SAVE

ein Paßwort in Form und Farbe

Helmut Schluderbacher DSK-515:\SAVE

INHALTSANGABE

SAVE (Symbol Active Verified Entry) ist eine Zutrittskontrolle zu einem Computer mit rein graphischen Elementen bzw. Codewörten.

Eine große Vielfalt an „Paßwörtern“ macht ein Zutrittskontrollsystem erst wirklich sicher. Der Benutzer selbst muß aber die Übersicht behalten können und mit einer schnellen Eingabe bzw. einem kurzen Erkennungswort Zutritt erhalten.

Einer der Ausgangspunkte der Entwicklung von **SAVE** war die Idee, daß der Benutzer die Möglichkeit hat, sein Paßwort einzugeben, ohne daß Zuseher die Gelegenheit haben, mit ihren Beobachtungen in den Besitz des Zutrittscodes zu kommen.

Ein anderer Aspekt waren die sogenannten vorgetäuschten Loginprogramme. Ein Benutzer muß praktisch immer sein Paßwort einem Programm anvertrauen, von welchem er im Vorhinein nicht weiß, ob es das richtige ist. Eine gute Zutrittskontrolle gibt ihm aber die Gelegenheit dazu (**Partnerkontrolle**).

Ein Hacker, der Paßwörter von der Leitung abhört, wird mit den erlauschten SAVE-Eingabewörtern keine Freude haben, da diese nur für diesen einen Zutritt gültig sind.

Die Realisierung und der Einsatz einer Zutrittskontrolle sollte ohne spezielle Hardware oder sonstige spezielle Eignung der Benutzer möglich und vor allem personenunabhängig sein. Es sollte also möglich sein, den Zutrittscode im Notfall auf eine andere Person zu übertragen.

Bei **SAVE** ist dies alles realisiert. Seit mehr als zwei Jahren ist eine Demonstrationsversion problemlos im Einsatz. In dieser Zeit haben die Anwender gute Erfahrungen damit gemacht.

Eine weitere Eigenschaft von **SAVE**, die ständig wechselnden Eingabewörter, bieten vor allem in großen, nicht abhörsicheren Netzen einen entscheidenten Vorteil gegenüber den herkömmlichen Paßwörtern.

Zudem ist es das erste wirklich graphische Zutrittskontrollsystem und eignet sich in hervorragender Weise für die jetzt in Verwendung befindlichen graphischen Benutzeroberflächen.

Diese Überlegungen dienen als Ausgangspunkt für den Entwurf von **SAVE** (Symbol Active Verified Entry) der in Kapitel 1 beschrieben ist. In Kapitel 2 werden die verschiedenen Sicherheitsaspekte von **SAVE** beleuchten und mit Bankomatcode und Paßwort verglichen. Daran anschließend folgt mit Kapitel 3 die Beschreibung der Demonstrationsprogramme und mit Kapitel 4 die Zusammenfassung.

DER SYSTEMAUFBAU

DIE SYMBOLE

Der Grundstock des Systems sind die Symbole. Sie sollten schnell erfaßbar sein und sich leicht voneinander unterscheiden lassen. Die **Symbole (S)** entstehen aus **Farben (C)** und **Formen (F)**. Jede Form tritt in jeder Farbe auf.

Die Farben müssen sich, ebenso wie die Formen, klar voneinander unterscheiden. Ähnliche Farben oder einander gleichende Formen vermindern die Erfassungszeit und auch die bei manchen Menschen vorhandene Farbfehlsichtigkeit muß berücksichtigt werden.

Die Symbole selbst haben keine Wertigkeit. Das bedeutet, daß die Reihenfolge der Symbole keine Bedeutung hat. Wichtig ist nur ihr Erscheinen.

DAS FENSTER

Die Symbole werden in einem **Fenster (W)** im Quadrat angeordnet. Es erscheinen somit genau vier Symbole gleichzeitig in einem Fenster.
Dem Anwender werden eine bestimmte Anzahl von Symbolen zugeordnet . Diese Symbole, die **richtigen (r)** Symbole (graphisch = ■), muß er sich merken. Neben diesen erscheinen im Fenster auch **falsche (f)** Symbole (graphisch = ○). Jedes Symbol kann höchstens einmal in einem Fenster auftreten.

Daraus ergeben sich folgende Möglichkeiten in einem Fenster:

1) Es erscheint kein richtiges Symbol oder alle richtigen.
2) Es erscheint genau ein richtiges Symbol.

Zusammen sind dies sechs Alternativen (***Abbildung 1.2.1***).

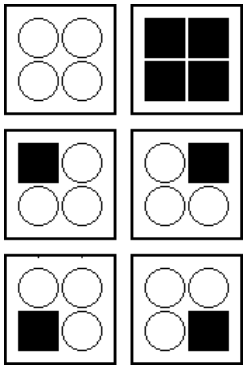

Abbildung 1.2.1

Bei zwei richtigen Symbolen gibt es noch sechs weitere Möglichkeiten (***Abbildung 1.2.2***).

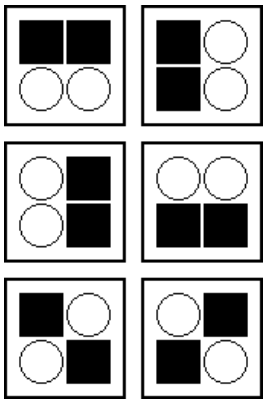

Abbildung 1.2.2

Sind somit 12 Möglichkeiten. Schließlich gibt es bei drei richtigen Symbolen vier weitere Möglichkeiten (***Abbildung 1.2.3***).

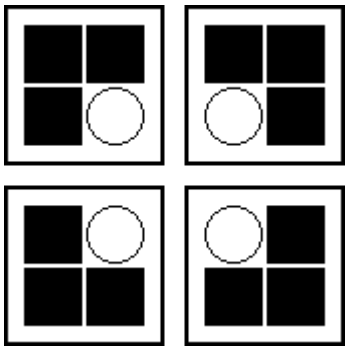

Abbildung 1.2.3

DAS EINGABEZEICHEN

Ein Fenster bietet also 16 Möglichkeiten bei vier Symbolen. Der Anwender muß jetzt die Möglichkeit erhalten, dem System seine richtig erkannten Symbole mitteilen. Dazu wird am Rand des Fensters ein Rahmen mit **Eingabezeichen** angebracht, welche sich auf die **Tasten (Tn)** (n=1,...,8) beziehen, die der Anwender drücken soll. Die Anordnung der Eingabezeichen auf dem Rahmen, soll es für den Anwender vereinfachen, den Zusammenhang zwischen den Symbolen und dem Eingabezeichen herzustellen (***Abbildung 1.3.1***).

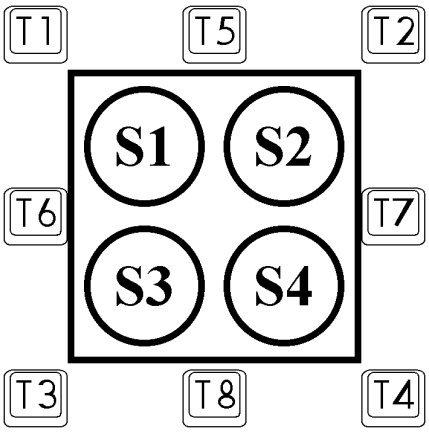

Abbildung 1.3.1

Jedes Eingabezeichen entspricht genau einer Taste auf der Tastatur, wobei gilt: Ti≠Tj für alle i≠j. Die Eingabezeichen beschränken sich auf die alphanumerischen Standardzeichen A bis Z plus Ê (Leerstelle), da diese Zeichen auf allen herkömmlichen Tastaturen vorhanden sind. Durch diese Einschränkung reduziert sich das **Eingabealphabeth** auf diese 27 Zeichen.

Erscheinen nur falsche Symbole im Fenster so drückt der Anwender den Ê. Erscheint genau ein richtiges Symbol im Fenster, so wird genau die Taste T1,...,T4 gedrückt, deren Zeichen sich in genau der Ecke des Fensters am Rahmen befindet. Ist zum Beispiel S1 das richtige Symbol, dann muß die Taste T1 gedrückt werden (siehe ***Abbildungen 1.3.2***). Analoges gilt für die Symbole S2 bis S4.

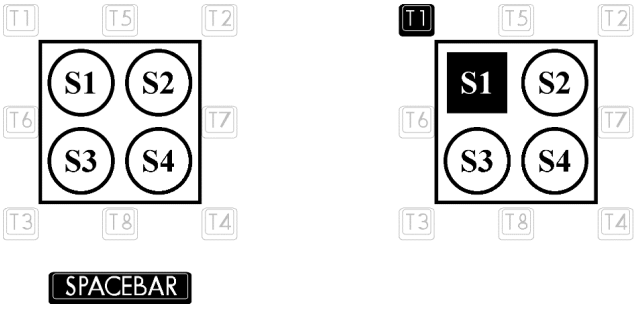

Abbildung 1.3.2

Für zwei richtige Symbole neben oder übereinander am Fensterrand, wird eine der Tasten T5,...,T8 am Rahmen zwischen den beiden Symbolen eingegeben. Sind zum Beispiel S1 & S2 die richtigen Symbole, dann muß die Taste T5 gedrückt werden (siehe ***Abbildung 1.3.3***). Analoges gilt für die Symbole S2 & S4 und S3 & S4 bzw. Tasten T6 bis T8.

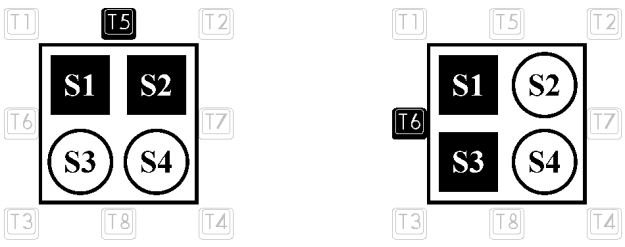

Abbildung 1.3.3

Für den Fall, daß die beiden Symbole diagonal im Fenster stehen, werden die zwei Tasten L & R reserviert (***Abbildung 1.3.4***). L bedeutet, daß die Symbole S4 & S1 richtig sind (**nach Links** von unten nach oben). R bedeutet, daß die Symbole S3 & S2 richtig sind (**nach Rechts**).

Für alle Möglichkeiten von drei oder vier richtigen Symbolen im Fenster ist wieder Ê vorgesehen (***Abbildung 1.3.5***). Analog gilt für die Symbole S1 & S2 & S4, S1 & S3 & S4, S2 & S3 & S4 und S1 & S2 & S3 & S4.

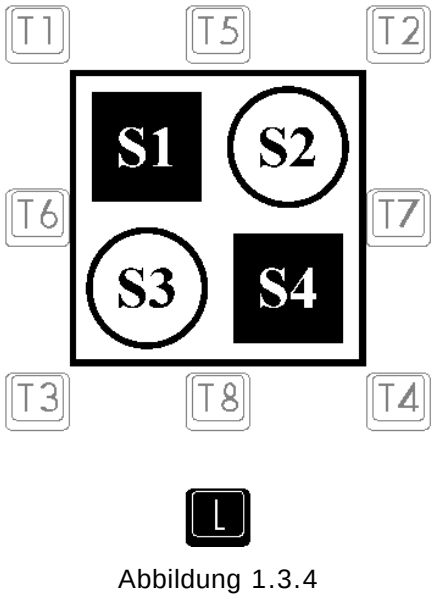

Abbildung 1.3.4

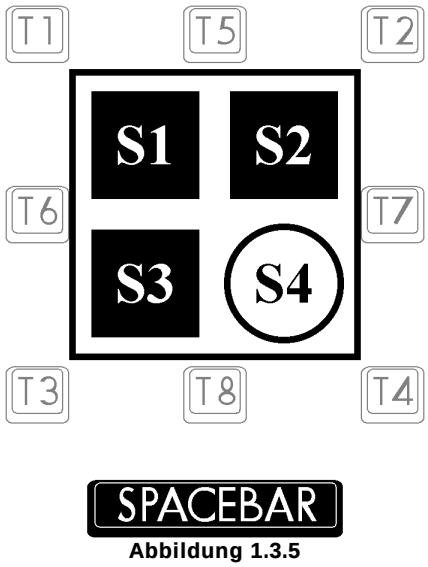

Abbildung 1.3.5

Der Anwender kann jetzt versorgt mit seinen richtigen Symbolen, auf Aufforderung des Systems dem System mit Hilfe des Eingabezeichens mitteilen, welche er als die richtigen Symbole erkennt.

DIE FENSTERMASKE

Dem Fenster, wir werden es von nun an **Anwenderfenster** nennen, werden noch einige andere Fenster hinzugefügt, wobei **(h)** die Anzahl der Fenster in der **Höhe** und **(b)** die Anzahl der Fenster in der **Breite** ist. Dabei gibt der kleinste Bildschirm im System die Gesamtanzahl der Fenster vor. Die hinzugefügten Fenster sind vom Anwenderfenster völlig unabhängig, obwohl sie möglicherweise die gleichen Symbole zeigen.

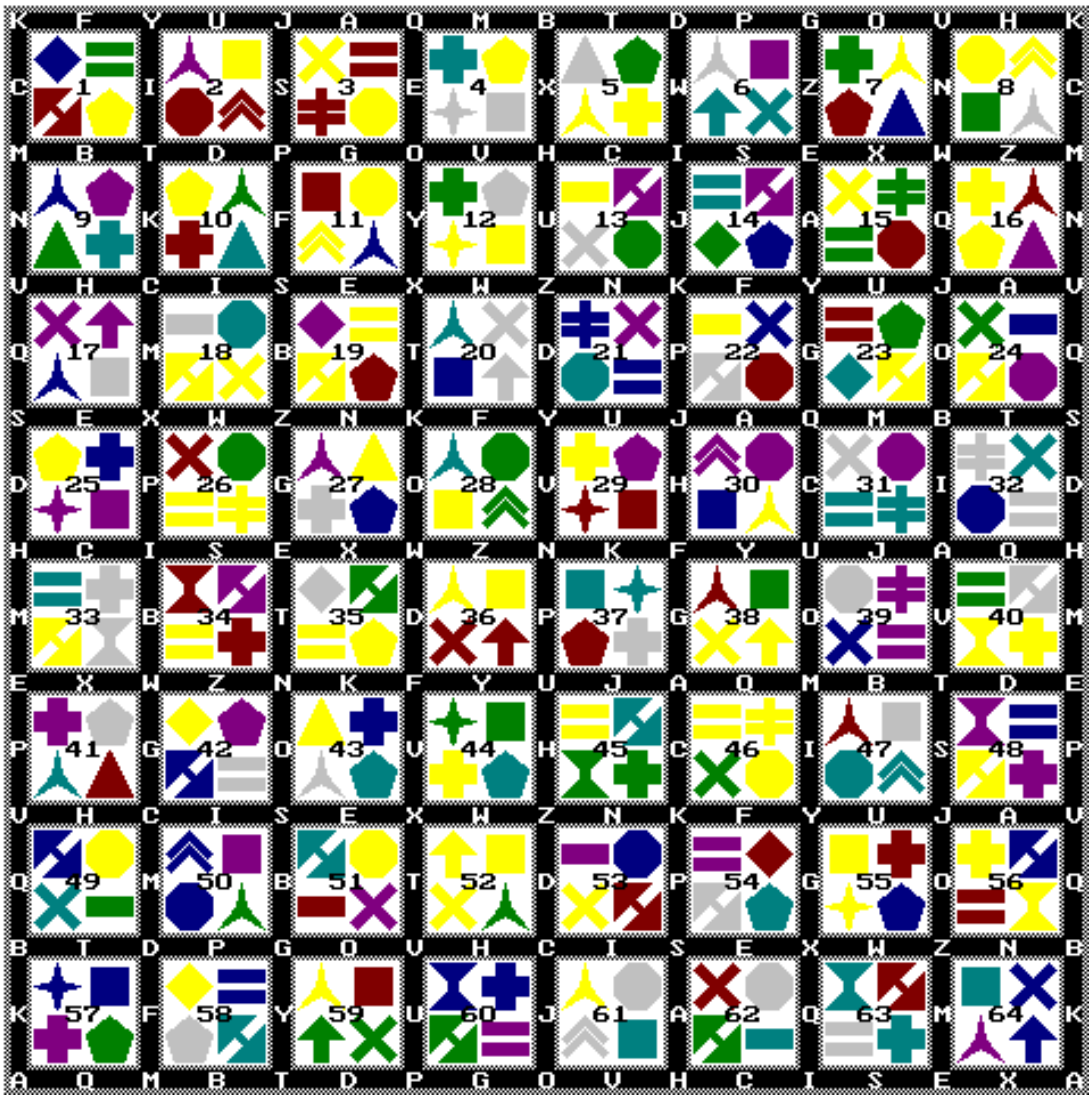

Abbildung 1.4.1

Die Fenster werden sehr dicht angeordnet, daher haben zwei Fenster, die mit den Kanten aneinander stoßen, drei Zeichen gemeinsam. Fenster, welche sich mit den Ecken berühren besitzen dort ein gemeinsames Zeichen. Zeichen welche auf der Position T1,...,T4 auftreten sind immer vier Fenstern zu zuordnen, Zeichen auf der Position T5,...,T8 zwei. Ausgenommen davon sind die Fenster am Rand oder in den Ecken der Fenstermaske.

Die Fenster werden von links nach rechts und von oben nach unten mit aufsteigenden Nummern durchnumeriert, indem die **Fensternummer (Wn)** in die Mitte der vier Symbole gesetzt wird. Die Abbildung 1.4.1 zeigt ein Beispiel für eine Fenstermaske mit b=8 und h=8 inklusive der Fensternummern.

Der Anwender muß also, zusätzlich zu seinen richtigen Symbolen, auch die Fensternummer, wo seine Symbole erscheinen, kennen. Für den Anwender sind seine richtigen Symbole und die Fensternummer sein **Symbolcode**.

Die Fensternummer steht nicht nur für ein Anwenderfenster in einer Fenstermaske von h∗b Fenstern, sondern es ist ein Punkt auf dem Bildschirm auf welchen man blickt.

DAS SYMBOLSET

Die richtigen Symbole müssen immer wieder im Anwenderfenster erscheinen. Deshalb werden nun zu den richtigen Symbolen bestimmte fix vorgegebene falsche hinzu gefügt, welche so wie die richtigen immer gemeinsam mit diesen im Fenster erscheinen. Diese Zusammenstellung heißt das **Anwender-Symbolset**.

Der Anwender muß sich nur die richtigen merken. Das komplette Anwender-Symbolset erstellt das System. Die Symbole im Anwender-Symbolset sind entweder richtig oder falsch. Die Anzahl **(s)** der Symbole im Anwender-Symbolset ist gleich der Summe von **r+f**. Alle Symbole außerhalb des Anwenderfensters werden als **unbekannt (u)** bezeichnet.

Der Anwender sieht beim wiederholten Benutzen immer wieder dasselbe Symbolset und kann somit nach einer gewissen Zeit die Symbole seines Anwender-Symbolsets von anderen Symbolen unterscheiden. Ein großes Problem für Trojan-Horse-Programme (TH-Programme) da sie einem Anwender meist nur unbekannte Symbole liefern können, welche der Anwender als ihm unbekannte Symbole erkennt. Der Anwender kann daher seinen Eingabecode nicht verraten. Denn wenn es den Symbolcode nicht kennt, kann es dem Anwender nicht das richtige Symbolset liefern.

Damit nicht nur das Anwenderfenster immer das gleiche Symbolset liefert werden auch die anderen Fenster mit je einem Symbolset versorgt.

DIE KLASSENEINTEILUNG

Wenn aus einer Menge von Symbolen immer zufällig welche auswählt werden, so ist es wahrscheinlicher, daß nur ein richtiges Symbol im Fenster erscheint, als zwei zugleich. Daraus folgt, daß die Tasten T1 bis T4 weitaus häufiger gedrückt werden als die übrigen Tasten, von Ê einmal abgesehen. Diese Problematik wird immer größer, je kleiner die Anzahl der richtigen Symbole wird, selbst wenn das Verhältnis von falschen Symbolen zu richtigen Symbolen gleich bleibt.

Mit einer speziellen Klasseneinteilung der Symbole kann diesem Problem aber entgegengesteuert werden. Diese Maßnahme gilt für alle anderen Fenster und deren zugeordneten Symbolsets analog.

DIE ZEICHENMASKE

Die **Zeichenmaske** ist ein Teil der Fenstermaske und enthält alle Zeichen (Tn) die der Anwender gegebenenfalls zu drücken hat, mit Ausnahme von L, R & Ê. Es werden zwei Gruppen gebildet. Die erste Gruppe enthält A bis Z ohne L & R. Die zweite Gruppe wird gebildet von L, R & Ê.

L steht für die richtigen Symbole S1 & S4 (*nach Links*), R steht für die richtigen Symbole S2 & S3 (*nach Rechts*) und Ê steht für *kein richtiges Symbol* oder *mehr als zwei richtige Symbole*. Die Zeichen der ersten Gruppe werden ständig, Fenstermaske für Fenstermaske variiert, damit sich nach der Eingabe die Position des eingegebenen Zeichens nicht nachvollziehen läßt.

Da es wesentlich wahrscheinlicher ist, daß ein Zeichen auf den Positionen T1 bis T4 gedrückt werden soll, als ein Zeichen auf T5 bis T8,

Wahrscheinlichkeit des Auftretens[2]	KURZ-LOGIN	NORMAL-LOGIN
von keinem richtigen Symbol	**(n = 6)**	**(n = 8)**
zweimal in einer Session:	32,03%	23,04%
dreimal in einer Session:	26,10%	28,15%
von einem richtigen Symbol		
zweimal in einer Session:	32,07%	23,14%
dreimal in einer Session:	26,02%	28,15%
von zwei richtigen Symbolen		
einmal in einer Session:	36,30%	27,78%
zweimal in einer Session:	29,03%	31,11%
mindestens einmal in einer Session:	81,09%	89,15%

Tabelle 2.1

SICHERHEIT	SAVE	BANKOMATCODE	PASSWÖRTER
Optische Sicherheit: (Sicherheit gegen Zuseher)	**Sehr gut** durch Unabhängigkeit des Eingabecodes vom Symbolcode	**Sehr schlecht** Zuseher in der Warteschlange könnten Zutrittscode erkennen	**Schlecht** Zuseher könnten Zutrittscode erkennen
Trojan-Horse-Sicherheit: (Sicherheit gegen Täuschungsprogramme)	**Sehr gut** durch Erkennen des richtigen Symbolsets	**Gut** durch Bankomatkasse	**Sehr schlecht** Nachahmungen sind leicht möglich
Logische-Sicherheit: (Verbindung Mensch-Zutrittscode)	**Sehr gut** durch Vergabe des Symbolcodes	**Sehr gut** durch Vergabe des Bankomatcodes	**Sehr schlecht** Anwender wählt Zutrittscode
Zutrittscode-Sicherheit: (Sicherheit gegen unbefugte Benutzer)	**Sehr gut** durch ausreichenden Symbolcode und Random-Modus	**Sehr gut** nach drei Versuchen wird abgebrochen	**Sehr gut** Theorie: 26^t **Sehr schlecht** In der Praxis

Tabelle 2.2

müssen Zeichen, welche auf T1,...,T4 erscheinen, zum Ausgleich auch auf T5,...,T8 bei einem anderen Fenster aufscheinen.

DER LOGINNAME

Nach der Eingabe der Identifikation liefert das System die richtige Fenstermaske. Diese Identifikation wird als **Loginnamen** bezeichnen. Erst durch diesen Loginnamen wird dem Anwender sein Symbolset in sein Fenster geliefert. Jedem Loginnamen darf zu jedem Zeitpunkt nur genau ein Anwender-Symbolset zugeordnet werden.

DIE SESSION

Ein Zeichen aus dem Eingabealphabeth beantwortet eine Fenstermaske. Erst eine wiederholte Ausführung verschiedener Fenstermasken bringt die erwartete Sicherheit. Die Folge der Eingabezeichen ergibt den **Eingabecode**. An Hand des Eingabecodes überprüft das System die Rechtmäßigkeit des Zutrittversuches. Der Eingabecode ist richtig, wenn alle Eingabezeichen richtig sind.

Jede Fenstermaske wird völlig unabhängig von den anderen erstellt. Eine Eingabe eines Loginnamens plus eine komplette Fenstermaskenfolge heißt **Session**. Die Auswahl der Symbole für die Fenstermaske erfolgt durch ein Zufallsverfahren.

Wieviele Fenstermasken **(n)** eine Session enthält ist sicherheitsabhängig und daher nicht vorgegeben. Die Beantwortung aller Fenstermasken beendet die Session. Eine Session ist also die Eingabe eines Loginnamens, der Durchlauf aller für diese Session vorgesehenen Fenstermasken und die Beantwortung dieser.

Für jeden beliebigen Loginnamen gibt es ein eindeutiges Symbolset. Wenn ein ungültiger Loginnamen eingegeben wird, liefert das System wie erwartet eine Fenstermaskenfolge. Diese Fenstermaskenfolge unterscheidet sich von anderen nur dadurch, daß kein gültiger Eingabecode existiert.

Damit ist das **SAVE-**Zutrittskontrollsystem in seiner Grundstruktur komplett. Jetzt werden wir noch eine Sicherheitsverbesserung, den Random-Modus, besprechen.

DER RANDOM-MODUS

Der **Random-Modus** unterscheidet sich vom **Normal-Modus** durch einen Zufallsgenerator welcher entscheidet, ob der nächste Eingabecode überhaupt überprüft wird. Wird der Eingabecode nicht überprüft, so wird der Anwender in jedem Fall abgewiesen. Es wird also noch vor der Ausgabe der Fenstermasken ermittelt, ob die eingegeben Zeichen einer Wertung unterzogen werden oder nicht.

Im Normal-Modus erfolgt die Überprüfung des Eingabecodes nach dem letzten Eingabezeichen. Sollte der Eingabecode nicht dem erwarteten Wort entsprechen, wird erneut eine Aufforderung zur Identifikation gestartet. Nach einer bestimmten Anzahl aufeinanderfolgender falscher Beantwortungen wird in den Random-Modus geschaltet.

Dies führt dazu, daß ein unbefugter Benutzer, möchte er einen Symbolcode auf seine Richtigkeit testen, eine wesentlich höhere Anzahl von Durchläufen benötigt, um die Fehlerwahrscheinlichkeit des getesteten Symbolcodes unter eine bestimmte prozentuelle Schranke zu drücken.

ZAHLEN UND VERGLEICHE

Die Möglichkeit, daß bei **SAVE** kein Symbol während einer Session in den Fenstern erscheint wird ausgeschlossen. In diesem Fall wird eine neue Auswahl getroffen.

In den nachfolgenden Tabellen ist einerseits die Wahrscheinlichkeiten der Symbole aufgelistet, andererseits sind die Vor- und Nachteile der verschiedenen Zutrittskontrollsysteme kurz zusammengefaßt. **Denn eine Zutrittskontrolle ist nur so gut, wie das schlechteste Paßwort.**

[2] Berechnet für das Demonstartionspaket (Fenster: 8*8, 2 richtige Symbole)

DAS DEMONSTRATIONSPAKET

EIN KURZER ÜBERBLICK

Was ist die Theorie ohne die Praxis! Schon kurz nach der ersten Idee hatte ich begonnen ein Modell zu programmieren, um Fehler und Verbesserungsmöglichkeiten zu erkennen. Dieses Kapitel befaßt sich mit dieser Implementierung einer Demonstrationsversion unter MS-DOS[3]. Da dies zugleich die Bedienungsanleitung zu diesen Programmen ist, bitte ich schon jetzt um Verständnis, wenn es gewisse Überschneidungen mit den vorhergehenden Kapiteln gibt.

SAVE ist sowohl beim Hochfahren des Rechners als auch bei einer kurzen Arbeitspause als Zutrittsschutz geeignet. Der eingebaute Bildschirmschoner ermöglicht es, den Arbeitsplatz jederzeit während des Testens zu verlassen, ohne sich um den Bildschirm Sorgen zu machen. **Um einen ordnungsgemäßen Betrieb zu gewährleisten, muß das gesamte SAVE-Paket mit SAVEINST installiert werden**.

Bei den Programmen handelt es sich um:

SAVE - ein vollfunktionsfähiges Programm für die Zutrittskontrolle.

SAVECODE - ein vollfunktionsfähiges Programm für den Symbolcodewechsel.

SAVEINST - das Installationsprogramm.

Obwohl es sich um ein Demonstrationspaket handelt, gibt es keinen Superuser-Eingang. Wenn Sie also dieses Paket installiert haben und Sie vergessen die Codesymbole gibt es von meiner Seite keine Möglichkeit Ihnen zu helfen!!!. Die Demonstrationsversion wurde ausschließlich für IBM kompatible Personalcomputer (PC) und VGA-Farbbildschirme in der Darstellungsform 640*480 geschrieben. Nur Graphikkarten, welche diesen Typ unterstützen, werden ein richtiges Bild liefern. Jedoch wurde bei der Erstellung des Programms bewußt diese Form gewählt, da sie auf praktisch allen Graphikkarten problemlos angewendet werden kann.

Die Technischen Einzelheiten des Demonstrationspaketes im Detail:

Die **Farben**:	**Grün**, **Blau**, **Cyan**, **Magenta**, **Grau**, **Gelb**, **Rot** & **Orange**.
Die **Formen**:	 also 16 Formen.
Das **Symbol**:	setzt sich aus je einer Form und einer Farbe zusammen. Ergibt somit F∗C=**128** verschiedene Symbole.
Das **Symbolset**:	besteht aus **16** Symbolen davon sind **2 richtig**.
Die **Fenstermaske**:	setzt sich aus **64** Fenstern (8*8) mit ihren Rahmen zusammen.
Die **Session**:	ist die zeitliche Aufeinanderfolge von **6-8** Fenstermasken plus einer Eingangsmaske.
Der **Kurz-Login**:	**6** Fenstermasken, Ein Kurz-Login ist dreimal nach einer richtig beantworteten Session möglich.
Der **Normal-Login**:	**8** Fenstermasken.
Der **Normal-Modus**:	Ein Normal-Modus ist dreimal nach einer richtig beantworteten Session möglich. Ein richtiger Eingabecode bedeutet das Passieren des Programms.
Der **Random-Modus**:	Die Zufallswahrscheinlichkeit für eine bewertete Session liegt fix bei **25** Prozent.

Ich werde auf die einzelnen Teile des System genauer eingehen und damit auch auf die Tasten, welche gegebenenfalls zu drücken sind. Für diese Beschreibung sowie auch für das ganze Paket gilt folgendes zu beachten:

j steht für **Cursor-Left**.

Zusätzlich zum Ê wird in dieser Version b bzw. e als *kein Symbol richtig* Eingabe akzeptiert.

Alle anderen Tastensymbole sind selbsterklärend.

SAVE - SYMBOL ACTIVE VERIFIED ENTRY

Nach der Eingabe von SAVEb in der Eingabezeile von MS-DOS erscheint die Eingangsmaske von **ACTIVE VERIFIED ENTRY**, mit der Aufforderung sich zu identifizieren.

Zur Identifizierung dient in der PC-Version ein mindestens vier- und höchstens zwanzigstelliges Wort. Jedem Loginnamen ist eindeutig, in Abhängigkeit vom Zeitpunkt der Symbolcodevergabe, ein Symbolcode zugeordnet.

Gültige Zeichen für den Loginnamen sind:

A bis Z in Groß- und Kleinschreibung (Kleinbuchstaben werden zu Großbuchstaben) und die deutschen Sonderzeichen **Ä**, **ä**, **Ö**, **ö**, **Ü**, **ü**, **ß** (jedoch wird **ß** in **SS** umgewandelt).

Der Loginname wird als nicht öffentlich angesehen. Daher wird aus Sicherheitsgründen für jedes eingegebene Zeichen nur je ein ***** ausgegeben.

Mit Á wird zwischen der Anzeige der Sterne und der eingegebenen Zeichen gewechselt.

Das Löschen des letzten geschriebenen Zeichens ist mit n oder j möglich.

Mit s wird die gesamte Eingabe gelöscht.

Die Eingabe muß mit b abgeschlossen werden, außer der Loginname hat genau zwanzig Zeichen. In diesem Fall wird nach der Eingabe des letzten Zeichens sofort mit der Ausgabe des Fensterrahmens und der Fensternummern begonnen.

Sollte keine Eingabe erfolgen, wird nach kurzer Zeit, je nach Rechnertyp, der Bildschirmschutz aktiviert. Der Bildschirmschutz löscht den Bildschirm, mit Ausnahme eines kleinen Logos, um zu zeigen, daß der Monitor eingeschaltet ist. Dieses Logo wandert im ein bis zwei Minuten Zyklus über den Bildschirm. Durch Drücken einer beliebigen Taste kommt man wieder zur Eingangsmaske.

Die Eingabe des Loginnamens wird mit b abgeschlossen. Wenn **SAVE** neu installiert ist oder der Symbolcode abgelaufen ist, erscheint 5 Sekunden lang ein roter Balken mit der Aufforderung, so bald wie möglich den Symbolcode zu wechseln. Diese Information bleibt zirka fünf Sekunden auf dem Bildschirm. Während dieser Zeit wird keine Eingabe akzeptiert. Dieser Hinweis blockiert also die Arbeit nicht, aber er behindert sie und motiviert dadurch den Wechsel. Nach erfolgreichem Loginvorgang sollte so rasch wie möglich der Symbolcode gewechselt werden. In dieser Ausführung von **SAVE** ist die Gültigkeitsdauer eines Symbolcodes auf ein Jahr beschränkt.

Nun erscheint die erste Maske aber vorerst werden nur die Fensternummern in die Fenster geschrieben (***Abbildung 3.2.1***). Auf der linken Bildschirmseite, neben den Fenstermasken, werden wichtige Informationen angezeigt.

Unterhalb des Logos erscheint **Kurz-Login** oder **Normal-Login**. Bei Anzeige von Kurz-Login müssen sechs Fenstermasken beantwortet werden, ansonsten acht. Ein Kurz-Login ist solange möglich, bis nach drei falschen Eingaben in drei aufeinanderfolgenden Sessions in den Random-Modus geschaltet wird.

Direkt darunter stehen der **Empfangstext**. Der Empfangstext besteht aus zwanzig, vom Anwender bei der Symbolcodevergabe selbst gewählten, Zeichen. Sollte der Empfangstext fehlen oder falsch sein, ist sofort mit s abzubrechen. Sollten trotz richtigem Loginnamen wiederholt nicht der richtige Empfangstext erscheinen, so handelt es sich mit größter Wahrscheinlichkeit nicht um das richtige **SAVE**-Programm oder der Loginname wurde aus der Logindatei gelöscht.

[3] Ab MS-DOS 5.0

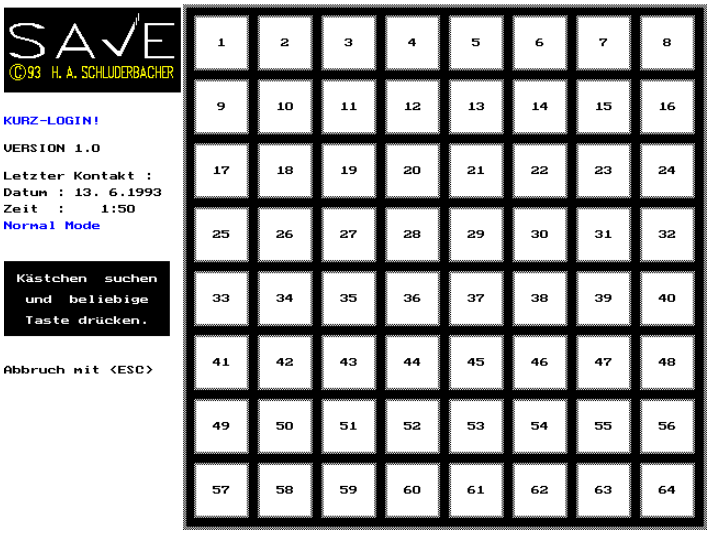

Abbildung 3.2.1

Weiters wird **Datum** und **Zeit** des letzten Zutritts oder Zutrittversuchs angezeigt. Diese Werte werden gespeichert, wenn eine komplette Session beantwortet wurde, ungeachtet dessen ob erfolgreich oder nicht.

In gleicher Farbe wie Datum und Zeit werden **Normal-Modus** oder **Random-Modus** ausgegeben. Normal-Modus bedeutet, daß jede komplette Beantwortung der Session mit richtig oder falsch bewertet wird und der Anwender dementsprechend passieren darf oder wieder zur Eingangsmaske gelangt. Im Random-Modus geschieht diese Auswertung nur mit einer Wahrscheinlichkeit von 25%. Das bedeutet, daß der Anwender möglicherweise, trotz komplett richtiger Beantwortung der Fenstermasken, nicht passieren darf.

Unter dem Informationsfeld befindet sich der Hinweis über die Möglichkeit mit S abzubrechen.

Nach Überprüfung der Informationen sucht der Anwender sein Anwenderfenster und drückt b oder eine beliebige andere Taste (ausgenommen S). Sollte keine Eingabe erfolgen, so kommt er, nach zirka ein bis zwei Minuten, wieder zur Eingangsmaske. Dies gilt auch für alle weiteren Fenstermasken. Die Ausgabe der Fenstermasken beginnt mit der Ausgabe der Symbole gefolgt von den Eingabezeichen (***Abbildung 3.2.2***).

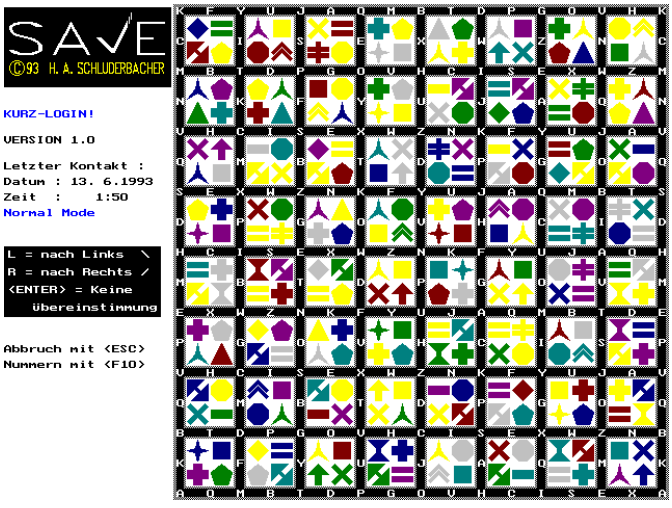

Abbildung 3.2.2

Unter dem nun erschienenen Infobalken für Links, Rechts und e befindet sich jetzt noch eine Information über ¼. Sollte der Anwender sein Fenster nicht wiederfinden, ist es möglich, mit ¼ die Nummern des Fensters zwischen die Symbole zu schreiben.

Es ist jederzeit möglich, die Fenstermasken durch Drücken von S zu verlassen. In diesem Fall werden Datum und Zeit des Loginvorgangs nicht gespeichert. Sollte also bei der Eingabe ein Fehler passiert sein, so bricht man am besten sofort mit S ab.

Die sechs bis acht Fenstermasken der kompletten Session sind vom Aufbau völlig gleich und unterscheiden sich nur durch die Anordnung der Symbole und Zeichen. Für den einzelnen Anwender ist jedoch nur sein Anwenderfenster von Bedeutung.

Der Anwender kennt mit der Zeit durch die Routine sein Symbolset, welches aus zwei richtigen und vierzehn falschen Symbolen besteht. Es ist ihm daher sofort möglich zu erkennen, ob dies auch sein Symbolset ist.

Sollte ein Anwender unbekannte Symbole im Fenster erkennen, so ist sofort mit S abzubrechen. Im Wiederholungsfall muß mit hoher Wahrscheinlichkeit mit Manipulationen, welche das Ausforschen des Symbolcodes zum Ziel haben, gerechnet werden.

Sofort nach einer Eingabe wird die Fenstermaske gelöscht, damit kein Zuseher die Gelegenheit hat von der Eingabe auf ein Fenster zuschließen. Sobald ein gültiges Zeichen A...Z, Ê, ¼ eingegeben wird, wechselt die Fenstermaske (einzige Ausnahme ¼). Sollte eine andere Taste gedrückt werden, wird ebenso wie bei S sofort abgebrochen. Dies ist notwendig, da beim Drücken der falschen Taste vielleicht die richtige Taste leicht zu erraten ist und damit die Sicherheit nicht gewährleistet wäre. Nach der letzten Fenstermaske wird der Eingabecode auf seine Richtigkeit überprüft und Datum und Zeitpunkt werden registriert. Wenn die Eingaben korrekt waren, terminiert das Programm sofort. Im Fehlerfall erscheint das Logo und man ist wieder in der Eingabemaske.

SAVECODE - SYMBOL ALTERNATIVE VALIDATE ENTRY

SAVECODE dient zum Wechseln
des **Symbolcodes**,
des **Loginnamens** und
des **Empfangstextes**.
Zur Sicherung dieses sensiblen Bereiches dient wieder **SAVE** und eine Abschaltautomatik, welche nach erfolgtem Loginvorgang, bei Nichtbedienung durch den Anwender, nach einer gewissen Zeitspanne das Programm beendet.

Das Zuteilen des Fensters und des Symbolsets ist eine Sicherheitsmaßnahme von **SAVE**. Der Anwender selbst hat, im Gegensatz zum Loginnamen und zum Empfangstext, keine Möglichkeit in diese Auswahl einzugreifen. Dadurch wird eine breite Streuung der verschiedenen Symbolcodes erreicht. Mit dem Symbolcode wird auch das Datum der Vergabe mitgespeichert, um nach Ablauf einer gewissen Frist dem Anwender das neuerliche Wechseln der Symbole zu empfehlen. In dieser Version beträgt diese Frist ein Jahr.

Nach der Eingabe von SAVECODEb erscheint eine ähnliche Eingangsmaske wie bei **SAVE**. Auch hier zunächst die Aufforderung sich zu identifizieren**.** Die Tasten ª, £ und ¢ sind vor einem erfolgreichem Loginvorgang nicht verfügbar. Aus Sicherheitsgründen gibt es auch keine Möglichkeit das Programm ohne einen erfolgreichen Loginvorgang zu verlassen. Die Tastenbelegung ist identisch mit der von **SAVE**.

Wie bei **SAVE** wird, auch wenn keine Eingabe erfolgt, nach ein bis zwei Minuten, je nach Rechnertyp, der Bildschirmschutz aktiviert. Auch bei den Fenstermasken unterscheiden sich die beiden Programme **SAVE** und **SAVECODE** nicht.

Nach der erfolgreichen Beantwortung der Fenstermasken erscheint die Eingangsmaske bzw. das Hauptmenü von **ALTERNATIVE VALIDATE ENTRY**.

Der Anwender ist damit im kritischsten Bereich des **SAVE-Systems**. Daher wird, wenn keine Eingabe erfolgt, nach kurzer Zeit das Programm **beendet**, ganz gleich in welcher Maske, in welchem Menü oder Stadium sich der Anwender befindet. Dies soll verhindern, daß während einer auch nur kurzen Abwesenheit der Anwenders, jemand unbefugt in Besitz des gültigen Symbolcodes gelangt.

Das Hauptmenü:

Zu den schon bekannten Tasten kommen nun noch drei neue dazu.

a: Diese Taste dient dazu einen neuen Symbolcode zu vergeben. Auch der Empfangstext und der Loginname kann in den entsprechenden Menüs gewechselt werden. Wobei gilt, ein Wechsel von Loginname und/oder Empfangstext zieht unweigerlich einen Wechsel des Symbolcodes nach sich.

£: Damit kann das Programm sofort und jederzeit mit dem Symbolcode verlassen werden, mit welchem man es betreten hat, auch wenn in der Zwischenzeit schon Programmintern neue Symbolcodes getestet wurden. Sollte der Symbolcode schon abgelaufen sein, bleibt aber auch der rote Balken beim Betreten von **SAVE** erhalten. Zum Thema *Testen des Symbolcodes* kommen wir etwas später.

¢: Mit dieser Taste wird dieses Programm mit dem neuen Symbolcode verlassen. Gegebenenfalls wird auch der neue Loginname und/oder Empfangstext abgespeichert. Allerdings sind noch einige Dinge zu erledigen, bevor dies möglich ist. Eine freigegebene ¢-Taste wird durch eine Grünfärbung der Anzeige signalisiert.

Doch zurück zum Anfang. Wir haben soeben das Hauptmenü betreten und können nun einen neuen Symbolcode,

- einen neuen Symbolcode plus einen neuen Loginnamen,
- einen neuen Symbolcode plus einen neuen Empfangstext oder
- einen neuen Symbolcode, einen neuen Loginnamen und einen neuen Empfangstext erhalten.

Als erstes müssen wir a drücken und haben dann die Möglichkeit in den entsprechenden Menüs die Auswahl zu treffen. Der Symbolcode wird automatisch gewechselt. Anschließend kommen wir wieder in das Hauptmenü zurück.

Im Hauptmenü erscheint nach unserer Rückkehr oberhalb des Loginnamen-Eingabebalkens die Nummer des Testlaufes. Ein Testlauf ist eine normale **SAVE**-Session welche aber bewertet wird. Ein richtig beantworteter Testlauf erhöht die Nummer über dem Eingabebalken um eins. Ein falsch beantworteter zieht von dieser Nummer wieder eins ab, außer es wurden schon zuvor drei richtige Testläufe absolviert. Abgebrochene Testläufe, zum Beispiel mit S, werden dabei allerdings nicht berücksichtigt. Ist die Hürde von drei richtigen Testläufen absolviert, so kann das Programm jederzeit mit dem neuen Symbolcode verlassen werden. Für einen Testlauf ist nur der Loginname einzugeben, mit b abzuschließen, und schon startet der Testlauf.

Zur Übung können bis zu neun Testläufen durchgeführt werden. Ab drei richtigen Testläufen werden die Testläufe mit falschen Eingaben, wie schon erwähnt, nicht mehr abgezogen, jedoch auch nicht dazu gerechnet. Man kann daher jederzeit das Programm mit ¢ verlassen. Es sei hier aber nochmals erwähnt, daß eine einminütige Pause in der Eingabe das Programm sofort und ohne Speicherung des neuen Symbolcodes abbricht. Nach neun positiven Testläufen wird der Anwender aufgefordert den Symbolcode mit ¢ abzuspeichern, einen neuen mit a zu laden oder mit £ das Programm zu verlassen.

Das Loginnamemenü:

Im Hauptmenü wird mit a der Symbolcode gewechselt. Bei Fehlbedienung wird der Anwender durch verschiedene Fehlermeldungen weitergeleitet. Nachdem die Taste a gedrückt wurde, wird der Anwender zur Sicherheit gefragt, ob er den Symbolcode wechseln möchte.

Mit N für Nein/No kommt man direkt weiter in das Empfangstextmenü zum Ändern des Empfangstextes. Durch diese Möglichkeit kann ich nachträglich zu einem neuen Symbolcode die Empfangsworte noch ändern. Will man aber den Symbolcode wechseln, so kommt man mit J oder Y für Ja/Yes in ein Loginnamenmenü in welchem ein neuer Loginname gewählt werden kann. Der Wechsel des Loginnamens impliziert den Wechsel des Symbolcodes, aber nicht umgekehrt.

Gültige Zeichen für einen neuen Loginnamen sind:

A bis **Z** in Groß- und Kleinschreibung (Kleinbuchstaben werden zu Großbuchstaben)

Die deutschen Sonderzeichen **Ä**, **ä**, **Ö**, **ö**, **Ü**, **ü**, **ß** (jedoch wird **ß** in **SS** umgewandelt)

Der neue Loginname wird mit b abgeschlossen. Das Loginnamenmenü enthält zusätzlich zu den bekannten Tasten die Taste ¥. Durch Drükken dieser Taste bestätigt man nur das Beibehalten des alten Loginnamens zum neuen Symbolcode und kommt gleich in das Menü für den Empfangstext.

Das Empfangstextmenü:

Auch im Empfangstextmenü kann man über die ¥ Taste den Empfangstext beibehalten. Der Wechsel des Empfangstextes inkludiert nicht den Wechsel des Symbolcodes. Wenn wir einen neuen Symbolcode erhalten haben, können wir den Empfangstext nachträglich so oft ändern wie wir wollen. Erst der letzte Empfangstext wird mit dem neuen Symbolcode gespeichert. Wird aber nur der Empfangstext geändert und der Symbolcode nicht, so wird **SAVECODE** anschließend einfach mit £ wieder verlassen und damit bleibt auch die Änderung des Empfangstextes ungespeichert!! Einzig der Symbolcode kann unabhängig von Empfangstext oder/und Loginname gewechselt und abgespeichert werden.

Gültige Zeichen für einen Empfangstextes sind:

Alle Zeichen von **Ê** (ASCII #32) bis **~** (ASCII #126) sowie die deutschen Sonderzeichen **Ä**, **ä**, **Ö**, **ö**, **Ü**, **ü**, **ß**.

Der neue Empfangstext wird mit b abgeschlossen. Damit kehren wir auch wieder in das Hauptmenü zurück und können mit den Testläufen beginnen.

Die Testläufe (*Abbildung 3.3.1*):

Mit den Testläufen soll sich der Anwender an Fenster, Symbole und Symbolset gewöhnen. Er sieht erst dadurch, ob sich in seinem Fenster vielleicht störende falsche Symbole befinden. Sind zum Beispiel ein grünes Plus und ein rotes Fünfeck als richtige Symbole gegeben und im kompletten Symbolset befindet sich auch ein rotes Plus, ein grünes Fünfeck oder beides, so ist ein neuerlicher Wechsel sinnvoll. Das System nimmt bei der Auswahl eines Sets keinerlei Rücksicht auf Ähnlichkeiten zwischen den Formen oder Farben. Diese muß der Anwender selbst feststellen, zumal jeder Anwender andere Kriterien als störend empfindet.

Es ist auch möglich, daß Symbole welche beim alten Symbolcode richtig waren, nun in diesem Symbolset falsch sind. Sollten solche Fälle auftreten, wird mit a im Hauptmenü ein neuer Symbolcode ausgewählt. Für jeden neuen Symbolcode müssen natürlich wieder drei positive Testläufe durchgeführt werden. Mit der Eingabe des Loginnamens wird der erste Testlauf eröffnet. Er unterscheidet sich durch kleine Details von den nachfolgenden. Zunächst wird nicht bei der Anzeige der Fenster angehalten, sondern es werden sofort die Symbole in die Fenster geschrieben. Anschließend werden automatisch die Nummern der Fenster zwischen den Symbolen angezeigt.

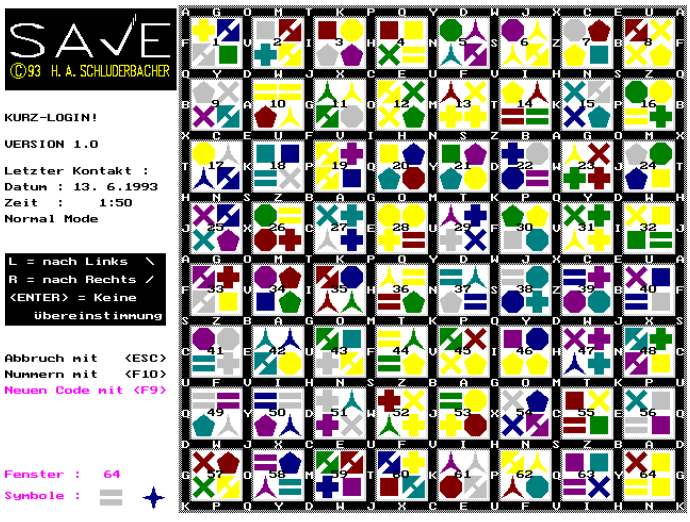

Abbildung 3.3.1

Durch Betätigen von », erscheint links unten die Nummer des Anwenderfensters, darunter die beiden richtigen Symbole. Diese Information ist nur solange sichtbar wie » gedrückt bleibt. Die weitere Eingabe ist analog der von **SAVE**. In allen Fenstermasken des ersten Testlaufes

werden die Nummern der Fenster angezeigt. Alle weiteren Testläufe verhalten sich, mit Ausnahme von », wie normale Sessions.

Wenn das Programm mit ¢ verlassen wurde und der Symbolcode abgespeichert ist, ist es nicht mehr möglich den Symbolcode anzuzeigen.

SAVEINST - INSTALLATIONSPROGRAMM

Um einen ordnungsgemäßen Betrieb von **SAVE** zu gewährleisten, muß das Paket mit **SAVEINST** installiert werden. Nur in diesem Fall können die Programme ihre Aufgabe erfüllen. Anzugeben ist nach Aufforderung der Pfad von **SAVE.EXE** und **SAVECODE.EXE**.

LOGINNAME UND SYMBOLCODE BEIM START

Wenn Sie **SAVE** 1.0x das erste Mal in Betrieb nehmen, ist es auf einen für alle Pakete **fix vorgegebenen Symbolcode** eingestellt:

Loginname		:	**SAVE**
Empfangstext		:	**Version 1.0**
Symbolcode	Fenster	:	**22**
	Symbol1	:	**roter dreizackiger Stern**
	Symbol2	:	**oranger dreizackiger Stern**.

Die Programme sind mit diesem Symbolcode voll funktionsfähig jedoch erscheint bei Betrieb von **SAVE** die Aufforderung den Symbolcode zu wechseln. **In jedem Fall sollte der Symbolcode so rasch wie möglich gewechselt werden**.

WAS TUN WENN ...

... **Sie den Symbolcode vergessen haben**: Geben Sie den Loginnamen ein und drücken Sie b. Schauen Sie bei welchem Fenster Sie sich *Zuhause fühlen*. Tippen Sie b, und beobachten Sie das Fenster mit seinen Symbolen. Nachdem Sie fünf Mal b eingeben haben brechen Sie mit s ab. Dies wiederholen Sie solange bis Sie ihre Symbole wiedererkennen.

... **Sie den Loginnamen vergessen haben**: Geben Sie alle Namen ein welchen Ihnen als mögliche Loginnamen einfallen und sehen Sie ob der richtige Empfangstext erscheint. Wenn ein falscher Text erscheint sofort mit s abbrechen und mit einem neuen Loginnamen fortfahren.

... **Sie den richtigen Loginnamen getippt haben und trotzdem nicht die richtige Fenstermaske bzw. den richtigen Empfangstext erhalten**: Überprüfen Sie ob Sie die richtige Tastatureinstellung haben. Tippen Sie vor der Eingabe Á und beobachten Sie die in dem Balken erscheinenden Zeichen. Bei deutschen Tastaturen kann es mit Y, Z und den deutschen Sonderzeichen, bei französischen mit A, M, Q, W und Z zu Problemen kommen.

... **Sie den richtigen Eingabecode getippt haben und trotzdem nicht hinein können**: Kontrollieren Sie, ob Sie sich im Random-Modus befinden. Sollte dies der Fall sein, bitte lesen Sie sich nochmals die Beschreibung des Systems, vor allem Abschnitt über den Randommodus. Andernfalls ist es möglich, daß es bei der Installation zu einem Fehler gekommen ist und die Tastatur ein falsches Zeichen an das Programm liefert. Vielleicht wurde vor kurzem die Tastatur gewechselt und/oder ein neuer Treiber installiert. In den diesen genannten Fällen vertauschen Sie, wenn der Eingabecode es verlangen sollte, bei deutschen Tastaturen Z mit Y und umgekehrt, bei französischen A mit Q, W mit Z und M mit ,.

HARDWAREANFORDERUNGEN

In der vorliegenden PC-Version ist folgende Mindestgrundaustattung notwendig:

- IBM-Kompatibler **386**SX mit einer entsprechenden Taktfrequenz.
- **VGA**-Farbschirm und -Karte mit (480*640) Bildpunkten.
- MS-**DOS 5.0** oder wirklich Kompatible.
- Eine Tastatur mit dazu passendem Treiber.

Obwohl dies ein graphisches Zutrittssystem ist, wurde auf Mouse-Unterstützung bewußt verzichtet. Was leicht erklärbar ist: Wie sollte ein Symbolcode geheim bleiben, wenn die Symbole oder der Rahmen mit den Zeichen angeklickt werden?

Es ist eine schnelle Bildschirmausgabe notwendig um dem Anwender rasch die nächste Fenstermaske zu zeigen. Bei langsamer Ausgabe zeigen sich Unterschiede bei den oberen und den unteren Fenstern in den Reaktionen der Anwender. Ein Anwender welcher Fensternummer 6 hat, wird bei einem langsamen Bildaufbau seine Symbole schon erkannt und analysiert haben während ein Anwender mit Fensternummer 61 seine Symbole noch nicht am Schirm hat. Dies ist mit ein Grund warum Eingaben vor Fertigstellung der Fenstermaske nicht akzeptiert werden. Bitte beachten Sie auch, daß viele der heute gelieferten Tastaturtreiber nicht voll kompatibel zu den Tastaturen sind.

ZUSAMMENFASSUNG

Der Schutz vor mehr oder weniger zufällig Anwesenden ist bei **SAVE** durch die Fenstertechnik gegeben. Ein oder mehrere Beobachter müßten die Eingabezeichen registrieren und das Fenster mit seinen Symbolen herausfinden, auf welches der Anwender blickt. Eine schier unlösbare Aufgabe.

Vor Trojan-Horse-Programmen oder -Einrichtungen schützt **SAVE** den Anwender durch das Anwender-Symbolset. Der Anwender erkennt also noch bevor er seinen Symbolcode bekanntgibt, ob er getäuscht werden soll. Selbst wenn er es nicht sofort erkennt, wird er im Regelfall nicht mehr als Ê eingeben und diese Taste gilt ja für alle Fenster.

Die Verbindung Mensch - Zutrittscode ist durch die Vergabe des Symbolcodes entkoppelt. Trotzdem ist dieser Symbolcode leicht zu merken. Die Nummer des Anwenderfensters beschreibt keine abstrakte Zahl, wie beim Bankomatcode, sondern eine Stelle in der Fenstermaske. Die Symbole selbst lassen sich leicht einprägen und haben trotz großer Vielfalt nur drei Informationsinhalte, nämlich *richtig*, *falsch* oder *unbekannt*. Daher sind schnelle Entscheidungen möglich. Die Symbolcodevergabe durch das System ermöglicht weiters die breite Streuung des Symbolcodes.

Die Sicherheit vor unbefugten Benutzern ist bei **SAVE** vom angewendeten Modell abhängig. Der Random-Modus garantiert jedoch in jedem Fall einen guten Schutz vor unbefugten Benutzern bei gleichzeitigem Offenhalten für den Anwender.

Seit mehr als zwei Jahren ist eine Demonstrationsversion ohne Probleme im Einsatz. In dieser Zeit haben sich die Anwender natürlich auf die Zutrittskontrolle eingestellt. Trotzdem war es nie ein Ärgernis, beim Hochfahren des Rechners den Eingabecode zu tippen, im Gegenteil. Es war eine sportliche Herausforderung das Fenster immer schneller zu finden, die Symbole noch schneller zu erkennen und ohne Fehler die Eingabezeichen einzugeben. Man könnte also durchaus sagen, daß jedes Mal am Anfang einer Arbeit auf dem Computer ein Spiel stand.

Aber warum soll Sicherheit nicht auch Spaß machen? **SAVE** ist also nicht nur eine notwendige Sicherheitsbarriere, sondern stellt auch eine Herausforderung an Geist und Reaktionsvermögen dar. Zudem ist es das erste wirklich graphische Zutrittskontrollsystem und eignet sich, in hervorragender Weise für die jetzt in Verbreitung befindlichen graphischen Benutzeroberflächen.

LITERATURVERZEICHNIS

[PIN] Axel Pinz.
Bildverstehen.
Vorlesungsunterlagen. 1990/91.

[PIL] Ernst Piller.
Paßwörter - Vom herkömmlichen Paßwort zu den Paßwortalgorithmen. Habilitationsschreiben. 1991.

[RID] B. L. Riddle, M. S. Miron and J. A. Semo. Passwords in use in a university timesharing environment. Computers & Security 8, 569 - 579. 1989.

[SCH] Helmut Schluderbacher.
SAVE - Ein Paßwort in Form und Farbe. Diplomarbeit 1994.

Für Fragen oder weitere Informationen stehe ich Ihnen gerne unter (0222)-602 04 19 zur Verfügung. □