Ukázali jsme, že lze zaútočit na bezpečnost čipů, říká brněnský expert

21. listopadu 2017 14:10

https://brno.idnes.cz/petr-svenda-cipy-bezpecnost-it-systemu-viry-pocitace-mobily-p5c-/brno-zpravy.aspx?c=A171120_365414_brno-zpravy_dh

Brněnský expert na bezpečnost IT systémů Petr Švenda bude dávat svým nejbližším pod stromeček zařízení proti počítačovým hackerům. Příhodnější dárek od něj ani čekat nelze. Švenda je členem týmu, jenž objevil „díru“ v bezpečnostních čipech společnosti Infineon Technologies.

Zvětšit fotografii

Zdroj: https://brno.idnes.cz/petr-svenda-cipy-bezpecnost-it-systemu-viry-pocitace-mobily-p5c-/brno-zpravy.aspx?c=A171120_365414_brno-zpravy_dh

Sedmatřicetiletý Petr Švenda je výzkumník a pedagog na Fakultě informatiky Masarykovy univerzity v Brně. | foto: Marie Stránská, MAFRA

Nedávno jste se vrátili z amerického Dallasu, kde jste svůj objev prezentovali. O co šlo?

Byla to jedna ze čtyř nejvýznamnějších akademických konferencí zaměřených na bezpečnost a její aplikaci do praxe. Zveřejnili jsme tam výsledky své celoroční práce. Zjistili jsme, že způsob, jakým se generují kryptografické klíče u čipů firmy Infineon, je problematický a že z veřejné části klíče se dá poměrně rychle získat jeho tajnou část, která má chránit citlivé údaje svého majitele. A vzhledem k tomu, že se čipy používají na celou řadu věcí, včetně elektronických podpisů, šifrování korespondence, na ověření uživatelů při vstupu do nějakého systému, u občanských průkazů nebo platebních karet, vyhodnotili jsme to jako velký problém a okamžitě firmu informovali. To bylo v únoru. Měla osm měsíců na to, aby problém odstranila. Proto jsme o objevu veřejnost informovali až nyní.

Kryptografický klíč, veřejná, tajná část... Jak to funguje?
Musíte mít nějaké „tajemství“, které dokáže, že jste to právě vy. Čipová karta je v podstatě malý počítač, relativně dost výkonný. Do něj přijdou nějaká data a to, co odejde zpět, bude například podpis. A aby to proběhlo, potřebujete nějaký podepisovací klíč, který zná jen jedna strana. Proto jsou dva klíče – veřejný a privátní. K veřejnému se může dostat kdokoli, privátní je jen na vaší čipové kartě. Tyto klíče musejí někde vzniknout. A my jsme objevili, že způsob vzniku je nešťastně udělaný. Z veřejného se dá poměrně rychle dopočítat klíč soukromý.

To znamená, že se pak za mě někdo může podepisovat, dešifrovat zprávy nebo odesílat bankovní příkazy, prostě cokoli?
Ano, jde také o to, jak je která země v digitalizaci daleko. Například Estonci na elektronickou agendu přesunuli velké množství operací, včetně možnosti volit. Problém nastal i na Slovensku, kde problematické čipy použili v občanských průkazech. Týká se to asi 300 tisíc lidí, z nichž digitální podpis aktivně používá asi desetina. Státy teď zneplatňují certifikáty pro zranitelné veřejné klíče. To udělali právě na Slovensku, v Estonsku nebo třeba ve Španělsku a lidé si nyní musí dojít na úřad a požádat o nový certifikát.

Pro vás je to tedy už uzavřená záležitost?
Úplně ne. Ukázali jsme, že lze na bezpečnost čipů zaútočit a je nutné ji zlepšit. Nyní pracujeme na ověření, do jaké míry lze útoky zrychlit. Realistická cena útoku je důležitá pro rozhodnutí, jak problém řešit. Dále zkoumáme i čipy od jiných výrobců, zda nemají podobný problém. Často se mě známí ptají, proč hledáme možnost zaútočit na systém, když nechceme nikomu škodit. Jenže pokud to nebudeme my a nám podobní dělat, tak to budou dělat pouze ti, kteří chtějí škodit.

Zmínil jste Slovensko, kde váš objev způsobil slušný poprask. Nebylo by lepší nic neříct a jen vše v tichosti opravit?
Nebylo, protože v dřívějších případech se často stávalo, že se na to firmy vykašlaly. Samotná oprava totiž stojí peníze, některé společnosti se dokonce soudily s objeviteli, aby jim zveřejnění chyby nekazilo renomé. A tím se otevíral prostor pro útočníky. Takže se v bezpečnostní komunitě ustálila dohoda o zodpovědném zveřejňování chyb. U těch v počítačových programech jsou na to tři měsíce, ale v tomto případě jde o komplikovaný problém, takže firma dostala více času.

Může se to stát i jinde?
Může, protože žádný software není bezchybný. U starších čipů je problém v tom, že výrobci museli řešit kompromis mezi rychlostí, s jakou se generují, a bezpečností. My si myslíme, že u případu s čipy německé firmy to tak bylo a bohužel zvolili nevhodné řešení.

Máte informace o tom, že by toho někdo zneužil?
Nemáme, ale je jen otázka času, kdy se nějaký problém objeví, protože ne všichni si své systémy aktualizují. A útočníci s tím počítají.

Říká se, že hackeři jsou vždycky o krok napřed.
Nejde nutně o to, že by útočníci byli o hodně chytřejší, ale že obránci musejí často chránit celou populaci a to jsou většinou běžní uživatelé, kteří moc nevědí, co se v systému děje. Když jim přijde mail s nějakým odkazem, prostě na něj kliknou. Takže

my jsme obránci softwaru, kteří se vžívají do role útočníků, aby našli chyby a opravili je.

Patřím k většině, která neví, co se děje. Jak můžu zabránit tomu, aby se mi nabourali do počítače?
Jsou opatření, která odfiltrují většinu útočníků, ale stoprocentně to nikdy nejde. Ještě před deseti lety se mluvilo o tom, že si za viry mohou lidé sami, protože na ten mail kliknou. Dnes už se tento názor překlopil do roviny: nemůžeme čekat, že by někdo všemu rozuměl a systémy mají uživatele i přesto maximálně chránit. Obecně je dobré užívat zdravý selský rozum. Je potřeba ignorovat maily se žádostí o zadání hesla či pinu nebo ty, co slibují peníze zadarmo. Banky je zásadně neposílají, to už by mělo být obecně známé. Důležité je využívat nástroj pro generování a ukládání hesel, není v lidských silách si dostatečně silná hesla pamatovat. Zásadní je také mít aktualizovaný počítač včetně všech běžících programů.

Jenže spousta lidí stále jede na programy stažené načerno.
To platilo hodně v době, kdy byly programy drahé, dnes už jsou dostupné alternativy často zadarmo. A dokonce i Microsoft už přešel na to, že si koupíte operační systém jen jednou a další aktualizace a ochranné záplaty jsou zdarma.

Vždycky, když jdu do internetového bankovnictví, trochu mě mrazí. Připadám si zranitelná...
Je otázka, jak vypadá váš počítač. Jestli ho máte záplatovaný a aktualizovaný a ještě nějakou kartu či mobil, čili jiné nezávislé zařízení, kterým transakci potvrzujete, riziko je malé. Problém může nastat, když zadáváte příkazy mobilem a na to samé zařízení vám přijde potvrzující SMS. Dnes se na mobilech opakuje situace, jaká tu byla v 90. letech na pevných počítačích. Koupíte si mobil a rok dva vám budou chodit aktualizace, a pak konec. Ohrožené jsou hlavně levnější mobily, za jeden, dva ale i pět tisíc korun.

Proč bych si ale měla kupovat nový, když ten můj funguje?
Ideálním řešením by bylo, aby výrobci i pro starší telefony vydávali bezpečnostní záplaty, to se ale bohužel neděje. Pokud je telefon zranitelný, tak stačí kliknout v prohlížeči na nějakou stránku se špatným kódem a okamžitě se vám nainstaluje program, který umí nejen odposlouchávat vaše hovory, ale i třeba změnit příjemce bankovního převodu. Zvládne také stáhnout soukromé fotografie nebo údaje, kterými se lidé stanou vydíratelnými. Množí se i případy, kdy vám škodlivý program zašifruje fotky na telefonu a odblokuje je, až když pošlete peníze. Způsobů je celá řada.

Co by si na mně kdo vzal? Nejsem žádná celebrita ani nemám v mobilu nic choulostivého.
Dobré mentální cvičení je říct si: Hodím mobil do záchodu. Jak moc by mi to vadilo? A najednou zjistíte, že tam máte spoustu rodinných fotek, videí, kontaktů a dalších důležitých údajů. Pak vám dojde, že jste ochotná za ně zaplatit. Typická platba je kolem 300 dolarů, což je kolem sedmi tisíc korun.

Co ještě můžu pro svoji bezpečnost udělat?
Najít si ve svém okolí někoho, kdo počítačům rozumí. Já je taky spravuji celé rodině. Potíž je, že se většinou lidé ozvou, až když jim počítač nejede. Je potřeba chodit průběžně a nechat si poradit, který program používat, co zaktualizovat, nemít všude stejné nebo podobné heslo.

Stejné heslo? Přesně tak to ale většina lidí má, aby si ho pamatovala.
Je to častá chyba. Na internetu existuje asi tak deset služeb, které lidé používají nejčastěji. A když máte na všech stejné heslo, stačí útočníkům, když „heknou“ jednu z nich, stáhnou si hesla, a pak se dostanou, kam chtějí.

Ale jak si ta všechna hesla a piny zapamatovat? Počítám, že napsat si je na papír také není zrovna nejbezpečnější...
Je jen málo lidí, kteří by vám vlezli do šuplíku a hledali tam hesla. Daleko nebezpečnější je uhodnutelné či stejné heslo. Heslo má být dlouhé a nezapamatovatelné. Existuje program na uchovávání hesel, kterému se říká password manager. Nebo si to opravdu pište na ten papír. A ještě lepší varianta je hardwarový klíč, tzv. FIDO U2F token, jímž si doplníte heslo, které znáte. Vypadá podobně jako flash disk, zasouvá se do portu USB a provede autentizaci za vás po stisknutí tlačítka. Snadno se používá a výrazně zvyšuje bezpečnost hesla. Nejsou příliš drahé, nejlevnější verze stojí kolem 18 dolarů, tedy necelé čtyři stovky korun. Já osobně je letos budu dávat rodině k Vánocům.

Autor: Milada Prokopová

Zdroj: https://brno.idnes.cz/petr-svenda-cipy-bezpecnost-it-systemu-viry-pocitace-mobily-p5c-/brno-zpravy.aspx?c=A171120_365414_brno-zpravy_dh