Molnet – möjligheter och begränsningar

HENRIK KARLZÉN

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R--3381--SE
ISSN 1650-1942 Februari 2012

Henrik Karlzén

Molnet – möjligheter och begränsningar

Titel	Molnet – möjligheter och begränsningar
Title	The Cloud – opportunities and limitations
Rapportnr/Report no	FOI-R--3381--SE
Rapporttyp/ Report Type	Användarrapport
Sidor/Pages	19 p
Månad/Month	Februari
Utgivningsår/Year	2012
ISSN	ISSN 1650-1942
Kund/Customer	Försvarsmakten
Projektnr/Project no	E53375
Godkänd av/Approved by	

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem
Box 1165
581 11 Linköping

FOI, Swedish Defence Research Agency
Information Systems
Box 1165
SE-581 11 Linköping

Sammanfattning

Molnet har på senare år blivit ett mycket populärt begrepp. Tidigare var så kallade grid den dominerande formen för distribuerad datorkraft, men molnet har alltmer tagit över med sin unika affärsmodell där priset bestäms av hur mycket som konsumeras. Detta ger vad som kan kallas datorkraft ”på kran” och för leverantörens del bygger det på att de totala resurserna kan utnyttjas mer effektivt med hjälp av virtualisering. Paralleller kan dras till nyttjande av stor- och superdatorer, där kunder hyr processortid, men molnet är mer flexibelt och har mer diversifierade kundbaser. Många stora datorföretag erbjuder numera molnbaserade tjänster som är kraftfulla och lättillgängliga.

Denna rapport ämnar ge insikt i vad molnet är samt fungera som introduktion till ämnet för tekniskt orienterade och säkerhetsmedvetna. Den exakta definitionen av vad moln är varierar i litteraturen och rapporten försöker bringa klarhet i det hela. Molnet analyseras och jämförs med närbesläktade begrepp för att påvisa likheter och skillnader samt vad som egentligen utgör det specifika med molnet. Dessutom utreds vilka möjligheter molnet ger. Kunden kan fokusera på sin verksamhet och slipper att investera i dyr infrastruktur medan molntillhandahållaren kan dra nytta av sin storlek och använda säkerhetsmekanismer som annars inte skulle vara kostnadseffektiva.

I rapporten beaktas också risker med molnet. Den nya affärsmodellen gör att lagar och regler i vissa fall är mindre väl anpassade och att dela resurser med andra kunder kan vara riskfyllt. Granskning och certifiering av tredje part är centralt för att kunden ska kunna lita på den som datorkraften köps av. Internets globala natur komplicerar riskbilden ytterligare och virtualisering av datorresurser gör det svårt att knyta data till en fysisk lagringsplats. Tillgänglighet är en viktig fråga då avbrott kan vara mycket dyra och säkerhetskopiering av en distribuerad infrastruktur komplex. Att byta moln tar ofta tid då interoperabilitet normalt saknas. Dessutom måste tekniska säkerhetsaspekter beaktas. Den klassiska perimetermodellen stämmer inte lika väl längre och kunden behöver försäkra sig om att molnägaren ordnar med tillräckligt skydd. Här kan en så kallad betrodd plattform intyga att en konfiguration är korrekt och kryptering kan skydda mot dataläckage. Särskilt intressant är den nya form av kryptering som tillåter beräkningar utan föregående dekryptering, men än så länge är metoden alltför långsam. Isolering mellan kunder är centralt och mer forskning kring säkerhet vid virtualisering av datorresurser krävs därför.

Nyckelord: Molnet, webbtjänster, SaaS, IaaS, PaaS, on-demand, virtualisering, virtuell maskin, VM, säkerhet, isolering, kryptering, objektbaserad säkerhet, betrodd plattform

Summary

The cloud has in recent years become a very popular concept. In the past, the so called grid was the dominant form of distributed computing, but the cloud has increasingly taken over with its unique on-demand business model. For the provider, this means that the resources can be utilized more efficiently through virtualization. Parallels can be drawn to the use of mainframe computers, where clients rent time, but the cloud is more flexible and has a more diverse customer base. Many major computer companies now offer cloud-based services that are powerful and highly accessible.

The precise definition of the cloud varies in the literature and this report tries to shed light on this. The report also explores the possibilities that the cloud provides. The customers can focus on their business and do not have to invest in expensive infrastructure, whereas the cloud service provider can leverage their size and use of security mechanisms that would not otherwise be cost effective.

At the same time, there are risks with the cloud. The new business model means that traditional laws and regulations are in some cases less well suited, and to share resources with other clients can be risky. Auditing and certification by third parties is vital for the customer to be able to trust the cloud provider. Internet's global nature further complicates matters and in combination with virtualization, it is difficult to link the data to a physical storage location. Availability is an important issue as disruptions can be very expensive and backup of a distributed infrastructure complex. Switching clouds often takes time since interoperability is normally missing. In addition, the technical security aspects must be taken into account. The classic perimeter model is not as useful anymore and the customer needs to ensure that the cloud owner will arrange adequate protection. In this case, a so-called trusted platform can certify that a configuration is correct and encryption can provide protection against data leakage. Particularly interesting is the new form of encryption that allows calculations without decryption, but so far the method is too slow. Isolation between customers is central and more research on virtual machines is therefore required.

Keywords: Cloud computing, cloud storage, web services, SaaS, IaaS, PaaS, on-demand, virtualisation, virtual machine, VM, security, isolation, cryptography, object based security, trusted platform

Innehållsförteckning

1 Inledning

Denna rapport behandlar ämnet molnet och beskriver dess egenskaper samt för- och nackdelar. I detta inledande avsnitt presenteras syfte och mål samt tillvägagångssättet.

1.1 Syfte

Molnet har fått stort utrymme i forskning och branschmedia på senare tid. Det är av stort intresse bland individer, företag, myndigheter och andra organisationer att förstå vad molnet är, hur det kan användas och vilka risker det medför. Många verksamheter har till viss del övergått till molnet och till och med den brittiska försvarsmakten har förlagt en betydande del av sin IT-infrastruktur i molnet. Syftet med denna studie är att öka förståelsen för vad som i allmänhet menas med begreppet, vad den nya trenden egentligen består av och hur säkerhetssituationen ser ut. Studien kan därmed utgöra underlag för beslutsfattare som överväger att flytta verksamhet till molnet, samt fungera som introduktion till ämnet för mer tekniskt orienterade säkerhetsmedvetna.

1.2 Mål

Målet med denna rapport är att:

- definiera termen molnet
- beskriva molnets möjligheter samt
- analysera relevanta risker.

Definitionen ska vara stringent för att reda ut vad som egentligen är nytt med molnet. Molnets möjligheter ska, ur en organisations synvinkel snarare än den enskilde individens, redogöras för. Säkerhetsdiskussionen ska främst vara teknisk i sitt perspektiv, men också täcka in vissa affärs- och kontraktsmässiga aspekter.

1.3 Metod

Studien utförs genom att söka befintlig vetenskaplig litteratur med betoning på rapporter som skrivits de senaste två åren för största möjliga relevans och tillfredsställande vetenskaplig höjd. Denna litteratur sammanställs sedan och väsentliga rubriker fastställs. Textmassan analyseras och källor jämförs sinsemellan för att säkerställa korrekthet och tillämplighet. Slutligen sammanställs behandlad text i form av en rapport och slutsatser dras.

2 Vad är molnet?

I detta kapitel definieras molnet. Dessutom beskrivs skillnader mellan molnet och liknande termer samt vad moln är lämpade för.

2.1 Definition

Begreppet moln (från engelskans the cloud) har på senare år blivit ett modeord [27] och den exakta definitionen är ofta oklar. Molnet bygger dessutom på tekniker och metoder som tidigare stått i fokus och som lett fram till ett alltmer distribuerat och flexibelt arbetssätt med tunna klienter, bärbara enheter och snabba internetuppkopplingar. Av dessa skäl kan det vara svårt att förstå exakt vad molnet är och vad som överhuvudtaget är nytt [41]. Till och med VD:n för ett av världens största mjukvaruföretag uttalade sig 2008 oförstående om molnet och menade att det definierats så att det innehöll allt inom IT [45].

Den idag vanligast förekommande definitionen är den som tagits fram av det amerikanska standardiseringsorganet National Institute of Standards and Technology (NIST). Enligt denna definition erbjuder molntillhandahållare (MT) sina kunder *en tjänst med lättillgänglig tillgång till konfigurerbar datorkraft* (som kan vara allt från hela servrar till applikationer) *där man snabbt och enkelt kan få tillgång till mer datorkraft och priset beror på hur mycket man använder* [32].

Kunden betalar alltså för vad som används på samma sätt som vid förbrukning av exempelvis el, en affärsmodell som i litteraturen förekommer med ett stort antal engelska namn: utility, pay-as-you-go, on-demand, commodity [27, 28, 29]. På detta sätt undviker kunden det resursslöseri som återfinns i traditionella datorstrukturer där servrar kan stå delvis oanvända under stora delar av tiden för att klara av sällsynta men ändå förekommande resurskrävande perioder.

Till viss del innebär molnet en tillbakagång till äldre infrastrukturer där man lånade tid i en stordator (eng. mainframe) [63]. Till skillnad från klassisk outsourcing innebär molnet vidare mer flexibilitet för kunden som enklare kan få tillgång till mer datorkraft när så behövs [27]. Det kan slutligen diskuteras om affärsmodellen bäst liknas vid att konsumera el eller om det snarare rör sig om att datorkraft hyrs på samma sätt som en lägenhet hyrs. I det senare fallet är det en möjlighet att det på lång sikt vore mer kostnadseffektivt att äga och själv stå för underhåll.

För att uppnå optimal resursanvändning nyttjar MT normalt resursabstraktion genom att virtualisera hela datorer och skapa så kallade virtuella maskiner (VM). Flera VM går att köra på en och samma dator och av säkerhetsskäl är dessa VM logiskt separerade från varandra, ofta med hjälp av en så kallad hypervisor. Virtualisering användes redan i kombination med stordatorer för att spara utrymme och kraft [28].

2.2 Liknande begrepp

Idén om datorkraft på kran har funnits åtminstone sedan 1960-talet [34]. Begreppen moln och dess släkting grid (det engelska ordet för elnät) myntades i slutet av 90-talet, men molnet populariserades inte på allvar förrän betydligt senare. Grid och moln har likartade mål men de skiljer sig från varandra på ett antal punkter. Begreppet grid myntades med betydelsen billig, kraftfull och tillgänglig datorinfrastruktur för beräkningar [34]. Moln har en specifikare definition av ”billig” samt mer fokus på flexibilitet i tillgången till resurserna och kan även brukas för lagring. Grid erbjuder mer informella samarbeten med en eventuell, och i så fall fix, avgift [34] och i praktiken ofta mindre starka tillgänglighetsgarantier [27]. Det är just affärsmodellen, och inte tekniken, som är den stora skillnaden mellan molnet och grid enligt [28].

En nyare griddefinition poängterar vidare att grid är decentraliserade datorsystem som bygger på öppna och standardiserade protokoll [34]. Medan moln är centralstyrda är alltså grid decentraliserade till sin natur. Grid har påstått brista vad gäller säkerhet [27]. Hittills har grid dessutom främst varit populära bland forskare som ofta har en annan hotbild och andra regler att följa än företag [17].

Botnät är ett annat begrepp som är ganska starkt relaterat till molnet och betyder en mängd datorer som tagits över av en angripare och sammanslutits i ett särskilt nätverk. Även om både affärsmodeller och säkerhetsaspekter är annorlunda har botnätsskapare redan lärt av moln, både vad gäller ny teknik och nya sätt att tjäna pengar. Därför kan det vara lämpligt att även molntillverkare lär av botnät [43], särskilt med tanke på den kreativitet som ofta präglar de nämnda angriparna. Botnät har liknats vid grid [42] och från att ha varit enkla applikationer har de utvecklats mot hela infrastrukturer med inbyggda säkerhetsmekanismer [47]. Numera hyrs näten även ut mot betalning. Enligt ett rättsfall kan ett botnät, som skapats genom att stjäla vanliga användares datorkraft, hyras ut för mindre än en krona per processorkärna, vilket är betydligt billigare än för vanliga moln [44].

Jämfört med andra webbtjänster skiljer sig moln främst vad gäller affärsmodellen. Till exempel är de populära sociala nätverkstjänsterna ofta gratis och dessutom mindre flexibla, vad gäller att få tillgång till mer datorkraft, än moln. Skillnaden är dock inte stor och i litteraturen förekommer ibland även dessa tjänster under kategorin moln. Distribuerade nätverk för fildelning är med sin decentraliserade natur snarare en avart av grid som erbjuder ett slags lagringsmöjlighet istället för beräkningskapacitet. Vissa webbplatshotell, där tjänstens omfattning och kvalitet beror på priset, kan dock ses som restriktiva varianter av moln. Fillagringstjänster som Dropbox är också en typ av enklare moln [41].

2.3 Typer av moln

Den datorkraft som MT tillhandahåller kan som nämnts ligga på olika nivå och normalt delas moln in i tre nivåer, även benämnda lager [9, 28]. Den första typ som erbjöds var färdiga mjukvarutjänster (eng. Software as a Service – SaaS) och som noterats ovan är det vad gäller en del webbtjänster ett gränsfall om de ska räknas som SaaS-moln eller om de inte är moln. Företaget Salesforce.com [54] var bland de första att erbjuda applikationer, specialsydda åt företag, via webben och email på webben var en tidig molnliknande tjänst, även om begreppet inte användes utbrett förrän mitten av 00-talet [24]. Nuförtiden är Google framstående på SaaS-marknaden med sitt Google Docs [57].

Google var med sin App Engine [52] en föregångare vad gäller plattformsnivån (eng. Platform as a Service – PaaS) där kunden har större möjligheter att skapa sina egna applikationer [9], men fortfarande utan att behöva bry sig om underliggande operativsystem och annat. Även Microsoft satsar på denna typ av moln med Windows Azure [53].

Mest flexibel av molnnivåerna är den som erbjuder ren infrastruktur (eng. Infrastructure as a Service – IaaS). Här står det kunden fritt att välja hur datorsystemet ska se ut ända ner till hårdvara eller motsvarande. Ofta delas denna typ av moln in i två underkategorier: moln för lagring respektive beräkningar. Störst på IaaS är Amazon [13] och företaget erbjuder både lagrings- och beräkningsmoln med Amazon Simple Storage Service (S3) [51] respektive Amazon Elastic Compute Cloud (EC2) [50].

Ibland lånar MT molndelar av varandra. Tillhandhållare med moln på lägre abstraktionsnivåer, det vill säga IaaS och PaaS, kan dessutom ha MT med moln på högre nivåer som kunder. Exempelvis kan en del av ett IaaS-moln hyras ut till någon som installerar en plattform och sedan erbjuder ett PaaS-moln till sina kunder [27]. På senare tid har leverantörer av IaaS-moln börjat erbjuda en sådan tjänst direkt till slutkunderna istället för att gå via en specialiserad plattformstillhandahållare[55].

Som nämnts ovan har många stora datorföretag gjort satsningar på molnet och fler är på väg. Nyligen har bland andra Dell [59], HP [60] och Apple [61] tagit fram molntjänster. Marknaden var enligt analytiker 2009 värd mellan 17 [28] och 45 miljarder dollar [58] och dessa siffror förväntas ha tredubblats senast 2013 [28, 39, 58]. Åtminstone en av dessa analyser inkluderar dock reklamintäkter från molntjänster [58].

Förutom att hyra del av ett moln från en MT kan en potentiell kund också skapa sitt eget, privata, moln där denne själv står för underhåll. På så vis undviks de säkerhetsproblem som finns förknippade med de hittills behandlade publika molnen, men samtidigt kan man inte fullt ut ta del av den fördelaktiga affärsmodell de senare utlovar [28]. Privata moln kan ses som ett steg i övergången från traditionell IT-infrastruktur till publika moln, men man bör vara noga med att se till att det privata molnet är kompatibelt med sina publika motsvarigheter så att själva bytet verkligen kan ske smidigt och enkelt. Eftersom privata moln är alltför begränsade kommer dessa inte att behandlas vidare i denna rapport.

Slutligen bör man notera en annan term som ibland förekommer, nämligen hybridmoln. Detta är en beteckning för två eller fler sammansatta moln och ofta med en privat och en publik del [32].

2.4 Fördelar med molnet

Molnet har ett antal inneboende fördelar. Kunden kan fokusera på sin verksamhet istället för infrastrukturen och betalar enbart för vad som används, vilket kan leda till lägre anskaffningskostnader och snabbare projektstarter. Dessutom kan det ge minskade operationella kostnader med tanke på att kunden inte behöver lägga lika mycket pengar på kompetens, underhåll, personal med mera [29, 25]. För att behålla vissa kontrollmöjligheter kan det dock vara rekommendabelt att ha kvar viss kompetens och uppdateringsprocedurer i sin organisation [47]. Det faktum att kunden slipper ha stöldbegärlig infrastruktur i sin organisation är ytterligare en fördel.

Molntillhandahållaren har betydligt större infrastruktur än den genomsnittliga potentiella kunden. Ofta kan MT dra nytta av sin stora storlek genom att använda säkerhetsmekanismer som annars inte skulle vara kostnadseffektiva eller genom att helt enkelt erbjuda starkare mekanismer. Till exempel kan MT använda information om en attack mot en kund och skydda övriga kunder mot den attacken bättre än om enskilda kunder skulle samarbeta utanför molnet [25]. Även sådant som svartlistning [15], realtidsövervakning, loggning, buggfixning och förstärkning av operativsystem blir kostnadseffektivare i större skala [28]. Fysiskt perimeterskydd blir billigare per resurs och även om en MT blir en mer attraktiv måltavla för angripare [21] är den också mer robust och har inbyggd flexibilitet mot överbelastningsattacker [28]. Större molntillhandahållare kan till och med anlita särskilda specialiserade leverantörer med molnliknande strukturer för säkerhet. Dessa leverantörer benämns på engelska Managed security service providers och de erbjuder säkerhet som tjänst (eng. Security as a Service) [28]. Slutligen kan molnet ge ökad total nyttjandegrad av tillgängliga resurser vilket kan tänkas ge miljömässiga fördelar.

3 Affärsrelaterade risker

Eftersom molnet för med sig en affärsmodell som är relativt ny, finns det en mängd rent kontraktsmässiga aspekter att beakta och i en del fall är lagar och dylikt inte anpassade för detta nya sätt att använda teknik och göra affärer. Bland annat kan begrepp som mål, angripare och lagringsplats bli otydliga i dessa sammanhang [24].

3.1 Ny affärsmodell

Potentiella kunder måste se till att deras intressen skyddas i de avtal som träffas med MT, framförallt i vad som på engelska kallas Service Level Agreement (SLA). Det kan dock vara svårt att, innan en molntjänst tas i bruk, förutse vad man kommer att behöva och vilja ha när tjänsten väl börjar nyttjas. Många MT har standardkontrakt och det finns viss varians i hur mycket tillhandhållare fokuserar på sekretess och annan säkerhet. En komplex sekretessfråga är att MT av faktureringsskäl måste få reda på kundens konsumtion samtidigt som kunden kan vilja hålla vissa detaljer hemliga [29]. Det är också viktigt att kunden skyddar sig mot en eventuell MT-konkurs vilket kan leda till att data förloras [29] men också hamnar i tredje parts händer [25].

I PaaS-moln är den kontrakterade sekretessnivån generellt lägre än i övriga moln [13], vilket kan tänkas förklaras med att den som molntyp är mindre vanlig och därmed mindre mogen. SaaS-moln är ofta riktade till privatpersoner vilket gör att sekretess begränsas till personlig integritet vilket kan vara lättare att hantera och i IaaS-moln är MT mer tillbakadragen som ägare. Övriga säkerhetsaspekter skyddas bäst i SLA:er för just IaaS-moln [13]. En möjlig förklaring är att kunderna här kräver extra stark säkerhet då det på grund av kompatibilitetsskäl är svårare att byta moln på denna nivå. Rent generellt är stora MT bättre på att informera om säkerhet än mindre [13] och ju flexiblare molnlösning desto mer ansvar för säkerheten faller på kunden. En möjlighet att hantera ökad risk är att försäkra sig och en typ av molnförsäkring har föreslagits [29].

Vissa kunder kan ha möjlighet att specialförhandla med MT för att få med sina önskemål i en SLA specifik för just dem. En molntillhandahållare gav staden Los Angeles i USA, inklusive dess polismyndighet, utökat skydd för sina applikationer i molnet. Bland annat planerades det att data som lagts ut i molnet och som tillhörde offentlig sektor skulle lagras i datorer som var fysiskt separerade från övriga molnet, något som kan vara av vikt på grund av kundinterna policyskäl eller om andra molnkunder agerar olagligt. Vidare lovade det statliga försvarsdepartementet att vissa molnanställda skulle specialcertifieras för att få hantera känslig data. Det är dock oklart om MT tillhandahållit det som överenskommits i specialkontraktet och fördröjningar uppstod vid införandet av molntjänsterna [47].

3.2 Granskning och certifiering

Även med ett för kunden bra kontrakt krävs uppföljning för att kontrollera att MT levererar den prestanda som utlovats och inte felfakturerar vad gäller konsumtion [11, 25]. Loggning och därpå följande granskning av loggarna samt annan typ av kontroll kan vara lämplig [24]. Avvikande inloggningsbeteende, som kan peka på att obehörig försöker få tillgång till systemet, är ett exempel på sådant som kan upptäckas genom loggrevision och som finns i vissa moln idag [16]. Information gällande versioner av mjukvara kan underlätta kundens riskutvärdering men också underlätta för riktade angrepp mot molnet varför en avvägning måste göras. Särskilt viktig är information om attacker som drabbat molnet eller den specifika kunden, för att lära sig av detta och förstärka försvaret [15].

Moln med många kunder kan ha svårt att tillgodose varje enskild kunds önskan om en särskild granskning [28]. Dessutom är ofta en kunds granskningsmöjligheter begränsade på grund av molnets storlek och det faktum att andra kunder inte vill att kunden rotar i

deras data. Därför kan det vara lämpligt att en tredjepartsgranskare anlitas även om inte heller dessa har någon lång erfarenhet inom molnet [25]. Dessa granskare kan kräva tillgång till underlag relaterat till MT:s interna säkerhet, såsom anställningsprocedurer och informationssäkerhetspolicy, samt ökad transparens vad gäller personalövervakning samt angående eventuella intrång [33]. Eftersom moln inte är standardiserade kan det vara svårt att inhämta granskningsinformation från dem [24]. Standardiseringsorganet Cloud Security Alliance erbjuder dock ett fritt tillgängligt protokoll för transparens i molnet [40]. Moln som bygger på öppen källkod kan också underlätta att skapa verktyg för inhämtning.

Certifiering av MT är ytterligare ett sätt att höja tilltron till dessa. I dagsläget är dock sådana möjligheter begränsade då traditionell certifiering, som även den kan ha sina brister, inte är anpassad till molnet [19, 28]. Dessutom gäller certifieringar inte nödvändigtvis i samtliga kunders länder.

3.3 Tillgänglighetsangrepp

Precis som webbsidor kan moln angripas med överbelastningsattacker för att hindra en organisation att utöva sin verksamhet. Verksamhet som tidigare var tydligare avskild från Internet blir mer sårbar vid nyttjande av molntjänster och andra molnkunder utgör ett särskilt hot.

Moln kan av flera orsaker bli otillgängliga och även om sådana händelser kan vara mycket ovanliga kan de få omfattande konsekvenser för enskilda kunder. Enskilda avbrott i stora molnlösningar har nyligen varat i många timmar per år i flera stora moln [36]. Ett moln kan också bli otillgängligt för en enskild kund, exempelvis som resultat av att en angripare fått denne användares konto låst som följd av upprepat felaktiga inloggningsförsök [21]. För att skydda sig mot dessa problem bör kunder med kritisk verksamhet överväga att säkerhetskopiera data som lagras i molnet och att ha alternativa resurser till hands om så behövs. Virtuella maskiner kan underlätta viss säkerhetskopiering eftersom de är byggda för att enkelt kunna kopieras i sin helhet. En kund kan också se till att anlita flera moln och sprida ut sina data i dessa eller använda dem som säkerhetskopior [11, 36, 37]. Det kan noteras att den amerikanska underrättelsetjänsten finansierar ett bolag som investerar i säkra moln som bygger på en viss typ av redundans [56]. Möjligheten att organisationens internetuppkoppling, eller internet som helhet, havererar återstår, vilket får mer allvarliga konsekvenser för verksamhet som främst bedrivs med hjälp av moln.

Eftersom det är möjligt att snabbt öka sina resurser i molnet kan en kund lockas av att skydda sig mot överbelastningsangrepp genom att växa i storlek i molnet i takt med angreppet. Då detta kan leda till väl höga kostnader även under kortare perioder bör dock metoden användas med försiktighet och det kan vara en idé att reglera maximalt acceptabel kostnad i SLA för att istället gå med på att stänga ner sin verksamhet i molnet vid en stark attack [25]. En MT som istället bjuder på sådana meravgifter riskerar att locka till sig kunder som ofta utsätts för just överbelastningsangrepp eller att bli ett slags försäkringsbolag i molnet. Kunder och moln kan också drabbas av tillgänglighetsproblem om någon kunds legitima eller illegitima verksamhet snabbt växer i storlek [25, 28].

Ett mer sofistikerat tillgänglighetsangrepp går ut på att en angripare poserar som potentiell kund i molnet och förhandlar fram kontraktskrav som på något sätt drabbar andra befintliga kunder [29]. Vidare kan en illasinnad molnkunds illegala aktiviteter gå ut över andra kunder vid en polisutredning där utrustning beslagtas. Att flera kunder delar på utrustningen kan också ge utredare juridiska problem att få tillgång till systemet [24]. Dessutom gör virtualiseringen att det kan vara svårt att knyta data till faktisk hårdvara vilket försvårar utredningar samt kan ge upphov till licensproblem för kunder [23, 29]. För att skydda sig mot illasinnade kunder kan MT ha striktare registreringsprocedurer med svarlistningskontroller samt övervakning av kundtrafiken, vilket dock kan vara kontroversiellt [33], och försvåra hanteringen av sekretess och personlig integritet.

3.4 Avveckling

Det kan vara svårt för en kund att avveckla sin verksamhet i ett moln eftersom det ställer krav på att kunna föra över sina projekt till en annan infrastruktur, såsom ett annat moln, samt att det går att ta bort data från det nuvarande molnet. Moln är vanligen inte fullt kompatibla med varandra och kunden kan därför tveka inför att byta molnleverantör [28]. Standarder kan underlätta, men sådana saknas vad gäller dataformat för migration av information samt att hitta andra moln och jämföra molns SLA:er [46]. En standard som kan vara lämplig att nyttja är Open Virtual Format som underlättar distribuering av mjukvara för virtuella maskiner [48]. Fler molnstandarder återfinns i [49]. Att ta bort data permanent från moln kan försvåras av den virtuella aspekten som innebär att det är svårare att identifiera var data är lagrad fysiskt. Dessutom går det inte att skriva över en hel disk eftersom den kan delas av andra kunders VM [28]. Därmed är det svårt att använda traditionella tekniker som att göra fysisk åverkan på disken eller att att skriva över data tillräckligt många gånger. Information som krypterats kan dock i princip tas bort permanent genom att dekrypteringsnyckeln förstörs [41].

3.5 Globaliseringsaspekten

Att lagra eller hantera data på Internet medför att det kan vara svårt att avgöra i vilket land informationen finns och därmed vilka lagar och regler som gäller. Data kanske av regelefterlevnadsskäl måste lagras i ett särskilt land och data som kan hanteras i ett land kan vara olaglig att hantera i ett annat [47]. Vissa MT erbjuder sina kunder möjligheten att lagra specifikt i bland annat USA eller EU [24, 62] men säkerhetskopiering kan komplicera det hela. Dock kan det land där MT är baserad utöva påtryckningar på denne att lämna över data även om den lagras i ett annat land. Vidare riskerar MT att bli tvingad av myndigheterna att stänga ner sitt moln eller läcka kundhemligheter. I det specialavtal som nämndes ovan förhandlade därför Los Angeles fram att man skulle upplysas om alla stämningar som riktades mot molnet ifråga [25]. Slutligen bör man observera att även om molndata lagras i samma land som kunden befinner sig i, kan datatrafik gå över landsgränser och det är normalt svårt att styra vilken väg trafik tar på internet.

4 Teknisk säkerhet

Det största hotet mot molnet är bristande teknisk säkerhet [35, 63]. Moln blir extremt komplexa jämfört med traditionella serverstrukturer och attackytan är stor [47]. Det faktum att flera kunder delar övergripande infrastruktur har också omfattande säkerhetsmässiga konsekvenser [3]. Därför behövs mycket starka säkerhetsmekanismer och nya varianter av säkerhetsverktyg [36] för att kunder ska våga hantera kritisk verksamhetsdata i molnet.

Även om många säkerhetsaspekter tillkommer i molnet är en del fortfarande samma, eller snarlika de, som föreligger i andra infrastrukturer. Beroende vilken nivå molnet ligger på finns det olika säkerhetsfunktioner kund respektive MT måste implementera. På SaaS-nivå kan kunden exempelvis nöja sig med att skydda sina data med kryptering eller vattenstämpling [9] för upphovsrättsskydd samt att se till att använda säker mjukvara. På PaaS-nivå måste virtuella maskiner säkras och isoleras och på IaaS-nivå återfinns standardfunktioner som intrångsdetekteringssystem, brandvägg samt skydd mot skadlig kod och tillgänglighetsangrepp [9]. Ju större möjligheter kunden har att påverka sin egen infrastruktur desto mer säkerhetsansvar måste kunden ta själv [29].

Integrering av kunds säkerhetsmekanismer med molnets tillhandahållna motsvarigheter kan vara av intresse. Enskilda noder i molnet saknar information om molnet i övrigt samtidigt som ett övergripande intrångsdetekteringssystem inte kan läsa kundkrypterad data varför ett samarbete ter sig lämpligt [12]. Ett alternativ är att nyttja en så kallad honeypot som, för en angripare, efterliknar en riktig nod men i själva verket har som enda mål att samla in information om angreppsmetoder. Just virtualisering skapar bra förutsättningar för användning av honeypots.

4.1 Risker hos slutanvändaren

Eftersom kunden har lagt ut data på internet kan inte klassiska säkerhetsmodeller med perimeterskydd direkt appliceras i molnet. Detta medför bland annat att kunden inte längre har någon fysisk åtkomstkontroll. Tvåfaktorautentisering där någon fysisk token krävs vid fjärråtkomst kan därför komma på fråga för att ge en fysisk koppling.

När kunden inte har tillgång till internet, men ändå måste komma åt sina data i ett lagringsmoln, krävs att kunden laddar ner data till lokala datorer vilket för med sig säkerhetsimplikationer. Att säkra infrastrukturen hos slutanvändarna är därmed av vikt. Arbetet kan underlättas av att de klienter som används kan vara mindre kraftfulla och hårdare styrda vad gäller vad som kan installeras. Så kallade tunna klienter kan användas även om dessa från början inte var tänkta att användas i detta sammanhang.

Det kan vidare vara lämpligt för kundens eget skydd att känsliga data är oåtkomliga för användare som nyttjar molnet från en osäker dator eller plats. Dock kan vissa undantag behöva göras. För att erhålla en sådan finmaskighet kan attributbaserad säkerhet vara passande [14]. Med denna visionära åtkomstkontrollsmodell binds dataobjekten ihop med säkerhetsattribut om desamma. Attributen är annorlunda än rent beskrivande, vilka nyttjas för sökning, och kräver högre assurans eftersom de ska användas för åtkomstkontroll. Då generering av dessa attribut kan bli mödosamt krävs någon form av automatisering. En användare som vill ha tillgång till ett objekt måste autentisera sig och användarens attribut, vars värden beror på dennes miljö, matchas sedan mot objektets säkerhetsattribut för att se om tillgång ska ges.

4.2 Kryptering i molnet

Även om kunden krypterar sina data kan angripare komma åt information kring kundens användning av molnet. Det kan vara exekveringstider vilket MT kan lägga märke till [25] eller trafikanalys av data mellan kund och moln. Det senare kan lösas med att även skicka

attrappdata för att förändra trafiken vilket dock gör systemet långsammare [30]. Ytterligare ett problem med molnet är att kunden riskerar att MT läser data under tiden den används, eftersom data måste dekrypteras före användning. Nyligen gjordes dock stora kryptografiska framsteg som möjliggör beräkningar på krypterad data utan föregående dekryptering [22]. Den typ av kryptoalgoritm som används kallas homomorfisk och bygger på att data behåller sin struktur när den krypteras, utan att data läcker ut [31]. Det går därmed att till exempel separat kryptera siffran fem respektive siffran sju och sedan addera de två kryptotexterna följt av dekryptering och siffran tolv erhålls. Själva additionen kan utföras av någon utomstående utan att denne kan komma fram till vilka tal som adderas eller vad resultatet blev [30]. Kryptots styrka är dock till viss del även en svaghet. Eftersom det går att manipulera krypterad data, utan att den förstörs och blir omöjlig att dekryptera, kan vem som helst ändra på krypterade data utan omedelbar upptäckt. I exempelvis den välkända kryptoalgoritmen RSA, som oavsiktligt är delvis homomorfisk i grunden, har särskilda steg tagits för att förhindra detta så att en eventuell förändring av data resulterar i oläsbar klartext efter dekryptering [31]. Alltså saknas den grund för kontroll av datas riktighet som ickehomomorfiska kryptoalgoritmer ger.

Homomorfisk kryptering har flera användningsområden, alla med anknytning till att utföra beräkningar på hemlig data i en osäker miljö. Metoden passar därför mycket väl i molnet [30]. MT kan dock, precis som i andra kryptoalgoritmer där beräkningar sker i klartext, påverka dataintegriteten. Detta passar alltså främst när konfidentialitet är viktigare än riktighet (integritet). I moln som bara används för lagring nyttjas ickehomomorfiskt krypto. Andra användningsområden för homomorfisk kryptering är bland annat så kallade mjukvaruagenter som samlar in data från datorer och rapporterar hem till en central server, skadlig kod som vill dölja sin närvaro eller exakta beteende samt upphovsrättsskydd där mjukvarutillverkare kan dölja sin kod [30]. I dagsläget är dock beräkningar med homomorfiska kryptotexter mycket långsamma varför mer forskning krävs innan det på allvar kan bli användbart i praktiken [22]. Mer om krypto i molnet kan läsas i avsnittet om sidokanaler nedan.

4.3 Betrodd plattform

Ett alternativ till homomorfisk kryptering är att kunden trots allt kan lita på infrastrukturen. För att försäkra att en dator är i ett visst betrott tillstånd och att den därmed inte har manipulerats av någon kan en betrodd plattform (eng. trusted platform) användas, som namnet till trots går att kombinera med alla molnnivåer. Den mest utbredda betrodda plattformen är Trusted Platform Module (TPM) [20] som bygger på både hårdvara och mjukvara. Hårdvaran innehåller bland annat en kryptogrundnyckel som bränts in. Datorns konfiguration och integritet kontrolleras före tillgång till kryptofunktioner ges. För att undvika att någon illasinnad applikation kan avlyssna kommunikation mellan TPM och applikation, används ett avskärmat minne samt förseglad lagring [5].

TPM är anpassat för att kunna intyga sin konfiguration för en certifikatserver vilket kan användas för att en kund ska kunna lita på att ett moln tillhandahåller en korrekt och säker TPM. Även om TPM anses förhållandevis motståndskraftigt mot fysiska angrepp, bör det noteras att plattformen inte designats för sådant [8, 6], och där har MT en specialställning. Vidare kan en hårdvarulösning vara kostsam och göra det svårare att byta infrastruktur eller moln [10]. Dessutom är TPM komplex vilket gör en säkerhetsanalys svårgenomförd.

4.4 Sidokanaler

En sidokanal är en oönskad sidoeffekt av legitim funktionalitet som kan användas av en illasinnad aktör för att kommunicera utan att traditionella brandväggar och liknande skydd kan upptäcka detta. Ett molnrelaterat exempel på en sidokanal beskrivs nedan.

För att spara på resurser som diskutrymme, bandbredd och ström använder en del MT som erbjuder lagringsmoln en teknik benämnd källbaserad deduplicering (eng. deduplication) [2, 1]. Om en kund försöker laddar upp data som är identisk med andra data som redan existerar i molnet genomförs ingen uppladdning i dessa system utan enbart en ny genväg eller pekare skapas. Om en annan användare var den som lade upp det första dataobjektet delar två användare nu på samma data. Det kan noteras att detta försvårar säkerhetskopiering för den enskilde kunden [18] och är ett slags motpunkt mot cachelagring. Dessutom bör det observeras att metoden som avgör om två filer är identiska eller ej bygger på så kallad hashning som inte nödvändigtvis är kollisionsfri. Det finns därmed en risk att två filer klassificeras som identiska fastän de inte är det.

Genom att göra uppladdningsförsök och mäta om försöket avbryts eller inte kan en illasinnad kund på grund av dedupliceringen ta reda på om viss data redan finns i molnet. Detta är en typ av sidokanal som exempelvis kan användas av upphovsrättsinnehavare som vill kontrollera om molnet lagrar upphovsrättsskyddad data. Dessutom kan det tänkas att en angripare känner till en del av en kunds fil men inte hela. Då kan angriparen prova sig fram genom att göra små ändringar i en fil och ladda upp tills rätt fil har hittats. Om en angripare lyckats ta sig in i en annan kunds konto, men inte kan kommunicera ut via vanliga kanaler utan att det märks i en brandvägg, kan den nämnda sidokanalen användas som dold kanal [18].

För att undvika denna sidokanal krävs någon form av kompromiss mellan resursbesparing och säkerhet, såsom att begränsa deduplicering till stora eller slumpmässiga filer, vilket dock kan vara kostsamt för MT [4]. Så kallad konvergent kryptering, som tillåter deduplicering, gör att också den beskrivna sidokanalen kvarstår. Denna ovanliga form av kryptering bygger på att nyckeln baserar sig på enbart klartexten vilket gör att två identiska filer får samma kryptotext [1].

Det är svårt att eliminera sidokanaler utan att också påverka molnets prestanda. Andra kunder kan, genom att mäta hur mycket de kan och får utnyttja molnets prestanda, ta reda på aspekter om andra kunders användning [25]. I större moln får dock sådana möjligheter ses som mycket begränsade om inte en betydande del av de andra kunderna hjälper till. Om VM inte är perfekt isolerade från varandra kan dataläckage ske på en molndator och därmed potentiellt mellan kunder. En stor kund kan som säkerhetsåtgärd se till att MT ordnar så att bara kunden får tillgång till en specifik dator. För mindre kunder skulle en sådan metod göra att molnet blir mindre effektivt [26]. Enligt [17] kände man 2010 inte till några dolda kanaler i moln.

4.5 Virtualiseringens risker

Virtuella maskiner är lättföränderliga och genom att ladda en annan så kallad virtuell bild (eng. virtual image) kan operativsystem bytas eller konfigurationer ändras. Detta kan leda till problem med proveniens och spårbarhet vid granskning [38]. Vidare går VM-instanser att klona vilket underlättar installationsprocedurer, men eftersom en klon samtidigt kan ha mer gemensamt med originalet än enbart operativsystem kan säkerhetsproblem uppstå. En angripare kan bli kund i molnet och specialstudera en VM, för att sedan angripa övriga molnet mer effektivt. Det faktum att flera virtuella maskiner körs på en dator kan påverka säkerheten för kryptografiska slumptal som hårdvaran genererar, genom att slumptal konsumeras för snabbt eller att klonade VM delar vissa hemligheter [21]. Ett annat säkerhetsproblem är att en avstängd virtuell maskin kan angripas på ett sätt som inte en avstängd dator kan. Eftersom perimetersskydd saknas, kan vissa säkerhetsverktyg potentiellt fungera dåligt i en VM-miljö. Dessutom blir processorkrävande applikationer såsom många antivirusprogram alltför långsamma i virtuella maskiner [7].

5 Slutsatser

Även med den relativt exakta definition som ges i början av denna rapport finns vissa gränsfall om vad som faller under benämningen moln och vad som är andra typer av tjänster via internet. Samtidigt kan molnskapare lära sig, och inspireras av, dessa närbesläktade tekniker och modeller. Datorkraft på kran är en ny trend som kan göra att organisationer bättre kan fokusera på sin verksamhet. På sikt kanske IT kommer att införskaffas på samma sätt som el med tillförlitlig distribution, men också reservkraft för essentiella processer. Flera stora datorföretag har gått över till att alltmer fokusera på molntjänster och för kunder är det nu möjligt att mycket snabbt få samma kraft som i en superdator.

I takt med att molnområdet mognar och stabiliseras måste man förvänta sig att lagar och regler bättre anpassas till den nya affärsmodellen samt de nya teknikerna. Dessutom krävs erfarna och specialiserade granskare samt certifieringsorgan för att kunder ska kunna lita på molnleverantörerna. Vidare är standardisering en kritisk aspekt för att undvika en inlåsningseffekt. Nya säkerhetsmodeller måste också tas fram, inte minst då den traditionella perimetermodellen inte längre är tillämplig. Attributbaserad säkerhet, betrodda plattformar, välisolerade virtuella maskiner och homomorfisk kryptering kan så småningom göra det möjligt att använda molnet för att lagra, och utföra beräkningar på, till och med de mest hemliga av data.

6 Källförteckning

1. Douceur et al., Reclaiming *Space from Duplicate Files in a Serverless Distributed File System*, IEEE, 2002.
2. Gunawi et al., *Deconstructing Commodity Storage Clusters*, IEEE, 2005.
3. Vaquero et al., *Locking the sky: a survey on IaaS cloud security*, Springer Verlag, 2011.
4. Dutch et al., *Understanding Data Deduplication Ratios,* Storage Networking Industry Association, 2009.
5. *TPM Main Part 1 Design Principles*, TCG, 2007.
6. Tarnovsky, *Hacking the Smartcard Chip,* Blackhat 2010.
7. Kaufman, *Can Public-Cloud Security Meet Its Unique Challenges?*, IEEE, 2010.
8. Halderman et al., *Lest We Remember: Cold Boot Attacks on Encryption Keys*, Princeton University, 2008.
9. Hwang et al., *Trusted Cloud Computing with Secure Resources and Data Coloring*, Trust & reputation management, IEEE, 2010.
10. Anderson, *Cryptography and Competition Policy - Issues with "Trusted Computing"*, Cambridge University, 2003.
11. Rocha et al., *Confidentiality and Privacy in the Final Fronier: Inside the Clouds*, IEEE, 2011.
12. Vieira et al., *Intrusion Detection for Grid and Cloud Computing*, IT Pro, IEEE, 2010.
13. Chakraborty et al., *The Information Assurance Practices of Cloud Computing Vendors*, Cybersecurity, ITPro, IEEE, 2010.
14. Kuhn et al., *Adding Attributes to Role-Based Access Control*, IEEE, 2010.
15. Spring, *Monitoring Cloud Computing by Layer, Part 1*, It All Depends, IEEE, 2011.
16. Spring, *Monitoring Cloud Computing by Layer, Part 2*, It All Depends, IEEE, 2011.
17. Jaeger et al., *Outlook: Cloudy with a Chance of Security Challenges and Improvements*, Secure Systems, IEEE, 2010.
18. Harnik et al., *Side Channels in Cloud Services*, Cloud computing, IEEE, 2010.
19. Borenstein et al., *Cloud Computing Standards Where's the Beef?*, Standards, IEEE, 2011.
20. ISO/IEC 11889-1:2009, *Information technology -- Trusted Platform Module -- Part 1: Overview*, ISO, 2009.
21. Grobauer et al., *Understanding Cloud Computing Vulnerabilities, Cloud computing*, IEEE, 2011.
22. Gentry, *Fully Homomorphic Encryption Using Ideal Lattices*, Stanford University, 2009.
23. Zhou et al., *Towards a Data-centric View of Cloud Security*, CloudDB 2010, 2010.
24. Taylor et al., *Forensic investigation of cloud computing systems*, Network Security, 2011.
25. Molnar et al., *Self Hosting vs. Cloud Hosting: Accounting for the security impact of hosting in the cloud*, Microsoft Research, 2010.
26. Ristenpart et al., *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds*, CCS 09, 2009.
27. Vaquero et al., *A Break in the Clouds: Towards a Cloud Definition*, ACM Sigcomm editorial, 2009.
28. Cloud computing, *Benefits, risks and recommendations for information security*, Enisa, 2009.
29. Takabi et al., *Security and Privacy Challenges in Cloud Computing Environments*, Cloud Computing, IEEE, 2010.
30. Young et al., *Malicious cryptography*, Wiley 2004.
31. Anderson, *Security Engineering*, Wiley, 2001.
32. *The NIST Definition of Cloud Computing (Draft)*, NIST, 2011.
33. *Top Threats to Cloud Computing V1.0, Cloud Security Alliance*, 2010.
34. Foster, *What is the grid? - a three point checklist*, GRIDtoday, 2002.
35. Bruening et al., *Privacy, Security Issues Raised by Cloud Computing*, Privacy &

Security Law, BNA, 2009.
36. Armbrust et al., *A view of cloud computing*, Communications of the ACM, 2010.
37. Bessani et al., *DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds*, ACM, 2011.
38. Wei et al., *Managing security of virtual machine images in a cloud environment*, CCSW 09, ACM, 2009.
39. Chow et al., *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control*, CCSW 09, 2009.
40. Knode, *Cloud Trust Protocol Orientation and Status*, Cloud Security Alliance, 2011.
41. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, Cloud Security Alliance, 2009.
42. Goasguen et al., *Involuntary Computing: Hacking the Cloud*, Clemson University School of Computing, 2010.
43. *Botnets: Detection, Measurement, Disinfection & Defence*, Enisa, 2011.
44. *Microsoft Security Intelligence Report*, Microsoft, 2010.
45. *Oracle's Ellison nails cloud computing*, Cnet, tillgänglig på http://news.cnet.com/8301-13953_3-10052188-80.html, 2008, kontrollerad 2011-08-29.
46. *NIST Cloud Computing Standards Roadmap*, NIST, 2011.
47. *Guidelines on Security and Privacy in Public Cloud Computing*, NIST, 2011.
48. *Open Virtualization Format Specification*, Distributed Management Task Force, 2010.
49. *Cloud Standards Wiki*, tillgänglig på http://cloud-standards.org, kontrollerad 2011-08-29.
50. *Amazon Elastic Compute Cloud (Amazon EC2)*, Amazon, tillgänglig på http://aws.amazon.com/ec2/, kontrollerad 2011-08-29.
51. *Amazon Simple Storage Service (Amazon S3)*, Amazon, tillgänglig på http://aws.amazon.com/s3/, kontrollerad 2011-08-29.
52. *Google App Engine*, Google, tillgänglig på http://code.google.com/intl/sv/appengine/, kontrollerad 2011-08-29.
53. *Windows Azure*, Microsoft, tillgänglig på http://www.microsoft.com/windowsazure/, kontrollerad 2011-08-29.
54. *Salesforce*, tillgänglig på http://www.salesforce.com, kontrollerad 2011-08-29.
55. *AWS CloudFormation Sample Templates*, Amazon Web Services, tillgänglig på http://aws.amazon.com/cloudformation/aws-cloudformation-templates/, kontrollerad 2011-08-29.
56. *Cleversafe Selected by IQT for Strategic Deployments Supporting U.S. Intelligence Community*, tillgänglig på http://www.iqt.org/news-and-press/press-releases/2010/Cleversafe_10_25_10.html, kontrollerad 2011-08-29.
57. *Google Docs*, tillgänglig på http://docs.google.com, kontrollerad 2011-08-29.
58. *Forecast: Sizing the Cloud; Understanding the Opportunities in Cloud Services*, Gartner, 2009.
59. *Dell Announces Its First Public Cloud Offering*, tillgänglig på http://content.dell.com/us/en/corp/d/press-releases/2011-8-29-dell-vmware-public-cloud-datacenter.aspx, kontrollerad 2011-08-29.
60. *HP Sets Strategy to Lead in Connected World with Services, Solutions and Technologies*, tillgänglig på http://www.hp.com/hpinfo/newsroom/press/2011/110314xa.html, kontrollerad 12:12 2011-08-29.
61. *iCloud*, tillgänglig på http://www.apple.com/icloud/, kontrollerad 2011-08-29.
62. *Secure applications to meet the needs of government*, tillgänglig på http://www.google.com/apps/intl/en/government/trust.html, kontrollerad 2011-08-29.
63. Oram et al., *Beautiful Security*, O'Reilly, 2009.