In-Webo Technologies

nCode iwlib 2.1

Cible de sécurité

1 Identification du produit et de la cible

Organisation éditrice	In-Webo Technologies
Lien vers l'organisation	http://www.in-webo.com
Nom commercial du produit	nCode iwlib
Numéro de la version évaluée	2.1
Catégorie de produit	librairie d'authentification forte

Version de la cible	Date	Auteur	Historique des modifications
0.1	20/4/2011	D. PERROT	Création du document, version de travail
0.2	16/6/2011	D. PERROT	Prise en compte de premières remarques formulées lors d'une réunion de travail avec le Centre de Certification
0.3	28/6/2011	D. PERROT	Prise en compte des remarques du Centre de Certification formulées sur la version 0.2 qui lui avait été transmise
0.4	27/10/2011	D. PERROT	Travail sur le contenu en vue de soumettre une version candidate au Centre de Certification
1.0	17/11/2011	D. PERROT	Cible pour l'évaluation

2 Argumentaire du produit

2.1 Description générale du produit

In-Webo nCode est un générateur universel de mots de passe à usage unique (OTP). Il se présente sous la forme d'une application s'installant et s'exécutant sur des plates-formes personnelles telles que des téléphones mobiles. La mise en œuvre de nCode permet de discriminer de façon plus fiable entre utilisateurs autorisés et attaquants que ne le fait un simple mot de passe. De plus, les fonctions de service disponibles sur nCode permettent une gestion plus simple des moyens d'authentification que lors de la mise en œuvre de moyens d'authentification à base de dispositifs matériels.

nCode iwlib est la librairie sur laquelle s'appuie nCode. nCode iwlib est disponible en C et java. La version soumise à évaluation est la librairie java.

L'usage principal permis par nCode – générer à la demande de l'utilisateur un OTP dédié à un service[1] – fonctionne de façon autonome, c'est-à-dire sans connexion ni échange de données avec un serveur distant. nCode est ainsi un outil d'authentification à la fois très simple d'usage, toujours disponible et opérationnel, et ne générant aucun coût de fonctionnement, ni pour les utilisateurs, ni pour les services requérant l'authentification.

L'algorithme de génération d'OTP embarqué dans nCode iwlib utilise des clés[2] stockées localement et, lorsque la politique du service requiert une authentification multi-facteur, le PIN[3] tel que saisi par l'utilisateur lors de la demande de génération d'OTP. Ces clés et informations sont utilisées comme paramètres d'entrée de fonctions à sens unique, en l'occurrence SHA-256. Certaines des clés sont mises à jour par la librairie à chaque demande de génération d'OTP, on parle de « clés dynamiques aléatoires ». Enfin, le stockage local de certaines des clés utilise un chiffrement AES128 mis en œuvre au niveau applicatif par la librairie nCode iwlib.

nCode iwlib offre également plusieurs « fonctions de service » telles que celles permettant pour l'utilisateur l'ajout d'un nouveau service, la réinitialisation du PIN associé à nCode, la réinitialisation de l'application si elle avait été bloquée intentionnellement ou non. Ces fonctions nécessitent la connexion de l'application aux serveurs de l'infrastructure d'In-Webo.

2.2 Description de la manière d'utiliser le produit

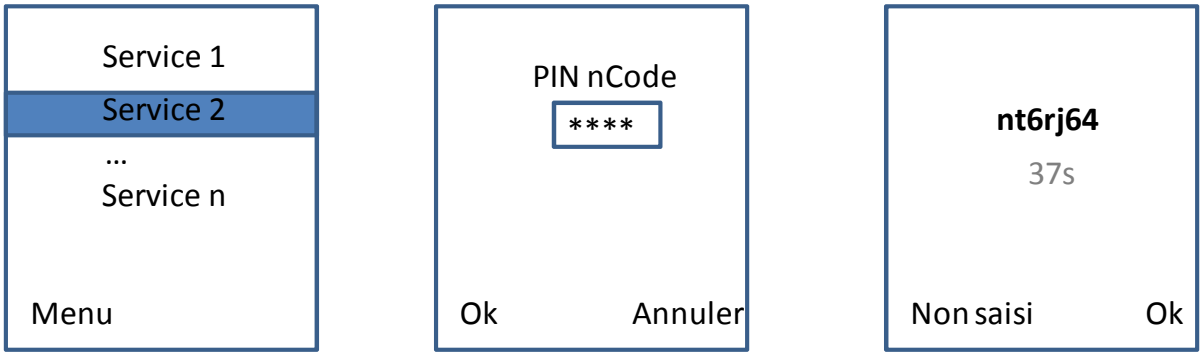
L'utilisateur doit lancer l'exécution de l'application nCode puis sélectionner le service pour lequel il souhaite obtenir un OTP. Si la politique de ce service l'exige, l'utilisateur doit alors saisir son code PIN. L'OTP est affiché, ainsi qu'un compte à rebours indiquant le laps de temps durant lequel il doit

[1] On désigne génériquement par « service » l'entité requérant l'authentification de ses utilisateurs. Il peut s'agir d'un service en ligne ou d'un site web grand public, d'une application professionnelle, d'un centre d'appel, etc. Le service implémente la partie serveur du protocole d'authentification (vérification) ou délègue cette implémentation à un prestataire spécialisé.

[2] Il ne s'agit pas de clés au sens cryptographique du terme, mais de données associées à un instant donné à un utilisateur et à un service

[3] Il s'agit d'une information secrète choisie par l'utilisateur lors de l'activation de nCode. L'utilisateur n'a pas à connaître la politique du service, celle-ci est implémentée par nCode - et bien sûr également par le serveur d'authentification

être fourni au service. A tout moment – lors de la saisie du PIN, lors de l'affichage de l'OTP, pendant une période après l'expiration du compte à rebours -, l'utilisateur peut annuler l'opération. Annuler l'opération lorsque l'OTP n'est pas réellement utilisé sur un service permet d'optimiser l'expérience utilisateur mais n'a pas d'influence sur le fonctionnement ni la sécurité du produit.



Etape 1 : lancement de l'application nCode et sélection d'un service

Etape 2 : saisie du PIN

Etape 3 : connexion manuelle au service en utilisant son login et l'OTP affiché par nCode

Fig 1 : Génération d'un mode de passe à usage unique avec l'application nCode

Pour mettre en œuvre les « fonctions de service », l'utilisateur doit lancer l'exécution de l'application et sélectionner la fonction souhaitée dans un menu. Selon la fonction, il doit ensuite saisir son code PIN et/ou des informations propres au contexte. Selon le support où nCode est installé, l'utilisateur peut devoir autoriser l'ouverture d'une connexion par nCode à un serveur distant[4]. nCode indique ensuite le résultat de l'opération effectuée, réussite ou échec.

Etape 1 : lancement de l'application nCode et choix d'une fonction de service dans le menu, ici l'ajout d'un nouveau « Favori » (service)

Etape 2 : saisie du PIN et du code d'activation

Etape 3 : confirmation

Fig 2 : Exemple de mise en œuvre d'une fonction de service, ici l'ajout d'un nouveau service (« Favori »)

[4] Lorsque nCode est installée sur un téléphone mobile, l'ouverture d'une connexion par une application requiert en général la confirmation explicite de l'utilisateur. Sur certains modèles de téléphone, le fait que l'application soit signée avec un certificat reconnu dans la chaîne de confiance embarquée dans le téléphone permet d'ouvrir des connexions sans confirmation explicite de l'utilisateur.

Un cas particulier de fonction de service est la personnalisation (activation) initiale de nCode pour cet utilisateur et pour un premier service. La spécificité de l'activation est que l'utilisateur n'a pas besoin de sélectionner cette fonction dans un menu : tant que nCode n'a pas été passé dans l'état activé, c'est la seule opération qu'il propose à l'utilisateur.

2.3 Description de l'environnement prévu pour son utilisation

nCode permet d'implémenter un contrôle d'accès pour des services à distance.

Les services à distance désignent par exemple des services Internet pour les professionnels ou les particuliers (l'OTP généré doit être saisi dans un formulaire d'un navigateur web), des services accessibles via un centre d'appel (l'OTP généré est dicté à un opérateur ou saisi sur un clavier téléphonique multifréquence), des applications disponibles sur un terminal ou une borne (l'OTP généré est saisi sur l'IHM de ce terminal ou de cette borne), etc.

Le service à distance doit implémenter la partie serveur du protocole d'authentification mis en œuvre côté client par nCode iwlib, ou déléguer cette implémentation à un acteur spécialisé, et dans ce cas être en mesure d'adresser des requêtes d'authentification à cet acteur.

De façon privilégiée, nCode est destiné à être installé et utilisé sur un téléphone portable ou un smartphone, outils personnels et toujours à portée de main des utilisateurs. L'environnement technique est précisé dans le §3.

2.4 Description des hypothèses sur l'environnement

H1) Le service à distance est présumé de confiance et opérationnel :

- Il doit être en mesure d'associer l'OTP avec un profil utilisateur déclaré dans le serveur d'authentification ;

H2) Le support sur lequel est exécuté nCode doit posséder des moyens d'embarquement et d'exécution d'applications ainsi qu'une capacité de se connecter à un serveur distant *lors de la personnalisation initiale et de la mise en œuvre des fonctions de service*. C'est en particulier le cas des téléphones portables utilisés sur des réseaux mobiles permettant la transmission de données en mode paquet ; l'utilisateur n'a pas besoin pour cela d'avoir souscrit une option particulière, il faut néanmoins que les services data soient autorisés sur la SIM insérée dans le téléphone portable (cette condition n'est pas systématiquement remplie pour des flottes d'utilisateurs en entreprise).

H3) L'utilisateur n'a pas enregistré son « code PIN » dans le support de nCode, ni dans une messagerie si celle-ci est accessible sans sécurité supplémentaire depuis le support de nCode ; il ne communique pas ce code PIN à des tiers

H4) L'utilisateur n'installe pas d'applications malveillantes sur le même support que nCode, et il n'autorise de connexions extérieures que pour des applications de confiance

H5) Le support sur lequel s'exécute nCode est protégé et à jour des dernières mises à jour de sécurité disponibles

2.5 Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit

Pas de dépendance identifiée au-delà des hypothèses faites au paragraphe 2.4

2.6 Description des utilisateurs typiques concernés (utilisateurs finaux, administrateurs, experts…) et de leur rôle particulier dans l'utilisation du produit

U1) Les utilisateurs de nCode autant pour générer un OTP que mettre en œuvre une fonction de service sont des utilisateurs finaux. Les fonctions de service peuvent requérir la saisie par l'utilisateur d'une information (« code d'activation ») fournie à l'utilisateur par le service à distance, par des moyens et canaux qui lui siéent – et de toutes façons indépendants de nCode, donc en dehors du champ de cette évaluation. Ils ne sont pas considérés hostiles, ni sciemment complices d'un agent menaçant, ni excessivement négligents (H3, H4, H5).

U2) Les administrateurs du service à distance (hors périmètre de l'évaluation) ne sont pas considérés comme hostiles, non pas parce qu'ils auraient une facilité accrue à générer des menaces contre le produit, mais parce qu'ils n'ont pas besoin d'attaquer la solution d'authentification pour accéder à un compte utilisateur ou aux ressources qu'il recèle. Dans le cas général, ces personnes n'administrent pas les applications nCode des utilisateurs ni leurs téléphones.

2.7 Définition du périmètre de l'évaluation, à savoir les caractéristiques de sécurité du produit concernées par l'évaluation

Les fonctions du produit incluses dans le périmètre de l'évaluation sont les suivantes :

- Génération d'un OTP à la demande
- Mise en œuvre d'une fonction de service

Elles sont décrites plus précisément dans le §6.1.

Ces fonctions mettent en œuvre

- Une IHM non soumise à évaluation
- La librairie nCode iwlib implémentant les fonctions de sécurité

3 Description de l'environnement technique dans lequel le produit doit fonctionner

3.1 Matériel compatible ou dédié

Equipement tel qu'un téléphone portable ou une tablette possédant un environnement d'exécution d'application (natif ou machine virtuelle java) et une capacité de connexion, par exemple équipé d'une carte SIM pour laquelle les fonctions data ne sont pas interdites, ou d'une connexion WiFi.

3.2 Systèmes d'exploitation retenus

Tout système d'exploitation ou environnement pour lequel une application In-Webo nCode utilisant la librairie iwlib 2.1 en java est disponible (téléphones ou tablettes java midp2.0, blackberry, android,

windows mobile). L'iOS n'en fait pas partie car pour ce système d'exploitation, la librairie utilisée par nCode est une librairie C (et non java).

4 Description des biens sensibles que le produit doit protéger

Les biens sensibles que le produit doit protéger sont les éléments d'information – clés et PIN utilisateur – dédiés à un utilisateur et à une application nCode qu'il détient, permettant de prédire des OTP de cet utilisateur, et donc de se faire passer pour cet utilisateur[5] auprès du service à distance mettant en œuvre une solution d'authentification incluant nCode.

Dans le détail, il s'agit

- Pour la mise en œuvre d'une fonction de service
  - D'une clé statique K_0 propre à une application nCode donnée, une fois celle-ci activée pour un premier service
  - D'une clé dynamique K_1 propre à une application nCode donnée, mise à jour lors de chaque mise en œuvre d'une fonction de service
  - Du PIN saisi par l'utilisateur lorsqu'il souhaite obtenir un OTP ou mettre en œuvre une fonction de service, défini lors de l'activation de nCode et modifiable ultérieurement grâce à une fonction de service dévolue à cet usage ; le PIN n'est pas stocké dans le terminal de l'utilisateur
- Pour la génération d'OTP
  - D'une clé dynamique K_1 propre à une application nCode donnée
  - D'une clé statique m_s propre à une application nCode et un service donnés, une fois ce service activé sur cette application
  - De clés dynamiques h, j, k propres à une application nCode donnée à un moment donné, mises à jour totalement ou partiellement lors de chaque mise en œuvre de la fonction de génération d'OTP
  - Du PIN saisi par l'utilisateur lorsqu'il souhaite obtenir un OTP ou mettre en œuvre une fonction de service ; le PIN n'est pas stocké dans le terminal de l'utilisateur

L'OTP généré est également sensible, au sens commun du terme, puisqu'il permet de se connecter au service sous l'identité de l'utilisateur - certes pendant un temps limité et une seule fois – mais n'est pas considéré comme un bien protégé par le produit, puisqu'il est affiché en clair et pendant près d'une minute par l'application nCode afin que l'utilisateur le saisisse dans le formulaire d'authentification du service.

5 Description des menaces

Les agents menaçants considérés sont les personnes tentant de prédire un OTP valide afin de se faire passer pour l'utilisateur auprès du service à distance. On considère plusieurs types d'agents menaçants, selon qu'ils effectuent des attaques « côté client » ou « côté serveur » :

[5] Dans les faits, il faudrait que l'attaquant possède d'autres informations (identifiant utilisateur, compteurs, numéro de série du téléphone, etc.) mais ces informations ne sont pas susceptibles d'être protégées ni en général, ni en particulier par le produit objet de l'évaluation.

- Attaquants « côté client » ou externes : tentent de prédire des OTP ou cloner l'application nCode, soit en volant le support de l'utilisateur, soit en effectuant une attaque ciblée sur ce support, le cas échéant interceptant les OTP saisis par l'utilisateur ;

- Attaquants « côté serveur » ou internes : tentent de prédire des OTP ou de cloner l'application nCode en accédant aux informations sensibles côté serveur d'authentification ; il peut en particulier s'agir d'un administrateur de l'acteur spécialisé mettant en œuvre le serveur d'authentification pour le compte du service à distance

Les attaques « côté serveur » ne sont pas directement liées à la cible et sortent du périmètre de l'évaluation. Elles sont « assurées » par l'hypothèse H1 sur l'utilisateur U2 et par des moyens techniques distincts du produit.

Description des menaces :

Les menaces prises en compte sont les suivantes :

M1) Un attaquant externe tente d'obtenir un ou plusieurs biens sensibles à partir de valeurs d'OTP observées, valides ou non

M2) Un attaquant externe tente d'obtenir le PIN et les biens sensibles chiffrés localement (j, k, m_s), en ayant accès à l'application nCode qui se trouve sur le support de l'utilisateur ou en ayant réalisé une attaque ciblée sur ce support

M3 (= M1+M2) Un attaquant externe tente d'obtenir le PIN et les biens sensibles chiffrés localement (j, k, m_s), en ayant accès à l'application nCode qui se trouve sur le support de l'utilisateur ou en ayant réalisé une attaque ciblée sur ce support, et en observant des valeurs d'OTP valides

6 Description des fonctions de sécurité du produit

Les fonctions de sécurité du produit dédiées à la protection en confidentialité et en intégrité des biens sensibles sont les suivantes :

Blocage du PIN

Le serveur bloque l'usage d'une application nCode donnée dès lors que 3 codes PIN faux consécutifs ont été mis en œuvre depuis cette application, quelle que soit la fonction considérée (génération d'un OTP ou fonction de service), et ce afin qu'un attaquant externe ne puisse pas déterminer ce PIN par déduction d'essais répétés. Le blocage lui-même n'est pas implémenté par la librairie, mais s'appuie sur la mise en œuvre du code PIN dans les fonctions de la librairie, génération d'OTP et fonctions de service.

Lors de la réception d'OTP aléatoires – c'est-à-dire qui n'ont pas été calculés par l'application nCode de l'utilisateur ciblé -, le serveur peut ne pas bloquer l'application nCode de l'utilisateur, d'une part parce que la probabilité de succès de ces essais est arbitrairement bornée, d'autre part parce qu'ils ne menacent pas les biens sensibles. En revanche, pour les fonctions de service exécutées depuis le

support de l'utilisateur, tout code PIN faux incrémente le compteur d'erreur conduisant à bloquer l'application.

Protection en confidentialité des clés stockées

Afin de ne pas être transmises en clair via l'OS ni stockées en clair, certaines des clés (j, k, m_s) sont chiffrées au niveau applicatif grâce à une clé dérivée du code PIN saisi par l'utilisateur et de données de l'environnement de l'application. En particulier, la librairie ne propose aucune fonction de chiffrement/déchiffrement à l'application hôte et ne fait aucune hypothèse de confiance, ni vis-à-vis de cette application, ni vis-à-vis de l'OS.

Protection en confidentialité des clés échangées lors de la mise en œuvre d'une fonction de service

Afin de ne pas être transmises en clair via l'OS, les clés *reçues du serveur* (K_0, K_1, h, j, k) sont chiffrées au niveau applicatif grâce à une clé dérivée du code PIN saisi par l'utilisateur et de données de l'environnement de l'application.

Les *clés transmises au serveur* (clé m_s et code PIN initialement défini par l'utilisateur) sont chiffrées par la partie publique de clés pouvant être protégées par un équipement de sécurité physique implémenté dans l'environnement du serveur d'authentification. Ces clés publiques sont fournies à la volée par le serveur, leur intégrité étant vérifiée grâce à une « clé usine » codée dans la librairie nCode iwlib.

Protection contre le key-logging du PIN

Lorsque le support de l'utilisateur le permet (écran tactile), le PIN est saisi via le clavier virtuel de l'application nCode, afin d'éviter que cette information ne circule en clair via l'OS. Ce clavier virtuel a vocation à devenir un clavier dynamique. N'étant pour le moment que partiellement mise en œuvre sur les matériels compatibles et les OS retenus, cette fonction de sécurité n'est PAS intégrée à la cible.

Protection en confidentialité des clés utilisées dans le calcul d'OTP

L'OTP calculé, susceptible d'être intercepté, dépend non seulement du PIN saisi par l'utilisateur et de clés statiques (m_s, K_1), mais également de clés dynamiques aléatoires (h, i, j, k).

Si aucun des biens sensibles n'a été exposé (menace M1 seule), leur calcul à partir d'observations de valeurs d'OTP est impossible du fait de la non-inversibilité des fonctions utilisées dans le calcul d'OTP.

Si certaines des clés ont été exposées (menace M2 : vol du support, copie de l'application ou attaque ciblée du support), le PIN reste bien protégé *même en cas d'interception d'OTP qui en dépendent* (menace M3), car du fait de la non-inversibilité des fonctions intervenant dans le calcul de l'OTP, l'attaquant recherchant le PIN doit effectuer une recherche exhaustive a minima sur le PIN et les clés dynamiques aléatoires, celles-ci ayant évolué entre le moment où elles ont pu être exposées et le moment où des OTP valides sont interceptés.

Dans le cas général où l'attaquant ne dispose pas d'information sur l'utilisation de l'application par l'utilisateur entre le moment où des clés ont été exposées et le moment où les OTP valides sont

interceptés, cette recherche exhaustive est infaisable en pratique (a minima de l'ordre de 2^{140} opérations dans l'implémentation fournie pour évaluation).

Dans le cas particulier où l'attaquant dispose d'informations supplémentaires précises et peut ainsi cibler sa recherche non pas sur les clés dynamiques aléatoires mais directement sur les aléas[6] qu'il n'a pas observés, la recherche exhaustive peut s'avérer faisable, mais le résultat sera inexploitable[7] s'il ne dispose pas d'une quantité suffisantes d'informations (OTP valides) au regard des informations qu'il recherche (PIN + aléas). En pratique pour l'implémentation fournie à évaluation, il suffit d'un ou deux OTP (aléas) non-observés pour que la valeur du PIN ne soit plus distinguable parmi les multiples solutions obtenues par l'attaquant, du fait des 3 essais maximum autorisés par le serveur d'authentification.

Protection en intégrité des biens sensibles

L'attaquant peut modifier des biens sensibles stockés s'il a accès au support où l'application nCode est installée, puisque les supports envisagés (téléphones ou tablettes) n'offrent pas, en général, de protection en intégrité. En revanche, cette modification est purement locale et ne concerne pas la version serveur des biens sensibles, ni le PIN qui n'est pas stocké par nCode.

On peut remarquer que la modification de la valeur locale des biens sensibles n'apporte aucun avantage à l'attaquant, notamment il ne peut pas 'tester' de valeurs de PIN supplémentaires par rapport aux 3 autorisées par le serveur.

La protection en intégrité des biens sensibles découle in fine du fait que, de par les fonctions de sécurité énumérées ci-dessus, l'attaquant ne peut pas s'authentifier en qu'utilisateur dans une fonction de service, ni vis-à-vis d'un service. Il ne peut donc pas exécuter avec succès une fonction de service qui lui permettrait de mettre à jour un secret (PIN) ou de régénérer un bien sensible (K_0, K_1 ou m_s par exemple).

[6] Les aléas sont générés par la librairie de l'application nCode à chaque mise en œuvre de la génération d'OTP ; ils permettent notamment de mettre à jour les clés dynamiques

[7] Beaucoup, voire toutes valeurs de PIN seront solutions du système d'équations à résoudre par l'attaquant