AUTOR: ING. FILIP KLASNA

SECURE OS Communicator X1 aneb šifrovaný telefon TAG T1 pro agenta 007 nebo českého ministra vnitra

V redakci mi přistála malá nenápadná krabička, která v sobě ukrývala zabezpečený telefon od společnosti spyshop24.cz. Když jsem ji otevřel, měl jsem pocit, že na mě kouká poněkud větší iPhone 3GS se svými hliníkovými zády... Ostatně telefon je vyráběný firmou Foxconn, která dělá pro Apple iPady a iPhony nebo počítače Mac mini, takže kvalita výrobku by měla být zaručena. Že se nejedná o zvětšený iPhone, je poznat podle 2 čoček fotoaparátu, diody blesku a dotykové plošky na čtení otisku prstu.

Hardware telefonu je zcela dostatečný pro účel, který má X1 plnit. Srdce telefonu tvoří čtyřjádrový procesor o frekvenci 1.3 GHz spolupracující s RAM o velikosti 3 GB, lokální úložiště disponuje velikostí 32 GB, baterie má kapacitu 3200 mAh. Fotoaparáty na zádech přístroje mají rozlišení 13 MP a 0,3 MP, čelní fotoaparát disponuje 5 MP. V horní části telefonu se nachází klasický audio jack, na spodní straně se nachází napájecí konektor USB-C.

Uvnitř telefonu se nachází speciální zabezpečená verze operačního systému Android od Secure Group s nečekaným jménem Secure OS. Tento operační systém nabízí ořezané základní funkce Androidu a přidává vojenské zabezpečení.

X1 disponuje end-to-end šifrováním, kdy informace uložené v zařízení a všechny datové přenosy mezi partnery jsou šifrovány, aby se zabránilo přístupu třetích stran.

Samostatné ověřování hesla chrání šifrovaný pevný disk, zabezpečený operační systém a komunikační aplikace. Výrobce se chlubí tím, že systém byl vyvinut po analýze hrozeb v mobilním prostředí a díky neustálému vývoji a patchům udržuje systém stále aktuální a zabezpečený proti stále novějším hrozbám.

Kontrola nad každou částí telefonního hardwaru umožňuje vypínat či povolovat různé funkčnosti telefonu, jako jsou bezdrátové přenosy, USB nebo kameru.

Secure OS je zcela zbaveno kódů společně využívaných různými aplikacemi, výrobce myslel i na možnost získat data ze zařízení v recovery módu tím, že tuto možnost z Secure OS zcela odstranil, a data uživatele jsou tak zcela zabezpečena proti zneužití a zcizení. Pokud dojde k pokusu o prolomení zařízení, Secure OS vymaže veškerá data, které v něm jsou uložená. Pokud se obáváte malwaru ve svém telefonu, tak X1 při každém restartu zkontroluje, zda nedošlo v operačním systému k neautorizované změně, a aplikace třetích stran navíc nemohou shromažďovat data z jiných aplikací.

X1 disponuje několika režimy, které určují chování a vzhled telefonu.

Máme zde zabezpečený defaultní režim, ve kterém je veškerá komunikace ať už telefonická, případně chatovací šifrována end-to-end a telefon má zakázaný přístup k aplikacím z Google obchodu. X1 běží ve zjednodušeném režimu jedné obrazovky, na které můžete zvolit pouze chat, telefonování a e-mail a vidíte stav telefonu, jako je mobilní signál, zbývající kapacita baterie apod. Přístup máte i do svého trezoru, do kterého můžete ukládat své fotografie, videa a poznámky. V okamžiku, kdy se snažíte dostat do jakékoliv aplikace telefonu, musíte vždy zadat číselné heslo, kdy se numerická klávesnice vždy nepatrně mění, takže si musíte dávat pozor, co zadáváte. V případě zadání chybného kódu vás X1 jemně varuje, že zbývá již jen 9 pokusů a následně dojde k destrukci obsahu celého zařízení. Takže i pokud byste nechali telefon odemčený na stole, díky požadavku na heslo při každé akci jsou vaše data a komunikace v bezpečí.

V zabezpečeném režimu je možné využívat chatování, kdy ochrana vašich dat je zajištěna pomocí nejmodernějších šifrovacích protokolů jako OMEMO, ZRTP a OTR. Samotné zprávy se neukládají na žádný server a stejně jako v případě známého komunikátoru pro Android a IOS Threema jdou rovnou na cílové zařízení. Stejně tak pokud si budete v chatu sdílet běžné soubory jako prostý text, word nebo excel, žádná data se neukládají na serverech, ale jdou přímo z jednoho zařízení na druhé bez prostředníka.

Šifrované VoIP volání typu peer-to-peer také neběží přes žádný server, a X1 tak není ohrožován odposlechy a útoky typu „člověk uprostřed", tedy Man-in-the-middle, kdy útočník odposlouchává komunikaci tím způsobem, že se stane aktivním prostředníkem v komunikaci, kterou začne řídit, případně může data měnit.

Pokud byste chtěli využívat telefon i jinak, je tu ještě pracovní režim, kdy telefon disponuje možností se podobat o něco více běžnému androidovému telefonu, kdy je funkčnost telefonu o něco vyšší a vy disponujete možností používat důvěryhodné aplikace běžící v sandboxu.

A konečně třetí mód, zvaný inkognito, umožňuje telefon bleskově přepnout ze zabezpečeného režimu do podoby, kdy obrazovka zobrazuje ikony, jako je Facebook, Instagram či prohlížeč Opera, a vypadá pro člověka který s vámi sedí u stolu, jako zcela normální, ničím nezajímavé zařízení, které ani náhodou neumí nic zvláštního. Aktivace režimu inkognito se provede přejetím prstu po obrazovce odspoda nahoru. Obrazovka zrudne a objeví se možnost okamžité smazání obsahu X1, poněkud nepochopitelná volba uvolnění paměti RAM nebo právě přepnutí do režimu inkognito.

Centrální správa zařízení

Pokud byste hodlali provozovat několik zařízení typu X1, výrobce nabízí jejich správu pomocí vlastní platformy pro správu mobilních zařízení Secure Administration System, ve kterém lze centrálně konfigurovat a nastavovat zařízení ve vaší správě, která lze zařazovat do skupin a konfigurovat tak najednou. Kromě telefonů je možné nastavovat pravidla a zásady i pro samotné uživatele.

Secure Administration System je schopné aktivovat či deaktivovat jednotlivé hardwarové komponenty X1, jako je fotoaparát, Wi-fi, Bluetooth a další. Stejně tak můžete nastavovat integrovaný firewall a nastavit tzv. blacklisty pro určité IP adresy.

Kromě HW parametrů přes centrální správu můžete konfigurovat také samotný operační systém a jeho chování. Je tedy možné zakázat třeba přiložení souborů do e-mailu, zakázat videohovory nebo ovlivnit, jaké verze aplikací je možné v OS využívat.

Samotný Secure OS přichází pouze s proprietárními šifrovanými aplikacemi vyvinutými společností Secure Group, ale právě díky centrální správě se dá na seznam povolených aplikací přidat aplikace nová.

V případě ztráty nebo odcizení zařízení je možné telefon na dálku smazat.

A SIM karta?

Telefon je dodáván spolu se SIM kartou, která umožňuje volání a používání internetu bez dalších poplatků po celém světě (internetový balíček 10 GB/měsíc). SIM karta spolupracuje se všemi lokálními operátory a 2 čísla IMSI umožňují získat nejlepší možný signál.

Agent nebo ministr

Pro koho je tedy telefon určený? Pro jednotlivce zcela určitě ne, musejí být minimálně dva, abyste využili potenciál tohoto přístroje v oblasti šifrované komunikace. Využití bych viděl u firem nakládajících s citlivými daty, u advokátních nebo právních kanceláří, ale i v rámci komunikace mezi politiky. Telefon lze provozovat jako druhý telefon k běžnému chytrému telefonu, protože jeho multimediální schopnosti neohromí a ostatně to ani není cílem tohoto zařízení.

Hodnocení:

+ bezpečnost komunikace
+ centrální správa
+ kvalitní provedení
+ cena