Invited talk:

Vlastimil Klíma and Martin Baroš: Data protection in clouds

Abstract

In the paper we present the main principles of solving the issue of data protection in clouds. Furthermore, we demonstrate possible security and cryptographic weaknesses, and suggest principles of ideal data protection, while simultaneously pointing out the disadvantages of ideal solutions using a concrete example.

Furthermore, we present our vision in the area of further evolution of mobile devices in the context of cloud repositories, as well as anticipated trends of data protection in them. In selected chapters concerning data protection we put currently available solutions available in the market and compare the level of protection they provide. We point out concrete correct implementation, as well as incorrect application of cryptographic concepts or other closely related security risks. Wherever relevant, we point out concrete instances (whether from a cryptographic or implementation perspective) where the given solution is failing, and finally we evaluate the impact on the security of the whole system.

Subsequently, we compare – using practical cryptographic examples – the performance of the traditional platform for implementation of cryptographic concepts (Java) to the new platform of natively supported web explorers (JavaScript). Taking into account current as well as predicted boom of mobile technologies, we conduct comparative tests even on selected mobile devices. We chose representatives both from the area of telephones and tablets. In the area of mobile devices, we compared the approach to the implementation of cryptographic algorithms on the native language platform and the implementation of algorithms using JavaScript library. The comparison is carried out with a representative volume of data, which grows in the course of the test, in order to define the key limits or benefits of the individual platforms, as applicable. In closing, the statistical results are summarized to make them usable as support for basic orientation when selecting target implementation platforms of cryptographic design. The aim of comparing the mobile platforms is to provide basic information as guidance in the decision-making process, as to whether it is possible to use the native code of the platform for the implementation of the intended solution or, alternatively, use HTML 5 enhanced by JavaScript. The latter alternative is promising as a feasible solution for all mobile and desktop platforms, save for certain limitations that we focus on as well.

Abstrakt

V příspěvku uvádíme hlavní principy řešení ochrany dat v cloudech. Poté ukazujeme na možné bezpečnostní a kryptografické slabiny a navrhujeme principy ideálního zabezpečení dat. Poukazujeme na nevýhody ideálního řešení a uvádíme konkrétní příklad.

Dále uvádíme naše vize, jak se bude dále vyvíjet oblast mobilních zařízení a jejich vztah ke cloudovým úložištím a jak se bude vyvíjet ochrana dat v těchto úložištích. U vybraných pasáží týkajících se ochrany dat dáváme do souvislostí existující řešení dostupná na současném trhu a jejich úroveň bezpečnosti. Poukazujeme na konkrétní korektní implementace příp. nesprávnou aplikaci kryptografických konceptů nebo jiných blízkých bezpečnostních rizik. V případě, že tomu tak u daného řešení je, poukazujeme na konkrétní místa (ať už z kryptografického nebo implementačního hlediska), kde dané řešení selhává, a zhodnocujeme dopad na bezpečnost celého systému.

Následně na praktických kryptografických příkladech provádíme srovnání výkonu tradiční platformy pro implementaci kryptografických konceptů (java) v porovnání s novou platformou nativně podporovanou webovými prohlížeči (javascript). S ohledem na současný i očekávaný rozmach mobilních technologií provádíme

srovnávací testy i na vybraných mobilních zařízeních. Vybíráme zástupce jak z řad telefonů, tak tabletů. V rámci mobilních zařízení je srovnáván přístup implementace kryptografických algoritmů v nativním jazyce platformy oproti implementaci algoritmů javascriptovou knihovnou. Porovnání je prováděno na reprezentativním objemu dat, který průběžně během testu narůstá, aby se projevily klíčové limity příp. výhody jednotlivých platforem. Statistické výsledky jsou v závěru sumarizovány tak, aby výsledky byly využitelné jako podklad pro základní orientaci při výběru cílové implementační platformy kryptografického designu. Cílem srovnání u mobilních platforem je poskytnout základní informace pro orientaci při rozhodování, zda je možné pro implementaci zamýšleného řešení využít nativní kód platformy nebo je možné využít HTML 5 obohacené javascriptem. Druhé zmiňované řešení slibuje možnost využívat řešení na všech mobilních i desktopových platformách, ale skýtá také několik omezení, na které poukážeme.

CV

Vlastimil Klíma

konzultant
v.klima@volny.cz
+420 739 658 004
Pod Haltýřem 1497/5, 148 00 Praha 4

RNDr. Vlastimil Klíma graduated from the Faculty of Mathematics and Physics of the Charles University in Prague. He devoted all his thirty years professional life to cryptology. He has been working for government, army, private companies and as a consultant now. In the Czech Republic, he is founder of the area of the side channel cryptanalysis. He has written more than 300 papers and lectures. In the world he is known by proposing the fastest MD5-collision searching method and by revealing weaknesses in OpenPGP and SSL/TLS. He proposed a new concept of hash functions and block ciphers DN (HDN). He is co-author and inventor of the fastest hash function (BMW) in the second round of the competition SHA-3.
Website: http://cryptography.hyperlink.cz

RNDr. Vlastimil Klíma je absolventem Matematicko-fyzikální fakulty Univerzity Karlovy v Praze. Celý svůj třicetiletý profesionální život zasvětil kryptologii. Pracoval pro vládu, armádu, soukromé společnosti a nyní jako konzultant. V ČR patří k zakladatelům oboru kryptoanalýzy postranními kanály. Je autorem přes 300 příspěvků a přednášek. Ve světě je znám nejrychlejší metodou hledání kolizí MD5, odhalením slabin v OpenPGP a SSL/TLS. Navrhl nový koncept hašovacích funkcí a blokových šifer DN (HDN). Je spoluautorem a vynálezcem nejrychlejší hašovací funkce (BMW) v druhém kole soutěže na SHA-3.
Osobní stránky: http://cryptography.hyperlink.cz

Martin Baroš

CEO Cryptelo s.r.o
www.cryptelo.com
baros@cryptelo.com
+420 777 002 493
Dělnická 1324/9, 170 00 Praha 7, Czech Republic

Martin Baroš je ředitelem společnosti Cryptelo. Zodpovídá za strategický rozvoj firmy a navrhuje nové typy bezpečnostních produktů firmy. Je absolventem Matematicko-fyzikální fakulty Univerzity Karlovy v Praze. Byl součástí vývojového týmu, který vytvářel aplikace pro finanční a bankovní sektor. Martin Baroš vedl tým pro vývoj klíčových prvků bankovnictví Air Bank. Rozhodl se věnovat bezpečnosti, protože má rád výzvy a nerad se vzdává.

Martin Baroš, CEO at Cryptelo, is responsible for leading expansion and bringing ideas for company's security products. He studied Charles University - Faculty of Mathematics and Physics. He was part of developer teams created application for financial and bank sector. He also lead team developed part of core banking features for Air Bank. Decided to focus on security, because he likes challenges and hates to give up.

Kontaktní autor:

Martin Baroš
Cryptelo s.r.o
Dělnická 1324/9, 170 00 Praha 7, Czech Republic
baros@cryptelo.com
+420 777 002 493