

Kognitiva metoder för användaridentifiering

TOBIAS WIDÉN



**KTH Datavetenskap
och kommunikation**

Kognitiva metoder för användaridentifiering

T O B I A S W I D É N

Examensarbete i datalogi om 15 högskolepoäng
vid Programmet för datateknik
Kungliga Tekniska Högskolan år 2010
Handledare på CSC var Lars Kjell Dahl
Examinator var Mads Dam

URL: [www.csc.kth.se/utbildning/kandidatexjobb/datateknik/2010/
widen_tobias_K10034.pdf](http://www.csc.kth.se/utbildning/kandidatexjobb/datateknik/2010/widen_tobias_K10034.pdf)

Kungliga tekniska högskolan
Skolan för datavetenskap och kommunikation

KTH CSC
100 44 Stockholm

URL: www.kth.se/csc

Sammanfattning

Det kandidatarbetet i datalogi som presenteras i denna rapport utvärderar nya metoder för användaridentifiering i IT-system. Rapporten innehåller en utförlig analys av riskerna med traditionella textbaserade lösenord och presenterar två metoder för att eliminera utantillinläring av text från identifieringsprocessen genom att införa ett grafiskt, klick-baserat gränssnitt.

En genomgång av existerande teknik beskriver PassPoint och en metod föreslagen av Daphna Weinshall år 2006.

Skillnaderna mellan alfabetiska och grafiska identifieringsmetoder diskuteras med hänsyn till människors och maskiners respektive styrkor och svagheter i informationsbehandling. Analysen tar i beaktande aspekter som användarvänlighet och möjligheten att avslöja en inloggning genom automatiserad testning och mänsklig associationsförmåga. Denna analys leder till slutsatser kring hur mänskliga kognitiva förmågor kan involveras i identitetskontroller för att öka säkerheten mot automatiserad testning för att avslöja lösenord.

Slutligen görs ett försök att konstruera en ny typ av inloggning baserad på kognitiva förmågor och grafik. Denna inloggningsmetod sammanför styrkorna från de studerade inloggningsteknikerna och försöker utesluta deras svagheter. Ett experiment utförs för att testa den nya teknikens praktiska användbarhet och möjliga tillämpningar.

Abstract

The Bachelor thesis presented in this report evaluates new schemes for personal identification in IT-systems. This report contains a thorough analysis of the risks with traditional text based passwords and presents two ways of eliminating the memorization of text from the identification process by replacing this element with graphics and click based human interaction. The techniques described are the PassPoint scheme and a scheme suggested by Daphna Weinshall in 2006.

The differences between the alphabetical and graphical approaches are discussed with respect to both the human's and the machine's strengths and weaknesses in information processing. The analysis includes the aspects of human usability and the possibility to retrieve a password through computerized testing as well as human reasoning. This leads to a conclusion in how to incorporate human cognitive abilities into the identification process, therefore making the process safe against computerized testing.

Finally an attempt is made at constructing a new cognitive authentication scheme, incorporating the strengths of comparable techniques and eliminating their weaknesses. An experiment is conducted to test this new scheme's practical usability and possible applications.

Innehåll

1	Inledning	5
1.1	Syfte	5
1.2	Uppgift och frågeställningar	6
1.3	Arbetsgång	6
2	Teoretisk bakgrund	6
2.1	Turingtestet	7
2.2	Alfabetiska lösenord	7
2.3	Weinshalls metod	8
2.4	PassPoint	9
2.5	Experiment	9
3	Metodteori	10
3.1	Applikation	10
3.1.1	Direktassocierad verifikation	10
3.1.2	Erfarenhetsbaserad verifikation	11
3.1.3	Bidningsbaserad verifikation	11
3.2	Enkätundersökning	11
3.3	Genomförande och utvärdering	11
3.3.1	Testmiljö	12
3.3.2	Rekrytering av deltagare	12
3.3.3	Utvärderingsmetod	12
3.3.4	Typiskt genomförande	13
4	Framställning av testapplikation	13
4.1	Krav	13
4.2	Design	14
4.3	Konstruktion	15
5	Experiment	16
5.1	Förberedelser	16
5.2	Genomförande	16
5.2.1	Applikation	16
5.2.2	Enkät	17
5.3	Analys	17
5.4	Resultat	17
5.4.1	Direktassocierad verifikation	18
5.4.2	Erfarenhetsbaserad verifikation	20
5.4.3	Bidningsbaserad verifikation	22
5.4.4	Enkätundersökning	24
5.5	Sammanställning av resultat	24
5.6	Fel och brister	26

5.7	Tidsmätningar	26
5.8	Slutsatser	27
5.8.1	Fördelar och nackdelar mot traditionella lösenord . . .	27
5.8.2	Fördelar och nackdelar mot Weinshall & PassPoint . .	27
5.8.3	Rimlig lösning ur användarens synvinkel	28
5.8.4	Rimlig lösning ur säkerhetssynpunkt	28
5.8.5	Fördelar till, eller diskriminering mot vissa användare?	29
6	Diskussion	29
7	Avslutande ord	30
	Referenser	31
	Bilagor	32
	Skärmbilder	32
	Enkät	37

Tabeller

1	Resultat för datoriserat test, del 1	18
2	Tidsmätningar, del 1	19
3	Resultat för datoriserat test, del 2	20
4	Tidsmätningar, del 2	21
5	Resultat för datoriserat test, del 3	23
6	Tidsmätningar, del 3	23
7	Resultat av enkätundersökning.	24
8	Jämförelse av positiva egenskaper hos studerade tekniker . . .	25

Figurer

1	Resultat för datoriserat test, del 1	18
2	Tidsmätningar, del 1	19
3	Resultat för datoriserat test, del 2	20
4	Tidsmätningar, del 2	21
5	Resultat för datoriserat test, del 3	22
6	Tidsmätningar, del 3	23
7	Resultat av enkätundersökning.	24

1 Inledning

I denna rapport presenteras ett kandidatexamensarbete som utförts på Kungliga Tekniska Högskolan i Stockholm. Arbetet har skett inom kursen DD143X som ges på nämnda skola. Syftet med uppsatsarbetet är primärt att testa och förfinas den studerandes analytiska färdigheter i att identifiera, förstå, analysera, bearbeta och kritisk evaluera ett vetenskapligt arbete inom datalogiområdet.

Ämnet för denna rapport är Cognitive Authentication Schemes (ingen källa indikerar en bra svensk översättning), vilket är ett sätt att hantera en användares inloggning utan att denne skriver in ett lösenord bokstav för bokstav. Istället beskrivs inloggningen som en bild, en tanke eller en regel. Något som antas vara mycket svårare att avlyssna eller genomskåda.

1.1 Syfte

Det har länge funnits ett behov i samhället att unikt identifiera personer på ett tillförlitligt sätt. Identitetskontroller på banker, postkontor, sjukhus och vid landsgränser baseras alla på ett personligt möte och identitetskontroll sker genom jämförelse av signatur och bild i en identitetshandling som utformats så att den ska vara svår att förfalska. Vi människor är kapabla att utföra sådana identifieringar tack vare våra kognitiva förmågor [5].

När identifiering ska ske av en användare i ett datorsystem kan inga sådana metoder användas. Datorn har inte människans förmåga att jämföra en person med ett fotografi taget flera år tidigare eller jämföra signaturer skrivna vid olika tillfällen. Det normala förfaringssättet är i dagsläget att användaren har ett hemligt lösenord. Lösenord riskerar dock alltid att glömmas eller avslöjas och detta är teknikens stora svaghet. I rapporten Cognitive Authentication Schemes Safe Against Spyware [9] föreslås en metod av vad som på engelska kallas cognitive authentication schemes (inga källor indikerar en bra svensk översättning). Detta är ett försök att utnyttja den mänskliga kognitiva förmågan för att unikt identifiera en användare i ett datorsystem. Identifieringen sker genom att presentera användaren med en fråga som är mycket mer komplex än ett lösenord, men som kan lösas enkelt tack vare kognitiva förmågor såsom perception, association, minne och problemlösning [5].

I dagsläget finns metoder för den här typen av inloggning med mycket hög säkerhet men det tar lång tid att träna en användare att använda dessa och även efter träning tar inloggningsförfarandet lång tid [9].

Detta projekt avser undersöka en metod där användaren minns en enda regel och sedan utför en aktivitet av bildassociationer utifrån denna. Resultatet av den undersökningen ställs emot tidigare forskning kring system där användaren måste lära sig stora mängder data utantill men där en korrekt inloggning är helt deterministisk. Målet är att avgöra om denna typ av an-

vändaridentifiering kan ersätta traditionella metoder samt diskutera andra tänkbara tillämpningar för tekniken.

1.2 Uppgift och frågeställningar

Några viktiga frågeställningar som har beaktats under arbetet är följande:

- Fördelar och nackdelar mot traditionella lösenord.
- Fördelar och nackdelar mot Weinshalls metod [9] och PassPoint [2].
- Vad är en rimlig lösning ur användarens synvinkel?
- Vad är en rimlig lösning ur säkerhetssynpunkt?
- Ger en lösning fördelar till, eller diskriminerar den vissa användare?
- Kan den undersökta tekniken användas i andra sammanhang än de tidigare föreslagna?

1.3 Arbetsgång

Arbetet har löpt från januari 2010 till maj 2010. De första två månaderna ägnades åt planering av upplägget kring undersökningen, studier av tidigare forskning och utformning av den testapplikation samt enkät som ligger till grund för innehållet i denna rapport. Därefter följde cirka två veckor av användartester. Tiden från detta fram till maj samma år ägnades åt analys av data samt rapportskrivning.

Planeringsfasen var den enskilt mest arbetskrävande då mycket material inhämtades för att ligga till grund för frågeställningar och utformning av det experiment som genomförts. Experimentet utformades så att det skulle bidra till forskning inom området och är avsedd att fungera som en vidareutveckling av denna kunskapsbank.

Efter att experimentet genomförts och data sammanställts skrevs rapporten samtidigt som pusselbitar lades till varandra och slutsatser från det inledande arbetet tog form och nedteknades.

2 Teoretisk bakgrund

De senaste decenniernas ökning i datorprestanda har resulterat i att maskinerna blivit allt bättre på att lösa avancerade kombinatoriska problem, helt enkelt genom att testa alla tänkbara lösningar. Detta har många positiva följder inom branscher som utför tunga beräkningar eller arbetar med att lösa svåra logiska problem. Tyvärr innebär det också att datorerna kan användas för att avslöja hemliga lösenord. Maskinerna arbetar så snabbt att de kan testa alla kombinationer av tecken och därmed hitta det magiska ordet för

att komma åt en skyddad webbplats eller känsligt system. En sådan metod för att hitta rätt kombination av siffror och bokstäver kallas totalsökning.

Det har också visat sig att lösenord av serier utav alfabetiska tecken inte alls är lämpliga för människor att minnas. Människor är mycket bättre på att minnas bilder [2].

Nedan diskuteras mer om bakgrunden till detta samt vilka åtgärder som skulle kunna vidtas för att höja säkerheten mot attacker på IT-system med hänsyn till både människor och maskiners respektive styrkor och svagheter.

2.1 Turingtestet

Turingtestet är ett tankeexperiment utformat av Alan Turing på 1950-talet då han sökte ett svar på frågan "Om en maskin kunde tänka, hur skulle vi veta det?" [6].

Testet skulle gå till så att en person satt vid en dator i ett rum och skickade meddelanden till andra datorer. Vissa av dessa datorer skulle vara bemannade av människor som svarade på dessa meddelanden men någon eller några datorer skulle svara automatiskt [8]. Turing menade att om det inte gick att avgöra om de automatiserade svaren kom från en dator eller en människa så hade den maskinen klarat Turingtestet [6].

Hittills har ingen dator klarat Turingtestet och varje år hålls Loebner-pristävlingen där forskare tävlar med sina datorprogram om vem som kommer närmast att klara testet. Om någon skulle klara det så är priset 100 000 dollar [4].

Datorer har med gott resultat använts till att bevisa matematiska teorem, styra missiler, sortera post, styra fabriksrobotar och förutsäga vädret [5]. Men de gör allt detta som automater. En dator är en maskin som tar någon form av indata och analyserar den för att sedan reagera. Den måste alltså redan på förhand veta hur den ska tolka indata medan en människa inte behöver veta någonting för att reagera på sin omgivning [5]. För att kunna bete sig som en människa måste alltså en dator redan ha information om allting, ty den saknar omdöme [5].

Av allt detta förstår man att det svåraste lösenordet för en dator att forcera är ett som kräver omdöme för att ange eller tolka innebörden av.

2.2 Alfabetiska lösenord

Det vanligaste sättet att identifiera sig som betrodd användare av ett IT-system är genom att ange ett användarnamn och ett hemligt lösenord. Lösenordet är en sekvens av skrivtecken. De kan antingen ha en språklig mening, som ett namn eller ett ord, eller vara helt slumpmässiga.

Lösenord med språklig betydelse är självklart enklare att komma ihåg än slumpmässiga sekvenser, varför ett vanligt sätt att angripa sådana system är att testa med alla ord ur stora ordlistor. Ett sådant angreppssätt kallas

dictionary-attack [9]. Att lösenord är svåra att komma ihåg ökar risken för att användare av systemet skriver ner sitt hemliga lösenord på papper och avslöjar det genom att förlora, eller bli bestulna på papperskopier. Samma problematik finns med de digitala dosor eller kort som vissa banker delar ut till sina kunder och som ger ett engångslösenord för varje identifiering. Dessa kan tappas bort, stjälas eller gå sönder [9].

En annan variant är att på något sätt avlyssna en dator på nätverket. Det kan antingen ske genom att i hemlighet installera mjukvara som spelar in och sänder vidare indata från användaren (tangentryckningar och musklick) eller att från en annan dator avlyssna nätverkstrafiken till och från en klient i nätverket. Detta kallas att avlyssna eller *eaves drop-attack* [9]. En sådan attack kan till exempel ske då man loggar in på sin internetbank på ett internetcafé.

Så kallad biometrisk identifiering (exempelvis: Ansiktsigenkänning, fingeravtryck, ögonscanning) är säkrare än lösenord eftersom själva nyckeln knappast kan bli stulen men data som skickas mellan klient och värddator kan avlyssnas och användas vid ett senare tillfälle för att återskapa omständigheterna för en lyckad inloggning [9].

Det vore önskvärt att finna en metod för inloggning som både var enkel och sådan att data som skickas över nätverket för en godkänd inloggning inte är samma som för nästa inloggning.

2.3 Weinshalls metod

I en artikel från 2006 föreslår Weinshall en icke namngiven metod där användaren lär sig att identifiera en stor mängd bilder, ca 50 stycken. När hon lärt sig att känna igen dessa bilder presenteras hon vid varje inloggning med en matris innehållande ca 200 bilder. Det är inte säkert att alla 50 av användarens egna bilder ingår i de 200 utan det kan vara en andel av dessa. Hon ska markera de rader där minst en av hennes 50 bilder förekommer. Förfarandet upprepas ett antal gånger och om hon gjort rätt varje gång är det en giltig inloggning [9].

Fördelarna uppges vara att det är mycket svårt att berätta sitt lösenord för någon annan eftersom det är svårt att räkna upp och beskriva 50 bilder men det är något enklare att identifiera dem i en mängd.

Trots att människor är benägna att lättare memorera bilder än bokstäver [2] är det svårt lära sig 50 bilder utantill. Dessutom är det lätt att glömma bilder och då kan man inte logga in. Av samma anledning som det är svårt att räkna upp alla bilderna för någon annan är det svårt att verifiera för egen del att man fortfarande minns alla bilderna. Dessutom uppger Weinshall att inloggningen tar lång tid, ca 10 minuter [9].

Sålunda kan man konstatera att denna typ av identifiering inte utnyttjar fördelen med att memorera bilder optimalt, de är helt enkelt för många för att det ska vara hanterbart. Anledningen till det stora antalet är att

metoden egentligen inte alls berör problemet med datoranalys. En maskin skulle kunna hitta lösningen genom att analysera ett antal inloggningar av samma användare [3]. Ju fler upprepningar en inloggning innehåller desto svårare blir den att forcera [3] men det adderar till den opraktiskt långa tid det tar att logga in.

2.4 PassPoint

Ett annat sätt att utnyttja människans medfödda förmåga att memorera bilder är ett system som kallas PassPoint [2]. För att skapa ett lösenord klickar användaren på ett antal punkter på en bild. Lösenordet blir att klicka på samma punkter, i samma ordning inom en given felmarginal (exempelvis 10 bildpunkter) [2]. Lösenordet uppges fungera ypperligt att minnas även under lång tid utan att det används [2].

Kritik har riktats mot tekniken eftersom användaren alltid klickar på samma ställen på bilden. En dator skulle kunna lagra koordinater för musklickarna och snabbt få reda på vilka punkter som klickas på [2]. Detta utgör en säkerhetsrisk.

2.5 Experiment

Ett bra lösenord bör vara både svårt att avslöja och enkelt att komma ihåg. Både PassPoint och den metod som Weinshall utarbetat använder bilder, vilket är deras styrkor, men båda kan forceras med datorkraft. Det bästa vore om det krävs omdöme för att ange lösenordet, vilket enligt Alan Turings tankeexperiment skulle höja säkerheten dramatiskt.

I de experiment som beskrivs nedan testas tre olika typer av inloggning. Alla är baserade på att användaren identifierar rader i en matris med bilder (i likhet med Weinshall) och identifieringen sker utifrån en regel som kräver någon form av omdöme istället för att söka och markera specifika bilder. Som lösenord används en minnesregel vilken är utformad så att den inte direkt identifierar någon enskild bild i matrisen.

I det första testet ska användaren identifiera ett mycket specifikt föremål och markera alla rader där bilder på det föremålet förekommer.

Det andra testet anger två kriterier nämligen var föremålet normalt förekommer och dess värde i förhållande till andra föremål.

I det tredje testet ska användaren hitta bilder utifrån ett abstrakt kriterium där hon skiljer figurer åt utifrån egna erfarenheter.

I detta experiment kommer alla försökspersoner att ställas inför samma tre regler, vilka utgör deras problemformulering för uppgiften. De tre olika reglerna som beskrivs ovan har alla utformats för att skilja sig åt på kritiska punkter för att kunna ge information om vad som karaktäriserar en lämplig minnesregel, om en sådan finns.

Tanken är att i en praktisk tillämpning ska inloggningsregeln vara unik för varje användare. Fördelarna med tekniken förväntas vara att inloggningen går snabbare än med Weinshalls metod och ingen träning ska vara nödvändig för att kunna använda systemet. Varje person ska direkt kunna använda sitt omdöme för att identifiera sig i ett IT-system.

De experiment som utförs ska besvara frågorna som formulerats i avsnitt 1.2.

3 Metodteori

Det främsta verktyget för att utföra studien är den testapplikation som utvecklas. Den ska visa hur lika, eller olika, människor tolkar och genomför en regel enligt 2.5 och därmed hur tillförlitlig en inloggning är. Dessutom genomförs en enkätundersökning som ska testa hur svårt det är att forcera inloggningen, det vill säga avslöja informationen som behövs för att logga in. I detta avsnitt kommer teorin bakom de olika utvärderingsmetoder som används att beskrivas.

En metod för inloggning är tillförlitlig då en person som kan logga in med den lyckas med detta på varje eller flertalet av sina försök. En otillförlitlig regel medför misslyckade inloggningar trots korrekt beteende av testpersonen eller att inloggningen lyckas trots att personen angett fel information.

3.1 Applikation

Testapplikationen är till för att samla in data om tillförlitlighet i inloggningen. Förhoppningen är att åtminstone en regel ska vara tillräckligt tillförlitlig för att kunna användas som inloggningmetod eller att resultaten ska visa på ett nytt användningsområde för tekniken. Applikationen ska simulera tre olika inloggningar (se avsnitt 2.5) och lagrar varje persons resultat på alla test, tillsammans med det namn personen anger. De tre inloggningarna som simuleras beskrivs nedan.

3.1.1 Direktassocierad verifikation

I det första testet ska användaren följa en väldigt direkt uppmaning, inget abstrakt tänkande eller resonemang är nödvändigt. Uppgiften är att användaren ska hitta och markera alla rader i bildmatrisen som innehåller bilder på hundar.

Denna enkla regel förväntas ha en hög andel godkända inloggningar eftersom den i största möjliga mån isolerar problemet till att hantera programgränssnittet.

3.1.2 Erfarenhetsbaserad verifikation

I det andra testet uppmanas användaren att markera alla rader i bildmatrisen som innehåller bilder på föremål som normalt förekommer i ett hushåll och som kostar mer än 1000 kronor. Detta ställer krav på användarens kännedom om normala hushållsartiklar och vad sådana kostar. En person som inte har haft ett eget hushåll skulle kunna uppfatta detta som svårt eller förvirrande. Förutsättningarna varierar också utifrån individens bakgrundskunskap om vad som normalt finns i ett hem. I en familj med många syskon kanske det alltid fanns en barnvagn, men inte för ett ensam barn.

Testets syfte är att, om möjligt, sätta en övre gräns till hur komplicerad och individkänslig en inloggningsregel av den här typen kan vara.

3.1.3 Bildningsbaserad verifikation

Det tredje testet är utformat så att användaren ska markera alla rader i bildmatrisen som innehåller bilder på fiktiva figurer. Vissa bilder är tecknade och vissa föreställer verkliga människor utklädda till fiktiva karaktärer, till exempel Spindelmannen. Detta ställer krav på personens kännedom om film, TV, serier, media och så vidare.

Detta test kombinerar en förhållandevis enkel uppmaning med att testpersonen måste använda både sin erfarenhet och sitt omdöme för att lösa uppgiften.

3.2 Enkätundersökning

Enkäten testar motsatsen till applikationen. Den ska samla in data om hur lätt eller svårt det är för en människa att genomskåda en inloggning genom att titta över axeln på den som utför inloggningen. Enkäten består av tre bilder på samma bildmatris som förekommer i applikationen, men de rader som innehåller nycklarna till inloggningen är markerade med röda rektanglar. Utifrån detta ska testpersonen försöka finna den inloggningsregel som korresponderar till enkätens bilder.

Den regel som bilderna beskriver är en markering av alla rader i bildmatrisen som innehåller bilder på personer som varit officiella ledare för länder.

Denna undersökning testar både hur svårt det är att genomskåda de regler som testats med applikationen och hur entydig en regel är. Det är relevant för testet hur många olika regler testpersonerna finner som stämmer in på bilderna de studerat.

3.3 Genomförande och utvärdering

Det här avsnittet beskriver under vilka omständigheter användartesterna genomförts och hur de data som samlats in har sammanställts.

3.3.1 Testmiljö

Testerna utförs i ett flertal varierande miljöer. Valet att göra så kommer av att en metod för inloggning ska kunna användas i vilken miljö som helst. I de flesta fall sker testerna i datorsalar på Kungliga Tekniska Högskolan i Stockholm men i vissa fall utförs testerna i hemmiljö. En del variationer i miljön såväl som yttre störningar i form av ljud och utomstående människor kan således förekomma.

Det är viktigt för experimentets utfall att testerna inte utförs i en laboratoriemiljö då tidigare forskning visat att det förändrar användartesternas utfall [2]. Testmiljön har således betydelse för resultatet. Valet har dock blivit att inte ta med den som en parameter utan att lita på att de varierande omständigheter under vilka testerna utförs ska ge en bra spridning av störningar i data.

Enkäten fylls i av testpersonerna efter att de har använt testapplikationen. De fyller i enkäten i samma miljö som testet utförs i. De tillåts inte att ta hjälp av andra personer.

3.3.2 Rekrytering av deltagare

Rekrytering sker i första hand genom att be familj och vänner genomföra testet. Därefter rekryteras testpersoner bland studenter på Kungliga Tekniska Högskolan i Stockholm. Även testpersoner utanför den tekniska akademiska sfären är önskvärda. Det enda krav som ställs på deltagarna är att man anser sig vara en van datoranvändare. Detta för att deltagarna är tvungna att använda ett enkelt grafiskt gränssnitt.

3.3.3 Utvärderingsmetod

Studiens första del består av tre testfall (se avsnitt 3.1), som genomförs tre gånger var på alla testpersoner. Programmet lagrar både de enskilda resultaten i varje upprepning samt vilka testpersoner som får tre rätt på samma test och därmed anses ha klarat att ”logga in” med tekniken. Genom att jämföra hur många som lyckas göra tre korrekt genomförda test i rad med hur många som klarar färre test kan slutsatser dras om teknikens tillförlitlighet (se avsnitt 3). Resultatet av varje test tolkas som godkänt eller icke godkänt, detta är i enlighet med hur en inloggning skulle fungera i ett verkligt system och är den förutsättning utifrån vilken alla data tolkas.

Även tiden det tar att genomföra varje test lagras för att avgöra om något av testen tar orimligt lång tid för att kunna användas i en praktisk tillämpning.

Enkätsvaren kontrolleras genom att undersöka om personernas svar är rimliga och entydiga för den uppgift de ställs inför.

3.3.4 Typiskt genomförande

Testpersonerna utför sina uppgifter sittande framför en bärbar dator. De får muntligen veta att all information de behöver under testets gång ges skriftligen genom applikationen och att deras uppgift kommer att vara att tolka regler och markera bilder utifrån detta. Därefter får de hjälp att starta programmet. Testet har inte någon tidsbegränsning.

Enkäten består av ett svarsformulär med problemformulering och tre skärmbilder från testapplikationen. Inte heller enkäten är tidsbegränsad.

Inga testpersoner får före, under eller efter testet veta vad lösningarna är eller de rätta inloggningsmönstren. Detta för att personer som ännu inte gjort testet inte ska få kunskap om testets innehåll.

4 Framställning av testapplikation

Utvecklingen av projektets applikation utfördes i enlighet med den så kallade vattenfallsmodellen [7]. I den första fasen formuleras de krav som ställs på mjukvaran. När samtliga krav formulerats och strukturerats behandlas denna information under designfasen och en implementationsplan skrivs. Under konstruktionsfasen sker all programmering och implementation av designen.

4.1 Krav

Nedan listas de krav som ställs på programmet. Det är enligt vattenfallsmodellen möjligt att dela upp dessa i krav som **ska** uppfyllas och krav som **bör** uppfyllas. Endast ska-krav används eftersom programmet ska innehålla ett absolut minimum av funktionalitet, men inte mindre.

1. Programmet ska testa inloggning enligt metoden beskriven i avsnitt 2.5.
2. Det ska visas en matris med 10 gånger 10 bilder på skärmen. Raderna ska vara numrerade.
3. Användaren ska presenteras med en instruktion om hur hon ska selektera rader ur denna matris.
4. Det ska gå att på något sätt markera raderna i matrisen.
5. Det måste vara enkelt att förstå gränssnittet.
6. Användaren ska inte få några val förutom svarsalternativ. Flödet genom programmet ska vara linjärt.
7. Det ska finnas möjlighet att formulera olika och nya tester att utföra på bildmatrisen.

8. Konstellationen av bilder i matrisen ska inte vara statisk utan bilderna placeras slumpmässigt inför varje test.
9. Programmet ska mäta tiden som varje test tar, för att avgöra om metoden kräver orimligt lång tid.
10. Det ska gå förhållandevis fort att programmera, eftersom tid är en begränsad resurs i projektet.
11. Programmet ska automatiskt rätta användarens svar utifrån det facit som testledaren skapat tillsammans med testet.
12. Programmet ska lagra alla testresultat på ett format som gör det enkelt att analysera data från användartesterna.
13. Urvalet av bilder ska vara så varierat som möjligt för att undvika oavsiktliga samband mellan bilder.

4.2 Design

När kraven formulerats så grupperas de efter hur de interagerar med varandra och en designlösning som tillgodoser varje kravgrupp såväl som varje individuellt krav tas fram.

Det första kravet, 1, beskriver programmets syfte och uppfylls genom de mer detaljerade kraven 2, 3, 4, 5 och 6 vilka definierar hur användaren interagerar med programmet. Programmet ska visas som två olika applikationsfönster. Den ena innehåller en figur med 10 gånger 10 små bilder, där raderna är numrerade från 1 till 10. Det andra fönstret har ett utseende som påminner om ett svarsformulär vid tipspromenad eller poängbrickan i bångolf, detta fönster kallas Testkontroll. Vid programstart visas en dialogruta som uppmanar användaren att skriva sitt namn. Om användaren inte skriver något så avslutas programmet. Därefter visar testkontrollen en instruktion som beskriver hur testet kommer att gå till, men avslöjar inte detaljerna kring de enskilda testfallen. Användaren klickar på testkontrollens enda knapp för att starta testet.

Fönstret med bildmatrisen och testkontrollen visar vilket test i ordningen som utförs, vad instruktionen är samt 10 kryssrutor numrerade "Rad 1" till och med "Rad 10". Användaren markerar i dessa kryssrutor de rader som hon anser matchar regeln och klickar därefter på den enda knappen, "Nästa test". Förfarandet upprepas tills alla tester är slut. Då tackas användaren skriftligen för hjälpen och får se vilka test som var rätt och vilka som var fel. Användaren får inte se de rätta svaren. Det finns inga alternativ, utan programmet avslutas.

Möjlighet att enkelt göra nya tester och ändra gamla, krav 7, ska uppfyllas genom att varje test på kodnivå struktureras som ett logiskt objekt (en

klass). Varje testobjekt sköter tidsmätning, krav 9, och rättar användarens svar utifrån bildmatrisen, krav 11.

Bildmatrisen representeras internt som en matris med samma dimensioner innehållande heltal. Heltalsmatrisens innehåll randomiseras innan varje test utförs, krav 8.

När alla tester utförts lagras resultaten (Namn, tid för varje test, resultat *godkänt/underkänt*) i textfiler på datorns hårddisk, krav 12.

Programmet skrivs i programmeringsspråket Java som har färdiga hjälpmedel för fönsterhantering, bildobjekt, grafik och filhantering. Javaprogram kan dessutom köras på de flesta vanliga datorer så testet blir portabelt och därför lättare att utföra, krav 10.

Bildstorlek väljs till $100 * 100$ pixlar eftersom allt för små bilder medför svårighet att avgöra motiv och därför bidrar till störningar i testet [2]. Bildstorleken gör att tio hela rader av bilder inte ryms på alla datorskärmar så programmet utrustas med en rullningslist så att alla bilder kan visas i den valda storleken.

För att samla in bilder användes ett script som slumpvis valde ord ur en nyhetstext och sökte på *Google Images* efter bilder i formatet $100 * 100$ pixlar. Bilderna sorterades sedan manuellt och de bilder som inte hade ett tydligt motiv vilket lätt kunde identifieras och benämnas raderades. Efter detta lades ett antal bilder till mängden vilka skulle utgöra nyckelbilder i inloggningsreglerna. På det viset åstadkoms ett urval av etthundra bilder med stor variation, krav 13.

4.3 Konstruktion

Det gick snabbt att implementera alla funktioner och programmera ett enkelt men komplett program för experimentet, mycket tack vare det grundliga arbetet under designfasen. Den första konceptuella modellen som innehöll alla funktioner och krav testades på fem personer för att se om de kunde använda applikationen och genomföra experimentet utan handledning. Deras tolkning av programmets instruktioner gjorde att deras svar inte skulle ha kunnat användas i studien. Med anledning av detta gjordes en ändring av den initiala instruktionen till programmet så att den förklarade att antalet rader som skulle markeras kunde variera mellan de olika testerna och rundorna. Vissa hade också problem med att testkontrollen hamnade bakom bildmatrisen på skärmen men det påverkade inte användarnas resultat då det kunde lösas på plats och inte påverkade deras uppfattning om uppgiften de skulle lösa.

Det första pilottestet av applikationen visade också att de testregler som skissats upp (de var då inte i sin slutgiltiga form) var tvetydiga. Det var härvidlag nödvändigt att byta ut vissa bilder och därmed bryta mot den ursprungliga intentionen (krav 13) att ha helt slumpmässiga motiv på bilderna. En bild som föreställde Jesus (Karaktär som finns i verkligheten eller fiktiv person?) togs bort och en annan regel omformulerades något så den

inte var lika beroende av vilka bilder testet innehöll.

Utöver kraven (se avsnitt 4.1) implementerades också en testfunktion. Genom att ange "test" som namn vid programstart kringgås att testresultat genererade i samband med felsökning blandas med verkliga testdata. Allt som testanvändaren gör sparas i en separat fil i felsökningssyfte.

5 Experiment

Efter att ha konstruerat och testat både applikationen och den enkät som ligger till grund för användartestningen genomfördes experimentet. I detta avsnitt beskrivs både de förberedelser som var nödvändiga och genomförandet av undersökningen. Resultaten redovisas samt analyser och slutsatser utifrån erhållna testdata och möjliga felkällor.

5.1 Förberedelser

Efter att applikationen blivit klar genomfördes ytterligare en utvärdering. Det huvudsakliga syftet med denna var att se hur programmet fungerade i praktiken och konstruera ett facit utifrån vilket uppgifterna skulle bedömas.

Fem personer fick titta på applikationens bildmatris och berätta vilka bilder de ansåg korresponderade till varje tests regel. De bilder som utpekats av 4 personer för en viss regel fördes in som facit i programmet.

För att skapa enkäten kopierades tre skärmbilder på fönstret med applikationens bildmatris. Utifrån den tänkta regeln markerades vissa rader med röda rektanglar.

5.2 Genomförande

Rekrytering av testpersoner skedde i första hand genom att be familj och vänner genomföra testet. Flertalet av dessa tyckte att både teorin bakom och själva genomförandet av testet var så intressant att de rekommenderade fler personer att delta. Således är den demografiska spridningen inom testgruppen okänd eftersom alla som velat delta fått göra detta. Det enda krav som ställts på deltagarna var att man ansåg sig vara van datoranvändare. Ingen presumtiv testperson har dock ansett sig ovan vid detta och därför har ingen nekats till att delta i studien.

Totalt deltog 23 personer i undersökningen. Utav dessa var 8 stycken kvinnor och 15 stycken män. Samtliga uppgav att de använder datorer dagligen privat eller i yrkeslivet.

5.2.1 Applikation

Vissa testpersoner tappade bort svarsformuläret på skärmen för att det hamnade bakom bildmatrisen. I dessa fall hjälpte testledaren dem att arrangera

applikationsfönstren på skärmen så att de aldrig överlappade varandra helt.

Testpersonerna har under försöket inte haft någon tidsbegränsning. De flesta har uttryckt att det var ett intressant test, särskilt som de efter att samtliga nio test med applikationen genomförts fått se sina resultat.

Bilder av applikationens utseende bifogas i bilaga A.

5.2.2 Enkät

Samtliga deltagare genomförde enkäten och lämnade in någon form av svar inom tio minuter. Dock har tiderna för att prestera ett svar inte noterats.

Vissa personer blev initialt överväldigade av det till synes komplicerade problemet men flertalet lämnade vad som verkade vara ett genomtänkt svar.

Inga testpersoner har före, under eller efter testet fått veta vad lösningarna var eller de rätta inloggningsmönstren.

Enkäten var densamma för alla testets deltagare och den bifogas i bilaga B.

5.3 Analys

Applikationen lagrade testpersonernas resultat i filer. Dessa filer har sedan sammanfattats i tabeller med ett kalkylprogram. Tabellerna har gjort det lätt att jämföra resultaten från de olika testerna och personerna. Resultatet har sammanställts i diagramform presenteras även i avsnitt 5.4.

Tabellerna används för att i löpande text sammanfatta och belysa resultaten av respektive test och för att göra systematiska jämförelser mellan de olika testerna.

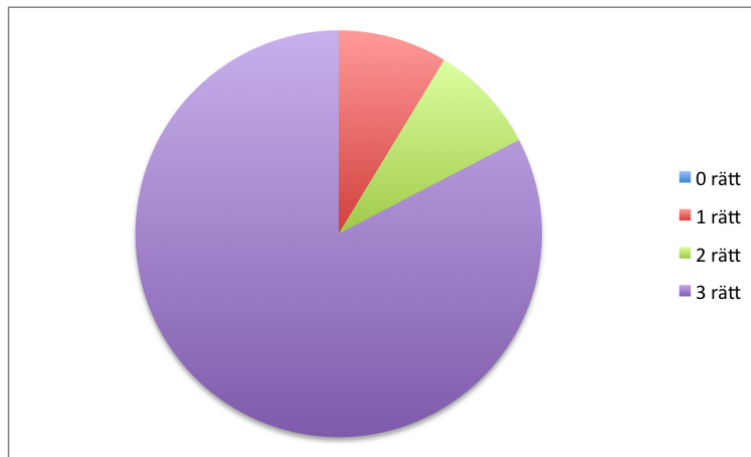
Enkätsvaren kontrollerades genom att undersöka om personernas svar var rimliga och entydiga för den uppgift de ställts inför. Om en persons svar inte var den regel som testet utformats utifrån men rimlig betraktades den som korrekt. Betydelsen av detta diskuteras i avsnitt 5.8.4.

5.4 Resultat

I denna del av rapporten kommer de olika resultaten av respektive test att presenteras. De enskilda testpersonernas svar har utelämnats och data har istället generaliserats till diagram och extrem-/medelvärden för att kunna göra bredare analyser av resultatet.

Huvuddelen av försökets resultat är kvantitativa och består av den information som testapplikationen samlat in samt enkätsvaren. Därutöver har observationer gjorts under testets utförande vilka används nedan för att stödja diskussioner och slutsatser.

5.4.1 Direktassocierad verifikation



Figur 1: Resultat för datoriserat test, del 1

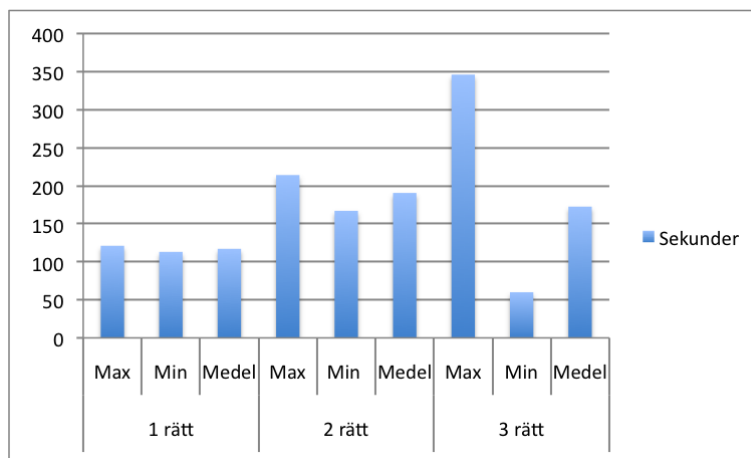
Som förväntat klarade en stor andel av försökspersonerna att tolka regeln och andelen som anses ha klarat att genomföra en korrekt inloggning med tre upprepningar är hög. Utfallet är mycket gynnsamt då det visar att principen med minnesregel som utpekare av rader med bilder fungerar. Själva gränssnittet mellan människa och maskin är därmed dugligt för att genomföra resterande tester.

Ingen person misslyckades helt med de tre på varandra följande testen. En minoritet misslyckades med ett eller två försök att markera raderna. Bakgrunden till detta antas vara att de misstolkat regeln, inmatningsmetoden (rader), förbisett en bild som ingick i inloggningen eller helt enkelt klickat fel. Detta är felaktigheter av en typ som man aldrig kan undvika helt.

Den höga andelen avklarade tester utpekar den här regeln som lämplig ur ett användarperspektiv.

Tabell 1: Resultat för datoriserat test, del 1

	Antal	Andel
0 Rätt	0	0 %
1 Rätt	2	8,7 %
2 Rätt	2	8,7 %
3 Rätt	19	82,6 %



Figur 2: Tidsmätningar, del 1

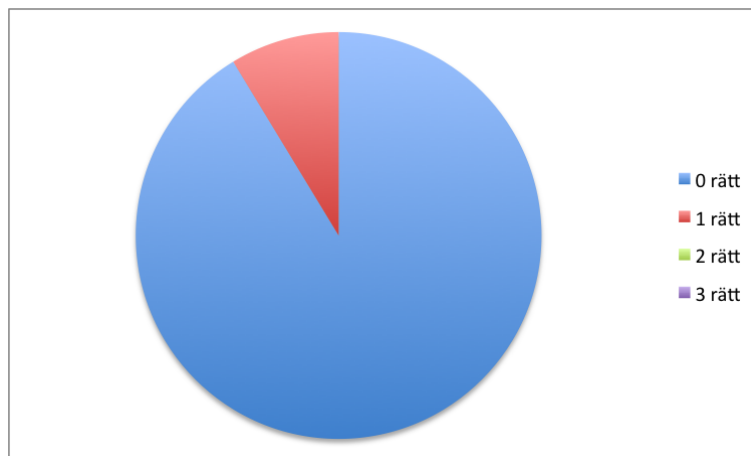
Den mest intressanta kategorin försökspersoner (på grund av dess dominans) är de som genomförde tre på varandra följande inloggningar helt korrekt. Man kan se att dessa hade både den tydligt längsta och kortaste tiden för de tre upprepningarna. Detta säger inte så mycket om testet förutom att de flesta resultaten hamnade i denna kategori och förmodligen är det anledningen till att de extrema värdena återfinns här.

De genomsnittliga tiderna för antalet möjliga rätt är jämnt fördelade. Detta tyder återigen på att de som inte fått alla rätt begått enkla misstag då de verkar ha ägnat lika stor tid åt att överväga sina svar som de personer som presterat 3 rätt.

Tabell 2: Tidsmätningar, del 1

	Max	Min	Medel
0 rätt	-	-	-
1 rätt	113 sekunder	113 sekunder	113 sekunder
2 rätt	214 sekunder	167 sekunder	191 sekunder
3 rätt	346 sekunder	60 sekunder	173 sekunder

5.4.2 Erfarenhetsbaserad verifikation



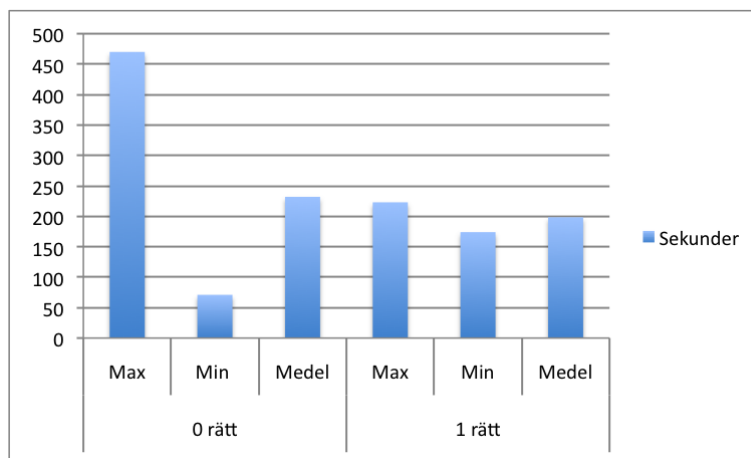
Figur 3: Resultat för datoriserat test, del 2

Även den erfarenhetsbaserade verifikationsmetoden visar stor likhet mellan testpersonernas resultat, vilket var förväntat (se avsnitt 3.1.2). Över 91 % fick noll rätt. Under testet uttryckte flertalet av personerna att de var förvirrade av regeln. Även om 1000 kronor är en fast gräns finns det inget bra sätt att jämföra den med priset för föremålen på bilderna. Det finns exempelvis skor för både betydligt mer och betydligt mindre än 1000 kronor.

Den låga andelen avklarade tester utpekar den här regeln som olämplig ur ett användarperspektiv.

Tabell 3: Resultat för datoriserat test, del 2

	Antal	Andel
0 Rätt	21	91,3 %
1 Rätt	2	8,7 %
2 Rätt	0	0 %
3 Rätt	0	0 %



Figur 4: Tidsmätningar, del 2

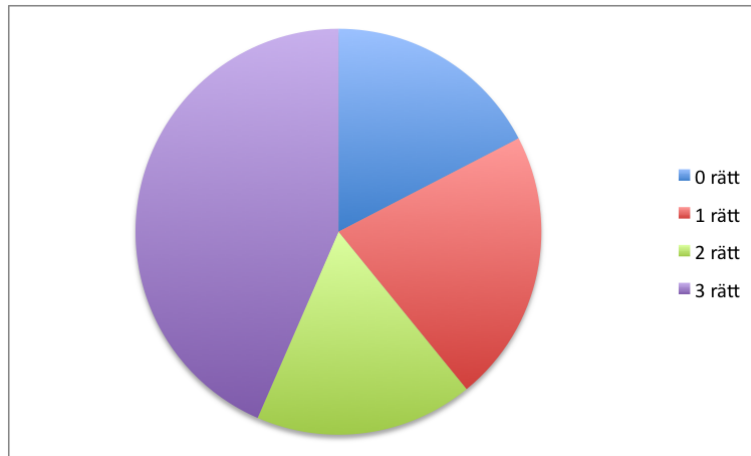
Testpersonernas osäkerhet inför testet avspeglas i hur lång tid det tog att logga in. Medeltiderna är cirka 30 % högre än för direkt associerad verifikation. Inte ens den testperson som tog längst tid på sig fick ett enda rätt.

Den genomsnittliga tiden för ett enda rätt är något lägre vilket indikerar att det inte beror på noggrannare övervägande än övriga testpersoner. Snarare har de två personer som lyckats få ett rätt klarat detta av ren slump. Denna tes styrks av att ingen lyckats få två eller fler rätt.

Tabell 4: Tidsmätningar, del 2

	Max	Min	Medel
0 rätt	470 sekunder	71 sekunder	232 sekunder
1 rätt	223 sekunder	174 sekunder	199 sekunder
2 rätt	-	-	-
3 rätt	-	-	-

5.4.3 Bildningsbaserad verifikation



Figur 5: Resultat för datoriserat test, del 3

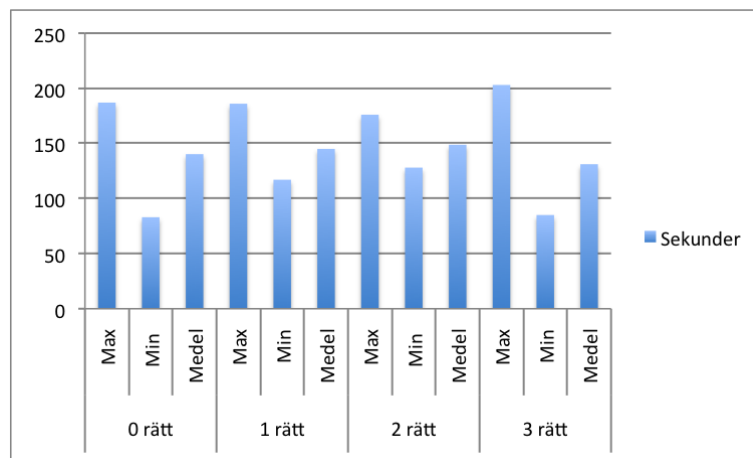
Testets utfall visar stor spridning mellan de olika testpersonernas resultat men med en tydlig övervikt på flera korrekta inloggningar i följd. Över 60% hade 2 eller 3 rätt, vilket med tanke på att det är ett system som testpersonerna aldrig tidigare använt eller introducerats till, är ett mycket gott resultat.

De testpersoner som fått noll rätt har förmodligen tolkat regeln på ett annat sätt än vad som avsetts då testet konstruerades. Detta visar att även denna regel har multipla tolkningar men att dessa personer åtminstone varit konsekventa i sin avvikande tolkning. Någon testperson kommenterade att vissa bilder föreställde personer som varken kunde sägas vara fiktiva eller ej då de var helt okända. Samma sak gällde för bilden på en nallebjörn, vilken för vissa personer kunde tolkas som en specifik björn och alltså som en fiktiv karaktär snarare än som ett anonymt föremål.

Den regel som användes för detta test har påfallande hög andel korrekt genomförda inloggningar och det verkar som att varje person kan bilda sig en uppfattning om hur han eller hon ska genomföra uppgiften. Denna typ av regel, eller likartade, har potential att användas som användarverifiering.

Tabell 5: Resultat för datoriserat test, del 3

	Antal	Andel
0 Rätt	4	17,4 %
1 Rätt	5	21,7 %
2 Rätt	4	17,4 %
3 Rätt	10	43,5 %



Figur 6: Tidsmätningar, del 3

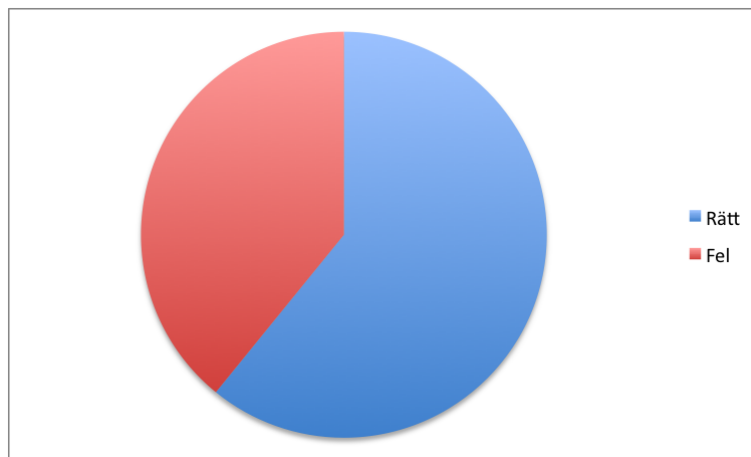
De tider som noterades fördelar sig jämnt över resultatkategorierna. Det framstår som att samtliga personer som genomgått testet ägnat lika lång tid åt att överväga sina svar och därmed haft en klar, personlig, tolkning av uppgiften.

De genomsnittliga tiderna ligger genomgående mellan två och två och en halv minut. Detta är betydligt längre tid än den tid det normalt tar att skriva in ett memorerat lösenord men inte lika lång tid som en inloggning tar med Weinshalls metod [9].

Tabell 6: Tidsmätningar, del 3

	Max	Min	Medel
0 rätt	187 sekunder	83 sekunder	140 sekunder
1 rätt	186 sekunder	117 sekunder	145 sekunder
2 rätt	176 sekunder	128 sekunder	149 sekunder
3 rätt	203 sekunder	85 sekunder	131 sekunder

5.4.4 Enkätundersökning



Figur 7: Resultat av enkätundersökning.

Lite oväntat visade det sig att över 60% av personerna som ingick i testet kunde lista ut regeln som använts för att skapa enkäten. Två olika korrekta regler inkom som svar. Den ena var olika formuleringar på temat "Personer som lett ett land", den andra var "Manliga politiker". Båda dessa var helt korrekta utifrån de bilder som tillhandahållits.

Oavsett hur det korrekta svaret formulerades är regeln jämförbar med den som testades i 5.4.3. Likheterna består i att användaren av systemet ska hitta bilder på personer eller karaktärer med en gemensam egenskap vilken kräver allmänbildning för att känna till.

Tabell 7: Resultat av enkätundersökning.

	Antal	Andel
Rätt	14	60,9 %
Fel	9	39,1 %

5.5 Sammanställning av resultat

I Tabell 8 presenteras de fakta och resultat som framkommit under projektet genom informationssökning och användartestning. Tabellen utgör en sammanställning av skillnader och likheter mellan den metod som undersökts genom experiment och studierna av Weinshalls metod [9], PassPoint [2] och vanliga textbaserade lösenord som användaren lär sig utantill [9, 2]. Ett antal positiva aspekter för inloggningstekniker har valts ut och tabellen

markerar vilka tekniker som uppfyller dessa egenskaper. Sammanställningen består av resultat och slutsatser från avsnitten 2 samt 5.4.

- *Lätt att lära sig*

Hur lätt är det att lära sig det lösenord, den regel eller annan information som är nödvändig för att identifiera sig i systemet utantill?

- *Lätt att minnas*

Hur lätt är det att minnas det lösenord, den regel eller annan information som är nödvändig för att identifiera sig i systemet?

- *Snabb inloggning*

Hur snabbt kan en person ange sina inloggningsuppgifter eller motsvarande? Ingen jämförd metod är lika snabb i detta avseende som det alfabetiska lösenordet men jämförelsen är gjord utifrån föreställningen om en rimlig tid för att genomföra en inloggning.

- *Svår att berätta*

Är det svårt att berätta för någon annan hur man gör för att logga in? Detta kriterium kan även beskrivas som hur svårt det är att formulera en beskrivning som i detalj anger hur inloggningen genomförs.

- *Svår att avlyssna*

Är det en teknik som är svår att forcera med automatiserad datortestning? Det vill säga om det går att hitta likheter och serier i flera på varandra följande inloggningar om man spelar in förfarandet genom att avlyssna tangentryckningar eller musklick.

- *Svår att tjuvkika*

Kan en person som tittar över axeln på någon som loggar in avslöja hur inloggningen gick till och skulle den personen efter detta kunna logga in på egen hand?

Tabell 8: Jämförelse av positiva egenskaper hos studerade tekniker

	PassPoint	Weinshall	Experiment	Lösenord
Lätt att lära sig	X		X	
Lätt att minnas	X		X	
Snabb inloggning	X			X
Svår att berätta	X	X		
Svår att avlyssna		X	X	
Svår att tjuvkika		X	X	

5.6 Fel och brister

Förutom att applikationens fönster ibland lade sig ovanpå varandra så att svarsformuläret skymdes verkar inga fel ha funnits i testapplikationen. Det är möjligt att regeln för erfarenhetsbaserad verifikation (se avsnitt 5.4.2) hade multipla tolkningar då flera personer frågade vad som menades med ett hushåll. De hänvisades då till att göra den bedömningen själva och genomföra testet utifrån detta.

Det ska noteras att huruvida inloggningarna betraktats som korrekta eller ej har bedömts utifrån vad som framkom i ett mindre pilottest (se avsnitt 5.1) innan någon av de faktiska testpersonerna använt applikationen. All rättning har skett utifrån vad som framkom ur detta pilottest. Enligt 5.4.1 och 5.4.2 verkar detta ha fungerat bra då även testets resultat överrensstämte väl med detta men i 5.4.3 fanns en stor andel misslyckade inloggningar. Det kan inte uteslutas att detta till viss del beror på något fel under pilottestet men betydligt mer sannolikt är att regeln inte är lämplig att användas i detta syfte.

Ett beslut som fattades vid det första användartestet var att inte låta någon träna med programmet innan de gjorde testet. Detta eftersom avsikten var att skapa en inloggning som kunde användas utan träning och gränssnittet ansågs inte utgöra något generellt hinder för att genomföra experimentet utan övning. Det skulle kunna vara intressant att göra en funktion i testapplikationen som lagrade första testets resultat separat, för att se om det fanns ett mått av ökad tillförlitlighet genom inläring i försökets utformning. Detta har dock inte skett. Att sådan information inte lagrats omöjliggör slutsatser om huruvida systemet trots allt har en inläringstid. Det är tänkbart, och troligt, att de lägsta resultaten skulle utebli om en kortare övningsperiod tilläts innan testet.

Flera försökspersoner förstod initialt inte att de tre bilderna i enkäten hörde ihop och att de skulle formulera en regel efter att ha studerat alla tre. Ett antal försökte finna en regel för varje bild och vissa struntade i de två sista bilderna och studerade bara den första. Denna brist uppdagades redan på den första testpersonen och därför har alla efter denna fått följande muntliga instruktion ”Det är samma regel för alla tre bilderna, du ska titta på tre bilder men bara hitta en regel”. Därmed bör detta inte ha haft negativ inverkan på resultaten.

5.7 Tidsmätningar

Tiderna för att genomföra ett test har mätts automatiskt av testapplikationen. Tidsmätningen har startat då testpersonen fått sin uppgift presenterad på datorskärmen och stoppats då den klickat på knappen för att gå vidare till nästa test. Tiderna inkluderar alltså både tiden som personen nyttjat för att tolka regeln, genomföra uppgiften och verifiera att uppgiften utförts. Först

därefter har personen bekräftat att hon anser sig att uppfyllt uppgiften.

De tider som presenteras i Tabell 6, Tabell 4 och Tabell 2 är de sammanlagda tiderna för att genomföra tre upprepningar av samma test. Figur 2, Figur 4 och Figur 6 illustrerar hur dessa tider förhåller sig till antalet korrekta inloggningar presterade på den tiden.

5.8 Slutsatser

Utifrån tabellen i stycke 5.5 följer här en ansats att besvara de frågeställningar som initialt formulerades i avsnitt 1.2.

5.8.1 Fördelar och nackdelar mot traditionella lösenord

Man kan se att fördelarna när det gäller traditionella textbaserade lösenord är att det är lättare att minnas en regel än ett ord, eftersom det är lättare att associera den till minnen och upplevelser [2]. Dessutom utför man vid varje inloggning associationen och bedömer vilka bilder som passar till regeln, vilket kan förstärka minnet vid varje inloggning [2, 5].

Genom den höga tillförlitligheten i 5.4.1 ser vi att den interaktion mellan människa och maskin som är en grundförutsättning för tekniken fungerar. Det är möjligt att använda tekniken för att överföra information från människa till maskin utan att budskapet går förlorat. Dessutom är den faktiska informationen gömd i vilka rader som markerats och därför dold för en utomstående observatör, åtminstone vid en första anblick (se avsnitt 5.4.4).

5.8.2 Fördelar och nackdelar mot Weinshall & PassPoint

Fördelen mot PassPoint är att det inte går att finna något mönster i de bilder som markeras, eftersom de slumpas ut. På det sättet är den information som användaren ger ny varje gång. Det går därför inte att analysera koordinaterna för musklicket och finna så kallade hot spots [2], vilka skulle kunna avslöja inloggningen. PassPoint har fördelarna att inloggningsförfarandet är betydligt snabbare och tack vare dess exakthet är det svårt att överföra information från människa till människa. Fördelen mot Weinshalls metod är att man inte behöver någon inlärningsperiod. Både den första (se avsnitt 5.4.1) och sista (se avsnitt 5.4.3) testinloggningen hade hög tillförlitlighet utan träning. Det är också en betydligt mindre mängd information att minnas.

Nackdelen mot Weinshalls metod är att nyckeln går att formulera med ord och därför överföra till andra användare. Till följd av detta är det dock svårt för en användare att lära sig sin Weinshall-inloggning och det är stor risk att delar av denna faller i glömska om den inte används regelbundet.

Den undersökta metoden bygger på samma gränssnitt för att överföra information om inloggningen från användare till dator som Weinshall. Därför

ger de lika mycket skydd mot automatiserad datortestning. Ur denna aspekt är alltså säkerhetsriskerna lika.

5.8.3 Rimlig lösning ur användarens synvinkel

Det är uppenbarligen allt för svårt för en användare att både bedöma vilka bilder som hör till en vagt definierad kontext och samtidigt jämföra objekt med avseende på deras värde (se avsnitt 5.4.3). Däremot kan fiktiva karaktärer markeras på rimligt lång tid och minnesregeln har hög träffsäkerhet (se avsnitt 5.4.2).

Det gränssnitt som använts för att utföra testerna har också visat sig fungera väl och utgör en lämplig modell om tekniken skulle implementeras i ett verkligt IT-system.

5.8.4 Rimlig lösning ur säkerhetssynpunkt

Problemet med att markera fiktiva karaktärer eller hundar är att så gott som alla människor klarar av att göra detta, bara de får reda på regeln som ska tillämpas. Tekniken erbjuder alltså jämförbar säkerhet med traditionella lösenord vad gäller att överföra information om inloggningen till andra individer.

Det är möjligt att testet med kontext-/värdejämförelse (se avsnitt 5.4.3) skulle få ett mer positivt utfall om varje användare först fick skapa sin egen inloggning genom att precisera vilka föremål den ansåg stämde in på associationsregeln. Detta skulle också stärka säkerheten i det att inloggningen skulle bli helt personlig, där denna undersökning strävat efter att jämföra individers generella beteende. Dock borde detta vara en uppgift som är svårlöst för en dator och resultatet är därför positivt ur säkerhetssynpunkt.

En central fråga är huruvida det går att resonera sig fram till den korrekta regeln genom att se på när någon loggar in. För kognitiva lösningar är detta teoretiskt svårt, på gränsen till omöjligt, för en dator att göra men möjligt för en människa tack vare hennes omdöme. I enkätundersökningen framkom en möjlig svaghet med tillvägagångssättet då det fanns åtminstone två olika regler som beskrev en korrekt inloggning. Att ha flera möjliga regler skulle vara detsamma som att ha flera traditionella lösenord som alla var rätt. Om vi betraktar det omvända; att det bara går att finna en passande regel finns risken att den är unik därför att den är uppenbar. Således måste vi dra slutsatsen att det inte går att undvika flera möjliga svar och att antalet korrekta regler inte säger något om säkerheten i tekniken.

I en verklig tillämpning av tekniken bör mängden av bilder vara större än det antal som visas på skärmen vid varje tillfälle. Detta skulle betydligt höja säkerheten mot såväl snokande människor som datoravlyssning.

5.8.5 Fördelar till, eller diskriminering mot vissa användare?

Erfarenhet är en stark begränsning i samtliga tre undersökta regler. De flesta människor har förmodligen en god bild av vad en hund är men någon som inte kan skilja dyra saker från billiga kan inte använda systemet. Likaså kan endast personer som vet att Spindelmannen inte är verklig använda systemet.

Vissa handikapp gör det svårt att använda systemet. Eftersom gränssnittet är av typen peka och klicka finns inga motoriska hinder, utöver de som datoranvändande i allmänhet innebär. Däremot är det högst sannolikt att olika typer av förståndshandikapp skulle vara till stor nackdel för en tänkbar användare då just förståelsen för den regel man tillämpar är högst central i processen.

Vissa psykiska sjukdomar gör att drabbade personer inte kan utföra associerande uppgifter. För att testa patienters sjukdomstillstånd använder man inom psykiatrien en rad olika test som involverar abstrakt tänkande [1]. Gemensamt för dessa test är att de graderar patientens förmåga att hantera förändringar i orientering, uppmärksamhet, minne och intelligens [1]. Enkla frågor som ”På vilken sätt är ett flygplan och en bil lika?” och mer komplicerade som ”På vilket sätt är en målning och ett poem lika?” är exempel på delar av sådana test [1].

Förmågan att korrekt kunna jämföra både fysiska föremål och abstrakta begrepp är absolut nödvändig för att kunna använda de typer av system som presenterats, vilket utesluter personer med nedsatta kognitiva förmågor som användare av tekniken.

6 Diskussion

I avsnitt 1.2 beskrivs de grundläggande frågeställningarna för projektet. Efter att ha gått igenom både resultat och slutsatser i tidigare kapitel återstår nu endast en diskussion kring huruvida den undersökta tekniken kan användas i andra sammanhang än de tidigare föreslagna.

Det finns ännu inte tillräckligt med information för att tekniken ska kunna användas för användaridentifiering i praktiska tillämpningar, den behöver finslipas och testas ytterligare. Dock ges en fingervisning om tänkbara användningsområden och nya spår att följa upp i framtida forskning.

Även om det inte verkar som om den kognitiva tekniken för identitetskontroll i dagsläget hindrar personer från att genomskåda varandras inloggningar så utgör den åtminstone en allvarlig svårighet för datorer att automatiskt avslöja och genomföra inloggningar. Tekniken skulle alltså kunna användas för att skilja människa från maskin (Turingtestet, se 2.1). Det skulle kunna utgöra ett skydd för webbplatser att utnyttjas för distribution av spam (automatiska datoriserade massutskick) genom att införa bildmatris och regel som bekräftelse i mailformulär på webbplatser.

Djupare undersökning ryms tyvärr inte inom ramarna för detta projekt men lämpliga fortsättningar är att arbeta vidare med att hitta karaktäristika för inloggningsregler med hög tillförlitlighet och att undersöka datorers möjlighet att med algoritmer för mönsterigenkänning och bildanalys avslöja minnesreglerna.

7 Avslutande ord

Ibland kan man få känslan av att datorn har kommit till av egen vilja och först därefter har det blivit människans uppgift att handskas med den. Alfabetiska lösenord är ett exempel på just detta. Datorer är makalösa räknemaskiner och därför utmärkta till att räkna ut om ett lösenord är rätt eller fel. Den litteratur som tagits upp i denna rapport visar dock entydigt att människor är dåliga på att båda minnas och hemlighålla sådan information.

Förhoppningsvis kan det här projektet ses som en pusselbit i arbetet att göra oss människor mer involverade i samarbetet mellan människa och maskin. Genom att studera och ta tillvara typiskt mänskliga förmågor i utformningen av ny teknik kan kanske datorn så småningom bli människans bästa vän och kunskapen om detta samarbete kommer förhoppningsvis att tas tillvara både för vardagliga sysslor och säkerhetsfunktioner i framtida system.

Referenser

- [1] Hagop S. Akiskal. The mental status examination. In S. Hossein Fatemi och Paula J. Clayton, editor, *The Medical Basis of Psychiatry*, pages 3–16. Humana Press, 2008.
- [2] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P. C. van Oorschot, and Robert Biddle. Multiple password interference in text passwords and click-based graphical passwords. In *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages 500–511, New York, NY, USA, 2009. ACM.
- [3] Philippe Golle and David Wagner. Cryptanalysis of a cognitive authentication scheme (extended abstract). In *SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 66–70, Washington, DC, USA, 2007. IEEE Computer Society.
- [4] Hugh Loebner. Home page of the loebner prize. <http://www.loebner.net/Prizef/loebner-prize.html>.
- [5] G. William Lycan. *Mind and Cognition: An Anthology*. Blackwell Publishing Ltd., Oxford, UK, 2nd edition, 1999.
- [6] John McLeish. *Matematikens kulturhistoria*. Stockholm Forum, Stockholm, 1996.
- [7] Ian Sommerville. *Software engineering (5th ed.)*. Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA, 1995.
- [8] A. M. Turing. Computing machinery and intelligence. *Mind*, 59:433–460, 1950.
- [9] Daphna Weinshall. Cognitive authentication schemes safe against spyware (short paper). In *SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy*, pages 295–300, Washington, DC, USA, 2006. IEEE Computer Society.

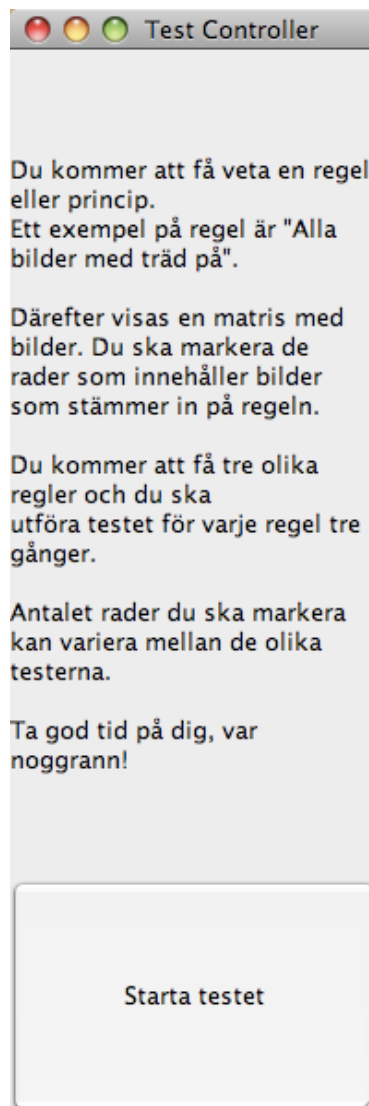
Bilaga A:

Skärmbilder från programmet



Skärmbild 1:

Då programmet startar uppmanas användaren att ange sitt namn.



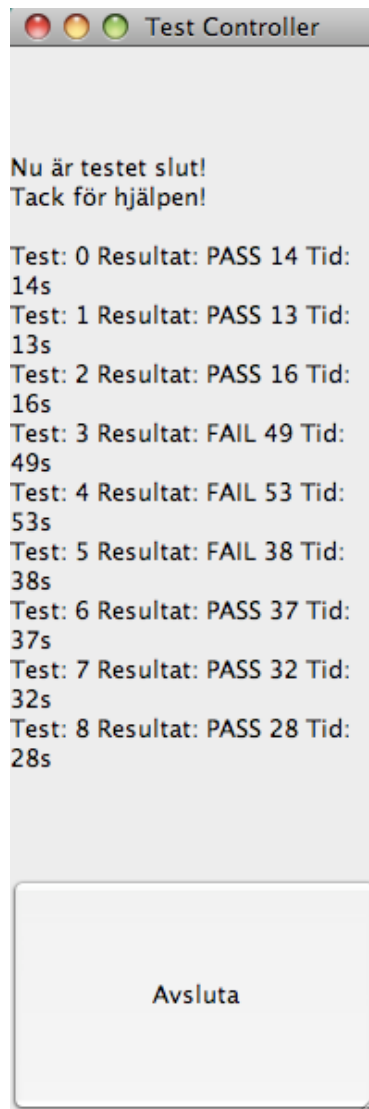
Skärmbild 2:

Efter att namnet lagrats visas denna information för användaren. Knappen startar testet.



Skärmbild 3:

Programmets utseende under drift. Svaren markeras i det mindre fönstret.
Bilderna visas i det stora fönstret med numrerade rader.



Skärmbild 4:

När samtliga test är slutförda visas användarens resultat på de olika delmomenten. Då knappen klickas avslutas programmet.

Bilaga B:

Enkät

Undersökningens andra del

Tänk dig att du tittar över axeln på en person som gör det test du nyss gjorde på datorn. Du ser vilka rader personen markerar men du vet inte vilken regel som används.

Titta på följande tre bilder. De rader som är markerade med en röd rektangel är de rader som personen markerat. Försök lista ut regeln!

Det är inte någon av de regler som ingick i datortestet, men den följer samma typ av logik.

Jag heter: _____

Jag tror att regeln är:

Kommentarer till testet:

1. Första urvalet



2. Andra urvalet



3. Tredje urvalet



