Förord

Denna rapport ingår i ett kandidatarbete utfört vid Institutionen för Data- och informationsteknik, Chalmers tekniska högskola våren 2013. Rapporten beskriver utvecklingen av ett NFC-baserat låssystem bestående av mjukvara till en Androidbaserad mobiltelefon samt en mikrokontroller av Arduino-typ.

Projektgruppen önskar tacka Lars Svensson för den tid han har lagt ner för att handleda projektet samt (någon mer för något annat?).

Abstract

In english motherfucker.

Sammanfattning

Mobiltelefonen utökas idag ständigt till att klara av att utföra fler och fler uppgifter åt dess användare. De saker vars funktioner nu erbjuds genom dagens mobiltelefoner behövs alltså inte längre tas med. Det här arbetet handlar om att ersätta nyckelknippan genom att ge mobiltelefonen funktionen att låsa upp en dörr, vilket ger att de otympliga nycklarna inte längre behöver tas med.

För att kunna erbjuda den önskade nya funktionalliteten har en applikation för Android utvecklats, vilken användaren agerar mot för att kunna låsa eller låsa upp dörren. Vidare har en låsenhet utvecklats kring Arduino-plattformen vilken kommunicerar mot mobilapplikationen via NFC (Near Field Communication) och har möjligheten att styra en elektrisk låskolv.

Säkerheten i systemet består i att användaren verifierar sig mot applikationen med förvald PIN-kod och kommunikationen är krypterad med krypteringsalgoritmen RSA(fotnot 1) med 512 bitar.

fotnot 1: efter upphovsmännen Ron Rivest, Adi Shamir och Len Adleman

Innehåll

1 Inledning

När mobiltelefonen först lanserades var den stor, otymplig och dyr, med kommunikation som enda syfte. Sedan dess har utveckligen eskalerat kraftigt och allt fler funktioner har integrerats, medan själva mobiltelefonen har gjorts mindre, smidigare och mer tillgänglig för allmänheten. Idag äger i princip alla en mobiltelefon och byter dessutom ofta, då det är både relativt billigt att köpa en ny samt att tekniken snabbt framskrider. På grund av detta är branchen hårdare än någonsin och för att överleva måste produkterna hela tiden utvecklas och innehålla nya, smarta funktioner för att bli konkurrenskraftiga på den snabbt skiftande marknaden.

Stryk den gamla inledningen här under, ett förslag. Allt sedan mobiltelefonen först lanserades har utvecklingen gått mot att integrera allt större funktionalitet i denna. Anledningen till detta är att mobilen oftast finns nära till hands och har därmed möjligheten att på sikt nästan ersätta alla de saker vi bär med oss. Anteckningar, miniräknare, alarmklocka, kalender och musikspelare är bara några av de funktioner som har integrerats och tillverkarna av mobiltelefoner ser det som en konkurrensfördel att föra in ytterligare funktioner i deras nya produkter.

På senare tid har övergången till så kallade smarta telefoner ytterligare bidragit till att öka funktionaliteten hos mobiltelefonen. Numera är den ej enbart ett redskap för kommunikation, utan en enhet med lika många eller till och med fler funktioner än en fullskalig persondator. En av anledningarna till denna utveckling är framstegen inom integrerade kretsar och dess tillverkningsteknik. Dessa faktorer har bidragit till att fler transistorer kan placeras på en mindre yta och därmed göra elektronikkomponenter både mindre, strömsnålare, snabbare och mer funktionella. Den direkta följden av detta är att mobiltelefonen nu kan inrymma både funktionaliteten av fler kringenheter, samt inneha kraft nog att hantera dem alla.

Wifi och Bluetooth är exempel på tekniker för kommunikation som i stort sett alltid finns inbyggt i en mobiltelefon och nu börjar även en ny teknik få allt större utbredning, NFC. Detta är en teknik för tillförlitlig kommunikation över korta avstånd som bland annat ligger till grund för en senare ansats att försöka ersätta något vi alltid bär med oss, plånboken. Tanken med denna produkt som i många fall kallas den mobila plånboken, vilket Timalsina (2012) beskriver, är att göra anspråk på att ersätta våra kontanter, rabatt- och kreditkort med programvara i mobiltelefonen.

Idén bakom detta arbete baseras på samma tankegångar som de som ligger bakom utvecklingen av trådlös betalning. Kandidatarbetet åsyftar till att utveckla en prototyp av ett låssystem som tillåter användaren att på ett

snabbt och bekvämt sätt låsa upp dörren till sitt hem med sin mobiltelefon. Till denna funktionalitet planeras användningen av samma kommunikationsteknik som ligger till grund för den mobila plånboken, NFC.

Resultatet av kandidatarbetet kan vara en mycket åtråvärd produkt för privatpersoner som är trötta på att leta efter sina hemnycklar samt önskar en flexiblare lösning än den klassiska nyckeln. Målet är att ytterligare följa trenden med en allt mer funktionell mobiltelefon genom att också använda den som en nyckel.

Visionen för en färdig produkt av detta slag, och alltså inte för resultatet av detta kandidatarbete, är att den funktionellt ska kunna användas i större företag där det finns hundratals dörrar som utrustats med det utvecklade låset samt tusentals anställda som alla använder den dedikerade mobilapplikationen för att kontrollera låsen. Många accessnivåer kan finnas där en specifik användare kan ingå i valfritt antal. Produkten kan underhållas av en central enhet som snabbt, smidigt och säkert kan konfigurera om systemet efter givna instruktioner.

Det finns också andra visioner för en färdig produkt av detta slag. Låssystemet behöver nödvändigtvis inte vara ett stort, relativt komplext och centraladministrerat system utan kan i stället vara litet, simpelt och mobilt så som ett cykellås eller ett hänglås. Då en låsprodukt av projektets slag kan utformas som sådant har en framtida produkt potential att ersätta även dem. Vem skulle inte önska sig ett hänglås där borttappandet av nyckeln inte innebär ett behov att klippa låset?

1.1 Syfte

Syftet med rapporten är att redogöra för hur en prototyp av ett låssystem designas och implementeras. Låssystemet består av en mobilapplikation och en mikrokontroller där mikrokontrollern är integrerad i låset samt exekverar egenutvecklad mjukvara. Skulle det visa sig att produkten inte uppfyller kravspecifikationen ska en analys genomföras i vilken en fullständig slutprodukt beskrivs teoretiskt.

1.2 Utmaningar

Tre huvudsakliga utmaningar identifierades.

- Stora delar av NFC:s kommunikationsstack måste implementeras för mikrokontrollern. Kommunikationsstacken måste vidare utformas efter hur Androids NFC-stack är uppbyggd. Att implementera kommunikationsstacken medför en större utmaning då den är relativt komplex,

innehåller ett flertal olika nivåer, och dokumentation kring Androids implementation är bristfällig.

- Att implementera en lättanvänd Androidapplikation vilken ska innehålla funktioner för att kommunicera mot mikrokontrollern via NFC. Androidutveckling medför ytterligare svårigheter jämfört med vanlig mjukvaruutveckling då hänsyn måste tas till Androids egenheter. En förståelse för de bibliotek vilka styr NFC-kommunikationen måste också byggas upp.

- Att implementera säkerhet vid NFC-kommunikation. Då en mikrokontroller generellt inte har mycket minne eller hög klockfrekvens kan dessa egenskaper skapa utmaningar då säkerhet i form av kryptering ofta kräver omfattande beräkningskapacitet samt minnesutrymme.

1.3 Omfattning

Rapporten beskriver endast konstruktionen av en prototyp utav en produkt av det beskrivna slaget. Vidare beskriver rapporten de nödvändiga förkunskaperna som krävs för en konstruktion av en sådan prototyp. Prototypen skall kortfattat utnyttja kommunikation via NFC med applicerad säkerhet och därför är förkunskaper inom dessa ämnen nödvändiga.

Mobilapplikationen begränsas till endast Android eftersom det är lättillgängligt, välkänt och lämpligt för användningsområdet. Denna avgränsning kommer också naturligt av att det bara finns stöd för NFC hos ett fåtal telefoner där merparten av dem är basereade på Android.

Mikrokontrollern med ansvar för låset baseras på Arduino-plattformen. Arduino valdes för dess enkla och tydliga utvecklingsmiljö samt för att många källkodsbibliotek finns att tillgå. Vidare har Arduino stöd för NFC i form av ett färdigutvecklat påstickskort, en så kallad sköld(fotnot 1), med tillhörande källkodsbibliotek.

Fokus ligger på att bygga en fungerande prototyp innehållande en låsenhet samt tillhörande mobilapplikation för till exempel privatpersoner, alltså inte för ett större företag. Då flera låsenheter eller flera användare av mobilapplikationen läggs till ökar komplexiteten för hela projektet och andra krav kommer att ställas på lösningen.

(fotnot 1) från engelskans shield

2 Metod

I den initiala fasen genomförs en analys från användarens perspektiv där de krav användaren ställer på prototypen listas. Dessa krav utformas sedan från låssystemets perspektiv och sammanställs till en kravspecifikation. Utifrån kravspecifikationen väljs de material, det vill säga de fysiska delarna vilken prototypen utgörs av, vilka är mest lämpade för utformningen av prototypen.

Under designfasen av projektet väljs hur prototypens funktionalitet distribueras ut i låssystemet och ett kommunikationsprotokoll för systemets delar samanställs. All funktionalitet som låssystemet innehåller delas upp på prototypens två enheter. Kommunikationsprotokollet beskriver hur den data som skickas mellan enheterna är uppbyggd, hur kommunikationsförloppet mellan enheterna ser ut samt hur säkerhet appliceras till kommunikationen.

Projektet övergår nu till en iterativ arbetsgång där ytterligare funktionalitet, utifrån kravspecifikationen, försöker implementeras för varje iteration. För att kunna utföra en iteration undersöks vilka eller vilket verktyg såsom källkodsbibliotek, utvecklingsmiljöer och information som krävs för att implementera funktionaliteten. Verktygen utvärderas och de som bedöms kunna bidra till, eller underlätta för implementering av den sökta funktionaliteten, väljs ut. Verktyget används sedan för fortskridandet av iterationen. Den nytillagda funktionaliteten utvärderas och om den lever upp till kravspecifikationen påbörjas nästa iteration, men skulle den nytillagda funktionalitet inte uppfylla de krav som ställs undersöks vad som är möjligt att ta med utav den nytillagda funktionaliteten till nästa iteration eller om resultatet av iterationen måste kasseras.

3 Teori

I detta kapitel beskrivs den teori som är nödvändig att förstå vid konstruktionen av prototypen. Teorin bidrar till en ökad förståelse men bidrar framförallt till det direkta framskridandet av projektet.

Eftersom prototypen använder NFC-teknik som kommunikationsmetod är kunskaper inom NFC relevant. Kunskaper inom NFC, och inte bara inom dess användande, är främst nödvändig för utvecklingen av mjukvaran till mikrokontrollern då kommunikationsstacken behöver implementeras från grunden. Detta står i kontrast till utvecklandet av Android-applikationen där kunskaper om användandet av Androids API för NFC är nödvändiga och kunskaper inom dess implementation är mindre viktigt.

Vidare är kunskaper inom säker kommunikation relevant eftersom NFC

inte har någon inbyggt säkerhet. En applikation som nyttjar NFC bör därför själv implementera säkerhet om behov finns och eftersom ett låssystem skall konstrueras är säkerhet ett krav. Säker kommunikation kan uppnås på många olika sätt och därför är kunskap för att både välja rätt metod och kunskap om den valda metodens implementering av stor vikt.

Utvecklingen av Android-applikationen kräver förutom kunskap i Java-programmering även kunskap kring applikationsutveckling för Android vilket tas upp i detta kapitel. Bland annat har applikationer för Android en speciell livscykel som är nödvändig att känna till. Det är även nödvändigt att känna till de Android-specifika API som finns att tillgå. Särskilt bör vetskap om de Android-specifika API för kommunikation via NFC besittas.

För att utveckla en applikation till Arduino-plattformen krävs förutom kunskaper inom C/C++-programmering även kunskap om Arduino vilket behandlas i detta kapitel. En Arduino har inte något operativsystem vilket gör att en Arduino-applikation kör direkt på den underliggande hårdvaran. Det betyder att kunskaper kring hur kretskorten ser ut måste beskrivas. Vidare behöver kännedom om hur kretskorten kommunicerar med varandra redogöras. Slutligen bör kunskaper angående de nödvändiga Arduino-specifika bibliotek samt hur Arduino kommunicerar via NFC beskrivas.

3.1 NFC

NFC (Near Field Communication) är en trådlös kommunikationsteknik över avstånd upp till ungefär 10 cm (Timalsina 2012) och standardiserades år 2006, tekniken är alltså relativt ny. NFC baseras på RFID (Radio Frequency Identification) vilket är en väletablerad trådlös kommunikationsteknik som funnits sedan 1983. Tekniken bygger vidare på RFID genom att erbjuda tvåvägskommunikation mellan två enheter med inbyggt stöd för NFC(Timalsina 2012).

Tekniken bygger på att två mikrochip med stöd för NFC-teknik kommunicerar med varandra genom magnetisk induktion, och mer specifikt genom att modifiera det andra mikrochipsets magnetfält(Timalsina 2012). NFC-tekniken opererar på frekvensen 13.56 Mhz och data kan skickas i hastigheter från 106 Kbps upp till 424 Kbps.

Enheter kan vara antingen passiva eller aktiva. Aktiva enheter har strömförsörjning och återfinns till exempel i mobiltelefoner medan passiva enheter saknar strömförsörjning och återfinns till exempel som taggar på posters eller i busskort.(Timalsina 2012)

Två aktiva enheter kan kommunicera med varandra. Aktiva enheter kan även kommunicera med passiva enheter genom att den aktiva enheten ger

strömförsörjning till den passiva enheten med hjälp av magnetisk induktion. Endast halv-duplex kommunikation stödjs, dvs kommunikation kan endast ske i en riktning i taget. Två passiva enheter kan inte kommunicera eftersom inget magnetfält uppstår utan tillförd energi.(Timalsina 2012)

NFC-Forum(2013) standardiserade NFC-tekniken år 2006 och är det organ som har ansvar för att ta fram de specifikationer som gör kommunikation via NFC möjlig mellan olika typer av enheter. De har också ansvar för att sprida och uppmuntra användandet av NFC-teknik samt utbilda företag i mål om att företagen ska följa de officiella specifikationerna så att tekniken kan fungera sömlöst mellan enheter från olika tillverkare.

I de följande teoriavsnitt som tar upp NFC beskrivs de protokoll NFC-Forum har specifiserat. Dessa protokoll utgör den NFC-stack som behövs då kommunikation mellan två aktiva enheter önskas. Vidare täcker protokollen hela OSI modellen förrutom applikations-skiktet och de protokollen är således allt som behövs för att implementera NFC-stacken.

3.1.1 NFC Stack

NFC-stacken är uppbyggd av ett antal protokoll som sträcker sig i stort sett över hela OSI-modellen, då endast applikationslagret med tillhörande säkerhet ej ingår i NFC-stacken. Detta är en kort översikt till de protokoll som ingår och NFC-stackens motsvarande OSI-skikt gås igenom uppifrån och ned.

- Data som sänds mellan två aktiva NFC-enheter kappslas in i ett meddelande av typen NDEF(NFC Data Exchange Format). Informationen ligger som ett eller flera fält i NDEF-meddelandet som så kallade NDEF-records.

- Vidare används protokollet NPP(NDEF Push Protocol) eller SNEP (Simple NDEF Exchange Protocol) för att utbyta NDEF-meddelanden mellan två aktiva NFC-enheter. Då NPP har ersatts av SNEP kommer bara SNEP att beskrivas.

- För att upprätta och hantera en länk mellan två aktiva NFC-enheter används LLCP(Logical Link Control Protocol). Protokollet hanterar också dataöverföringen mellan enheterna och ser till att den görs utan förluster.

- Den fysiska överföringen av bitarna hanteras av RF-protokollen där bland annat hur och i vilka hastigheter data kan skickas specifieras.

NDEF

SNEP

LLCP

RF-protokoll

Ett typiskt kommunikationsförlopp

3.1.2 Säkerhet

Detta avsnitt är baserat på artikeln Strengths and Weaknesses of Near Field Communication (NFC) Technology[14].

NFC har likt RFID i sitt grundutförande inga inbyggda säkerhetsfunktioner som förhindrar avlyssning, modifiering eller utstörning av kommunikationen. Eftersom kommunikationen är trådlös så kommer avlyssning alltid att vara möjligt och det är upp till sändare och mottagare att kryptera meddelanden om behovet finns. Följande sektioner beskriver hur dessa säkerhetsbrister kan åtgärdas.