SMS ENCRYPTION IN MOBILE COMMUNICATION

David Lisoněk
Master Degree Programme(1), FIT VUT
E-mail: xlison00@stud.fit.vutbr.cz

Supervised by: Martin Drahanský
E-mail: drahan@fit.vutbr.cz

ABSTRACT

This text describes basic features of SMS messages and basic principle of SMS message transmission in GSM networks. The Symbian OS has been choosen as a suitable platform for programming of mobile devices. For SMS encryption and decryption, there is used the asymetric cypher RSA. The certification authority provides public key exchange.

1. ÚVOD

Mobilní telefony se již dnes staly nedílnou součástí moderního životního stylu. Jsou využívány celou populací, od dětí na základní škole, přes lidi v produktivním věku, až po staré lidi v důchodu. Dnešní mobilní telefon je, ač si to mnoho lidi neuvědomuje, velmi osobní věc. Citlivé informace jsou uloženy v každém mobilním telefonu nejen ve formě telefonních kontaktů a uložených SMS zpráv, ale také např. ve formě poznámek uložených v kalendáři, nebo fotek pořízených fotoaparátem mobilního telefonu. Ochrana těchto informací závisí do jisté míry na uživateli, který musí zabránit zcizení přístroje. Dostane-li se přístroj do nepovolaných rukou je většina těchto informací dostupná bez vynaložení většího úsilí. Odcizení přístroje pozná uživatel téměř okamžitě, odposlech přenášených hovorů, SMS nebo dat nemusí poznat vůbec. A právě cena přenášené informace může být v danou dobu mnohem vyšší než cena mobilního telefonu a informací v něm uložených.

2. SÍŤ GSM

Komunikace probíhá přes digitální bezdrátovou síť s buňkovou strukturou typu GSM. Oblíbenost je dána standardizací, podporou výrobců a také možného rozšíření do budoucna. Tento typ sítě je využíván ve většině zemí a používají ho přes 2 miliardy lidí na celém světě.

2.1. Bezpečnost sítě

U bezdrátového přenosu dat je nemožné zamezit útočníku odposlech. V našem případě jsou přenášecí medium rádiové vlny. Mobilní telefony dokáží komunikovat i na vzdálenost několika kilometrů. Útočník však nemusí pouze odposlouchávat, ale může se vydávat za někoho jiného. Proto se přenos informací nejen šifruje, ale je ověřována i totožnost uživatele. Každý mobilní účastník má přiděleno telefonní číslo, které je vázáno na SIM kartu.

Po přihlášení je po uživateli požadováno heslo, které zpřístupní služby SIM karty, takzvaný PIN kód. Po zadání správného hesla proběhne přihlášení do sítě. Bezdrátová komunikace mezi mobilním telefonem a základnovou radiovou stanicí BTS, která se stará o příjem radiového signálu od mobilních telefonů, je šifrovaná. Přenosová cesta od BTS dále již šifrována být nemusí. A zde je možnost pro útočníka odposlechnout přenášená data.

2.2. Zprávy sms

Systém GSM poskytuje také alternativu k „drahému" volání. Touto alternativou je posílání krátkých textových zpráv Short message service. Díky včasnému začlenění této služby do GSM standardu umožňují práci s SMS všechny dnešní mobilní telefony, proto je šifrování SMS výhodnější než šifrování např. MMS, datového spojení GPRS, e-mailu a podobně.

Velikost SMS zprávy je pouze 140 bytů. Při použití 7 bitového kódování může zpráva obsahovat až 160 znaků. Toto kódování však nepodporuje znaky národních abeced. Při použití např. znaků s českou diakritikou, se SMS zpráva kóduje 16 bitově, pomocí kódovaní Unicode. Pak je uživatelský prostor jen 70 znaků. Lze použít i 8 bitové kódování, které je vhodné pro přenos dat.

Po vytvoření je SMS zpráva odeslána do SMS centra, kde je uložena. SMS centrum se snaží zprávu doručit příjemci. Není-li příjemce v dosahu, pokusí se o doručení později. Pokusy o doručení probíhají dokud SMS zprávě nevyprší platnost. Tady je další možnost pro odposlechnutí SMS zprávy. SMS se zde může vyskytovat i delší dobu než dojde k doručení příjemci.

3. PLATFORMY

Všechny moderní mobilní telefony dnes umožňují spuštění jednoduchého vlastního programu. Při potřebě vyššího výpočetního výkonu nebo pro využití všech periferií je třeba využít tvz. Smartphonu, tedy telefonů disponujícími pokročilejšími funkcemi a lepším API pro spuštění externích programů.

3.1. Java ME

Je vyvíjena firmou Sun Microsystems. Tuto programovou platformu dnes obsahují snad všechny mobilní telefony. Bohužel díky takto široké podpoře API je vcelku chudé na využití pokročilejších funkcí (např. VoIP). Kód programu je spouštěn na virtuálním stroji. Tato koncepce odstíní hardware různých typu, ale jeho výpočetní výkon nemusí být dostatečný pro některé aplikace (např. asymetrická kryptografie).

3.2. Windows Mobile

Je vyvíjena firmou Microsoft. Využívaná u smartpfonou. Menší zastoupení na trhu se smartphony.

3.3. Symbian OS

Je vyvíjen firmou Nokia a dalšími. Využit u smartphonou. Největší zastoupení na trhu smartphonu. Dobrá podpora vývojářů. Portování standardních POSIXových knihoven (např. libcrypt, libcrypto) v projektu Open C. Možnost urychlení vývoje aplikace pomocí programovacího jazyka Python [1].

3.4. Ostatní

Linux on Mobile, Apple iphone, Google Android a další. Mají zatím mizivé zastoupení na trhu s mobilními telefony. Je pouze pár typů telefonů podporující tyto operační systémy.

4. POŽADAVKY A NÁVRH ŘEŠENÍ

Byla vybrána platforma Symbian OS, která poskytuje dostatečný přístup k funkcím mobilních telefonů a je i nejrozšířenější. Pro implementaci GUI, práci s SMS a soubory se využívá programovací jazyk Python. Pro šifrování byla zvolena asymetrická kryptografie, u které odpadá nutnost distribuce klíče zabezpečenou cestou. Pro utajení je využita šifra RSA, která je obsažena v knihovně libcrypto. Tato knihovna je začleněna do projektu Open C. Knihovna je napsána v jazyce C, proto bylo nutné implementovat rozhraní volání C knihoven z jazyka Python.

Vlastní distribuce veřejného klíče je provedena buď výměnou mezi uživateli, kde si vymění soubor s daným klíčem. Nebo budou klíče uloženy u třetí nezávislé strany certifikační autority, od které si certifikát s klíčem budou moci uživatelé stáhnout ve formě souboru.

Před samotným zašifrováním bude text zprávy vyplněn do velikosti SMS. Pro vyplnění se využije postup OAEP[2]. Pro šifrování byla zvolena asymetrická šifra RSA. Odesilatel zná telefonní číslo příjemce. Požádá Certifikační autoritu o veřejný klíč příjemce a ta mu klíč vydá. Zpráva je poté zašifrována veřejným klíčem příjemce. Při překročení velikosti zprávy bude rozdělena do více SMS zpráv. Následuje odeslání skrz GSM síť. Po doručení, příjemce může zprávu dešifrovat svým soukromím klíčem.

5. ZÁVĚR

Šifrování SMS zpráv ocení zejména lidé, pro které má přenášená informace velkou cenu. Tito lidé mohou být nebo jsou terčem odposlechu. Odposlech nemusí být pouze nelegální, může být také nařízen státní správou, která však nemusí vždy jednat v rámci zákona. Díky použití asymetrické kryptografie a Certifikační autority bude možno pohodlně zabezpečeně komunikovat pomocí SMS mezi více uživateli.

LITERATURA

[1] Frank H.P. Fitzek, Frank Reichert: Mobile Phone Programming and its Application to Wireless Networking, Springer 2007, ISBN 978-1-4020-5969-8

[2] Wikipedia contributors: Optimal Asymmetric Encryption Padding, c2008 [citováno 2008-02-20], Dostupný z WWW: http://en.wikipedia.org/wiki/Optimal_Asymmetric_Encryption_Padding