Objev roku: Vadné čipy způsobily poprask

Jen málokterý objev vědců Muni vyvolá takový rozruch a má takový dopad na společnost jako ten, který se loni povedl na fakultě informatiky. Tým z Centra výzkumu v kryptografii a bezpečnosti upozornil na zranitelnost čipů, které jsou například v zahraničních občanských průkazech. Cena rektora za významný tvůrčí počin tak měla jasného vítěze.

Foto: Jitka Janů

Když se loni v říjnu objevila na veřejnosti zpráva, že je možné u čipů německé firmy Infineon Technologies používaných u zvlášť citlivých zařízení a dokumentů či v dokladech vysledovat proces, jakým se u nich generují kryptografické klíče, byla to rána už spíš pro veřejnost než pro jejich producenta. Ten o tom dávno věděl.

„Na zranitelnost jsme přišli už v lednu loňského roku a ihned jsme upozornili výrobce, aby sjednal nápravu. Standardně se dává čas tři měsíce, než se informace zveřejní, v tomto případě to bylo ale až osm, protože šlo o hardwarovou chybu, která se hůř odstraňuje," popsal Petr Švenda, jeden ze skupiny objevitelů.

Zároveň s tím výzkumníci kontaktovali i univerzitní právníky. „Byla to taková naše pojistka kdyby náhodou. Dnes už jsou firmy většinou velice poctivé, když někdo najde takovou chybu, je to pro ně přece jen pomoc, ale v minulosti se stalo, že firma šla proti univerzitě, aby se výsledky nepublikovaly. Proto jsme byli opatrní," doplnil Švendu kolega Václav Matyáš.

Informatici na problém přicházeli postupně. Už v roce 2016 publikovali článek, ve kterém ukázali, že jsou schopni rozlišovat kryptografické klíče mezi sebou, což byl výsledek cenný hlavně v odborné komunitě. Přišli tak na metodologii, která později umožnila ještě konkrétnější objev. Už s tím prvním se ale badatelé dostali na důležitou oborovou konferenci. „Za čtyřicet let existence oboru na takovém typu konference uspělo pět příspěvků z Česka a Československa, přičemž tři z nich byly naše," podotknul Matyáš.

Následný objev, na který přišli výzkumníci loni v lednu, už byl praktičtější a ukázal na konkrétní problém. Jak dával výrobce postupně

Sekeru, kterou mají informatici na fotce, dostali jako vtipný dárek za pomoc s řešením problému s čipy od slovenského ministerstva vnitra.

vědět všem odběratelům svých čipů, ukazovalo se víc a víc, že se týká masivního množství lidí a zařízení. Problematické čipy byly například ve slovenských, estonských a španělských občanských průkazech. Nepoužívaly se v platebních kartách, jak se na začátku spekulovalo, banky je měly ale také v identifikačních kartách, jimiž se prokazují zaměstnanci.

Jakmile se zjistilo, kde všude se čipy nacházejí, stal se z laboratorního výsledku tak trochu i politický problém. Napadnutelné čipy znamenají potenciální zneužitelnost identit vlastníků občanských průkazů a to je pro každý stát bolavá záležitost. Z pohledu objevitelů tak bylo zajímavé sledovat, jak se kdo k takové komplikaci staví.

Estonci zareagovali velice rychle. Podle mínění obou odborníků proto, že jsou v oblasti kybernetické bezpečnosti obecně lídry, kteří se snaží systémy pořád zlepšovat. Na Slovensku se problém nejdřív trochu bagatelizoval, ale i tam musely nakonec vláda a příslušné úřady reagovat. Řešení nakonec našly oba státy, byť každý jiné.

„Estonci teď používají jiný způsob, jak generovat a používat bezpečnostní klíče. Slováci používají tytéž klíče, ale delší, vůči kterým teď útok prakticky není proveditelný," popsal Švenda s doplňkem, že na slovenské straně je to spíš dočasné řešení, které ovšem dává smysl. Kdyby mohli, přikročili by k němu nejspíš i Estonci, jenže jejich karty možnost využití delších klíčů nepodporovaly.

Estonci se do problematiky ponořili víc. Aby ukázali, jak velký problém je, provedli pracovníci vládní agentury pro informatickou bezpečnost (RIA) dopředu ohlášený útok na elektronickou identitu jednoho z hlavních vývojářů elektronických občanských průkazů. Nezveřejnili jeho přesné detaily, ale chtěli tím ukázat, že za cenu několika tisíc eur je opravdu možné efektivně zaútočit na kohokoliv.

V květnu navíc Estonci pořádají i konferenci, kde se bude mluvit o tom, co všechno zemi objev zranitelnosti dal a na co je nutné se do budoucna zaměřit. Na akci míří samozřejmě i členové týmu z fakulty informatiky. Kromě věhlasu ve světě kybernetické bezpečnosti jim objev přihrál i řadu nových akademických spoluprací.

Martina Fojtů

Česká archeologie by měla být za hranicemi víc vidět

Propojovat českou archeologii s tou zahraniční pomáhá svojí prací archeolog Jan Kolář, který letos dostal cenu rektora za mimořádné výzkumné výsledky pro mladé vědce do 35 let. Podílel se totiž na startovacím ERC grantu a daří se mu prosazovat v cizojazyčných časopisech a na konferencích.

Před pár týdny se vrátil z Fulbrightova programu na Pensylvánské univerzitě a za pár dní se chystá pro změnu do Španělska. „Obecně se cítím lépe v kolektivech, které jsou heterogenní a mluví se v nich více jazyky. Potkávají se v nich lidé s různými zkušenostmi, což se u nás v Česku pořád ještě moc neděje. Proto potřebuju každou chvíli někam vyjet," říká s úsměvem Kolář, který je zároveň zaměstnaný na Filozofické fakultě MU a v Botanickém ústavu Akademie věd ČR.

Právě tam spolupracoval na startovacím ERC grantu, projektu, jakých je v Česku pořád jen málo. Kolář fungoval jako člen týmu, který tvořili historici, archeologové, vegetační ekologové a paleoekologové. Společně vytvářeli model vývoje středoevropských lesů za posledních deset tisíc let a konkrétně Kolář budoval archeologický soubor dat, který k tomu byl použit. Obecně ho nejvíc zajímá třetí tisíciletí před Kristem a hlavně vztah lidských společností a prostředí, v němž společnosti žily a žijí.

„Ve střední Evropě je zakořeněná tradice, že se zaměřujeme na studium nalezených artefaktů nebo popis archeologických situací. Výstupy pak vypadají jako výstavy nálezů a i odborné články jsou tak koncipovány. Když se ale člověk zabývá vztahem společnosti a jejího životního prostředí v minulosti, můžeme z toho vyvodit hodně pro náš dnešní život a poučit se třeba v tom, jak se svým okolím a přírodními zdroji lépe interagovat," vysvětluje Kolář svůj po-

Jan Kolář se dobře cítí v mezinárodních týmech, které jsou heterogenní. Proto také často a rád vyjíždí do zahraničí.

hled na věc s tím, že celá věda je pak podle něj přínosnější.

Mimo jiné to byl důvod, proč vyrazil na Pensylvánskou univerzitu. Americká tradice je totiž taková, že archeologie je součástí antropologie, která do sebe natahuje i další v Česku odděleně fungující disciplíny, takže vědecké výsledky jsou pak komplexnější a mají větší relevanci.

Právě absence relevance je podle Koláře jeden z důvodů, proč nejsou čeští archeologové v zahraničních vědeckých časopisech tolik vidět. Historicky i v současnosti se prosazují v souvislosti s velkými objevy v Pavlově a Dolních Věstonicích, protože archeologie paleolitu funguje už od počátku mezinárodně. Archeologům zkoumajícím pozdější období se už ale do mezinárodního prostředí nedaří dostat tak často.

Martina Fojtů