NOTE TECHNIQUE 28042000

Rédacteur : Élie AOUAD

Analyse et Attaques contre les dispositifs calculettes

Je dédie ce document à M. JM ROUX

1. Introduction

J'ai assisté récemment à une présentation sur l'utilisation des calculettes dans le monde Internet. Je ne ferai pas de commentaire sur certaines choses qui ont été dites:

- quel était le premier composant DES qui a été créé dans le monde,
- ni sur les brevets liés à l'utilisation des mots de passe dynamiques,
- ni sur l'idée de la transformation de nombres en succession de points lumineux sur écran PC (la grenouille de la société IBSI a été crée il y a une douzaine d'années).

Je ferai juste une analyse de ces dispositifs calculettes, et donnerai les arguments en faveur ou contre leur utilisation.

Mais je commence par dire que dans tous les cas il ne faut pas oublier d'appliquer une méthodologie de sécurité (risques, besoins, évolution, normes) avant tout choix de solution.

2. Présentation

Le dispositif calculette se présente souvent sous la forme d'une calculatrice. Sa première fonctionnalité est de fournir des mots de passe dynamiques ; ce qui permet une authentification dite forte basée sur la possession du dispositif et la connaissance d'un PIN pouvant activer le dispositif lui même.
A chaque utilisation d'un dispositif un nouveau mot de passe est généré et est affiché sur l'écran de la calculette. Le propriétaire présente le nouveau mot de passe à son application. Côté serveur un logiciel permet de vérifier en fonction de l'horodatage et du propriétaire si le mot de passe est bon.

Ce schéma peut être amélioré par authentification basée sur le principe de question réponse. Le serveur génère un nombre aléatoire qu'il envoie vers l'utilisateur. Celui-ci saisit le nombre aléatoire sur la calculette ou le capte par les détecteurs de la calculette, qui lui rend une réponse. La réponse est ensuite transmise au serveur qui la vérifie.

Une deuxième fonction est le scellement de données. L'utilisateur introduit une succession de données à sceller sur sa calculette qui lui rend le sceau. La calculette prend en compte l'identité de l'utilisateur, l'horodatage, et les données pour calculer le sceau. Ce qui a été présenté par le fabricant était un sceau de 6 digits basé sur du M.A.C. Le fabricant de cette calculette présente ce sceau comme une signature (car le sceau est basé sur l'identité de la personne).

3. En faveur de la calculette

La calculette présente une facilité d'utilisation sans égal :
Pas d'installation de logiciels chez les utilisateurs,
Indépendance du type de la machine, du système d'exploitation, du réseau.
La calculette peut être utilisée sur des terminaux VTxx, Questar, PC, Mac, GSM, ….

Compte tenu du coût unitaire de la calculette et du manque de coût d'installation une solution basée sur les calculettes est relativement économique.

Dans un environnement fermé (réseau local, terminaux passifs, ….) l'utilisation de la calculette pour le contrôle d'accès reste intéressante. Aucun fichier de mots de passe à gérer ! ! ! Mais surtout aucun risque de rejeu.

4. Contre la calculette

On va considérer les deux fonctions.

4.1 Contrôle d'accès/ Authentification

Envisageons maintenant un environnement ouvert de type Internet avec accès Web par exemple :
L'attaque de base est la mascarade par l'homme au milieu (Man in the Middle) ; qui consiste à intercepter la communication (p.e. au niveau d'un routeur) et à se présenter pour le client en tant que serveur et pour le serveur en tant que client. Quand le serveur demande à l'utilisateur d'être authentifié , l'attaquant présente la requête au véritable client puis transfère la bonne réponse au serveur. Le serveur considère alors l'attaquant comme un véritable client, qui a dans ce cas tout type d'accès sur le serveur.
Est ce que le SSLV2 (authentification du serveur) améliore les choses ? Oui partiellement. Mais l'attaque est toujours la même en utilisant un certificat auto-signé.
Est ce que le SSLV3 (authentification mutuelle) améliore les choses ? Oui partiellement. Mais l'attaque est toujours la même en utilisant un certificat auto-signé et en interceptant les échanges de certificats. Mais supposons que cette attaque est tellement difficile qu'elle ne peut pas arriver. Dans ce cas à quoi sert une calculette : A RIEN ! ! l'authentification par SSLV3 étant plus forte.

4.2 Scellement/ Signature

L'une des premières attaques que j'ai appris il y a plusieurs années est l'attaque par les dates d'anniversaire qui se résume à la problématique suivante :
Dans une assemblée quel est le nombre minimal de personnes présentes pour qu'au moins deux personnes aient la même date d'anniversaire (jour et mois) avec une probabilité de 50%. Le résultat peut étonner certains mais il est de 23 . (Voir dans la page divertissement pour le calcul).
L'application de cette attaque dans le monde cryptographique est que la date correspond au sceau et que les personnes correspondent aux données scellées. Deux messages avec un même sceau correspondent à une collision. Cette fréquence est croissante en fonction du nombre de messages. D'où l'une des caractéristiques d'un bon algorithme de scellement est de diminuer la fréquence des collisions et d'offrir une bonne taille de sceau (128 ou 160 bits actuellement) ; qui dans le cas des dates d'anniversaire consiste à prendre en compte l'année et lieu de naissance aussi.

Autre attaque est l'attaque exhaustive sur résultat connu. Là connaissant le sceau du message attaqué quel est le temps nécessaire pour arriver à un message ayant le même sceau que le message attaqué ? Ce temps est d'autant plus important que la taille du sceau est plus importante.

Revenons un petit peu à nos fameuses calculettes :

- Sceau sur 6 digits (1000000 de valeurs possibles) ! ! ! taille très largement inférieure à 128 ou 160 bits hexa.
- Je me suis amusé de simuler les attaques (sources sur simple demande à eaouad@easeit.fr). L'attaque des dates d'anniversaire donne 1178 messages. L'attaque exhaustive donne souvent moins que 5 secondes (66% des essais) pour arriver à un autre message ayant le même sceau sur 6 digits.
- Sur le serveur : un logiciel est utilisé pour la vérification. Or le schéma de scellement est basé un algorithme symétrique (DES ou 3DES). Donc le logiciel serveur doit faire le même scellement que l'utilisateur et de le comparer au résultat de l'utilisateur. Même si uniquement la fonction de vérification est offerte sur le serveur, un bon débogueur permet de tomber sur le routine de calcul du sceau qui précède tout simplement le memcmp dans la fonction de vérification. Imaginons donc côté serveur un exploitant qui fait un scellement/signature sur une transaction bancaire ! !
- Et dans le cas de litige : un bon avocat et un bon expert informatique peuvent facilement démontrer que le serveur peut calculer de la même façon de sceau (signer) que le client.

5. Conclusions et Conseils

Il est intéressant d'utiliser la calculette en authentification pour:
Les projets Internet où les risques d'attaques par l'homme au milieu sont peu probables (projets pour particuliers par exemple où le jeu ne vaut pas la chandelle) , ou des projets en réseau fermé.

Il est fortement déconseillé d'utiliser les calculettes dans les schémas de signature surtout dans le cadre de projets pour entreprises. Malgré la lourdeur des PKIs, ils offrent les meilleurs schémas de signature.

Mais dans tous les cas il faut toujours commencer par appliquer une méthodologie de sécurité (risques, besoins, évolution, normes) avant toute offre de solution.