

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií



Teze diplomové práce

**Provádění platebních operací za pomoci mobilní
platformy Android OS**

Bc. Jakub Zemen

© 2015 ČZU v Praze

Provádění platebních operací za pomoci mobilní platformy Android OS

Souhrn

Práce je zaměřena na služby mobilních bankovních (smartbanking) aplikací, na jejich využívání v ČR a na jejich další možnosti (funkcionality). Autor práce zvolil nejrozšířenější mobilní platformu Android OS, která je v práci zkoumána jak z pohledu struktury, tak i z pohledu bezpečnostních rizik, jež by mohly postihnout uživatele mobilní bankovní aplikace. Analytická část práce je konkrétně zaměřena na určení oblastí, které mohou pomoci rozšířit řady uživatelů těchto smartbanking aplikací. V první části jsou analyzovány závislosti kvalitativních znaků vztahujících se k postojům uživatelů elektronického bankovníctví. Druhá část je zaměřena na analýzu preferencí uživatelů vůči jednotlivým nabízeným funkcionalitám. Z literární rešerše a analytické části práce je v jejím závěru určeno, že případná absence funkcionalit silně ovlivní normalizovaný přínos pro uživatele a které konkrétní funkce na něj mají nejvyšší vliv. Na podkladě těchto zjištění jsou uvedeny závěry, které napomohou rozšířit řady reálných uživatelů a eliminují případná bezpečnostní rizika například využíváním antivirové aplikace či návrhem na ochranu proti útokům typu DoubleDirect.

Klíčová slova: Android OS, smartbanking, bankovní operace, funkcionality mobilních bankovních aplikací, bezpečnost, rizika, malware, antivirové aplikace, Google Security, sandbox.

1. Cíle a metodika

Cíle práce jsou zaměřeny na:

- 1) Stanovení návrhu na eliminaci bezpečnostních rizik a rezerv nabízených funkcionalit mobilních bankovních aplikací pro rozšíření počtu reálných uživatelů.
- 2) Stanovení současného pohledu na mobilní bankovníctví a jeho využívání.
- 3) Analýzu bezpečnostních rizik mobilní platformy Android OS a určení reálných hrozeb pro uživatele mobilní bankovní aplikace.

- 4) Provedení analýzy závislosti kvalitativních znaků vycházejících z dotazníkového šetření.
- 5) Provedení vícekriteriální analýzy variant, vycházejících z dotazníkového šetření, pro určení preference uživatelů na dostupné funkcionality ve třech předem zvolených bankovních aplikacích

Metodika práce byla zvolena na podkladě provedené literární rešerše, která je hlavním zdrojem teoretických podkladů vytvořených textací, analýz a vyhodnocených cílů v závěru. V rámci rešerše jsou využity mnohé webové zdroje, mezi kterými jsou především specializované servery zaměřené na platformu Android OS a bezpečnostní rizika.

Po sestavení teoretické struktury práce byla vytvořena datová základna pro analytickou část práce, pro kterou jsou nezbytná data načerpána z dotazníkového šetření na předem nespécifikovanou skupinu respondentů. Samotný sběr dat vychází z online dotazníku vytvořeného za pomoci bezplatné služby Google Forms, přičemž jeho sestavení vychází z praxe autora v oblasti výzkumu trhu s ohledem na požadavky, které jsou kladeny na dotazníková šetření.

Po vytvoření popisných statistik a souhrnného popisu získaných dat je využito statistických metod k určení závislosti kvalitativních znaků, která je v datech prokazována za pomoci Fisherova a Chí-kvadrát testu. V případě, že se závislost kvalitativních znaků potvrdí, bude určena i její síla za pomoci Cramerova či Phi koeficientu. Předpoklad výskytu závislosti kvalitativních znaků autor práce předpokládá především mezi oblastmi využívání internetového bankovníctví, znalosti pojmu smartbanking, využívání mobilních bankovních aplikací a orientace respondentů v oblasti ICT.

Význam využití vícekriteriální analýzy variant se nalézají v samotných nabízených funkcionalitách dostupných v třech předem zvolených mobilních bankovních aplikacích. Získaná data umožní určit váhu jejich absence vzhledem k požadavkům uživatelů. V rámci postupu byla využita bodovací metoda pro vytvoření matice výskytu nabízených funkcí, jelikož metoda pořadí by zde ztrácela význam pro své zaměření na ordinální informace. Dále byla aplikována bodovací metoda s vahami, jež vychází z preferencí stanovených uživateli. Rovněž byl vypočten normalizovaný přínos pro uživatele, kterým je určeno pořadí významnosti zvolených aplikací.

Pro získání závěrů zpracované problematiky bylo vyjma analytických nástrojů využito i metod kritického vyhodnocení výsledků analýz a dedukce. Konkrétně jsou za pomoci dedukce určeny závěry o změně návyků a postojů uživatelů a návrh k poskytnutí garance mobilní bankovní aplikaci. Na základě metody kritického vyhodnocení výsledků analýz poté byly navrženy a sledovány dvě nové funkcionality, které doposud aplikace nenabízí a stanoven návrh řešení pro předávání informací uživatelům.

2. Závěr

V souhrnném pohledu je možno říci, že využívání mobilních bankovních aplikací je dle informací o aktuálním počtu uživatelů a objemu prováděných finančních transakcí uvedených v kapitole 3.4 na vzestupu, avšak vzhledem ke konzervativnějším postojům uživatelů je potřeba tento trend podpořit. Dále je možné určit, že na základě využívání mobilního zařízení ke správě finančních prostředků se následně logicky mění i postoje a návyky uživatelů. Nejen totiž s odkazem na tuto kapitolu, ale i v rámci analytické části práce bylo v kapitole 6.3.1 prokázáno, že pro uživatele je dle nejvyšší vypočtené preference velmi podstatná možnost sledovat zůstatky a zobrazit si historii platebních operací. Tato skutečnost je v praxi podložena častějším přístupem do mobilní bankovní aplikace, než tomu bylo u běžného internetového bankovníctví. Se změnou návyků uživatele je rovněž možné očekávat i vyšší požadavky na nabízené funkce a služby v mobilních bankovních aplikacích, přičemž tento předpoklad byl zároveň potvrzen i v rámci vypočtených normalizovaných přínosů pro uživatele z vícekritériálních analýz variant v kapitolách 6.3 a 6.3.1.

Prostor pro rozšíření řad uživatelů se tedy otevírá v samotných možnostech mobilních bankovních aplikací. Mezi sledované preference funkcionalit tak byly autorem práce přidány 2 funkcionality.

V prvním případě se jednalo o možnost nahlášení škodné události. Vzhledem ke skutečnosti, že aplikace Komerční banky nabízí možnost sjednání pojištění, se na základě nabízených služeb možnost nahlášení škodné události autorovi práce jeví logickým požadavkem. Tato funkce se dle vah kritérií určených z preferencí respondentů pohybovala v blízkosti aritmetického průměru všech vah, takže je možné hovořit o prakticky

neutrálním postoji všech respondentů vůči její absenci, což má střední vliv na normalizovaný přínos pro uživatele.

Druhá přidaná funkcionalita, kterou byla možnost individualizace bankovní aplikace, dle vah kritérií stanovených z preferencí všech uživatelů, jež jsou uvedeny v kapitole 6.3, získala stěžejnější třetí místo ze všech sledovaných funkcionalit. Její absence tedy má velmi silný vliv na normalizovaný přínos pro uživatele.

Rovněž by se jejím přidáním vyřešil i případný problém s přehledností aplikace po přidání dalších funkcí, jelikož by si uživatel mohl v ideálním případě sám navolit, které funkce se mu zobrazí. Aplikace by tak nativně obsahovala veškeré funkcionality a individualizace by spočívala pouze v jejich zobrazování. Případně se zde nabízí alternativa v podobně možnosti uspořádat si funkce do pořadí dle individuálních potřeb uživatele například za pomoci funkce drag and drop.

Návrh řešení na rozšíření počtu uživatelů s ohledem na oblast bezpečnostních rizik, se zde otevírá na straně finančních institucí, jelikož očekávání, že uživatelé budou aktivně prohlubovat svoji informační gramotnost, není příliš reálná. Ideální formou je začít u předávání informací, kdy v případě prokázané závislosti kvalitativních znaků u zájmu o provádění platebních operací za pomoci mobilního zařízení vůči využívání internetového bankovníctví řešené v kapitole 6.2.1, by mohlo dojít k umístění informačního banneru přímo do dané webové bankovní aplikace. Celkově byla v kapitole 6.2.2 potvrzena závislost kvalitativních znaků mezi znalostí mobilních bankovních aplikací a zájmem o mobilní platby, přičemž u komunikace prostřednictvím funkce zprávy z banky není zaručeno, že uživatel tyto zprávy vybírá a banka tak zároveň nemá žádný nástroj, jak uživatele k přijetí zprávy přimět. Dále propagací v multimédiích či za pomoci online marketingových nástrojů, které by mohly oslovit i konzervativnější uživatele.

Jednoznačný prostor pro zvýšení počtu uživatelů tedy autor práce spatřuje v oblasti bezpečnostních rizik a informovanosti klientů o vhodném bezpečném používání zařízení na platformě Android OS, které je aktuálně velmi sporadické.

Vhodným řešením by bylo vytvoření partnerského programu s jedním z vývojářů antivirových aplikací, který vyšel z provedených testů řešených v kapitolách 5.7.1 a 5.7.2 s nejvyšším hodnocením a následné distribuce dané aplikace, či umístění odkazu do Obchod Play, přímo na stránky dané banky, čímž by dané řešení bylo důvěryhodně komunikováno přímo oficiálním informačním kanálem. Vzhledem ke skutečnosti uvedené

v kapitole 5.7.2, že mezi sedmi nejlépe hodnocenými aplikacemi bylo pět aplikací z oblasti freeware, by tak dané finanční instituci nevznikaly téměř žádné dodatečné náklady. Paralelně by tak finanční instituce pasivně zvyšovala bezpečnost svých klientů a poskytla případně prostor k předání informací o zanedbatelném vlivu antivirové aplikace na výdrž baterie či hardware zátěž daného zařízení, jak také vyplývá i z výše uvedených kapitol o testování antivirových aplikací.

Další vhodné řešení, vycházející z kapitoly 5.8, se nalézá v poskytnutí garance pro danou aplikaci, která samozřejmě může být podmíněna nutností instalace antivirové aplikace a disponováním zařízení bez přidělených práv superuživatele. Na základě kapitoly 5.5 bylo potvrzeno, že práva superuživatele v daném zařízení jsou vzhledem k bezpečnostním rizikům zcela nežádoucí. Dále vzhledem ke zjištěným skutečnostem z kapitol 5.3 a 5.4, že i přes případnou důkladnou pozornost uživatele vůči přidělovaným právům při instalaci aplikace mohou některé náказы proniknout i do oficiálního zdroje aplikací Obchod Play, aniž by je podchytil analytický nástroj Google Security a zároveň jsou schopné obejít několikvrstvou ochranu systému, se využití antivirové aplikace rovněž stává prakticky nezbytnou. V případě instalace aplikací třetích stran se stává dle zpracované problematiky přítomnost antivirové aplikace zcela zásadní.

Řešení tohoto typu by výsledně přineslo vyšší účinek, než pouhé snahy o rozšiřování informační gramotnosti. Poskytnutím garance dává finanční instituce najevo důvěru ve vlastní softwarový produkt, která je přenášena na klienta.

Samozřejmě je však stále potřeba rozvíjet i informační gramotnost vzhledem k rizikům podvodných technik uvedených v kapitole 5.2, které si kladou za cíl na základě nepozornosti uživatele získat jeho citlivé uživatelské údaje. V této oblasti nejsou rizika až tak vysoká, jako tomu je v případě internetového bankovníctví, avšak nejen malware pro Android OS dle kapitol 5.1 a 5.6 prochází rychlým vývojem, a tak i tyto podvodné techniky jsou rychle modifikovány pro oblast mobilních telefonů, jak i vyplynulo z kapitol 5.2.1, 5.2.3, 5.2.4, 5.2.5 a 5.2.7.1.

Značné ohrožení autor práce spatřuje v útoku typu DoubleDirect, který lze eliminovat vypnutím ICMP přesměrování paketů, což je však pro uživatele spjato s pro tuto oblast zcela nežádoucími právy superuživatele. Východisko autor práce spatřuje v diskusi s vývojáři, aby byla funkce ICMP Redirect volitelná v GUI Android OS. Možnost volby deaktivace funkce přesměrování paketů by tak zamezila útokům typu

DoubleDirect. Vyšší hrozbu autor práce spatřuje v útocích typu Keylogger na základě běžného rozložení softwarové klávesnice či v případě zneužití Keyloggeru, který byl na zařízení instalován za účelem tzv. rodičovské kontroly. Zde se otevírá prostor k nabídce krátkých interaktivních demo náhledů z aplikace obsahující bezpečnostní doporučení a nabídce konzultací bezpečnostních rizik prostřednictvím Helpdesku či zákaznických linek.

3. Zdroje

1. **IDC Research, Inc.** Smartphone OS Market Share, 2015 Q2. *Http://www.idc.com*. [Online] 2015. [Citace: 12. září 2015.] <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>.
2. **Statista.** Distribution of Android operating systems used by Android phone owners in October 2015, by platform version. *Statista - The Statistic Portal*. [Online] 2015. [Citace: 29. říjen 2015.] <http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/>.
3. **Era.** Era portál – nové internetové bankovníctví. *Https://www.erasvet.cz*. [Online] 2015. [Citace: 12. září 2015.] <https://www.erasvet.cz/fyzicke-osoby/ostatni/stranky/internetove-bankovnictvi/co-je-nutne-k-zalozeni.aspx>.
4. **ING.** Mezi Čechy je oproti zbytku Evropanů jen velmi málo uživatelů mobilního bankovníctví. *Http://www.ingbank.cz*. [Online] 2015. [Citace: 13. září 2015.] <http://www.ingbank.cz/tiskove-centrum/zpravodaj-ing-bank/clanky/mezi-cechy-je-oproti-zbytku-evropanu-jen-velmi-malo-uzivatelu-mobilniho-bankovnictvi.html>.
5. **Zemen, Jakub.** *Internetové bankovníctví*. Praha : Česká zemědělská univerzita v Praze, 2012. Bakalářská práce. Vedoucí práce Ing. Jan Jarolímeck, Ph.D..
6. **ČNB.** Upozornění České národní banky na rizika spojená s využíváním elektronického bankovníctví. *Https://www.cnb.cz*. [Online] ČESKÁ NÁRODNÍ BANKA, 2015. [Citace: 13. září 2015.] https://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/upozorneni_el_bankovnictvi.html.
7. 8. **METODY A TECHNIKY SBĚRU DAT.** *Http://management-marketingu.blogspot.com*. [Online] 2015. [Citace: 15. září 2015.] <http://management-marketingu.blogspot.com/2010/09/8-metody-techniky-sberu-dat.html>.
8. **Vojtíšek, Petr.** Výzkumné metody - Metody a techniky výzkumu a jejich aplikace v absolventských pracích vyšších odborných škol. [Online] 2012. [Citace: 15. září 2015.] Studijní text. http://skoly.praha.eu/files/=84121/Skripta+++Vyzkumne_metody.pdf. ISBN 978-80-905109-3-7.
9. **Kohoutek, Rudolf.** Dotazník jako průzkumná metoda. *Psychologie v teorii a praxi*. [Online] 2010. [Citace: 15. září 2015.] <http://rudolfkohoutek.blog.cz/1002/dotaznik-jako-pruzkumna-metoda>.

10. **Kábrt, Milan.** Test chí-kvadrát nezávislosti v kontingenční tabulce. *Aplikovaná statistika*. [Online] 2011. [Citace: 8. září 2015.] <http://www.milankabrt.cz/testNezavislosti/>.
11. **Petr Mareš, Ladislav Rabušic.** LEKCE09 MĚŘENÍ (SÍLY) ASOCIACE MEZI DVĚMA SPOJITÝMI PROMĚNNÝMI: KORELAČNÍ KOEFICIENTY A GRAFY . <https://is.muni.cz>. [Online] 2012. [Citace: 4. říjen 2015.] https://is.muni.cz/el/1423/podzim2004/SOC418/SPSS_8_korelace.pdf.
12. **Brožová Helena, Tomáš Šubrt, Milan Houška.** *Modely pro vícekritériální rozhodování*. Praha : Credit, 2014. ISBN 978-80-213-1019-3.
13. **ČNB.** ČESKÁ NÁRODNÍ BANKA. *Slovník pojmů ČNB*. [Online] [Citace: 12. říjen 2015.] <http://www.cnb.cz/cs/obecne/slovník/e.html>.
14. **Máče, Miroslav.** *Platební styk: klasický a elektronický*. Praha : Grada, 2006. ISBN 80-247-1725.
15. **Schlossberger, Otakar.** *Elektronické platební prostředky*. Praha : Bankovní institut vysoká škola, 2005. ISBN 80-7265-073-4.
16. **Chvátal, Dalibor Z.** Mobilní bankovní SIM Toolkit je odsouzen k zániku, je staromódní. *měšec.cz*. [Online] 4. duben 2015. [Citace: 19. říjen 2015.] <http://www.mesec.cz/clanky/mobilni-bankovnictvi-bude-pohodlne-ale-mene-bezpecne/>.
17. **Sovová, Eva.** Banka v mobilu začíná ovlivňovat nákupní a finanční chování Čechů. *iDnes.cz/Finance*. [Online] 9. leden 2015. [Citace: 9. září 2015.] http://finance.idnes.cz/analyza-banka-v-mobilu-a-vyuzivani-aplikaci-fky-/viteze.aspx?c=A150108_110432_viteze_sov.
18. **Bubák, Zdeněk.** Začínáme seriál o mobilním bankovníctví v Česku. Postupně představíme aplikace vybraných bank. *Finparáda*. [Online] 27. březen 2015. [Citace: 22. říjen 2015.] <http://www.finparada.cz/2665-Zaciname-serial-o-mobilnim-bankovnictvi-v-Cesku.aspx>.
19. **Schwarzmann, Marek.** Banku v mobilu používá více než 1,1 milionu Čechů. *E15.cz*. [Online] 19. říjen 2015. [Citace: 29. říjen 2015.] <http://e-svet.e15.cz/technika/banku-v-mobilu-pouziva-vice-nej-1-1-milionu-cechu-1237524>.
20. **mBank.** Mobilní aplikace. Jednoduchá, intuitivní a pohodlná. *mBank*. [Online] mBank, 2015. [Citace: 28. říjen 2015.] <http://www.mbank.cz/firemni/sluzby/mobilni-aplikace/>.
21. **ING, Bank.** GENERAL REGULATIONS. <https://www.ing.be>. [Online] 18. srpen 2013. [Citace: 22. listopad 2015.] https://www.ing.be/xpedio/groups/transaction/@transaction/@ibe/@homebank/documents/portalcontent/060776_en.pdf.
22. **Bank, UniCredit.** Služby a parametry GWS. *UniCredit Bank*. [Online] 1. červen 2015. [Citace: 28. říjen 2015.] https://www.unicreditbank.cz/files/download/prime_bankovnictvi/Sluzby_a_parametry_GWS.pdf.

23. **Kuinam J. Kim, Naruemon Wattanapongsakorn.** *Mobile and Wireless Technology 2015*. Berlin : Springer, 2015. ISBN 978-3-662-47668-0.
24. **SocialCompare Collaborative comparsion, engine.** Android versions comparsion. *SocialCompare Collaborative comparsion engine*. [Online] 13. říjen 2015. [Citace: 16. říjen 2015.] <http://socialcompare.com/en/comparison/android-versions-comparison>.
25. **Sarah Mitroff, Jessica Dolcourt.** The Android era: From G1 to Lollipop. *CNET*. [Online] 8. květen 2014. [Citace: 16. říjen 2015.] <http://www.cnet.com/news/history-of-android/>.
26. **Air Bank, a. s.** Mobilní bankovníctví. *Google Play*. [Online] 2015. [Citace: 17. říjen 2015.] <https://play.google.com/store/apps/details?id=cz.airbank.android&hl=cs>.
27. **KB.** Mobilní banka. *Komerční banka*. [Online] Komerční banka, 2015. [Citace: 17. říjen 2015.] <http://www.kb.cz/cs/lide/obcane/mobilni-banka-2.shtml>.
28. **ČS.** SERVIS 24 Mobilní banka. *Česká spořitelna*. [Online] Česká spořitelna, 2015. [Citace: 17. říjen 2015.] <http://www.csas.cz/banka/nav/osobni-finance/servis-24-mobilni-banka/o-produktu-d00024634>.
29. **UniCredit, Bank.** Smart Banking. *UniCredit Bank*. [Online] 2015. [Citace: 30. říjen 2015.] <https://www.unicreditbank.cz/web/obcane/online-sluzby/smart-banking>.
30. **Anmol Misra, Abhishek Dubey.** *Android Security: Attacks and Defenses*. New York : CRC Press, 2013. ISBN 9781439896471.
31. **SocialCompare.** Mobile OSes: developer comparsion. *SocialCompare Collaborative comparsion engine*. [Online] 28. duben 2015. [Citace: 18. říjen 2015.] <http://socialcompare.com/en/comparison/mobile-os-comparison-developer-view>.
32. **TechTerms.** Android Definition. *TechTerms*. [Online] 4. leden 2010. [Citace: 15. říjen 2015.] <http://techterms.com/definition/android>.
33. **Parvez Faruki, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Singh Gaur, Mauro Conti, Muttukrishnan Rajarajan.** Android Security: A Survey of Issues, Malware Penetration and Defenses. *ResearchGate*. [Online] 30. srpen 2015. [Citace: 11. říjen 2015.] http://www.researchgate.net/publication/274013709_Android_Security_A_Survey_of_Issues_Malware_Penetration_and_Defenses. ISSN 1553-877X.
34. **Google, Inc.** Security. *android*. [Online] 2015. [Citace: 10. září 2015.] <https://source.android.com/devices/tech/security/>.
35. **Google, Inc.** The Android Source Code. *android*. [Online] 2015. [Citace: 17. říjen 2015.] <http://source.android.com/source/index.html>.
36. **Tišnovský, Pavel.** Architektura mikrořadičů s jádrem ARM Cortex-M3. *Root.cz*. [Online] 6. září 2015. [Citace: 30. říjen 2015.] <http://www.root.cz/clanky/architektura-mikroradice-s-jadrem-arm-cortex-m3/>.

37. **Suhas Holla, Mahima M Katti.** ANDROID BASED MOBILE APPLICATION DEVELOPMENT and its SECURITY. *http://www.internationaljournalsrsg.org/*. [Online] 2012. [Citace: 3. říjen 2015.] <http://ijcttjournal.org/Volume3/issue-3/IJCTT-V3I3P130.pdf>. ISSN: 2231-2803.
38. **Sebastian Neuner, Victor van der Veen, Martina Lindorfer, Markus Huber, Georg Merzdovnik, Martin Mulazzani, Edgar Weippl***. Enter Sandbox: Android Sandbox Comparison. *Cornell University Library*. [Online] 28. listopad 2014. [Citace: 7. září 2015.] <http://arxiv.org/ftp/arxiv/papers/1410/1410.7749.pdf>.
39. **Šlik, Jáchym.** „Vývojáři mobilních antivirů jsou šarlatáni a podvodníci,“ uvedl expert z Google. *ANDROID MARKET*. [Online] 2011. [Citace: 14. říjen 2015.] <http://androidmarket.cz/ruzne/vyvojari-mobilnich-antiviru-jsou-sarlatani-a-podvodnici-uvedl-expert-z-google/>.
40. **Shankland, Stephen.** Googler: Android antivirus software is scareware from 'charlatans'. *http://www.cnet.com/*. [Online] 18. listopad 2011. [Citace: 16. říjen 2015.] <http://www.cnet.com/news/googler-android-antivirus-software-is-scareware-from-charlatans/>.
41. **Kilián, Karel.** Nové škodlivé aplikace objeveny v Android Marketu. *SVĚT ANDROIDA*. [Online] 12. červenec 2011. [Citace: 12. září 2015.] <http://www.svetandroida.cz/nove-skodlive-aplikace-objeveny-v-android-marketu-201107>.
42. **Golson, Jordan.** Phil Schiller Tweets Link to Mobile Malware Report That Slams Android. *MacRumors*. [Online] 7. březen 2013. [Citace: 4. říjen 2015.] <http://www.macrumors.com/2013/03/07/phil-schiller-tweets-link-to-mobile-malware-report-that-slams-android/>.
43. **Selinger, Markus.** 35 Android Protection Apps Put to a 6-Month Endurance Test. *AV.TEST - The Independent IT-Security Institute*. [Online] 17. prosinec 2014. [Citace: 28. září 2015.] <https://www.av-test.org/en/news/news-single-view/35-android-protection-apps-put-to-a-6-month-endurance-test/>.
44. **Zetter, Kim.** Hacker Lexicon: What Are Phishing and Spear Phishing? *WIRED*. [Online] 4. červenec 2015. [Citace: 18. září 2015.] <http://www.wired.com/2015/04/hacker-lexicon-spear-phishing/>.
45. **Kalabis, Zbyněk.** *Základy bankovníctví: bankovníctví, obchody, služby, operace a rizika*. Brno : BizBooks, 2012. ISBN 978-80-265-0001-8.
46. **Keylogger, Android.** Android Keylogger – 2015 Best Keylogger App for Android. *Android Keylogger*. [Online] 2015. [Citace: 19. říjen 2015.] <http://www.android-keylogger.net/>.
47. **Coob, Michael.** Mobile keyloggers: Defense measures against mobile keystroke logging. *TechTarget - SearchSecurity*. [Online] červen 2014. [Citace: 3. říjen 2015.] <http://searchsecurity.techtarget.com/answer/Mobile-keyloggers-Defense-measures-against-mobile-keystroke-logging>.

48. **Cherian, Blessen.** Preventing DDoS Attacks. *LinuxSecurity.com*. [Online] 2015. [Citace: 6. říjen 2015.] <http://www.linuxsecurity.com/content/view/121960/49/>.
49. **Asaf Shabtai, Dudu Mimran, Yuval Elovici.** Evaluation of Security Solutions for Android Systems. *Cornell University Library*. [Online] 17. únor 2015. [Citace: 28. září 2015.] <http://arxiv.org/ftp/arxiv/papers/1502/1502.04870.pdf>.
50. **Weber, Johannes.** IPv6 Security - An Overview. *RIPE NCC*. [Online] 18. červen 2013. [Citace: 13. září 2015.] https://labs.ripe.net/Members/johannes_weber/ipv6-security-an-overview.
51. **Paganini, Pierluigi.** DoubleDirect MitM Attacks are targeting users worldwide. *security affairs*. [Online] 22. listopad 2014. [Citace: 8. říjen 2015.] <http://securityaffairs.co/wordpress/30417/cyber-crime/doubledirect-mitm-attacks.html>.
52. **COMPUTERWORLD.** Computerworld.cz. *O bezpečnosti aplikací pro Android si můžeme nechat zdát*. [Online] 11. březen 2013. [Citace: 15. duben 2014.] <http://computerworld.cz/securityworld/o-bezpecnosti-aplikaci-pro-android-si-muzeme-nechat-zdat-49594>.
53. **Havryluk, Michal.** Bezpečnost Androidu v číslech. Ještě lepší než jsme doufali. *Mobil.idnes.cz*. [Online] 2014. [Citace: 15. duben 2014.] http://mobil.idnes.cz/bezpecnost-androidu-0lm-/mob_tech.aspx?c=A131102_160512_mob_tech_ham.
54. **Stloukal, Ivan.** Android a bezpečnost - Google zveřejnil data. *Dotekomanie.cz*. [Online] 2014. [Citace: 15. duben 2014.] <http://dotekomanie.cz/2013/10/google-uverejnuje-informace-jak-je-ve-skutecnosti-bezpecnosti-androidu/>.
55. **GmbH, AV-TEST.** AV TEST - The Independent IT-Security Institute. *The best antivirus software for Android*. [Online] 2014. [Citace: 15. duben 2014.] <http://www.av-test.org/en/tests/mobile-devices/android/sep-2013/>.
56. **Nápravník, Jiří.** Největší hrozbou internetového bankovníctví není uživatel. *měšec.cz*. [Online] 11. květen 2015. [Citace: 24. září 2015.] <http://www.mesec.cz/clanky/nejvetsi-hrozbou-internetoveho-bankovnictvi-neni-uzivatel/>.
57. **Horáček, Filip.** Průměrná mzda v Česku stoupla na 26 287 korun, firmám chybí lidi. *iDnes.cz/Ekonomika*. [Online] 4. září 2015. [Citace: 7. listopad 2015.] http://ekonomika.idnes.cz/prumerna-mzda-v-cesku-stoupla-na-26-287-korun-fi8-/ekonomika.aspx?c=A150904_092018_ekonomika_fih.
58. **Dvořák, Jiří.** Vícekriteriální rozhodování. *SlidePlayer*. [Online] 2007. [Citace: 7. listopad 2015.] <http://slideplayer.cz/slide/3032309/#>.
59. **Miroslav Haluza, Jan Macháček.** Využití multikriteriální analýzy (MCA) pro hodnocení inteligentních elektroinstalací. *tzbinfo*. [Online] Fakulta elektrotechniky a komunikačních technologií VUT v Brně, 14. červenec 2011. [Citace: 9. listopad 2015.] <http://elektro.tzb->

info.cz/inteligentni-budovy/7651-vyuziti-multikriterialni-analyzy-mca-pro-hodnoceni-inteligentnich-elektroinstalaci.

60. **ČNB.** Upozornění České národní banky na rizika spojená s využíváním elektronického bankovníctví. *ČESKÁ NÁRODNÍ BANKA*. [Online] 2015. [Citace: 17. říjen 2015.] http://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/upozorneni_el_bankovnictvi.html.