Techniekseminar

Umgang mit Passwörter

Kushtrim Lulaj

14-05-20012

Gliederung

1. Psychologische Aspekte
   a) Umgang mit Informationen
2. Passwörter
   a) Einsatz von Passwörtern
   b) Ungeeigneter Umgang mit Passwörtern
3. Passwort-Cracking
   3.1 Brute-Force Methode
   3.2 Wörterbuchangriff
   3.3 BarsWF MD5 Passwort Knacker

Gliederung

4. Social-Engineering
   - 4.1 Computer Basen Social Engineering
     a) Phishing
     b) Pharming
     c) Trojaner als Keylogger
5. Quellen

1.Psychologische Aspekte

1. Umgang mit Informationen

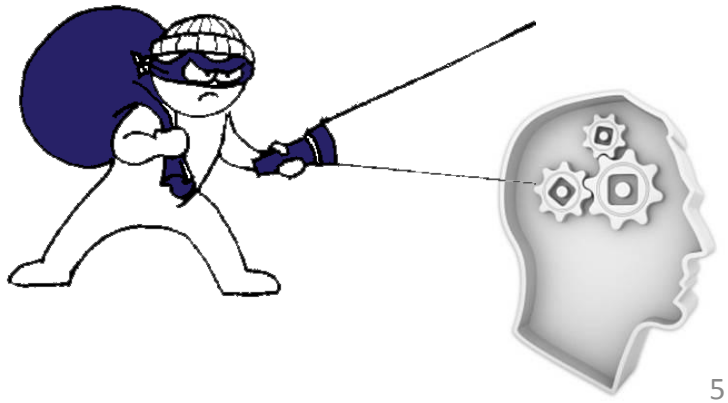
- menschliches Bestreben Informationen zu teilen!
- „freiwilliges“ Hochladen von Informationen
  - **Facebook, Twitter**
- Umgekehrt: Bestreben vertrauliche Informationen zu schützen
  - **Staat/ Regierung**
  - **Geheimdienste**
  - **Militär**
  - **Unternehmen**
  - **Private Personen**

1.Psychologische Aspekte

- menschliches Bestreben Informationen zu beschaffen

Legaler Weg

Illegaler Weg



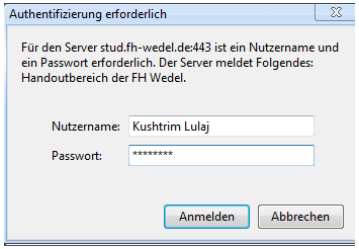
1.Psychologische Aspekte

- Maßnahmen für den Schutz von Informationen
  - **Verschlüsselung** von Nachrichten
  - Symmetrisches Kryptosystem
    - Beide Teilnehmer haben den gleichen Schlüssel
    - AES (**Advanced Encryption Standard**)
  - Asymmetrisches Kryptosystem
    - Benutzer erzeugt ein **Schlüsselpaar**
      - **Privater Schlüssel und öffentlicher Schlüssel**

1.Psychologische Aspekte

- **Einsatz von:**
  - **Security-Token**

- Passwörter



  - **biometrische Merkmale**

1.Psychologische Aspekte

1. **Umgang mit Informationen**
2. Passwörter
3. Brute-Force Methode
4. Social Engineering
5. Quellen

Frage: Können Passwörter vor Missbrauch wirklich schützen

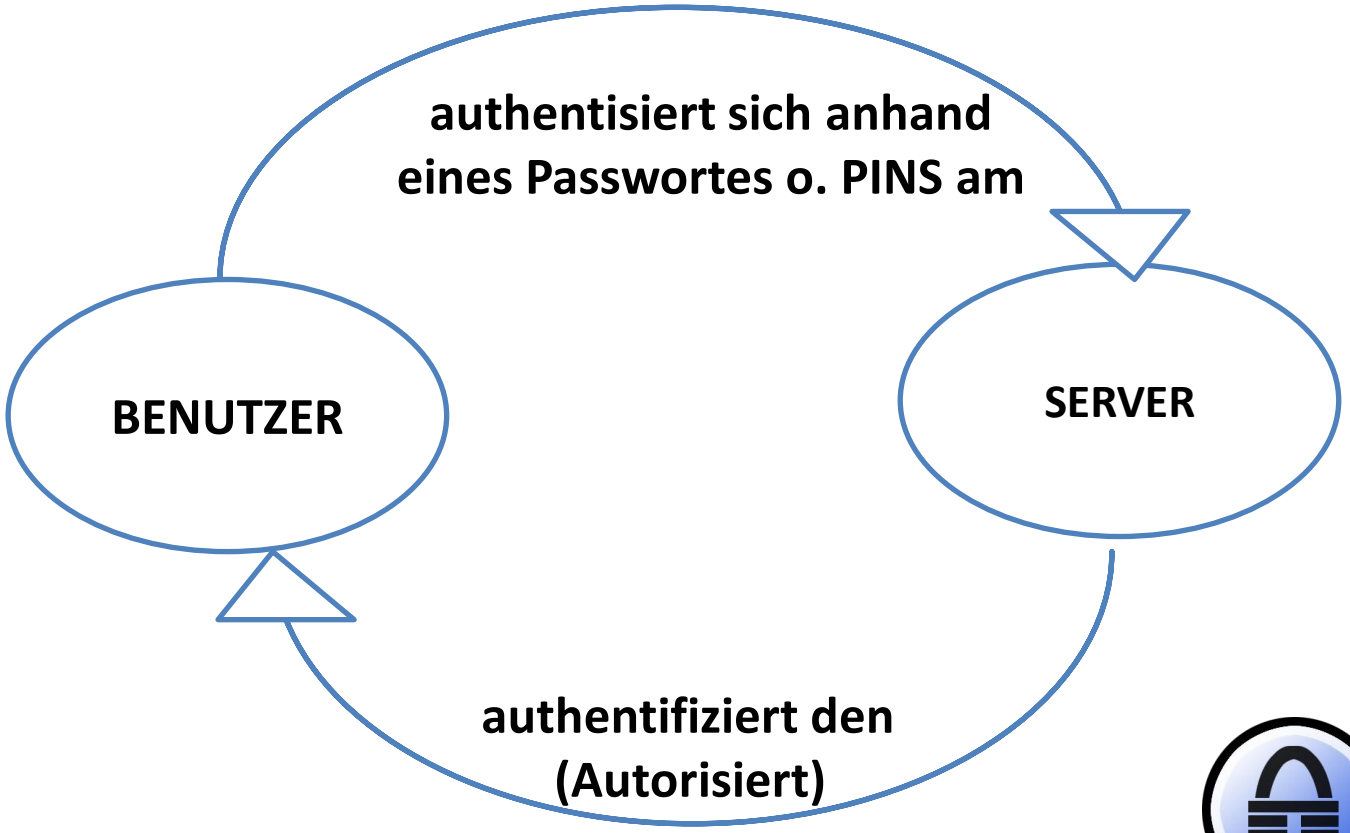
2. Umgang mit Passwörtern

2. Passwörter

- Passphrase, Kennwort, Schlüsselwort, Codewort (auch Kodewort), Lösung, PIN-Code, Lösungswort oder Parole.
- dient zur **Authentifizierung** und der eindeutigen **Identifizierung**
- **Kognitive Identifikation**
  - Authentifizierung anhand von Wissen
- am meisten genutztes Verfahren

2. Umgang mit Passwörtern

- **Authentifizierung ???**



2. Umgang mit Passwörtern

a) Anwendungen von Passwörtern

- Passwörter werden in unterschiedlichen Bereichen angewendet
- Ob es Nutzer in der privaten oder beruflichen Welt sind
  - Regierungen, Geheimdienst ect.
  - Organisationen
  - Im einen Unternehmen
  - Im privaten Bereich

2. Umgang mit Passwörtern

a) Anwendung von Passwörtern

– Anwendung von Passwörtern am PC

- **BIOS**-Passwort
- **Administrator**-Passwort
- **Benutzer**-Passwort
- **Benutzerkonto(Accounts) –**Passwort
- **Ordner-**Passwort

2. Umgang mit Passwörtern

b) Ungeeigneter Umgang mit Passworten 1

- Durchdachte Authentifikationsverfahren helfen **NICHT** vor naiven Umgang mit Zugangsmitteln.

- Passwörter, PIN, Token werden immer wieder weiter gegeben oder unsicher aufbewahrt.

2. Umgang mit Passwörtern

b) Ungeeigneter Umgang mit Passwörtern 2

- Häufig werden Passwörter innerhalb von Gruppen geteilt.
- Zwang zur Passwortbenutzung wird oft als lästig empfunden.
- dadurch werden Passwörter selten bis nie gewechselt.
- durch die Vielzahl an Passwörtern werden diese auch immer vergessen

2. Umgang mit Passwörtern

b) Ungeeigneter Umgang mit Passwörtern 3

- unnötiger Aufwand, um im System weiter zu arbeiten.
- Benutzerdaten können verloren gehen
- Passwörter werden oft notiert.
  - Passwortaufbewahrung am Arbeitsplatz.
- Qualität der Passwörter wird unterschätzt.

2. Umgang mit Passwörtern

b) Beispiele 1:

- In einem Unternehmen wurde festgestellt, dass Passwörter zu schlecht gewählt worden sind bzw. selten gewechselt worden.
- Es wurde technisch erzwungen, Passwörter monatlich zu wechseln.
- Zahlen und Sonderzeichen mussten zudem benutzt werden.

2. Umgang mit Passwörtern

b) Beispiele 1:

- Der Mitarbeiter empfindet es als lästig, sich immer neue Passwörter zu merken.

- Hat eine Idee, um sich Passwörter leicht zu merken!

2. Umgang mit Passwörtern

b) Beispiele 1:

- Er wählte die Passwörter wie folgt aus: Januar2009, Februar2009, Maerz2009,…
- Diese Passwörter entsprechen zwar den Vorgaben, waren aber leicht erratbar.

2. Umgang mit Passwörtern

b) Beispiele 2:

- Passwörter in einer Behörde
- Viele Benutzer hatten das gleiche Passwort
- Alle diese Nutzer hatten ihr Büro zur Straßenseite
- Passwort: Name des gegenüberliegenden Hotels

2. Umgang mit Passwörtern

b) Merkmale für falsch gewählte Passwörter

- Geburtsdatum
- Name
- Sprüche
- Wörter die in jedem Lexikon auftauchen
- Top 10 der einfachen Passwörter

2. Umgang mit Passwörtern

- 50 % der Passwörter bei Rockyou.com waren mit diesen Top 10 belegt.
- Die Hacker ziehen Schlüsse von solchen einfachen Passwörtern.
- Passen ihre Programme an.
- und Passwortknacker wie die Brute Force Methode oder Wörterbuch Angriff werden effektiver.

2. Umgang mit Passwörtern

a) Was ist Brute-Force?

- Auch unter dem Namen *erschöpfende Suche* bekannt
- Es wird jede mögliche Passwort-kombination simpel ausprobiert.
- Rein theoretisch muss das irgendwann funktionieren
- Praktisch, ist es jedoch nicht immer möglich.

2. Umgang mit Passwörtern

a) Was ist Brute-Force?

- es gibt verschiedene Brute-Force Programme und Tools, die man runter laden kann 
- diese führen die Passwortabfragen einfach durch.
- Simples Vorgehen, was jeder Mensch rein theoretisch probiert hat.

2. Umgang mit Passwörtern

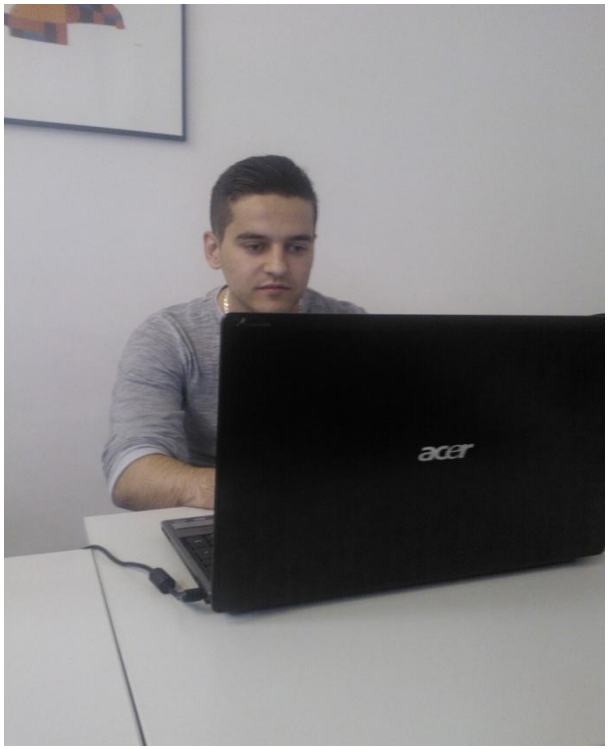
a) Was ist Brute-Force?

- Klartext und Geheimtext ist (x,y)
- $K = \{k_1, \ldots k_k\}$ der Schlüsselraum aller möglichen Schlüssel k_i .
- Brute-Force- Attacke prüft für jeden $k_i \in K$ ob $d_{ki}(y)=x$ zutrifft.
- trifft die Gleichung zu = Passwort korrekt
- Wenn nein nächste Möglichkeit

2. Umgang mit Passwörtern

a) Szenario einer illegalen Brute-Force A.

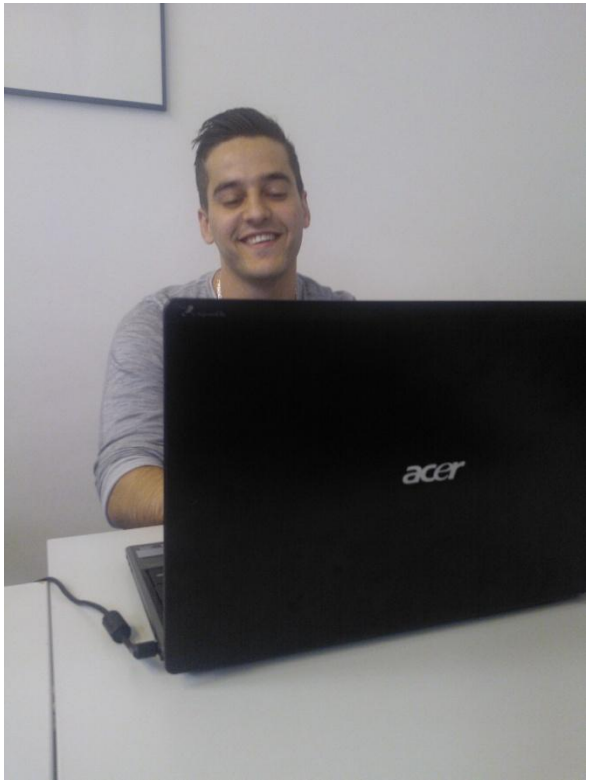
Täter



Opfer

2. Umgang mit Passwörtern

a) Wie läuft ein Brute-Force Attacke ab?



Täter sieht

GEHEIM.zip

2. Umgang mit Passwörtern

a) Wie läuft ein Brute-Force Attacke ab?

– Täter geht zuerst wie folgt vor!

```
C:\Users\Kushtrim\Documents>7z.exe x -p12345 geheim.zip
```

– Erster Versuch: Falsches Passwort

– **Fehlermeldung:**

```
Extracting  geheim.txt     CRC Failed in encrypted file. Wrong password?

Sub items Errors: 1
```

2. Umgang mit Passwörtern

a) Täter erinnert sich an EidP

2. Umgang mit Passwörtern

a) Quellcode eines Brute-Force Programm

Project1 - Form1 (Code)

Command1 | Click

```
Private Sub Command1_Click()
Dim start As Long
Dim ende As Long
Dim passwort As Long

start = CLng(Text1.Text)
ende = CLng(Text2.Text)
passwort = CLng(Text4.Text)
Label6.Caption = Format(Now, "hh:mm:ss")

For i = start To ende
Text3.Text = CStr(i)
Text3.Refresh
Me.Refresh
DoEvents

'Eigentliche Versuchszeile für 7Zip
If i = passwort Then
Label4.Caption = "Passwort wurde gefunden!"
Label7.Caption = Format(Now, "hh:mm:ss")
Exit Sub
```

2. Umgang mit Passwörtern

a) Konsole eines Brute-Force Programms

2. Umgang mit Passwörtern

a) John the Ripper

- **beliebtes Programm zum Dekodieren und Testen von Passwörtern.**
- **Verfahren verschlüsselt einen beliebigen Text und vergleicht ihn anschließend mit dem verschlüsselten Passwort.**
  - Verschlüsselung eine Textstrings „Kandidaten“
  - Vergleich mit den verschlüsselten Passwort
  - Sind beide gleich, so findet eine *Hash-Kollision* statt= Passwort gefunden

2. Umgang mit Passwörtern

i. Was ist eine Hash-Funktion (1) ?

- Eine Abbildung, die zu jeder Eingabe aus einer größeren Quellenmenge, eine Ausgabe aus einer kleineren Zielmenge erzeugt.
  - Den sog. Hash-Wert oder Hash-Code
- Daten „zerhacken“ und verstreuen.
- Werden in Form eines Algorithmus spezifiziert.

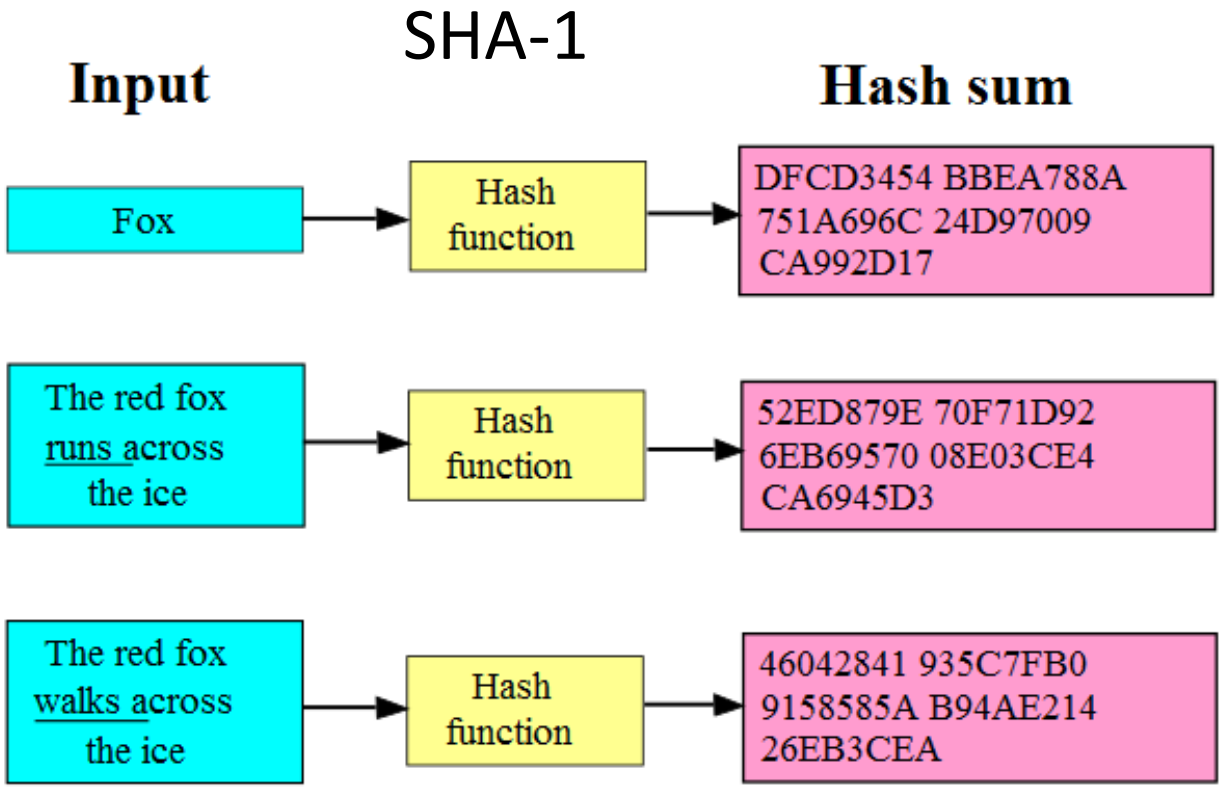
2. Umgang mit Passwörtern

i. Was ist eine Hash-Funktion (2) ?

- Erzeugt für ein Dokument einen charakteristischen *Fingerabdruck*
- Kann mit Hilfe von **Blockchiffren** oder **eigenständig** konstruiert werden
- Auf Basis einer Hashfunktion wird auch ein **„Message Authentication Code“ (HMAC)** gebildet

2. Umgang mit Passwörtern

i. Was ist eine Hash-Funktion (3)?



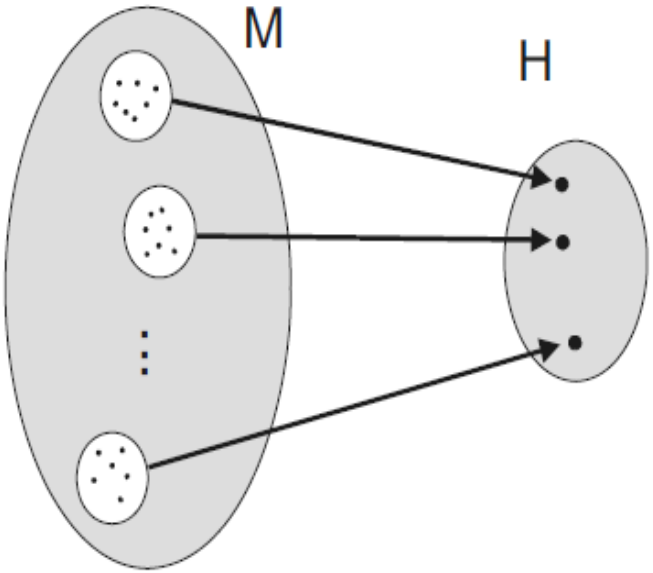
2. Umgang mit Passwörtern

ii. Hashkollision ?

- Eine Kollision trifft auf, wenn derselbe Hashwert auf zwei verschiedene Datenstrukturen geordnet wird.
- Mathematisch muss das zutreffen
- h(m) = h(m‘)

2. Umgang mit Passwörtern

ii. Hashkollision ?



m=1 Kbyte $|M| = 2^{8000}$
h = 160 Bit $|H| = 2^{160}$

Menge der Nachrichten mit gleichem Hashwert:

$|M| / |H| = 2^{7840}$

Abbildung einer Menge **M** Nachrichten

auf eine Menge **H** von Hashwerten z.B 160 Bit

2. Umgang mit Passwörtern

iii. Grenzen einer Brute-Force Attacke

1. Passwortlänge

a) Umso länger ein Passwort ist, desto länger dauert es das Passwort zu knacken!

b) Rechenoperationen steigen proportional zur Anzahl der zu probierenden, möglichen Lösungen.

2. Mathematische Formel

Passwortlänge

Kombinationen = Zeichenanzahl

2. Umgang mit Passwörtern

iii. Grenzen einer Brute-Force Attacke

1. Beispiel:

Kombination= 26^7

= 8.031.810.176

Zeit, für das knacken eines Passwortes:

$$\frac{\text{Kombinationen}}{\text{Anzahl der generierten Schlüssel pro S}}$$

2. Umgang mit Passwörtern

iii. Grenzen einer Brute-Force Attacke

1. Beispiel:

1. **Schneller PC mit spezieller Software generiert knapp 2,1 Milliarden Schlüssel pro Sekunde**

$$\frac{8.031.810.176}{2.096.204.400}$$

Ergebnis:= 3,83 s

Bei einer Zeichenanzahl von 52 und einer Passwortlänge von 8 Zeichen = 7,08 Stunden

2. Umgang mit Passwörtern

b. Dictionary – Angriff

- gehört zu der Brute Force Methode
- kann die Brute Force Attacke abkürzen
- Es werden nicht alle Kombinationen getestet, nur die, die einen Sinn ergeben
- das entsprechende Programm liest ein Wörterbuch aus
- Wenn das Passwort ein Wort ist, das in einem Wörterbuch auftaucht, dann ist es geknackt.

2. Umgang mit Passwörtern

c) BarsWF MD5 Passwort Knacker

- MD5 Kryptographische Hashfunktion
- Eine beliebige Nachricht kann ein 128-Bit Hashwert (Prüfsumme) erzeugen
- 1991, unteranderem von Ronald L. Rivest entwickelt
- MD5 Hashes werden als 32 Stellige Hexadezimalzahlen dargestellt.

c) MD5 Passwort Knacker

```
md5("Franz jagt im komplett verwahrlosten Taxi quer durch Bayern") =
a3cca2b2aa1e3b5b3b5aad99a8529074
```

```
md5("Frank jagt im komplett verwahrlosten Taxi quer durch Bayern") =
7e716d0e702df0505fc72e2b89467910
```

2. Umgang mit Passwörtern

c) MD5 Passwort Knacker

- BarsWF
- mehrere Millionen Hashes pro Sekunde
- GPU als Co-Prozessor
  - CUDA Framework von nVidia 2007 zur Vefügung gestellt
- Mit einer ATI Radeon HD 4800 über 893 MHash/sec

2. Umgang mit Passwörtern

c) FAZIT BarsWF MD5 Knacker

- Albtraum für kurze Passwörter
- einfacher und schneller als Brute Force und John the Ripper
- Nachteil: nur MD5- Algorithmus wird unterstützt (NOCH)

2. Umgang mit Passwörtern

4.Social Engineering

- „soziale Manipulation“
- zwischenmenschliche Beeinflussung mit dem Ziel, den Menschen dazu zu bringen vertrauliche Informationen preis zu geben.
- Verschieden Methoden für Social-Enginnering

2. Umgang mit Passwörtern

4.1 Methoden

I. Computer Based Social Engineering

a) Phishing

b) Pharming

c) Trojaner als Keyloger

II. Human Based Social Engineering

III. Reverse Sozial Engineering

2. Umgang mit Passwörtern

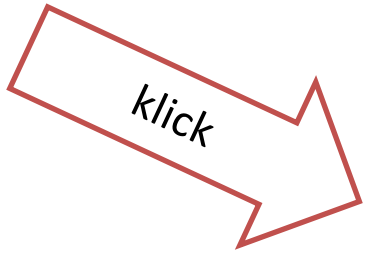
i. Phishing

- fishing + Phreaking = Phishing
- „Angeln nach Passwörtern mit Ködern“
- Versuche mittels gefälschten www-Adressen, E-Mails oder Kurznachrichten an vertrauliche Informationen zu kommen, um diese wiederum z.B. für Kontoplünderung einzusetzen.

2. Umgang mit Passwörtern

i. Phishing

- erste Versuche des Pishings im Internet, Nutzern von Instant-Messengern wie z.B. ICQ über E-Mails aufzufordern, Ihre Zugangsdaten in ein Formular einzutragen
- Pishing-Angriffe im Bereich des Online-Banking



2. Umgang mit Passwörtern

i. Phishing

- Benutzer wird aufgefordert seine Bankdaten einzugeben inkl. PIN und TAN Nummern
- Danach wird der Benutzer weiter auf die normale Seite weiter geleitet.
- Benutzer ist zufrieden, doch seine Daten sind in falschen Händen
- Diese Webseiten authentisieren in der Regel nur über ihr Aussehen.

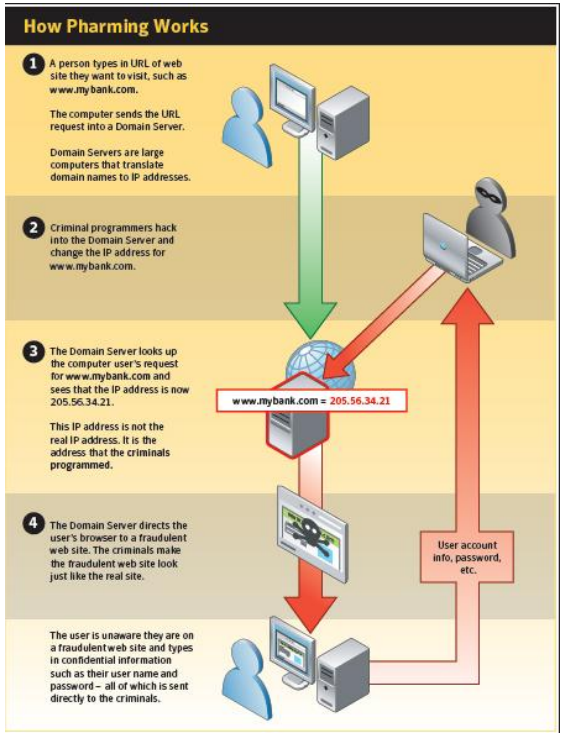
2. Umgang mit Passwörtern

ii. Pharming – Phishing ohne E-Mail

- Hier gibt der User die korrekte URL seiner Bank ein.
- Wird jedoch nicht mit dem Server der Bank verbunden, sondern mit dem Server des Angreifers.
- Dies kann dann passieren, wenn vorher ein Angriff auf den DNS Server und/ oder *Routingprotokolle* stattgefunden hat.

2. Umgang mit Passwörtern

ii. Pharming- Phishing ohne E-Mail



2. Umgang mit Passwörtern

ii. Pharming – Phishing ohne E-Mail

- SSL – Zertifikate durch Hashfunktionen
- seit 2009 Schwachstellen bei den Hashfunktionen MD5 und SHA-1
- Es ist nicht mehr ausgeschlossen, dass „echte“ Zertifikate von böswilligen Angreifer

2. Umgang mit Passwörtern

iii. Trojaner und Keylogger

- Trojaner die als Keylogger arbeiten
- Dabei werden alle Eingaben des Nutzers mitprotokolliert oder verändert.
- neueste Generation an Trojaner kann sogar die Kontodaten ändern
- Verschleiert die Manipulation mit Hilfe eines PopUp –Fensters
- 20 % aller Firmen sollen mit solchen Trojaner infiziert sein
- im privatem Bereich, Tendenz steigent.

2. Umgang mit Passwörtern

6. Quellen

I. Bücher:

1) **Kryptographie und IT-Sicherheit (Springer 2008);** Joachim Swoboda | Stephan Spitz | Michael Pramateftakis

2) **Einführung in die Kryptographie**

II. Zeitschrifte

1) **Hacking Februar 2010**

2. Umgang mit Passwörtern

6. Quellen

III. Internet

- http://de.wikipedia.org/wiki/Passwort
- http://de.wikipedia.org/wiki/Authentifizierung
- http://www.heise.de/security/artikel/Passwoerter-unknackbar-speichern-1253931.html
- http://de.wikipedia.org/wiki/MD5
- http://de.wikipedia.org/wiki/Kryptologische_Hashfunktion
- http://www.youtube.com/watch?v=NbzQjCjVoGY

Techniksеminar

Vielen Dank für Ihre Aufmerksamkeit

NOCH FRAGEN ?

Kushtrim Lulaj

wing8869@fh-wedel.de

Tel: 01578/ 2541919