Ett keylogger-resistent bildbaserat inloggningssystem

GUSTAV HEDIN
och ALEXANDER SAMUELSSON

KTH Datavetenskap
och kommunikation

Examensarbete
Stockholm, Sverige 2010

Ett keylogger-resistent bildbaserat inloggningssystem

G U S T A V H E D I N
o c h A L E X A N D E R S A M U E L S S O N

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

URL: www.csc.kth.se/utbildning/kandidatexjobb/datateknik/2010/hedin_gustav_OCH_samuelsson_alexander_K10069.pdf

Kungliga tekniska högskolan
Skolan för datavetenskap och kommunikation

KTH CSC
100 44 Stockholm

URL: www.kth.se/csc

Ett keylogger-resistent bildbaserat inloggningssystem

Sammanfattning

Vi har utvecklat två bildbaserade autentiseringssystem, där ett skyddar mot traditionella keyloggers. Systemen består av en matris av bilder med tillhörande tecken, och en användare autentiserar sig mot systemet genom att ange en teckensekvens som motsvarar en tidigare vald bildsekvens. Det ena systemet slumpar bildernas position inför varje inloggningsförsök så att en teckensekvens bara går att autentisera sig med en gång. Det andra systemet har fasta bildpositioner.

Vi har låtit användare testa systemen och därefter låtit dem svara på en anonym enkät på Internet, där de fått svara på frågor om systemens användbarhet och jämföra dem mot engångslösenord. Vi har också utvärderat våra system mot textbaserade autentiseringssystem och engångslösenord ur säkerhetssynpunkt.

Data från enkäten visade att de flesta användare tyckte att det var svårt att autentisera sig mot systemet med slumpmässiga bildpositioner, men att de föredrog det systemet över det med fasta bildpositioner för att komma åt känslig data. I slutet av rapporten diskuterar vi hur systemen kan förbättras både ur användbarhets- och säkerhetssynpunkt.

A keylogger resistant picture based authentication scheme

Abstract

We have implemented two picture based authentication schemes of which one is resistant to traditional key logging software. The systems consists of a matrix of pictures with corresponding characters, where a user authenticates by entering a character sequence that corresponds to a sequence of pictures previously defined. In one of the implementations, the picture order in the matrix is randomly generated before each login attempt, so that the character sequence that a user authenticate with will be useless for future authentications. In the other system the picture positions are fixed.

The systems have been tested by users which have then answered an online survey where the usability of the systems have been rated and compared to that of one time passwords. We have also compared our implementations against text based authentication and one time passwords in a safety point of view.

Data from our survey showed that most people find it hard to authenticate using random image positions, but that they prefered that system over that with fixed image positions for accessing sensitive information. In the end of the report we discuss how to increase both security and usability of the authentication systems.

Förord

Detta är en kandidatexjobbsrapport vid CSC, KTH inom datalogi. Vår handledare under perioden som denna rapport skrivits har varit Cristian Bogdan, vi vill tacka Cristian och alla de som var med i vår undersökning.

Implementationen av prototypsystemen har skrivits av Alexander Samuelsson med hjälp av ideér från Gustav Hedin. Rapporten har skrivits av oss båda och bara arbetats på när båda parterna varit närvarande.

Innehållsförteckning

Förord....3
Inledning....4
Bakgrund....5
Syfte....5
Problemformulering....5
Teori....6
Hot....6
Hotet från keyloggers....6
Van Eck-phreaking och Shoulder surfing....6
Olika typer av inloggningssystem....7
Grafiska inloggningssystem....7
Engångslösenord....7
Biometriska inloggningssystem....8
Våra system....8
Metod....9
Användbarhetstest....9
Säkerhetsanalys....9
Resultat....9
Säkerhetshot....9
Hotet från traditionella keyloggers....9
Hotet från avancerade keyloggers....10
Mappning....10
Brister i slumptalsgenerering....10
Van Eck-phreaking och Shoulder surfing....11
Användartest....11
Lättare att logga in med fasta bildpositioner....11
Jämförelse med engångslösenord....12
Diskussion....13
Förslag till förbättringar....13
Slutsats....14

Inledning

Inloggningssystem, eller autentiseringssystem, är något de flesta människor använder flera gånger om dagen. Olika system måste autentisera dig när du ska ta ut pengar, när du ska läsa din e-post, när du använder ditt nyckelkort på jobbet, och vid flera andra tillfällen.

Det kanske vanligaste sättet för ett system att autentisera en användare är genom textbaserade lösenord. Inloggningssystem som parar ihop användare med textsträngar har dock en rad svagheter, framförallt ur ett säkerhetsperspektiv. Det är vanligt att användare väljer ord som förekommer i ordlistor, eller som har en direkt koppling till användaren i fråga. Detta gör att mängden teckensträngar som behöver testas för att forcera en användares autentiseringsnyckel är betydligt mindre än antalet möjliga teckenkombinationer. Dessutom finns det metoder för att registrera det en användare skriver på sitt tangentbord, vilket kan ge en tredje part dennes lösenord i klartext.

Då datorer nuförtiden inte nödvändigtvis behöver ta indata från ett tangentbord och visa utdata i en text-terminal så finns det möjlighet att skapa mer avancerade inloggningssystem som har andra svagheter och styrkor än dagens textbaserade motsvarigheter.

Bakgrund

En keylogger är programvara eller hårdvara som registrerar de tangenttryckningar som en datoranvändare genererar. Mer avancerade keyloggers har även funktioner för att ta skärmdumpar eller registrera muspekarens position vid olika tidpunkter eller händelser[1].

Egenskaperna hos en keylogger gör den till ett allvarligt säkerhetshot mot vissa inloggningssystem och användares integritet. Trots detta används fortfarande system som är sårbara för denna typ av attacker i stor utsträckning.

Det finns en rad olika tekniker för att skydda inloggningssystem mot keyloggers, där en del grafiska inloggningssystem utgör en delmängd.

Syfte

Syftet med denna rapport är att undersöka två av oss utvecklade bildbaserade inloggningssystem, ett med fasta bildpositioner och ett med slumpmässiga, och att låta några personer testa och utvärdera systemen. Med hjälp av användartesterna och egna jämförelser hoppas vi kunna identifiera eventuella problem med våra implementationer och få förslag till förbättringar ur ett användar- och säkerhetsperspektiv. Denna information kan förhoppningsvis användas av oss eller läsare av rapporten för att utveckla framtida lösenordssystem eller förbättra befintliga implementationer.

1 Sachin Shetty, "Introduction to Spyware Keyloggers" (6 April, 2010): http://www.symantec.com/connect/articles/introduction-spyware-keyloggers

Problemformulering

Denna rapport ska besvara följande fyra huvudfrågor:

- Hur användbara är våra autentiseringssystem?
- Kan användare tänka sig att använda något av våra system?
- Hur står sig våra system mot referenssystemen ur ett säkerhetsperspektiv?
- Hur står sig våra system mot engångslösenord ur ett användarperspektiv?

Teori

Hot

Hotet från keyloggers

Keyloggers kan implementeras både i hårdvara och mjukvara. En hårdvarubaserad keylogger kopplas in mellan tangentbordet och datorn (eller i själva tangentbordet) där den registrerar informationen som skickas däremellan. Hårdvarubaserade keyloggers kan inte upptäckas av mjukvara[2], då de inte modifierar den information som skickas mellan tangentbordet och datorn.

Mjukvarubaserade keyloggers kan delas in i två olika kategorier, kärn-/drivrutinsbaserade keyloggers eller API-baserade keyloggers. Den tidigare varianten arbetar på samma nivå som operativsystemets kärna och mottager tangenttryckningar direkt från tangentbordet. Denna typ av keyloggers kan göras mycket svårupptäckta då de startar tidigare än, och har tillgång till tangenttryckningar före, alla program på högre nivåer.[2] Nackdelen med dessa keyloggers är att de inte kan registrera information som genereras på användarnivå, t.ex automatiskt ifyllda fält.

API-baserade keyloggers arbetar på samma nivå som användaren och är därför lättare att upptäcka. De registrerar tangenttryckningar och eventuellt annan information (beroende på API) genom att anropa funktioner i användargränssnittets API. Exempel på sådan information kan vara vad som är lagrat i textfält eller i urklipp, vilket fönster som har fokus i användargränssnittet eller skärmdumpar.[2]

Van Eck-phreaking och Shoulder surfing

Van Eck phreaking är en teknik för att avlyssna skärmar på avstånd genom att fånga upp den elektromagnetiska strålning som de sänder ut och på så sätt skapa en egen kopia av det som visas på skärmen.[3] Denna teknik har inte setts som ett reellt hot förrän på senare tid, då den utrustning som krävs har sjunkit i pris. I maj 2004 presenterades en rapport från universitetet i Cambridge, som visar hur Van Eck-phreaking utförs mot LCD-skärmar på tio meters avstånd med utrustning till ett pris under $2000.[4] Van Eck-phreaking är egentligen bara shoulder surfing (tjuvkikande på någon annans skärm) som utförs på avstånd.

2 Sachin Shetty, "Introduction to Spyware Keyloggers" (6 April, 2010): http://www.symantec.com/connect/articles/introduction-spyware-keyloggers

3 Wim van Eck, "Display Units: An Eavesdropping Risk?" (3 Maj, 2010): http://jya.com/emr.pdf

4 Markus G. Kuhn, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays " (1 Maj, 2010): http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf

Olika typer av inloggningssystem

Grafiska inloggningssystem

Grafiska inloggningssystem utnyttjar datorns grafiska gränssnitt för att styrka en användares identitet. Exempel på detta är system där användaren väljer en sekvens av bilder eller ritar en figur för att verifiera sig mot systemet.[5] En fördel med grafiska inloggningssystem är att de kan skydda mot konventionella keyloggers då inmatning från tangentbordet inte alltid behövs.[6] Grafiska inloggningssystem kan däremot vara sårbara mot keyloggers som tar skärmdumpar, men det finns system som också försöker skydda mot den typen av keyloggers.

Ett exempel på ett sådant system är banken i onlinespelet RuneScape.[7] För att logga in i deras bank anges en fyrsiffrig PIN-kod genom att klicka på ett grafiskt tangentbord. Siffrorna på det grafiska tangentbordet kastas om efter varje siffra i koden som anges av användaren. På det här sättet så skyddar systemet mot keyloggers som registrerar muspekarens position vid musklick. Vidare görs den siffran som muspekaren hålls över osynlig för att göra skärmdumpar som tas i ett litet område runt muspekaren oanvändbara. En skärmdump som får med hela det grafiska tangentbordet knäcker systemet då det är lätt att se vilken siffra som är dold när alla andra är synliga (se Fig 1).

Fig 1: RuneScapes bankinloggningssystem

Engångslösenord

Engångslösenordssystem låter användaren autentisera sig med olika lösenord vid varje inloggningsförsök. Ett sätt att generera engångslösenord är att ge en tidsstämpel (koddosor som banker skickar ut använder ofta denna metod) eller det förra engångslösenordet som indata, eventuellt tillsammans med slumpad data till en hashningsfunktion.[8,9] På detta sätt kan inte en tredje part få fram nästa lösenord utan att känna till den bakomliggande hashningsfunktionen och tidigare indata.

---

5 Fabian Monrose och Michael K. Reiter, "Security and Usability", 2005, Chapter 9, ISBN: 0-596-00827-9

6 Krzysztof Golofit, "Picture Passwords Superiority and Picture Passwords Dictionary Attacks" (6 April, 2010): http://www.mirlabs.org/jias/golofit.pdf

7 www.runescape.com

8 Ugo Piazzalunga, Paolo Salvaneschi, Paolo Coffetti, "Security and Usability", 2005, Chapter 12, ISBN: 0-596-00827-9

9 Dan Griffin, "Safer Authentication with a One-Time Password solution" (2 Maj, 2010): http://msdn.microsoft.com/en-us/magazine/cc507635.aspx

En nackdel med engångslösenord är att de på något sätt måste skickas ut till användaren eller genereras av någon utrustning på användarsidan, vilket kostar pengar och kan upplevas som omständigt av användaren.

Biometriska inloggningssystem

Biometriska inloggningssystem identifierar användare med hjälp av deras fysiologiska egenskaper eller deras beteende.[10] Exempel på detta är fingeravtrycksigenkänning, iris-scanning och röstigenkänning. Dessa system är helt säkra mot keyloggers eftersom de inte behöver någon indata från vare sig tangentbord eller mus och inte behöver presentera någon, för tredje part användbar, information på en monitor. Några nackdelar med biometriska inloggningssystem är att extra utrustning behöver köpas in, och att utrustningen i sig kan ha brister som gör att de går att komma runt. Vissa fingeravtryckläsare har till exempel problem med att urskilja slitna eller skadade fingeravtryck.

Våra system

De bildinloggningssystem som vi har utvecklat består av en matris av bilder med tillhörande tecken (se Fig 2). För att autentisera sig mot systemet matar en användare in en teckensekvens som motsvarar en av användaren tidigare vald bildsekvens. För att användaren ska bli godkänd av systemet krävs det att tecknen anges i rätt ordning så att de exakt motsvarar den ordning i vilken användaren har valt sina bilder.

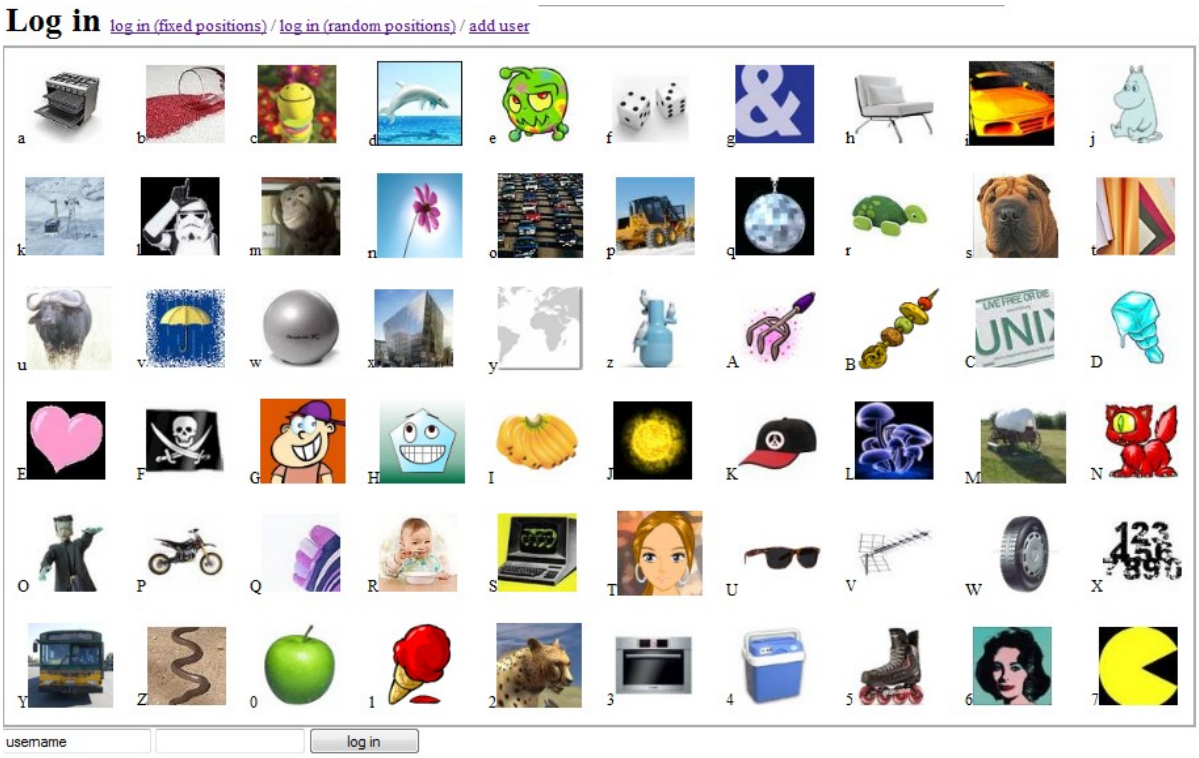

Fig 2: Egenutvecklat bildinloggningssystem

10 Lynne Coventry, "Security and Usability", 2005, Chapter 10, ISBN: 0-596-00827-9

Vi har implementerat två system, ett där bildernas placering i matrisen är slumpmässig för varje inloggningsförsök och ett där positionerna är fasta.

För att systemet med slumpmässig bildplacering ska kunna autentisera en användare måste det ha en metod för att koppla ihop de slumpade bildpositionerna och dess motsvarande sträng. I vårat system möjliggör vi detta genom att skapa så kallade mappningsfiler vid varje inloggningsförsök, där det tecken som hör till en position i matrisen kopplas samman med ett bildalias.

Metod

Användbarhetstest

Vi har låtit användare testa våra system och därefter svara på en anonym enkät[11] på Internet, för att få en uppfattning om hur användbara systemen är. I enkäten får användarna förutom att svara på frågor om hur de upplever systemen också jämföra dem med engångslösenord och betygsätta sin egen datorvana.

Användartestet består av en hemsida där användare får testa de två olika systemen genom att autentisera sig med en av oss vald bildsekvens, eller med en egenvald sekvens. Därefter kan användaren gå vidare till enkäten och utvärdera systemen. Enkäten består av sju frågor där användaren får ange hur hon upplever systemen, i vilka syften hon kan tänka sig att använda systemen, och hur hon betygsätter systemen gentemot varandra och engångslösenord.

Säkerhetsanalys

För att utvärdera våra inloggningssystem ur ett säkerhetsperspektiv har vi jämfört hur sårbara de är för olika hot jämfört med engångslösenord och textbaserade inloggningssystem. Kunskap om hur de olika säkerhetshoten fungerar bygger vi på litteratur och vetenskapliga rapporter.

Resultat

Säkerhetshot

I detta avsnitt går vi igenom säkerhetshot och jämför sårbarheter mellan våra inloggningssystem, engångslösenord och textbaserade inloggningssystem.

Hotet från traditionella keyloggers

Den här typen av keylogger är sällan ett hot mot grafiska inloggningssystem då de oftast använder sig av andra enheter än tangentbord, t.ex pekskärmar eller möss. Våra system är undantag då de använder sig av indata från tangentbordet. Det är däremot, beroende på vilket lösenord användaren har valt inget stort hot mot systemet med slumpmässiga bildpositioner då den data som keyloggern registrerar inte kommer att vara till stor användning. En viss information går förvisso att få ifrån den data som en keylogger registrerat, däribland längden på lösenordet och antalet unika bilder i bildsekvensen.

11 "Picture login" (3 Maj, 2010): http://spreadsheets.google.com/viewform?formkey=dHJydDh4MHZzZGc3cVlacFhOdlVPNkE6MQ&ifq

Skyddet mot hotet från traditionella keyloggers i systemet med slumpade bildpositioner, står eller faller med den slumpgenerator som används för att placera ut bilderna i matrisen och att användarna väljer bildsekvenser med många unika bilder. Versionen med fasta bildpositioner, eller vanliga textbaserade lösenord skyddar inte mot traditionella keyloggers på något sätt då en användare hela tiden autentiserar sig med samma textsträng, och en traditionell keylogger kan registrera den.

Engångslösenordssystem kan skydda mot traditionella keyloggers genom att varje inloggningsförsök har en unik eller slumpmässig nyckel, som påverkar hashningsfunktionens utdata. Ett engångslösenord som läckt till tredje part kan därför inte användas av denne då det inte är giltigt för dess inloggningsförsök.

Hotet från avancerade keyloggers

Det är möjligt att skapa en keylogger som registrerar all indata och utdata till och från en dator, varför inget inloggningssystem som inte tar hjälp av extern utrustning helt kan skydda mot tillräckligt avancerade keyloggers. Vår implementation med slumpmässig bildplacering skyddar inte mot en keylogger som både registrerar tangentbordstryckningar och tar en skärmdump vid ett inloggningsförsök. Systemet med fasta bildpositioner skyddar inte mot traditionella keyloggers, och därmed inte heller mot mer avancerade typer av keyloggers.

Engångslösenordssytem är lika sårbara mot avancerade keyloggers som mot traditionella keyloggers, då en avancerad keylogger inte ger någon ytterligare information som kan forcera systemet.

Mappning

Inloggningssystem som bygger på någon form av slumpfaktor måste på något sätt kunna koppla ihop en användares slumpmässiga autentiseringsnyckel med en fast motsvarighet, annars finns det inget sätt för systemet att avgöra om nyckeln är korrekt. I vår implementation görs detta genom att en mappningsfil skapas där de slumpmässiga bildpositionerna kopplas samman med bildernas fasta namn. Denna information utgör ett hot om en tredje part kan koppla samman den med ett specifikt inloggningsförsök, då informationen tillsammans med en användares autentiseringsnyckel skulle berätta hur användarens bildsekvens är utformad.

Engångslösenord och textbaserade autentiseringssystem behöver ingen mappning för att fungera, så de är inte sårbara mot denna typ av hot.

Brister i slumptalsgenerering

System som bygger sin säkerhet på slump kräver en bra slumptalsgenerator för att bibehålla säkerheten. Problemet med datorer i detta sammanhang är att de är deterministiska maskiner och därför kan de inte producera riktiga slumptal på egen hand.

En brist i slumptalsgenereringen i ett system skulle kunna innebära att tredje part kan lista ut hur inloggningssystemet kommer att bete sig över tid. I fallet med engångslösenord skulle det kunna innebära att någon obehörig kan räkna ut en användares framtida engångslösenord efter att ha observerat en mängd tidigare använda engångslösenord. I vårat inloggningssystem med slumpmässiga bildpositioner, skulle en dålig slumptalsgenerator kunna göra det möjligt för tredje part att lista ut villka bilder en användare valt genom att registrera flera teckensträngar som användaren angett vid sina inloggningsförsök. Textbaserade inloggningssystem och vår implementation med fasta bildpositioner är

inte sårbara då de inte bygger sin säkerhet på slump.

Van Eck-phreaking och Shoulder surfing

System där all information för att autentisera sig och användarens indata syns på datorns monitor är sårbara för den här typen av attack. Anledningen till att vi låter användaren välja bilder genom att ange tecken i ett fält där de inskrivna tecknena visas som asterisker (ett s.k. lösenordsfält) är för att skydda mot just dessa hot.

Textbaserade lösenordssystem är normalt skyddade mot dessa attacker då lösenordet matas in i ett lösenordsfält. Engångslösenordssystem kan däremot vara sårbara mot denna attack om lösenordet inte matas in i ett skyddat fält och systemet i fråga inte har något skydd mot att en tredje part autentiserar sig före den riktige användaren.

Användartest

39 användare testade våra system och svarade på den anonyma enkäten. Genomsnittsanvändaren uppgav att hon hade en datorvana över medel (se Fig 3), vilket kan ha påverkat resultaten i en positiv riktning när det gäller utvärderingen av användbarheten hos våra system och referenssystemen. En mindre van användare kan finna systemen mer komplicerade, och kanske inte heller förstår problemet med keyloggers och dess funktion.

Fig 3: How would you rate your experience with computers?

Lättare att logga in med fasta bildpositioner

Undersökningen visar tydligt att de som svarat på enkäten upplever det lättare att använda den version av systemet med fasta bildpositioner än versionen med slumpade positioner. En användare ger följande kommentar: "Jag föreslår att ni låter bilderna ligga på sina respektive platser och istället flyttar runt tecknen. Det blir lättare att hitta på det sättet, eftersom bilderna är index och man letar efter tecken. [...]". Data från enkäten visar att användare i snitt gav systemet med fasta bildpositioner 56,5% högre betyg än systemet med slumpade bildpositioner gällande användbarheten (se fig 4 och 5).

Fig 4: How easy did you think it was to log in when the picture positions were fixed?

Fig 5: How easy did you think it was to log in when the picture positions were random?

Jämförelse med engångslösenord

I enkäten ingick två frågor där användare fick jämföra våra system mot engångslösenordssystem. Majoriteten av användarna tyckte att systemet med fasta bildpositioner var lättare att använda än engångslösenord medan situationen var omvänd när bildpositionerna var slumpmässiga (se fig 6 och 7).

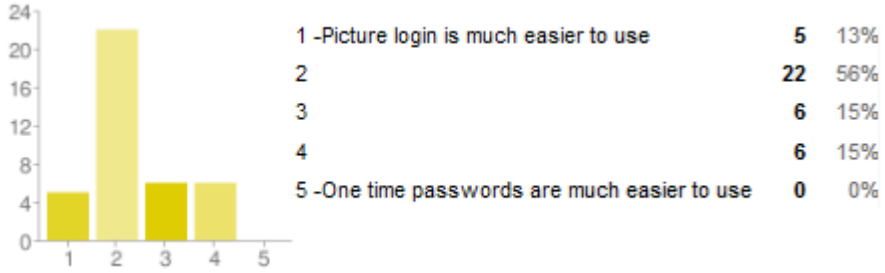

Fig 6: Which system do you think is easiest to use, picture login with fixed image positions or one time passwords?

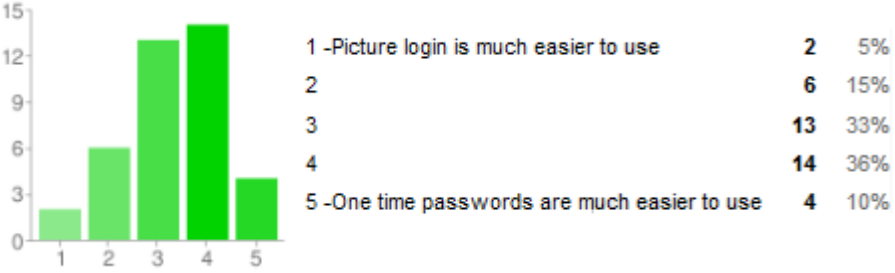

Fig 7: Which system do you think is easiest to use, picture login with randomized image positions or one time passwords?

Majoriteten av användarna kunde däremot inte tänka sig att använda systemet med fasta bildpositioner för att komma åt känslig data, t.ex en internetbank, medan 44% kunde tänka sig att använda systemet med slumpmässiga bildpositioner i detta syfte. De flesta användarna föredrog engångslösenord för att komma åt känslig data (se fig 8).

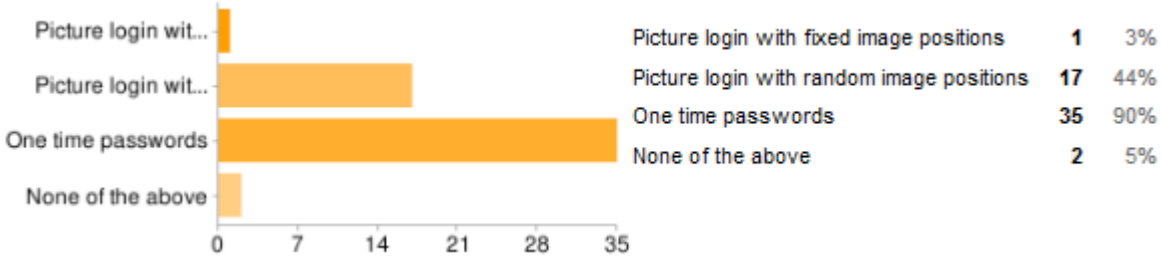

Fig 8: What systems would you consider using to access sensitive information? (e.g. internet banks)

För att komma åt mindre känslig data, t.ex diskussionsforum eller datorspel, kan 79% tänka sig att använda sig av fasta bilder för att få tillgång till systemet och endast en av våra testpersoner kunde tänka sig att använda engångslösenord (se fig 9).

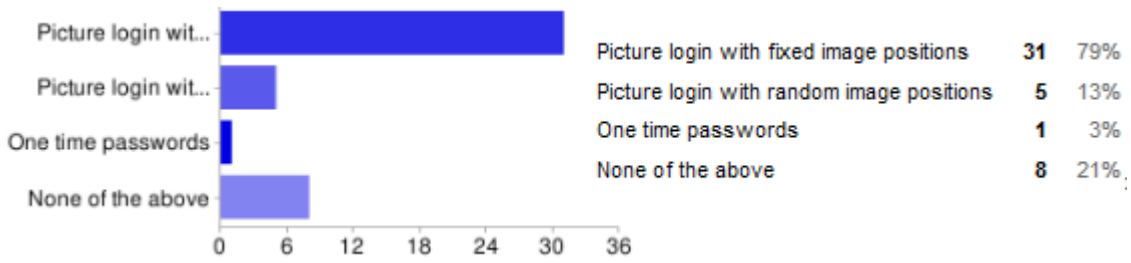

Fig 9: What systems would you consider using to access less sensitive information (e.g. games, discussion forums)

Diskussion

Förslag till förbättringar

Våra användartester visar att de flesta användare upplever att det är lättare att autentisera sig mot systemet när bilderna har fasta positioner. Därför är det möjligt att det underlättar för användarna om tecknens positioner slumpas i matrisen istället för bildernas, vilket också en av testpersonerna påpekade. Detta skulle inte påverka säkerheten hos systemet på något sätt.

Ett fåtal personer som utförde användartestet nämnde att de skulle föredra om det gick att välja bilder genom att klicka på dem istället för att skriva in dess respektive tecken i matrisen. En sådan implementation skulle vara sårbar mot både shoulder surfing, Van Eck-phreaking och en keylogger som tar skärmdumpar vid musklick.

Systemet kan modifieras för bättre skydd mot keyloggers med skärmdumpsfunktion, till en kostnad av högre komplexitet i implementationen och möjligen på bekostnad av användbarhet. Ett exempel är genom att använda en metod liknande den som RuneScapes virtuella bank använder, och låta alla bilder döljas när användaren håller muspekaren över en bild. Med denna metod skulle användare kunna använda musen för att välja bilder och systemet skulle ändå skydda mot keyloggers som kan ta skärmdumpar.

En annan möjlig implementation är att användaren måste bläddra igenom de olika bilderna så att bara några få i taget är synliga. Detta skulle tvinga en keylogger att registrera skärmdumpar vid flera tillfällen under ett inloggningsförsök för att få med all information, men detta skulle förmodligen också försvåra för användaren.

Slutsats

Datan från vår enkät visar att 79% av användarna tycker att det är tillräckligt enkelt att autentisera sig med vårat system med fasta bildpositioner för att de ska kunna tänka sig att använda det för att komma åt mindre känslig data. Vidare angav 44% av de som svarade på enkäten uppgav att de skulle kunna tänka sig att använda systemet med slumpmässiga bildpositioner för att komma åt känslig data som t.ex Internetbanker. Därmed bör förslaget där teckenpositionerna i matrisen slumpas och bilderna är fasta, kunna användas för att autentisera användare mot system innehållandes både känslig och mindre känslig data. Ett sådant system skulle öka skyddet mot traditionella keyloggers i jämförelse med ett textbaserat system samtidigt som kostnader som tillkommer med engångslösenord elimineras då ingen extra utrustning på användarsidan behövs.

Engångslösenord bör ändå användas för att autentisera användare mot mycket säkerhetskritiska system då ett bra implementerat engångslösenordssystem skyddar mot alla typer av keyloggers och shoulder surfing.