TRÉNINK BOJE PROTI HACKERŮM A UŽIVATELSKÉ ASPEKTY BEZPEČNOSTI – I TÍM SE ZABÝVAJÍ EXPERTI NA FI MUNI

Jeden z předních odborníků na bezpečnost, profesor **Václav Matyáš** z Fakulty informatiky Masarykovy univerzity (FI MUNI), nám představil aspekty kybernetické bezpečnosti, jimiž se zabývá v laboratoři CRoCS.

Profesor Václav Matyáš začínal jako expert na šifrování, postupně ale dospěl k tomu, že o bezpečnosti sebelepšího systému nakonec stejně rozhoduje především to, jestli s ním umí správně zacházet jeho uživatel. Právě to je oblast, na kterou se ve své laboratoři CRoCS (Centre for Research on Cryptography and Security) jako vedoucí výzkumné skupiny zaměřené na bezpečnost informačních technologií v posledních letech orientuje. Zároveň na fakultě usiluje o to, aby se vzdělávání studentů smysluplně provazovalo s aplikační sférou.

Když se řekne bezpečnost informačních technologií, člověk si může představit celou řadu věcí. Co je oním jádrem, kterému se ve Vaší laboratoři CRoCS věnujete?
Shrnul bych to pojmem autentizace. Buď ověřování toho, kdo je uživatel, který se chce někam dostat, nebo potvrzování, že ten, kdo vám posílá data, je skutečně ten pravý. Věnujeme se jak čistě informaticky orientovaným věcem, jako je aplikovaná kryptografie, kde hledáme slabiny různých algoritmů, tak i multidisciplinárním tématům, jako je usable security, čili uživatelsky přívětivá bezpečnost.

Co si pod tím představit?
Jsou to už desítky let, co se IT odborníci snaží vylepšovat zabezpečovací systémy, jenže problém je v tom, že sebebezpečnější systém nakonec závisí na svých uživatelích. Pokud ho neumí ovládat, tak bezpečný být nemůže. Celá zmíněná oblast výzkumu se proto orientuje na to, jak systém nastavit, aby uživatel všechno pochopil a neskončilo to kontraproduktivně.

Jak to může vypadat v praxi?
Často to znamená vyřešit otázku, jak vhodně zjednodušit ovládání. Představit si to můžete třeba přes internetový prohlížeč. Buď můžete nastavovat zabezpečení přes jednotlivé parametry, kterých jsou desítky a málokdo jim všem rozumí. Anebo něco přednastavíte a necháte uživatele, aby si vybral, jak moc chce být chráněný třeba na třístupňové škále. On si jen pohne nějakou lištou a vlastně řadě detailů nemusí skoro vůbec rozumět.

Spadá do Vaší oblasti i vyhodnocování kvality hesla?
Ano, to je podobné. Když jste dřív zadávali heslo, tak vám většina systémů pouze řekla, jestli je dobré, nebo špatné. Dneska už máte v systémech různé barometry, které vám ukážou, často za pomocí barevné signalizace, zda je heslo slabé, středně silné nebo super bezpečné. To všechno je důsledek toho, že se odborníci začali zabývat bezpečností z pohledu uživatele.

To už ale asi není jen o informatice…
Ano, hodně intenzivně proto spolupracujeme s Fakultou sociálních studií s týmem profesora Davida Šmahela, ale také s Právnickou fakultou a s lidmi kolem docenta Radima Polčáka. Zatím se jedná přibližně o jednu pětinu objemu práce naší skupiny, ale je to pořád na vzestupu a také je tu zájem ze soukromého sektoru. Když jsme na fakultě rozbíhali možnost sponzorování doktorských studentů konkrétními firmami, tak na usable security slyšeli všichni. I lidé, co nerozumí bezpečnosti, chápou, že je to nezbytné. Když jsme teď potřebovali dodatečně sehnat stipendium pro jednoho studenta, který se bude této problematice věnovat, nebyl to vůbec problém.

STUDIUM KYBERNETICKÉ BEZPEČNOSTI NA FI MUNI? ZÁBAVA A ADRENALIN!

Kybernetickou bezpečnost lze na FI MUNI studovat v navazujícím magisterském oboru Bezpečnost informačních technologií. Boj proti hackerům si studenti mohou natrénovat v unikátním Kybernetickém polygonu (KYPO).

Kybernetický polygon se skládá ze dvou částí. Zahrnuje fyzicky existující halu v budově fakulty informatiky a virtuální prostor kopírující realitu. Díky nim mohou informatici neomezeně a bez rizika zkoušet počítačové útoky hackerů.

Nabyté znalosti si mohou v praxi ověřit u více než 30 průmyslových partnerů fakulty. Mnohé z těchto firem sídlí přímo v jedné z budov v areálu fakulty. Studenti také stále častěji využívají možnost psát závěrečnou práci ve spolupráci s komerčním partnerem.

@ fi_muni, crocs_muni /FI.MUNI.cz # fimuni obory.fi.muni.cz

Prof. Václav Matyáš
Je profesorem Fakulty informatiky Masarykovy univerzity a jejím proděkanem pro vztahy s průmyslem a absolventy. Věnuje se aplikované kryptografii, bezpečnosti IT a ochraně informačního soukromí. Podílel se na výzkumu a vývoji pro akademické, průmyslové i státní instituce v České republice i v zahraničí (Velká Británie, USA, Kanada, Švýcarsko) a na vývoji Společných kritérií a norem ISO/IEC.

Jedním z velkých témat Vaší laboratoře byvaly platební karty a jejich zabezpečení. Proč už to neděláte?
Když se něco stane komoditní technologií a není v té oblasti nic vědecky zajímavého v horizontu několika let, nemá to pro nás příliš smysl. Jakmile si uvědomíme, že saháme na věc, kterou už si bere trh a řeší to řada konzultantských firem, tak mi instinkt říká, že je čas se posunout dál. Tak to bylo i s těmi kartami. Nebyla tam pro nás už žádná výzva. Hodně nás to ale posunulo. Už před těmi deseti lety jsme se dotkli toho, jak uživatel zachází s bezpečností, což je dnes jedno z klíčových témat naší laboratoře.

Co je pro Vás hlavní motivací, proč se zabývat bezpečností?
Poznat, co se dělá na informačních technologiích špatně a jak se to dá zneužít, a pak nacházet řešení, jak to udělat lépe a minimalizovat možnost zneužití. To je hlavní důvod, proč o tom vykládáme studentům a proč to zkoumáme.

Není problém s tím, že vlastně učíte i jak útočit?
Ještě před 20 lety s tím problémy bývaly. Ale dnes už všichni chápou, že abyste se mohl účinně bránit, musíte jednoduše vědět, jak přemýšlí útočník.

Vlastně si musíte hrát na hackera…
To je naprosto přirozené. Pro mě osobně je na bezpečnosti právě to nejzajímavější, že člověk musí umět přepínat mezi dvěma polohami. Jednak musím přemýšlet o tom, co je na systému špatného a jak se do něj dostat. A jednak zvažovat dostupné zdroje a uživatelskou praxi a v tomto kontextu hledat, jak vše udělat lepší. Bezpečnost totiž typicky není o tom, že bychom realizovali neprůstřelné řešení. Spíš jen zvýšíme bariéru útočníkovi. Samozřejmě můžete udělat totálně neprůstřelný systém, jenže ten je pak nepoužitelný pro uživatele.

> „SAMOZŘEJMĚ MŮŽETE UDĚLAT TOTÁLNĚ NEPRŮSTŘELNÝ SYSTÉM, JENŽE TEN JE PAK NEPOUŽITELNÝ PRO UŽIVATELE.“

Existuje čistě teoreticky možnost, jak něco zašifrovat nebo jinak zabezpečit tak, aby to bylo z principiálního hlediska nepřekonatelné?
Možné to je, ale jen pro velice malé komponenty systému. Můžete udělat algoritmus, který je prokazatelně bezpečný. Už teď teoreticky umíme věci, o kterých víme, že je nespočítají ani kvantové počítače. Jenže vám do toho vždycky vstoupí lidský faktor. Ten algoritmus musí někdo naprogramovat. I když ho naprogramuje výborně, pak ho musí někdo nainstalovat. A když ho nainstaluje bez chyby, tak ještě přichází uživatel. Takhle vznikají chyby a díry pro útočníky.

Takže se znovu dostáváme k usable security…
Přesně tak. I já jsem začínal s kryptografií a zajímaly mě spíš technické aspekty. Ale pak jsem čím dál tím víc zjišťoval, že systém můžeme sebelíp naprogramovat, ale když to uživatel použije jinak, než jak jsme zamýšleli, je to vlastně k ničemu. To platí v IT obecně, že často programátor něco nějak myslí, ale nedovede se na to podívat okem uživatele.

Jak si představit typickou bezpečnostní hrozbu. Je to hacker?
Hackeři napadající systém zvenku jsou jednotky procent bezpečnostních incidentů, to je jen špička ledovce. Drtivá většina problémů je způsobená tím, že se počítačové technologie používají nevhodným způsobem. Další významný faktor je zneužití informačních technologií současnými nebo bývalými uživateli. Typicky jsou to někdejší zaměstnanci, kteří se mstí, nebo současní zaměstnanci, kteří jsou nespokojení. Třeba jsou mizerně placení, ale starají se o informační systém, který je životně důležitý nebo obsahuje citlivé údaje.

Když ale čtete o tom, že nějaký server čelí stovkám útoků denně, kdo to dělá? Vypuštění roboti?
Velmi často. Otázka je, zda to můžeme považovat za opravdový útok. Typická je situace, kdy si dítě stáhne software, který spustí, a on pak zkouší náhodné útoky po síti. Takové věci nejsou moc nebezpečné, protože zpravidla bezpečnostní komunita ví, o co jde, a základním nastavením svých systémů se proti tomu umí rutinně bránit. Formálně to sice útok je, ale asi tak významný, jako když vám někdo začne ze stříkací pistole střílet na auto se zavřenými okny.

To bylo hezké přirovnání na závěr ☺
Děkujeme za rozhovor. ▣