Bezpečnost systému závisí na uživatelské přívětivosti

věda & výzkum 1. května 2016 | David Povolný

Foto: Ondrej Surý

To, jak uživatel zachází s bezpečností, je dnes jedno z klíčových témat naší laboratoře, říká bezpečnostní expert Václav Matyáš.

Programátor často něco nějak myslí, ale nedovede se na to podívat okem uživatele.

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 jako vedoucí výzkumné skupiny zaměřené na bezpečnost informačních technologií, v posledních letech orientuje. Zároveň na **Fakultě informatiky MU** usiluje o to, aby se vzdělávání studentů smysluplně provazovalo s aplikační sférou.

pozvánky >>

Pondělí 5. 9. Týden pohybových aktivit a zdraví pro zaměstnance MU

Čtvrtek 8. 9. Odborná konference Novela zákona o vysokých školách

Pátek 9. 9. Výstava kaktusů a jiných sukulentů

Pondělí 19. 9. Začátek nového semestru

Středa 21. 9. Zahájení akademického roku 2016/2017

Newsletter: Zůstaňte v obraze

Bioskop vědecké výukové centrum MU

Virtuální prohlídky vědeckých pracovišť MU

nenechte si ujít

Když se řekne bezpečnost informačních technologií, člověk si může představit celou řadu věcí. Co je jádro toho, čemu se ve vaší laboratoři CRoCS věnujete?

Shrnul bych to pojmem autentizace. Ověřování buď 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 dost multidisciplinárním věcem, 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 výzkum 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.

Nadání dětí není za trest. Psychologové ukazují, jak s nimi pracovat

Badatelna – 23. díl: Jak si zahrát flétnou na plamenomet

Turecký student Muni: Erdoganův režim o demokracii nestojí

Spadá tam i vyhodnocování kvality hesla?
Ano, to je podobné. Když jste dřív zadával heslo, tak vám většina systémů řekla jen, jestli je dobré, nebo z nějakého důvodu špatné. Dneska už máte v systémech různé barometry, které vám ukážou i s pomocí barevné signalizace, jestli je heslo slabé, středně silné nebo úplně super bezpečné. To všechno je důsledek toho, že se odborníci začali zabývat bezpečností z pohledu uživatele.

To už ale asi není jen o informatice...
Hodně intenzivně proto spolupracujeme s **fakultou sociálních studií** s týmem **Davida Šmahela**, ale taky s **právnickou fakultou** a s lidmi kolem **Radima Polčáka**. Zatím je to tak pětina objemu práce naší skupiny, ale je to pořád na vzestupu a taky je tu zájem ze soukromého sektoru. Když jsme na fakultě rozbíhali možnost sponzorování doktorských studentů konkrétními firmami, tak na usable security všichni slyšeli. I lidi, co nerozumí bezpečnosti, chápou, že je to potřebné. Když jsme teď potřebovali dodatečně sehnat stipendium pro jednoho studenta, který se tomu bude věnovat, nebyl to vůbec problém. Spíš bylo zájemců o sponzoring moc.

Jedním z velkých témat vaší laboratoře bývaly platební karty a jejich zabezpečení. Proč už to neděláte?
Jakmile se něco stane komoditní technologií a není v té oblasti nic vědecky zajímavého v horizontu několika let, tak to pro nás nemá moc smysl. Prostě 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 tehdy před těmi deseti lety jsme se dotkli toho, jak uživatel zachází s bezpečností, což je dnes jedno z klíčových témat naší laboratoře.

Co je hlavní motivace, proč se zabývat bezpečností? Je to obrana?
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.

Nenapadá někdo, že vlastně učíte i jak útočit?
Ještě před 20 lety s tím problémy bývaly. Ale dnes už všichni rozumí tomu, že abyste se mohl účinně bránit, musíte prostě vědět, jak přemýšlí útočník.

Vlastně si musíte hrát na hackera.
To je naprosto přirozené. I dobrý policista se musí naučit finty zlodějů, aby mohl být o krok před nimi. 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. Vy samozřejmě můžete udělat totálně neprůstřelný systém, jenže on je pak nepoužitelný pro uživatele.

Existuje čistě teoreticky možnost, jak něco zašifrovat nebo jinak zabezpečit tak, že je to 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 zase 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 to 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. Ajťáci pak nadávají a existuje na to i spousta vtipů, jak jsou ti uživatelé hloupí – „problém“ ale je, že se to prostě dělá pro ně. Oni jsou ti, kteří to potřebují používat a kteří za to platí.

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. Lidi si to prostě udělají sami. 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? To jsou vypuštění roboti?

Velmi často. Otázka je, jestli to můžete považovat za opravdový útok. Typicky je to tak, že nějaké děcko si 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.

Normální člověk má zavřená okna...

Když na vás bude najednou stříkat milion vodních pistolek, tak vám to auto asi i zastaví, ale šance, že se to stane, je malá. Jiná věc je, když je takový software vymyšlený někým tak, aby napadal jedno místo na síti. To se pak ty děti ale stávají nástrojem někoho dalšího s jasným záměrem.

Už jste zmiňoval, že někteří doktorandi jsou na fakultě informatiky sponzorovaní firmami a že u tématu usable security bylo zájemců z firem dokonce víc. To zní skoro jako sci-fi. Je to běžné?

Přímé sponzorování doktorandů je na fakultě poměrně nová věc, která se týká zatím spíše jednotlivců. Dospěli jsme k tomu až po letech oťukávání s průmyslovými partnery fakulty, ale doufám, že toto se běžnou věcí stane.

Proč ty roky oťukávání?

Když firma přijde na fakultu s nějakým nápadem nebo problémem, který by bylo potřeba řešit, zpravidla je to něco v horizontu měsíců. Což je samozřejmě pochopitelné, ale pro nás to znamená, že je to využitelné jen do určité míry. Může to být něco, co zapadá do směřování doktoranda, ale dizertaci na tom nenapíše. Může to být zajímavé zpestření práce pro někoho, kdo se potřebujeme jednou týdně odreagovat u jiného tématu, než je to, kterým se primárně zabývá. Každopádně jsme se takhle naučili pracovat, a protože se to osvědčilo, časem se firmy nechaly přesvědčit, že má cenu do nějakého studenta zainvestovat i dlouhodobě. Třeba právě na čtyři roky, které trvá doktorské studium.

To je asi velký zlom.

Ohromný. Firmy tím totiž přistoupily na určité riziko. Říkají tím: My sice nevíme, co přesně budeme dělat za tři roky, ale věříme, že to, co děláte na fakultě vy, je perspektivní. Navíc první rok až dva toho studenta prakticky neuvidí, maximálně na kvartální schůzce. Můžou sice mluvit do plánu jeho studia, ale reálně uvidí nějaké hmatatelné výsledky jeho práce až třeba po dvou letech. Skvěle nám to už teď funguje s firmami Y Soft a Red Hat a další se přidávají. Na spadnutí je teď třeba Konica Minolta nebo Lexical Computing.

Zní to tak trochu jako určitá forma transferu technologií.
V podstatě ano. Představa, že bychom jako na přírodovědecké fakultě přišli na něco, co se dá zapouzdřit, patentově ochránit a pak prodat, tu není moc naplnitelná. I když se samozřejmě najdou výjimky. Stane se, že děláme na nějakém problému, který nás zajímá akademicky a pedagogicky a třeba za tři roky ho uvidíte jako produkt, ale ve většině případů neděláme věci firmě na míru. Spíš společně pracujeme na vzdělání studenta, sdílíme diplomku, firma dává fakultě nějaké peníze, případně studenta ještě zaměstnává na částečný úvazek, a v okamžiku, kdy absolvuje, může u ní plynule pokračovat třeba jako vývojář.

Prostě společně pracujete na člověku, není to tolik o společném programování.
Ne že bychom společně nedělali nějaký výzkum, ale prostě fakulta není software house. U spousty institucí a někdy i firem je bohužel vidět takové očekávání. Představují si, že by naši studenti mohli vyvíjet nejrůznější z mého pohledu triviální věci, na které vám z fleku udělá nabídku deset firem z Brna.

Možná očekávají, že se na tom studenti něco naučí.
Ano, taková spolupráce může studentovi hodně dát, ale musí se vhodně nastavit tak, aby to nebyla jen programátorská rutina. Tu si může student odbýt na praxi, ke které fakultu nepotřebuje. Nám se se **Sdružením průmyslových partnerů FI** podařilo dostat do stádia, že máme více než stovku závěrečných prací obhájených ve spolupráci se soukromými firmami, což je více než pětina všech diplomových prací na fakultě.

Jak vznikají zadání?
Téma přichází buď od nás a firmu zaujme, nebo firma přijde s problémem a společně vymyslíme, jak to přetavit v zadání diplomové práce. Student pak má dva konzultanty, jednoho technického přímo ve firmě a jednoho na fakultě, který hlídá zejména akademické standardy. Taková spolupráce studenty ohromně posouvá. Někdy končí tím, že ve firmě plynule pokračují, a někdy se stane, že student zjistí, že chce jít dál a zkusit práci zase jinde. To je taky užitečné.

Sdružení vzniklo už v roce 2007. Změnila se koncepce?

Dnes už vlastně pracujeme na čtvrté revizi, ale základní parametry jsou stejné. Zůstali jsme na třech segmentech partnerů podle míry spolupráce. Jen dřív to bylo založené víc na financích, které firma do našeho vztahu investuje. Dnes klademe větší důraz na počet úspěšně obhájených závěrečných prací. Ukázalo se totiž, že pro některé firmy nebyl problém zaplatit peníze za nejnižší stupeň partnerství, a získat tak přístup na fakultu, ale už pro ně byl problém efektivně spolupracovat s větším počtem studentů na diplomové práci. Kritéria jsme proto změnili, protože peníze pro nás nejsou to hlavní. Chceme hlavně studenty kvalitně vzdělávat, teoreticky i prakticky.

Doktorát si domlouvali po e-mailu

Václav Matyáš přišel před 20 lety na fakultu informatiky a už vychoval řadu studentů.

Univerzita hostí bezpečnostní experty. Do Brna se přesunou z Cambridge

Na akci se diskutuje o záležitostech, které se často zdají jako sci-fi, většinou se ale stanou realitou.

Bezpečnostní tým z Masarykovy univerzity odhalil hackera

Za posledních sedm napadl škodlivým softwarem nejméně 1500 počítačů. Snažil se získat přístupová hesla.

>> události
>> komentáře
>> absolventi
>> student
>> sport
>> věda & výzkum
>> téma
>> víte...?
>> podívejte se
>> kultura a společnost
>> přírodní vědy
>> zdraví a medicína
>> byznys a ekonomie
>> IT a technologie