Attacke

auf die

Authentifizierung

Wichtigkeit der Feststellung der verschiedenen Identitätskennungen und des Identity Management im PKI Umfeld

Version 1.5
Juni 2004

Daniel Muster
Bit Pattern Security
Feldblumenweg 43
8048 Zürich

Attacke auf die Authentifizierung

Einleitung

Worum geht es

Anhand verschiedener Attacken soll gezeigt werden, dass mit der Identifikation einer Person oder Instanz[1] noch nicht genug bestimmt worden ist, damit ein Zertifikat problemlos ausgestellt werden kann. Die soeben erwähnten Attacken können die Authentisierung umgehen, ohne dass ein kryptographischer Algorithmus gebrochen werden muss, sofern mindestens einer der folgenden Bedingungen erfüllt ist:

- Bei der Zertifikatsausstellung sind gewisse Felder nicht richtig oder gar nicht ausgefüllt worden.
- Die Sicherheitsapplikation weist gewisse Schwächen in der Auswertung der Zertifikatsinhalte auf.
- Der Benutzer ignoriert gewisse Warnungen beim Browser, bei der E-Mail oder einer anderen Applikation.

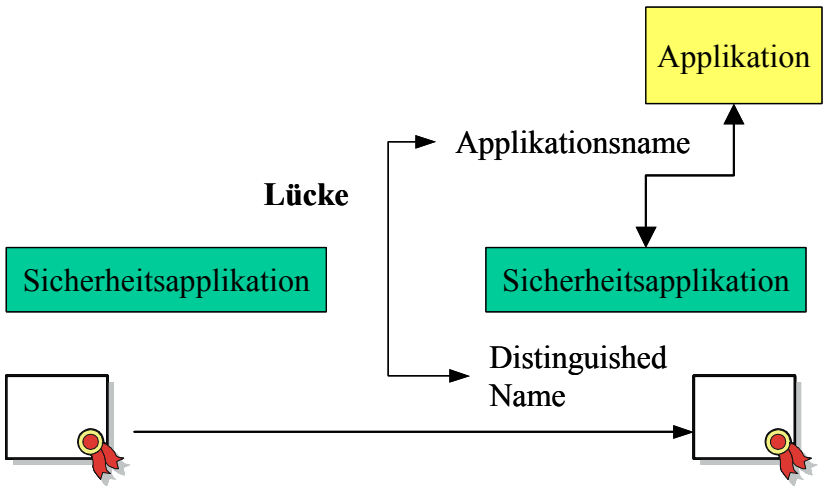
Prinzip der Attacke

Eine Applikation, welche sensitive Daten austauscht, wird durch eine Sicherheitsapplikation oder Sicherheitstechnologie geschützt, welche auf Public Key Verfahren basiert. Die Authentifizierung einer Instanz oder Person geschieht mit einer auf Public Key Verfahren basierenden Sicherheitsapplikation/-technologie grundsätzlich in folgenden Schritten:

- Zuerst wird das Zertifikat der zu authentifizierenden Person/Instanz überprüft.
- Dabei wird u.a. verifiziert, ob das Zertifikat noch gültig ist, d.h. nicht abgelaufen, nicht bereits revoziert worden ist und eine gültige Signatur aufweist.
- Verläuft diese Verifikation erfolgreich, wird überprüft, ob die zu authentifizierende Person/Instanz im Besitz des privaten Schlüssels ist, welcher mit dem öffentlichen Schlüssel im Zertifikat übereinstimmt. Dabei muss die zu authentisierende Person/Instanz eine Operation mit ihrem privaten Schlüssel durchführen (lassen). Die Person/Instanz muss aber den privaten Schlüssel der Gegenpartei nicht verraten, um die Gegenpartei zu davon überzeugen, dass sie im Besitz des privaten Schlüssels ist.
- Die Gegenpartei, welche authentisiert, verifiziert den Besitz des privaten Schlüssels mit Hilfe des dazu passenden öffentlichen Schlüssels im Zertifikat der zu authensierenden Person/Instanz.

[1] Eine Instanz muss nicht eine natürliche Person sein, sondern kann ein Server, ein Programm sein.

Die Attacke nutzt nun aus, dass die Hauptidentitätskennung im Zertifikat (Distinguished Name) in den meisten Fällen anders ist, als die Identitätskennung derselben Person/Instanz in der zu schützenden Applikation. Die Sicherheitsapplikation verwendet nämlich für dieselbe Person/Instanz meist eine andere Identitätskennung als die zu schützende Applikation. Die Attacke nutzt nun diese Lücke oder die Unterschiedlichkeit der verschiedenen Identitätskennungen aus, um die Authentisierung zu umgehen.



Darstellung der Lücke bei Identitätskennung zwischen Sicherheitsapplikation und der zu schützenden Applikation.

Beispiele für unterschiedliche Identitätskennungen:

- Im Zertifikat der Distinguished Name, im E-Mail die E-Mail Adresse
- Im Zertifikat der Distinguished Name, auf dem Web Server die URL Adresse (z.B. http://www.sorglos.ch)
- Im Zertifikat der Distinguished Name, Username bei SAP

In folgenden Unterkapiteln wird je für den Schutz der E-Mail und für die SSL/TLS Verbindung mit einem Browser exemplarisch gezeigt, wie die Attacke funktioniert. Dabei wird zwischen folgenden Fällen unterschieden:

- Die Sicherheitsapplikation weist gewisse Schwächen in der Auswertung der Inhalte der Zertifikate auf.
- Bei der Zertifikatsausstellung sind gewisse Felder gar nicht ausgefüllt worden.
- Im Zertifikat sind gewisse Felder nicht richtig ausgefüllt.
- Der Benutzer ignoriert gewisse Warnungen beim Browser, bei der E-Mail oder einer anderen Applikation.

Attacke bei E-Mail

Sicherheitsapplikation mit Schwächen

In diesem Unterkapitel wird erklärt, wie eine Attacke auf die Authentizität einer E-Mail gestartet werden kann, welche digital signiert worden ist. Die Attacke nutzt dabei eine mögliche Schwäche bei der Implementation der Sicherheitsapplikation aus. Die Schwäche liegt dann vor, wenn die Sicherheitsapplikation der E-Mail die Absenderadresse mit dem Feld Subject Alternative Name[2] im Zertifikat **nicht** vergleicht, in dem der öffentliche Schlüssel zur Verifikation der digitalen Signatur enthalten ist.

Angenommen, eine Sicherheitsapplikation einer E-Mail vergleicht **nicht** die Absenderadresse mit dem Feld Subject Alternative Name im Zertifikat, in dem der öffentliche Schlüssel zur Verifikation der digitalen Signatur enthalten ist. Dann kann folgende Attacke erfolgen:

> Alice und Bob haben ein Vertrauensverhältnis und Bob führt die von Alice in der E-Mail beschriebenen Wünsche aus.
> Carl kann nun eine E-Mail mit der Absenderadresse von Alice verfassen, wie alice.sorglos@trust.com. Er signiert die E-Mail aber mit seinem privaten Schlüssel und stellt die E-Mail Bob zu. Die Sicherheitsapplikation von Bob verifiziert die Signatur und stellt dabei fest, dass sie gültig ist.
>
> **Nota bene:** Die Sicherheitsapplikation (S/MIME, Outlook oder Lotus [Plugin]) hat bei der Prüfung des Zertifikats das Zertifikat von Carl genommen und den darin enthaltenen öffentlichen Schlüssel verwendet.
>
> Da die Sicherheitsapplikation keine Fehlermeldung herausgibt, nimmt Bob zu Recht an, dass die Signatur gültig ist. Er merkt aber nicht, dass die Signatur nicht von Alice stammt. Bob nimmt aber wegen der Absenderadresse von Alice nämlich an, dass die E-Mail von Alice stammt, und führt die in der E-Mail enthaltenen Instruktionen aus.

Damit die Attacke funktioniert, müssen folgende Voraussetzungen miteinander erfüllt sein:

- Bob muss bei der Sicherheitsapplikation die CA als vertrauenswürdig erklären, welche das Zertifikat von Carl ausgestellt hat. Dies erfolgt meistens dadurch, dass das entsprechende CA Zertifikat in die Sicherheitsapplikation/-technologie aufgenommen wird.
- Die Sicherheitsapplikation beim Empfänger vergleicht die E-Mail Adresse im Zertifikat **nicht** mit der E-Mail Adresse des Absenders.

[2] Im Feld Subject Alternative Name kann u.a. die E-Mail Adresse des Zertifikatbenutzers enthalten sein.

Felder im Zertifikat nicht vorhanden

Angenommen, im Zertifikat ist die E-Mail Adresse von Carl nicht aufgeführt, dann funktioniert die vorher beschriebene Attacke noch besser, denn eine einwandfreie Sicherheitsapplikation kann die E-Mail Adresse im Zertifikat mit der E-Mail Adresse des Absenders gar nicht vergleichen. Somit kann sie keinen Fehler entdecken, was dem Verhalten gemäss RFC 2632 entspricht.

Damit die Attacke funktioniert, muss folgende Voraussetzung erfüllt miteinander sein:

- Bob muss bei der Sicherheitsapplikation die CA als vertrauenswürdig erklären, welche das Zertifikat von Carl ausgestellt hat.

Felder im Zertifikat nicht korrekt ausgefüllt

Angenommen, Carl kann eine Zertifizierungsstelle (CA) dazu veranlassen, ihm ein Zertifikat mit der E-Mail Adresse von Alice alice.sorglos@trust.com auszustellen, dann funktioniert die beschriebene Attacke auch wunderbar. Damit die Attacke funktioniert, müssen folgende Voraussetzungen miteinander erfüllt sein:

- Bob traut der CA, welche das Zertifikat von Carl ausgestellt hat. Bob hat z.B. das entsprechende CA Zertifikat in seine Sicherheitsapplikation geladen und als vertrauenswürdig deklariert.
- Die CA kontrolliert nicht, ob die von Carl bei der Zertifikatsausstellung angegebene E-Mail Adresse zu Carl gehört.

Benutzer ignoriert Warnmeldung

Die Sicherheitsapplikation funktioniert einwandfrei, und die E-Mail Adresse im Zertifikat ist korrekt ausgefüllt worden. Startet nun Carl die Attacke, dann sollte die Sicherheitsapplikation bei Bob nach der Attacke durch Carl eine Warnmeldung anzeigen. Ignoriert der Benutzer die Warnmeldung, z.B., weil er diese nicht versteht, dann funktioniert die Attacke auch. Dass ein ungeschulter Benutzer die Warnmeldung nicht versteht und der Warnmeldung zuwider handelt, ist des Öfteren der Fall.

Browser

Im Browser Umfeld ist zu unterscheiden, ob

1. die Authentisierung des Client (Alice)
2. oder die Authentisierung des Server (Bob) umgangen wird.

Im ersten Fall hängt es davon ab, wie der SSL/TLS Server die Identitätskennung der authentisierten Person/Instanz an die zu schützende Applikation übergibt. In den meisten Fällen erfolgt eine solche Übergabe der Identitätskennung vom SSL/TLS Server an die zu schützende Applikation nicht, sondern der Benutzer muss sich noch einmal mit Username und Passwort anmelden. Hierbei kann niemanden Carl daran hindern, den Username von Alice und deren Passwort einzugeben, sofern er beides kennt.

Ermöglicht der SSL/TLS Server eine Übergabe einer Identitätskennung im Zertifikat an die zu schützende Applikation, dann hängt der Erfolg der Attacke davon ab, ob die Identitätskennung im Zertifikat richtig angegeben worden ist und korrekt an die Applikation übergeben wird.

Im zweiten Fall (Umgehung der Authentisierung des Server) hängt die erfolgreiche Attacke davon ab, ob die URL Adresse des Server im Zertifikat aufgeführt ist und überprüft wird. In den kommenden Unterkapiteln werden die folgenden, verschiedenen Fällen bezüglich der Überprüfung der URL Adresse behandelt:

- Die Sicherheitsapplikation weist gewisse Schwächen in der Auswertung der URL Adresse im Zertifikat auf.
- Im Zertifikat ist die URL Adresse gar nicht aufgeführt.
- Bei der Zertifikatsausstellung ist die URL Adresse falsch ausgefüllt worden.
- Der Benutzer ignoriert gewisse Warnungen beim Browser.

Sicherheitsapplikation mit Schwächen

Angenommen, Carl vermag beim DNS Server die IP Adresse von Bob zur URL Adresse von Bob (www.bob-sorglos.ch) mit einer IP Adresse von seinem Server auszutauschen. Folglich werden die HTTP Pakete beim Aufstarten von Bobs Adresse im Browser an Carls Server gesandt. Der Server von Carl hat Carls Zertifikat gespeichert und liefert dieses beim SSL/TLS Handshake aus.

Falls die Sicherheitsapplikation im Browser die URL Adresse im Zertifikat mit der URL Adresse im Browser nicht vergleicht, merkt niemand, dass er mit einem anderen Server kommuniziert.

Nota bene: Die Sicherheit der Authentisierung des SSL/TLS Server hängt nun einzig von der Sicherheit des DNS Server und des Netzwerks ab.

Voraussetzungen für das Funktionieren der Attacke sind:

- IP Adresse von Bob kann bei der URL Adresse von Bob ausgetauscht oder die IP Pakete mit Zieladresse von Bob können zum Server von Carl umgeleitet werden.
- Der Browser vertraut der CA, welche Carls Zertifikat ausgestellt hat.

Felder im Zertifikat nicht vorhanden

Falls die URL Adresse im Zertifikat von Carl nicht enthalten ist und die Sicherheitsapplikation bei der Prüfung der URL Adresse dies nicht beanstandet, dann funktioniert die Identifikation des Server einwandfrei und niemand merkt etwas, sofern der entsprechende Eintrag im DNS Server vorgenommen werden konnte.

Voraussetzungen für das Funktionieren der Attacke sind:

- IP Adresse von Bob kann bei der URL Adresse von Bob ausgetauscht oder die IP Pakete mit Zieladresse von Bob können zum Server von Carl umgeleitet werden.
- Der Browser (Alice) vertraut der CA, welche Carls Zertifikat ausgestellt hat.

Felder im Zertifikat nicht korrekt ausgefüllt

Angenommen, Carl kann eine Zertifizierungsstelle (CA) dazu veranlassen, ihm ein Zertifikat mit der URL Adresse von Bob auszustellen, wie beispielsweise www.admin.ch, www.ubs.com, www.cs.com. Dann funktioniert die beschriebene Attacke auch wunderbar.

Damit die Attacke funktioniert, müssen folgende Voraussetzungen erfüllt sein:

- Alice traut der CA, welche Carls Zertifikat ausgestellt hat. Alice hat z.B. das CA Zertifikat in ihren Browser geladen und als vertrauenswürdig deklariert.
- Die CA kontrolliert nicht oder nicht sorgfältig genug, ob die von Carl bei der Zertifikatsausstellung angegebene URL Adresse zu Carl gehört.
- Die IP Adresse zur URL Adresse von Bob kann ausgetauscht oder die IP Pakete mit Zieladresse von Bob können zum Server von Carl umgeleitet werden.

Benutzer ignoriert die Warnmeldung

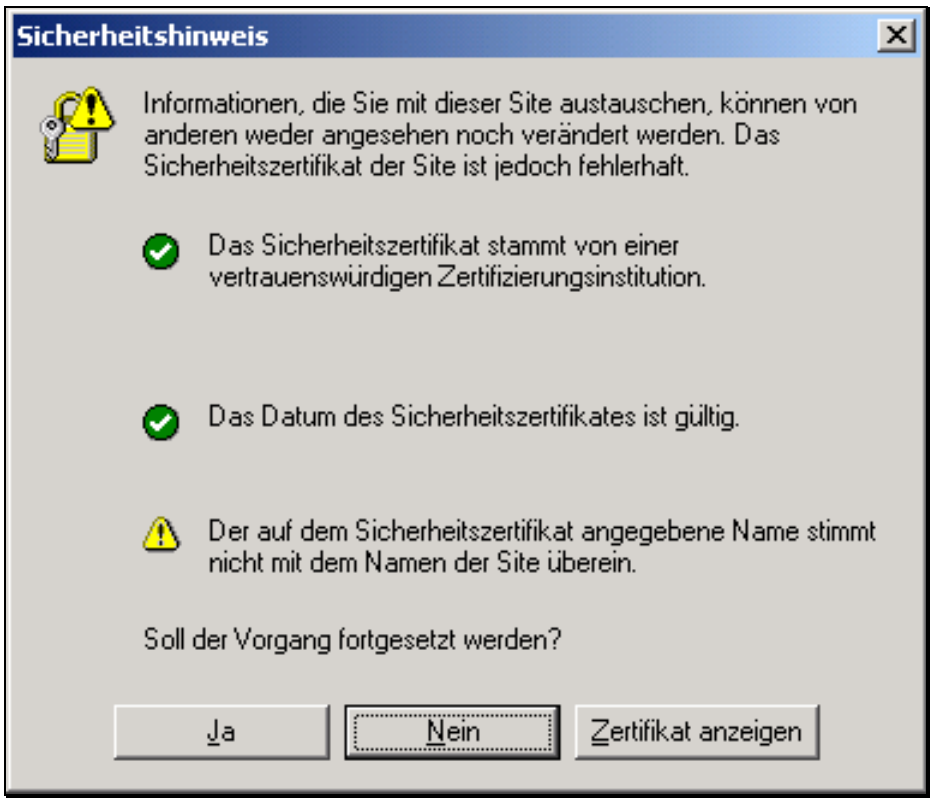
Die Sicherheitsapplikation funktioniert einwandfrei, d.h.:

- Die URL Adresse im Zertifikat wird mit derjenigen im Browser verglichen.
- Ein Unterschied in den beiden URL Adressen oder eine fehlende URL Adresse im Zertifikat wird dem Benutzer gemeldet und beanstandet.

Weiter sind die URL Adressen bei allen Zertifizierungsstellen, welche in der Sicherheitstechnologie/-applikation als vertrauenswürdig deklariert worden sind, korrekt ausgefüllt worden.

Startet nun Carl die Attacke und tauscht die entsprechende IP Adresse beim DNS Server aus, dann sollte die Sicherheitsapplikation bei Alice nach der Attacke durch Carl eine Warnmeldung anzeigen. Ignoriert der Benutzer, hier Alice, die Warnmeldung oder versteht sie nicht, dann funktioniert die Attacke auch. Dass ein ungeschulter Benutzer die Warnmeldung nicht versteht und der Warnmeldung zuwider handelt, ist des Öfteren der Fall.

In folgender Abbildung ist die Fehlermeldung dargestellt, welche erscheint, wenn die URL der angewählten Web Seite nicht mit der URL im Zertifikat übereinstimmt:



Fehlermeldung im Browser (URL Adresse im Zertifikat nicht identisch mit der URL Adresse der angewählten Web Seite)

Dass ein in Public Key Verfahren unversierter Benutzer (User) eine solche Fehlermeldung ignorieren kann, ist aus Sicht des Autors verständlich.

Risiken

Nota bene: Grundsätzlich sind die hier vorgestellten Attacken nicht nur im Browser/Server und im E-Mail Umfeld anwendbar, sondern überall, wo eine Applikation mit einer auf Public Key basierenden Sicherheitstechnologie, wie z.B. IPSEC, abgesichert wird. Wesentlich ist dabei einzig, dass die Identitätskennungen der Personen/Instanzen im Zertifikat und in der Applikation unterschiedlich sind.

In folgenden Unterkapiteln wird eine Einschätzung darüber gemacht, wie hoch die Risiken aus Sicht des Autors für die hier vorgestellte Attacke sind. Dabei wird wieder zwischen folgenden Fällen unterschieden:

- Die Sicherheitsapplikation weist gewisse Schwächen in der Auswertung der Inhalte der Zertifikate auf.
- Bei der Zertifikatsausstellung sind gewisse Felder gar nicht ausgefüllt worden.
- Im Zertifikat sind gewisse Felder nicht richtig angegeben worden.
- Der Benutzer ignoriert gewisse Warnungen beim Browser, bei der E-Mail oder einer anderen Applikation.

Sicherheitsapplikation mit Schwächen

Was die Authentisierung des Server betrifft, ist Folgendes zu bemerken:

> Dass eine Sicherheitsapplikation die Identitätskennung im Zertifikat mit der entsprechenden Identitätskennung in der zu schützenden Applikation nicht ordentlich vergleicht, ist im Browser Umfeld eher selten.

Doch was die Authentisierung der Client und deren Autorisierung beim Server betrifft, gibt es sicherlich noch Applikationen, welche keine Autorisierung auf Basis einer Identitätskennung im Zertifikat vornehmen können.

Bei Sicherheitstechnologien, welche E-Mails schützen, sind noch vor kurzem entsprechende Technologien auf dem Markt gewesen, welche die hier beschriebene Schwäche aufweisen. Dies ist aber im Widerspruch dazu, was in der entsprechenden RFC 2632 gefordert wird.

Es gibt sicherlich bei den verschiedenen Implementationen bestehender Sicherheitstechnologien die hier beschriebenen Mängel zu beanstanden. In jedem Fall sind die jeweiligen Sicherheitstechnologien auf die hier beschriebenen Schwächen zu testen.

Risiko: Die Häufigkeit, dass eine Sicherheitsapplikation eine solche Schwäche aufweist, ist eher selten im Browser und E-Mail Umfeld, doch bei Outlook Plugins ist zu verifizieren, ob die Schwäche vorhanden ist. Bei IPSEC z.B. besteht das Problem, dass die Sicherheitsapplikation die Daten nur bis zur Firewall schützt, aber nicht bis zum Applikation Server mit den zu schützenden Daten. Hier kann kaum eine auf Zertifikatsbasis funktionierende Authentifikation bis zum Applikation Server bewerkstelligt werden. Dies gilt sicherlich dann, wenn das mit IPSEC geschützte Protokoll keine Proxy Funktionalität aufweist und folglich die Firewall für die zu authentisierende Instanz die Authentisierung nicht vornehmen kann.

Im Bereich Web Services ist noch wenig bekannt, ob der XML Namespace ins Zertifikat eingefügt wird und von der Sicherheitsapplikation verifiziert und verglichen wird.

Falls die hier beschriebene Schwäche vorhanden sein sollte, ist das Risiko einer Attacke je nach Arbeitsumfeld und je nach Art der Sensitivität der Daten nicht zu vernachlässigen.

Felder im Zertifikat nicht vorhanden

Falls eine PKI für den internen Zweck eines Unternehmens oder einer staatlichen Institution eingerichtet und betrieben wird, können die entsprechenden Identitätskennungen in die dazu passenden Felder des Zertifikats eingefüllt werden. Schwierig wird es dann, wenn bereits Tausende von Zertifikaten ausgestellt worden sind und eine neue Applikation und deren Sicherheitstechnologie eingeführt wird, welche eine neue und noch nicht bestehende Kennung im Zertifikat zwingend verlangt.

Im Umfeld einer öffentlich anerkannten CA kann es z.B. vorkommen, dass die E-Mail Adresse im Zertifikat nicht enthalten ist. Dies kann dann das mit Public Key Verfahren geschützte eBusiness, Internetbanking oder eGovernment beeinträchtigen.

Risiko: Im Umfeld einer öffentlich anerkannten CA kann es durchaus häufig vorkommen, dass z.B. die E-Mail Adresse nicht ins Zertifikat aufgenommen wird, weil die Benutzer vielleicht flexibel in der Auswahl ihres Internet und E-Mail Provider sein wollen.

Felder im Zertifikat nicht korrekt ausgefüllt

Ob die Felder im Zertifikat korrekt ausgefüllt werden und wie gut die inkorrekten Felder bei der Ausstellung der Zertifikate erkannt werden, hängt von folgenden Faktoren ab:

- Genauigkeit, wie die ins Zertifikat aufgenommenen Identitätskennungen überprüft werden. Dies hängt meistens von der Klasse des Zertifikats ab.
- Welche CA Zertifikate im Browser oder in der E-Mail als vertrauenswürdig erachtet worden sind. Gerade beim Browser sind standardmässig eine Fülle von CA Zertifikaten als vertrauenswürdig deklariert, welche zur Verifikation der jeweiligen Zertifikate benötigt werden.

Risiko: Unkorrekte Felder im Zertifikat sind nichts Aussergewöhnliches; besonders dann, wenn sie gar nicht auf Richtigkeit überprüft werden. Dies kann im Bereich der öffentlich anerkannten und betriebenen CA der Fall sein. Es ist bekannt, dass eine CA in der Vereinigten Staaten irrtümlicherweise ein Zertifikat für einen grossen SW Betriebsystemhersteller ausgestellt hat.

Benutzer ignoriert die Warnmeldung

Dass Warnmeldungen von den Benutzern ignoriert, nicht verstanden werden und deshalb die Benutzer der Warnmeldung entgegengesetzt handeln, kommt leider häufig vor.

Das Ignorieren von Fehlermeldungen kann auch dadurch gefördert werden, dass die Sicherheitstechnologie wie erwartet eine Warnmeldungen herausgibt, aber es sich hierbei um einen Fehlalarm handelt. Die Häufung von Fehlalarmen kann die Benutzer dazu veranlassen, die Fehlermeldungen zu ignorieren und eine wirkliche Alarmmeldung als Fehlalarm zu deklarieren. Beispiel für einen Fehlalarm:

> Im Zertifikat einer öffentlich anerkannten CA ist die E-Mail Adresse des Benutzers nicht aufgenommen worden. Der Benutzer kommuniziert per E-Mail mit Behörden oder der Bank und unterschreibt die versandten E-Mail. Wenn die Sicherheitsapplikation korrekt funktioniert, wird eine Fehlermeldung beim Empfänger herausgegeben. Kommuniziert der Absender mit seiner wirklichen Absenderadresse, dann handelt es sich bei der Fehlermeldung um einen Fehlalarm.

Zusammenfassung

Folgende Risiken, welche die hier beschriebene Attacke unterstützen, sind aus Sicht des Autors am grössten:

- Fehlverhalten der Benutzer infolge mangelnder Ausbildung und folglich fehlerhaften Bewertung der Fehlermeldung und deren mögliche Konsequenzen.
- Fehlende oder falsche Identitätskennung im Zertifikat. Dadurch wird es der Sicherheitsapplikation verunmöglicht, die beiden Namen (Distinguished Name und den adressierten Applikationsnamen) korrekt zu vergleichen und im Fall eines Unterschieds die richtigen Fehlermeldungen herauszugeben oder die vorgegebenen Massnahmen einzuleiten.

Das Risiko, dass die hier beschriebene Attacke erfolgreich durchgeführt werden kann, steigt mit der Anzahl der Zertifizierungsstellen, welche als vertrauenswürdig in der Sicherheitstechnologie/-applikation deklariert worden sind. Per se sind eine Fülle von Zertifizierungsstellen (CA) beim Browser als vertrauensvoll eingestuft.

Die Attacke wird wohl am ehesten im eBusiness mit vertraulichen Daten und im eGovernment auftreten. Sei, dass sich jemand z.B. als Behördenmietglied ausgibt, sei, dass sich jemand unter falscher Identität z.B. bei der Behörde meldet und sensitive, nicht für ihn bestimmte Daten anfordert.

Massnahmen

In den folgenden Unterkapiteln werden mögliche Massnahmen aufgezeigt, wie das geschilderte Problem ansatzweise gelöst werden kann.

Sicherheitsapplikation mit Schwächen

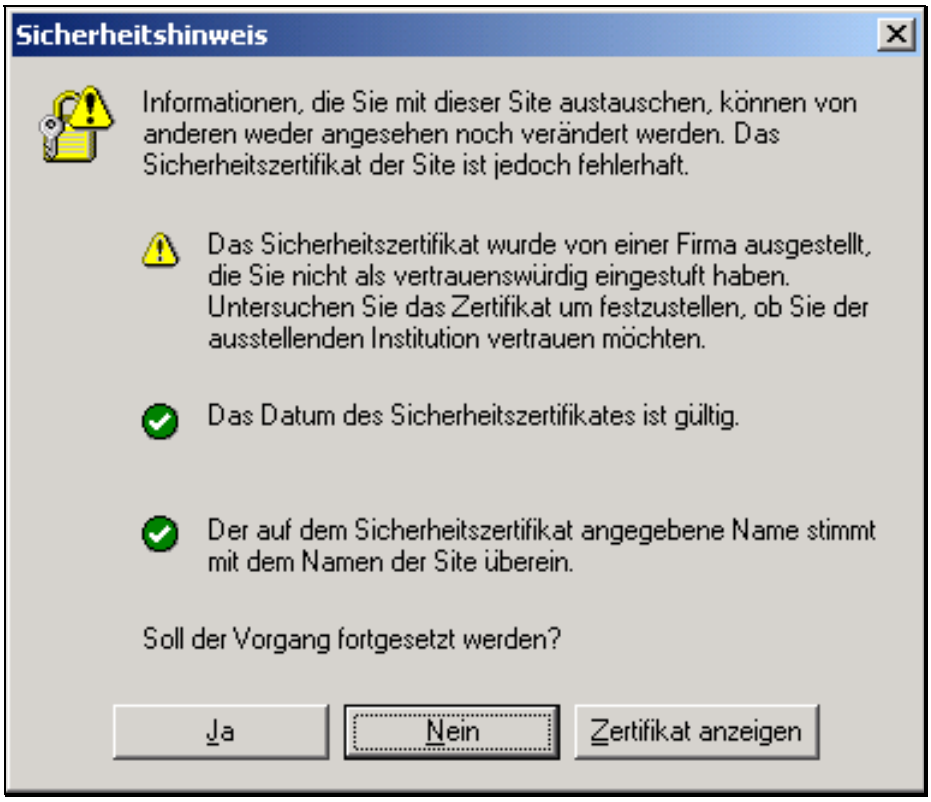
Hier gilt nur eines: Testen, bevor kaufen und implementieren und ausbreiten. Sicherheitsapplikationen/-technologien mit solchen Schwächen sollten nicht eingesetzt werden.

Felder im Zertifikat nicht oder nicht korrekt vorhanden

Die entsprechenden Identitätskennungen sind in das Zertifikat korrekt aufzunehmen. Dabei ist zu achten, dass die Identitätskennung pro Instanz oder Person eindeutig sind. Damit die verschiedenen Identitätskennungen eindeutig und konsistent vorliegen, empfiehlt sich ein **Identity Management und der Betrieb eines Meta Directory**. Im Directory sind die entsprechenden Identitätskennungen der verschiedenen zu schützenden Applikationen eindeutig aufzunehmen und dann zu verwalten. Ein Directory wird sinnvoll nur bei einer für interne Zwecke betriebenen CA aufgebaut und verwaltet.

Bei einer öffentlich anerkannten CA ist die Prüfung der Identitätskennung, wie E-Mail Adresse, schwierig, weil eine authentisierte und vertrauenswürdige Verbindung zu den Vergabestellen für DNS, URL Namen oder E-Mail Adressen (z.B. daniel.s.muster@bluewin.ch) bestehen muss.

Bemerkung: Wenn man alle als nicht sehr vertrauenswürdige CA Zertifikate im Browser herausnähme, würde zwar das Risiko der Attacke minimiert, aber der Komfort beim Surfen beeinträchtigt und es würden sich folgende Fehlermeldungen häufen.



Sicherheitshinweis im Browser, wenn das CA Zertifikat nicht als vertrauenswürdig erachtet wird.

Wird der zuvor dargestellte Sicherheitshinweis von den Benutzern im Laufe der Zeit kategorisch ignoriert und ihr zuwider sensitive Daten ausgetauscht, dann bestünde ebenfalls eine Sicherheitslücke.

Als Ausweg aus der soeben geschilderten Situation könnte man zwei Browser mit unterschiedlicher Konfiguration verwenden; einer für das Internetbanking oder eGovernment und einer für das Surfen. Der Browser für das Internetbanking oder eGovernment wird besonders sicher konfiguriert. Insbesondere würde man nur noch einem oder zwei CA Zertifikaten vertrauen, welche zur Verifikation des Server Zertifikats benötigt werden.

Benutzer ignoriert die Warnmeldung

In diesem Fall hilft nur Schulung, sofern sich die Fehlalarmmeldungen nicht häufen. Bei der Schulung der Benutzer muss auch darauf geachtet werden, dass sie das Zertifikat, welches zur Prüfung der Authentisierung verwendet wird, visuell überprüfen können. Dies setzt aber voraus, dass die Sicherheitsapplikation eine solche Schnittstelle zur visuellen Überprüfung von Zertifikaten zur Verfügung stellt. Unter Umständen müssen z.B. beim E-Mail Verkehr mit den Behörden in der unterschriebenen E-Mail eine Identitätskennung angefügt werden, welche im Zertifikat enthalten ist, damit eine visuelle Prüfung ermöglicht wird.

Anmerkung

Die hier beschriebene Attacke ist in Zusammenarbeit mit Armand Portmann an der FH Luzern am IT Labor des Instituts für Wirtschaftsinformatik (IWI) erkannt worden. Der Autor hat auf die Problematik der Lücke infolge unterschiedlicher Identitätskennungen bereits in seinem Buch [Mud] hingewiesen. Armand Portmann hat Beispiele aus der Praxis beigesteuert.

Literaturverzeichnis

[Mud]	Muster Daniel, Digitale Unterschriften und PKI, 2. Auflage, ISBN 3 9522387 2 4
RFC 2632	S/MIME Version 3 Certificate Handling