Studentská konference Fakulty mechatroniky, informatiky a mezioborových studií
10. červen 2013, Liberec, Česká republika

Ukládání a výměna dat u mobilní aplikace v datovém online a offline režimu

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky a mezioborových studií

Bc. Martin Pelák
Ing. Igor Kopetschke

ABSTRAKT

This diploma thesis deals with a problem of online and offline data transfer among mobile devices. The main aim is to find possible ways on how to transfer data securely. The theoretical part suggests possible solutions using public-key cryptography. It describes how to use certificates signed by a certificate authority or how to use self-signed certificates for the secure connection. Furthermore, it introduces a certificate-free solution based on manual data encryption.

Moreover, it describes and explains terms related to problems such as certification authority, digital signature and introduces tools for managing certificates.

The practical part of the diploma thesis is based on the theoretical part and it implements all suggested solutions into two demo applications. Each of them was created for different mobile operating system, one for Windows Phone 8 and the other one for Android.

CÍL

Cílem je najít řešení pro bezpečné ukládání dat na mobilních zařízení a zabezpečit online a offline datový přenos. Nalezená řešení budou implementována do ukázkové applikace (WP8, Android)

VSTUP DO PROBLEMATIKY

V dnešní době se velmi rozšiřuje použití chytrých mobilních telefonů a tabletů jako zařízení neustále připojených do sítě internet. To jejich uživatelům poskytuje širší možnosti využití, ale také přináší nové bezpečností hrozby.

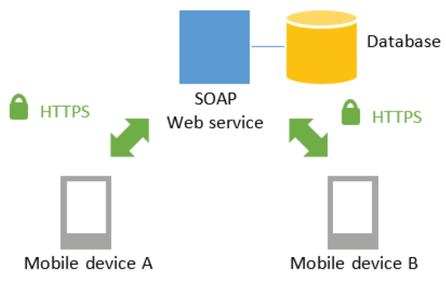
Z těchto důvodů je třeba se zaměřit na hledání potenciálních bezpečnostních hrozeb a těm předcházet. Nesmíme ovšem opemenou bezpečnost přenášených dat i v offline režimu.

Obrázek 1 - aplikace pro Windows Phone 8

METODIKA

Stručný popis algoritmu vytvořených aplikaci:

- Výměna dat probíhá mezi zařízeními pomocí SOAP webové služby.



- Celá online komunikace je zabezpečena certifikátem podepsaným certifikační autoritou. Dále byly vytvořeny další aplikace, které využívají certifikát podepsaný sám sebou.
- Aplikace v pravidelných intervalech dotazuje webovou službu, jestli nemá nevyzvednuté zprávy. Pokud ano, uloží je do lokálního úložiště. V případě Androidu je to sqlite. Windows Phone 8 využívá LINQ.
- Pokud uživatel chce odeslat zprávu, aplikace kontaktuje webovou službu a zprávu jí předá. Při nedostupnosti připojení k internetu je uživateli nabídnuto, že jeho zpráva bude doručena prostřednictvím SMS. Funkční kód pro šifrování SMS byl realizován v jazyce JAVA. Windows Phone 8 nedovoluje aplikacím, aby manipulovaly s SMS zprávami, proto je jejich šifrování prakticky nerealizovatelné.

VÝSLEDKY

V práci se podařilo splnit všechny požadované body zadání. Postupně bylo představeno několik řešení pro zabezpečení online přenosu dat s využitím asymetrické šifry. První řešení využívá certifikát podepsaný certifikační autoritou, další řešení pak certifikát podepsaný sám sebou. Poslední možnost pak využívá ručního šifrování.

Pro offline přenos dat byla využita služba SMS. Šifrování krátkých textových zpráv bylo realizováno symetrickou šifrou AES.

Zabezpečení citlivých dat vychází ze znalostí získaných při hledání řešení pro online a offline přenos. V práci je nastíněna možnost šifrování na základě symetrického šifrování, podobně jako v případě přenosu šifrovaných SMS zpráv.

Výsledkem jsou dvě ukázkové aplikace, které fungují jako dva IM klienti. Řešení je multiplatformní. Jedna aplikace běží na Windows Phone 8 a druhá na Android 4.

DISKUSE, ZÁVĚRY

Závěry:

- Online datový přenos může být zapezpečen pomocí šifrování založeném na asymetrickém šifrování. V praxi často realizované pomocí protokolu nad SSL vrstvou
- Offline datový přenost byl řešen přes pomocí SMS. Tento přenos lze zabezpečen pomocí šifry symetrické. Avšak aplikace pro Windows Phone 8 nemají oprávnění pro manipulaci se SMS.
- Ukládaná data mohou být šifrována pomocí symetrické šifry

Diskuse:

- je výhodnější pro potenciálního útočníka využít sociální inženýrství nebo se pokusit získat fyzický přístup k zařízení?
- jaká data jsou opravdu citlivá?

REFERENCE

[1] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF [online]. 2008 [cit. 2013-04-26]. Available at: http://tools.ietf.org/html/rfc5280

[2] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2. IETF Tools [online]. 2008 [cit. 2013-04-26]. Available at: http://tools.ietf.org/html/rfc5246#page-4

[3] Web Services Architecture. World Wide Web Consortium (W3C) [online]. 2004 [cit. 2013-04-26]. Available at: http://www.w3.org/TR/ws-arch/

[4] 3GPP TS 23.038 V10.0.0: Alphabets and language-specific information [online]. zip .doc file. 2011 [cit. 2013-04-26]. Available at: http://www.3gpp.org/ftp/specs/archive/23_series/23.038/23038-a00.zip

[5] Murphy, M.L., Android 2 Průvodce programováním mobilních aplikací, Computer Press a.s., 2011, ISBN 978-80-251-3194-7

KONTAKT

Bc. Martin Pelák
E-mail: martin.pelak@live.co.uk

Tato práce byla podpořena z projektu Studentské grantové soutěže (SGS) na Technické univerzitě v Liberci v roce 2013