Contents

1 Standard Frage

1. Wo mit Beschäftigt sich IT-Sicherheit(Definition)?
IT-Sicherheit beschäftigt sich mit der Vorbeugung, dem Erkennen und der Reaktion auf Ereignisse, die die Integrität der Daten, die Nutzbarkeit der Systeme und die (digitale) Privatsphäre gefährden.

2. Vor welchen drei Gefährdungen müssen Rechner- und Netzwehrkomponenten geschützt werden?

- Spionage
- Sabotage
- Missbrauch

3. Nennen Sie die in der Vorlesung genannten drei Schutzziele für Rechner- und Netzkomponenten.

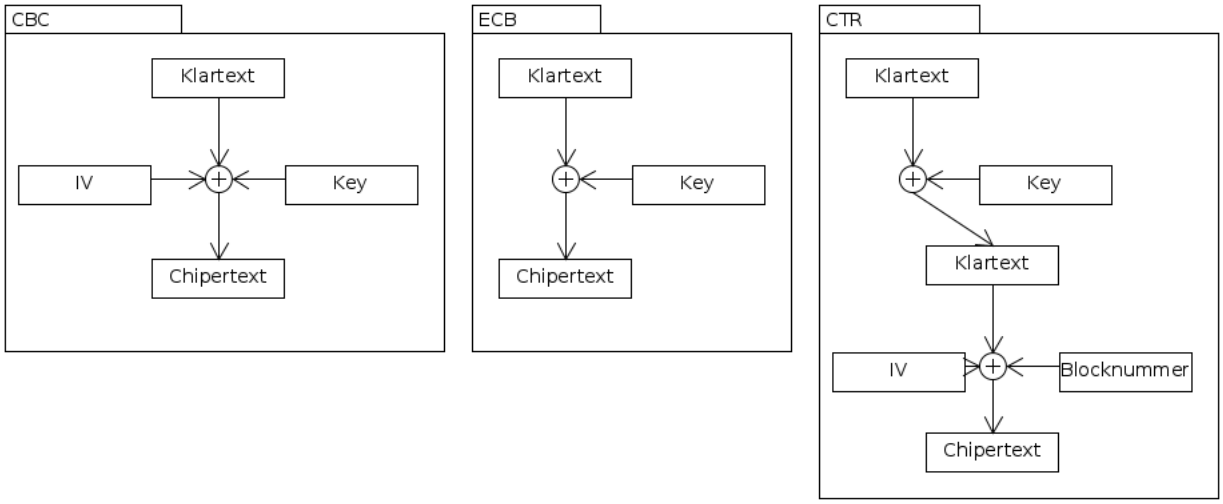
- Vertraulichkeit
- Integrität
- Verfügbarkeit

2 Eigener Verschlüsslungs Algo.

12 Stellige Passwörter werden nach dem Muster abuvcdwxefyz gebildet. Wobei uvwxyz der Passwort Kern &asz6K ist. und ab die ersten beiden Buchstaben der url entsprechen. cd den dritten und vierten Buchstaben welche um ROT+1 verschoben sind. Und schlussendlich ef die letzten beiden Buchstaben welche um ROT-1 verschoben sind. URLs Kürzer als 6 zeichen werden einfach wiederholt.

www.heise.de => heiseh
abuvcdwxefyz
he&ajtszdg6K

3 CBC ECB CTR



4 Anhang

XOR	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

ASCI Tabelle

1. Num Lock einschalten
2. ALT + ASCI Zahl

Beispiel: ALT+64 = @

ASCI	Zeichen	ASCI	Zeichen	ASCI	Zeichen	ASCI	Zeichen	ASCI	Zeichen	ASCI	Zeichen
000	(Null)	046	.	92	\	138	è	184	©	230	µ
001	☺	047	/	93	]	139	ï	185	╣	231	þ
002	☻	048	0	94	^	140	î	186	║	232	Þ
003	♥	049	1	95	_	141	ì	187	╗	233	Ú
004	♦	050	2	96	`	142	Ä	188	╝	234	Û
005	♣	051	3	97	a	143	å	189	¢	235	Ù
006	♠	052	4	98	b	144	É	190	¥	236	ý
007	•	053	5	99	c	145	æ	191	┐	237	Ý
008	◘	054	6	100	d	146	Æ	192	└	238	¯
009	○	055	7	101	e	147	ô	193	┴	239	´
010	◙	056	8	102	f	148	ö	194	┬	240	-
011	♂	057	9	103	g	149	ò	195	├	241	±
012	♀	058	:	104	h	150	û	196	─	242	‗
013	♪	059	;	105	i	151	ù	197	┼	243	¾
014	♫	060	<	106	j	152	ÿ	198	ã	244	¶
015	☼	061	=	107	k	153	Ö	199	Ã	245	§
016	►	062	>	108	l	154	Ü	200	╚	246	÷
017	◄	063	?	109	m	155	ø	201	╔	247	¸
018	↕	064	@	110	n	156	£	202	╩	248	°
019	‼	065	A	111	o	157	Ø	203	╦	249	¨
020	¶	066	B	112	p	158	×	204	╠	250	·
021	§	067	C	113	q	159	ƒ	205	═	251	¹
022	▬	068	D	114	r	160	á	206	╬	252	³
023	↨	069	E	115	s	161	í	207	¤	253	²
024	↑	070	F	116	t	162	ó	208	ð	254	■
025	↓	071	G	117	u	163	ú	209	Ð	255	(leer)
026	→	072	H	118	v	164	ñ	210	Ê		
027	←	073	I	119	w	165	Ñ	211	Ë		
028	∟	074	J	120	x	166	ª	212	È		
029	↔	075	K	121	y	167	º	213	ı		
030	▲	076	L	122	z	168	¿	214	Í		
031	▼	077	M	123	{	169	®	215	Î		
032	(Leerstelle)	078	N	124	|	170	¬	216	Ï		
033	!	079	O	125	}	171	½	217	┘		
034	"	080	P	126	~	172	¼	218	┌		
035	#	081	Q	127	⌂	173	¡	219	█		
036	$	82	R	128	Ç	174	«	220	▄		
037	%	83	S	129	ü	175	»	221	¦		
038	&	84	T	130	é	176	░	222	Ì		
039		85	U	131	â	177	▒	223	▀		
040	(	86	V	132	ä	178	▓	224	Ó		
041	)	87	W	133	à	179	│	225	ß		
042	*	88	X	134	å	180	┤	226	Ô		
043	+	89	Y	135	ç	181	Á	227	Ò		
044	,	90	Z	136	ê	182	Â	228	õ		
045	"-"	91	[	137	ë	183	À	229	Õ		

1 IP Tables

1.1 Initialisieren

```
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

1.2 NAT (Port Forwarding)

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 443 -j DNAT --to 192.168.0.x:443

-t = Tabelle
-A = Füge Regel zu ausgewählter Kette hinzu
PREROUTING: Bearbeiten der Pakete sobald sie reinkommen
POSTROUTING: Pakete erst bearbeiten, sobald sie rausgehen
-o = out-interface
-i = in-interface
-p = Protkoll
--dport = Destination Port
--sport = Source Port
eth0 = In diesem Fall Interface zum Internet
eth1 = In diesem Fall Interface ins Interne Netz
-j = Auszuführende Regel

1.3 Beispiel Forwarding Regel

iptables -A FORWARD -p tcp -i eth0 -d 192.168.101.x --dport 443 -j ACCEPT

iptables -A FORWARD -p tcp -o eth0 -s 192.168.101.x --sport 443 -j ACCEPT

-d = destination IP
-s = source IP

1.4 Beispiel Nur hergestellte Verbindung

iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT

-m = match
--state = der zu vergleichende Status

1.5 Beispiel DHCP-Server

iptables -A INPUT -i eth1 -p udp --dport 67 --sport 68 -j ACCEPT

iptables -A OUTPUT -o eth1 -p udp --dport 68 --sport 67 -j ACCEPT

--dport = destination Port
--sport = source Port

2 Funktionen & Bedenklichkeiten

Bedenklich	Attacke	Verbesserung
char *gets(char *str); gets(song)	Buffer Overflow	char *fgets(char *str, int num, FILE *stream); fgets(song, sizeof(song), stdin)
int sprintf(char *str, const char *fomat, …); int sprintf(command, „get %s.mp3“, song);	Buffer Overflow	int snprintf(char *s, size_t n, const char * format, …); int snprintf(command, sozeof(command), „get%s.mp3“, song); command[sizeof(command)-1]=‘\0‘;
size_t strlen(const char *s); len = strlen(str);	Buffer Overflow	size_t strnlen(const char *s, size_t maxlen); len = strnlen_s(str, sizeof str);

char * strcpy (char * destination, const char * source);
`strcpy (str2,str1);`
	Buffer Overflow	size_t strlcpy(char *destination, const char *source, size_t size); ODER
		char * strncpy(char *destination, const char *source, size_t size);
		strncpy (str2, str1, sizeof(str2));
		len = strlcpy(str2, str1, sizeof(str2));

char *strcat(char *destination, const char *source) strcat(to, from)	Command Injection	size_t strlcat(char *dst, const char *src, size_t size); strlcat(to, from, sizeof(to));
gets(input); [anz. in n= „%s%n\n“,buf,&n] printf(input);	Formatstring-Attacke	Herausfiltern der Zeichen. Erkennung → %n (anzahl Zeichen) [input = „%s%n\n“,buf,&n]
filename= mktemp(template); fd = open(filename, O_RDWR);	Race Condition	Zwischen dem erzeugen und dem Öffnen der Datei existiert eine Race Condition, da die Datei in der Zwischenzeit der beiden Aufrufe geändert worden sein könnte

3 Sonstige Bedenklichkeiten

- Kein Salz
- least privilege
- Rückgabewerte von Funktionen nicht ausgewertet
- sscanf oder ähnliches
- Signale nicht abgefangen
- Schutz vor Swapping fehlt
- Challenge kein Zufallswert