KTH Computer Science
and Communication

Kognitiva autentiseringsmetoder

Ur användarvänlighetens perspektiv

DANIEL GOUCHER
GABRIEL ZAMORE

Examensrapport på grundnivå vid CSC, DD143X, KTH
Handledare: Mikael Goldmann
Examinator: Mads Dam

2011-04-14

Referat

I den här rapporten behandlas ämnet kognitiva autentiseringsmetoder med inriktning på deras användarvänlighet. Anledningen till att vi koncentrerar denna rapport på användarvänligheten är att vi i första hand anser att det är viktigt att inloggningssystem fungerar i det avseendet. Dock så behövs en genomgång av säkerheten för att få en bra helhetsbild av hur autentiseringsmetoder fungerar.

För att undersöka om kognitiva autentiseringsmetoder är en tänkbar metod för inloggningar så går vi igenom flera existerande autentiseringsmetoder och säkerhetsproblem. Detta för att använda som grund till en egen användarvänlig prototyp som utvärderas m.h.a. en användarundersökning. I undersökningen kommer användarnas åsikter om vårt inloggningssystem fram, där det visar sig att användarna kan tänka sig att använda en av våra prototyper. Att användare kan tänka sig att använda kognitiva autentiseringsmetoder är väldigt intressant och området kräver definitivt mer undersökning för att skapa ett inloggningssystem som majoriteten anser är både säkert och användarvänligt.

Abstract

Cognitive Authentication Schemes

In this report the area of cognitive authentication schemes is investigated with a special emphasis on user-friendliness. The reason for this emphasis is that we view the user-friendliness as an important problem to have solved. This emphasis does however not rule out a short analysis of the security of such schemes.

To investigate if cognitive authentication schemes are realistic methods to use for authentication we have researched many different existing authentication schemes and security problems. The reason for this is so that we can use those as a basis for our own prototype which is evaluated using a user survey. Using this survey we have been able to gather the users' thoughts on our prototypes and evaluate them. The results from this survey show that people are open to using one of our prototypes. This is a very interesting result as it suggests that people would be open to switching to a different authentication scheme than the default text based one and that more research into the field is warranted.

Statement of collaboration

I detta projekt så har inga arbetsuppgfiter explicit uppdelats, båda projektmedlemmarna har varit närvarande när allt jobb på projektet har gjorts. Båda har också varit närvarande vid skapandet av prototyp där Daniel hade mer ansvar för kodande och Gabriel för användarundersökningen och skapandet av bilder.

Innehåll

Kapitel 1

Inledning

Vår kandidatuppsats behandlar ämnet kognitiva autentiseringsmetoder. En kognitiv autentiseringsmetod är en metod som förväntar sig att användaren utnyttjar sig av kognitiva mekanismer exempelvis minne och perception, för att bli autentiserad. Tanken med en sådan metod är att minska risken att den som lyckas logga in i systemet är ett program som göra ett otillåtet intrång istället för en människa. Genom att ställa kognitiva krav som enkelt kan uppfyllas av en människa så minskas risken för intrång från automatiserade program eftersom datorer inte kan utnyttja kognitiva mekanismer. Vi ska utreda om det finns något bra sätt att verifiera inloggningar med hjälp av bilder istället för vanliga lösenord bestående av bokstäver och tecken [10].

1.1 Bakgrund

I dagens samhälle är textbaserade lösenord väldigt vanliga för autentisering. Denna typ av lösenord används bland annat av användare för att kolla sin e-post, logga in på sin arbetsdator etc. Fördelen med dessa lösenord är att de är väldigt lättanvända eftersom de väljes av användaren själv och kan därför vara lättare att komma ihåg. Men just på grund av att användaren väljer sitt eget lösenord så finns risken att lösenordets säkerhet minskar. En vanlig person kommer med stor sannolikhet välja ett lösenord som är enkelt att komma ihåg istället för att välja ett mer svårknäckt lösenord som bl.a. innehåller olika specialtecken, siffror, versaler och gemener. En annan nackdel med teckenbaserade lösenord är att de är väldigt känsliga för avlyssning. Detta eftersom en dator inte kan se skillnad på den riktiga användaren och en annan användare som har lyckats ta reda på lösenordet.

Eftersom textlösenord har funnits ett tag och de uppenbarligen har svagheter borde det undersökas vad det finns för alternativ. Några av de alternativen som finns är exempelvis skanning av fingeravtryck, engångslösenord och e-legitimation. Problemen

med de två första (och eventuellt även den tredje) metoderna är att de är beroende av fysiska tillbehör. Fingeravtrycksavläsning behöver någon form av dosa som kan utföra skanningen, engångslösenord behövs hämtas ut och läsas av från papper och vissa e-legitimationer kräver en inloggningsdosa med tillhörande identitetsstärkande kort. Detta gör inloggningarna säkrare men också mer omständliga.

1.2 Syfte

I materialet som vi läst har vi hittat ett flertal olika förslag på kognitiva autentiseringsmetoder samt argument och bevis som förespråkar den ena över den andra. Vårt syfte med denna rapport är inte att hitta den säkraste kognitiva autentiseringsmetoden eftersom vi inte har tillräcklig kunskap om eller erfarenhet av detta område. Istället hade vi tänkt oss att undersöka hur användarvänlig en kognitiv autentiseringsmetod egentligen är. Trots att det kan gå att skapa en extremt säker autentiseringsmetod så kvarstår ett problem; är det någon som praktiskt vill använda den? Syftet med vår rapport är alltså att undersöka om den kognitiva autentiseringsmetod som vi modellerar överhuvudtaget är användbar ur ett användarvänligt perspektiv. Tanken med detta är att undersöka för framtiden om det verkligen är värt att lägga ner tid och pengar på denna typ av kognitiva autentiseringsmetoder om de i praktiken inte är speciellt användarvänliga.

1.3 Problemformulering

Utifrån det vi diskuterade tidigare definierar vi nu vår problemformulering till följande:

”Vilka kognitiva autentiseringsmetoder finns det och är de bra nog för att ersätta de klassiska teckenbaserade lösenorden ur ett användarvänligt perspektiv?”

Med en användarvänlig autentiseringsmetod menar vi en metod som är lika lättanvänd och självklar som en vanlig textbaserad autentiseringsmetod. Andra viktiga faktorer som påverkar är systemets hastighet och smidighet att mata in lösenord.

Kapitel 2

Skapande av prototyp

I enlighet med vår problemformulering har vi undersökt olika typer av kognitiva autentiseringsmetoder, skapat vår egen autentiseringsmetod och uppmanat vanliga användare att utvärdera denna genom att svara på en användarundersökning. Dessutom har vi utrett existerande säkerhetsproblem på Internet som används för att stjäla användares lösenord. Denna kunskap har vi använt oss av för att skapa en prototyp som är framtagen med säkerhetsproblemen i åtanke samtidigt som vi fokuserar på att göra den så användarvänlig som möjligt.

2.1 Säkerhetsproblem

Säkerhet är ett av de stora bekymren när det gäller lösenord. Textlösenord är ett välanvänt system som många anser är säkert. Ett sådant lösenord som exempelvis innehåller 6-7 tecken med en blandning av versaler, gemener, siffror etc tar väldigt lång tid att gissa sig till. Problemet är att människor ofta väljer ett lösenord som de har lätt att komma ihåg istället för ett lösenord som är svårare att knäcka. Svagare lösenord som är lättare att gissa sig till skulle kunna vara namnet på en person i användarens omgivning, exempelvis användarens partner, mamma eller pappa etc. Den typen av information kan vara lätt att få tag på då många personer delar med sig av personlig information över Internet, exempelvis via Facebook [13]. Nu när så mycket av ens personliga information finns tillgängligt för allmän beskådan har det uppstått en giltig anledning till att se över autentisering på Internet.

Idag finns det tre vanliga tekniker som används för att komma åt lösenord, dessa är phishing, keylogging och brute-force attacker. De tre teknikerna fungerar på olika sätt men i slutändan har de alla samma mål: komma åt en användares lösenord. Det som gör dessa tekniker extra skrämmande är att det bara krävs grundläggande programmerings kunskaper för att skapa ett eget program som kan användas för att stjäla en användares lösenord. Det är inte längre bara säkerhetsexperter som kan

stjäla lösenord, det skulle lika gärna kunna vara en 14 årig kille på sina föräldrars pc. Förutom dessa teknologiska verktyg för att stjäla en användares lösenord så finns det enklare varianter, som att helt enkelt tjuvkika på vad en person knappar in på sitt tangentbord, så kallad ”Shoulder surfing”.

2.1.1 Phishing

En av de största säkerhetsproblemen på Internet nu för tiden är phishing. Tekniken bygger på att lura användarna att besöka en falsk hemsida som till utseendet är väldigt lik den riktiga hemsidan. Ett exempel på detta skulle kunna vara att du uppmanas att logga in på din bank via Internet efter att ha fått ett E-postmeddelande som ser ut att vara skickat från din bank. I meddelandet finns det en länk till din banks hemsida och hemsidan du kommer till ser ut som den brukar. Du går sedan till inloggningssidan och skriver in ditt lösenord, efter det kommer det upp en varning som säger att du skrev in fel lösenord. Vad som har hänt är att du lurats att skriva in dina uppgifter på den falska hemsidan, den falska sidan har sedan skickat dig vidare till den riktiga hemsidan som skriver ut en varning att du skrivit in fel inloggningsuppgifter (eftersom du inte har matat in några uppgifter överhuvudtaget på den riktiga hemsidan). Det enda annorlunda var att på sidan där du skrev in ditt lösenord så var adressen i adressfältet några tecken annorlunda från bankens verkliga sida.

Figur 2.1. I exempelbilden ovan kan skillnaden i adressfältet ses mellan den verkliga versionen av PayPal (till vänster) och en påhittad phishing-version av PayPal (till höger).

Som det kan ses i Figur 2.1 så är det väldigt lätt att utsättas för phishing sidor eftersom det kräver att personen som loggar in är väldigt uppmärksam, annars är det svårt att lägga märke till de små ändringarna i adressfältet. En av anledningarna som gör phishing så skrämmande är att det kan ta flera veckor för användaren att upptäcka att ens konto blivit rensat eftersom användaren hela tiden tror att inloggningen skedde till sin bank som vanligt. Phishing-hemsidor är extremt lätta att skapa vilket gör dem ännu mer skrämmande. Allt som behövs är att en person skapar en hemsida, kopierar källkoden från originalsidan och sedan sparar undan allt som skrivs i inloggningsfältet. Detta är något som en person med minimal kunskap inom skapande av hemsidor skulle kunna göra.

Phishingattacker bygger generellt sätt på att en användare klickar på en länk som för en till någon sida där användaren tillbes att mata in sina detaljer. Dessa länkar kan ligga i E-post, forum, hemsidor eller någon annanstans där det kan finnas länkar. Ett bra tips är att helt undvika att klicka på länkar till sidor som kräver inloggning och istället komma ihåg adresserna eller använda bokmärken i webbläsaren [8].

2.1.2 Keyloggers

Ett annat väldigt stort problem med textlösenord är keyloggers. En keylogger är ett typ av program som göms på en användares dator exempelvis med hjälp av ett virus. Keyloggern fungerar på så sätt den ligger och kör i bakgrunden på datorn och sparar alla tryckningar som görs på tangentbordet. Regelbundet skickar keyloggern iväg informationen den samlat in till en dator någonstans som analyserar dessa knapptryck. Det är inte så svårt att tolka vad som är lösenord då de ofta ligger direkt efter något som liknar ett användarnamn eller en E-postadress.

Precis som phishing är keyloggers något som är väldigt lätt att skapa, det krävs bara runt 100 rader kod för att skapa en fungerande version. Oftast så kan en användare skydda sig mot sådan skadlig programvara genom att ha bra antivirusskydd, men hur bra det skyddet än är så kommer den inte att fånga alla virus och keyloggers [7].

2.1.3 Brute-force attacker

Brute-force attacker är en typ av attack där någon sätter igång ett program som sitter och testar alla olika möjligheter av lösenord som kan finnas. Den här typen av attacker finns i många varianter. Ett par exempel på utvidgningar som kan göras av den här tekniken är ordboks- och hybrid- attacker. En ordboksattack är helt enkelt en attack då ett program körs som testar alla ord i ordboken eftersom många användare utnyttjar riktiga ord som lösenord då de är lätta att komma ihåg. Då detta används tillsammans med en ren brute-force attack så blir det en hybridvariant. Programmet som kör en sådan hybridattack går igenom alla ord i

ordboken och testar dem tillsammans med några olika siffror på slutet. Anledningen till detta är att många användare helt enkelt bara lägger till några siffror när ett lösenord ska bytas eller för att en registrering tvingar en användare att ha några siffror i sitt lösenord [11]. Det enda skydd ett system kan ha emot en sådan här attack är att låsa ner konton då de har för många felaktiga inloggningar i rad. Som användare så finns det däremot mer som kan göras, genom att t.ex. ha ett lösenord bestående av 7 tecken som använder alla olika sorters tecken så skulle det ta ca 2 år att komma in på kontot från en vanlig dator [12].

2.1.4 Shoulder Surfing

Ett annat stort problem är så kallad ”Shoulder surfing” som är en teknik då någon observerar vad du trycker in när du loggar in på ett system. Detta har varit ett stort problem för banker då det är relativt enkelt att installera små kameror som tittar på vilka PIN-koder folk trycker in när de hämtar ut pengar från en bankomat eller betalar med sitt kort på en affär [9]. En annan enklare variant av ”Shoulder surfing” är då någon tittar över ens axel då ett lösenord skrivs in, detta är en variant som många ofta glömmer bort eftersom det är svårt (och omständligt) att komma ihåg att alltid titta över axeln då ett lösenord ska skrivas in.

2.2 Kognitiva autentiseringsmetoder

I försök att hitta alternativ till textlösenord har det skapats flera olika typer av kognitiva autentiseringsmetoder. Det gemensamma för dessa metoder är att de ska vara mer motståndskraftiga mot keyloggers/phishing/”Shoulder surfing” där den som vill få tag på en användares inloggningsuppgifter inte ska kunna läsa av vad användaren matar in. I våra efterforskningar har vi hittat olika typer av kognitiva autentiseringsmetoder som vi valt att dela in i två grupper, inmatningsbaserade och klickbaserade grafiska lösenord. I de inmatningsbaserade grafiska lösenorden är det *vad* användaren matar in som har betydelse till skillnad mot de klickbaserade lösenorden där det är *var* inmatningen sker som spelar roll.

2.2.1 Inmatningsbaserade kognitiva autentiseringsmetoder

Dessa grafiska lösenord har vi valt att dela upp i två olika grupper, QPAH (Question public, answer hidden) och QHAP (Question hidden, answer public). Dessa två grupper är vår egen uppdelning av det material vi använt oss av.

QPAH är en typ av kognitiva autentiseringsmetoder där det antas att frågan som användaren skall svara på är tillgänglig för alla men att svaret som användaren matar in inte är entydigt. På detta sätt kan den som läser av användarens svar

inte dra några slutsatser om användarens lösenord. Metoder som vi hittat och som passar in under QPAH har alla samma grund men skiljer sig i hur en användares inmatning sker. Varje användare får en mängd bilder A som bildar användarens bildlösenord. Mängden A är en delmängd av den totala mängden bilder B som innehåller betydligt fler bilder än A.

QHAP är typen av metoder där det antas att frågan som användaren skall svara på är icke-allmän men användarens svar kan läsas av. Utan att veta frågan så ger användarens svar flera tänkbara alternativ till vad lösernordet skulle kunna vara.

QPAH - Bildlabyrint

Denna metod visar en stor matris av bilder tagna från B. Längs den nedre och högra kanten av matrisen är varje rad och kolumn markerad med en siffra 0-3. Användarens uppgift är att navigera sig genom matrisen och slutligen nå antigen den nedre eller högra kanten och mata in siffran från motsvarande rad/kolumn. Användaren startar i det övre vänstra hörnet och förflyttar sig ett steg ner om bilden som för tillfället är aktuell tillhör A, annars förflyttas fokus till bilden ett steg åt höger. Detta upprepas ett flertal gånger och för att bli inloggad krävs det att användaren minst har svarat rätt på ett fördefinierat antal procent av omgångarna [1].

Bildlabyrinten är stark mot alla av säkerhetsproblemen vi tagit upp men lider av att den är väldigt omständlig. Bildlabyrinten är stark mot ”Shoulder surfing” eftersom man inte pekar ut bilderna i sitt lösenord, stark mot phishing och keyloggers eftersom siffrorna som matas in kan inte kopplas till några bilder (svaret är inte entydigt eftersom det finns flera vägar som ger samma svar). För att den ska vara stark mot brute-force attacker måste användaren genomgå många omgångar för bli autentiserad och leder till att metoden är väldigt omständlig, vilket är väldigt dåligt ur en användarvänlig synvinkel.

QPAH - Omplacering av bilder

I denna metod presenteras två stycken lika stora matriser. Den vänstra matrisen innehåller en av bilderna från A och resten av bilderna tillhör B men inte A. Den högra matrisen innehåller samma mängd bilder som den vänstra men de båda matrisernas bilder placeras ut utan hänsyn till varandra. Det är användarens uppgift att flytta om bilden (som tillhör A) i den högre matrisen så att den finns på samma position i både den vänstra och högra matrisen. Endast en bild ska flyttas i varje omgång, om en felaktig bild flyttas misslyckas inloggningen. Övriga bilders placering har ingen betydelse. Efter att ha gjort detta för alla bilder i A är användaren autentiserad [6].

Omplacering av bilder är stark mot phishing och brute-force attacker men är svag mot ”Shoulder surfing” och kan potentiellt vara svag mot keyloggers. Den stora nackdelen med denna metod är att du öppet visar vilken bild som tillhör ditt lösenord. Därför är den uppenbarligen svag mot ”Shoulder surfing” och en smart keylogger skulle exempelvis kunna ta en skärmdump varje gång du klickar med musen och på så sätt se vilket lösenord du har. Omplacering av bilder är även omständlig på grund av att du behöver göra många omgångar för att vara stark mot brute-force attacker.

QHAP - Shoulder Surfing Safe Login

Denna metod används för att autentisera en användare vars lösenord är en PIN-kod. För användaren visas två stycken paneler, den vänstra tittar användaren på och den högra används för inmatning. Den vänstra panelen består av en 5x5 matris där en 3x3 matris i mitten av den stora matrisen har sina rutor lite mörkare än de yttre rutorna. Den inre matrisen är numrerade med siffrorna 1-9 där varje siffra är unik. Ramen (de ljusare rutorna) består av en eller flera av sifforna 1-9 så att varje siffra i de mörka rutorna kan på 0 eller 1 steg nå alla siffrorna 1-9. Den högra panelen består av en 3x3 matris där varje ruta står för en riktning dvs: upp, ner, höger, vänster, stå still, snett uppåt höger, snett nedåt vänster osv, där varje riktning är representerade med hjälp av en pil. För att användaren skall bli autentiserad måste han svara rätt på ett antal frågor, en för varje siffra i sin PIN-kod. Frågan är en framslumpad siffra 1-9 (som bara användaren vet) och denna siffra skall nås från från nuvarande siffra i användarens PIN-kod. Om den framslumpade siffran (dvs frågan) befinner sig snett nedåt höger i förhållande till nuvarande siffra i PIN-koden så skall användaren svara ”snett nedåt höger” i den högra panelen [5].

SSSL är stark mot keyloggers, phishing och shoulder surfing men svag mot brute-force attacker. Den är stark mot keyloggers, phishing och ”Shoulder surfing” på grund av att svaret man skickar in inte är entydigt och därför kan inga slutsatser dras om lösenordet. SSSL är svag mot brute-force attacker eftersom totala antalet valmöjligheter är väldigt liten och kan därför testas med enkelhet.

2.2.2 Klickbaserade kognitiva autentiseringsmetoder

En sådan här typ av autentiseringsmetod går ut på att en användare klickar på olika objekt för att verifiera sin identitet. Ett exempel på en sådan metod är då ”PassPoints” som beskrivs i mer detalj nedan.

PassPoints

I denna metod som vi hittat tilldelas varje användare en bild i hög upplösning. I bilden ”gömmer” användaren själv ett antal punkter eller så kallade ”hotspots”. Dessa punkter göms med en viss felmarginal så att användaren inte skall behöva pricka rätt på den exakta pixeln. För att bli autentiserad krävs det helt enkelt att användaren hittar (dvs klickar på) alla sina hotspots i rätt ordning [3].

En sådan metod är bra mot brute-force attacker eftersom det finns väldigt många olika valmöjligheter som måste testas. Däremot är den svag mot ”Shoulder surfing”, avancerade keyloggers (som tar skärmdumpar vid musklick) och phishing eftersom inmatningen kan avläsas.

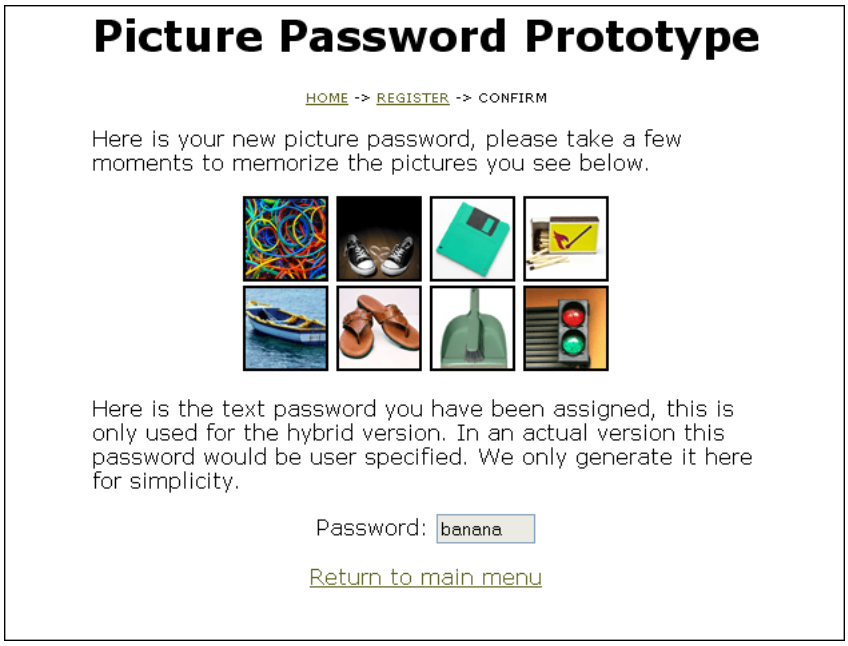
Figur 2.2. I bilden finns användarens ”hotspots” ritade i form av röda kvadrater. För att bli autentiserad krävs det att användaren klickar inom alla kvadraterna i rätt ordning (kvadraterna visas självklart inte vid inloggningen).

2.3 Design av prototyp

Efter att ha undersökt de olika typerna av kognitiva autentiseringsmetoder så bestämde vi oss för att göra en inmatningsbaserad prototyp. Detta eftersom vi anser

att en inmatningsbaserad prototyp kommer att kännas mer bekant för en vanlig användare än en klickbaserad prototyp då textlösenord också inmatningsbaserad. Vi anser att den inmatningsbaserade metoden ska vara av typen QPAH. Det valet har sin grund i att vi vill göra det så lätt för användaren som möjligt, då vi tror att det kan bli för komplicerat med en autentiseringsmetod som slumpar fram olika frågor varje omgång (istället för att använda samma fråga varje omgång). Av de två QPAH-metoderna ”Labyrint” och ”Omplacering av bilder” så tycker vi att ”Labyrint” är för omständlig och ”Omplacering av bilder” dålig ur en ”Shoulder surfing”-synvinkel eftersom användaren kan tvingas att peka ut sina bilder ur lösenordet. Vi valde därför att skapa en egen metod som utgår från grunden av en QPAH-metod men ska vara så simpel att varje vanlig användare skall kunna använda den samtidigt som vi har säkerhetsproblemen i åtanke.

Vår prototyp valde vi att dela upp i två mindre prototyper, en ”Image only version” och en ”Hybrid version”. Varje användare måste registrera sig och tilldelas då ett slumpat bildlösenord (används i båda versionerna) som består av 8 bilder plockade från den totala mängden av ca 200 st bilder samt ett textlösenord (används i ”Hybrid version”).



Figur 2.3. Bilden visar en användares text- och bildlösenord.

För att bli autentiserad krävs det att användaren svarar rätt på alla frågor (omgångarna). Inför varje omgång slumpar systemet fram en icke tidigare använd bild ur användarens bildlösenord samt 48 bilder från den totala bildmängden där bilden ur bildlösenordet inte är samma som någon av de 48 bilderna från den totala bildmängden. De 49 framslumpade bilderna placeras i en matris med 7 rader och 7 bilder på

varje rad. Till vänster om matrisen skapas en kolumn med ”radio buttons” för att användaren bara ska kunna välja en av raderna. Kolumnen och matrisen visas för användaren och uppgiften (eller frågan) är nu att välja den rad som innehåller en bild från sitt bildlösenord. Detta upplägg kan ses i Figur 2.6.

I designen av vår prototyp lånade vi egenskaper från de olika varianterna av autentiseringsmetoderna som vi ansåg skulle göra vår prototyp så användarvänlig och säker som möjligt. De viktigaste säkerhetsproblemen som behövdes lösas var phishing och keyloggers eftersom dessa två tekniker ställer till mest problem för lösenord idag. Lösningen till detta problem blev att låta användaren välja en mängd av bilder (en rad) där en av bilderna tillhör bildlösenordet. Detta steg upprepas flertalet gånger tills chansen att gissa sig till lösenordet blir tillräckligt liten. Ett sådant litet steg som detta ställer till rejäla problem för phishing och keyloggers då de två teknikerna bygger på att informationen som användaren skriver in är entydig. Däremot så har en variant som denna vissa problem i att den skulle kunna uppfattas som seg och att den inte har lika stor säkerhet mot brute-force attacker som vanliga textlösenord. Detta var anledningen till att vi också bestämde oss för att göra en hybrid variant där de bästa av båda varianterna tas med. Idén till att använda en två-stegs säkerhetslösning fick vi från [4] där samma idé används. I hybrid varianten måste användaren först skriva in ett textlösenord innan man får tillgång till omgångarna med bilder. Då har prototypen både skydd mot phishing och keyloggers, samt skydd mot brute-force attacker.

2.3.1 Image only version

Denna prototyp använder sig enbart av bilder för att autentisera en användare. För att bli autentiserad krävs det att användaren matar in ett godkänt användarnamn och svarar rätt på alla omgångar. Vi har valt att låta användaren genomlöpa 6 omgångar.

Figur 2.4. Bilden visar inloggningsskärmen för ”Image only version”.

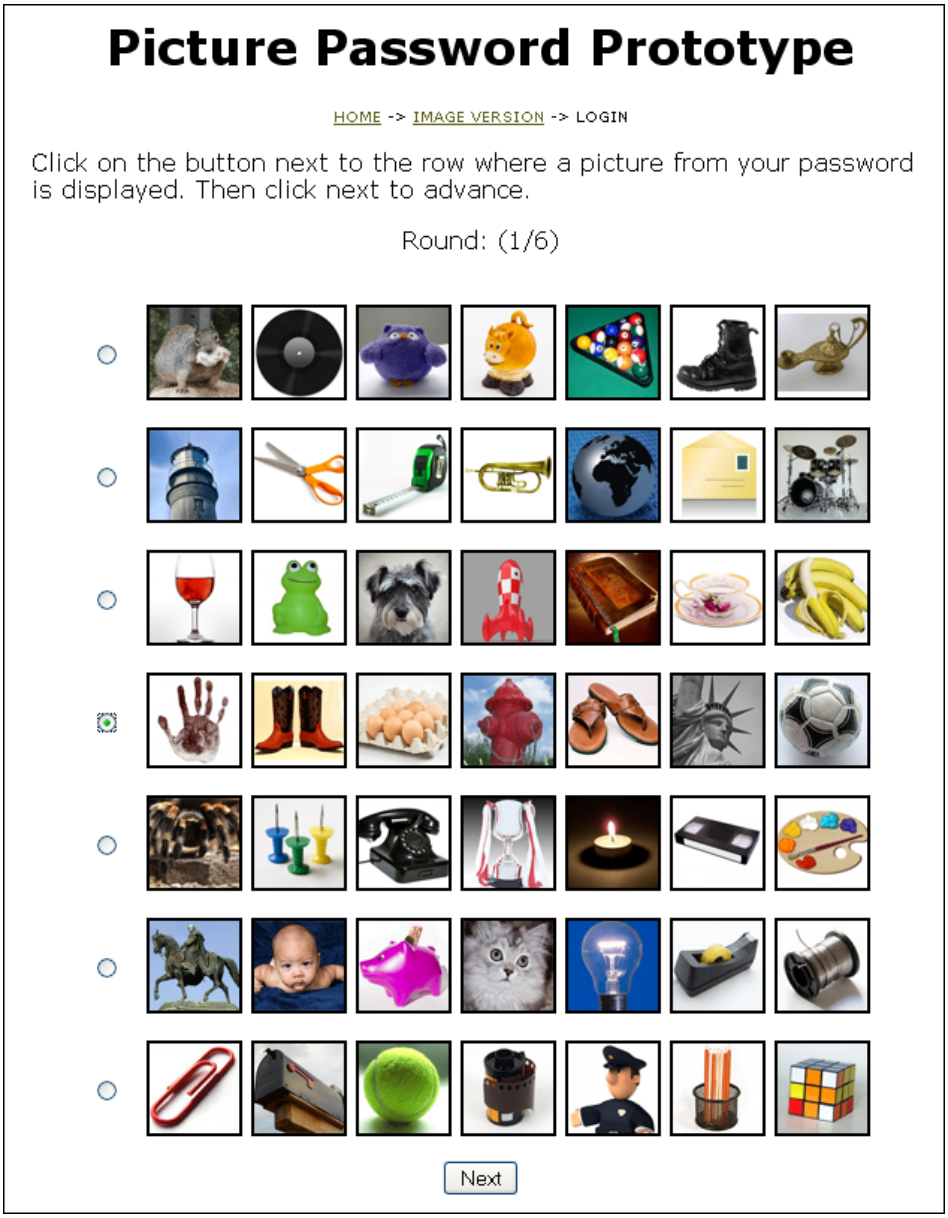
2.3.2 Hybrid version

Denna prototyp använder sig av ett textlösenord och bilder för att autentisera en användare. För att bli autentiserad krävs det att användaren matar in ett godkänt användarnamn, textlösenord och svarar rätt på alla omgångar. I denna version har vi har valt att låta användaren genomlöpa 3 omgångar istället för 6 som i ”Image only version”. Sänkningen av antal omgångar har vi gjort eftersom vi har gjort inloggningen ”jobbigare” eftersom användaren nu måste komma ihåg sitt textlösenord.

Figur 2.5. Bilden visar inloggningsskärmen för ”Hybrid version”.

2.3.3 Autentiseringssvy

Denna vy visas för användaren i varje omgång i autentiseringsprocessen. Antalet omgångar beror på vilken prototyp användaren använder; 3 omgångar för ”Hybrid version” och 6 omgångar för ”Image only version”.



Figur 2.6. Bilden visar en inloggningsomgång för prototyperna, antalet omgångar beror på vilken prototyp som används.

2.4 Användarundersökning

Utöver vår prototyp har vi även skapat en enkät som vi uppmanade användarna att fylla i. Eftersom vi undersöker hur användarvänlig vår prototyp är så försökte vi skapa en bra undersökning som täcker in de delar av prototypen som vi tror kan upplevas som jobbiga eller omständliga. Vi passade även på att fråga om användarnas inställning till våra prototyper kontra vanliga textlösenord. Enkäten finns i sin helhet i Bilaga A.

Exempel på saker som vi frågade om var antalet omgångar som användarna skulle tänka sig att svara på och om någon av användarna skulle kunna tänka sig att ersätta sina textlösenord till förmån för någon av våra prototyper.

Kapitel 3

Resultat

Detta kapitel är uppdelad i två delar; i sektion 3.1 analyserar vi resultatet från vår användarundersökning och i sektion 3.3 diskuterar vi analysen och försöker dra slutsatser.

3.1 Analys av användarundersökning

I denna sektion presenterar vi resultaten från vår användarundersökning. Ur denna undersökning har vi hittat några gemensamma åsikter och trender som vi diskuterar nedan. Totalt sätt fick vi in 36 svar på användarundersökningen, se Bilaga A.

3.1.1 Träningssession

Många av användarna upplevde det som svårt att komma ihåg sitt bildlösenord. Detta tror vi beror på att användarna har tagit sig för lite tid till att memorera bilderna och hoppat på inloggningarna direkt. Vi har noterat i statistiken från vår databas att många användare försöker logga in och ger upp om första försöket misslyckas. Ett sätt att motivera användarna att lära sig sina bildlösenord ordentligt är att införa någon form av träningsläge. I träningsläget ska användarna kunna träna på sitt bildlösenord innan de testar i ”skarpt läge”. Ett exempel på ett sådant läge skulle vara att köra vår inloggningsprocess som vanligt och om användaren gör fel markeras den korrekta bilden så att användaren lär sig den.

3.1.2 Välja/lägga till egna bilder

Som tidigare sagt så har användarna svårt att komma ihåg sina bilder. Ett lösningsförslag som vi fick från enkäten är att låta användarna själva välja sitt bildlösenord

ur den totala mängden av bilder. Flera användare skulle förmodligen uppleva det som lättare att komma ihåg sitt lösenord men riskerar samtidigt att sänka lösenordets säkerhet. Detta eftersom det finns en risk att många användare väljer bilder till sitt bildlösenord som är populära och därför lättare att gissa sig till.

Ett annat förslag är att användarna skulle vilja ladda upp sina egna bilder och använda dessa i sitt bildlösenord. Möjligheten för användaren att ladda upp egna bilder är implementerbart men skulle medföra flera problem. Exempelvis så finns det då inget som hindrar olika användare att ladda upp snarlika bilder som är svåra att urskilja eller bilder av dålig kvallitet som ger programmet minskad trovärdighet.

3.1.3 Användarvänlighet

I användarundersökningen ställde vi konkreta frågor som användes för att ta reda på användarnas syn på våra prototyper och om de skulle kunna tänka sig att använda dem. Den första frågan som ställdes till användarna behandlade användarvänligheten av våra system, vi bad dem betygsätta detta på en skala av 1 till 10. ”Image only version” fick ett medelbetyg av 5,75 medan ”Hybrid version” fick 7,26. Med hjälp av dessa data så kan det sägas med rätt stor säkerhet att ”Hybrid version” är den som majoriteten av användarna föredrar att använda när det kommer till användarvänlighet.

	Image only version	Hybrid version
How would you rate our prototypes in terms of user friendliness?	5,75	7,26
How secure do you feel using our prototypes?	7,49	7,86

Tabell 3.1. Tabellen visar frågorna som ställdes och till höger resultaten: ett medelvärde av svaren vi fick då vi bad användarna betygsätta prototypen på en skala mellan 1 och 10.

Den andra frågan vi ställde handlade om hur säkra användarna kände sig när de använde våra prototyper, även här bad vi användarna betygsätta på en skala av 1 till 10. I det här fallet så fick ”Image only version” 7,49 medan ”Hybrid version” fick 7,86 i medelvärde. Här kan det ses att ”Hybrid version” upplevs av användarna som säkrast, även om ”Image only version” också anses som säker.

Då frågorna om användarvänlighet och säkerhet hade ställts så bad vi användarna svara på frågor mer relaterade till vår implementation av prototypen och hur de skulle vilja ha den. Den första frågan vi ställde var om hur många bilder per rad en användare skulle vilja se. Medelvärdet av det svaret blev då 4,75 vilket är betyd-

ligt minder än 7 som vi hade satt som standard. Detta är något som skulle kunna implementeras utan att dra ner alltför mycket på säkerheten. Den enda skillnaden det skulle skapa är att det skulle bli lite lättare att gissa vilken bild som tillhör lösenordsmängden då någon ser en inloggning.

How many pictures per row would you like to have in one round of questioning?	4,75

Tabell 3.2. Tabellen visar ett medelvärde av svaren vi fick när vi bad användarna svara på hur många bilder som skulle visas på varje rad vid en inloggning. Värdet som användes i prototypen var 7.

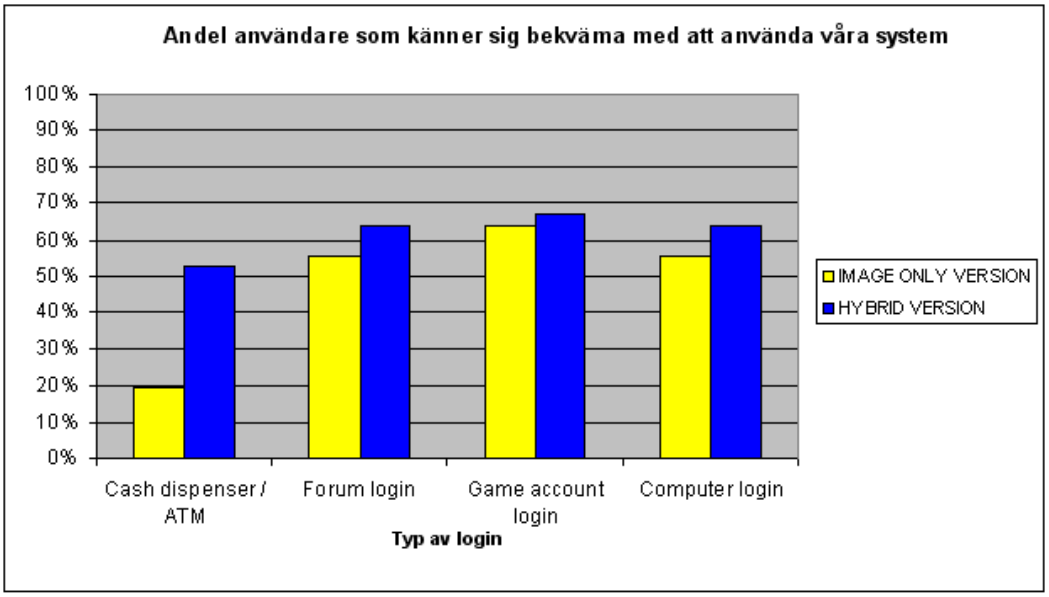
En annan fråga vi ställde till användarna var hur många omgångar de skulle vilja svara på i varje implementation. Här fick vi svaren att ”Image only version” hade ett medelvärde på 4,71 omgångar och ”Hybrid version” ett medelvärde på 3,41 omgångar. I vår implementation så hade vi 6 omgångar i ”Image only version” och 3 omgångar i ”Hybrid version”. Som kan ses på datat så tycker användarna att ”Image only version” tar för lång tid och vill ha mindre omgångar medan ”Hybrid version” har ungefär rätt antal omgångar. Svaret som vi fick från ”Image only version” utför ett ganska stort problem för den prototypen då mindre än 6 omgångar skulle innebära en alltför dålig säkerhet mot brute-force attacker. Detta eftersom det helt enkelt inte skulle finnas tillräckligt med olika möjliga svar för att stoppa en sådan attack i en längre tid.

	Image only version	Hybrid version
How many question rounds would you like to answer in our prototypes?	4,71	3,41

Tabell 3.3. Tabellen visar ett medelvärde av svaren vi fick när vi bad användarna svara på hur många omgångar som de ansåg borde besvaras innan en inloggning i båda prototyperna.

3.1.4 Användningsområden

En fråga som vi också ställde till användarna var om de skulle kunna tänka sig att använda en eller båda av våra prototyper i riktiga scenarion, exempelvis vid uttag av pengar vid en bankomat eller inloggning på sin dator. I Figur 3.1 kan resultatet från en sådan fråga beskådas.



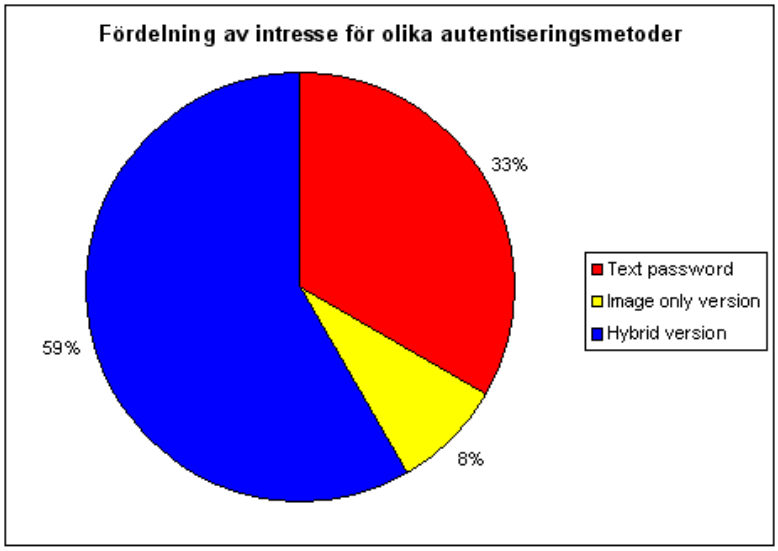
Figur 3.1. Figuren visar hur stor andel av användarna skulle känna sig bekväma att använda våra inloggningssystem vid olika typer av situationer.

Detta är en avgörande fråga för framtiden då resultatet kan ge en hint om hur intresserade användarna är av att använda en kognitiv autentiseringsmetod. Resultatet i denna fråga visar tydligt att över hälften av de tillfrågade skulle känna sig bekväma med att använda ”Hybrid version” i alla fyra olika scenarion och ”Image only version” i tre av fyra scenarion.

Utifrån dessa resultat kan man alltså dra slutsatsen att kognitiva autentiseringsmetoder är någonting som skulle accepteras av användarna.

3.1.5 Hybrid version: det nya textlösenordet?

Den sista frågan i vår undersökning är också en av de mest intressanta. Vi frågade användarna vilken av de tre autentiseringsmetoderna (textlösenord, image only version eller hybrid version) de skulle välja om de bara fick välja en. Resultatet kan beskådas i Figur 3.2. Överraskande så var det ”Hybrid version” som med stor majoritet som var den mest omtyckta autentiseringsmetoden.



Figur 3.2. Figuren visar vilken typ av inloggning som användarna helst skulle använda i majoriteten av fallen. Här kan det avläsas att 59% av användarna valde ”Hybrid version”.

3.2 Analys av prototypens säkerhet

I detta avsnitt analyserar vi säkerheten för textlösenord samt våra prototyper; ”Image only version” och ”Hybrid version”. I tabell 3.4 har vi listat upp de olika formlerna som används för att räkna ut sannolikheten att gissa en användares lösenord för de olika autentiseringsmetoderna. Nedan finns en lathund som förklarar de olika variablerna i formlerna.

t = antal unika tecken som finns tillgängliga

n = längden av textlösenordet

r = antal rader att välja mellan vid varje runda av inloggning

m = antal rundor

s = chansen att en person gissar rätt lösenord

Textlösenord	$s = (1/t)^n$
Image only version	$s = (1/r)^m$
Hybrid version	$s = (1/t)^n * (1/r)^m$

Tabell 3.4. Den här tabellen visar formler för beräkning av chansen att gissa lösenordet i de olika autentiseringsmetoderna.

Fördelen med ”Image only version” är att den är motståndskraftig mot keyloggers, phishing och ”Shoulder surfing” eftersom användaren vid inloggning inte explicit matar in sitt lösenord (väljer en rad av bilder istället för enskilda bilder). Nackdelen med ”Image only version” är den är mycket svag mot brute-force attacker eftersom sannolikheten att gissa sig igenom inloggningen är betydligt högre än vanliga textlösenord. Hur bra de olika autentiseringsmetoderna är mot brute-force attacker kan ses i tabell 3.5. Tanken med ”Image only version” är att den ska vara användarvänlig och för att höja säkerheten måste antalet valbara rader ökas eller/och öka antalet omgångar. Om den förändring skulle göras kommer användarvänligheten för ”Image only version” sjunka, alltså helt i strid med målet med vår prototyp.

I tabell 3.5 nedan så kan det avläsas hur stor chans det är för ett program att gissa sig till lösenordet i de olika autentiseringsmetoderna. Vi antar här att textlösenordet kan bestå av ca 80 olika tecken; stora och små bokstäver, siffror och specialtecken.

	10000 försök	100000 försök	1000000 försök
Textlösenord	0,00000305%	0,0000305%	0,000305%
Image only version	8,49%	84,9%	>100%
Hybrid version	0,00000000891%	0,0000000891%	0,000000891%

Tabell 3.5. Den här tabellen visar chansen för att ett lösenord knäcks i de olika autentiseringssystemen när olika antal försök görs.

Den stora fördelen med att använda textlösenord är att sannolikheten att gissa sig till ett sådant lösenord är väldigt liten vilket leder till att denna typ av lösenord är motståndskraftiga mot brute-force attacker. Nackdelen med denna denna typ av lösenord är att de är väldigt känsliga mot keyloggers, phishing och ”Shoulder surfing”

eftersom du explicit matar in ditt lösenord. Är det någon som tjuvlyssnar på vad du som användare skriver in är det enkelt för avlyssnaren att använda användarens uppgifter för sina egna behov. En annan stor nackdel med sådana lösenord är att användare ofta använder lösenord som är lätta att komma ihåg vilka också är lätta att gissa.

I "Hybrid version" kombinerar vi egenskaperna hos textlösenord med egenskaperna hos "Image only version" för att skapa en autentiseringsmetod som komplimenterar varandra. "Hybrid version" är en säkrare autentiseringsmetod än både textlösenord och "Image only version" eftersom det nu finns ett extra lager av säkerhet som löser svagheterna hos respektive autentiseringsmetod. Eftersom det finns ett extra lager av säkerhet går det att mellan varje lager kolla att användaren faktiskt klarade autentiseringen för detta lager. Om det visar sig att användaren misslyckas på ett eller flera lager nekas användaren åtkomst. För att förhindra brute-force attacker kan en gräns sättas för hur många misslyckade inloggningar en användare får göra. Denna gräns sätts då på den kognitiva delen, för om en användare klarar textlösenordet men misslyckas på kognitiva delen så är det troligt att det inte är den korrekta användaren som försöker logga in.

3.3 Diskussion

Innan användarundersökningen genomfördes var vi båda ganska säkra på att det fortfarande skulle vara textlösenorden som var den populäraste autentiseringsmetoden. Det visade sig tydligt att vi hade fel då hela 59% av de svarande användarna valde "Hybrid version", en av våra egna prototyper. Det verkar alltså som att användarna är medvetna om att de klassiska textlösenorden har stora brister och är villiga att byta ut dem. Detta endast om det finns ett nytt system som erbjuder bättre säkerhet utan att nedprioritera användarvänligheten allt för mycket. Därför anser vi att kognitiva autentiseringsmetoder är någonting som det finns ett intresse för bland vanliga användare och är något som behövs undersökas i större skala. En större undersökning behövs genomföras eftersom vår undersökning enbart består av 36 st svarande användare och kan ge en missvisande bild av hur stort intresset egentligen är för kognitiva autentiseringsmetoder.

För att "Hybrid version" skall vara användbar i ett riktigt system bör det implementeras någon form av spärr som hindrar användaren från att logga in om textlösenordet är rätt men användaren misslyckats med ett antal bildinloggningar. På så sätt stoppar man brute-force attacker som annars skulle kunna lyckas logga in med hjälp av rena chansningar. För att åter kunna använda sitt konto måste användaren återaktivera det via mail där användaren får ett nytt text- och bildlösenord.

I dagens samhälle finns det många säkerhetsrisker, exempelvis på Internet där

många av de vanliga användarna är villiga att dela med sig av sin personlig information. Eftersom den personliga informationen redan finns tillgänglig och är förmodligen omöjlig att ta tillbaka måste förändringen ske på säkerhetssidan. Enligt vår undersökning finns det ett intresse för kognitiva autentiseringsmetoder och nytänkande när det gälla autentisering. På grund av dessa resultat anser vi att kognitiva autentiseringsmetoder är något som bör undersökas mera och kan i framtiden ersätta textlösenorden om intresset är tillräckligt stort.

Litteraturförteckning

[1] Daphna Weinshall: Cognitive Authentication Schemes Safe Against Spyware (2011-04-14)
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=\&arnumber=1624019

[2] Golle and Wagner: Cryptanalysis of a Cognitive Authentication Scheme (2011-04-14)
http://crypto.stanford.edu/~pgolle/papers/sat.pdf

[3] Sonia Chiasson Robert Biddle P.C. van Oorschot: A Second Look at the Usability of Click-Based Graphical Passwords (2011-04-14)
http://www.scs.carleton.ca/~schiasso/Chiasson_SOUPS2007_Click_based_GP.pdf

[4] P.C. van Oorschot: TwoStep: An Authentication Method Combining Text and Graphical Passwords (2011-04-14)
http://www.ccsl.carleton.ca/paper-archive/van-Oorschot-MCETECH-09.pdf

[5] T. Perkovic', M. C' agalj, N. Rakic: SSSL: Shoulder Surfing Safe Login (2011-04-14)
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5306871

[6] Kenneth Revett, Hamid Jahankhani, Sérgio Tenreiro de Magalhães, and Henrique M.D. Santos: User Dynamics in Graphical Authentication Systems (2011-04-14)
http://www.springerlink.com/content/n30p1526013n44k3/fulltext.pdf

[7] Stefano Ortolani, Cristiano Giuffrida, Bruno Crispo: Bait your Hook, A Novel Detection Technique for Keyloggers (2011-04-14)
http://www.cs.vu.nl/~giuffrida/papers/raid-2010-talk.pdf

[8] S. H. Khayal, A. Khan, N. Bibi and T. Ashraf: Analysis of Password Login Phishing Based Protocols for Security Improvements (2011-04-14)
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5353144

[9] European Network and Information Security Agency (ENISA): ATM crime, Overview of the European situation and golden rules on how to avoid it (2011-04-14)
http://www.enisa.europa.eu/act/ar/deliverables/2009/atmcrime/at_download/fullReport

[10] Martin Karlsson: Kognitiv Psykologi (2011-04-14)
http://webstaff.itn.liu.se/~marka/TNMK31-2006/fo3.pdf

[11] Rob Shimonski: Hacking Techniques, Introduction to password cracking (2011-03-27)
http://www.ibm.com/developerworks/library/s-crack/index.html

[12] John Pozadzides: How I'd Hack Your Weak Passwords (2011-03-27)
http://onemansblog.com/2007/03/26/how-id-hack-your-weak-passwords/

[13] Joan Goodchild: 10 Security Reasons to Quit Facebook (And One Reason to Stay On) (2011-04-14)
http://www.csoonline.com/article/584813/10-security-reasons-to-quit-facebook-and-one-reason-to-stay-on-

Bilaga A

Enkät

What username did you use for the prototype?

What is your Internet experience level?

	1	2	3	4	5	
Novice						Advanced

How would you rate the "Image only version" in terms of user friendliness?

	1	2	3	4	5	6	7	8	9	10	
Terrible											Excellent

How would you rate the "Hybrid version" in terms of user friendliness?

	1	2	3	4	5	6	7	8	9	10	
Terrible											Excellent

How secure do you feel using the "Image only version"?

	1	2	3	4	5	6	7	8	9	10	
Extremely insecure											Extremely secure

How secure do you feel using the "Hybrid version"?

	1	2	3	4	5	6	7	8	9	10	
Extremely insecure											Extremely secure

How many pictures per row would you like to have in one round of questioning?
In our prototypes we are using seven pictures per row. How many would you like to have?

- 3
- 4
- 5
- 6
- 7
- 8+

How many question rounds would you like to answer in the "Image only version"?
In the "Image only version" we are using six rounds of questioning. How many would you like to have?

- 3
- 4
- 5
- 6
- 7
- 8+

How many question rounds would you like to answer in the "Hybrid version"?
In the "Hybrid version" we are using three rounds of questioning. How many would you like to have?

- 2
- 3
- 4
- 5
- 6+

In which scenarios would you feel comfortable using the "Image only version" for authentication?

- Cash dispenser / ATM
- Forum login
- Game account login (e.g. WoW, Xbox Live, FIFA UT)
- Computer login
- Other:

In which scenarios would you feel comfortable using the "Hybrid version" for authentication?

- Cash dispenser / ATM
- Forum login
- Game account login (e.g. WoW, Xbox Live, FIFA UT)
- Computer login
- Other:

If you had to use one of the following types of authentication, which one would you pick?

- Text password
- Image only version
- Hybrid version

Any other comments?