Arbeitskreis IT-Sicherheit
- Paßwort -

O.Gießelmann Gelsenkirchen, 15.10.04

Inhaltsverzeichnis

1. Sicherheit von Paßwörtern 2
2. Angriffe auf Passwörter 2
3. Generierung von Passwörtern 3
3.1 manuelle Passwörter 3
3.2 automatisch generierte Paßwörter 4
3.3 Paßwortlänge und –komplexität 4
3.4 Tipps (schlechte und gute Passwörter) 5
3.5 Paßwortverschlüsselung 6
4. Verwaltung von Paßwörtern 9
4.1 manuelle Passwortverwaltung 9
4.2 Software 9
4.2.1 AMP (Alle meine Passwörter) 9
4.2.2 1PW 10
4.2.3 CrypTool 10
4.2.4 Norton™ Password Manager 10
4.2.5 Password Depot 11
4.3 in Browsern 11
4.3.1 Internet Explorer 12
4.3.2 Opera 12
4.3.3 Netscape 13
4.4 Fazit 13
5. PGP Verschlüsselung von Daten und e-mails 13
6. Umgehung von Paßwörter 15
7. Grundlagen zum möglichst sicheren Umgang mit Passwörtern und Systemen 15
8. Literaturhinweise 16

1. Sicherheit von Paßwörtern

Der Sinn und Zweck eines Passwortes ist es einen Zugang zu einem elektronischen System vor unbefugtem Zugriff zu schützen und eine Authentifizierung des eigentlichen Benutzers zu ermöglichen.

Zur personifizierten Authentifizierung und Anmeldung an ein solches System gehört daher immer der **Benutzername** und ein „**sicheres Passwort**“ (s. weiter).

Ein „**unsicheres Passwort**“ kann evtl. von einem potentiellen Angreifer ermittelt (**cracken**) werden und eröffnet damit den Zugriff auf das Konto mit dessen Berechtigungen. Der Angreifer kann somit unter falschem Namen agieren und evtl. beliebigen Schaden anrichten. Um so schlimmer ist es sein, wenn ein Administrator – Kennwort gecrackt worden ist und der Angreifer nun volle Kontrolle über das System erhalten hat.

Passwörter müssen daher immer geheim gehalten werden und dürfen nicht an dritte weitergegeben werden oder denen zugänglich gemacht werden.
Die sicherste Möglichkeit der Passwort – Verwaltung ist es daher immer, die Passwörter im Kopf zu behalten und nicht auszusprechen.
Bei der Fülle an Passwörter kann dies evtl. schwierig oder gar unmöglich sein, daher ist es u.U. zweckmäßig Passwörter zu notieren und an einer für andere nicht zugänglichen Stelle aufzubewahren (Tresor, Hosentasche).
Wird eine Speicherung auf einem elektronischen System in Betracht gezogen, muß auf jeden Fall gewährleistet sein, daß niemand anderes auf dieses System bzw. auf diese Daten zugreifen kann. Dies kann z.B. durch eine Software geschehen, die einen relativ sicheren Verschlüsselungsalgorithmus bietet (siehe später). In diesem Fall braucht sich der Anwender also nur das Passwort dieser Software zumerken.

Dies alles setzt aber einen verantwortungsvollen Umgang mit dem eingesetzten System voraus, also auch z.B. das Sperren des PC’s beim Verlassen des Arbeitsplatzes.

2. Angriffe auf Passwörter

Wie bereits erwähnt braucht ein Angreifer bei einem nicht gesperrten System nur aktiv zu werden und gar kein Paßwort auskundschaften.

Ein unachtsam weggelegter Notizzettel mit dem Passwort ist ebenfalls ein leichter Zugang. Gleichbedeutend ist der Versand von Kennwörtern mittels unverschlüsselter Transportmedien, also z.B. per e-mail. Eine e-mail ist in unverschlüsselter Form (PGP) wie eine Postkarte anzusehen, die im Zweifelfall von jedem gelesen werden kann!

Eine weitere Möglichkeit, um an ein Passwort zu gelangen, ist es, dem Benutzer bei der Eingabe seines Passwortes über die Schulter zu blicken und sich die Tastenkombination zu merken!!!

Es gibt aber auch auf elektronischem Wege Möglichkeiten an Passwörter fremder Personen zugelangen.
Hierzu werden vom Angreifer mittels entsprechender Software (Crack Programme) z.B. die Datenbank eines Systems, die zur Authentifikationsverifikation nun mal notwendig ist, untersucht.

Diese Programme sind in der Lage z.B. anhand von **integrierten Wörterbüchern** und Bibiliotheken dort abgelegte Passwörter zu ermitteln.
Unter Umständen sind diese Bibiliotheken sogar lernfähig oder durch Hinzufügen weiterer Bibiliotheken erweiterbar.
Somit kennt eine solche Software z.B. auch lateinische oder medizinische Fachbegriffe.
Wenn ein Passwort also z.B. „Hypertonie“ (Bluthochdruck) heißt, kennt auch die Cracksoftware diesen Begriff und hat das Passwort in sehr kurzer Zeit ermittelt!!!

Wenn die Methode der Bibiliotheken versagt, kann das Passwort mittels eines „**Brute Force**“ nach rein mathematischen Algorithmen einfach ausgerechnet bzw. ausprobiert werden.

Bei der Verwendung von **Key-Logger Programmen** werden die Tastatureingaben des unwissenden Benutzers einfach mitprotokolliert und stehen dem Angreifer damit in Klarschrift zur Verfügung. Key-Logger stehen auch als Hardware Varianten zur Verfügung. Dies sind elektronische Speicher auf Microcontrollerbasis, die zwischen Tastatur und PS/2 Port (Tastatur – Buchse) geschaltet werden oder direkt in die Tastatur eingebaut werden können.

Auch Office Produkte bieten dem Benutzer die Möglichkeit seine Dokumente von unbefugtem Zugriff zu schützen.
Während Word 6.0 und 7.0 (´95) aufgrund des verwendeten Verschlüsselungsalgorithmusses einen eher schwachen Schutz bieten, sind Dokumente die in Word 97, 2000 und XP erstellt wurden, relativ gut geschützt. Vorrausgesetzt man hält sich bei der Generierung der Passwörter an die später noch angesprochenen Grundsätze. Die Wahl der eingeschränkten Sicherheit (Schwache Codierung (XOR)), die ab Word XP bereitgestellt wird, ist eher **nicht zu empfehlen**, da sie dem Standard von Word 95 Nahe kommt. Einen erhöhten Schutz, bezogen auf Word 97, bieten die Verfahren (RC4, Microsoft Base Cryptographic Provider v1.0).
Diese Dokumente sind nach dem Vergessen der Kennwörter nicht mehr zu öffnen!

3. Generierung von Passwörtern

Es gibt grundsätzlich die Möglichkeiten sich ein Passwort selber einfallen zulassen oder es mittels eines Zufallsgenerators generieren zulassen.

3.1 manuelle Passwörter

Bei manuellen ausgedachten Passwörter neigt man vermutlich dazu, ein möglichst leicht zu merkendes, auszuwählen.
Auch ist es sehr gebräuchlich den Benutzernamen gleich mit als Passwort zu verwenden oder diesen nur geringfügig, z.B. durch Anhängen einer Zahl oder eines Sonderzeichens (Schultz04), zu verändern.
Ebenso sind die sich vielfach im Einsatz befindlichen „trivialen“ oder „assoziativen“ Passwörter aus sicherheitsrelevanter Sicht nicht zulässig, da die zuvor angesprochenen Crack-Programme genau diese Schwachstelle des Benutzers auszunutzen wissen!

Zur Generierung sicherer manueller Passwörter schreibt man sich am besten einige Sätze, inklusive oder ergänzt durch Sonderzeichen und Zahlen zeilenweise auf und wählt dann nach einem persönlich ausgedachten Muster einige Zeichen daraus aus. Z.B. nehme man jeden ersten Buchstaben eines Wortes oder aber wähle eine Spalte aus, die dann die Passwörter ergeben.

Beispiel:
Text:

F	e	s	t		g	e	m	a	u	e	r	t		i	n		d	e	r		E	r	d	e	N						
S	t	e	h	t		d	i	e	5	F	o	r	m	,		a	u	s	7	L	e	h	m		g	e	b	r	a	n	n	t	.
H	e	u	t	e		m	u	ß	3	d	i	e		G	l	o	c	k	e		w	e	r	d	e	n	.					
F	r	i	s	c	h		G	e	s	e	l	l	e	n	,		s	e	i	d		z	u	r		H	a	n	d	.			
V	o	n		d	e	r		S	t	i	r	n	e		h	e	i	ß														
R	i	n	n	e	n		m	u	ß		d	e	r		S	c	h	w	e	i	ß	,										
S	o	l	l		d	a	s		W	e	r	k		d	e	n		M	e	i	s	t	e	r		l	o	b	e	n	,		
D	o	c	h		d	e	r		S	e	g	e	n		k	o	m	m	t		v	o	n		o	b	e	n	.			

Die sich daraus ergebenden Passwörter:
FguidESd5F,a7Lg u53stßWS -> siehe auch Kapitel 3.3

3.2 automatisch generierte Paßwörter

Mittels diverser u.a. auch als Free- oder Shareware erhältlicher Programme können Passwörter beliebiger Komplexität und Länge automatisch generiert werden.
Bsp.: Passwort-Generator 2.2, AmP 2.2 (Alle meine Passworte) Zu Bedenken ist aber, daß eine beliebige Software von unbekannten Personen programmiert wurde und man den genauen Algorithmus der Erstellung bzw. eine mögliche Speicherung nicht einsehen kann (! Trojanische Pferde)

3.3 Paßwortlänge und –komplexität

Mit der Beschaffenheit eines Passwortes steht oder fällt die Sicherheit eines Systems.

Die Kombinatorik lehrt uns, daß es bei einem Zeichenvorrat von **n** Zeichen und **m** Stellen genau $\mathbf{n^m}$ Kombinationsmöglichkeiten gibt.
Dies entspräche z.B. im dezimalen Zahlensystem bei 10 Zahlen und zwei Stellen genau $10^2 = 100$ Kombinationsmöglichkeiten.
Überträgt man diese Überlegung nun auf die Passwortsicherheit ergibt sich gleiches.
Je mehr Zeichenvorrat (Komplexität) und je mehr Stellen (Länge), um so größer ist die Anzahl der Kombinationsmöglichkeiten und um so sicherer ist das Passwort.

Hier einige Rechenbeispiele zur Verdeutlichung:

Bsp.1:
Ein Passwort besteht aus dem Zeichenvorrat der kleinen Buchstaben (a-z) und einer Stelle:
Es ergeben sich folglich $26^1 =$ **26** Kombinationen.

Bsp.2:
Ein Passwort besteht aus dem Zeichenvorrat der kleinen Buchstaben (a-z) und acht Stellen:
Es ergeben sich folglich 26^8 = 208.827.064.600 = **208.827 Mio.** Kombinationen.

Bsp.3:
Ein Passwort besteht aus dem Zeichenvorrat der kleinen Buchstaben (a-z), der großen Buchstaben (A-Z) und acht Stellen:
Es ergeben sich folglich 52^8 = 53.459.728.530.000.000 = **53.459.728 Mio.** Kombinationen.
Bsp.4:
Verwendet man zusätzlich alle Zahlen (0-9) und 33 Sonderzeichen **(** °!“§$%&/()=?`^{[]}\,.-;:_#’+*~<>| **)** bei 8-stelligem Passwort, ermittelt man
95^8 = **6.634.204.313 Mio.** Kombinationen.

Bsp.5:
Nun wird die Anzahl der Stellen auf 10 erhöht:
95^{10} = **59.873.693.920.000.000 Mio.** Kombinationen.

Setzt man nun im weiteren einen PC mit 3 GHz Prozessor voraus, der abhängig vom Hersteller und Betriebssystem, innerhalb einer Sekunde ca. 20.000.000 = 20 Mio. Keys / Sekunde errechnen kann, wäre

das Passwort aus **Bsp.1** in $1{,}3*10^{-6}$ s = **1,3 Mikrosekunden** berechnet.
Für das Passwort aus **Bsp2.** benötigt der PC 10441 Sek. = 174 Min. = **2,9 Std.**
Im **Bsp3**. ergeben sich 89099 Minuten = 1484 Stunden = **61Tage**
Für das Kennwort aus **Bsp.4** rechnet er schon 184283 Std. = 7678 Tage = **21 Jahre**
Das Passwort aus **Bsp.5** könnte erst nach 69.298.256 Tagen = **189858 Jahren** errechnet werden.

Aber auch eine Brute Force Attacke könnte, wenn auch unwahrscheinlich, gleich bei der 1. Probe zum Erfolg führen. Setzt man voraus, daß durchschnittlich jede 1000. Probe ein Erfolg ist, verbliebe also für
Bsp.1: 1,3 ns,
Bsp.2: 10 s,
Bsp.3: 44 min
Bsp.4: 5528 min = 92 Std. = 3,8 Tage.
Bsp.5: 49894 min = 831579 Std. = 34649 Tage = 94 Jahre

Zu empfehlen ist also ein Passwort aus **min. 10 Zeichen** und dem **gesamten zur Verfügung stehenden Zeichenvorrat (** A-Z, a-z, 0-9, °!“§$%&/()=?`^{[]}\,.-;:_#’+*~<>| **)**

3.4 Tipps (schlechte und gute Passwörter)

Bsp. Schlechte Passwörter

einfache PW:	Januar01, Januar04, Januar2004, Februar02, PC01, Informatik1
aus Namen:	Sabine65, Susi, Diana, Opel, Schumi, Ferrari, Harry,
aus persönlichen Daten:	HMSK47 (Harry Müller (Jahrgang 1947) + Susi Krämer), 12.03.1970,
KFz Kennz.:	GE-OG2109,
Tastaturmuster:	qwert, 123456, asdfg

Beispiele für mittel gute Passwörter, welche man sich leicht merken kann:
surinam*3, 7fenster?

Beispiele für gute Passwörter, welche man sich noch einigermaßen merken kann
?zazuli?, Sa65bi%ne, O11pel!, viwazfe%%, $gunozvi,

Beispiel für sehr gute Passwörter, welches man sich aber kaum merken kann
m3üf[Kfv=, fk3(d%oI39, TnZ4&2kaq

3.5 Paßwortverschlüsselung

Bei der Übertragung von Daten innerhalb eines Netzwerkes, auch dem Internet, werden die Daten in Form von Datenpaketen ausgehend vom Sender über viele Router zu einem Empfänger übermittelt. Mögliche Angreifer könnten sich in diese Übertragungsstrecke mit einklinken, um einen solchen Datenstrom mitzulesen oder zu modifizieren. Enthält der Datenstrom nun sensible Daten, wie z.B. Passwörter, Kreditkartennummern, o.ä., die unverschlüsselt übertragen werden, könnte ein möglicher Angreifer also diese im Klartext mitlesen oder verändern.
Ziel einer Datenverschlüsselung ist es also, sensible Daten so zu chiffrieren, daß die Nachricht nur vom Empfänger wieder dechiffriert und damit lesbar gemacht werden kann.
Die hierzu entwickelten und mit der Zeit modifizierten und verbesserten Verschlüsselungsverfahren können natürlich nicht nur sicheren zur Nachrichtenübertragung, sondern auch zur sicheren lokalen Datenspeicherung eingesetzt werden.
Die Kryptographie soll somit also die Integrität (Unversehrtheit), Authentizität (eindeutige Herkunft) und Verbindlichkeit (Übertragungskontrolle) der Daten sicherstellen.
Die folgende Tabelle soll eine Übersicht über die kryptografischen Verfahren und Ihre Eigenschaften geben.

Verfahren	E. Datum	Art	Arbeitsweise	Sicherheit	Anwendung
AES (Advanced Encryption Standard)	Okt. 2000	Rijndael, zum AES gekürt Blockchiffre, symmetrischer Verschlüsselungs-algorithmus	Blocklänge und Schlüssellänge unabhängig voneinander die Werte 128, 192 oder 256 Bit Versch. Teilschlüssels nacheinander auf den Klartext-Block angewendet, Anzahl der Runden variiert, abhängig von Schlüssellänge und Blockgröße.		AES wird u.a. von WPA, dem Verschl.proto für WLAN und bei SSH genutzt
Blowfish	1993,94,95 Bruce Schneier	symmetrische Blockchiffre	64-Bit-Blöcke Schlüssel zw. 32 und 448 Bit lang Feistelchiffre mit 16 Runden	keine wesentliche Schwäche	
DES/3 DES	1973 NIST/ NSA/ NBS und IBM	symmetrischer Verschlüsselungs-algorithmus	jeder Block wird unter Verwendung des Schlüssels einzeln chiffriert, wobei die Daten in 16 Iterationen bzw. Runden von Substitutionen und Transpositionen (Permutation) nach dem Schema von Feistel "verwürfelt" werden.	Schlüssellänge von 128 Bits auf 56 Bits gesenkt, aufgrund seiner geringen Schlüssellänge als nicht mehr sicher genug, aber Vorbild für andere Algorithmen	
IDEA	1990 ETH Zürich von James L. Massey und Xueija Lai	Sym. Blockchiffre,	128-Bit-Schlüssel, Zerteilung Klartext in 64-Bit-Blöcke, Zerteilung Schlüssel in 16-Bit-Blöcke, Die Verschlüsselung geschieht durch Kombination der logischen Operation XOR, der Addition modulo 2^{16} und der Multiplikation modulo $2^{16}+1$	optimiert, Angriffen durch differentielle Kryptoanalyse zu widerstehen	

IPSec	1998	symmetrischen wie asymmetrischen Schlüssel, manuell oder automatisch ausgehandelt	Protokoll, entwickelt, um die Schwächen des Internetprotokolls (IP) zu beheben gewährleistet Vertraulichkeit, Authentizität und Integrität über TCP/IP, schützt vor Replay-Angriffen. Verwendet IKE, basiert auf UDP und nutzt std. Port 500	Kritikpunkte: hohe Komplexität und Fehleranfälligkeit, beste derzeit erhältliche IP-Sicherheits-Protokoll	
MD2	1989 Ronald L. Rivest	Hash-Funktion	Bildung des Hashwert (Streuwertfunktion) einer Nachricht, durch Bildung des Vielfachen der Blocklänge (128 Bit bzw. 16 Byte), anhängen einer Prüfsumme optimiert für 8-Bit Rechner	unsicher, da mangelnde Kollisionsbeständigkeit	
MD4	1990 Ronald L. Rivest	Hash-Algorithmus	auf 32 Bit Rechnern besonders schnell und einfach. erzeugt einen Hashwert mit einer Länge von 128 Bit.	Unsicher, s. MD2 Methode bekannt, die in 1 Stunde zwei Nachrichten erzeugen kann, die denselben Hashwert ergeben	
MD5	<1994 Ronald L. Rivest	Einweg-Hash-Funktion	4 (statt 3 bei MD4) gegenüber MD4 modifizierte Runden, erzeugt einen Hashwert von 128 Bit. SHA-1 besser	Theor. Angriffs-szenario denkbar, wg. Pseudo-Kollisionen, modif. Ver. Von MD5 geknackt, wahre nicht	
RC4	1987 Ronald L. Rivest	für Software optimierter Stromchiffrierer	variable Schlüssellänge, kann bis zu 2048 Bit betragen. RC4 verschlüsselt immer ein Byte auf einmal. substitution box eine Grundkomponente von sym. Verschlüsselungsverfahren ändert sich während der Verschlüsselung fortlaufend	Quellcode 1994 anonym veröffentlicht	Verschlüsselung von Daten
RIPEMD		Algorithmus für eine kryptograph-ische Hashfunktion, die eine 160-Bit-Prüfziffer liefert	basiert auf MD4 , gleicht aber in Stärke und Performanz SHA-1	fragwürdige Scherheit keine Patentbeschränkungen	
RIPEMD-160 ...	1996 Hans Dobbertin, Antoon Bosselaers und Bart Preneel	kryptographische Hashfunktion, die eine 160-Bit-Prüfziffer liefert	Es existieren auch 128-, 256- und 320-Bit-Versionen dieses Algorithmus' namens RIPEMD-128, RIPEMD-256 bzw. RIPEMD-320. Die letzteren reduzieren die Wahrschein-lichkeit von Hashwert-Kollisionen	weniger Sicherheitslücken als SHA, jedoch unpopuläler	
RSA	1977 Ronald L. Rivest, Adi Shamir und Leonard Adleman	asymmetrisches Verschlüsselungsverfahren	Ronald L. **Ri**vest, Adi **S**hamir and Leonard **A**dleman stiessen bei der Beweisführung der Unsicherheit verschiedener Verfahren auf eines, wo sie keinerlei Angriffspunkte fanden. Einwegfunktionen, mit Falltürfunktionen, um allerdings die Entschlüsselung tatsächlich möglich zu machen. Verwendung öffentlicher Schlüssel Promfaktorzerlegung Verschlüsseln: $C \equiv K^e \bmod N$ Entschlüsseln: $K \equiv C^d \bmod N$	Sicherheit besteht darin, daß der An-greifer d nicht kennt Um d zu berechnen benötigt er $\varphi(N)$. $\varphi(N)$ ist aber für grosse Zahlen nicht effizient berechenbar. Bisher 174-ziffrige Zahl zu faktorisieren! Die z.Z verwendete 300-ziffrige Schlüssel-zahl kann bisher noch nicht erreicht werden.	Signieren von Nachrichten, Datenübertragung
SHA	1993 NIST/NSA	Secure Hash Algorithmus Hash-Funktion	Länge 160 Bit für Nachrichten mit einer Größe von bis zu 264 Bit ähnelt im Aufbau dem von Ronald L. Rivest entwickelten MD4 Mit seinem längeren Hashwert widerstandsfähiger gegen Brute-Force Angriffe und Kollisionen	Design-Fehler im 1993 -> SHA-1	zum Signieren gedacht
SHA-1	1995 NIST/NSA	Secure Hash Algorithmus Hash-Funktion	Durch Einsatz einer fünften Variablen ist SHA-1 auch im Vergleich zu MD5 resistenter gegen Kollisionen	bisher keine wirkungsvollen kryptografischen Angriffe bekannt	zum Signieren gedacht

SHA-512...	2002 NIST/NSA	Secure Hash Algorithmus Hash-Funktion	SHA-256, SHA-384 und SHA-512 Basieren auf Vorgängerversionen, größere Hashwerte angefügte Zahl = Länge des Hashwerts 384 und 512 = Vorteil, da sie Dateien bis zu einer Größe von 2^{128} Bit	s.o.	zum Signieren gedacht
SSL	1996 Firma Netscape	SSL (Secure Sockets Layer) bezeichnet ein von der Firma Netscape entwickeltes Übertragungsprotokoll, mit dem verschlüsselte Kommunikation mittels Tunneling möglich ist.	Das SSL-Protokoll besteht aus zwei Schichten (layers): Zu Grunde liegt in der untersten Ebene das SSL Record Protocol, das zur Kapselung verschiedener höherer Protokolle (higher level protocols) dient. Der Vorteil des SSL-Protokolls ist die Möglichkeit, jedes höhere Protokoll auf Basis des SSL Protokolls zu implementieren. Damit ist eine Unabhängigkeit von Applikationen und Systemen gewährleistet		Häufige Anwendung findet SSL bei der sicheren Fernadministration per SSH oder der Übertragung verschlüsselter Webseiten per HTTPS.
TLS	1996 Firma Netscape	Transport Layer Security (TLS) ist ein Protokoll zur Verschlüsselung von Datenübertragungen im Internet	Im OSI-Modell ist es über TCP und unter Applikationsprotokollen wie HTTP oder SMTP angesiedelt. Als Basis zur Entwicklung von TLS wurde das 1996 von der Netscape Communications Corporation veröffentlichte Protokoll SSL 3.0 verwendet.		Verschlüsselung von Datenübertragungen im Internet
Twofish	1998/1999 Bruce Schneier	symmetrischer Verschlüsselungs-algorithmus, Kandidat für den Advanced Encryption Standard -> 3.	Nachfolger von Blowfish stellte sich 1998/1999 dem Ausscheid zum Advanced Encryption Standard Twofish erlaubt die Schlüssellängen 128, 192 und 256 Bit. Der Textblock wird in vier 32-Bit-Worte aufgeteilt, XOR-Verknüpfung, 16/32 Runden, Rotation in der Funktion F , Aufteilung in vier Byte und Substitution in der S-Box. Die Outputs der S-Boxen werden zu einem Vektor zusammengefasst und mit der Matrix MDS multipliziert, Pseudo-Hadamard-Transformation, XOR-Verknüpfung und Rotation Dieser Vorgang wird insgesamt 16-mal durchgeführt, Vertauschung der Worte XOR-Verknüpfung		
Rijndael	Oktober 2000	Advanced Encryption Standard (AES) -> 1.	Nachfolger für DES bzw. 3DES		
Serpent	Ross Anderson, Eli Biham und Lars Knudsen	symmetrischer Verschlüsselungsalgorithmus Kandidat für den Advanced Encryption Standard -> 2.	Blockgröße von 128 Bit und kann mit jeder Schlüsselgröße bis 256 Bit umgehen, 32 Runden	etwas langsamer	
Cast128		Feistel ciphers	Input: 64Bit Wörter, 128Bit-Schlüssel, Output: 64-Bitwort Spaltung des Input in 2 Worthälften und des Keys in 16 Subkeys, Berechnung des Outputs in 16 Runden und Zusammenfügen. Es werden 8 S-Boxen verwendet.		

Die unterschiedlichen Geschwindigkeiten einigen Verschlüsselungsalgorithmen:

Verschlüsselung	max. Schlüssellänge	Geschwindigkeit
Blowfish	448 Bits	2.46MB/sek
Cast128	128 Bits	2.60MB/sek
Cast	256 Bits	1.63MB/sek
RC2	1.024 Bits	0.47MB/sek
Rijndael	256 Bits	2.12MB/sek
Twofish	256 Bits	2.12MB/sek

4. Verwaltung von Paßwörtern

4.1 manuelle Passwortverwaltung

Mit maueller Passwortverwaltung ist das im Kopf behalten der Passwörter oder das Notieren auf einem Zettel gemeint.
Ersteres ist zwar einigermaßen gegen Mißbrauch sicher, allerdings bei zunehmender Anzahl und regelmäßiges Wechseln der Passwörter auch aufgrund von Datenverlust unsicher.
Wenn Passwörter auf einem Zettel notiert werden, besteht immer die Gefahr, daß der Zettel durch Unachtsamkeit abhanden kommt und die Passwörter dann in Klarschrift 3. Personen zugänglich wären. Bei dieser Praxis ist also große Disziplin und Sorgfalt des Anwenders von Nöten. Notfalls müssen bei Verlust sämtliche Passwörter unverzüglich zurückgesetzt und erneuert werden, damit das gesamte Computersystem nicht angeifbar wird.

4.2 Software

Es stehen inzwischen einige Programme zur Verfügung, mit denen sich die Flut von Passwörtern in einer verschlüsselten Datenbank verwalten lassen. Einige Varianten stehen auch als Shareware oder Freeware Version zur Verfügung. Hier muß allerdings beachtet werden, daß die „abgespeckten“ Derivate möglicherweise nur eingeschränkte Funktionen, also auch eingeschränkte Verschlüsselungsmethoden zur Verfügung stellen, die dann wiederum ein Sicherheitsrisiko darstellen. Im folgenden werden einige Beispiele dargestellt.

4.2.1 AMP (Alle meine Passwörter)

Die Software AMP liegt aktuell in der Freeware Version 2.21 vor und wurde von Mirko Böer, Softwareentwicklung, Prinzenweg 14, D - 04277 Leipzig, entwickelt.
Es bietet nach der Installation die Möglichkeit, Passwörter und Zugangsdaten verschiedener Benutzer nach Kategorien geordnet in verschlüsselbaren Datenbanken abzulegen.
Als Zugangssicherung wird je Benutzer ein Name und Passwort abgefragt. Selbsterklärend ist, dass das Passwort der Schlüssel zu allen anderen in der Datenbank abgelegten Passwörtern darstellt und daher sehr sorgfältig, unter Anwendung der oben erklärten Kriterien eines sicheren Passwortes gewählt werden muss!!!
Man hat nun die Möglichkeit zu einem Zugangsnamen 2 Passwörter einzutragen, oder aber mit dem integrierten PW-Generator ein zufälliges Passwort erzeugen zu lassen.
Ferner kann ein Kommentar hinzugefügt und ein zugehöriges Programm, Webseite etc. automatisch geöffnet werden.
Die Anzeige kann wahlweise in Sternchen codiert oder in Klartext erfolgen.
Der PW-Generator ist in PW-Länge und Komplexität einzustellen, und damit je nach Einstellung, in der Lage sichere Passwörter zu generieren.
Als weiteres Feature bietet das Programm die Option, beliebige Dateien mit einem der integrierten Algorithmen zu verschlüsseln.
Die integrierten Algorithmen sind BlowFish, TwoFish, Cast128, RC2, RC5 und RC6.

Mit den gleichen Algorithmen können natürlich auch die angelegten Passwortdateien chiffriert werden.
Die Datenbank kann als .CSV-Datei importiert und als .TXT, .HTML, .XML, Excel und Word exportiert werden.

4.2.2 1PW

Das Passwort Verwaltungsprogramm 1PW liegt aktuell in der Version 3.9 vor und enthält ebenso wie AMP ein Passwortgenerator, kann Dateien verschlüsseln und kann ***-Passwortfeldern auslesen, um vergessene Passwörter wieder sichtbar zu machen, dies funktioniert allerdings nicht in Webseiten.
Das Programm ist käuflich erhältlich (privat 5,- EUR, Firmen, Vereine und Schulen 15 EUR / Lizenz), kann aber auch als Shareware und Freeware Variante heruntergeladen werden.
In der Shareware Variante können max. 3 Benutzer mit je 10 Datensätzen angelegt werden.
In der Freeware Version verschlüsselt es die gespeicherten Daten mit einem simplen Verfahren. **Die Daten sind nicht sicher!**
Im wesentlichen arbeitet das Programm nach gleichem Muster wie AmP, wirkt jedoch etwas professioneller. Dies äußert sich z.B. darin, daß nach Eingabe des Zugangspasswortes, dieses automatisch auf seine Sicherheit untersucht und prozentual angibt.
Als Verschlüsselungsalgorithmen stehen Blowfish, Cast128, Gost, RC2, Rijndael (AES) und Twofish zur Verfügung.
Auch hier ist wie bei AmP Import und Export möglich, jedoch nicht in den MS-Formaten.

4.2.3 CrypTool

Die Software CryptTool liegt aktuell in der Version 1.3.05 als Freeware Demoprogramm vor und dient neben dem Verschlüsseln beliebiger Dateien auch der Einarbeitung der verschiedenen Kryptographie Algorithmen. Die Verschlüsselungsschlüssel müssen jedoch manuell eingegeben werden.

4.2.4 Norton™ Password Manager

Mit Norton™ Password Manager 2004 von Symantec können Kennwörter sicher und ohne großen Aufwand verwaltet werden. Norton Password Manager speichert Kennwörter und andere vertrauliche Informationen für jeden einzelnen Benutzer. Anschließend ruft er automatisch die Daten ab, die Sie für Ihre E-Mail-Anmeldungen, Bestellformulare, Bankgeschäfte und andere Online-Aktivitäten benötigen. Und da dies alles von Ihrem eigenen PC aus geschieht, sind Ihre Daten jederzeit geschützt.

Funktionen:
Speichert Kennwörter, Telefonnummern, Adressen, Kreditkartennummern und andere vertrauliche Informationen sicher und bequem auf Ihrem Computer;
Ruft automatisch die Daten für kennwortgeschützte Anwendungen und Websites ab;
Schützt Ihre Daten vor unberechtigten Zugriffen durch leistungsstarke Verschlüsselung;
Der Setup-Assistent für vereinfacht das Erstellen sicherer Datenprofile für jedes Mitglied Ihres Haushalts;
Mehrere Profile ermöglichen die individuelle Organisation Ihrer Online-Informationen;
Profilkennwörter sorgen dafür, dass Benutzer nur jeweils ihre eigenen Daten abrufen können;
Die Sicherheitsmessung für Kennwörter hilft Ihnen bei der Einrichtung starker Profilkennwörter;
Mit drei verschiedenen Sicherheitsstufen lässt sich festlegen, wie häufig

das Profilkennwort abgefragt werden soll.

http://www.symantec.com/region/de/product/npm_index.html

Der Verschlüsselungsalgorithmus wurde angefragt, jedoch von Symantec nicht offengelegt.

4.2.5 Password Depot

Password Depot ist ein Produkt der Fa. Ace Bit GmbH und liegt aktuell in der Version 1.7.1.2 vor. Es ist auch als Freeware Version auf der Webseite http://www.password-depot.de/ erhältlich. Möchte man allerdings mehr als 20 Kennwörter gleichzeitig verwenden, muß man die Professional Edition für 29,- EUR kaufen.
Password Depot fordert direkt nach dem ersten Start auf, einen List Access Key einzugeben. Nun können neue Passwörter in einem Fenster neu eingegeben werden und mit Beschreibung, User Name und Link auf eine Adresse versehen werden. Ferner kann für das neue Password eine Sicherheitsabstufung und ein Ablaufdatum eingestellt werden. Mit der Funktion „Generate Random Password“ ist man in der Lage, ein zufällliges Password zuerstellen. Mit Hilfe eines verrauschten Feldes, über das man mit der Maus fährt, wird ein Password mit einstellbarer Komplexität und Länge erstellt.

4.3 in Browsern

Internet Browser, wie Internet Explorer (Microsoft), Opera, Netscape oder auch weitere bieten häufig die Möglichkeit, Passwörter zu speichern, um dem User das Arbeiten zu erleichtern. Hierbei werden die Passwörter direkt auf der Festplatte gespeichert. Je nach Betriebssystem werden die Kennwörter unterschiedlich abgespeichert. Windows 9x speichert die Kennwörter noch in der Passwortdatei des Benutzers, da diese Datei aber auch noch andere Informationen enthält ist es nicht anzuraten diese Datei zu löschen.

Bei Windows NT/2000 und XP werden die Kennwörter in der Registry abgelegt. Hier liegen die Kennwörter in der Registry des Benutzers in einem abgesicherten Bereich auf dem nur das System zugreifen kann. Unter:

HKEY_CURRENT_USER\ Software\ Microsoft\ Protected Storage System Provider

wird für jede Webseite ein extra Schlüssel angelegt in dem das Passwort wiederum Verschlüsselt abgelegt wird.
Trotz Verschlüsselung sollte man mit dem speichern von Passwörter vorsichtig sein, besonders wenn die Benutzung des Systems mit anderen User geteilt wird. Es gibt Tools, die eigentlich geschrieben wurden, um ein vergessenes aber gespeichertes Passwort wieder hervor zu zaubern oder einfach um die Eingaben zu sichern und auf einem anderen System zu benutzen. Diese Tools knacken die Verschlüsselung, können aber auch missbraucht werden.

Mit der Option:
"Verschlüsselte Seiten nicht auf der Festplatte speichern" aktivieren (nur Internet Explorer)
Damit können Sie verhindern, daß die angeforderten Seiten im Cache auf der Festplatte abgelegt werden. Somit ist es dann nicht möglich, die Daten später aus dem Cache zu lesen und Mißbrauch damit zu betreiben. Bei Internet Explorer sollten Sie diese Option unbedingt aktivieren, beim Netscape Navigator ist sie voreingestellt.

Mit Java können sogenannte Java-Applets erstellt werden und diese werden in eine Webseite eingebunden und dort ausgeführt. Durch einige Fehler in Java-Applets können diese ein Sicherheitsrisiko darstellen. Auf vertrauenswürdigen Seiten ist es jedoch eine nützliche Technik (z.B. für Online-Banking).
Ist Java aktiviert, kann mit JavaScript auf ein Java-Applet zugegriffen werden, das Schaden anrichten kann. Für **Netscape** / Mozilla und **Opera** gilt, daß bei deaktiviertem Java JavaScript zwar zu Ärgerlichkeiten führen kann, aber die Datensicherheit auf dem PC nicht gefährdet. Beim **Internet Explorer** stimmt das nicht ganz. Auf den ersten Blick könnte man meinen, daß bei deaktiviertem Java und ActiveX hier JScript (JavaScript für den IE) ebenfalls keinen Schaden anrichten kann. Dies ist falsch, weil mit dem Aktivieren von Scripting im Internet Explorer zugleich auch VBScript aktiviert wird und VBScript ein Sicherheitsrisiko ist.

4.3.1 Internet Explorer

Im Menü Extras, Befehl Internetoptionen, Kategorie Inhalte, Unterpunkt AutoVervollständigen: Deaktivieren Sie bitte die Kontrollkästchen **AutoVervollständigen verwenden für "Formulare" und "Benutzernamen und Kennwörter für Formulare".** Damit wird verhindert, daß erfasste Daten (Benutzernamen, Kennwörter, Formulardaten) auf der Festplatte gespeichert werden und somit von Dritten missbräuchlich verwendet werden können.
Die Kennwörter für die Internetseiten können nicht direkt gelöscht werden. Wenn Sie eine kennwortgeschützte Seite wieder aufrufen, haben Sie die Möglichkeit das Kennwort wieder aus der Liste zu entfernen, dafür müssen Sie den Hacken bei "Kennwort in Kennwortliste speichern" entfernen.

4.3.2 Opera

Der Browser Opera bietet, im Gegensatz zu Netscape uns Internet Explorer, einige zweckmäßige Features und Einstellmöglichkeiten.
Opera unterstützt die Verschlüsselungen TLS, SSL2, SSL3, 128 und 168 bit DES .

Menü Datei, Befehl Einstellungen, Punkt Privatssphäre (Alt-P):

Mit dem Deaktivieren von „*Mitloggen des Referers zulassen*“ verhindert man, daß der Browser Informationen Herkunfts-Log-Daten (Referrer) sendet. Bei den anderen nicht einstellbar.
Mit „*Automatische Weiterleitung zulassen*“ stellt man ein, ob der Browser automatisch auf andere Webseiten springen kann.
Deaktivieren Sie bitte das Kontrollkästchen "*Cookies benutzen, um passwortgeschützte Seiten zu verfolgen*".

Unter „Sicherheit“ kann der Passwort-Manager ausgeschaltet werden.
Unter „Verlauf und Cache“ kann der Festplatten Cache (Zwischenspeicher) gelöscht werden.
Unter „Fenster“ kann z.B. eingestellt werden, ob Pop-Up-Fenster aufgehen dürfen.

Ferner gibt Opera bessere Warnhinweise z.B. in Bezug auf Spammer und anderen Schädlinge die wirkliche Verweisziele zu verstecken versuchen. Zum Beispiel, führt die URL http://www.microsoft.com nicht zu Microsofts Homepage!!! Wenn man mit der Maus über den Link fährt, erkennt man den tatsächlichen Verweis **www.microsoft.com@69.0.231.197** , auch in der Statuszeile zu erkennen. Andere Browser würden hier wirklich nur www.microsoft.com anzeigen und den User über das wirkliche Ziel, einer Seite mit einem

Benutzernamen im unklaren lassen! Wird der Link trotzdem betätigt erscheint außerdem eine Warnmeldung! (siehe auch: http://tntluoma.com/opera/lover/7/16/de/ mit verschiedenen Browsern)
Opera steht unter anderem auf der Seite http://www.opera.com/ wahlweise als Vollversion oder als Freeware Version zur Verfügung. Die Freeware blendet in der Ecke oben rechts ein kleinen Werbe Banner ein.

4.3.3 Netscape

Im Menü „*Bearbeiten, Befehl Einstellungen, Kategorie Privatsphäre und Sicherheit, Unterpunkt Passwörter*“: sollte das Kontrollkästchen "*Passwörter speichern*" deaktiviert sein.
Netscape bietet nicht die Features feinen Einstellungsmöglichkeiten von Opera.

4.4 Fazit

Aus der Tatsache heraus, daß man generell mehrere Passwörter für verschiedene Rechner und Accounts verwenden sollte, die zudem auch noch möglichst komplex sein sollten, leitet sich also die Empfehlung ab, eine Software zur Verwaltung der Passworte zu verwenden.

Hierbei sticht für mein dafürhalten die Anwendung **AmP** heraus. Die Software besitzt außer etwas Werbeeinblendung keine Einschränkungen, ist einfach zu bedienen, gibt aufgrund der Verschlüsselungsalgorithmen gute Sicherheit und ist für mehrere Benutzer verwendbar.
Ferner kann das Programm auch z.B. auf einem Memory-(USB)-stick installiert werden und die Passwortdatei an einem beliebigen Ort gespeichert werden. Somit kann man seine Passwörter immer in digitaler Form bei sich haben. Zubeachten ist aber, daß man hier natürlich erst zugreifen kann, wenn man sich ans System angemeldet hat!

Ebenso weißt das Programm **Password Depot** eine einfache Bedienbarkeit auf, läuft aber nicht vom USB-Stick und ist auf max. 20 Kennwörter begrenzt.

5. PGP Verschlüsselung von Daten und e-mails

PGP steht für "Pretty Good™ Privacy", zu deutsch etwa "recht gute Privatsphäre". PGP ist ein Verschlüsselungsverfahren, daß es ermöglicht, Dateien und / oder e-mail digital zu verschlüsseln.
Wird eine e-mail „normal“ über das Netz versendet, kann man sie mit einer Postkarte vergleichen, die im Zweifelsfall jeder im Klartext lesen kann.
Verschlüsselt man diese mail mit PGP, kommt ein als äußerst sicher geltender Verschlüsselungsalgorithmus zu Anwendung, so daß die Information nur noch mit Hilfe eines „digitalen Schlüssel“ wieder entschlüsselbar und damit lesbar ist.
Somit wurde quasi die Postkarte in einen Umschlag gepackt, zuklebt und vom Postboten persönlich mit Rückantwort übermittelt. Man ist sich also (sicher), daß die Nachricht nur vom Schlüsselinhaber gelesen wurde.
PGP ist auch als Freeware erhältlich und kann z.B. auf der Seite:
http://www.pgp.com/products/de/freeware.html heruntergeladen werden.

Grundsätzliches:
Grundsätzlich muß man bei Verschlüsselungsverfahren zwischen symetrischen und asymetrischen Verfahren unterscheiden.

Bei den symetrischen Verfahren gibt es einen mehr oder weniger komplexen Schlüssel, der sowohl beim Verschlüsseln, als auch beim entschlüsseln verwendet wird.
Bei den asymetrischen Verfahren, gibt es für jeden Anwender ein Schlüsselpaar, einen öffentlichen und einen geheimen Schlüssel. Was mit dem öffentlichen Schlüssel verschlüsselt wurde, kann nur mit dem dazugehörigen geheimen Schlüssel entschlüsselt werden. Ein Nachteil dieser Verfahren ist die geringe Arbeitsgeschwindigkeit. Daher wurden hybride Verschlüsselungsverfahren entwickelt, die die Vorteile beider Varianten miteinander kombinieren.
Verschlüsselung:
PGP generiert für jede Verschlüsselung hierzu einen zufällig ausgewählten Schlüssel, der nur ein einziges Mal verwendet wird. Mit diesem Schlüssel verschlüsselt PGP die Nachricht mit einem schnellen, guten, symmetrischen Verfahren. Anschließend wird dieser Sitzungs-Schlüssel mit dem öffentlichen Schlüssel des Empfängers codiert und zusammen mit der verschlüsselten Nachricht in eine Datei geschrieben. Der Empfänger kann nun mit Hilfe seines privaten Schlüssels den zufällig gewählten Schlüssel wieder entziffern und die gesamte Nachricht damit lesbar machen.
Also bildlich: Der Absender verpackt die Nachricht in einen (frisch erzeugten) Safe mit zufällig gewähltem Schlüssel. Diesen Schlüssel steckt er in den Briefkasten des Empfängers und schickt beides auf die Reise. Der Empfänger öffnet den Briefkasten, nimmt den Schlüssel zum Safe heraus und öffnet den Safe.
Signatur:
Weiterhin bieten einige asymmetrische Verfahren die Möglichkeit, eine Nachricht zu "unterschreiben" ("digitale Unterschrift"). Hierzu kann der Absender einer Nachricht diese mit seinem privaten Signaturschlüssel codieren, und jeder Empfänger kann die Echtheit des Absenders mit dessen öffentlichem Signaturschlüssel prüfen. Gelingt dies, so ist die Nachricht mit dem privaten Schlüssel codiert, also unterschrieben worden.
Verschlüsselung und digitale Unterschrift können natürlich miteinander kombiniert werden, um Briefgeheimnis und Authentizität des Absenders zu gewährleisten: Die Nachricht wird zunächst mit dem eigenen privaten Signaturschlüssel signiert und diese unterschriebene Nachricht anschließend mit dem öffentlichen Schlüssel der Empfängerin codiert. Diese decodiert die Nachricht zunächst mit ihrem privaten Schlüssel und prüft anschließend mit dem öffentlichen Signaturschlüssel des Absenders die Unterschrift. PGP erledigt die einzelnen Schritte automatisch, ohne daß Sie sich um die Einzelheiten kümmern müssen.
siehe hierzu auch: http://www.foebud.org/pgp/

Nach Aufruf der Installationsroutine wird man zunächst gefragt, ob man bereits digitale Schlüssel besitzt oder nicht. Es folgt die Pfadangabe des Installationsverzeichnisses und eine Auswahl der zu installierenden Komponenten.
Nun lassen sich die PGP-Programmkomponenten über den Start-Button oder direkt im Explorer über die Dateieigenschaften starten und anwenden. Mittels Klick mit der rechten Maustaste auf ein Laufwerk, einem Ordner oder einer Datei kann man die entsprechenden Optionen (**Encrypt, Sign, Encrypt & Sign, Wipe und Create SDA**) wählen. Die ersten drei Optionen sind selbsterklärend (verschlüsseln, signieren, verschlüsseln & signieren).
Mit Wipe können Dateien restlos von der Festplatte gelöscht werden. Dabei wird der Speicherbereich auch einstellbar oft überschrieben, so daß der ursprüngliche Inhalt nicht mehr rekonstruierbar ist. Ein SDA stellt ein selbstentschlüsselndes Archiv dar, daß mit einem konventionellen Code verschlüsselt wird und nach Versendung nur unter Angabe des Schlüssels wieder zu dechiffrieren ist.

6. Umgehung von Paßwörter

Es besteht immer noch die Möglichkeit einen PC von Diskette oder CD zu starten, ohne auf das, auf der Festplatte installierte Betriebssystem (DOS, Windows, Unix, Linux, MacOs, ...), zugreifen zu müssen. So ermöglicht z.B. eine Diskette mit DOS und dem kleinen Zusatz NTFSDOS auch Zugriff auf NTFS-Partitionen, die sonst nur mit Windows erreichbar sind.

Empfehlenswert ist es daher, im **BIOS** (Basic Input Output System) des PC's, daß meißt über die gedrückte Taste „*Entf*" oder „*Del*" beim booten (s. Bildschirm), zu erreichen ist, die Bootreihenfolge dahin gehend abzuändern, daß der PC nur noch über die Festplatte gebootet werden kann (Sicherheit des Betriebssystems). Vergibt man nun noch ein BIOS-Passwort, kann der PC nur noch nach Eingabe dieses Passwortes und Abänderung der Parameter, von einem anderen Laufwerk gestartet werden. Die Option „*boot from other device*" sollte dann ebenso deaktiviert werden.

7. Grundlagen zum möglichst sicheren Umgang mit Passwörtern und Systemen

- Sicherheitsmechanismen sorgfältig auswählen
  (Verwaltungs-, Verschlüsselungstools)

- Ausschließlich sichere Passwörter einsetzen
  (min. 10 Zeichen inkl., Zahlen u. Sonderzeichen, s. Kapitel 3.3, 3.4)

- Voreingestellte oder leere Passwörter sind sofort zu ändern
  (neu eingerichteter Account, neu installierte Software ...)

- PC beim Verlassen immer sperren (Ctrl., Alt, Del bei Windows)

- PC regelmäßig auf Viren und Trojaner sowie mögliche Spionageprogramme untersuchen lassen, z.B. mit:
  Antivirus: AntiVir, Symantec Norton AntiVirus, Sophos, ...
  Spyware, Trojanische Pferde, Browser Hijacking, Malware, Keylogger, ...:
  SpyBot, Ad-Aware (www.bsi.de)
  Suche nach Programmen, die beim Start des Computers aktiviert werden:
  HijackThis (www.bsi.de)

- Regelmäßige Aktualisierung der obigen Programme oder deren Definitionsdateien, um auch neue Schädlinge aufspüren zu können.

- Sensitive Daten (Passwörter) und Systeme speziell schützen (verschlüsseln), oder gar nicht speichern.
  (Einstellung der Windows Zugriffsberechtigungen, Verschlüsselung, Geheimhaltung)

- Keine kabellosen Tastaturen verwenden, die unverschlüsselt senden, jeder Tastendruck könnte ausgespäht werden! Funkwellen dringen auch durch Wände in die Nachbarräume!

- Die gleichen Sicherheitsbedenken bestehen natürlich ebenso bei Funknetzwerken (WLAN). Siehe hierzu auch z.B.: http://www.hadels.com/wlan/wardriving.html

- Passwörter immer nur einmal verwenden.

8. Literaturhinweise

http://www.cert.dfn.de/infoserv/dib/dib-9501.html
http://www.taubenschlag.uni-frankfurt.de/passwortsicherheit.html
http://www.microsoft.com/germany/ms/solutioncenter/infobrief/april02/passwort.htm
http://www.metaner.de/1pw/brute-force.html
http://www.1pw.de/
http://www.rpgcommunity.de/clanwissen/php_i_md5_mehr_sicherheit.php
http://www.rpgcommunity.de/clanwissen/p_g_pass_sicherheit.php?was=pw
http://www.electronic-security.de/archiv/hacking/bios/bios-passwoerter/#4.2
http://www.lugg.de/~lugg111/publications/vhs-kurs/passwd/passwd.htm
http://helpdesk.rus.uni-stuttgart.de/~rustomfi/Passwort-Cracker/
http://home.eunet.no/~pnordahl/ntpasswd/
http://cert.uni-stuttgart.de/
www.bsi.de IT-Grundschutz Leitfaden

Downloads:

BSI:
http://www.bsi.bund.de/av/hijack/browserhj.htm

AmP:
www.zdnet.de/downloads/prg/d/u/deZ3DU-wc.html

1PW:
http://www.1pw.de/

CryptTool:
http://www.cryptool.de/

Password Depot:
http://www.password-depot.com/

Opera:
http://www.opera.com/

Netscape:
http://www.netscape.de/

Mozilla:
http://www.mozilla-europe.org/de/

Gelsenkirchen, 15.10.04 O. Gießelmann, Dipl.- Ing. (FH)