EMULATING CONTACTLESS SMART CARD WITH HM12 CRYPTOGRAPHIC PROTOCOL ON ANDROID OS

Marek Orgoň
Master Degree Programme (2), FEEC BUT
E-mail: xorgon01@stud.feec.vutbr.cz

Supervised by: Jan Hajný
E-mail: hajny@feec.vutbr.cz

Abstract: The paper deals with the software emulation of contactless smart cards on Android using NFC and Android 4.4 API. Security of storing and using sensitive data for security applications are discussed. Paper also descibe the HM12 unlinkable attribute-based credentials protocol with practical revocation and its implementation on Android. Furthermore, the performance analysis of software-emulated smart card is provided.

Keywords: Android, Smart card, security, NFC

1 ÚVOD

Android [1] je operační systém, který se používá převážně na mobilních telefonech. Mobilní telefon je zařízení, které si uživatel běžně nosí společně s peněženkou, doklady a klíči. Spousta mobilních telefonů se systémem Android obsahuje NFC (Near Field Communication) čip. V současné době lze NFC v telefonu použít pro výměnu malého objemu dat na krátkou vzdálenost, například: kontaktní údaje, internetovou adresu, data pro párování zařízení bluetooth.

Technologie NFC je kompatibilní s technologií, kterou používají bezkontaktní čipové karty. Proto by telefon měl být schopen nahradit různé klubové karty, doklady, pěněženku (bezkontaktní platební karty se již běžně používají) i klíče (karta ISIC je na VUT používána k přístupu do učeben). Tato práce pojednává o možnostech použití systému Android pro emulaci těchto karet. Se samotnou emulací je spojena i bezpečnost uložení a používání citlivých dat a klíčů, které jsou uloženy na klasických smart kartách.

Pro praktickou ukázku byl zvolen kryptografický protokol HM12 [3], který slouží k prokázání, že uživatel disponuje konkrétním atributem (věk, řidičské oprávnění, zaplacené jízdné...) bez sdělení dalších atributů ověřovateli. Protokol dále umožňuje odhalit škodlivého uživatele s ohledem na ochranu soukromí.

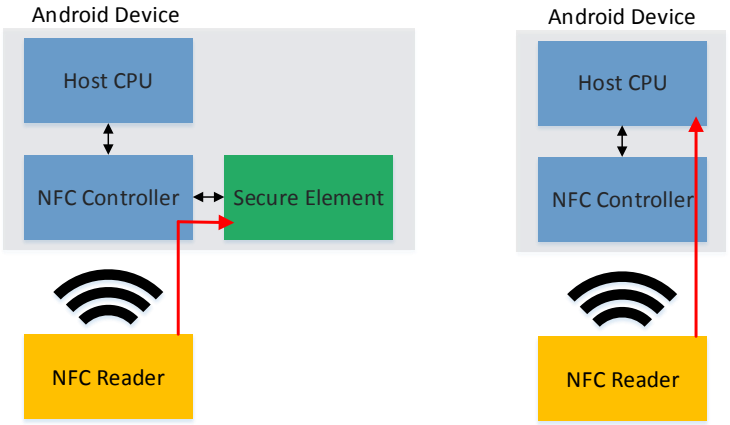
2 ANDROID A EMULACE BEZKONTAKTNÍCH ČIPOVÝCH KARET

Emulace bezkontaktních čipových karet je v systému Adroid možná již od verze 2.3, kde bylo představeno API (Application Programming Interface) pro používání NFC. K emulaci se využíval Secure Element (SE), který byl součástí NFC čipu, na SIM (Subscriber Identity Module) kartě případně na SD (Secure Digital) kartě. Secure Element je jednočipový počítač stejný jako se používá na čipových kartách a ve spojení s NFC je umožněn i bezkontaktní přenos. V tomto případě lze na SE nahrát stejný applet jaký je použit na čipové kartě. Schéma komunikace je na obrázku 1 vlevo. Zásadním problémem tohoto řešení je, že vývojářům není umožněn přístup na SE.

Od roku 2013, bylo do systému Android přidáno API [2], které umožňuje softwarovou emulaci bezkontaktních čipových karet. Toto API tedy umožňuje, aby aplikace třetích stran mohly využít telefon

jako čipovou kartu a to na stejné hardwarové úrovni jako klasické bezkontaktní čipové karty. Lze tedy využít stejnou infrastrukturu čteček a protokoly, které jsou používány pro běžné čipové karty.

Emulace v systému funguje na úrovni služby, která je registrována pro konkrétní skupinu identifikátorů aplikace (AID). Pokud telefon přijme požadavek na komunikaci s aplikací, která je registrována příslušným AID, je spuštěna služba, která přijímá a případně odesílá standardní komunikační APDU (Application Protocol Data Unit) jednotky. Schéma komunikace je na obrázku 1 vpravo. Tato služba tedy musí mít implementovaný daný komunikační protokol.



Obrázek 1: Schéma komunikace při použití SE a při emulování čipové karty

3 BEZPEČNOST CITLIVÝCH DAT

V případě softwarové emulace není nijak obecně řešena bezpečnost případných dat protokolů. Každá aplikace má vyhrazeno vlastní úložiště, ke kterému má přístup standardně pouze ona. Data nejsou nijak šifrována a v případě ztráty zařízení je lze získat. Dále v případě, že uživatel přidělí jiné aplikaci práva root může tato aplikace číst data ostatních aplikací. Proto je potřeba citlivá data šifrovat.

Android poskytuje API pro zabezpečené úložiště, které je rozděleno na Hardware-Backed a Software-Backed. Hardware-Backed úložiště používá speciální hardwarový modul, který umožňuje generovat a používat RSA klíče v zabezpečeném odděleném běhovém prostředí. Vygenerované RSA klíče toto prostředí neopustí a nedostanou se do hlavní paměti zařízení. Do tohoto prostředí ale není možné nahrát vlastní aplikace. V případě Software-Backed úložiště operace s RSA již probíhá v hlavním systému zařízení a RSA klíče jsou šifrovány pomocí masterkey klíče, který je odvozen pomocí PBKDF2 algoritmu s 8192 iteracemi a náhodně generovanou solí z hesla/pinu zámku obrazovky.

Toto API je tedy vhodné pro šifrování klíčů protokolu pomocí RSA. V případě Hardware-Backed úložiště by útočník neměl být schopen klíče získat ani při fyzickém přístupu k zařízení. V případě Software-Backed úložiště ale útočník s fyzickým přístupem k zařízení nebo s právy root je schopen ze zařízení získat masterkey a šifrovaná data a pokusit se je například hrubou silou dešifrovat. Dalším problémem je, že z aplikační strany nelze stanovit pravidla pro složitost zamykacího hesla/pinu a v případě pinu je minimální délka 4 numerické znaky.

4 PROTOKOL HM12

Protokol HM12 [3] patří do skupiny protokolů sloužících k ověření určitého atributu (národnost, věk...). Jeho cílem je provést toto ověření bez odhalení identity ověřovaného. Aby toho mohlo být dosaženo, musí protokol splňovat následující vlastnosti: anonymita (identita uživatele není při ověřování odhalena), nevysledovatelnost (vydané atributy nelze sledovat), nespojovatelnost (jednotlivá

ověření nelze přiřadit k uživateli), zrušitelnost ověřovacích údajů (vydané atributy se dají odvolat), identifikace škodlivých uživatelů (i když je ověřování anonymní lze odhalit škodlivé uživatele).

Protokol se skládá ze čtyř entit: vydavatele, ověřovatele, odvolávatele a uživatele. Vydavatel vydává atributy uživateli a jako jediná entita zná uživatelovy údaje. Odvolávatel působí jako třetí strana v odvolávacím procesu a rozhoduje o zrušení nespojovatelnosti protokolu nebo anonymity uživatele. Ověřovatel ověřuje zda uživatel disponuje daným atributem a o každém ověřování si vede záznamy. Není schopen k záznamům ověření přiřadit uživatele natož zjistit jeho identitu, ověřování probíhá off-line.

Aby protokol splňoval tyto vlastnosti, jsou jeho matematické operace výpočetně náročné. Protokol pracuje s čísly o délce 1024b a vyšší. Provádí se série mocnění, násobení a modulární redukce, která při implementaci na čipových kartách trvá až 2s. Proto bylo nutné nalézt výkonnější zařízení, ideálně takové, které již uživatel běžně nosí sebou. Mobilní telefon splňuje obě tyto podmínky a zároveň umožňuje emulaci čipových karet. Tento příspěvek perezentuje první aplikaci svého druhu, kde mobil je zcela zaměnitelný za kartu pro ověření uživatele.

5 IMPLEMENTACE PROTOKOLU HM12

Protokol HM12 byl implementován pro systém android v jazyce JAVA, pro operace s velkými čísly používá funkce třídy `BigInteger` a využívá API pro softwarovou emulaci čipové karty.

Implementována je část protokolu, která se zabývá ověřováním atributů. Všechny APDU, které se posílají mezi emulovanou kartou a čtečkou jsou ve stejném formátu který používá klasická čipová karta. Díky tomu je telefon plně zaměnitelný za klasickou čipovou kartu a funguje na stávající softwarové i hardwarové infrastruktuře čteček.

V případě klasické čipové karty trvá ověření atributu kolem 2s. V případě emulované karty kolem 500ms, což je výrazné zrychlení a v případě potřeby použití složitějších protokolů zde nejsme tak výrazně limitováni výkonem.

6 ZÁVĚR

Implementace protokolu HM12 z klasických čipových karet do zařízení se systémem Android proběhla úspěsně a lze tímto způsobem emulovat i jiné protokoly na čipových kartách. Z pohledu uživatele se jedná o přenesení fyzické karty do mobilního telefonu. Z pohledu vývojáře lze na emulovaných kartách provádět složitější výpočty. Z pohledu bezpečnosti ale není tak jednoduché zajistit bezpečnost citlivých dat protokolu na alespoň stejné úrovni jako mají čipové karty, lze však použít složitější kryptografické postupy, které zvyšují bezpečnost.

Další práce na tomto projektu se bude věnovat návrhu co nejbezpečnějšího systému pro ukládaní a práci s citlivými daty.

REFERENCE

[1] *Android developers* [online]. Poslední aktualizace 2. 12. 2013 [cit. 2. 2. 2014]. Dostupné z URL: <http://developer.android.com/develop/index.html>.

[2] *Host-based Card Emulation* [online]. Poslední aktualizace 2. 12. 2013 [cit. 2. 2. 2014]. Dostupné z URL: <http://developer.android.com/guide/topics/connectivity/nfc/hce.html>.

[3] HAJNÝ, J.; MALINA, L. *Unlinkable Attribute-Based Credentials with Practical Revocation on Smart- Cards. In Smart Card Research and Advanced Applications. Lecture Notes in Computer Science. LNCS. Berlin: Springer- Verlag*, 2013. s. 62-76. ISBN: 978-3-642-37287- 2. ISSN: 0302-9743.