Burch Gürler 820915-1433

Uppsala universitet
Institutionen för informatik och media
Informationssystem och systemutveckling
HT 2013
2013-10-15

Informationssäkerhet

Med ett tekniskt perspektiv på SSL

Innehållsförteckning

1. Inledning

Vi lever idag i ett informationssamhälle där samtliga företag och organisationer handskas och kommunicerar mängder av information. Detta måste ske på ett säkert sätt, därför är det viktigt att förstå vad säker informationshantering har för betydelse och påverkan.

IT-projekt skapas, utvecklas och outsourcas dagligen för olika organisationers och företags behov i dagens informationssamhälle. Detta sker genom väl beprövade utvecklingsmetoder t.ex. Vattenfallsmodellen eller Agil systemutveckling där valet av modell tas efter projektets krav och bakomliggande egenskaper. IT-projekt går igenom livscykeln kallad SDLC (system development life cycle) som består utav fyra olika, men sammanhängande delar nämligen planering, analys, design och implementationsfas (Dennis.A, 2012, s. 8).

Informationen som behandlas i ett IT-system sänds och sparas i form av data och denna vill man alltid hålla säker av flera skäl. Ett exempel är en webbplats för e-handel där kunddatabaser och transaktioner måste skyddas så att obehöriga inte kan få tillträde.

Informationssäkerhet finns på agendan hos många företagsledningar redan från början av ett IT-projekt och genom en välfungerande Informationssäkerhets plattform får man kunder att känna sig säkra och på sätt tillfredsställs behoven för både parterna.

Säkerhet handlar inte bara om sårbarheter, hackers och dataintrång utan mer om frågor vad gäller systemets stabilitet, tillgänglighet och säkerställande av att information som processas av systemet faktiskt håller en viss nivå av kvalitet.

Detta förhållningssätt, samt även vikten av dimensionen av personlig integritet på nätet är också en fråga som behandlas på högsta politiska nivåer exempelvis på EU-nivå.

Primärt bestäms vilken typ av säkerhet som skall användas i design fasen. Behov av säkerhetnivå fastslås i analysfasen i kravspecifikationen, men vilka säkerhetsimplementationer som skall användas väljs under designfasen.

1.1 Syfte

Uppsatsens syfte ligger vid att utröna hur e-handelssajter kan skydda information som överförs till och från kunder via ett webbgränssnitt? Vidare så kommer också dagens praxis för överförningsteknologi att beröras.

1.2 Frågeställning

Med beaktande av erforderlig säkerhetsnivå för e-handel, på vilket sätt ska vi skydda information som överförs mellan en webbserver och webbklient?

2. Teori

För att kunna etablera en säker e-handelsmiljö så krävs det att e-handelsbutiken skyddar data som överförs mellan butiken och klienten alltså kunden som handlar. Detta uppnås genom att e-handelssajten skaffar sig ett SSL certifikat utfärdat av en betrodd SSL-utgivare. SSL-certifikatet, beroende av vilken certifikatsnivå man använder, fungerar som en slags garant för att trafiken skyddas och i många fall att utgivaren kontrollerat identitetsuppgifter för den e-handelsbutik som inhandlat SSL-certifikatet.

2.1 Avvägning av säkerhetsnivå

När information ska skyddas så måste en avvägning göras med hänsyn till kostnader och applicerbarhet i projektet. En fördubbling av bitstorlek för en krypteringsnyckel, innebär inte per definition att man är "dubbelt så säker" utan kan snarare innebära större overhead trafikmässigt, större krav på hårdvara, ökade kostnader för inköp och andra aspekter som bör vägas in.

Säkerhetsvärlden är en värld i ständig förändring, i takt med ökad processorkraft och granskning av algoritmer så kan en standard som ansågs vara säker igår anses som osäker imorgon. Genom lite omvärldsanalys kan man komma fram till vilka standarder som anses säkra per dags datum.

När man gör en avvägning av säkerhetskraven måste också externa krav tas i beaktande, såsom lagstiftning (exempelvis Personuppgiftslagen) samt eventuella överenskommelser med externa parter som inkluderar säkerhetskrav i avtal (t ex om e-handelssiten hämtar personuppgifter från en extern leverantör och lagrar dessa lokalt på servern). Branschstandarder bör också beaktas, som vuxit fram genom erfarenheter som etablerade marknadsparter tagit till sig, dessa standarder är också något som både konsumenter och partners utgår ifrån att branschen håller sig till - skyddande av person- och andra potentiellt känsliga data är ett exempel på detta.

I designfasen, ansvarar systemarkitekterna för att implementera säkerhetsdesign och systemutvecklarna ansvarar för implementering av säkerhetfunktioner i projektet "system developers" (Dennis.A, 2012, s. 295).

2.2 SSL- och TLS-handskakning

För att etablera en SSL- eller TLS-krypterad session, måste en så kallad handskakning mellan klient och server genomföras. Denna handskakning sker i ett antal steg:

1) Klienten begär en session.

2) Servern svarar med sitt Certifikat som också är serverns publika nyckel.

3) Klienten verifierar publika nyckeln mot en lista av betrodda utgivare.

4) Klienten genererar en symmetrisk nyckel som den krypterar med serverns publika nyckel.

5) Servern dekrypterar den krypterade informationen och får reda på vilken symmetrisk nyckel som ska användas för sessionen, denna nyckel används sedan för att kryptera data mellan klienten och servern.

2.3 Nyckelstorlek

Nyckeln i krypteringssammanhang syftar till det urvalsdata som används i algoritmen för att kryptera slutdata. Med längre nyckellängd minskar risken för att någon med hjälp av gissningsattacker "brute force" och mycket datorkraft lyckas "gissa" nyckeln och därmed får tillgång till den dekryptera datan.

För att förenkla detta, tänk dig att du har en resväska med sifferkombinationslås. Om du har tre siffror att jobba med för att skapa din "nyckel" så kommer du ha 1000 möjliga kombinationer (000-999). Om du utökar låset till ett lås med fyra siffror att jobba med så

innebär det en tiofaldig ökning av möjliga “nycklar” (0000-9999). Denna princip kan i stort sett appliceras på den nyckellängden som genereras som bas för krypteringen mellan klient och server via SSL-protokollet - även om krypteringsalgoritmerna skapar ett mycket mer avancerat skydd.

När kärnverksamheten har med information- och olika typer av informationstransaktioner att göra så är informationskvaliteten- samt integriteten viktiga nyckelprinciper för att få projektet att leverera förväntat resultat. Förutom faktorer som renommé och kundernas tillit till projektet och varumärket så har man också ett ansvar att skydda de data som potentiellt kan innebära intrång i privatlivet.

Dataintegritet är en viktig komponent i säkerhetsarbetet, det är inte bara mot nyfikna ögon som man vill skydda informationstransaktioner utan även för att garantera kvalitet i leverans.

3. Empiri

3.1 Krypteringsstandarder för populära webbplatser skyddade av SSL eller TLS

Granskningen är genomförd med hjälp av en vanlig webbläsare (Google Chrome). Värt att nämna i detta fall är att krypteringsstandarden förhandlas mellan klient och server. Beroende på hur systemutvecklarna konfigurerat server- samt hur webbklienten är konfigurerad så kan krypteringsstandarden förändras. Exempelvis kan vissa äldre webbläsare begära en lättare form av kryptering, om servern stöder detta och inte explicit kräver en högre krypteringsstandard så kommer förbindelsen att förhandlas fram med lägre standard.

Nedan är en kort förteckning över vissa populära siter som använder SSL- eller TLS för kryptering av trafik mellan klient och server.

Tjänst	**Protokoll**	**Krypteringsstandard för överföring av data**
Google Gmail	TLS 1.2	RC4_128
Klarna	TLS 1.2	RC4_128
Paypal	TLS 1.2	RC4_128
CDON	TLS 1.0	RC4_128
Amazon	TLS 1.0	RC4_128
SEB	TLS 1.2	RC4_128
Handelsbanken	TLS 1.0	AES_256_CBC
SF BIO	TLS 1.2	RC4_128

Fig. 1

4. Analys

Enligt Delone-modellens funktionsdel (functionality) så förutsätter denna att två komponenter är på plats, systemkvalitet och informationskvalitet. Man kan argumentera för att informationskvalitet även innefattar integritet av information, d.v.s. att man kan säkerställa att information som överförs i ett system inte förändras eller manipuleras. Medhänvisning till Delone-modellen nedan.

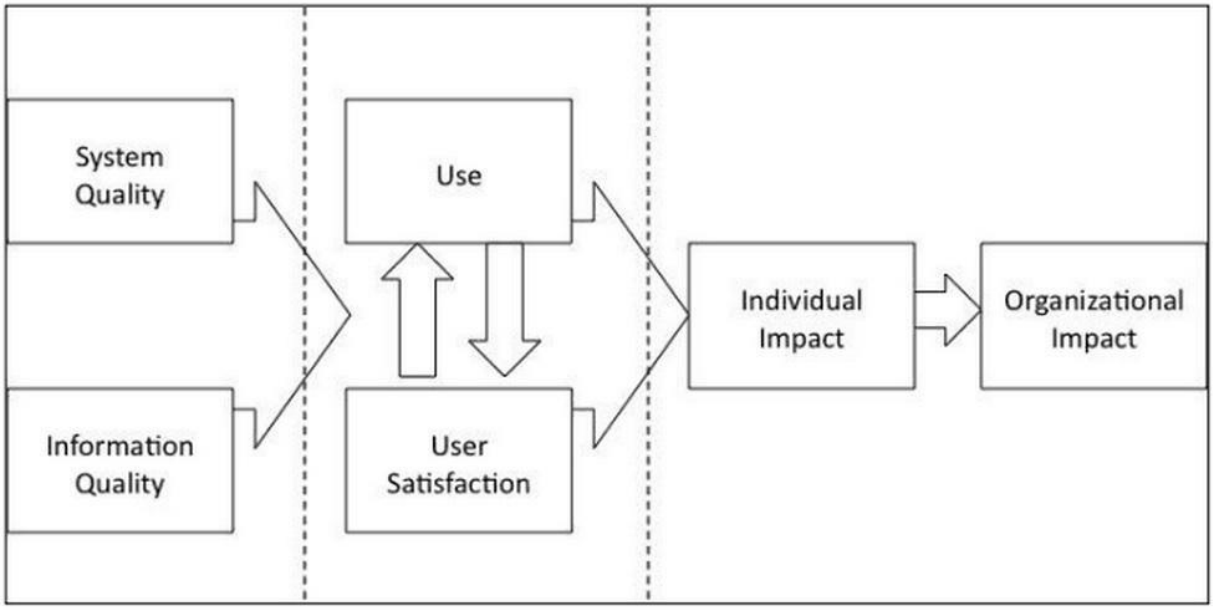

Fig. 2

Om vi stegar igenom Delone-modellen förutsätter modellen systemkvalitet och informationskvalitet för att användning och användarnmjdöjlighet skall tillfredställas. Om inte systemet håller en viss kvalitet och levererar förväntat resultat kommer detta leda till avbrott i systemet som i sin tur orsakar problem i t.ex. affärsmodeller som förutsätter kontinuitet förslagsvis en e-handelsplats.

Avsteg från kvalitet, dataintegritet skulle då på enskild basis och organisationell basis även innebära att hela affärsmodellen omkullkastas p.g.a. av nämnda anledningar. Man kan därför genom detta resonemang vara säker på att en förutsättning för denna typ av system för en e-handelsplats förutsätter informationsintegritet som en av de viktiga komponenterna för att säkerställa systemets helhet och därmed projektets värde.

Parallellt i jakten med att uppnå ett värde behövs en regelrätt förhållning mot rådande lagar och direktiv. Dataskyddsdirektivet kan vara problematiskt att förhålla sig till eftersom beskrivningen av data ses som ett fysiskt objekt, var på den egentligen finns överallt. Förslagsvis skulle en ”lag modell” vara till nytta (Birnhack.M, 2008, s. 518).

5. Diskussion och slutsats

Vid beaktande av erforderlig säkerhetsnivå för en e-handelsplats bör man dels undersöka dagens praxis för säkerställande av informationsintegritet och de standarder som finns implementerade samt tillgängliga för detta.

Det som betraktas som erforderlig säkerhetsstandard idag, är kanske inte erforderlig imorgon - beroende av utvecklingen på teknik- och säkerhetsområdet exempelvis upptäckt av brister i algoritmer, populära implementationer av standardprotokoll.

Eftersom företag med miljardomsättning och hög e-handelsaktivitet på Internet har stora resurser så som personal- och kompetensmässiga aspekter att sätta av för planerings- och säkerhetsarbete så kan vi vara rätt säkra på att det som betraktas som erforderlig standard av dessa bolag, kan anses vara branschstandard. Därför har jag också tittat på vilka algoritmer och protokollstandarder som flertalet av dessa stora giganter använder för sina webbplatser för att säkerställa dataintegritet mellan webbserver och klienter eller kunder.

De flesta moderna webbläsare idag klarar TLS 1.2 och har stöd för flertalet avancerade krypteringsalgoritmer. I den undersökning som jag utfört så har det visat sig att just överföringsprotokollet TLS 1.2 en utveckling av SSL-standarden och krypteringsalgoritmen 128-bitars RC4-kryptering varit den vanligast förekommande säkerhets implementationen.

Vid etableringen av en e-handelsplats måste man dock i en del fall genomföra en väl viktad analys av vad som betraktas som erfoderlig säkerhetsnivå. Det är helt avhängigt av vad man ämnar erbjuda för typ av produkt och därmed också vad för typ av data som överförs mellan klient- och server.

Till detta säkerhetsavvägande måste man vikta externa krav från exempelvis lagstadgade sådana samt eventuella kontraktuella förhållanden till kunder, partners och leverantörer. Idag regleras informationsintegritetskrav ofta i kommersiella avtal där en leverantör av exempelvis persondata för mappning mot kunder, vilket då också kan innebära att det ställs högre krav på integritet av data. Under planeringsfasen för projektet, bör man enligt Gehling kartlägga och identifiera tillgångar, hot och sårbarheter (Gehling.B, 2005, s.33).

En ytterligare dimension till säkerhetsavvägandet är de strikta krav som EU har tagit fram för behandlade av persondata är att det kommer att finnas starka finansiella incitament för storbolag som processar-, överför- och lagrar persondata att se till att detta görs på ett adekvat och säkert sätt. Enligt det slutgiltiga EU-förslaget kommer större bolag att påföras böter om upp till 2 procent av bolagets totala omsättning om bolaget inte följer den lagstadgade förordningen som börjar gälla under nästa år (EU dataskydds lag 2012 s.93).

Säkerhet blir inte bara viktigt under designfasen, utan totalt väsentligt för ett bolags överlevnad i och med det nya förslaget. Dessa frågor blir därför hierarkiskt viktigt då dessa måste vädras i styrelserum och på ledningsnivå.

Avslutningsvis egenskaperna bakom säkerhet är och har en stor och mångfacetterad komplexitet. Detta går inte att ta till sig enbart med studier och kanske inte heller med en kort arbetslivserfarenhet. Det är genom en gedigen utbildning och långvarig arbetslivserfarenhet som man kan få rätt verktyg som ger rätt förutsättningar för att lyckas inom denna bransch. Med detta arbete har jag ordagrant bara skrapat på ytan utav innebörden av vad säkerhet betyder.

6. Källförteckning

Böcker:

Paul Beynon-Davies. (2013). *Business information Systems*. 2nd Edition. New York. Palgrave-Macmillan.

Alan Dennis, Barbara Haley Wixom, Roberta M. Roth. (2012) *Systems Analysis and Design*. 5th Edition. Wiley.

Elektroniska resurser:

http://dl.acm.org.ezproxy.its.uu.se/citation.cfm?id=1107631 [Hämtad 13.10.25].

http://www.sciencedirect.com.ezproxy.its.uu.se/science/article/pii/S0267364908001337 [Hämtad 13.10.25].

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf sd [Hämtad 13.10.25].

http://www.openssl.org/ [Hämtad 13.10.25].

http://en.wikipedia.org/wiki/Transport_Layer_Security [Hämtad 13.10.25].

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html [Hämtad 13.10.25].

7. Bilagor

7.1

Burch Gürler
Uppsala Universitet
Informationssystem A
Informationssystem HT 2013
v42

Programmering och Algoritmer

Inledning

Eftersom jag har begränsade kunskaper inom detta område samtidigt som jag finner det väldigt intressant är detta ett bra tillfälle att lära och ta till sig kunskap inom detta område.

Bakgrund

Utan att överdriva kan man påstå och bevisa att programmering och algoritmer är en viktig entitet för både små och stora projekt. Stora projekt kopplade till stora företag t.ex. inom finanssektorn och statliga myndigheter har ett stort intresse för att programmeringen och eventuella algoritmer som används fungerar korrekt. Detta gäller även för mindre projekt där målet är att allt skall fungera som det är tänk.

Syfte

Jag vill erhålla en fördjupad kunskap i detta område.

Frågeställning

Varför är programmering och algoritmer så viktigt i nutida informationssamhälle?

Metod

Genom fortsatta diskussioner i min grupp och läsa till mig kunskap från kurslitteraturen, internet.

7.2

Burch Gürler
Uppsala Universitet
Informationssystem A
Informationssystem HT 2013
v43

Säkerhet

Inledning

Då jag har begränsade kunskaper inom detta område samtidigt som jag finner det väldigt intressant är detta ett bra tillfälle att lära och ta till sig kunskap inom detta område.

Bakgrund

Säkerhet har alltid varit viktigt. Detta är känt hos samtliga ledningar inom olika IT-projekt. Jag vill veta vilka säkerhets åtgärder som används för e-handel och hur man håller kund data säkert.

Syfte

Jag vill erhålla en fördjupad kunskap i detta område och det finns väldigt mycket man kan ta till sig här men jag ska ta reda vilken typ av säkerhet som används t.ex. vid e-handel.

Frågeställning

Vad är det som behövs för att e-handel skall ske på ett säkert. Hur vet man att sidan man går in på är den man tror att det är? Hur skyddas mina uppgifter? Hur skyddar e-handels webbplatser kundernas kundinformation?

Metod

Fortsatta diskussioner i min grupp och läsa till mig kunskap från kurslitteraturen, internet och eventuellt en intervju med en yrkesverksam inom området.