Rozšířený Abstrakt

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

Martin Pelák, Ing. Igor Kopetschke

Abstrakt

Úvod

Diplomová práce se zabývá problematikou přenosu online a offline data mezi mobilními zařízeními. Hlavním cílem je najít možné řešení jak data přenášet zabezpečeně. Teoretická část navrhuje možné řešení za použití asymetrické kryptografie. Popisuje, jak použít certifikáty podepsané certifikační autoritou nebo jak využít vlastnoručně podepsaný certifikát pro bezpečnou výměnu dat. Dále představuje řešení bez certifikátu, které je založeno na ručním šifrování dat.

V práci jsou popsány a vysvětleny termíny vztahující se k dané problematice, např. certifikační autorita, digitální podpis a představuje nástroje pro správu certifikátů.

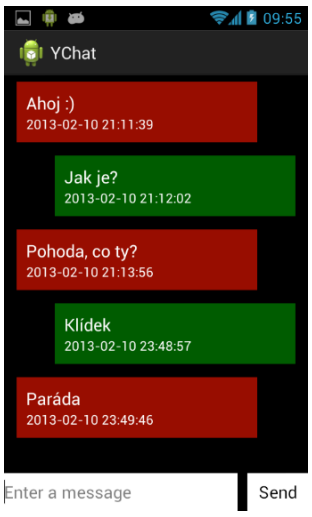
Praktická část diplomové práce vychází z teoretické části a implementuje navrhovaná řešení do dvou ukázkových aplikací. Každá aplikace byla vytvořena pro jiný operační systém, jedna pro Windows Phone 8, druhá pro Android.

Experiment a metody

Jako referenční mobilní zařízení byl použit Windows Phone HTC 8x a LG Optimus 2x s operačním systémem Android 4.

Online přenos data mezi mobilními zařízeními byl řešen prostřednictvím SOAP webové služby. Ta je realizována prostřednictvím PHP frameworku Yii, který zjednodušuje vytváření podobných služeb. Samotná webová služba běží na webovém serveru Apach a je nutností, aby byl nainstalovaný a povolený SOAP balíček.

Offline přenos data využívá služeb operátora a z tohoto pohledu nevyžaduje další dodatečné hardwarové či softwarové prostředky. Přenos je závislí na službě SMS. Ta bývá zpravidla placená.



Obrázek 1: Android

Obrázek 1: Windows Phone 8

Rozšířený Abstrakt

Výsledky a diskuze

Výsledkem práce jsou dvě ukázkové mobilní aplikace s implementovaným řešením pro bezpečnou výměnu data v online a offline režimu, dále pak řešení pro bezpečné ukládání dat. Každá aplikace byla vytvořena pro jiný mobilní operační systém (Windows Phone 8, Android).

Závěr

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.

Nezáleží, jak sofistikované řešení je navrženo, celý systém zůstává vždy tak silný, jak jeho nejslabší část. Bezpečnost je velice relativní pojem a vždy se odvíjí od množství času a peněz, které je potenciální útočník ochoten do dekódování investovat. Avšak pokud vezmeme v potaz citlivost dat, uvedená řešení mohou být dostatečná pro většinu dnes používaných mobilních aplikací.

Poděkování

Chtěl bych poděkovat všem, kteří mi pomáhali s tvorbou diplomové práce. V první řadě bych chtěl poděkovat vedoucímu této diplomové práce Ing. Igor Kopetschkemu za jeho čas, poskytnuté rady a materiály.

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