Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

Sécurité des Usages TIC

Examen — mai 2024

Durée : 1h30 — Tous documents autorisés

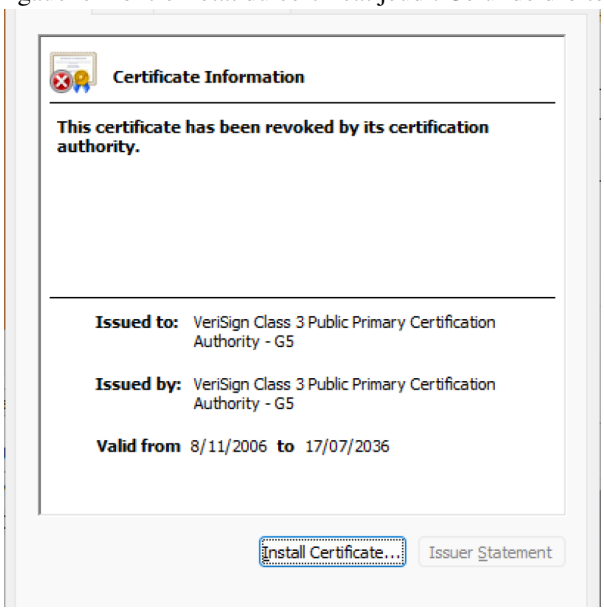
PKI & Certificats — 13 points

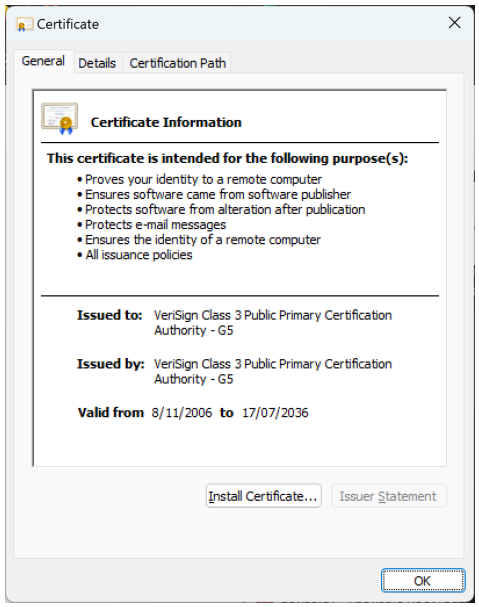
Certificat renégat supprimé de Windows. puis il revient. Microsoft reste silencieux.
Le certificat, créé à l'origine par Symantec, devait être banni il y a des années.
Ars Technica – Dan Goodin - 8/26/2023, 1:41 AM

Depuis trois jours, les administrateurs système corrigent les erreurs qui empêchent les utilisateurs de Windows d'exécuter des applications telles que Quick Books et Avatax. Nous en connaissons maintenant la cause : une décision ou un glitch de Microsoft qui a supprimé un certificat numérique autrefois largement utilisé dans Windows.❶

L'élément supprimé est appelé certificat racine, ce qui signifie qu'il assure la confiance de centaines ou de milliers de certificats intermédiaires et individuels. Le certificat racine, portant le numéro de série 18dad19e267de8bb4a2158cdcc6b3b4a et l'empreinte digitale sha1 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5, n'était plus reconnu comme fiable dans Windows. Parce que cette racine était liée à des certificats qui certifient l'authenticité et la confiance d'applications, les personnes essayant d'utiliser ou d'installer ces applications ont reçu une erreur. ❷

Quelques minutes seulement avant la mise en ligne de cet article, les chercheurs ont appris que le certificat avait été restauré dans Windows. On ne sait pas comment ni pourquoi cela s'est produit. Le certificat de gauche montre l'état du certificat jeudi. Celui de droite montre l'état vendredi. ❸





L'époque où les certificats de Symantec étaient bannis d'Internet

Microsoft n'a pas encore répondu à une demande d'explication des erreurs. Il se peut qu'un problème ait amené Windows à supprimer le certificat racine. Il est également possible que la suppression ait été intentionnelle, étant donné qu'il s'agit de l'un des nombreux cas de blocage complet suite à la découverte en 2015 que son émetteur parent de l'époque, Symantec, avait émis de manière inappropriée des certificats pour google.com, www.google.com, et un autre domaine. (Symantec a vendu ses activités d'autorité de certification (ca) à DigiCert en 2017.) ❹

Après que des chercheurs de Google ont affirmé quelques semaines plus tard que le nombre de certificats émis de manière frauduleuse était beaucoup plus élevé, Symantec a révisé ce nombre à 164 certificats pour 76 domaines et à 2 458 certificats pour des domaines qui n'avaient jamais été enregistrés. À la lumière de ces nouvelles informations, Google a lancé un ultimatum à Symantec : rendre compte en détail des difficultés de son processus d'autorité de certification ou risquer que le navigateur le plus populaire au

monde, Chrome, émette des avertissements de sécurité sur les certificats Symantec chaque fois que les utilisateurs finaux visitaient des sites Web protégés par https qui les utilisaient. ❺
Quelque 17 mois plus tard, Google a mis sa menace à exécution après que son enquête a conclu que pendant des années, les ACs, propriété de Symantec, avaient émis de manière frauduleuse plus de 30 000 certificats. La société a commencé à annuler progressivement la confiance de Chrome dans tous les certificats émis par ces ACs, qui étaient vendus sous des marques telles que Verisign, Thawte et GeoTrust. À compter de ce moment-là, Chrome a cessé de reconnaître le statut de Validation Étendu, « *Extended Validation* », EV, de ces certificats et, au fil du temps, le navigateur a révoqué de plus en plus sa confiance. ❻
Les certificats frauduleux représentent une menace critique pour la quasi-totalité de la population d'Internet ; ils permettent aux titulaires d'usurper l'identité cryptographiquement des sites concernés, et de surveiller ou de falsifier les communications échangées entre les visiteurs et les serveurs légitimes. En particulier, les certificats pour des domaines inexistants ou des domaines appartenant à des parties autres que le titulaires, constituent des violations majeures des exigences dites de base, « *baseline* », que les principaux fabricants de navigateurs imposent au ACs comme condition pour que leur logiciel leur fasse confiance. ❼

1 – 13pts **Questions :**

a. Pourquoi les utilisateurs ne pouvaient plus utiliser ou installer des outils tels que Quickbox et Avatax ❶ ? *(1pt)*

b. Pourquoi le numéro de série d'un certificat est important ❷ ? *(1,5pts)*
À quoi sert-il?
Pouvez vous donner un exemple où il est indispensable ?

c. Une empreinte SHA1 est fournie : à quoi sert-elle ❷ ? *(1,5pts)*
Comment est-elle calculée ?
L'usage de SHA-1 est déconseillé, est-ce important ?

d. Comment l'ordinateur fait-il la différence entre les deux états du certificat ❸ ? *(1pt)*
Y-a-t-il un risque qu'un ordinateur utilise quand même le certificat?

e. Pourquoi est-ce possible que Symantec ait pu émettre un certificat pour Google ❹ ? *(1,5pts)*
Est-ce dangereux ?
Comment peut-on se prémunir contre cela ?

f. Pourquoi est-il difficile de connaître le nombre total de certificats émis par Symantec ❺ ? *(1,5pts)*
Est-ce qu'un service de la PKI permet de le savoir ?
Lequel s'il existe ?

g. Qu'est-ce qu'un certificat EV ❻ ? *(1pt)*

h. Pourquoi les propriétaires de ces certificats peuvent usurper cryptographiquement l'identité des sites affectés ❼ ? *(2pts)*
Comment peuvent-ils intervenir dans les communications entre un utilisateur et le serveur légitime ?

i. Quelles recommendations donneriez vous à un utilisateur lors de la connexion de son navigateur à un site important, pour éviter de se faire abuser par ces certificats frauduleux dans le cas où son navigateur ne lui dit rien ? *(2pts)*

Analyse de risques – 4 points

2 – 4pts Dans l'objectif d'une analyse de risque, comparez une PKI avec une solution de type Kerberos ?
Vous vous limiterez aux critères DICT.

Modélisation de protocole – 3 points

3 – 3pts

a. Concernant les protocoles cryptographiques, expliquer la différence entre **l'authentification de message** et **l'authentification d'agent**. Considérez l'échange ci-dessous, K_{AB} est une clé symétrique connue seulement de A et de B, N_A est un nonce. *(1pt)*
- $A \rightarrow B : A, N_A$
- $B \rightarrow A : \{B, N_a, \text{"}4u2c\text{"}\}K_{ab}$

b. Cet échange permet-il **l'authentification du second message** ? *(1pt)*

c. Cet échange permet-il **l'authentification d'un agent** par un autre (si oui lequel ou lesquels) ? *(1pt)*