TECH

KDO BY NECHTĚL BÝT ASPOŇ NA CHVÍLI HACKEREM?

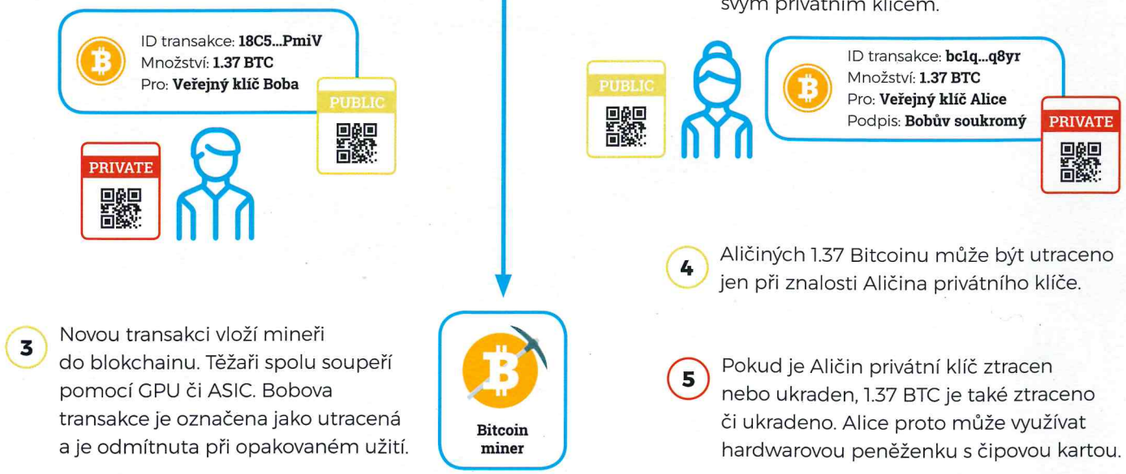
Autor: Filip Šmejkal

Petr Švenda působí jako odborný asistent a pedagog na Fakultě informatiky Masarykovy univerzity. Patří k předním expertům na kyberbezpečnost a z kryptoměn je dle svých slov přímo nadšený!

V České republice patříte k největším expertům na kybernetickou bezpečnost. Hrozí našim datům reálné nebezpečí?
Samozřejmě ano. Se vzrůstající hodnotou dat vzrůstá i zájem o jejich zneužití. Zatímco ale v běžném životě umíme nebezpečí většinou rozpoznat a nenosíme v kapse celý svůj majetek, v tom digitálním se to ještě učíme. A útočníci mívají před běžným člověkem náskok. Nemusí se ale jednat jen o krádež dat jako takových, útočník může třeba „ukrást" výpočetní čas na vašem počítači a rozesílat z něj spam nebo na něm těžit kryptoměny.

Sám se zabýváte především bezpečností čipových karet. S jakými specifiky se v tomto oboru setkáváte?
Na rozdíl od většiny jiných zařízení a jejich programů jsou kryptografické čipové karty od začátku navrženy s ohledem na vysokou bezpečnost vůči útočníkům. Včetně těch, kteří kartu drží fyzicky v ruce, zkoušejí ovlivňovat její fungování či se pomocí mikrosond snaží přečíst její paměť. Zároveň se jedná i o docela tajnůstkářský průmysl, kde není snadné získat popis jejich provedení – částečně kvůli ochraně před konkurencí a částečně z historické setrvačnosti. Tedy i nezávislé ověření jejich bezpečnosti je obtížnější a chyby mívají větší dopad.

JAK FUNGUJE PŘEVOD BITCOINU



Zdroj: Petr Švenda

Zdroj: Archiv Petra Švendy

Řeší se v současné době nějaký velký či aktuální problém/incident, který se týká kybernetické bezpečnosti?
Právě minulý rok se nám podařilo odhalit velmi závažnou zranitelnost v čipových kartách jednoho z největších výrobců – způsob, jakým generoval privátní klíče byl vadný a umožňoval útočníkům jeho hodnotu z veřejné části dopočítat. Tyto čipy se používají v elektronických občankách několika zemí včetně Slovenska, Estonska či Španělska a také třeba pro ukládání klíčů pro šifrování disku programem Microsoft Bitlocker. Ve spolupráci s výrobcem jsme pak pomáhali mapovat a řešit dopad problému, který vedl k zneplatnění desítek miliónů uživatelských certifikátů, komunikaci s bezpečnostními týmy Microsoftu, Googlu nebo třeba i GitHubu a vydání softwarových záplat od většiny výrobců notebooků.

Je na denním pořádku, že se z médií dozvídáme zprávy o vývoji kryptoměn. Považujete jejich nákup z kybernetického hlediska za bezpečný?
Nákup samotný z pohledu provedení platební transakce bezpečný být může – stačí třeba využít Bitcoin bankomat nebo běžný SEPA převod na některou ze zavedených burz kryptoměn. S udržením hodnoty takové investice je to složitější – kryptoměny mohou narůst nebo propadnout o desítky procent denně a opakovaně se to děje.

Vidíte v boomu virtuálních měn více pozitivního či negativního?
Osobně jsem z nich, nejen z pohledu učitele a výzkumníka, nadšený. Jde na nich velmi pěkně ukazovat spoustu principů z kryptografie jako například digitální podpisy na bázi eliptických křivek, hašovací funkce a hledání částečných kolizí využívaných při tzv. těžení (mining), možnosti anonymizace transakcí nebo způsoby zabezpečení privátních klíčů v peněženkách. Naši studenti si sami staví těžící „farmy" z grafických karet, píší digitální kontrakty (smart contracts) nebo analyzují historii transakcí ve veřejném blockchainu. Je v tom obrovská energie pramenící nejen z možnosti vydělat nějaké peníze, ale hlavně být součástí něčeho nového. Navíc je drtivá většina projektů kolem kryptoměn programována s otevřeným zdrojovým kódem (open-source), takže i když některé kryptoměny zaniknou, tak po nich zůstane velmi zajímavá a dále použitelná technologie.

Jakým způsobem je možné virtuální měnu zabezpečit proti hackerům?
V současné době nejlépe využíváním hardwarové peněženky, při které není privátní klíč nutný pro převod kryptoměny uložen v souboru na počítači, ale v čipové kartě s vlastním displejem, kterou je velice obtížné kompromitovat, i když útočník zcela ovládne váš počítač. Navíc lze privátní klíč rozdělit na dvě či více částí, opět pěkná ukázka konceptů z kryptografie v praxi.

Učí se v dostatečné míře čelit moderním bezpečnostním hrozbám také studenti informaticky zaměřených studijních oborů na vysokých školách?
Poptávka po absolventech v oblasti počítačové bezpečnosti je obrovská. Jen umět nainstalovat antivirus a firewall dnes už nestačí. My studenty učíme, jak nalézt stopy exfiltrace firemních dokumentů v zachyceném síťovém provozu, psát exploit na zranitelný program, a naopak se takovým chybám ve vlastním programu vyhnout nebo jak vytvořit třeba již zmiňovanou peněženku na kryptoměny.

Je vůbec z pohledu kantora možné zachytit všechny nejnovější trendy a triky v kybernetickém zločinu? Nakolik využijí Vaši studenti aktuální znalosti za několik let?
Zachytit všechny samozřejmě možné není, naším cílem je vysvětlit důležité principy, na kterých tyto triky a následná obrana proti nim stojí – a ty se mění již pomaleji. Na aktuálních způsobech provádění útoků si tyto obecnější principy studenti ale osvojují. Zcela nejdůležitější je studenty pro počítačovou bezpečnost nadchnout, což lze naštěstí většinou snadno – kdo by nechtěl být aspoň na chvíli hackerem? A díky tomuto nadšení je pak sledování novinek v oboru i po ukončení školy nejen nutností, ale i radostí.

VĚDA A VÝZKUM

KRYPTOMĚNA MĚNÍ SVĚT VĚDY

Autor: Jan Novák

Oblast kryptoměn je vysoce kompetitivní prostředí. Není velkou spekulací, že do budoucna přežijí pouze ty nejsilnější, respektive pouze ty, které nabízejí něco unikátního.

To je patrné i na žebříčku nejobchodovanějších kryptoměn, kde dominuje historicky nejstarší Bitcoin, jemuž sekunduje Ethereum s téměř geniálním způsobem provádění transakcí či kryptoměna Ripple jedinečná pro svoji centralizaci. To, čím jednotlivé kryptoměny nejsou specifické, je způsob jejich těžby. Existuje sice celá řada algoritmů, pomocí kterých těžba probíhá, samotná těžba je však početní zpracování zcela abstraktních dat. Existuje však alternativa v podobě měny Gridcoin, kde je za těžbou schováno mnohem více, než je tomu v případě jiných kryptoměn.

Těžba kryptoměn je z globálního hlediska neuvěřitelně energeticky náročná aktivita. Americký meteorolog Eric Holthaus odhaduje, že pokud nedojde ke změně provádění transakcí Bitcoinu, zkonzumuje do budoucna provoz této kryptoměny více elektrické energie než celé USA. A to již v červenci 2019! Ačkoliv lze taková prohlášení vnímat s jistou rezervou, již dnes dle analytiků ze serveru Digiconomist zkonzumuje provoz Bitcoinu více elektrické energie než země jako Maďarsko či Irsko, s tím, že tato spotřeba roste v podstatě exponenciálně. A to mluvíme pouze o jedné kryptoměně.

Unikátní je v tomto ohledu kryptoměna Grindcoin. Na první pohled se tato kryptoměna může jevit jako každá jiná. Standardní multiplatformní peněženka, transakce prováděné v peer to peer síti ukládané pomocí technologie blockchain a také trojí způsob samotnou měnu získat. Směnou za jinou měnu, potvrzováním transakcí a těžbou. A samotná těžba je to, oč tu běží.

pokračování na str. 24 >>>

Ptali jsme se akademiků

RNDr. Petr Švenda, Ph.D.,
Fakulta informatiky, Masarykova univerzita

Jaký je Váš názor na využití dobrovolnických sítí pro distribuované výpočty ve vědě, jako je například projekt BOINC?
BOINC je velmi přínosný program, a to nejen pro dobrovolnické počítání – lze jej využít na snadnou distribuci výpočetních úloh i na vlastních strojích. Velmi důležité je dobrovolníky svým projektem opravdu zaujmout, protože jich nyní mají na výběr celou řadu.

Ve kterých oblastech vědeckého výzkumu se mohou distribuované výpočty uplatňovat?
Opravdu v široké škále – tam kde potřebujete zpracovat velká data nebo provést intenzivní dlouhý výpočet. Fakt, že je výpočet distribuovaný, může mít i další výhody – nemusí být potřeba přenášet obrovská data tam, kde jsou výpočetní stroje, ale naopak přenést výpočetní program tam, kde jsou data již uložena.

Považujete za správné zkombinovat distribuované výpočty s těžbou kryptoměny, tedy odměňovat dobrovolníky za poskytnutý výpočetní výkon kryptoměnou s hypotetickou finanční hodnotou?
Spíše ne. Je potřeba dobrovolníkům jasně vysvětlit, že dostávají token se silně spekulativní hodnotou. Navíc je otázka, zda stále zůstávají dobrovolníky, když jsou určitým způsobem placeni – spíše je to využití naivity dobrovolníků a jejich víry, že časem bude hodnota Gridcoinu podobná, jako např. Bitcoinu. Opravdu zajímavé by bylo vytvořit systém, ve kterém by samotný algoritmus těžby prováděl namísto např. SHA-2 haše použitého u Bitcoinu užitečnou operaci – je ale obtížné zkombinovat potřebnou flexibilitu (jiné operace se použijí pro hledání léků a jiné při faktorizaci velkých čísel) a energetickou úspornost. To ale zmiňovaný Gridcoin nedělá.

Foto: Archiv Petra Švendy