Relevans av tekniskt skydd för tillit

Smeets, Ben

Published in:
DigiTrust: Tillit i det digitala. Tvärvetenskapliga perspektiv från ett forskningsprojekt

2014

Relevans av tekniskt skydd för tillit

Ben Smeets

En intressant fråga är i vilken utsträckning som tillit i det digitala samhället beror på säkerheten i de tekniska lösningarna. För en tekniskt kunnig person kan det kännas uppenbart att tekniken i ett digitalt system måste vara korrekt vald och utförd för att systemet ska vara tillförlitligt. I de fall där brister i säkerheten kan medföra stor skadeinverkan, är tekniken en viktig del i att begränsa riskerna att skada uppstår, eller att en viss lösning överhuvudtaget kan skapas och användas.

Det är dock oklart hur tekniken i sig leder till att användare litar på ett digitalt system. Men innan vi går vidare med denna fundering så är det relevant att undersöka hur yrkesverksamma inom IT-säkerhet ser på tillitsfrågan. Där har det blivit viktigare att produkten inte bara implementerar lämpliga säkerhetsmekanismer, men också att man kan lämna dokumentation på att dessa är realiserade på ett korrekt sätt för ändamålet.

Ett exempel hur man arbetar kring dessa frågor är tillämpningen av Common Criteria-metodiken (CC) som är standardiserad i ISO/IEC15408 standarden, se (Common Criteria). Med hjälp av CC kan en beställare och tillverkare beskriva säkerheten för sitt system och vilken nivå av grundlighet man vill ha, samt har uppnått vid tillverkning.

Även om CC har sina brister (Zhou C & Ramacciott S, 2011) – det anses vara dyrt och byråkratiskt samt att det nämligen går att avgränsa sitt system till den grad att CC inte kan ta tillräckligt med hänsyn till systemets faktiska användning – så ger användandet av CC en viss försäkran att en IT-produkt uppfyller de säkerhetskrav man förväntar sig, och följaktligen går att lita på. CC är dock enbart ett instrument som riktar sig till de som beställare, tillverkar och granskar produkter. Användare, bortsett från ev. krav på dokumentation och instruktioner, betraktas ej. Dessutom kräver CC-dokumenten att läsaren är kunnig i området, vilket medför att en användare i regel inte kan tolka CC-dokument på ett sådant sätt att det ökar dennes tillit

till produkten. Detta är dock egentligen inget fel hos CC, utan snarare en typisk brist: att det krävs mycket kunskap för att tolka det tekniska säkerhetsarbetet kring en IT-produkt.

När man då frågar en person i vilken utsträckning denne litar på ett IT-system, är det för de flesta en fråga som personen i fråga inte kan basera på egen kunskap om systemets tekniska säkerhet. Det blir en fråga där personen viktar sina olika åsikter och erfarenheter. Enkätsvaren tyder på att det är möjligt att ha IT-system i drift som människor huvudsakligen litar på. Vi såg att 85% svarar att de instämmer helt eller delvis på frågan om de har förtroende för olika betalningsmetoder och internetbaserade banktjänster för att betala räkningar och 87% när det gäller kontoöverföringar. Motsvarande siffra för kontanter är 87%. Bankernas internetbaserade tjänster för betalningar åtnjuter alltså en hög tillit som ligger på samma nivå som kontantbetalningar. Vad gör bankerna mer rätt än andra, mer tekniskt profilerade företag, som är aktiva inom sociala media? Det finns studier som behandlar frågan (Eriksson et al, 2005; Meuter et al, 2000). Utan grundligare studier om de inblandade mekanismer na om hur bilden om tillit växer fram, så kan vi inte säga mer än att det finns skillnader i hur man lyckas med att skapa tillit. Som ett första led att hitta en förklaring är det intressant att peka på några egenskaper som kan spela en roll.

Banker investerar mycket pengar i olika säkerhetssystem, såväl vid fysisk utformning (säkra serverhallar) som vid val och realisering, och drift av procedurer och IT-system. Det gör de även om tjänsten som banken säljer i sig inte är en säkerhetsprodukt (om vi bortser från att banken förvarar tillgångar). Bankerna använder mycket teknik för att skapa säkerhet, men kompletterar detta också med procedurer och image-formande aktiviteter där de vill måla upp en bild av en stark och pålitlig internetbank, ex. SEB: ”--- Internetbanken är alltid öppen och lika trygg som ett vanligt bankkontor. ---”

Bankernas verksamhet är ganska regelstyrd av olika föreskrifter och erforderliga tillstånd. Detta framgår av lagen (2004:297) samt förordningen (2004:329) om bank- finansieringsrörelse. För sparbanker finns det även regler i sparbankslagen (1987:619) och för medlemsbanker i lagen (1995:1570) om medlemsbanker. Dessutom finns det en viss tillsyn av bankverksamheten så att den uppfyller de ställda kraven för tillstånd. I Sverige hanteras detta av Finansinspektionen (FI). Det finns alltså – beroende på hur samhället i allmänhet fungerar i sin kravställning och uppföljning – mekanismer som ska ge en försäkran att banken uppför sig som allmänheten förväntar sig. Detta i sig skapar en sorts tillit, men kanske viktigare är förutsägbarheten som uppstår av ett transparent regelverk och tillsyn. Den bidrar till en bild att bankverksamheten i sin helhet går att lita på.

Slutligen finns det inte markanta skillnader vad gäller de internet-relaterade banktjänster som bankerna erbjuder sina kunder. Här ser slutkunder ofta de skillnader som finns bland de metoder bankerna använder för att realisera autentisering, dvs metoden som banken använder för att säkerställa vem som logga in, samt de behörigheter som ska gälla för den som släpps in i banktjänstsystemet. Här finns allt från manuella koder som kunderna får hemskickade, till s.k. inloggningsdosor och speciella appar till mobila enheter (ex. Mobilt BankID).

Dessa metoder upplevs av kunderna på ett sådant sätt som skulle kunna påverka helhetsbilden, men vi har inga öppna fakta för att kunna förstår hur och i vilken utsträckning som kunderna påverkas. (dock vet vi från studier att användarvänligheten spelar en roll vad gäller adoption (Lichtenstein & Williamson, 2006). Men återigen så har kunderna svårt att kunna bedöma säkerheten. Även de som är kunniga säkerhetsmässigt kan för det mesta inte skapa en komplett helhetsbild för att göra en sådan bedömning. Bankerna brukar vara medvetet sparsamma med information om sina system. Vilket man i regel inte är för att man vill dölja brister i sitt system, istället styrs detta mer av vetskapen att utsattheten ökar om personer utanför har precisa kunskaper om systemets olika delar och funktioner.

En annan faktor som kan bidra till resultatet för den höga tilliten i banktjänster kan finnas påvisad i andra studier, t.ex. Hain, (2003) där man konstaterar att banktjänstanvändare som inte använder internettjänsterna, är mer bekymrade kring säkerhet och integritet än användare som använder internettjänsterna. Många respondenter (74%) i vår studie instämmer helt eller delvis med påståendet "Jag har god kunskap om hur man använder Internet". 72% av de som svarar instämmer helt eller delvis att de hjälper gärna andra med att använda Internet. Vi har alltså en grupp som känner sig veta hur man använder bankernas internettjänster och som är positivt kring att hjälpa andra med Internetanvändning.

Bilden som framträder är att kopplingen mellan teknikval i en digital banktjänst och tillit finns, men att kundernas tillit förmodligen är ett resultat av en rad andra faktorer. En direkt följdfråga är då om bankkunderna gör rätt att lita på deras banktjänster. Eftersom man strikt taget inte kan få några garantier som kund är svaret här egentligen: nej det gör de inte. Här finns också resultaten från olika studier, t.ex. (Hole, 2008, 2011) i Norge, brister i vissa implementeringar av säkerhetsprotokollet TLS (2011, 2013, 2014) men också allvarliga driftstörningar som gör att man inte kan lita på banktjänsten. Eftersom det inte finns en bank (i Sverige) som upplevs som felfri i detta hänseende och eftersom man rent praktiskt är tvungen att använda en banktjänst är således slutsatsen att ett konstaterande att man strikt taget inte kan lita på banken är praktiskt oanvändbart. Medvetet eller omedvetet så är man tvungen

att ta risker om man vill använda digitala banktjänster. Utöver dessa överväganden så är tillitsfrågan också en fråga om bilden som banken målar upp om sig själv och de rykten kring hur man klarar av hantera brister och misstag. Faktum kvarstår att i praktiken så är den enskilde tvungen att praktisera en viss tillit till sin digitala banktjänst om han eller hon vill använda den och tilliten då inte direkt bottnar i bankens teknikval vad gäller säkerhet.

Kan man då våga dra slutsatsen att bankernas arbete med säkerhetsteknik är onödig eftersom deras kunder inte värdesätter den? Troligen inte. Förmodligen säger resultaten enbart att bankerna har inget att vinna på att synliggöra för kunderna deras val av teknik för att förbättra kundernas tillit. Arbetet med säkerhetsteknik är då mer en konsekvens av formella krav på verksamheten samt en del av arbetet med att upprätthålla ett skydd mot missbruk och attacker mot bankens digitala banktjänster. I vissa fall kan konkurrenternas agerande eller konsumentgrupper påverka val av teknik. Vidare kan rätt val av teknik minimera risken att något går fel och att proceduren att hantera eventuella fel inte blir kostsamma.

Det är frestande att tänka sig att också för andra digitala tjänster vi har en liknande situation att slutanvändarnas tillit inte alls eller bara i liten omfattning direkt påverkas av teknikval vad gäller säkerheten. I likhet med bankerna så används tekniken där av tjänsteleverantören som ett medel för att uppfylla formella och informella krav samt som ett medel att förebygga problem på grund av missbruk eller intrång. Det är få digitala tjänster där säkerhetsteknik lyfts särskild fram som en del av argumentationen att man kan lita på tjänsten. Mest känd är de så-kallade VPN tjänsterna för att skapa krypterade tunnlar för dataöverföring och molnlagring där data som läggs i molnet är krypterad och därmed oläsbart även för den som tillhandahåller lagringstjänsten. Dock, också här är argumentationen mot kunder mer byggd varför man behöver en VPN, att man har många kunder och att man eventuellt kan mer konkret peka på kända grupper eller personer som använder en specifik lösning. I regel måste kunderna som vill veta mer om de tekniska lösningarna gräva fram denna information genom egen analys eller via användarfora. I regel vet många användarna av VPN-tjänster inte ens om vilken teknik som används i den VPN tjänst man använder; t.ex. så kan du bygga på (D)TLS protokollet eller IPsec protokollet. Kunskapen om detta kan spela en roll om något fel upptäckts in en viss lösning, jmf Heartbleed-problemet i TLS implementationen Open SSL. Bortsett från enstaka kunniga och yrkesmässiga så har de flesta som använder digitala tjänster inte den förmågan att själv bedöma om man kan lita på tjänsten eller ej. De flesta användarna är beroende av vad andra säger eller vilka lösningar andra använder när man ska välja en digital tjänst eller måste bedöma om man kan lita på tjänsten.

Referenser

Common Criteria (n.d.). *Common criteria for information technology security evaluation (ISO/IEC 15408) for computer security certification.* http://www.commoncriteriaportal.org/cc/ [2014-05-19]

Duong, T. & Rizzo, J. (TLS 2011). Here Come The ⊕ Ninjas, http://www.infoworld.com/sites/infoworld.com/files/pdfe/BEAST_Duong_Rizzo.pdf [2014-05-19]

Eriksson, K.; Kerem, K. & Nilsson, D. (2005). Customer acceptance of internet banking in Estonia, *Int Journal of Bank Marketing,* 23 (2), 200-216.

Hole, K.J.; Tjøstheim, T.; Moen, V.; Netland, L.-H.; Espelid, Y. & Klingsheim, A.N. (2008). Next generation internet banking in Norway. *Teknisk Rapport 371*, Institutt for informatikk: Universitet Bergen. http://www.nowires.org/Papers-PDF/BankIDevaluation.pdf [2014-05-19]

Hole, K.J.; Klingsheim, A.N.; Netland, L.H.; Espelid, Y.; Østheim, T. & Moen, V. (2009). Risk assessment of a national security infrastructure. *IEEE Security & Privacy*, 7(1), 34-41

Jackson, W. (2007). Under attack: common criteria has loads of critics, but is it getting a bum rap. *Government Computer News, Aug.* http://gcn.com/articles/%202007/08/10/under-attack.aspx [2014-05-20]

Lichtenstein, S. & Williamson, K. (2006). Understanding consumer adoption of internet

banking: an interpretive study in the Australian banking context. *Journal of Electronic Commerce Research*, 7(2), 50-66.

Meuter,M.L.; Ostron,A.L.; Roundtree, R.I. & Bitner, M.J., (2000), Self-service

technologies: understanding customer satisfaction with technology based service encounters, *Journal of Marketing*, 64 (3), 50-64.

Sepehrdad, P; Vaudenay, S.; Vuagnoux, M. (TLS 2013). Discovery and exploitation of new biases in RC4. *Lecture Notes in Computer Science* 6544, 74–91.

Heartbleed bug (TLS 2014). Bug CVE – CVE-2014-0160". Cve.mitre.org. [2014-05-11]

Zhou, C. & Ramacciott, S. (2011). Common criteria: its limitations and advice on improvement. *Information Systems Security Association Journal,* April 2011, 24-28.