

# Attacke auf die Authentifizierung

Daniel Muster  
Bit Pattern Security  
8048 Zürich

© Copyright  
D. Muster

## Überblick

- Prinzip der Attacke
- Beispiele der Attacke anhand der E-Mail und dem Browser
- Risikobewertung der Attacke
- Massnahmen

© Copyright  
D. Muster

## Prinzip der Attacke

### Einleitung

Mit der Identifikation einer Person ist für die Ausstellung eines Zertifikats noch nicht genug bestimmt worden.

Die Authentifizierung auf Basis digitaler Unterschriften kann umgangen werden, ohne dass ein kryptographischer Algorithmus gebrochen wird.

© Copyright  
D. Muster

## Prinzip der Attacke

### Einleitung

Eine der folgenden Bedingungen erfüllt:

- 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.

© Copyright  
D. Muster

## Prinzip der Attacke

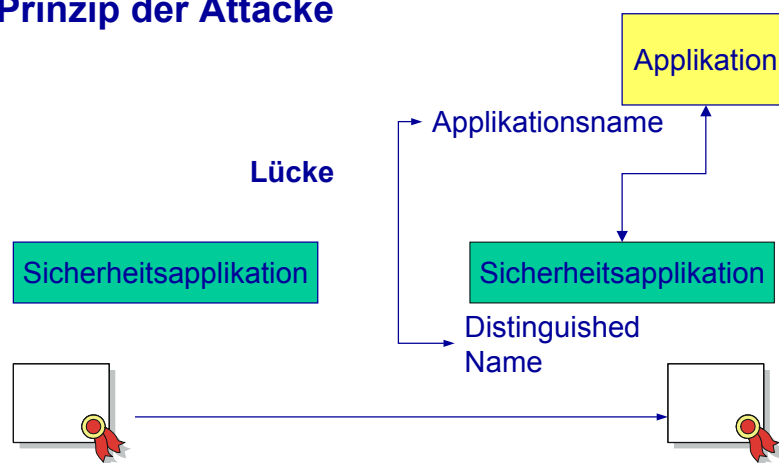
### Authentisierung der Person/Instanz

- Das Zertifikat der zu authentifizierenden Person/ Instanz überprüfen. U.a. wird verifiziert:
  - das Zertifikat noch gültig
  - nicht bereits revoziert
  - eine gültige Signatur
- Wird überprüft, ob die zu authentifizierende Person/ Instanz im Besitz des privaten Schlüssels ist.
- Dabei muss die Person/ Instanz eine Operation mit ihrem privaten Schlüssel durchführen (lassen).

© Copyright  
D. Muster

## Prinzip der Attacke

### Prinzip der Attacke



© Copyright  
D. Muster

# Prinzip der Attacke

Für E-Mail und SSL/TLS beim Browser

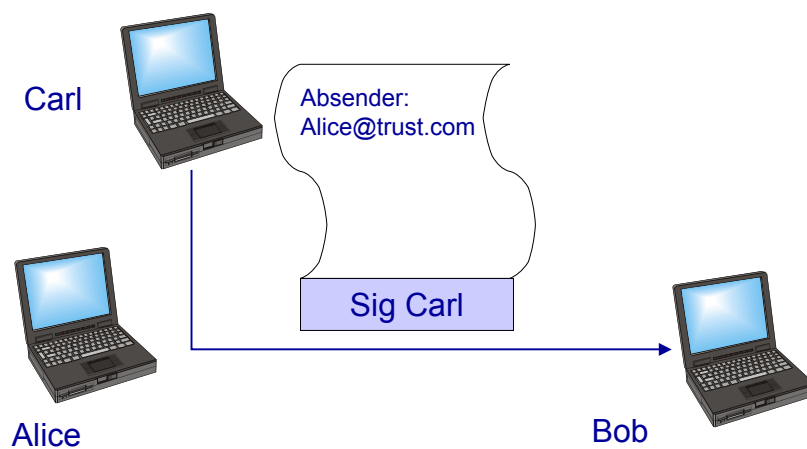
4 Fälle:

- Die Sicherheitsapplikation weist gewisse Schwächen auf.
- Bei der Zertifikatsausstellung sind gewisse Felder nicht ausgefüllt worden.
- Im Zertifikat sind gewisse Felder nicht richtig ausgefüllt.
- Der Benutzer ignoriert gewisse Warnungen.

© Copyright  
D. Muster

## E-Mail

**Sicherheitsapplikation gewisse Schwächen**



© Copyright  
D. Muster

## E-Mail

### Die Sicherheitsapplikation gewisse Schwächen

Bedingungen:

- Bob muss die CA als vertrauenswürdig erachten, welche das Zertifikat von Carl ausgestellt hat.
- Sicherheitsapplikation beim Empfänger vergleicht die E-Mail Adresse im Zertifikat **nicht** mit der E-Mail Adresse des Absenders.

© Copyright  
D. Muster

## E-Mail

### E-Mail Adresse im Zertifikat nicht vorhanden

Die Applikation kann nichts vergleichen ==> theoretisch keine Fehlermeldung

Bedingungen:

- Bob muss die CA als vertrauenswürdig erachten, welche das Zertifikat von Carl ausgestellt hat.

© Copyright  
D. Muster

## E-Mail

### E-Mail Adresse im Zertifikat nicht korrekt

Carl veranlasst die CA, ein Zertifikat mit der E-Mail Adresse von Alice auszustellen.

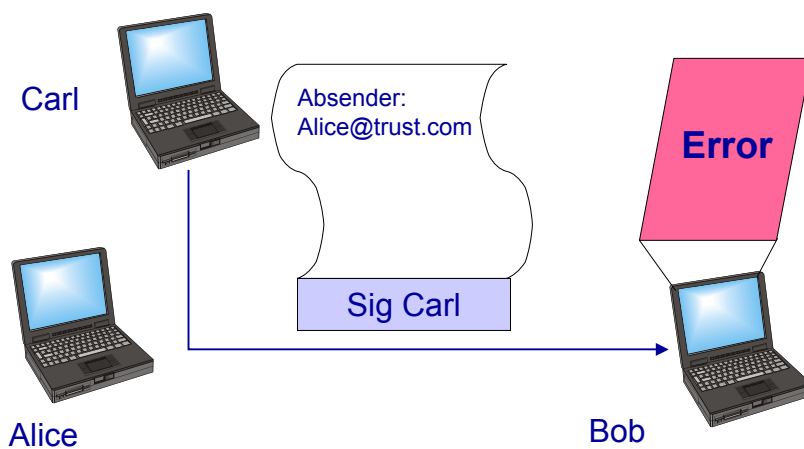
Bedingungen:

- Bob muss die CA als vertrauenswürdig erachten, welche das Zertifikat von Carl ausgestellt hat.
- Die CA kontrolliert nicht, ob die von Carl angegebene E-Mail Adresse zu Carl gehört.

© Copyright  
D. Muster

## E-Mail

### Benutzer ignoriert Warnmeldung



© Copyright  
D. Muster

# Browser

## 2 Fälle zu unterscheiden:

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

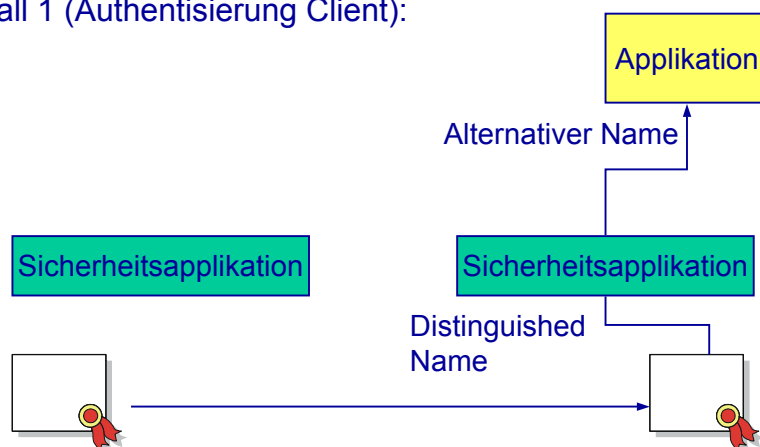
### Fall 1:

Wie der SSL/TLS Server die Identitätskennung der authentisierten Person/ Instanz an die zu schützende Applikation übergibt.

© Copyright  
D. Muster

# Browser

## Fall 1 (Authentisierung Client):



© Copyright  
D. Muster

## Browser

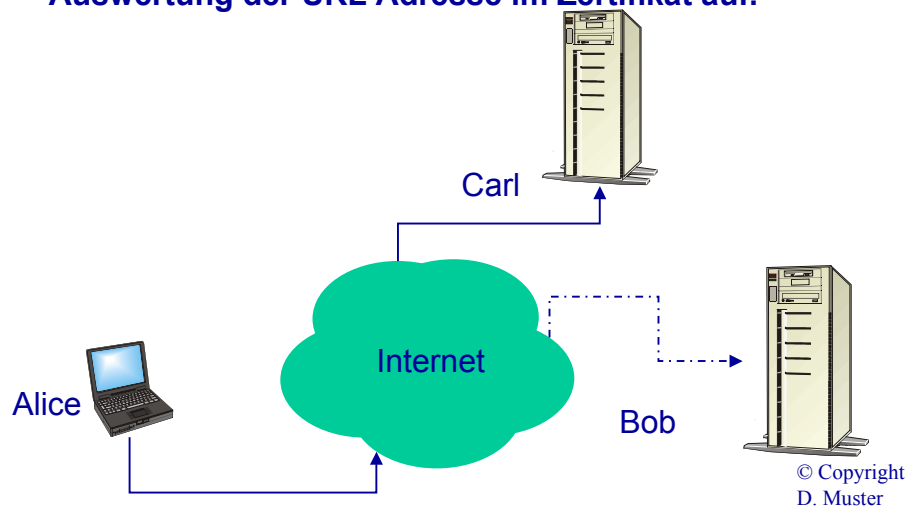
Fall 2 (Authentisierung Server):

- 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.

© Copyright  
D. Muster

## Browser

**Sicherheitsapplikation gewisse Schwächen in der Auswertung der URL Adresse im Zertifikat auf.**



© Copyright  
D. Muster

## Browser

### **Sicherheitsapplikation gewisse Schwächen in der Auswertung der URL Adresse im Zertifikat auf.**

Voraussetzungen:

- IP Adresse von Bob kann bei der URL Adresse von Bob im DNS Server 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.

© Copyright  
D. Muster

## Browser

### **Im Zertifikat URL Adresse nicht aufgeführt.**

Voraussetzungen:

- IP Adresse von Bob kann bei der URL Adresse von Bob im DNS Server 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.

© Copyright  
D. Muster

## Browser

### Bei der Zertifikatsausstellung ist die URL Adresse falsch ausgefüllt worden.

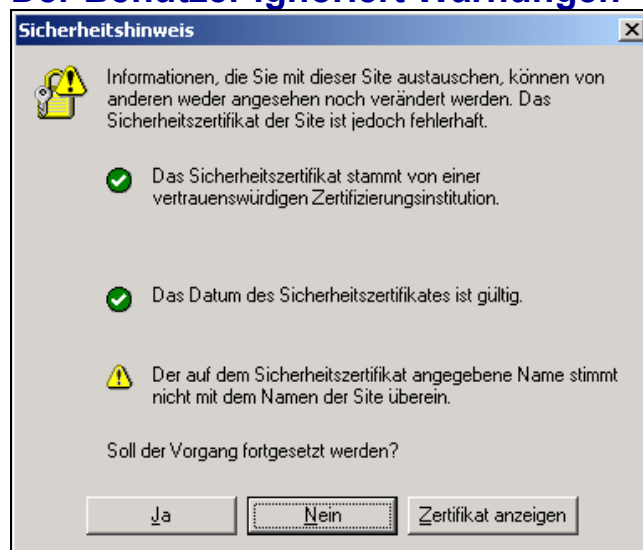
Voraussetzungen:

- Die CA kontrolliert nicht sorgfältig genug, ob die von Carl bei der Zertifikatsausstellung angegebene URL Adresse zu Carl gehört.
- IP Adresse von Bob kann bei der URL Adresse von Bob im DNS Server 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.

© Copyright  
D. Muster

## Browser

### Der Benutzer ignoriert Warnungen



© Copyright  
D. Muster

# Browser

## **Der Benutzer ignoriert Warnungen.**

Voraussetzungen:

- IP Adresse von Bob kann bei der URL Adresse von Bob im DNS Server 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.

© Copyright  
D. Muster

# Risiken

## **Sicherheitsapplikation gewisse Schwächen**

Die Häufigkeit, dass eine Sicherheitsapplikation eine solche Schwäche aufweist, ist eher selten im Browser und E-Mail Umfeld. Falls die Schwäche vorhanden sein sollte, ist das Risiko einer Attacke je nach Arbeitsumfeld nicht zu vernachlässigen.

© Copyright  
D. Muster

## Risiken

### **Adresse im Zertifikat nicht vorhanden**

Im Umfeld einer öffentlichen CA kann es vorkommen, dass die E-Mail Adresse oder die URL nicht ins Zertifikat aufgenommen wird, weil

- die Benutzer will flexibel in der Auswahl ihres Internet und E-Mail Provider sein.
- die Vergabe der URL soll flexibel gestaltet werden.
- Die URL ist bereits wieder vergeben worden.

© Copyright  
D. Muster

## Risiken

### **Adresse im Zertifikat nicht korrekt**

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.

Beispiel: Verisign und Microsoft

© Copyright  
D. Muster

# Risiken

## **Benutzer ignoriert Fehlermeldung**

Gründe:

- Benutzer versteht Fehlermeldung nicht
- Benutzer ignoriert Fehlermeldung infolge vieler Fehlalarme

© Copyright  
D. Muster

# Risiken

## **Zusammenfassung**

Folgende Risiken sind aus Sicht des Autors am grössten:

- Fehlverhalten der Benutzer
- Fehlende oder falsche Identitätskennung im Zertifikat
- Sicherheitsapplikation weist Fehler auf.

© Copyright  
D. Muster

## Massnahmen

Sicherheitsapplikation gewisse Schwächen

- Testen

**Fehlverhalten der Benutzer**

- Schulung

© Copyright  
D. Muster

## Massnahmen

**Fehlende oder nicht korrekte  
Identitätskennungen**

- Identitätskennungen sind ins Zertifikat aufzunehmen
- Identitätskennungen sind auf Eindeutigkeit zu prüfen
- Minimieren der als vertrauenswürdig erachteten CA

© Copyright  
D. Muster