MAGAZÍN
MU
LEDEN 2022

Filozofickou fakultu nově povede žena. Irena Radová

Mladý lékař pořídil snímky z mikrosvěta
strana **8**

Farmaceut si užil stáž v Kanadě
strana **22**

Dva studenti MU míří na olympiádu
strana **28**

Kryptografie: místo pro základní a aplikovaný výzkum

Pro doktorské studium si zvolil Centre for Research on Cryptography and Security na Fakultě informatiky MU. Ve volnu hledá VLADIMÍR SEDLÁČEK způsoby, jak lidi nadchnout pro matematický styl myšlení.

TEXT: MARTA VRLOVÁ
FOTO: ARCHIV V. SEDLÁČKA

Jak byste vysvětlil, co je kryptografie?
Kryptografie je věda, nebo dokonce umění, zabývající se bezpečnou komunikací v situacích, kdy předpokládáme přítomnost nepřátelské strany. Je to relativně malá část bezpečnosti, ale velmi důležitá. Systém je samozřejmě třeba dobře nastavit jako celek, protože kryptografie nás nezachrání před všemi hrozbami, ale je takovou poslední linií obrany. Proto chceme, aby byla hodně silná. Praktické využití v dnešní době nacházíme u šifrování dat při komunikaci nebo při využívání elektronických podpisů.

Může běžný uživatel dnešních technologií zabránit úniku svých dat?
Každý útok je prakticky jen otázkou ceny, tedy absolutní garance neexistuje. Můžeme ale zvýšit lafku tak, abychom nebyli výhodným cílem. Dobrým základem je zřízení správce hesel, který umožní mít pro každý účet silné a unikátní heslo. Další obranou je vícefaktorová autentizace, poskytující přístup jen tomu, kdo má kontrolu nad všemi faktory. Jednoduchou formou jsou mobilní aplikace generující jednorázové kódy. Jen pozor na SMS. Šikovný útočník je teoreticky může odchytit na cestě od operátora. A taky pomáhá lidem na potkání nesdělovat citlivé údaje, jakkoli nevinně se můžou ptát.

Co vás jako teoretického matematika přivedlo k informatice?
Vždy mě bavila teorie a abstrakce, naopak o praktické aplikace jsem se skoro nezajímal. Postupem času mi ale přišlo důležité pracovat na něčem, co má potenciál pomoci lidem ještě za mého života. Kryptografie byla dobrým kompromisem, protože využívá krásnou algebru a teorii čísel a zároveň má velký dopad na reálný svět. Našel jsem tak ideální místo na pomezí základního a aplikovaného výzkumu.

Proč jste si vybral fakultu informatiky?
Na FI jsem vždycky oceňoval podporu zapojení studentů do výuky, výzkumu v laboratořích a dalších aktivit. Sám jsem s FI začal spolupracovat díky studentskému Spolku přátel severské zvěře už jako student matematiky na Přírodovědecké fakultě MU. Také kladně hodnotím spolupráci s průmyslovými partnery a zahraničními institucemi, která umožňuje si z každé oblasti brát to nejlepší.

Čím konkrétně jste se zabýval?
Z mnoha různých úhlů jsem zkoumal kryptografii eliptických křivek, objektů s bohatou algebraickou i geometrickou strukturou, které se dnes hojně využívají. Studoval jsem, kdy může být křivka méně bezpečná, než se na první pohled jeví, a zda je do ní možné takovou zranitelnost záměrně ukrýt. S kolegy jsme mimo jiné vytvořili volně přístupný projekt DiSSECT, který komukoli umožňuje snadno prozkoumávat křivky standardizované různými organizacemi. Také jsem se snažil napadat existující systémy, protože eliptické křivky jsou velmi obtížná oblast na bezchybné naprogramování. Abychom mohli vytvořit solidní obranu, je důležité zahrát si na útočníka a upozorňovat komunitu na možné problémy.

Přibližte nám prosím, co byl útok Minerva?
Jednalo se právě o jeden z útoků, které se nám s kolegy podařilo najít. Kolega Ján Jančár, který se věnuje útokům skrze postranní kanály, v roce 2019 prozkoumával různé kryptografické knihovny a čipové karty, které eliptické křivky využívaly. Všiml si, že u některých implementací doba vzniku digitálního podpisu prozrazuje velikost pomocné hodnoty, takzvané nonce, kterou podepisovací algoritmus využívá. To sice vypadá jako poměrně neškodná informace, ale skrze mřížkové techniky jsme tyto dílky informací poskládali dohromady a po pozorování několika set až jednotek tisíc podpisů jsme byli schopni do pár minut nalézt soukromý klíč. To je sen každého útočníka, protože pak v praxi může zfalšovat podpis jakéhokoliv dokumentu. Náš útok nebyl úplně nový, pár podobných variant už existovalo. Proto jsme provedli rozsáhlé experimenty na porovnání jejich efektivity a přidali jsme několik vlastních vylepšených verzí. Za tento systematický přehled jsme na konferenci CHES 2020 získali Best Paper Award.

POPULARIZACE JE SKVĚLÝ ZPŮSOB, JAK KOMUNIKOVAT DŮLEŽITÉ MYŠLENKY NAPŘÍČ VŠEMI OBORY.

Vědou se zabýváte i ve svém volném čase. Co vás motivovalo k popularizaci vědy skrze účast na Science Slamu a ve Fame Lab?
Snažím se hledat způsoby, jak lidi nadchnout pro matematický styl myšlení. Dlouhodobě organizuji hravé soutěže a soustředění pro středoškoláky a v poslední době se snažím mířit i na širší veřejnost. Proto experimentuji s novými formami jako Fame Lab nebo Science Slam a objevuji, co je přínosné, co zábavné a co škáluje. S kamarádem jsme založili podcast Místo problémů, který je mým srdečním projektem. Věřím, že popularizace je mimo jiné skvělý způsob, jak si utřídit myšlení, zbourat sociální bariéry a naučit se lépe komunikovat důležité myšlenky napříč obory.

Nedávno jste na FI MU odevzdal disertaci, kam směřujete dál?
Právě jsem nastoupil na postdoc pozici ve Francii, ale ve spolupráci s FI budu rád pokračovat, pokud k tomu bude příležitost. Chci se dál věnovat výzkumu a využívat matematický pohled k řešení těžkých a důležitých problémů. Kryptografie v akademické sféře mě naplňuje a zatím plánuji tímto směrem jít dále, ale do budoucna nevylučuji ani jiné alternativy. Také chci určitě dál spojovat výzkum s jeho rozšiřováním do jiných kruhů, abych nezůstal zavřený v izolovaném světě. •

Celé znění rozhovoru, včetně odkazů na zmíněná vystoupení a projekty, najdete v Galerii absolventů FI MU na webových stránkách fakulty fi.muni.cz.