Stačí

Před několika lety mohli počítačoví hackeři způsobit denně škody za jednu miliardu dolarů. Dnes je to podle odhadů odborníků více než čtyřicet miliard. »Jednou z možností, jak se dostat nelegálně k velkým penězům v bankách, je rozluštění kryptografické ochrany bankovních serverů.« Říká to Tomáš Rosa, jeden z našich nejlepších odborníků v oblasti ochrany dat, včetně stupně přísně tajné.

TEXT: PETR MELNIČUK ● SNÍMKY: HN – IVO GOLDBACH ● KOLÁŽ: HN ŠÁRKA KLOMÍNKOVÁ

Tomáš Rosa: najít správný klíč

Nedávno jste s dvěma kolegy publikoval alarmující informaci, že byla objevena chyba v zašifrované ochraně počítačové sítě a že mnohé systémy nejsou bezpečně chráněny proti zásahům zvenčí. Z čeho jste vycházeli?

Ze dvou mimořádně vážných argumentů: Ze šesti set náhodně vybraných českých i zahraničních počítačů nebyly imunní proti pirátským zásahům plné dvě třetiny. Naše testy prokázaly, že napadení bylo a je prakticky možné.

Jak jednoduše si můžeme představit onu zmíněnou slabinu?

Pokusím se o to příkladem. Když s někým hovoříte a chcete se něco dozvědět, používáte jazyk, slova, skládáte věty, kladete otázky. U počítačů je to stejné. Když si jeho prostřednictvím chcete koupit například knihu nebo ledničku v internetovém obchodě, váš počítač i ten na druhé straně u obchodníka, si vyměňují různá data. V jejich případě se domluva neodehrává v jazyce, ale v tzv. protokolech. My jsme přišli na to, že v jednom z nich, který má chránit vzájemnou komunikaci, je chyba a že poskytovaná ochrana tak není dostatečná. Tím pádem má útočník velkou šanci dostat se k utajovaným datům. Když je vyluští, ví, co si ten který zákazník objednával, jak platil, případně jakou použil platební kartu.

Jak se chová člověk, který chce krást zboží nebo peníze prostřednictvím počítače?

Nejprve si nahraje počítačovou komunikaci mezi zaměstnanci firmy nebo klienty a internetovými obchody či bankami. Protože jejich domluva probíhá na síti internetu, informace v ní přecházejí přes desítky počítačových uzlů. Když se chce útočník k informacím dostat, musí proniknout do jednoho z nich nebo do místa mezi nimi.

Je to technicky složité?

Není. Pokud jsou uzly spojené třeba mikrovlnnými pojítky, informace se zachytí přímo ze vzduchu. Když jsou spojeny optickým kabelem, stačí se dostat do příslušného kolektoru, kde se kabel opatrně přeruší a dá se tam odbočka. Pak už odposlouchávání nic nebrání. Hovořím o tom všem úmyslně zjednodušeně, v praxi to je složitější, možná i technicky komplikovanější. Musíme ale počítat s tím, že počítačoví piráti nejsou amatéři vybavení technikou jako studenti druhého ročníku vysoké školy, kteří si chtějí jenom vyzkoušet, jak to funguje.

Koho si máme představit v pozici profesionálního počítačového útočníka?

Především to nejsou jedinci, ale celé skupiny, které jsou součástí velkého organizovaného zločinu. Fungují naprosto racionálně jako jiné firmy. Jejich postup je přímočarý: Vyhodnotí si cenu informací, které chtějí získat, a podle toho se rozhodnou, jestli a kolik budou investovat do nákupu vysoce sofistikované techniky.

TOMÁŠ ROSA

28 let, svobodný. Vystudoval teoretickou informatiku na Katedře počítačů elektrotechnické fakulty ČVUT. Ve společnosti ICZ, a. s., pracuje jako vedoucí kryptolog na výzkumu a vývoji projektů v oblasti ochrany státního tajemství, včetně stupně přísně tajné. V rámci doktorského postgraduálního studia se intenzívně zabývá teorií tzv. postranních kanálů. Své práce přednáší na našich i zahraničních univerzitách, seminářích a konferencích.

Jak se dostanou k obsahu zašifrovaných informací, aby měly pro organizovaný zločin vůbec nějaký význam?

Tak, že podle matematického algoritmu formulují otázky, které odesílají například napadenému bankovnímu serveru. Komunikace není pro něj ničím neobvyklým, proto bez váhání odpovídá. Například: *Ano, ne, nevím.* Z jejich velkého počtu se získá dost podkladů k tomu, aby útočníci dokázali rozluštit hlavní klíč daného spojení tzv. *premastrer-secret.* Když ho mají, pak už jednoduše dešifrují všechny zachycené informace. Dozvědí se třeba jak, kdy a kolik peněz ukládali různí lidé na účet v bance, případně získají čísla platebních karet zcela neznámých lidí.

Neběhá vám z toho mráz po zádech?

Běhá, i když na druhé straně vás mohu ubezpečit, že každá počítačová ochrana je správně vázána na několik různých systémů. I když se někdo dostane k číslům účtů nebo platebních karet, nemusí se ještě dostat k převodům nebo výběrům. Pro ty potřebujete další informace například privátní klíč uložený na čipové kartě uživatele nebo serveru. U dobře navrženého systému tyto klíče nikdo nezná. Navíc, systém je většinou konstruován tak, že i kdyby někdo kupříkladu podplatil příslušného administrátora, tak on nebude schopen klíč získat, i kdyby počítač rozmontoval. V případě, že by k tomu přesto došlo, srdce systému to zaznamená a v zájmu bezpečnosti se zničí.

Kolik času je zapotřebí ke zdolání serveru?

Pro nás není určující čas, ale počet dotazů a potřebných odpovědí s napadeným systémem, při kterém musíme předstírat, že jsme jeho normální uživatelé. Pro vaši představu, je to jako kdybych zazvonil u dveří vašeho bytu a díval se, jakým způsobem mi otevíráte dveře. A pak znova, po chvilce, až je zabouchnete, bych vám zase zazvonil, a opět bych se díval, jak je otevíráte. Nepřestal bych do té doby, než bych se po nějakém počtu zazvonění nedověděl, na jakém principu fungují vaše dveřní zámky a co musím udělat zvenčí, abych se dostal dovnitř.

Kolik těch zazvonění je?

V běžném případě přibližně 14 miliónů, na které budete potřebovat přibližně 55 hodin. Útočník musí být ale opatrný. Nemůže zvonit v jednom kuse plných pětapadesát hodin, byl by nápadný. Čas musí rozprostřít do třech nebo pěti měsíců. Důvodem je jeho ukrytí, protože by mohlo být nápadné, že někdo zvoní už po pětimiliónté a nikdo za dveřmi po otevření není. Čím technicky je systém vyspělejší, tím kratší doba je nutná na vedení útoku. Kuriózní je, že napadený systém sám pracuje proti sobě tím, že mnohem rychleji odpovídá na otázky a rychleji tak pod sebou podřízne větev. Se špičkově sestaveným počítačem trvá útok kolem jedné hodiny.

Jak běžný střadatel pozná, že jeho banka je dobře střežená?

Jestli je banka seriózní po všech stránkách, to se z venčí těžko pozná. Nicméně banky by měly respektovat princip alespoň dvou a více nezávislých ochran na každém místě. To znamená, měly by předpokládat, že některá z nich může selhat a že by účty mohly být ve vážném ohrožení.

Nejsou piráti tak trochu vaši profesní kolegové?

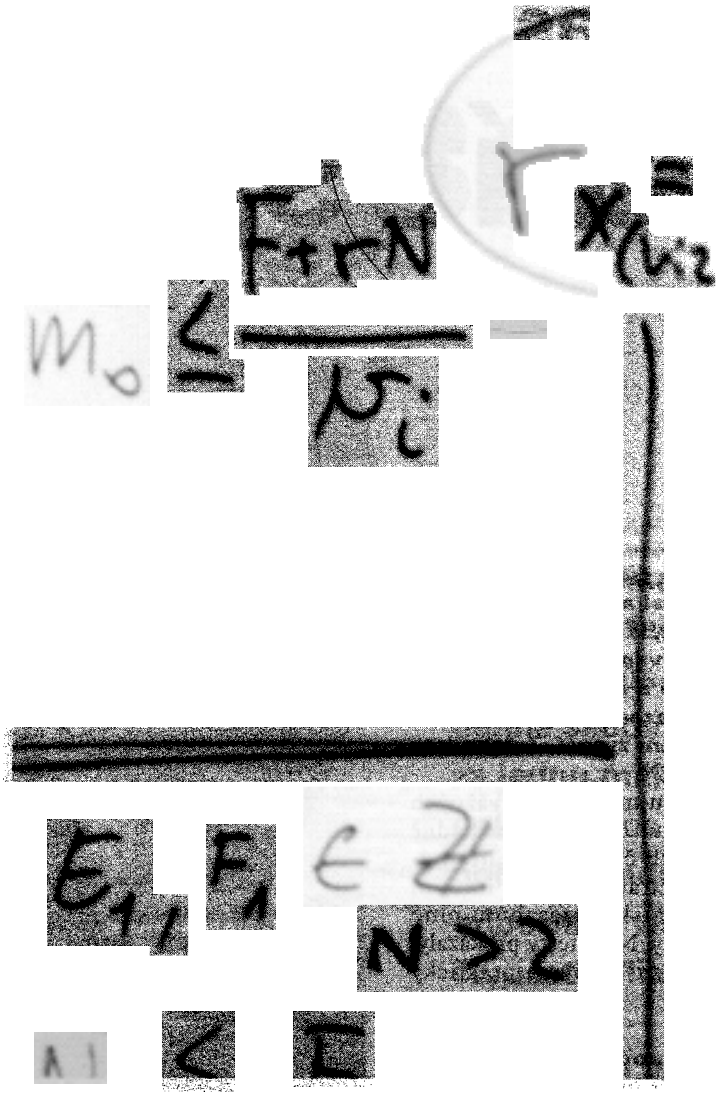
Jsou, ovšem na jiné straně zákona. Dnes je zcela zřejmé, že veškeré profese, které existují v legálních firmách, jsou duplikovány ve zločineckých organizacích. To znamená, že firma, která se rutinně zabývá prolamováním počítačových systémů, zaměstnává také špičkové kryptology.

Jsou ti, kdo prolamují ochranné kryptografické systémy počítačů, klasičtí hackeři?

Nejde o klasické hackery, kteří si zakládají na tom, že umějí využívat chyby v programech. Prolomit kryptografickou ochranu je cosi virtuóznějšího, je to počítačový majstrštych. Umí ho jen profesně skvělý kryptoanalytik, který najde například klíč k zavřeným sejfům s penězi.

Lze hledání onoho klíče považovat za určitou odnož počítačové subkultury?

Záleží na motivaci. Ve chvíli, kdy chce v elektronické síti útočník dokázat něco, co umí jen pár lidí, tam bych to považoval za velmi specifickou formu počítačové kultury. Ovšem ve chvíli, kdy jde o krádež informací, zboží nebo peněz, nejde o kulturu, ale prostý zločin.



Nejsou kryptoanalytici často o krok kupředu před profesionálními tvůrci počítačových systémů?

Až tak to nevidím. Na obou stranách jsou profesionálové. Řekl bych, že naše soupeření je vyrovnané.

Řekl jste, že když jsou ve hře cenné informace a velké peníze, organizovaný zločin nešetří na nákupech nejlepší techniky. Není v tomto směru o zmíněný krok vpředu?

Technika je samozřejmě důležitá, ale stejně tak důležité jsou schopnosti luštitelů. Tady mi nahráváte na vysvětlení, proč my, kteří navrhujeme bezpečnostní systémy, známe i pohled z druhé strany. My jsme si totiž už před lety uvědomili, že na naší straně musí bezpodmínečně existovat skupiny lidí, které provádějí analýzu systémů. V podstatě si v práci hrají na loupežníky, což je i můj případ, snaží se konstruovat všemožné scénáře, jak daná konta vykrást. Díky tomu jsou na stejné úrovni jako profesionální útočníci. Rozdíl je pouze v tom, že skuteční piráti předají svým bossům hlášení: Tato konta je možné vykrást. Naopak analytici na straně legální firmy volají: Bankovníci pozor, zabezpečte jinak klientské účty!

Jaké schopnosti vám, »šifrařům«, nesmí chybět?

Především schopnost kombinovat abstraktní matematické myšlení s realitou. Nazval bych to pragmatickou matematikou. Tuhle schopnost má jen málo

»Prolomit kryptografickou ochranu je počítačový majstrštych. Umí ho jen profesně skvělý kryptoanalytik, který najde klíč k zavřeným sejfům s penězi.«

lidí. Většinou se umějí pohybovat buď v abstraktním matematickém světě nebo v technickém světě. Často jim chybí schopnost propojit oba protipóly.

Jací jsou čeští kryptologové?

Patří k uznávané světové úrovni. Usuzujeme tak z různých pozvání na mnohé odborné konference a semináře v zahraničí i vážnosti, s kterou jsme tam přijímáni.

Čím si to vysvětlujete?

Bude se to zdát komické, ale práce kryptologa velmi těsně souvisí s naší českou, někdy až švejkovskou povahou. Když nám něco nejde, tedy když to nejde dveřmi, zkusíme to po straně nebo oknem. Podobně to dělá »počítačový luštitel«, který napadá servery tzv. postranními kanály. Navíc, Češi mají velký dar improvizace, který chybí mnohým zahraničním odborníkům.

Vyučuje se u nás kryptologie?

Ještě donedávna to bylo tak, že na různých českých univerzitách existovalo několik roztroušených předmětů, které se tu více, tu méně kryptologií zabývaly. Dnes je jiná situace, na Matematicko-fyzikální fakultě Univerzity Karlovy se zakládá obor, který se zabývá jenom kryptologií. Studenti se tam budou od prvního do posledního ročníku systematicky připravovat na úlohu kryptologa. Už dnes vím, že tam studují lidé, kteří budou za krátký čas ve světě něco znamenat.

Co jste míval z matematiky ve škole?

Pokud vím, tak na střední škole vždycky jedničku. Na vysoké pak byla paleta už pestřejší. Některé matematické předměty tam totiž nesloužily ani tak k rozšiřování znalostí, jako síto na studenty. Z běžných předmětů mi moc neseděly dějepis, zeměpis a tělocvik. A můj vztah k matematice? Nikdy bych neřekl, že mě bude živit. Situace se změnila až na vysoké škole.

Máte nějaké slabiny?

Hodně mi utíkají běžné denní věci a zvyklosti. Nevím už kolik let po sobě se učím na jaře kupovat sněženky, drobné dárky na Velikonoce nebo i tehdy, když má někdo svátek nebo narozeniny.

Je pro vás, v čase volna, těžké nemyslet na práci?

I to se učím, ale moc mi to nejde. Například nedávno mě při pěší túře na Sněžku pronásledovala velmi jednoduchá šifra používaná v počítačovém bezpečnostním modulu. Musel jsem se několikrát zastavit a zapsat si poznámky. Moje přítelkyně má naštěstí pro mě pochopení.

Neláká vás, že byste si vzal starou kamennou destičku s klínovým písmem a pomocí matematických metod se pokusil rozluštit obsah textu?

Abych byl upřímný, nikdy jsem o tom nepřemýšlel. Pokud by mě ale někdo oslovil, že potřebuje pomoct s částí matematické formulace problému a nějakým způsobem se pokusil ho řešit, tak na to bych si troufl.

Máte pro něco slabost?

Strašně rád čtu detektivky. Mými oblíbenci jsou klasické postavy detektivního žánru, jako jsou komisař Columbo, Hercule Poirot, Sherlock Holmes, Adam Dalgliesh nebo Maigret. Jejich příběhy záměrně nedočítám až do konce. Chci sám přijít na to, jak všechno dopadne, kdo je zloděj nebo vrah. Většinou se strefím. Někdy ovšem také ne, stejně jako v kryptoanalýze. Žádný luštitel na světě totiž nedokáže přijít úplně na všechno. ■