Informationssicherheit

3. Schwachstellen

Prof. Dr. Christoph Skornia
christoph.skornia@oth-regensburg.de

Schwachstellen

Generell unterscheiden wir 3 Typen von Schwachstellen:

1. Konzeptionelle Schwachstellen z.B.
   - keine oder keine ausreichende Klassifizierung von Information
   - fehlende Rollenkonzepte
   - fehlende Sicherheitsregularien für Datenflüsse
     - USB-Sticks
     - Mobiltelefone
     - etc.
   - Keine ausreichenden Konzepte zur Identifikation von Subjekten
   - Keine ausreichende Schulung der Mitarbeiter $\rightarrow$ Social Engineering

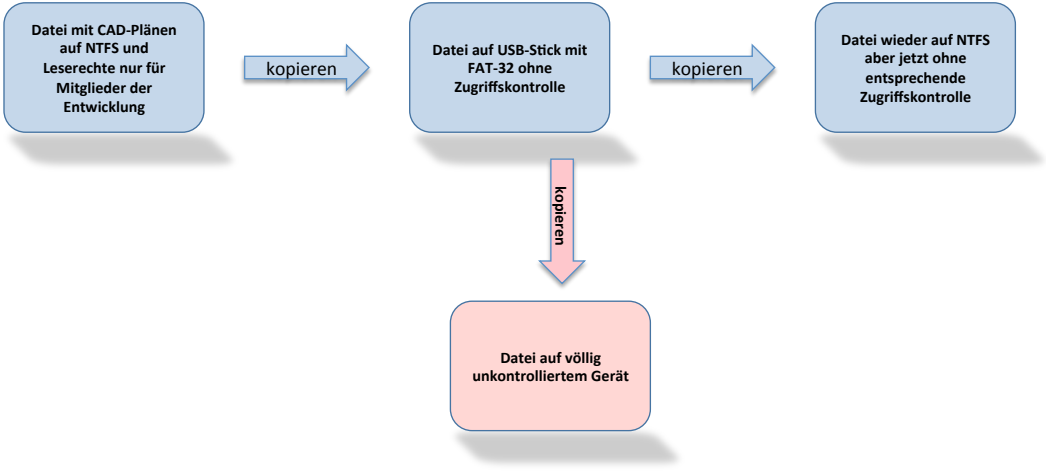
Schwachstellen

2. Schwachstellen in der Konfiguration z.B.
   - Konfigurationsfehler z.B. Änderung der Boot-Reihenfolge ohne Passwort
   - Firewall erlaubt gefährliche Kommunikation
   - unsichere Verschlüsselungsverfahren sind erlaubt
   - Patchmanagement

3. Schwachstellen in der Programmierung eingesetzter Software
   - Fehlende Validierung von Benutzereingaben
   - unverschlüsselte temporäre Daten zur Laufzeit
   - Beliebige Fehler, welche ein Programm unkontrolliert „abstürzen" lassen

Konzeptionelle Schwachstellen

Beispiel: Fehlende Datenflusskontrolle (z.B. USB-Stick)



Konzeptionelle Schwachstellen

Beispiel: Social Engineering

- Mein Name ist Fritz Müller von HP-Leasing und ich müsste dringend die Firmware Ihrer Drucker updaten. Der Fehler kann dazu führen, dass ein Gerät abbrennt.

- Mein Name ist Marta Gruber und ich habe eine neuen Umstecker für die Tastatur, damit diese nach dem nächsten Update noch funktioniert.

- Mein Name ist Paul Maier, Sie müssten Ihre Benutzerinformationen in unserem Bestellsystem aktualisieren, gehen Sie bitte dazu auf folgende Seite.

Konzeptionelle Schwachstellen

Beispiel: Social Engineering

- Mein Name ist Fritz Müller von HP-Leasing und ich müsste dringend die Firmware Ihrer Drucker updaten. Der Fehler kann dazu führen, dass ein Gerät abbrennt.

  Es wird eine Firmware aufgespielt, welche sämtliche gedruckten Daten speichert oder (entsprechend intelligent) ins Internet verschickt.

- Mein Name ist Marta Gruber und ich habe eine neuen Umstecker für die Tastatur, damit diese nach dem nächsten Update noch funktioniert.

- Mein Name ist Paul Maier, Sie müssten Ihre Benutzerinformationen in unserem Bestellsystem aktualisieren, gehen Sie bitte dazu auf folgende Seite.

Konzeptionelle Schwachstellen

Beispiel: Social Engineering

- Mein Name ist Fritz Müller von HP-Leasing und ich müsste dringend die Firmware Ihrer Drucker updaten. Der Fehler kann dazu führen, dass ein Gerät abbrennt.

  Es wird eine Firmware aufgespielt, welche sämtliche gedruckten Daten speichert oder (entsprechend intelligent) ins Internet verschickt.

- Mein Name ist Marta Gruber und ich habe eine neuen Umstecker für die Tastatur, damit diese nach dem nächsten Update noch funktioniert.

- Mein Name ist Paul Maier, Sie müssten Ihre Benutzerinformationen in unserem Bestellsystem aktualisieren, gehen Sie bitte dazu auf folgende Seite.

Konzeptionelle Schwachstellen

Beispiel: Social Engineering

- Mein Name ist Fritz Müller von HP-Leasing und ich müsste dringend die Firmware Ihrer Drucker updaten. Der Fehler kann dazu führen, dass ein Gerät abbrennt.

  Es wird eine Firmware aufgespielt, welche sämtliche gedruckten Daten speichert oder (entsprechend intelligent) ins Internet verschickt.

- Mein Name ist Marta Gruber und ich habe eine neuen Umstecker für die Tastatur, damit diese nach dem nächsten Update noch funktioniert.

  Der „Umstecker" ist natürlich ein Keylogger

- Mein Name ist Paul Maier, Sie müssten Ihre Benutzerinformationen in unserem Bestellsystem aktualisieren, gehen Sie bitte dazu auf folgende Seite.

Konzeptionelle Schwachstellen

Beispiel: Social Engineering

- Mein Name ist Fritz Müller von HP-Leasing und ich müsste dringend die Firmware Ihrer Drucker updaten. Der Fehler kann dazu führen, dass ein Gerät abbrennt.

  Es wird eine Firmware aufgespielt, welche sämtliche gedruckten Daten speichert oder (entsprechend intelligent) ins Internet verschickt.

- Mein Name ist Marta Gruber und ich habe eine neuen Umstecker für die Tastatur, damit diese nach dem nächsten Update noch funktioniert.

  Der „Umstecker" ist natürlich ein Keylogger

- Mein Name ist Paul Maier, Sie müssten Ihre Benutzerinformationen in unserem Bestellsystem aktualisieren, gehen Sie bitte dazu auf folgende Seite.

Konzeptionelle Schwachstellen

Beispiel: Social Engineering

- Mein Name ist Fritz Müller von HP-Leasing und ich müsste dringend die Firmware Ihrer Drucker updaten. Der Fehler kann dazu führen, dass ein Gerät abbrennt.

  Es wird eine Firmware aufgespielt, welche sämtliche gedruckten Daten speichert oder (entsprechend intelligent) ins Internet verschickt.

- Mein Name ist Marta Gruber und ich habe eine neuen Umstecker für die Tastatur, damit diese nach dem nächsten Update noch funktioniert.

  Der „Umstecker" ist natürlich ein Keylogger

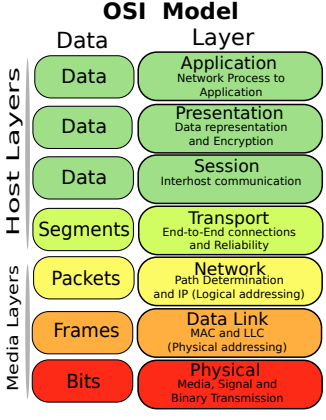
- Mein Name ist Paul Maier, Sie müssten Ihre Benutzerinformationen in unserem Bestellsystem aktualisieren, gehen Sie bitte dazu auf folgende Seite.

  Die Seite ist ein Fake und dient nur dazu um Passworte abzufragen.

Konzeptionelle Schwachstellen

Beispiel: Netzwerk

- Keine ausreichende Identifikation von Subjekten:
  - d.h. es ist möglich sich als jemand anderes auszugeben
  - engl. spoofing = Verschleierung (der Identität)



- Auf allen Schichten des OSI-Modells:
  - Schicht 2: z.B. ARP-Spoofing
  - Schicht 3: z.B. IP-Adress-Spoofing
  - Schicht 4,5: z.B. Session Hijacking
  - Schicht 7:
    - z.B. DNS-Spoofing
    - z.B. falscher E-Mail-Absender
    - z.B. Web-Spoofing

Fehlende Identifikation

ARP-Spoofing:

Im Security-Labor möchte der Win-7-Host Daten vom Ubuntu-Host abrufen

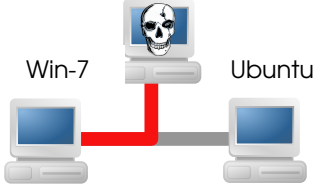
1. er weiß die IP-Adresse aber nicht die MAC-Adresse
2. ARP-Broadcast: Welche MAC gehört zur IP 10.y.2.3
3. Ubuntu-Host antwortet mit seiner MAC und XP-Rechner speichert diese im ARP-Cache
4. Alle können kommunizieren und sind glücklich!

Fehlende Identifikation

ARP-Spoofing:

Im Security-Labor möchte der Win-7-Host Daten vom Ubuntu-Host abrufen

1. er weiß die IP-Adresse aber nicht die MAC-Adresse
2. ARP-Broadcast: Welche MAC gehört zur IP 10.y.2.3
3. ein anderer (bösartiger) Rechner im gleichen Segment antwortet mit seiner MAC
4. der XP-Host speichert diese (falsche) MAC im ARP-Cache (das passiert, wenn der bösartige Rechner einfach schneller antwortet oder auch der Ubuntu-Rechner vom Netz genommen wurde)
5. der XP-Rechner kommuniziert jetzt ohne es zu merken mit dem bösartigen Rechner und nur dieser ist glücklich!

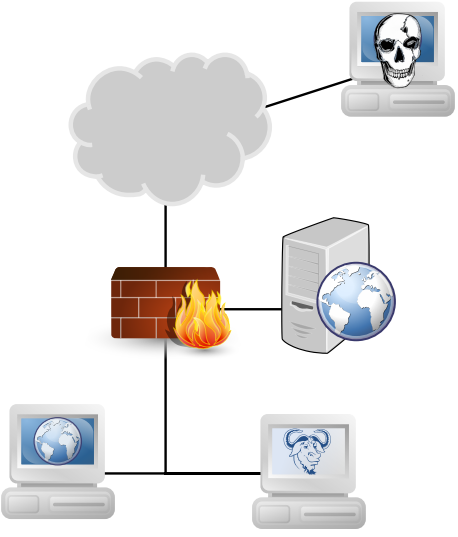


Fehlende Identifikation

IP-Spoofing:

Ein Schadrechner möchte aus dem Internet Pakete schädliche Pakete an einen internen Rechner schicken.

1. Die Firewall lässt aber nur Pakete durch deren Absenderadresse aus dem internen Adressbereich kommt
2. Die Kommunikation kommt daher nicht zustande und der Win-XP-Rechner ist sicher
3. Alle sind glücklich!



RFC 791 (Internet Protocol)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Identification           |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fehlende Identifikation

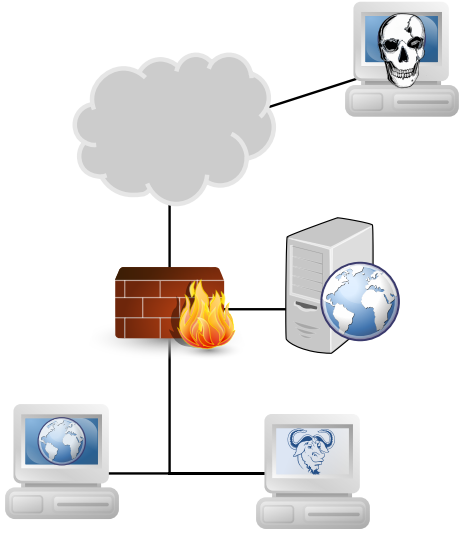
IP-Spoofing:

Ein Schadrechner möchte aus dem Internet Pakete schädliche Pakete an einen internen Rechner schicken.

1. Die Firewall lässt aber nur Pakete durch deren Absenderadresse aus dem internen Adressbereich kommt
2. Der Host aus dem Internet schreibt eine Absenderadresse aus dem internen Adressbereich in den Header des IP-Pakets
3. Die Firewall lässt das Paket durch
4. Der Angreifer ist glücklich!

RFC 791 (Internet Protocol)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Identification           |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

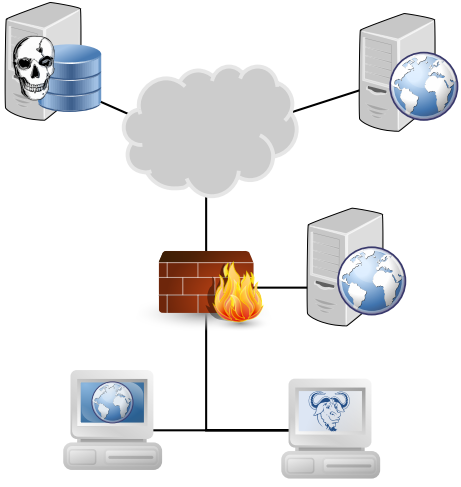


Fehlende Identifikation

DNS-Spoofing:

Im Security-Labor möchte der User am Windows-7-Host gerne auf die Homepage seiner Hausbank zugreifen und gibt in den Browser http://www.meibank.by ein

1. Der DNS-Server löst die IP auf und liefert die dazugehörige IP-Adresse zurück
2. Die Kommunikation kommt zustande
3. Alle sind glücklich!

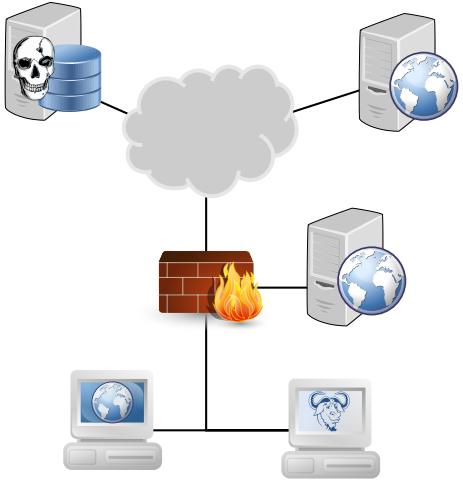


Fehlende Identifikation

DNS-Spoofing:

Im Security-Labor möchte der User am Windows-7-Host gerne auf die Homepage seiner Hausbank zugreifen und gibt in den Browser http://www.meibank.by ein

1. Der DNS-Server ist unter Kontrolle eines Angreifers und liefert die IP-Adresse eines bösartigen Webservers zurück
2. Der User loggt sich mit seinen Bankzugangsdaten in das Webinterface auf dem Webserver des Angreifers ein
3. Der Angreifer ist glücklich!



Fehlende Identifikation

Web-Spoofing:

Im Security-Labor sucht der User nach einer Möglichkeit unter XP Gruppenrechte zu vergeben

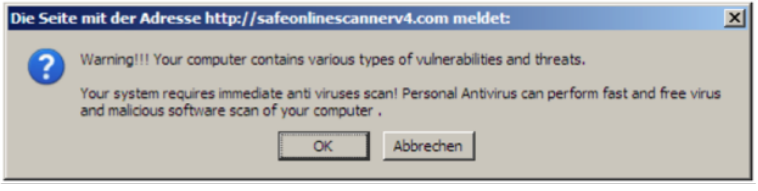
1. Der User wird bei Google fündig
2. Er holt sich die dazugehörige Information
3. Alle sind glücklich!

Fehlende Identifikation

Web-Spoofing:

Im Security-Labor sucht der User nach einer Möglichkeit unter XP Gruppenrechte zu vergeben

1. Der User wird bei Google fündig
2. Die gefundene Seite zeigt an:

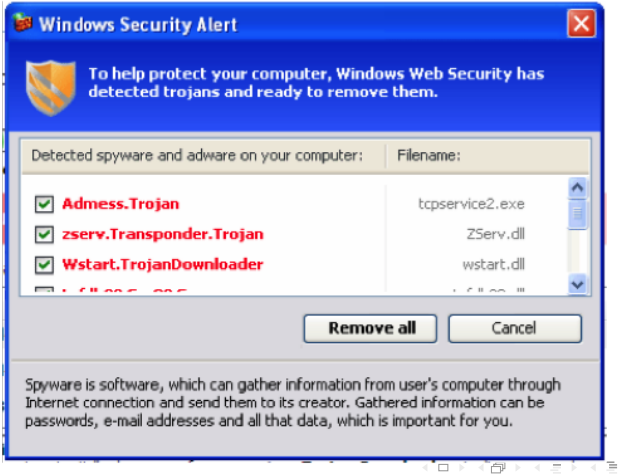


Fehlende Identifikation

Web-Spoofing:

Im Security-Labor sucht der User nach einer Möglichkeit unter XP Gruppenrechte zu vergeben

1. Der User wird bei Google fündig
2. Die gefundene Seite zeigt an:
3. Der User liest flüchtig und klickt OK
4. Es erscheint:

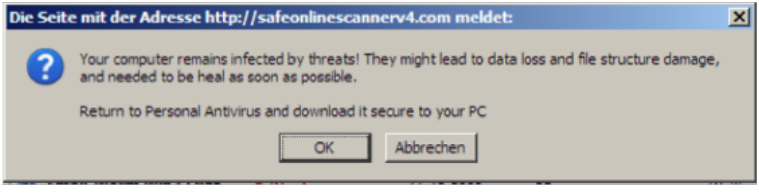


Fehlende Identifikation

Web-Spoofing:

Im Security-Labor sucht der User nach einer Möglichkeit unter XP Gruppenrechte zu vergeben

1. Der User wird bei Google fündig
2. Die gefundene Seite zeigt an:
3. Der User liest flüchtig und klickt OK
4. Es erscheint:
5. Der User liest flüchtig und klickt OK
6. Es erscheint:



Fehlende Identifikation

Web-Spoofing:

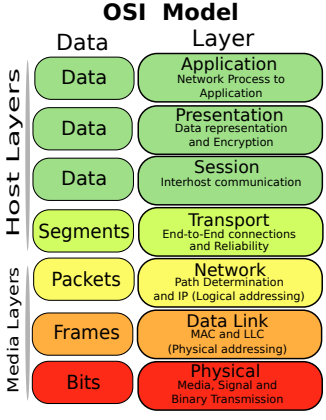
Im Security-Labor sucht der User nach einer Möglichkeit unter XP Gruppenrechte zu vergeben

1. Der User wird bei Google fündig
2. Die gefundene Seite zeigt an:
3. Der User liest flüchtig und klickt OK
4. Es erscheint:
5. Der User liest flüchtig und klickt OK
6. Es erscheint:
7. Der User liest flüchtig und klickt OK
8. Er lädt sich die Security-Software runter und installiert diese
9. Der Angreifer ist glücklich

Fehlende Identifikation

Konsequenzen:

- Bei der Konzeption der IP-Protokolle wurde kein Schwerpunkt auf Identifikation gelegt
- Identitäten sind in der Regel leicht fälschbar
- Benötigt werden daher:
  - starke Authentifizierungs- und Autorisierungsverfahren
  - Identitätsmanagement
  - Sichere Verwaltung von Credentials



Danke für Ihr Interesse

Fortsetzung folgt