perte d'une clé particulière et entraîner l'arrêt d'un service, il est essentiel de mettre en place une solution de sauvegarde et de récupération des clés.

10.2 Gestion des identités et contrôle d'accès

La gestion des identités doit être assurée pour les entités du service de bureau intelligent. Elle peut fournir les données brutes relatives au contrôle d'accès, aux autorisations et aux vérifications.

– Elle prend en charge la gestion des identités tout au long de leur cycle de vie, notamment l'enregistrement, l'attribution d'un rôle et d'une permission, la modification d'une permission et la suppression. En outre, l'enregistrement et la modification des identités doivent faire l'objet d'une procédure d'approbation par un administrateur.

– Elle prend en charge la gestion des mots de passe des entités, ce qui inclut l'ensemble des politiques de mot de passe des entités fondées sur la politique de sécurité du client, par exemple les algorithmes de chiffrement, la longueur et la complexité des mots de passe ainsi que la fréquence à laquelle ils doivent être modifiés. Elle peut prendre en charge différents types de mots de passe, tels que les mots de passe graphiques, les mots de passe fondés sur le son, etc. Elle peut également prendre en charge les fonctions de synchronisation et de réinitialisation des mots de passe.
– La gestion des identités doit inclure une politique de nommage des comptes concernant des identités ainsi qu'une politique de demande de comptes concernant des identités.

Le contrôle d'accès doit être assuré pour gérer l'accès au service de bureau intelligent par les entités. Il utilise l'identité authentifiée d'une entité ou la capacité d'une entité pour déterminer et faire appliquer les droits d'accès de celle-ci. Le contrôle d'accès peut rejeter les tentatives d'accès non autorisées ou incorrectes et les signaler, afin de déclencher une alarme ou de générer un journal d'audit de sécurité.

– La possession et la présentation des données d'authentification, telles que les mots de passe, comme preuve de l'autorisation d'accès dont bénéficie une entité.
– Étiquette de sécurité générée conformément à la politique de sécurité établie.
– Heure de la tentative d'accès.
– Trajet de la tentative d'accès.
– Durée de l'accès.
– Emplacement physique de la tentative d'accès.

10.3 Vérification de l'intégrité

La vérification de l'intégrité des données se fait sur deux niveaux:

– **Unité ou champ de données unique**: la vérification au niveau d'une unité de données unique comprend deux processus, l'un au niveau de l'entité expéditrice et l'autre au niveau de l'entité réceptrice. L'entité expéditrice associe aux données une quantité qui est fonction des données elles-mêmes. L'entité réceptrice génère une quantité correspondante et compare le résultat à la quantité reçue pour déterminer si l'élément de données a été modifié pendant la transmission.
– **Flux d'unités ou de champs de données**: la vérification du flux d'unités de données nécessite l'adjonction d'une forme d'ordonnancement explicite telle que la numérotation des séquences, l'horodatage ou le chaînage cryptographique.

Vérification de l'intégrité des données à l'aide d'un mécanisme déployé au préalable permettant de vérifier le format des données et d'un mécanisme de signatures numériques générées par chiffrement permettant de vérifier les données non altérées.

10.4 Vérification de l'intégrité des logiciels et du ou des algorithmes effectuée au moyen d'un mécanisme de signatures numériques générées par chiffrement – Surveillance de la sécurité et réponse en cas d'événement lié à la sécurité

La surveillance de la sécurité peut être fournie aux administrateurs de services afin qu'ils puissent examiner les dérangements de service ainsi que la qualité de fonctionnement. La surveillance comprend notamment les éléments suivants:

– **Surveillance de l'état de fonctionnement**: comprend la collecte et l'affichage du journal des événements de sécurité, des informations sur les vulnérabilités, de l'altération de la configuration des dispositifs de sécurité, de la qualité de fonctionnement et de l'état opérationnel du service. Cette fonctionnalité aide les administrateurs à connaître l'état général de fonctionnement des services.

– **Détection des comportements anormaux**: comprend la connexion illicite, l'accès illicite et l'accès en violation à des services spécifiques et les modifications anormales d'un dispositif physique.
– **Surveillance de la sécurité physique**: comprend le suivi de la température et de l'humidité, la télévision en circuit fermé (CCTV), la présence d'un gardien aux entrées, un système de protection incendie, une climatisation, un système d'alimentation électrique et des activités de surveillance.

La réponse en cas d'événement lié à la sécurité porte sur les demandes et le rétablissement provenant de mécanismes tels que les fonctions de traitement et de gestion des événements et entreprend des actions de récupération comme résultat de l'application d'un ensemble de règles.

10.5 Rappel à l'utilisateur

Le rappel à l'utilisateur constitue un mécanisme permettant de garantir que les données recueillies à partir du dispositif de détection seront utilisées après que l'utilisateur des services de bureau intelligent fondés sur la localisation aura autorisé leur utilisation.

L'essentiel est qu'un service de bureau intelligent fondé sur la localisation devant recueillir des données d'utilisateur le rappelle, le présente et l'explique brièvement à l'utilisateur. Un rappel peut être adressé à l'utilisateur pour lui indiquer s'il est prévu de recueillir des données et la nature des données qui seront recueillies. Les utilisateurs seront également informés de la façon dont les données seront traitées et gérées.

10.6 Relations entre les fonctions de sécurité et les exigences de sécurité

Le Tableau 7 présente les fonctions de sécurité à appliquer pour respecter les exigences de sécurité correspondantes relatives à un service de bureau intelligent fondé sur la localisation.

Tableau 7 – Exigences de sécurité relatives aux applications intelligentes en fonction des menaces de sécurité

Fonctions de sécurité	Exigences de sécurité	
Chiffrement des données et gestion des clés	Pour les données: E-01	
	Exigences de sécurité relatives aux dispositifs	E-09, E-10, E-11
	Exigences de sécurité relatives aux interfaces	E-14
Gestion des identités et contrôle d'accès	Exigences de sécurité relatives aux données	E-03, E-04, E-05
	Exigences de sécurité relatives aux interfaces	E-12, E-13, E-15, E-16
	Exigences de sécurité relatives aux plates-formes	E-19, E-20
	Exigences de sécurité relatives aux applications intelligentes	E-21, E-22, E-23
Vérification de l'intégrité	Exigences de sécurité relatives aux données	E-02, E-06
	Exigences de sécurité relatives aux interfaces	E-17
	Exigences de sécurité relatives aux plates-formes	E-18
Surveillance de la sécurité et réponse en cas d'événement lié à la sécurité	Exigences de sécurité relatives aux dispositifs	E-08, E-09
	Exigences de sécurité relatives aux applications intelligentes	E-24
Rappel à l'utilisateur	Exigences de sécurité relatives aux données	E-07

Bibliographie

[b-UIT-T X.1121] Recommandation UIT-T X.1121 (2004), *Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout*.

[b-ISO/CEI 9796-3] ISO/CEI 9796-3:2006, *Technologies de l'information – Techniques de sécurité – Schémas de signature numérique rétablissant le message – Partie 3: Mécanismes basés sur les logarithmes discrets*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Publié en Suisse
Genève, 2024