Aplikace pro ochranu mobilní komunikace před odposlechem a zneužitím citlivých informací.

Radim Rindler
Obchodní ředitel CircleTech s.r.o.

CircleTech

CircleTech s.r.o.

Společnost CircleTech, s.r.o. založili v lednu roku 2004 dva studenti Matematicko-fyzikální fakulty Univerzity Karlovy v Praze, Jiří Šatánek a Marian Kechlibar.

Od svého vzniku se zabývá aplikovanou kryptografií.

Prvním produktem byla v roce 2005 aplikace SMS007 pro šifrování SMS zpráv, která měla ve své době tisíce spokojených uživatelů v České republice i v zahraničí.
Rozšířenost aplikace SMS007 už v roce 2007 upoutala pozornost informační služby BIS. Nemožnost dešifrování SMS se pokoušela řešit způsobem, který byl vnímán jako nepřiměřený nátlak. Filozofií společnosti CircleTech je přesvědčení o nezadatelném právu každého člověka na soukromí, a to i v čase mobilní komunikace. Proto byla spolupráce s BIS odmítnuta a případ široce medializován.
Uvedení systému CryptoCult na trh v roce 2010 a svěřená důvěra klientů vedla k rychlému růstu společnosti. Společnost CircleTech je v současnosti dominantním hráčem v oblasti zabezpečení mobilní komunikace v České republice. Klientelu tvoří lidé a společnosti, kterým na bezpečnosti skutečně záleží.

CircleTech

V roce 2012 proběhla úspěšná expanze na slovenský trh.

V současné době probíhají finální jednání pro vstup na trh v USA, Brazílii, Malajsii, Polsku a dalších zemích EU i mimo ni.

CircleTech

Technologie odposlechů

Výzkumník Karsten Nohl z berlínské Security Research Labs říká, že mu k odposlechu GSM hovoru stačí mobil Motorola za pár set korun, notebook, bezplatně dostupný software a tři minuty času.

Oficiální varování US Gov na telefonním automatu.

Postup prý není nijak složitý. Levný mobil Motorola s modifikovaným firmwarem je použit k „vyčmuchání“ lokalizačních dat, která jsou nutná pro správné nasměrování hovorů (či textovek) v síti. V tomto případě však poslouží k identifikaci cíle (odposlouchávaného). Dalším krokem je nahrání hrubých dat přes USB do počítače. K rozšifrování je použita tzv. rainbow table (tabulka použitých klíčů). Crackovacímu programu prý trvá asi 20 sekund, aby mohl začít živě nahrávat odposlech telefonního hovoru.

CircleTech

Řešení ochrany mobilní komunikace a citlivých dat

CryptoCult

CryptoCult je systém pro zabezpečení mobilní komunikace. S CryptoCultem můžete bezpečně telefonovat, psát zprávy a e-maily. Tento systém je jednoduchý a intuitivní, ovládání a reakce jsou velmi podobné jako u Vašeho mobilního telefonu. Veškerá komunikace probíhá za použití internetu, pro provoz stačí základní datový tarif, nebo připojení k síti WiFi. Pokud jste připojeni prostřednictvím sítě WiFi, je možné CryptoCult využívat i bez SIM karty.

Volání

Volání přes CryptoCult probíhá na stejné úrovni jako Vaše běžné hovory. O jejich zabezpečení se stará šifra AES-256. Pro šifrování hovoru je použit jednorázový unikátní klíč, který je platný pouze po dobu hovoru. Po jeho ukončení okamžitě zanikne a pro další komunikaci je už generován klíč nový – zpětné dešifrování tudíž není možné.

Integrovaná komunikační aplikace

Zprávy
Systém obsluhy zpráv je v CryptoCultu velmi podobný tomu, na který jste zvyklí z Vašeho telefonu. Navíc podporuje výpisy o doručení i přečtení zprávy, posílání vizitek i příloh. Zprávy jsou zabezpečeny standardem PGP.

E-mail
E-mailový klient CryptoCultu Vám umožní pohodlně odesílat a přijímat šifrované e-maily z jakékoliv Vaší e-mailové schránky, včetně odesílání a přijímání příloh. Pro zabezpečení je stejně jako u zpráv použit standard PGP.

Kalendář
Aplikace Kalendář umožňuje ukládat a zobrazovat plánované události a schůzky a bezpečně je sdílet s ostatními uživateli CryptoCultu. Díky kalendáři můžete bezpečně zvát další uživatele CryptoCultu na schůzky nebo spolu schůzky synchronizovat.

CircleTech

Technologie

VoIP

Šifrování AES-256 – hlas

PGP - text

Infrastruktura:
SIP server – modifikovaný pro spojení CC uživatelů (Klient <-> Klient).
Veškerá tvorba klíčů pro hovory, PGP klíčů probíhá bez prostřednictví PKI (Public Key Infrastructure).
Vlastního přenosu se nezúčastňuje žádný prostředník umožňující otevřít ‚zadní vrátka‘

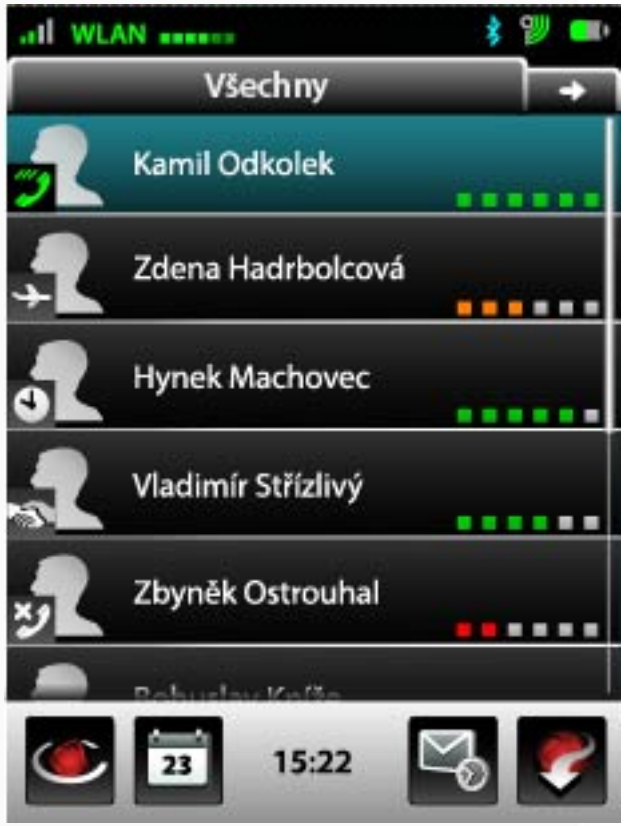
CircleTech

Správa kontaktů

Příjem a odeslání vizitky včetně veřejného PGP klíče

Typ připojení uživatele (WLAN, 3G, EDGE, GPRS)

Stav uživatele



CircleTech

Ochrana proti triangulaci - MiTMA

CircleTech

Zprávy – Instant Messaging

Obdoba SMS/MMS

5000 znaků + Přílohy

Pouze uživatelé CC

Šifrování PGP včetně příloh

CircleTech

E-mail

10 mailových schránek

Automatická správa PGP klíčů

Možnost přijímání a odesílání šifrovaných i nešifrovaných zpráv

Ukládání šifrovaných příloh

CircleTech

Kalendář

Šifrování PGP

Group Time Management – sdílení a organizace událostí

Možnost importu a exportu záznamů

CircleTech

Trezor

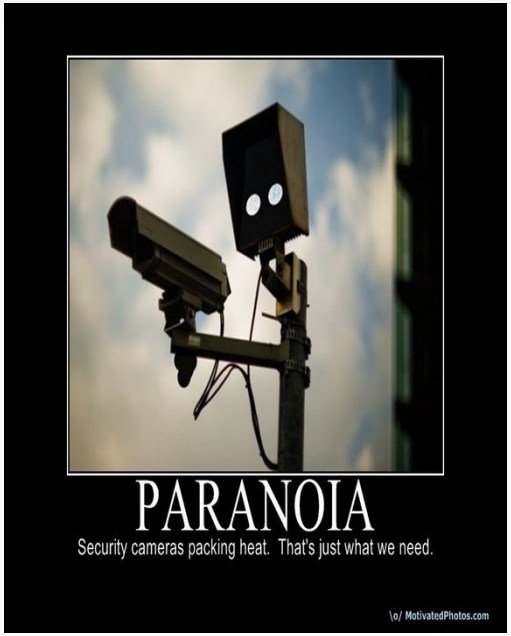
Šifrované úložiště užitečných údajů

Hesla
PIN
Údaje kreditních karet

Možnost přeposlání údajů jinému uživateli CryptoCult!

CircleTech

Přínosy řešení chráněné komunikace CryptoCult



- Ochrana proti odposlechu a zneužití citlivých soukromých, či podnikových informací - možnosti zneužití jsou široké.
- Svobodná komunikace mezi uživateli CC - Uvolnění při hovoru.
- Efektivní komunikace.
- Vyšší míra soukromí - vyšší míra osobní svobody.

- Ochrana duševního zdraví

CircleTech

Otázky ?

Děkuji za pozornost!

Radim Rindler
Obchodní ředitel CircleTech s.r.o.