https://www.online.muni.cz/veda-a-vyzkum/9794-informatici-muni-nasli-zavaznou-slabinu-v-bezpecnostnich-cipech

Informatici Muni našli závažnou slabinu v bezpečnostních čipech

Věda & výzkum

19. října 2017

Martina Fojtů

Foto: Martin Kopáček /

Experti z Fakulty informatiky MU v čele s Petrem Švendou přišli na chybu náhodou. Zkoumali totiž kryptografické klíče generované z velkého množství různých knihoven v čipech a sledovali, jaké mají vlastnosti.

Zranitelné čipy jsou zabudované například v moderních elektronických občanských průkazech.

Slabé místo, které může ohrozit funkčnost bezpečnostních čipů, našli při výzkumu informatici Masarykovy univerzity. Čipy používané jako ochrana u zvlášť citlivých zařízení a dokumentů či v dokladech totožnosti vyrábí jeden ze tří největších výrobců na světě, německá společnost Infineon Technologies. Informatici jí o problému dali vědět už krátce po objevu před osmi měsíci. Zranitelná část systému už by měla být v nově vydaných čipech ošetřená. Problémem zůstávají dříve vydané čipy. Výzkumníci alespoň vydali nástroj pro jejich včasnou detekci.

Experti z fakulty informatiky přišli na chybu náhodou. Zkoumali totiž kryptografické klíče generované z velkého množství různých knihoven v čipech a sledovali, jaké mají vlastnosti. „Přitom jsme přišli na to, že způsob, jakým se generují klíče u výrobku zmíněné firmy, je problematický. Z veřejné části klíče lze získat jeho tajnou část výrazně rychleji, než by to mělo být možné," přiblížil Petr Švenda, vedoucí výzkumný skupiny z Laboratoře bezpečnosti a aplikované kryptografie (CRoCS).

Její členové ihned po nalezení zranitelnosti informovali výrobce, který následně kontaktoval odběratele produktu a začal s nimi problém řešit. Zranitelnost se týká celé produktové řady a výrobků, které společnost prodávala už minimálně před pěti lety. Vada se tak dotýká velkého množství uživatelů, protože obdobných čipů se po světě prodají miliardy ročně, i když ne všechny jsou postižené.

Hrnhast

Zranitelné čipy jsou zabudované například v moderních elektronických občanských průkazech. Ačkoliv prolomení ochrany u nejčastěji používané délky klíčů vyžaduje relativně velkou finanční investici, závažnou situaci teď horečně řeší slovenské ministerstvo vnitra. Právě slovenské občanské průkazy konkrétně tyto problematické čipy mají.

„Kompletně vyřešeno to ještě není, taková zranitelnost se odstraňuje jenom složitě. Příslušné firmy už vydaly aktualizace pro oblasti, kde je to možné. V ostatních případech je ale nutné přejít na jiný algoritmus nebo v krajním případě přistoupit ke stažení dotčených čipů," uvedl Švenda a doplnil, že českých dokladů se chyba zřejmě netýká, neboť používají kombinaci čipu a knihovny jiného výrobce.