Jak uživatelé přemýšlejí o bezpečnosti v kontextu mobilního bankovnictví?

Data security management | 27.6.2019 | Rubrika: Použitelná bezpečnost | Strana: 11 |
Autor: Petr Doležal Agáta Daňbujanová Lenka Knapová | Téma: Masarykova univerzita, vysoké školy

usable security (použitelná bezpečnost) mentální model autentizační metody mobilní bankovnictví

Představujeme dílčí výstupy několika kol uživatelského testování autentizačních metod v rámci mobilního bankovnictví za účelem vývoje bezpečnějšího, efektivnějšího a uživatelsky příjemnějšího způsobu autentizace.

Celkem proběhla čtyři kola testování s postupným vývojem aplikace a bylo otestováno 33 uživatelů z řad laické veřejnosti (včetně seniorů). Podrobněji představíme tu část výsledků, která se věnovala využití NFC čipu v bezkontaktních platebních kartách, ale i další fázi autentizace na vzorku deseti uživatelů (pět žen a pět mužů ve věku 26–33 let, m = 28,3; jeden středoškolsky vzdělaný a devět vysokoškolsky vzdělaných; všichni mimo IT). Naším cílem bylo porozumět tomu, jak uživatelé přemýšlejí o bezpečnosti a použitelnosti této metody ve srovnání s použitím jim známých metod, a to otisku prstu nebo PIN kódu.

Interakce člověka s počítačem a bezpečnost

Dříve se mělo za to, že se uživatelé nechovají bezpečně, protože jsou líní a neopatrní. Tento pohled se ale pomalu mění a jak upozorňuje Adams a Sasse (1), skutečným důvodem může být spíše nedostatečná uživatelská použitelnost (angl. usability) systému. Uživatelská použitelnost je definována jako míra, do jaké je systém pro specifické uživatele efektivní a příjemný na použití v daném kontextu. Nízká uživatelská použitelnost může vést k nevhodnému používání, obcházení bezpečnostních prvků nebo ukončení používání. Autentizaci můžeme jen stěží považovat za příjemnou nebo vyhledávanou aktivitu, a tak je důležité klást důraz na to, aby byl tento proces pro uživatele co nejpřívětivější. Cílem by mělo být navrhování a testování systémů, které budou maximalizovat uživatelskou použitelnost i bezpečnost. Zároveň je nutné chápat obě perspektivy jako vzájemně se ovlivňující. Je důležité, aby systém byl dostatečně bezpečnostně robustní, ale zároveň ne příliš složitý, jako celek i ve svých částech, aby se neobcházely bezpečnostní prvky (2).
Většina běžných uživatelů se snaží najít kompromis mezi bezpečností a uživatelskou použitelností. Nevolí tak vždy to nejbezpečnější řešení, ale to, které je podle nich vyhovující. Existují měřitelné parametry systému na straně uživatelské použitelnosti, např. efektivita, přesnost, úspornost nebo náročnost na dovednosti. Na straně bezpečnosti jsou to technické parametry, schopnost systému nasměrovat pozornost uživatele na důležité bezpečnostní prvky a udržet ji nebo zda systém sám svým chováním nepodmiňuje uživatele k nebezpečnému jednání (např. příliš časté opakování určitých úloh může vést k jejich bezmyšlenkovitému „odkliknutí“) (2). Mimo technické parametry na straně systémů hrají roli i psychologické proměnné na straně uživatele (3, 4). Mezi ně patří tzv. mentální modely, podle nichž uživatelé upravují své chování v kontextu ICT bezpečnosti (5, 6).

Mentální modely

Podle Westa (7) lze psychologické principy spojené s počítačovou bezpečností shrnout do následujících bodů: lidé podceňují rizika, mají omezený čas a mentální kapacity, bezpečnostní rizika jsou pro uživatele často těžko uchopitelná, protože jsou příliš abstraktní.
Mentální modely (viz Box 1) lidem umožňují utvořit si heuristickou zkratku pro vyhodnocování rizik, pomáhají s orientací ve světě IT bezpečnostních rizik, který je pro uživatele abstraktní, a následně ovlivňují jejich chování.
Uživatelé se snaží přenést odpovědnost na externí aktéry, a to technologické (např. používají správce hesel), sociální (najímají si odborníky na IT bezpečnost) nebo institucionální (důvěřují velkým institucím, jako jsou banky, že jejich data zabezpečí). I přesto ale spoustu rozhodnutí činí sami a my dosud příliš nevíme, na základě jakých mentálních modelů tato rozhodnutí dělají. Nemělo by být cílem pouze posoudit, zda uživatelé mají modely chybné nebo správné, ale více porozumět jejich tvorbě a

logice, tedy pochopit, jak uživatelé přemýšlejí nad bezpečností a čím je toto uvažování ovlivněno. To nám může pomoci jak při vývoji systémů, které budou brát v potaz uživatelskou logiku, tak při osvětě, která bude respektovat způsoby, jakými se tyto modely utvářejí a podle čeho se uživatelé rozhodují. Může to pomoci lépe zacílit rady týkající se bezpečnosti. Prakticky to znamená, že v uživatelských studiích netestujeme jen průchody aplikací a spokojenost uživatelů, ale snažíme se zjistit, jak nad bezpečností uvažují a podle čeho dělají svá rozhodnutí.

Uživatelská studie využití bezkontaktní platební karty

V prvních třech kolech jsme při testování autentizace pomocí hardwarového tokenu s tlačítkem nebo čtečky platebních karet zjistili, že uživatelé mají velké výhrady k vlastnictví dalšího zařízení. Jako důvody uváděli zejména nepraktičnost vlastnictví další věci a riziko ztráty. Rozhodli jsme se proto připravit kvalitativní studii (viz Box 2) se třemi autentizačními scénáři: Uživatelé nejprve prováděli běžnou platbu částky 11 500 Kč a autentizaci prováděli pomocí otisku prstu nebo PIN kódu (dle osobní preference).
Následně stejnou platbu potvrzovali pomocí autentizace skrze kartu s NFC čipem.
Na závěr prováděli platbu vyšší částky 270 000 Kč, kde byla použita dvoufaktorová autentizace, tedy platební karta společně s otiskem prstu nebo PINem (dle osobní preference). Metody

Subjektivně vnímaná uživatelská použitelnost a bezpečnost byla zjišťována formou dotazníků, které byly převzaty z předcházejících studií (8) a upraveny. Dotazníky sledovaly čtyři oblasti: užitečnost, jednoduchost použití, bezpečnost a celkový dojem.
Pro detailnější porozumění uživatelské perspektivě byl veden výzkumný rozhovor, který byl přepsán a analyzován pomocí tematické analýzy (viz Box 3).
Cílem bylo porovnat postoje uživatelů k jednotlivým autentizačním metodám a lépe porozumět mentálním modelům spojeným s autentizací a bezpečností v kontextu mobilního bankovnictví. Vedení rozhovorů a jejich následná systematická analýza nám mohou pomoci do hloubky porozumět chování uživatelů – odpovědět na otázky, proč a jak se chovají určitým způsobem. Uživatelé nebyli nijak proškoleni ohledně rizik nebo výhod a nevýhod jednotlivých metod, abychom se co nejvíce přiblížili jejich současnému uvažování nad bezpečností v oblasti mobilní bezpečnosti.

Dotazníkové výsledky

Společně s preferencí při volbě metod autentizace1 poukazovaly u testovaných uživatelů na: preferenci využití otisku prstu před PIN kódem, vnímání autentizace pomocí otisku prstu jako užitečnější metody než použití NFC čtečky telefonu a platební karty, vnímání autentizace pomocí otisku prstu jako bezpečnější metody než použití NFC čtečky a platební karty.

1 Obojí má vzhledem k velikosti vzorku pouze informativní charakter.

Výsledky tematické analýzy

Jednotlivé kategorie definují zdroje výsledného hodnocení uživatelů, tedy na základě čeho uživatelé utvářejí svá hodnocení. Nabízejí detailnější pohled na způsob, jakým uživatelé mohou formovat své postoje. Byly identifikovány tři tematické kategorie: teoretické předpoklady, osobní zkušenosti a osobní preference. V následné analýze byly identifikovány parametry mentálního modelu uživatelů.

Teoretické předpoklady

Ve svém hodnocení uživatelé čerpají z externích zdrojů nebo se jedná o vlastní úvahy, ale nikoli zkušenosti. Mezi důležité aspekty patří: kdo nese za bezpečnost odpovědnost (v závislosti na tom, kdo to je, mohou uživatelé měnit své bezpečnostní preference), vnímaná bezpečnost jednotlivých komponent (vycházející z představ o principech fungování daného řešení, které ale nemusí odrážet realitu), předpokládaná rizika a hrozby (představy uživatelů o událostech, které se jim mohou přihodit), předpokládané rozšíření metod (uživatelé chtějí záruky, že jejich investovaná energie nepřijde nazmar a produkt se bude dále používat).

Osobní zkušenosti

Uživatelé čerpali z vlastních zkušeností s bezpečnostními metodami, od kterých dále odvíjeli své hodnocení testovaných metod. Odvolávali se na současné i minulé zkušenosti. Důležité pro ně byly zejména oblasti: spolehlivost (jaká jsou záložní řešení, pokud metoda selže), subjektivně vnímaná funkčnost metody (např. rychlost jejího použití).

Osobní preference

Uživatelé hodnotili metody i s ohledem na vlastní specifické preference, u kterých ovšem reflektovali, že jsou pro ně jedinečné. Jeden z uživatelů např. preferoval otisk prstu, neboť se přesouvá mezi třemi byty – líbila se mu jistota, že svůj prst má vždy u sebe a nemůže jej nikde zapomenout. To znamená, že v úvahách uživatelů o bezpečnosti hrají roli i proměnné, které nemůžeme přímo ovlivnit.

Mentální model

U námi testovaných uživatelů se odvíjí od vnímání hrozeb, které jsme pojmenovali jako fyzické. To znamená, že rizika, o nichž přemýšleli, a opatření, která se jim zdála vhodná, byla spojena s fyzickým využíváním mobilních telefonů a zařízení pro autentizaci. Uživatelé měli obavu, že svá zařízení ztratí nebo jim budou odcizena, a proto v předešlých fázích testování kritizovali hardwarové tokeny a čtečky karet. K podobným výsledkům dospěli i jiní autoři (11, 12), kteří popisují obavy britských uživatelů. Otisk prstu byl hodnocen jako uživatelsky přívětivý kvůli své rychlosti a pohotovosti, ale zároveň uživatelům přišel i bezpečnější kvůli své unikátnosti a tomu, že jej nelze jednoduše odcizit nebo ztratit. V případě využití platebních karet se uživatelé obávali, že s nimi nejsou fyzicky spojeny, že je někdo může odcizit společně s telefonem nebo že může pohledem zachytit a zneužít údaje, které jsou na nich napsány. Uživatelé ovšem nereflektovali, že bezkontaktní platební kartu používají běžně pro platbu v obchodech, a nikdo nezmínil, že by se při těchto činnostech obával stejných rizik.

Interpretace výsledků

Při porovnání autentizačních metod dělají uživatelé poměrně komplexní rozhodnutí, zvažují mnoho různých souvislostí a nehodnotí bezpečnost metody jen podle technických parametrů. Uživatelskou použitelnost pro ně nedefinuje pouze to, jak se chová samotná metoda nebo aplikace, ale např. i její potenciální rozšíření nebo uživatelská podpora při selhání. Z hlediska bezpečnosti zvažují jednotlivé komponenty, jejich spolehlivost a možnost záložních řešení. Jedním z důvodů, proč otisk prstu v hodnocení uživatelů předčil bezkontaktní platební kartu, bylo to, že uživatelé vnímají otisk v kontextu dosavadního užívání dohromady s PIN kódem a zároveň vědí, co mají dělat, pokud některá z jim známých metod nefunguje. U karty tyto krizové scénáře neznali, což snižovalo jimi subjektivně vnímanou bezpečnost a použitelnost. Obdobně pro ně bylo důležité vědět, kdo nese za rizika odpovědnost a kdo bude případné bezpečnostní obtíže řešit. Bezpečnost pro uživatele nesymbolizuje jen samotné technické řešení, ale i instituce, služby a další aktéři, kteří tato řešení doprovázejí. Uživatelé bezpečnost posuzují podle více kritérií svého mentálního modelu možných hrozeb. Námi testovaní uživatelé ve svém hodnocení, a dost možná i v bezpečnostním chování, vycházejí z modelu, který zdůrazňuje fyzické hrozby, jako je např. krádež. Tento model je ale nepřesný a neumožňuje jim adekvátně zhodnotit digitální hrozby, i když je může motivovat k bezpečnějšímu chování, např. k provádění transakcí na neveřejném místě.
Uživatelé zvažují, co jim daná autentizační metoda přinese. Pokud ji vnímají pouze jako další vrstvu zabezpečení, která ale není dostatečně odůvodněná („Proč doteď stačil jen otisk prstu?“), odmítají ji. To klade důraz buď na využívání technologií k více účelům (např. možnost platby pomocí NFC čtečky i v e-shopech), nebo hledání takových technologií, které uživatele nezatíží dalším zařízením.

Proč uživatelé preferují otisk prstu?

1. Uživatelé věří, že každý otisk prstu je na celém světě jedinečný. Mají pocit, že této technologii rozumějí natolik, že jí mohou důvěřovat.

2. Rizika, která vnímají (únos či useknutí prstu), jsou v českém prostředí velmi nepravděpodobná, proto se jich příliš neobávají.
3. Z jejich pohledu není v případě otisku prstu nutné žádné
speciální bezpečnostní chování.
4. Otisk prstu je velmi rozšířenou metodou, která je dnes podporována téměř každým chytrým telefonem. Uživatelé díky tomu věří, že se technologie bude využívat i do budoucna. To snižuje jejich motivaci přijímat technologie nové.
5. Při této autentizační metodě uživatelé nepotřebují žádná další zařízení, je to rychlé, jednoduché a intuitivní. V případě nemožnosti použití je vždy k dispozici záložní metoda (obvykle PIN).
Jejich porozumění principům fungování otisku prstu je v souladu s jejich mentálním modelem hrozeb, je pro ně uživatelsky přívětivý, rozšířený a mají představu záložních řešení. Zde se tak projevuje, že preference a mentální modely uživatelů nemusejí vždy odrážet reálnou bezpečnost technologie a reflektovat hrozby s ní spojené (např. reálnou možnost dešifrování souboru v telefonu, ve kterém je otisk prstu uložen). Pro další výzkum by mohlo být zajímavé více se zaměřit na to, jak daný mentální model vzniká. To by mohlo přinést i více informací, jak jej případně ovlivňovat směrem k přesnější a v důsledku bezpečnější reprezentaci potenciálních hrozeb.

Doporučení pro vývoj a zavádění autentizačních metod

1. Navrhované nové metody autentizace musejí být nabízeny a představovány jako komplexní služba se zapojením relevantních institucí (jako jsou banky) a služeb (jako je podpora uživatele při bezpečnostním selhání).
2. Vydavatel nové metody by měl znát mentální modely uživatelů, na které cílí. Při edukaci běžných uživatelů je potřeba jim nabídnout uchopitelné metafory popisující hrozby a preventivní opatření, které budou vycházet z již existujících mentální modelů (např. fyzického ohrožení) nebo na ně navazovat.
3. Při případném vývoji nových metod je vhodné hledat takové, které využijí již stávající metody a pro uživatele rychle dostupná zařízení.
4. Nové metody by mohly být využity pro více úkonů i mimo mobilní bankovnictví, aby se zvýšila jejich užitečnost a přijatelnost pro uživatele.
5. S ohledem na relativní stálost mentálních modelů uživatelů a z nich plynoucích preferencí autentizačních metod lze doporučit, aby se usilovalo o zvýšení bezpečnosti preferovaných metod (např. zabezpečení čteček otisků prstů s kontrolou živosti).

Mentální modely BOX 1 Popisují, jak uživatelé přemýšlejí o problémech. Jde o uživatelovu představu o tom, jak věci fungují a jaké efekty budou mít různé druhy jednání. (5) Často nejsou přesnou reprezentací reálného světa a mohou vést k chybnému chování (ale také nemusejí, i chybný model může být funkční). (5) Bývají sdílené mezi určitou populací, tj. jsou spoluvytvářeny sociálními a kulturními vlivy. (5) Je důležité se jimi zabývat, abychom nevyvíjeli systémy, které nereflektují, podle čeho uživatelé reálně jednají.

Kvalitativní výzkum BOX 2 Kvalitativní metody umožňují porozumět zkoumaným fenoménům do větší hloubky, protože ne všechny odpovědi na otázky lze smysluplně redukovat na čísla pro statistické vyhodnocení. Kvalitativní výzkum umožňuje nejen zaznamenat, co respondenti dělají, ale také zjistit, jaký význam připisují svým akcím, proč tak činí a jak porozumění ovlivňuje jejich chování. V našem výzkumu jsme si kladli otázku, jaký (myšlenkový) proces se skrývá za preferencemi uživatelů a jak tento proces ovlivňuje to, co upřednostňují. V kvalitativním výzkumu se neusiluje o reprezentativní vzorek respondentů, protože cílem není zobecnit výsledky na populaci a ani to není prakticky proveditelné, protože se zde nepracuje s několika málo definovatelnými proměnnými. Jde o porozumění danému jevu v daném kontextu a v co možná největší hloubce a nuancích. Obvyklé jsou nižší počty respondentů postačující k teoretické saturaci, kdy sběr dat od dalších respondentů již nepřináší nová porozumění (9, 10). Tematická analýza BOX 3 Tematická analýza spočívá v hledání určitých témat nebo vzorců napříč (celým) souborem dat, tj. doslovnými přepisy rozhovorů s uživateli. Tato témata vznikají na základě systematického kódování významových jednotek textu. Systematický přístup k analýze pomáhá předejít zaujatým interpretacím a zdůraznění pouze dílčích témat. Mgr. Petr Doležal

Psycholog, který se v rámci projektu na **Fakultě informatiky** Masarykovy univerzity zabývá kvalitativní metodologii při výzkumu psychologických aspektů usable security.

Mgr. Agáta Dařbujanová

Jako členka Centra pro výzkum kryptografie a bezpečnosti na **Fakultě informatiky** Masarykovy univerzity se ve svém výzkumu zabývá usable security v oblasti autentizačních metod, a to často ve spolupráci s komerčními firmami.

Mgr. Lenka Knapová Věnuje se výzkumu v oblasti počítačové bezpečnosti na **Fakultě informatiky** Masarykovy univerzity. S ohledem na své předchozí vzdělání v oblasti psychologie přistupuje ke zkoumání bezpečnosti z pohledu uživatele. Zaměřuje se na psychologické aspekty počítačové bezpečnosti ovlivňující rozhodování a chování uživatelů a nalezení rovnováhy mezi bezpečností a použitelností.

POUŽITÉ ZDROJE (1) ADAMS, A.; SASSE, M. A. Users are not the enemy. Communications of the ACM. 1999, vol. 42, pp. 40–46. (2) KAINDA, R.; FLECHAIS, I.; ROSCOE, A. W. Security and Usability: Analysis and Evaluation. 2010 International Conference on Availability, Reliability and Security. 2010, pp. 275–282. (3) HOWE, A. E.; RAY, I.; ROBERTS, M.; URBANSKA M.; BYRNE, Z. The Psychology of Security for the Home Computer User. 2012 IEEE Symposium on Security and Privacy. 2012, pp. 209–223. (4) BENENSON, Z.; KROLL-PETERS, O.; KRUPP, M. Attitudes to **IT** security when using a smartphone. 2012 Federated Conference on Computer Science & Information Systems (FedCSIS). 2012, pp. 1179–1183. (5) WASH, R. Folk Models of Home Computer Security. Proceedings of the Sixth Symposium on Usable Privacy and Security, 2010. (6) WASH, R.; RADER, E. Influencing Mental Models of Security: A Research Agenda. Proceedings of the 2011 New Security Paradigms Workshop. 2011, pp. 57–66. (7) WEST, R. The Psychology of Security. Communications of the ACM. 2008, vol. 51, no. 4, pp. 34–41. (8) RAMOS-DE-LUNA, I.; MONTORO-RÍOS, F.; LIÉBANA-CABANILLAS, F. Determinants of the Intention to Use NFC Technology as a Payment System: An Acceptance Model Approach. Information Systems and e-Business Management. 2016, vol. 14, no. 2, pp. 293–314. (9) MAXWELL, J. A. Qualitative Research Design. An Interactive Approach (3rd ed.). Sage, London, 2013. ISBN 978-1-4129-8119-4. (10) CHARMAZ, K. Constructing Grounded Theory. A Practical Guide Through Qualitative Analysis. Sage, London, 2006. ISBN-10 0-7619-7352-4. (11) PAUL C. L., MORSE E., ZHANG A., CHOONG YY., THEOFANOS M. (2011) A Field Study of User Behavior and Perceptions in Smartcard Authentication. In: Campos P., Graham N., Jorge J., Nunes N., Palanque P., Winckler M. (eds) Human-Computer Interaction – INTERACT 2011. INTERACT 2011. Lecture Notes in Computer Science, vol 6949. Springer, Berlin, Heidelberg (12) KROL, K.; PHILIPPOU, E.; CRISTOFARO, E.; SASSE, M. “They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. CoRR. 2015.

Foto popis|

O autorovi| Petr Doležal Agáta Dařbujanová Lenka Knapová, pdolezal@mail.muni.cz xdarbuj@mail.muni.cz knapova@mail.muni.cz