BADGES ET SÉCURITÉ

POUR LE CONTRÔLE D'ACCÈS

NCS
SCALINE

RÉSUMÉ

Les systèmes de contrôle d'accès physique font partie intégrante de l'infrastructure d'une entreprise et permettent son bon fonctionnement et la pérennité de son activité. A ce titre, les choix liés à l'emploi des moyens d'identification des personnes ont un impact considérable sur la sécurité globale de l'entreprise. On doit donc veiller à s'appuyer sur des technologies de badges permettant de sécuriser le contenu qui y est stocké. Cette sécurité doit être garantie tant au niveau du fonctionnement des tags qu'à celui de leur mise en œuvre spécifique par le système. Par ailleurs, pour s'assurer que le système garantisse ce niveau de sécurité, il doit aussi déployer des communications sécurisées entre tous les éléments du système : automates, lecteurs et serveur central. Enfin, les procédures et les outils mis à la disposition des opérateurs par le système doivent eux aussi garantir la pérennité des moyens sur lesquels s'appuie la sécurité des badges. Ce livre blanc détaille l'ensemble des critères qui doivent être garantis.

Le contrôle d'accès et les identifiants physiques

Usage des tags pour le contrôle d'accès

Dans un système de contrôle d'accès, des éléments sont utilisés pour identifier des personnes ou des objets et permettre à leur porteur d'accéder à des lieux sécurisés. Ils entrent en interaction avec le reste du système d'une façon qu'il est possible de décrire comme suit :

- le porteur présente son badge à un lecteur qui y lit un numéro.
- le système connecté au lecteur fait ensuite le lien entre ce numéro et un des usagers enregistrés dans sa base de données.
- Si ce numéro existe et correspond à un utilisateur possédant des droits d'accès sur une zone contrôlée par le lecteur sur lequel le tag a été lu, l'accès est autorisé.

Nous désignerons, dans la suite de ce document, ces éléments d'identification sous le terme générique de « tags ». Un tag est donc le moyen d'identification de son porteur pour permettre au système de décider si l'accès doit lui être permis. Etant donné l'investissement qu'un tel système représente, il est essentiel que ce tag offre le plus haut niveau de sécurité. Il est en effet au cœur de la fonction de décision d'accès.

Plusieurs problèmes se posent dès lors qu'une technologie doit être choisie pour intégrer cet usage :

- Des problèmes de protection de la vie privée du porteur de tag (qui ne seront pas abordés extensivement ici)
- Des problèmes concernant la sécurité de son détenteur
- Des problèmes concernant la sécurité du système qui l'utilise pour identifier les personnes.

Fonctionnement du tag

Le tag RFID contient un circuit électronique relié à une antenne intégrée. Ce circuit électronique contient :

- Un module de gestion de son alimentation
- Un module dédié à la communication avec un lecteur à travers un champ électromagnétique (interface RF)
- Un contrôleur gérant son comportement
- Un mémoire permettant d'y stocker des données
- Différents périphériques supportant des fonctions spécifiques (cryptographie, génération de nombres aléatoires, ...)

Lorsqu'un tag est présenté à un lecteur, celui-ci lui fournit, par induction électromagnétique, l'énergie nécessaire à son fonctionnement. On parle alors d'un tag passif. Il existe aussi des tags actifs possédant leur propre batterie. Le lecteur permet aussi d'établir un lien de communication avec le tag; dès lors qu'ils sont à proximité, un échange d'information peut se produire entre eux. Celui-ci peut être relativement simple, comme la diffusion unidirectionnelle d'une série de données, mais, pour des technologies plus évoluées, des commandes peuvent être envoyées depuis le lecteur. Le tag peut alors y répondre pour, par exemple, établir une authentification et permettre au lecteur de manipuler les données qui y sont stockées.

Pour les technologies conformes au standard ISO/IEC-14443, comme les badges des familles MIFARE® de NXP®, le tag fournit initialement un identifiant (ID), unique ou non, qui permet au lecteur de l'adresser pour toute la durée de la conversation, et ce, de manière à pouvoir le discriminer d'autres tags éventuellement présents dans son champ. En fonction de la technologie, d'autres fonctions sont aussi disponibles, comme la lecture de contenu stocké sur le tag (celui-ci étant éventuellement protégé par des algorithmes de chiffrement et d'authentification). Ces données sont stockées et lues directement à un emplacement « physique » dans la mémoire du tag ou manipulées à l'intérieur d'un système complexe, répartissant des fichiers au sein d'applications, ces dernières pouvant bénéficier d'une gestion de droits d'accès sécurisée.

La sécurité des tags et des identifiants.

Étant donnés la longue durée de vie des systèmes (un système de contrôle d'accès dure en moyenne 10 ans), la complexité des techniques employées et le coût que représente le remplacement de tous les tags présents dans une entreprise, les solutions déployés sont souvent exposés à des failles de sécurité liées à ces tags au regard des possibilités proposées par l'évolution technologique récente. Nous reprenons ici les principales et donnons une idée des solutions à adopter.

Les problèmes d'unicité et de clonage

Dans de nombreux systèmes existant aujourd'hui, on utilise encore l'identifiant (ID) envoyé au début de la session tag-lecteur comme moyen direct d'identification de son porteur. Ceci pose plusieurs problèmes de sécurité :

- Aujourd'hui, pour certaines de technologies, par exemple les tags MIFARE Classic®, on ne peut plus parler « d'identifiant unique » car la longueur du codage (parfois seulement de 4 octets / 32 bits) s'avère trop faible au regard du nombre de badges déployés.
- Par ailleurs, ce numéro passant « en clair » en début de session, toute personne, bien ou mal intentionnée, qui s'approcherait du tag avec une antenne serait libre d'observer leur conversation et de récupérer cet identifiant.

Ceci peut aussi induire des risques pour des usagers du système de contrôle d'accès : pour les technologies pour lesquelles le tag diffuse toujours le même numéro, il devient en effet possible, une fois ce numéro connu, de suivre une personne et de pouvoir retracer ses parcours ou détecter sa présence sans nécessairement être à proximité directe. De plus, il est à noter que, en fonction du type transpondeur NFC (Near Field Communication) présent dans les smartphone, il est possible de les placer en mode émulation de tag et, au moyen d'un logiciel dédié, de forcer la valeur de l'ID diffusée lors d'une transaction avec un lecteur. Ceci peut permettre à une personne qui aurait pu observer l'ID du tag d'un tiers, de se faire passer pour cette personne auprès du système de contrôle d'accès.

Il faut aussi prendre en compte qu'il existe, aujourd'hui sur le marché des tags MIFARE Classic contrefaits entièrement programmables, disponibles pour moins de 2€ pièce et pour lesquelles il est possible de reprogrammer la valeur de l'ID diffusé.

ID aléatoire et contenu mémorisé

Afin de contrecarrer ces problèmes, on devra utiliser des technologies gérant un identifiant aléatoire pour la création de la session tag-lecteur et différent pour chacune de ces sessions.

On veillera aussi à placer les identifiants des personnes utilisés par le contrôle d'accès, dans la mémoire embarquée du tag. L'accès à ce contenu devra, quant à lui, être protégé par l'usage de méthodes de sécurité appropriées, comme une authentification mutuelle entre le tag et le lecteur. L'usage des bons algorithmes et des bons protocoles de sécurité est important pour garantir la sécurité des informations stockées dans le badge et des échanges intervenants entre le lecteur et le badge.

Les algorithmes.

On s'assurera aussi que la technologie de badge utilisée supporte l'usage d'algorithmes et de protocoles modernes, standardisés, publiés et bien étudiés. On s'attachera aussi à ce que les études relatives à ces méthodes aient démontré leur fiabilité.

Dans ce contexte, il faudra éviter l'usage des badges de type « MIFARE® Classic® », qui utilisent l'algorithme propriétaire CRYPTO-1. Celui-ci, outre qu'il présente une taille de clé trop faible aujourd'hui, et bien qu'il n'ait jusqu'alors jamais été publié, a été cassé ; cela a fait l'objet de nombreuses publications entre 2007 et 2009. Des chercheurs ont ainsi pu le cryptanalyser et déterminer les clés secrètes manipulées par des tags s'appuyant sur lui, cela en quelques minutes sur un ordinateur standard de l'époque [1] [2]. Par ailleurs, NXP a depuis rendu publiques différentes notes d'applications reprenant des attaques possibles sur ces tags [3]. Sur ces bases, il a aussi été montré que l'émulation d'un tag MIFARE Classic volé était non-seulement possible, mais réalisable à l'aide de moyens limités [4]. Le grand nombre de faiblesses ainsi démontrées a mis en avant l'importance d'avoir des algorithmes bien étudiés et le danger d'une sécurité basée sur l'obscurité (entendez : l'emploi d'une méthode dont un des principaux arguments de sécurité est le secret de sa recette).

On privilégiera donc des technologies supportant des algorithmes publics et bien étudiés ainsi que des protocoles bien structurés. Pour ces raisons, AES (Advanced Encryption Standard) [5] est un algorithme à privilégier.

Les protocoles d'échange

Les protocoles doivent mettre en œuvre une identification active et mutuelle entre le tag et le lecteur (ou l'application derrière celui-ci) faisant intervenir

- des nombres aléatoires, différents pour chaque session d'identification, afin d'éviter des attaques impliquant de « rejouer » des échanges qui seraient déjà intervenus entre un tag et un lecteur et qui auraient pu être observés (une antenne suffisamment proche peut capter ces échanges) par un attaquant mal intentionné.
- la dérivation d'une clé de session, permettant de chiffrer et/ou authentifier la communication entre le tag et le lecteur et n'étant plus valide à la fin de cette session.

La protection des tags par l'architecture du système.

En dehors des aspects purement « mathématiques » de la sécurité apportés par la technologie utilisée, il faut aussi veiller à ce que la mise en œuvre de ces badges au sein d'un système garantisse le plus haut niveau de sécurité [6] . Certains aspects sont repris ici.

Cloisonnement des données

Il faut d'abord veiller à ce que les informations reprises sur le tag et les clés qui y sont mises en œuvre respectent des principes de cloisonnement. En effet, seul le système qui doit accéder aux données d'un tag devrait être autorisé à le faire. Si un autre système doit pouvoir identifier le porteur de ce badge, on veillera à configurer ce tag avec des données et des clés qui lui soient propres. De cette façon, si ce second système subit une faille de sécurité, ce n'est pas l'ensemble des systèmes déployés avec ce tag qui est compromis, mais seulement celui pour lequel une vulnérabilité a été exploitée. Dans ce cadre, on s'attachera à n'utiliser que des technologies supportant des applications multiples, chacune possédant son espace de fonctionnement privilégié.

Chiffrement des communications

Afin de garantir la confidentialité des données échangées, ainsi que leur intégrité et leur authenticité, on veillera à choisir (et à bien activer ces modes) des technologies supportant des communications chiffrées et authentifiées.

- Chiffrée : une clé de session dérivée lors de l'authentification est utilisée pour rendre la lecture des données échangées impossible par une entité qui n'aurait pas participé à cette authentification.
- Authentifiée : les messages, bien que déjà chiffrés, doivent être accompagnés d'un code d'authentification faisant appel à une clé, elle aussi dérivée de l'authentification. Ceci permet de garantir que le contenu du message n'a pas été altéré et qu'il provient bien d'une entité qui a participé à l'authentification.

Minimisation de la surface d'attaque

Ensuite, on préviendra aussi la vulnérabilité en cas d'attaque réussie sur un tag particulier. De cette façon, on choisira des architectures pour lesquelles la clé secrète utilisée pour un tag lui sera propre et ne pourra pas être utilisée pour casser la sécurité de l'ensemble du système.

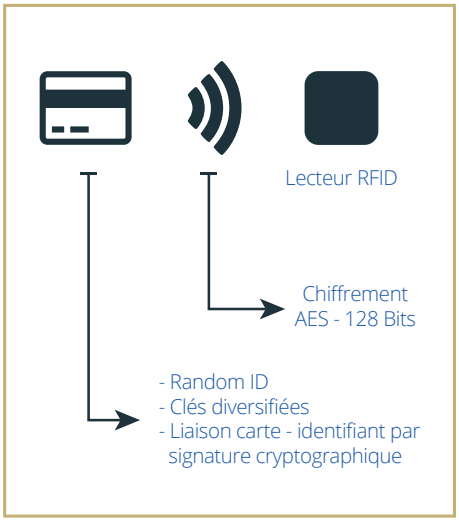
Il existe en effet des attaques qui permettent, pour certaines technologies, d'utiliser non pas des vulnérabilités des algorithmes utilisés, mais bien de leur mise en œuvre concrète au sein d'un circuit électronique ou d'un logiciel [10]. De cette façon, une attaque pratique a pu être montée sur un tag de type MIFARE DESFire® et qui a permis de retrouver les secrets manipulés par celle-ci [7].

Dès lors, si les secrets sont propres à chaque tag, une fois un tag attaqué éliminé du système (par exemple en le déclarant comme volé ou perdu pour qu'il soit exclu), cette attaque ne peut pas être utilisée pour mettre en péril l'intégralité du système.

Pour intégrer cette solution, on aura recours à « la diversification de clés ». Ce mécanisme, qui met en œuvre des algorithmes cryptographiques complexes, une clé secrète liée au système et des éléments uniques pour chaque badge (comme son numéro d'identifiant fixe), permet de déterminer, au moment de la programmation du badge, des secrets qui sont propres à celui-ci. Il implique cependant que le système, et donc, par extension, les lecteurs et/ou les éléments qui y sont connectés, soient capables de déterminer, à partir du secret « système », le secret propre à chaque tag, et de les utiliser dans des temps n'affectant pas le confort d'utilisation du système.

Sécurité renforcée contre une modification du contenu des tags.

En plus des mesures de sécurité citées ci-dessus, on peut encore renforcer le système en s'assurant que, si un attaquant venait à pouvoir casser un tag sans que son possesseur s'en rende compte, ou, tout du moins, sans que cela soit rapporté, il soit impossible de modifier le contenu du tag sans que cela soit détecté. En effet, à travers un mécanisme de signature numérique, on peut créer une signature du contenu du tag qui implique l'identifiant fixe non diffusé et une clé secrète, qui, elle, n'est pas présente sur le badge mais est bien connue du système qui doit identifier le porteur. Lorsque le tag est lu par le système, cette signature est transférée depuis le tag vers le lecteur (ou l'application qui y est connectée) en même temps que le contenu servant à l'identification du porteur. Le lecteur devant connaître l'identifiant fixe pour gérer la diversification des clés, il peut recalculer la signature sur base du contenu à protéger et de cet identifiant fixe et valider que la signature reçue du badge y correspond. Si ces données sont équivalentes, alors le contenu peut être considéré comme légitime.



La sécurité de l'équipement de contrôle d'accès

Les tags de contrôle d'accès devant dialoguer avec le système de contrôle d'accès, il faut prendre en compte que les éléments secrets garantissant la sécurité des tags sont eux aussi présents dans d'autres éléments du système et que celui-ci doit donc être sécurisé.

Le lien lecteur-automates

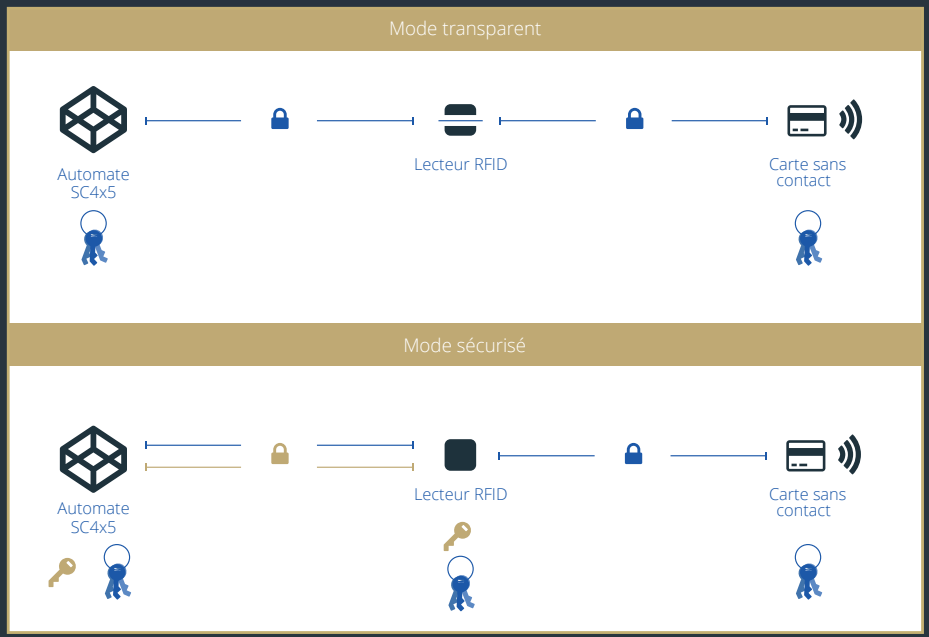
La solution idéale consiste à employer des lecteurs supportant un mode de communication dit « transparent » ; les lecteurs ne sont alors que des relais entre les tags et les éléments décisionnels du système. Dès lors, l'ensemble des clés reste, par exemple, dans la mémoire des automates logés en zone sécurisée et ceux-ci sont en charge de gérer l'ensemble de la communication avec les tags.
Si cela ne se révèle pas possible, on choisira des lecteurs garantissant, par un composants adéquat tel un SAM (Secure Access Module) ou HSM (Hardware Security Module), que les clés qui y sont stockées ne peuvent être extraites de leur mémoire. En effet, ces lecteurs, localisés en zone non-sécurisée, présentent un point d'entrée vulnérable sur le système pour un attaquant. Par ailleurs, ils devront pouvoir assurer un dialogue sécurisé (chiffré et authentifié) et bidirectionnel avec les éléments du système prenant les décisions d'accès (tels les automates de contrôle d'accès) afin de garantir le secret des identifiants lus sur un tag et d'éviter qu'un attaquant puisse écouter un dialogue valide et tenter de le rejouer.

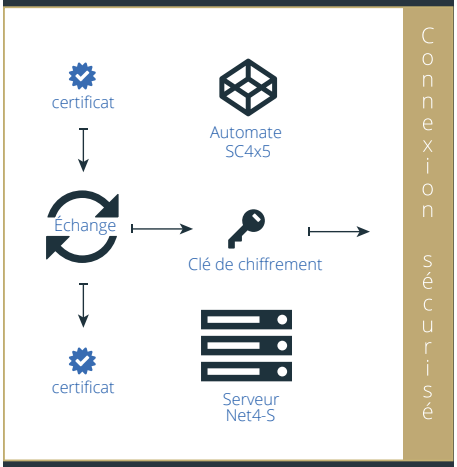
Ces deux solutions représentent un changement drastique au sein de l'infrastructure physique des communications. En effet, elles nécessitent d'abandonner le protocole dit « Wiegand », au moins au niveau des lecteurs, au bénéfice de protocole série comme le RS-232 ou le RS-485 pour établir une communication bidirectionnelle.

Au niveau de l'automate, on pourrait avoir recours à des modules de conversion, ceci ayant cependant les désavantages :

- De rajouter un coût et une source de panne potentielle supplémentaires à l'infrastructure ;
- De diminuer l'avantage que certains automates peuvent offrir puisque, lorsque l'on utilise des protocoles RS-485, plusieurs éléments peuvent partager un bus là où, sur un seul bus, un seul lecteur Wiegand peut être placé ;
- Dans le cadre de protocoles du type Wiegand, il peut être impossible de « descendre » les clés de manière centralisée dans les lecteurs alors que cela est inhérent à l'architecture si le contrôleur est en charge de gérer ces secrets. Dans le cas Wiegand, cela revient en outre à ajouter un élément de vulnérabilité par la présence de badges de programmation.
- Ces solutions nécessitent des automates de dernière génération pour lesquels une infrastructure cohérente existe et qui permettent un stockage garantissant la sécurité des éléments secrets.

«En mode transparent, l'automate gère directement tous les échanges avec les badges, et particulièrement leur sécurité. Le lecteur agit alors comme antenne relais. Pour le mode sécurisé, l'automate et le lecteur dialoguent sur un canal chiffré et l'automate fournit le clés nécessaires à la communication avec les badges. Le lecteur intervient cependant dans les échanges avec ceux-ci.»





«On peut s'appuyer sur des certificats cryptographiques pour prouver les identités de chacunes des entités communiquantes et négocier une clé de session. Les échanges sont alors chiffrés à l'aide de celle-ci pour établir un canal sécurisé.»

«Les opérateurs sont munis de badges spéciaux ne contenant que les secrets liés à leur niveau d'habilitation. A l'aide de ceux-ci et d'un mot de passe personnel, ils peuvent communiquer avec les badges d'accès, soit pour en lire, soit en modifier le contenu, par exemple, lors de leur programmation.»

Le lien serveur central–automates

Lorsque les automates sont en charge de gérer les secrets liés à la manipulation des tags, il faut s'intéresser à l'architecture permettant leur communication avec le serveur central. En effet, bien qu'ils soient localisés en zones sécurisées, il n'en va pas nécessairement de même des liens avec le serveur, qui dans certains cas, sont parfois partagés avec le reste de l'infrastructure réseau de l'entreprise.

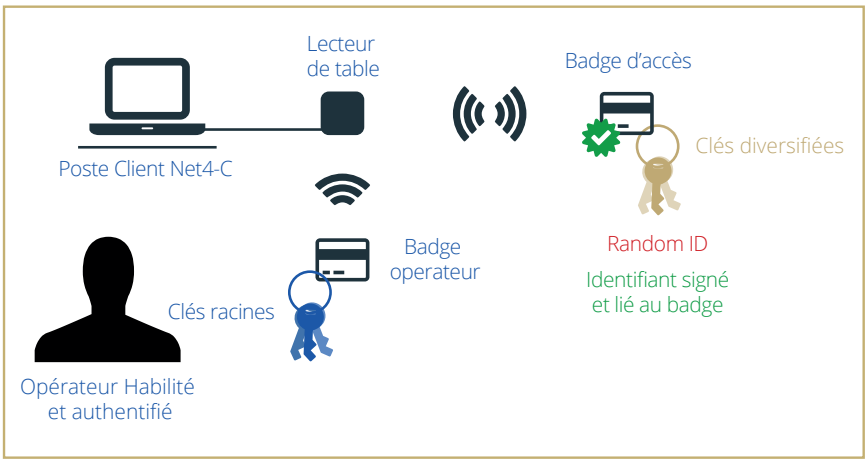
Différents principes peuvent alors être mis en œuvre pour garantir la sécurité des données échangées (dont les secrets utilisés pour les tags) sur ces liens de communication :

- Dédier l'infrastructure de communication avec les automates lorsque cela est possible. Qu'il s'agisse de mettre en place un VLAN (Virtual Local Area Network) ou un réel sous-réseau physique, si cela est possible, le réseau TCP/IP utilisé avec les automates devrait leur être dédié.
- Chiffrer les liens de communication, et surtout ceux passant dans des zones non sécurisées ou faisant intervenir des éléments du réseau (comme des switchs ou des routeurs) partagés avec d'autres infrastructures de l'entreprise. Dans l'idéal, on privilégiera l'utilisation de protocoles standardisés, comme TLS 1.2, puisqu'ils sont bien étudiés et régulièrement mis à jour pour palier d'éventuels défauts de sécurité. Dans le cadre de TLS, on privilégiera aussi l'utilisation de méthodes dites à « clés publiques » (PKI – Public Key Infrastructure) faisant intervenir des certificats cryptographiques. En effet, ces méthodes permettent des déploiements plus automatisés et mieux contrôlés que l'emploi de méthodes faisant intervenir des clés secrètes partagées (PSK – Pre-Shared Key).

Habilitations des opérateurs sur le système

Il faut par ailleurs garantir la sécurité des données sensibles du système liées à la manipulation des badges. En effet, parmi elles, on retrouve les clés de programmation et de lecture/écriture du contenu des tags de contrôle d'accès. On doit donc faire en sorte que les opérateurs du système n'aient accès qu'au minimum d'information leur permettant d'effectuer leur fonction sur le système. On ne donnera ainsi accès à la valeur réelle des clés qu'aux opérateurs qui doivent définir ces clés. Les autres devront posséder les moyens d'accéder à ces clés sans nécessairement en connaître la valeur. Cela peut se faire en leur fournissant des tags sécurisés et dédiés à leur usage personnel (ces tags ne contenant que les secrets qu'ils sont habilités à utiliser) ; le système aura accès au contenu de ces tags à travers une lecture de ces tags initiée par un mot de passe propre à l'opérateur et uniquement lié au contenu de son tag. Par ailleurs, de cette façon, ces clés n'étant pas stockées dans le système, cela prévient la divulgation d'information liée au système lors d'une attaque informatique de l'ordinateur hébergeant l'application.

En appliquant des procédures de travail obligeant de stocker ces tags dans des zones protégées lorsque l'opérateur ne doit pas les utiliser, on minimise aussi la possibilité qu'une perte entraine un danger pour la sécurité du système.



Conclusions

Les éléments précédents démontrent que le choix d'une méthode adéquate d'identification des usagers d'un système de contrôle d'accès impose une étude complète de celui-ci et des éléments technologiques qui le constituent. Le tableau ci-dessous résume les principaux points de sécurité auxquels les constituants du système doivent répondre.

Élément de sécurité	Elément Système	Description
Identifiant de tag aléatoire	Tag	Empêche un attaquant de rejouer une discussion entre le tag et le lecteur. Il protège aussi le porteur du tag en empêchant que l'on puisse l'identifier à partir de l'identifiant de son tag.
Identifiant des personnes stocké en mémoire	Tag	L'utilisation de la mémoire du tag et des mécanismes de protection d'accès associés assure que le contenu stocké ne soit consulté que par un « lecteur » correctement authentifié
Cryptographie de qualité	Tag Lecteur Automate Système	L'emploi d'algorithmes reconnus garantit la fourniture d'une sécurité correctement étudiée et ayant fait l'objet d'analyses pointues.
Communications sécurisées	Tag Lecteur Automate Système	L'emploi de communications chiffrées et authentifiées permet de garantir le secret et la non-modification de données confidentielles échangées entre ses éléments constituants.
Support de clés diversifiées	Tag Lecteur Automate	Les clés diversifiées permettent de garantir qu'une attaque réussie pour un seul tag n'impacte que sa sécurité et pas celle de l'ensemble du système.
Lien identifiant du tag – identifiant de la personne	Automate	Le lien entre l'identifiant du tag et celui de la personne permet de valider que le contenu du tag n'ait pas été altéré sans que le système en soit au courant.
Mode « Transparent »	Lecteur Automate	Permet d'obtenir un haut niveau de sécurité en concentrant l'ensemble des secrets dans l'automate placé en zone sécurisée et ne pouvant pas être dérobé afin d'y mener une attaque « off-line ».
TLS 1.2 et certificats	Automate Système	Permet de garantir un transport sécurisé vers l'automate des éléments servant à établir la sécurité des tags. L'emploi de certificats cryptographiques permet un déploiement aisé d'un plus haut niveau de sécurité que celui fourni par une authentification de type PSK sur TLS.
Limitation des secrets partagés aux opérateurs + stockage sécurisé	Système	Limitation de la surface d'attaque du système. Un opérateur qui n'a pas connaissance de la valeur d'un secret ne pourra pas le révéler. Le stockage sécurisé lui permet néanmoins de pouvoir le manipuler lorsqu'il en a besoin.

Un tel système offre de grandes garanties de sécurité et est conforme aux recommandations édictées, par exemple, par l'état Français à travers l'ANSSI [9]. Dans la gamme de produits de NCS®, l'option SECURE™ du système SCNET4™ permet de concevoir un système correspondant à celui décrit dans ce livre blanc. A travers cette option et l'emploi de tag en technologie MIFARE DESFire EV1, l'ensemble des critères établis ici sont rencontrés de façon économique et adaptable aux besoins particuliers de chaque installation. N'hésitez pas à nous contacter ou à consulter notre site internet (https://ncs-scaline.com/produits/scnet4-secure/).

BADGES ET SÉCURITÉ
POUR LE CONTRÔLE D'ACCÈS

Références

[1] Karsten Nohl, Starbug, Henryk Plötz, « Lost MIFARE obscurity raises concerns over security of OV-Chipkaart », https://www.cs.virginia.edu/~kn5f/OV-card_security.html

[2] Karsten Nohl, « Cryptanalysis of Crypto-1 », http://www.cs.virginia.edu/~kn5f/Mifare.Cryptanalysis.htm

[3] AN155122, « End to end system security risk considerations for Implementing MIFARE Classic », http://www.nxp.com/documents/application_note/155122_MIFARE_Classic_an.pdf

[4] Márcio Almeida, « Hacking MIFARE Classic Cards », Blackhat Regional Summit Sao Paulo 2014, https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf

[5] FIPS 197, Advanced Encryption Standard, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[6] AN10969 – System level security measures for MIFARE Installations (http://www.nxp.com/documents/application_note/AN10969.pdf)

[7] D. Oswald & C. Paar, « Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World », CHES 2011, présentation disponible à https://www.iacr.org/workshops/ches/ches2011/presentations/Session%205/CHES2011_Session5_1.pdf

[8] RFC5246, The Transport Layer Security (TLS) Protocol Version 1.2, https://tools.ietf.org/html/rfc5246

[9] ANSSI, « La sécurité des technologies sans contact pour le contrôle d'accès physique », http://www.ssi.gouv.fr/administration/guide/la-securite-des-technologies-sans-contact-pour-le-controle-des-acces-physiques/

[10] Y. Zhou, D. Feng, « Side-Channel Attacks : Ten years after its publication and the impacts on cryptographic module security testing », http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf

Notices pour la propriété intellectuelle

CONTACT
Site Internet : https://ncs-scaline.com
Email : contact@ncs-scaline.com