Objev zranitelných čipů zbořil systém elektronických podpisů několika zemí

věda & výzkum

7. prosince 2017

Martina Fojtů

Foto: Martin Kopáček

Petr Švenda z Laboratoře bezpečnosti a aplikované kryptografie na Fakultě informatiky MU.

Informatici přišli s objevem už na začátku roku a řešili ho v první řadě s výrobcem čipů. Až po dohodě s ním publikovali informace o problému a také nástroj pro hledání zranitelných klíčů.

Velký ohlas mezi laickou i odbornou veřejností vzbudila práce informatiků Masarykovy univerzity, kteří našli zranitelnost v bezpečnostních čipech německé firmy Infineon Technologies. Ukázalo se, že vada je ještě rozšířenější a čipy jednodušeji napadnutelné, než se původně soudilo. Také díky velkému společenskému dopadu dostal tým z Laboratoře bezpečnosti a aplikované kryptografie cenu na **prestižní konferenci ACM Conference**

on Computer and Communications Security v Dallasu, kam je úspěch se už jen nominovat.
Ocenění se informatikům dostalo v kategorii zohledňující dopad na reálný svět. „Organizátoři tak vyzvedli, že se daly výsledky našeho výzkumu ihned použít pro zlepšení bezpečnosti citlivých systémů, jako jsou například občanské průkazy nebo ochrana dat na šifrovaných discích," uvedl Petr Švenda, jeden z členů týmu, podle něhož je to dobrá zpráva hlavně pro navazování nových pracovních kontaktů.
Informatici přišli při výzkumu bezpečnostních čipů na to, že u výrobku zmíněné firmy je problematický způsob, jakým se generují bezpečnostní klíče. Z veřejné části totiž lze získat jeho tajnou část. Velké problémy to znamenalo třeba pro Slovensko, protože právě tento čip používá místní státní správa pro autentizaci a v občanských průkazech. Ministr vnitra Robert Kaliňák problém nejdřív bagatelizoval, později ho ale musel přiznat.

Totéž se stalo i v Estonsku a nečekaně také ve Španělsku, kde se po rozšíření informací o problému rovněž přišlo na to, že jsou místní občanské průkazy osazené stejným čipem. „Navíc je jich tam zřejmě přes deset milionů, tedy řádově víc než v Estonsku a na Slovensku dohromady," podotknul Švenda.

Informatici přišli s objevem už na začátku roku a řešili ho v první řadě s výrobcem čipů. Až po dohodě s ním publikovali informace o problému a také nástroj pro hledání zranitelných klíčů. Přišlo se tak na to, že zranitelné už jsou čipy nejméně od roku 2007, tedy o pět let starší, než se původně myslelo.

Celosvětový dopad

Masivní dopad objevu ilustruje nejen ocenění na konferenci, ale také pozornost médií, která se tématu věnovala. Článek o něm vydala agentura Reutersa magazín Forbes chybu vyhodnotil dokonce jako horší než je nedávno objevená zranitelnost wi-fi. Kvůli velkému dopadu bylo téma zranitelných čipů několik týdnů tím nejžádanějším také mezi slovenskými médii.
Na objev hned navázali další odborníci v IT sektoru. „Příjemně nás překvapila open-source komunita, která náš detekční nástroj začala živě rozvíjet a integrovat do používaných bezpečnostních nástrojů tak, aby se již zranitelné klíče dále nešířily," popsal Švenda a jako příklad uvedl certifikační autoritu Let's Encrypt, která zranitelné klíče automaticky odmítá.

Jiné překvapení na brněnské odborníky čekalo, když začali jejich práci rozvíjet zahraniční kolegové. „Už během prvního týdne po oznámení problému a ještě před zveřejněním našeho článku se všemi detaily, dokázali Tanja Lange a Daniel J. Bernstein nezávisle na sobě i na nás nejen zjistit

tvar zranitelných klíčů, ale i navrhnout a implementovat útok, který je dokonce o něco rychlejší než ten náš," vypíchnul Švenda.

Sám bere celou kauzu jako příležitost, jak bezpečnostní systémy vylepšit.