Posudek práce

předložené na Přírodovědecké fakultě JU

☑posudek vedoucího ❑posudek oponenta
☑ bakalářské práce ❑ diplomové práce

Autor/ka:	Petr Holub
Název práce:	Bezpečnost OTP zasílaného formou SMS, autentizačního a autorizačního nástroje a nebezpečí zneužití služeb elektronického bankovnictví ovládnutím počítače a chytrého telefonu klienta
Studijní program a obor:	Aplikovaná informatika
Rok odevzdání:	2017

Jméno a tituly vedoucího/~~oponenta~~:	Jan Doubek, MBA
Pracoviště:	Česká pošta, s.p.
Kontaktní e-mail:	Doubek.Jan@cpost.cz

Odborná úroveň práce:
❑ vynikající ☑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Věcné chyby:
❑ téměř žádné ☑ vzhledem k rozsahu přiměřený počet ❑ méně podstatné četné ❑ závažné

Výsledky:
❑ originální ☑ původní i převzaté ❑ netriviální kompilace ❑ citované z literatury ❑ opsané

Rozsah práce:
❑ veliký ☑ standardní ❑ dostatečný ❑ nedostatečný

Grafická, jazyková a formální úroveň:
❑ vynikající ❑ velmi dobrá ☑ průměrná ❑ podprůměrná ❑ nevyhovující

Tiskové chyby:
❑ téměř žádné ☑vzhledem k rozsahu a tématu přiměřený počet ❑ četné

Celková úroveň práce:
❑ vynikající ☑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:

Práce je zpracována přehledně, v úvodních kapitolách stručně popisuje oblast elektronického bankovnictví a do ní pak v kapitole č. 4 zasazuje Internetové bankovnictví, které je hlavním dějištěm zkoumané problematiky. Tou je současné vnímání úrovně bezpečnosti nejrozšířenějšího nástroje pro autentizaci a autorizaci – One Time Password (jednorázově používaného kódu, dále jen OTP), zasílaného formou SMS (krátké textové zprávy) na mobilní telefon klienta.

V kapitole 5. je velice pěkně popsáno obecné modus operandi útoků na peněžní prostředky klientů bank, kteří používají internetové bankovnictví k řešení svých finančních transakcí. I když je vše popsáno obecně, je zcela přesně uveden postup a nástroje vedoucí k ovládnutí počítačů, které klienti používají k internetovým bankovním transakcím, a také k ovládnutí mobilních telefonů, jenž slouží jako nezávislé komunikační kanály pro získání OTP za účelem autentizace (potvrzení oprávněnosti při vstupu do systému internetového bankovnictví) nebo autorizace (potvrzení) transakce zadávané přes internetové bankovnictví.

Je nutné upozornit, že zde popsané schéma útoku skutečně odpovídá stovkám a možná dnes již i tisícům skutečně realizovaných útoků na účty klientů, používajících internetová bankovnictví největších bank v ČR, s reálnými škodami ve výši mnoha milionů Kč. Některé uvedené konkrétní případy pak jsou jen ilustrací mnoha dalších a rozhodně nejsou jejich úplným výčtem. Oceňuji však jejich výběr, neboť jsou vhodným a srozumitelným příkladem a zároveň východiskem dalších úvah této práce.

V další části jde autor práce k jádru skutečného problému a tím je ohrožení kdysi zcela bezpečného nástroje (OTP zasílaného formou SMS), vlastním vývojem používané komunikační technologie – mobilního telefonu. Tzv. chytré telefony sice stále používají formát SMS, ale z hlediska bezpečnosti přenosu a zpracování těchto komunikačních dat ve vlastním přístroji otevírají útočníkům možnosti získání a zneužití obsahu těchto dat, dříve zcela vyloučené.

Od popisu problematiky se autor dále dostává k návrhům alternativních řešení současné situace, z nichž některé jsou v bankách již ve stádiu úvah, zkoušek nebo dokonce užití pro část klientely. Všechny navrhované alternativy jsou reálně možné a autor zde nepřichází s žádnou originální myšlenkou. Načrtnuta je i stručná SWOT analýza jednotlivých alternativ, ale právě v této části práce jsem očekával o krůček více. Přesto hodnotím práci jako zdařilou a rozhodně doporučuji uznat jí jako bakalářskou práci.

Případné otázky při obhajobě a náměty do diskuze:

K ovládnutí chytrého telefonu klienta dochází tak, že uživatel sám povolí instalaci škodlivého malware do svého telefonu. Tato škodlivá aplikace je obvykle instalována z prostředí mimo oficiální obchody s aplikacemi pro tato zařízení. Proto je nebezpečí největší pro telefony s OS Android, neboť ostatní OS obvykle nedovolují instalaci aplikace mimo oficiální distribuci, kde probíhá jistá cenzura vlastností aplikací před jejich zařazením do distribuce. Zde je tedy vhodné položit otázku:

Které chytré telefony jsou pro popsaný typ útoku, vedoucího k ovládnutí takového telefonu útočníkem nejvíce náchylné, a proč tomu tak je?

Myslíte si, že popisované aplikace pro generování OTP přímo v telefonu klienta budou lépe chráněny proti napadení takového přístroje jiným typem malware? Pokud ano, proč?

Práci

☑ doporučuji

❑ nedoporučuji

uznat jako diplomovou/bakalářskou.

Navrhuji hodnocení stupněm:

❑ výborně ☑ velmi dobře ❑ dobře ❑ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:

V Českých Budějovicích, 11. 5. 2017