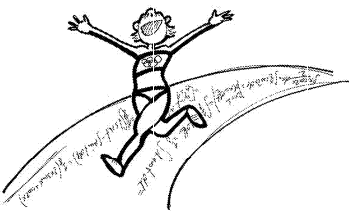
INFORMATIKA

61. ročník Matematické olympiády – 2011/2012

Úlohy domácího kola kategorie P



Úlohy P-I-1 a P-I-2 jsou praktické, vaším úkolem v nich je vytvořit a odladit efektivní program v jazyce Pascal, C nebo C++. Řešení těchto dvou úloh odevzdávejte ve formě zdrojového kódu přes webové rozhraní přístupné na stránce *http://mo.mff.cuni.cz/ /submit/*, kde také naleznete další informace. Odevzdaná řešení budou automaticky vyhodnocena pomocí připravených vstupních dat a výsledky vyhodnocení se dozvíte krátce po odevzdání. Pokud váš program nezíská plný počet bodů, můžete své řešení opravit a znovu odevzdat.

Úlohy P-I-3 a P-I-4 jsou teoretické, vaším úkolem je nalézt efektivní algoritmus řešící zadaný problém. Řešení úlohy se skládá z popisu navrženého algoritmu, zdůvodnění jeho správnosti (funkčnosti) a odhadu časové a paměťové složitosti. Součástí řešení je i zápis algoritmu ve formě zdrojového kódu nebo pseudokódu v úloze P-I-3 a výsledný zlomkový program v úloze P-I-4. Řešení těchto dvou úloh odevzdávejte ve formě souboru typu PDF přes výše uvedené webové rozhraní.

Řešení všech úloh můžete odevzdávat do 15. listopadu 2011. Opravená řešení úloh a seznam postupujících do krajského kola najdete na webových stránkách olympiády na adrese *http://mo.mff.cuni.cz/*, kde jsou také k dispozici další informace o kategorii P.

P-I-1 Bezpečná planeta

Ve vesmíru existují tři typy planet:

- *typ 0: neobyvatelné* planety, na nichž člověk okamžitě zahyne,
- *typ 1: nehostinné* planety, na nichž člověk může chvíli přežít, ale nemůže tam žít dlouhodobě,
- *typ 2: přívětivé* planety, na nichž člověk může žít dlouhodobě.

Mezi jednotlivými planetami cestujeme vesmírem pomocí *jednosměrných* teleportů.

Planetu nazveme *bezpečnou,* jestliže je přívětivá a zároveň jsou přívětivé také všechny planety, na které se z ní můžeme dostat pomocí teleportů (třeba i několika po sobě). Pokud tedy vysadíte člověka na bezpečné planetě, máte jistotu, že může spokojeně žít všude, kam z ní docestuje.

Planetu označíme jako *snesitelnou,* jestliže sice není bezpečná, ale můžeme se z ní pomocí teleportů (třeba i několika po sobě) dostat na bezpečnou planetu, aniž abychom museli cestou navštívit nějakou neobyvatelnou planetu. Pokud tedy vysadíte člověka na snesitelné planetě a dáte mu vhodné instrukce, jak má cestovat, po čase dorazí živý a zdravý na nějakou bezpečnou planetu. Všimněte si, že žádná neobyvatelná planeta nemůže být snesitelná.

Soutěžní úloha

Je dán počet planet n, počet teleportů m, pro každou planetu její typ a pro každý teleport odkud kam vede. Určete všechny bezpečné a všechny snesitelné planety.

Formát vstupu

První řádek standardního vstupu obsahuje dvě celá čísla n (počet planet) a m (počet teleportů). Všechny planety si očíslujeme od 1 do n. Druhý řádek vstupu obsahuje n mezerami oddělených celých čísel z množiny $\{0, 1, 2\}$ – postupně pro každé i je to typ planety číslo i. Zbytek vstupu tvoří m řádků, z nichž každý popisuje jeden teleport. Popis teleportu je tvořen dvěma čísly planet – odkud a kam tento teleport vede.

Ve vstupech, za které lze získat celkem 5 bodů, bude $1 \leq n \leq 500$ a $0 \leq m \leq 10\,000$.

V ostatních vstupech bude $1 \leq n \leq 100\,000$ a $0 \leq m \leq 200\,000$.

Formát výstupu

Program vypíše na standardní výstup dva řádky. První z nich začíná řetězcem „`bezpecne:`“ a za ním následuje posloupnost čísel všech bezpečných planet. Čísla planet vypište v rostoucím pořadí a před každým z nich vypište jednu mezeru. Druhý řádek výstupu začíná řetězcem „`snesitelne:`“, za kterým následuje posloupnost čísel všech snesitelných planet ve stejném formátu, jako na prvním řádku. Je-li některá z posloupností prázdná, pak bezprostředně za dvojtečkou bude následovat konec řádku.

Příklad

Vstup:	*Výstup:*

`7 8`
`2 1 2 2 2 2 0`
`1 2`
`2 3`
`3 4`
`4 5`
`5 3`
`2 6`
`6 7`
`7 6`
	`bezpecne: 3 4 5`
	`snesitelne: 1 2`

P-I-2 Naložená loď

Na planety, které ještě nemají vybudovány teleportové terminály, létají meziplanetární kosmické lodě s lidskou posádkou. A ta potřebuje jíst. Vaší úlohou bude přesně naplnit celý potravinový nákladní prostor kosmické lodě balíčky s jídlem.

Problém spočívá v tom, že balíčky s jídlem se připravují na Zemi, zatímco loď čeká na oběžné dráze. Balíčky je pak třeba dopravit ze Země na kosmickou loď. Vezme se vždy několik balíčků, naloží se do dopravní kapsle, ta se vystřelí ze Země na oběžnou dráhu a tam už si ji posádka lodě odchytí.

Existuje n typů dopravních kapslí. Kapsle i-tého typu má kapacitu přesně a_i balíčků. Nevejde se do ní více balíčků, ale zároveň jich nesmí být ani méně kvůli správnému vyvážení a doletu. Máme k dispozici dostatečné množství kapslí všech typů.

Soutěžní úloha

Napište program, který na základě zadaných typů kapslí a jejich kapacit spočítá *nejmenší možný počet* kapslí potřebný k úplnému naložení kosmické lodě. Součet kapacit použitých kapslí musí tedy být *přesně roven* kapacitě k nákladního prostoru lodě.

Formát vstupu

První řádek standardního vstupu obsahuje jedno celé číslo n – počet typů kapslí. Druhý řádek obsahuje n celých čísel $a_1, \ldots, a_n$ oddělených mezerami – kapacity kapslí jednotlivých typů. Třetí řádek obsahuje jedno celé číslo k – kapacitu nákladního prostoru lodě.

Můžete předpokládat, že $a_1 < \ldots < a_n$ a že $a_1 = 1$ (tedy vždy existuje způsob, jak lze přesně celou loď naložit).

- Ve vstupech za 3 body bude platit $n \leq 5$, $a_n \leq 2\,000$ a $k \leq 30$.
- Ve vstupech za další 4 body bude platit $n \leq 30$, $a_n \leq 2\,000$ a $k \leq 1\,000\,000$.
- Ve vstupech za zbývající 3 body bude platit $n \leq 30$, $a_n \leq 2\,000$ a $k \leq 10^{18}$.

Všimněte si, že pro uložení hodnoty k musíte použít 64-bitovou proměnnou:

`long long` v C/C++, `int64` v Pascalu.

Formát výstupu

Na první řádek standardního výstupu program vypíše nejmenší počet kapslí potřebný k přesnému naložení naší kosmické lodě.

Na druhý řádek vypíše jedno libovolné řešení, které využívá tento počet kapslí. Řádek bude obsahovat n celých čísel $b_1, \ldots, b_n$ oddělených mezerami, přičemž b_i udává počet použitých kapslí velikosti a_i.

Příklady

Vstup:	*Výstup:*

`4`
`1 10 100 1000`
`147`
	`12`
	`7 4 1 0`

Použijeme jednu kapsli s kapacitou 100, čtyři kapsle s kapacitou 10 a sedm kapslí s kapacitou 1. To je cekem $1 + 4 + 7 = 12$ kapslí.

Vstup:	*Výstup:*
3 1 8 10 16	2 0 2 0

Optimální řešení využívá dvě kapsle s kapacitou 8.

P-I-3 Skladník

Ignác byl skladníkem. Pil alkohol, sprostě nadával a v pracovní době většinou spal. Není divu, že mu šéf už dlouhá léta vyhrožoval, že ho nahradí počítačem. Až jednoho dne ta chvíle opravdu nastala. Šéf koupil počítač, posadil ho na vrátnici skladu a Ignáce propustil. Tím dosáhl přesně stejného stavu jako dosud, jenom počítači už nemusel platit žádnou mzdu.

Netrvalo dlouho a šéf si uvědomil, že počítač dokonce může zapnout a používat. Potřebuje k tomu ale od vás napsat vhodný program.

a) *(4 body)* Navrhněte co nejefektivnější algoritmus, který bude spravovat inventář skladu. Na vstup algoritmu budou přicházet informace o tom, kolik kusů jakého druhu zboží přibylo nebo ubylo. Po každém načtení nové informace musí váš algoritmus vypsat dva údaje: celkový počet kusů zboží ve skladu a počet různých druhů zboží ve skladu.

b) *(6 bodů)* Napište ještě druhý algoritmus, který bude rovněž spravovat inventář skladu. Jeho vstup bude vypadat stejně jako vstup prvního algoritmu. Po každém načtení nové informace musí tento algoritmus vypsat dva údaje: název druhu zboží, od kterého je momentálně ve skladu největší počet kusů, a tento počet kusů. Pokud existuje více takových druhů zboží, algoritmus vypíše ten z nich, jehož název je první v abecedním pořadí.

Formát vstupu

Na každém řádku vstupu je uvedeno nejprve jedno nenulové celé číslo δ_i a za ním jeden řetězec s_i tvořený nejvýše ℓ znaky anglické abecedy. Tento řádek znamená, že počet kusů zboží s_i ve skladu se změnil o δ_i.

Při návrhu algoritmů můžete předpokládat, že $\ell \leq 50$, že počet druhů zboží ve skladu nikdy nepřekročí 100 000 a že celkový počet kusů zboží ve skladu nikdy nepřekročí 10^{18}. Můžete také předpokládat, že nikdy nedostanete pokyn, který by počet kusů nějakého zboží ve skladu změnil na záporný.

Příklad

Vstup:	*Výstup pro podúlohu a:*	*Výstup pro podúlohu b:*
`+3 koberec`	`kusů: 3, typů: 1`	`koberec 3`
`+2 buldozer`	`kusů: 5, typů: 2`	`koberec 3`
`+1 buldozer`	`kusů: 6, typů: 2`	`buldozer 3`
`+7 zebrik`	`kusů: 13, typů: 3`	`zebrik 7`
`-3 buldozer`	`kusů: 10, typů: 2`	`zebrik 7`
`-5 zebrik`	`kusů: 5, typů: 2`	`koberec 3`

Hodnocení

Každá podúloha se hodnotí samostatně.

Ve svém řešení uveďte odhad, jak *nejdéle* (tj. v nejhorším možném případě) může každému z vašich programů trvat zpracování n-tého pokynu. (V tomto odhadu můžete použít proměnnou t pro aktuální počet druhů zboží ve skladu, proměnnou k pro aktuální počet kusů zboží ve skladu a proměnnou ℓ pro maximální délku názvu zboží.) Tato časová složitost bude hlavním kritériem hodnocení. Snažte se tedy, aby váš program zpracoval co nejrychleji každý pokyn zadaný na vstupu.

Připomínáme, že pokud používáte ve svém programu netriviální algoritmy nebo datové struktury (např. různé součásti STL v C++), potom váš popis algoritmu musí obsahovat také dostatečný popis jejich implementace, případně popis implementace příbuzné datové struktury se stejnou časovou složitostí operací.

P-I-4 Zlomkové programy

V letošním ročníku olympiády se budeme v každém soutěžním kole setkávat se zlomkovými programy. Ve studijním textu uvedeném za zadáním této úlohy je popsáno, jak zlomkové programy fungují.

Soutěžní úloha

a) *(5 bodů)* Na vstupu je číslo n tvaru $2^x 3^y 5$, přičemž $x, y \geq 0$. Napište zlomkový program, který ho převede na číslo 5, jestliže $x = y$, resp. na číslo 7, jestliže $x \neq y$.

b) *(5 bodů)* Na vstupu je číslo n tvaru $2^x 3$, přičemž $x \geq 0$. Napište zlomkový program, který ho převede na číslo tvaru 2^y, kde $y = \lfloor x/2 \rfloor$.

Interpret

Dříve než svoje řešení odevzdáte, můžete si ho otestovat. Na webových stránkách olympiády (*http://mo.mff.cuni.cz/*) najdete odkaz na interpret zlomkových programů.

Studijní text

Zlomkové programy slouží k výpočtu některých funkcí na přirozených číslech. Zlomkový program má velmi jednoduchý zápis – je to konečná posloupnost zlomků, tedy kladných racionálních čísel $(z_1, \ldots, z_k)$.

Výpočet zlomkového programu probíhá po jednotlivých krocích. Během výpočtu si udržujeme jediné celé číslo a, tzv. *aktuální hodnotu*. Na začátku výpočtu se tato hodnota rovná hodnotě na vstupu. V každém kroku výpočtu najdeme nejmenší i takové, že $a \cdot z_i$ je celé číslo, a změníme aktuální hodnotu na $a \cdot z_i$. Pokud takové i neexistuje, výpočet končí.

Příklad 1: Ukážeme si program, který pro vstup $n = 2^x$ (kde $x \geq 0$) dává výstup 3^y, kde $y = x \bmod 3$.

Jedním takovým programem je posloupnost $(1/8, 9/4, 3/2)$. Slovně si popíšeme průběh výpočtu tohoto programu: Dokud to jde, zmenšuj x o 3. Když už to nejde, máme v a číslo 1, 2, nebo 4, a převedeme ho tedy snadno na 1, 3, nebo 9.

Například pro $n = 1024 = 2^{10}$ se hodnota a bude měnit takto:

$$2^{10} \xrightarrow{1} 2^7 \xrightarrow{1} 2^4 \xrightarrow{1} 2 \xrightarrow{3} 3.$$

(Číslo nad šipkou je pořadovým číslem zlomku, kterým jsme a v daném kroku násobili.)

Pro přesnost dodejme, že velmi záleží na pořadí jednotlivých zlomků. Například program $(9/4, 3/2, 1/8)$ by z čísla 2^x vyrobil číslo 3^x. Zlomek $1/8$ by se při výpočtech tohoto programu nikdy nepoužil.

Jiné vyhovující programy jsou $(1/8, 3/2)$, $(3/2, 1/27)$ a $(1/27, 3/2)$. Rozmyslete si, proč každý z nich řeší správně Příklad 1.

Příklad 2: Co spočítá program $(2/2)$ pro vstup $n = 4$? A co spočítá pro vstup $n = 7$?

Častou chybou je odpovědět, že pro vstup $n = 4$ se tento program zacyklí, ale pro vstup $n = 7$ se výpočet programu zastaví, neboť 7 není dělitelné dvěma. Správnou odpovědí ale je, že v *obou* případech poběží výpočet programu do nekonečna. Zajímají nás totiž jenom hodnoty zlomků, nikoli

jejich zápis. Zlomek $2/2$ představuje racionální číslo 1, takže $7 \cdot (2/2) = 7 \cdot 1$ je celé číslo.

Abyste se ve svých řešeních takto nespletli, doporučujeme vám psát všechny zlomky v základním tvaru. Pro posloupnost zlomků zapsaných v základním tvaru platí, že v každém kroku výpočtu hledáme nejmenší i takové, že jmenovatel i-tého zlomku dělí beze zbytku aktuální hodnotu.

Příklad 3: Ukážeme si program, který pro vstup $n = 2^{x+1}$ (kde $x \geq 0$) dává výstup 3^{x+2}.

Číslo zadané na vstupu je určitě sudé a není dělitelné žádným prvočíslem různým od 2. Použijeme prvočíslo 11 jako příznak, že už nejsme na začátku výpočtu. V prvním kroku tedy přepíšeme číslo 2^{x+1} na $2^x 3^2 \cdot 11$. Toho dosáhneme zlomkem $3^2 \cdot 11/2 = 99/2$.

Jakmile se objeví v prvočíselném rozkladu aktuální hodnoty prvočíslo 11, znamená to, že první krok výpočtu máme úspěšně za sebou. Můžeme tedy dále klidně „měnit dvojky na trojky“. To můžeme zajistit například posloupností zlomků $(3 \cdot 13)/(2 \cdot 11)$ a $11/13$. Všimněte si, že nestačí použít jeden zlomek $33/22$. Není-li vám jasné proč, přečtěte si ještě jednou Příklad 2.

Postupně se takto dostaneme k číslu $3^{x+2}11$. V této situaci už stačí jenom vydělit aktuální hodnotu číslem 11 a můžeme skončit.

Musíme dát pozor na to, abychom ve zlomkovém programu výše popsané zlomky správně seřadili: $(39/22, 11/13, 1/11, 99/2)$. V prvním kroku výpočtu se jistě použije poslední zlomek. Od této chvíle je aktuální hodnota dělitelná číslem 11 nebo 13. Střídavě se proto používají první dva zlomky, dokud se nedostaneme do situace $a = 3^{x+2}11$. Pak už se první ani druhý zlomek použít nedá. Použije se proto třetí zlomek, čímž získáme hodnotu $a = 3^{x+2}$ a výpočet zjevně skončí.

Poznámka: V zápisu podobných řešení jako v příkladu 3 není nutné čitatele a jmenovatele zlomků roznásobovat. Své řešení můžete uvést ve tvaru

$$\left(\frac{3 \cdot 13}{2 \cdot 11}, \frac{11}{13}, \frac{1}{11}, \frac{3^2 \cdot 11}{2}\right).$$

(Autorkou úvodní ilustrace je Mgr. Jaroslava Čermáková.)

Sociální inženýrství

DAGMAR BRECHLEROVÁ

Provozně ekonomická fakulta ČZU, Praha

Již mnoho institucí i jednotlivců se stalo obětí útoků na jejich informační systém; cílem útočníků je získat důležité a citlivé informace uložené v těchto informačních systémech a využít je ke svému prospěchu a ke škodě napadeného. Bezpečnost informačních systémů není zdaleka jen záležitostí technickou, ale velmi významným prvkem této (ne)bezpečnosti je prvek lidský. Dá se říci, že nejslabším článkem kteréhokoliv informačního systému bývá člověk. A jak známo, každý systém je právě tak silný (resp. slabý), jak je silný resp. slabý jeho nejslabší článek. Můžeme tedy použít veškeré technické prostředky, instalovat nové a nové antivirové a jiné anti programy, použít veškeré dostupné záplaty, důležité informace šifrovat stále silněji, ale nakonec zásadní chyby stejně dělá člověk.

Technická řešení bezpečnosti informačních systémů jsou již často na velmi vysoké úrovni a je obtížné je překonat. Proto se v posledních letech velmi rozvinulo tzv. sociální inženýrství, které je netechnickou metodou útoků na bezpečnost informačních systémů a které využívá nikoliv překonávání technických překážek a zábran, ale znalosti lidského chování a lidské nedokonalosti, a různými způsoby, které dále popíšeme, s lidmi manipuluje, za účelem provedení určité akce nebo získání určité informace.

Cílem tohoto textu je objasnit hlavní hrozby sociálního inženýrství s tím, že by se přiměřená informace o nich měla stát i součástí výuky a výchovy dětí, žáků a studentů.

Sociální inženýrství a lidský faktor bezpečnosti

Některým lidským selháním lze zabránit vhodným nastavením SW; dnes je velká snaha vyvinout SW tak, aby řadu chyb vůbec neumožnil. Jsou ale situace, kdy nejde lidským chybám (únavě, hlouposti, naivitě nebo i záměrné škodě) technickými prostředky zabránit. Sociální inženýrství zneužívá uvedených lidských slabin, ale i emocí a zvědavosti. Jelikož děti či mladí lidé ještě nejsou dostatečně sociálně zralí, vůbec si podobné nebezpečí nepřipouštějí. Na svých stránkách na sociálních sítích prozrazují o sobě a o své rodině spoustu informací, i velmi citlivých, které mohou vést

třeba k získání hesla jejich rodičů, informací o pohybu dítěte, informací o majetkových poměrech rodiny apod. Podobně každá škola má uložena osobní data svých žáků či studentů (třeba i informace o zdravotním stavu dětí) a jejich prozrazení je již trestný čin.

Chce-li se někdo dozvědět z určité organizace či firmy, školy, či o nějakém člověku některé pro něj významné informace, může postupovat různými způsoby. V mediích jsou často prezentovaným způsobem *technické* metody útočníků (*crackerů*, ne zcela korektně zvaných *hackeři*; tento pojem má širší obsah), tj. nabourání do systému, útok přes slabá místa na webových stránkách apod. Z hlediska medií jde jistě o zajímavé a přitažlivé téma, které konec konců bylo již mnohokrát i literárně a filmově ztvárněno. Představa útočníka, který se „probourává" do přísně tajných sítí Pentagonu či jiného zajímavého zdroje, je opravdu zajímavá. Ale upřímně řečeno, často lze mnohem rychleji a pohodlněji získat informace jinou cestou, sice ne tak dobrodružnou, ale mnohokrát kratší a méně namáhavou. Povídavá či zmatená sekretářka nebo nezodpovědný student působící jako správce sítě však již tak zajímaví z hlediska dobrodružných filmů nejsou. Navíc ta první zmíněná (technická) a více dobrodružná cesta je od 1. ledna 2010 trestná již i v České republice [1].

Sociotechniky

Sociotechniky (metody sociálního inženýrství) patří k netechnickým metodám. Jejich součástí je přesvědčování a ovlivňování lidí s cílem oklamat je tak, aby uvěřili, že útočník je někdo jiný, a zmanipulovat je k vyzrazení informací nebo provedení určitých úkonů. Při těchto metodách se útočník pokouší pomocí manipulace přesvědčit oběť, aby prozradila nějakou významnou informaci. Např. oběť sdělí heslo někomu, kdo se představí jako správce systému (po telefonu nebo je vyžádáno podvrženým formulářem). Často je dokonce úspěch sociálního inženýrství založen na přesvědčení oklamaného, že udělal dobrou věc, že někomu pomohl, pomohl své firmě apod.

Zvláště děti nedovedou odhadnout, jak informace, které o sobě na Internetu poskytují, mohou být zneužity. Zejména sociální sítě, které děti či mládež považují za běžnou součást svého života, jsou dnes stále více zneužívány ke získání soukromých informací. I psaní blogu (to je webová aplikace obsahující příspěvky obvykle jednoho editora, často ve formě deníku) může být zneužito ke získání hesla, neboť řada lidí má jako své heslo jméno dětí, psa atd. A právě o nich často píší na svém na blogu.

Podle pokusu, který v České republice uskutečnili novináři v roce 2009 [2], velké procento uživatelů sociální sítě Facebook zařadí mezi své „přátele“ i člověka, kterého vůbec neznají. Konkrétně se jednalo o vymyšlený profil neexistujícího chlapce a dívky, kdy se tyto fiktivní osoby snažily dostat jako přátelé k celkem 100 dalším mladým mužům a 100 mladým ženám. Výsledky jsou následující.

Test idnes 2009

- Profil fiktivní dívky si přidalo 60 % oslovených uživatelů Facebooku.
- Profil fiktivního chlapce 42 % dotázaných.
- Průměrný věk důvěřivců 19 let.
- Email poskytlo 97 % „přátel“.
- Fotografie poskytlo 90 %.
- Informace o své identifikaci ICQ, Skype poskytlo 56 %.
- Číslo mobilního telefonu poskytlo 23 %.
- Dokonce jeden 19tiletý student z Prahy poskytl svým novým „přátelům“ vše, včetně kompletní adresy domu.

Poznámka: ICQ je komunikační program přenášející informace v reálném čase, Skype je nástroj pro telefonování po Internetu, obě aplikace ale mají i další funkce.

Je tedy jasné, že pokud někdo chce o nás efektivně získat detailnější údaje, pokusí se dostat mezi naše „přátele“ na sociální síti a vyzvídat dál. Proto prozrazovat o sobě víc, než je nutné, kdekoliv na internetu je dost nebezpečné.

Nadbytečné a nebezpečné informace

Další metodou sociotechniků je získání původně zcela nevinné informace, ze které si pak útočník odvodí nějakou informaci významnější. Často mají organizace (včetně škol) na svých stránkách řadu jednotlivých zdánlivě nedůležitých informací, které však při jejich vhodné kombinaci mohou vést k získání dalších údajů pro organizaci důležitých (např. o rozpočtu), které by organizace jinak tajila. Proto, pokud sociotechnik chystá na nějakou organizaci útok, začne právě studiem internetových stránek, odkud získá jména, internetové adresy, případně telefony pracovníků firmy, šéfů, učitelů, ředitele atd. Pak je možno pokračovat i na osobní stránky těchto lidí, kde jsou opět někdy zajímavé informace. I když je totiž v bezpečnostní politice dané organizace zajištěno, co smí a nesmí být na firemních (školních) stránkách, již obvykle nikdo nezjišťuje, co má daný člověk na

svých soukromých stránkách, s čím vstupuje do diskusí na internetu atd. A zdaleka ne všichni jsou natolik obezřetní, aby třeba měli pro různé účely různé adresy a různá hesla.

Proto by mezi základní bezpečnostní opatření mělo patřit to, že se provede určitý audit stránek organizace, zjistí se, zda neobsahují nadbytečné údaje, či zda tam vývojář nenechal nějaké zbytečné informace. Dále je nutno dbát na to, aby informace, které jsou vhodné pro intranet, nebyly zbytečně umísťovány na internetu. Je dobré dohlédnout na to, zda informací poskytovaných veřejnosti není zbytečně moc. I z informací na první pohled nevinných může útočník pro sebe získat něco vhodného. Mělo by patřit k pravidelným činnostem archivovat již nepotřebné informace a poté je ze stránek odstranit. To, že by intranet měl být skutečně intranetem a nebýt otevřený široké veřejnosti, je snad jasné, ale občas se chyba vloudí.

V minulých letech prováděla diplomantka autorky tohoto textu podobný audit v jisté organizaci resp. na jejich stránkách. Např. zde našla informace o tom, jak je v dané organizaci vytvářen login, způsob odvození uživatelského jména, dále zjistila, jaký software používají servery, apod. Jiná diplomantka zase uhodla hesla svých dočasných spolupracovníků při praxi jen za znalosti jejich jmen, jmen dětí atd.

Sociotechnické fígle

Pro získání základních informací může útočník využít i telefon. Nejsnazší je to ve velké organizaci, kde se lidé navzájem neznají a kde se může útočník vydávat za pracovníka sice ze stejné firmy, ale z jiné pobočky, z ústředí atd. Pak je možno třeba zavolat novému zaměstnanci a přes něj se pokusit získat informace. Sociotechnik mu zavolá, přivítá ho jako nového pracovníka ve firmě a začne např. s bezpečným nastavením hesla a připojením k síti. Nový pracovník je nadšený tím, že se zde o něj tak dobře starají, a je ochoten udělat skoro cokoliv (např. nahrát si „doplněk“ k SW). Navíc, i pokud bude mít nějaké podezření, tak si přece na novém pracovišti nebude hned dělat problémy.

Důležité je, aby oběť neměla příliš mnoho času na přemýšlení. Proto obvykle sociotechnici naléhají na důležitost daného úkonu nebo na časovou tíseň, takže se oběť nezamyslí nad důsledky daného úkonu a tím se zvětší pravděpodobnost, že bude útok úspěšný.

Sociotechnické útoky mohou mít řadu různých podob a mohou být zaměřeny i na „normální občany“ a přímo na peníze. Například dostaneme od solidně se prezentující firmy mail, že „právě teď je ta výjimečná pří-

ležitost získat výhodnou půjčku, jen vyplňte a vraťte přiloženou žádost a do tehdy a tehdy zašlete na to a to konto vstupní poplatek tolik a tolik korun. Do (např.) deseti dnů máte sjednanou půjčku na svém kontě". Nám se půjčka hodí, vše splníme a vícekrát o té firmě neuslyšíme. Podobné to bývá i s objednávkami zboží při placení předem.

Útoky na firmy bývají složitější, ale také tam jde o větší peníze, ale třeba i o získání informací o zákaznících, o průmyslovou špionáž atd. Na jedné bezpečnostní konferenci prezentoval zajímavý příběh pracovník auditorské firmy, která mj. prováděla také bezpečnostní audit v jisté bance. Tento pracovník byl fingovaně najat do banky (se souhlasem vedení) a kromě dalších pokusů o útok obvolal vybrané pracovníky s tím, že je nutno změnit heslo za nové, které jim bylo nadiktováno po telefonu. Poté obešel všechny, kterým volal, a zjišťoval, kolik lidí si změní heslo na jiné, které jim kdosi neznámý (leč jistě vystupující ve vhodné roli) nadiktuje. Dle jeho líčení to byla zhruba polovina lidí, ovšem ostatní si heslo nezměnili hlavně kvůli tomu, že to nedovedli, ne že by nechtěli.

Podle názorů auditorů jsou dnes velmi úspěšné i takové útoky, při kterých jsou např. v kuchyňkách (kde si lidé vaří čaj a kávu) na pracovišti fingovaně ponechána různá přenosná media. Ačkoliv zaměstnanci jinak dodržují pravidla při zacházení s emaily či jiná bezpečností pravidla, velké procento lidí se na tato nastrčená media nechá nachytat a podívá se na ně ve svém počítači bez jakýchkoliv bezpečnostních opatření.

Sociotechnici se často ptají na nedůležité, na první pohled nezajímavé informace, které nedávají žádný smysl, ale pak je postupně poskládají dohromady a pokusí se o úspěšný útok. Dalším z tahů k oklamání lidí je získat si jejich důvěru (např. Dobrý den, já jsem ten a ten z oddělení ABC a pracuji s Frantou a Honzou, znáte Honzu? Říkal mi, že se mu moc líbíte.). Oběť (dívka) věří útočníkovi, že zná jejího kamaráda Honzu, protože útočník si získal i další informace z Honzova života, takže mu bude plně důvěřovat.

Další způsob je ovlivňování lidí pomocí autority: pokud například sociotechnik na oběť naléhá, že „je to pro šéfa a už to dávno mělo být hotové", tak chudák asistentka ze strachu udělá, o co je požádána.

Někteří lidé jsou velmi povídaví a ve vhodném prostředí vyzradí kdeco. Není tedy dobré na veřejnosti jako v dopravních prostředcích, obchodech mluvit o svých soukromých či pracovních záležitostech.

Phishing

Způsobů, jak využít lidskou naivitu (nepozornost, neznalost, ješitnost) je mnoho. Jedním z velmi nebezpečných útoků využívajících sociotechniky je tzv. *phishing*. Jedná se o velmi závažnou hrozbu, o které stále nejsou všichni běžní uživatelé dostatečně informováni

Phishing je druh internetového podvodu, jehož cílem je vylákat z uživatele citlivé informace, jako např. číslo účtu, heslo, číslo karty a jiné. Při phishingu je uživatel útočníkem manipulován k tomu, aby svá data zadal na podvrženou stránku, a přitom je využito sociotechnik, které uživatele dovedou právě k použití podvrhu. Útočník si pořídí seznam emailových adres, na které odešle zprávu, která se tváři (tj. je tak graficky upravena) jako oficiální oznámení dané organizace – zatím nejčastěji finanční instituce. Pro útok jsou vybírány spíše známé banky, takže je vysoká šance, že část oslovených je klientem této banky a na útok reaguje. V mailu je přímo odkaz na podvrženou stránku, která se od „pravé“ může lišit velmi nepatrně, např. jenom v lehce odlišném URL (URL, celým názvem Uniform Resource Locator, tj. „jednotný lokátor zdrojů“, je řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístění zdrojů informací ve smyslu dokument nebo služba, viz Wikipedie). To, že má klient svá data zadat na podvrženou stránku, je obvykle věrohodně vysvětleno nějakým proběhlým bezpečnostním incidentem, který banka dobře zvládla, ale přece jen a pro jistotu potřebuje znovu některé údaje potvrdit, a to co nejrychleji. Technické provedení tohoto útoku je pro útočníka bohužel poměrně snadné.

Úspěšnost útoku se pohybuje dle dostupných informací zpravidla mezi 2 – 20 procenty. Tímto způsobem se tedy dají poměrně snadno získat údaje, které pak slouží zejména k vybírání účtů. Je však jasné, že se takto dají získat i jména a hesla nejen k bankovním účtům, ale i k jiným citlivým informacím chráněným jménem a heslem.

Tyto útoky se datují zhruba od roku 2005 až 2006. Již za prvních šest měsíců roku 2006 Symantec zaznamenal prudký nárůst zpráv, které od uživatelů lákaly jejich osobní či jiná citlivá data (tj. phishing), která lze využít například k nabourání finančního konta. Dominantním cílem phishingu byly nejprve finanční služby, které tvořily 84 procent zpráv. Prvním významnějším útokem v České republice byl útok ze 3. 3. 2006 na Citibank, dále následoval útok na Českou spořitelnu. Od roku 2006 se počet těchto útoků znásobil, praktický každý se s nimi již setkal. Některý software je však již uzpůsoben tak, že na podezřelé maily upozorňuje. Také znalost

veřejnosti o tomto druhu nebezpečí je stále vyšší, přesto jsou stále důvěřiví lidé, kteří své jméno a heslo na podvrženou stránku zadají. Zásadní obranou je „neklikat“ v mailu na žádné odkazy. V poslední době se cílem phishingových útoků staly i sociální sítě.

Pharming

Pokračovatelem phishingu je tzv. *pharming*. Jde o útok více sofistikovaný, více nebezpečný a těžko odhalitelný. Název vychází ze zkomolení slova farming, čili zemědělství, pěstovat atd. Při phishingu útočníci využívají podobnosti názvu stránek, který uživatel přehlédne (www.lse.cz, www.1se.cz), zde se pouze liší malé l a jednička. Pozorný uživatel si jednak může rozdílu všimnout a jednak příslušná doména musí být zaregistrována a útočník tedy může být dopaden. Při pharmingu ovšem jde o to, že uživatel se sice snaží připojit na regulérní web, ale je mu podstrčena stránka jiná.

Ke své činnosti využívá překladu jména serveru na odpovídající IP adresu (to je číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá tzv. internetový protokol), útočí tedy na tzv. DNS (Domain Name Systém systém doménových jmen). Funkce DNS serveru je dobře vysvětlena např. v [3]. DNS server přiřazuje k sobě adresu a název stránky. Použití DNS plyne z toho, že pro uživatele je těžké pamatovat si dlouhé adresy, ale lehké zapamatovat si název, např. www.seznam.cz. Pokud se útočníkovi podaří změnit DNS záznam uživatelem zadané příslušné organizace, např. banky, přesměruje se komunikace na jiné stránky, které však na první pohled nelze rozpoznat od originálu. Nic netušící uživatel tedy zadá požadované přihlašovací údaje, a bez větších překážek je pošle útočníkovi. Proti pharmingu je obrana mnohem složitější, např. rozšíření DNS na DNSSEC, které zvyšuje bezpečnost DNS za pomoci asymetrické kryptografie (vysvětlení viz v [4]). Podrobnější vysvětlení Pharmingu je už mimo možnosti tohoto přehledného článku.

Trashing

K metodám získání potřebných informací se dá také počítat tzv. *trashing*, kdy se prohlížejí skutečné odpadky a nejenom virtuální (prolézání firemních odpadů), z nichž se zjišťují nebo rekonstruují různé dokumenty, informace o struktuře sítě, jména pracovníků, hesla atp.

Další hrozby

Společnost McAfee vydává dvakrát ročně McAfee Security Journal [5], kde referuje o nevýznamnějších hrozbách v oblasti počítačové bezpečnosti.

Podle těchto informací od roku 2008 a dále se útočníci zaměřují právě na metody sociálního inženýrství, a to často za pomoci tzv. sociálních sítí. Uživatelé těchto sítí se zde chovají velmi uvolněně, a často nevědomky sdělují tzv. „přátelům“ ze sítí informace, ze kterých se pak dají odvodit další informace. Problémem jsou také bloggeři (autoři blogů, viz dříve), kteří na svých blozích rádi vyzradí kdeco. Útoky na sociální sítě se považují za jednu z nejvýznamnějších hrozeb do budoucna.

Nebezpečí přinášejí i další metody, jako je šíření škodlivého kódu typu trojský kůň (zvaný trojan) určeného k prozrazení uložených dat. Pokud si tedy uživatel tento software sám nevědomky nainstaluje do počítače, je někdy velký problém s odhalením, protože se může jednat o software, který není možno běžně odhalit současnými antivirovými programy. Tyto škodlivé druhy software využívají nedostatků běžně používaných protokolů, a jsou tedy silnou hrozbou pro bezpečnost informací.

Lidské vlastnosti vhodné pro sociotechnický útok

Většina autorů, kteří se zabývají sociotechnikami, udává těchto 6 základních lidských vlastností, které se dají použít pro sociotechnický útok a které bychom měli mít na paměti.

Autorita – lidé mají tendenci se podřídit osobě s vyšší funkcí (mocí). Jedinou obranou proti tomuto je dodržování daných bezpečnostních pravidel všemi, i vedoucími pracovníky. Nelze podávat informace ani třeba řediteli firmy, pokud tento neprokáže svou identitu.

Sympatie – sociotechnik může získat sympatie oběti několika způsoby: stejné názory, zájmy, sport atd. Pokud sociotechnik získá sympatie případné oběti, pak od ní může získat příslušné informace.

Vzájemnost – je mnohem větší pravděpodobnost, že sociotechnikům oběť vyhoví, když pro ní předtím něco udělají. Například sociotechnik nejprve vyřeší problém se sítí (i třeba imaginární) a pak řekne oběti, ať si nainstaluje program, který bude síť hlídat, což přitom ve skutečnosti může být škodlivý kód typu trojský kůň, nebo program, který umí sledovat klávesy stisklé na klávesnici atp. Obranou je opět dodržování bezpečnostní politiky ve všech situacích.

Důslednost – lidé mají tendenci se podřídit, jestliže předtím veřejně vyhlásili svou podporu a angažovanost v určité záležitosti.

Společenský souhlas – sociotechnik zavolá a zeptá se, zda-li nemá oběť čas, že by potřeboval vyplnit dotazník, který už všichni ostatní s ním vyplnili. Zde je onen tlak: „Již všichni...“

Vzácná příležitost – viz posílání mailů. Tohoto způsobu využívá kdekdo: prvních 100 vyhrává, byl jste vylosován (nakonec zjistíme, že tzv. vylosováni byli všichni). „Jenom vyplňte Vaše údaje atd.“

Řada výše uvedených poznatků pochází od nejslavnějšího sociotechnika *Kevina Mitnicka*. Server DNAIndia.com sestavil zajímavý žebříček deseti „nejúspěšnějších hackerů“ historie. Mezi těchto 10 nejvýznamnějších hackerů historie (zde je termín hacker míněn šířeji, než je obvyklé) patří právě Kevin Mitnick a jeho sociální inženýrství. Kevin Mitnick, který dokonce získal 1. místo, dnes již téměř „mediální hvězda“, působil na počátku 90. let 20. století. Nebyl to zdatný programátor či odborník na bezpečnost sítí, ale spíše výborný psycholog. On sám své aktivity označuje pojmem *sociální inženýrství* a proslul svou drzostí a schopností „vetřít se“ skoro kamkoliv. Mnoho informací či dokonce přístupových hesel získal pouhým telefonátem, kdy se vydával za pracovníka technického oddělení a „zmatená“ sekretářka, ale i zkušenější a rádoby technicky zdatnější uživatelé bez mrknutí oka prozradili své heslo. Ve své době pronikal do systémů významných firem, jako je například Motorola, Nokia, Fujitsu nebo Sun Microsystems. Jeho činnost ukončila FBI v roce 1995, byl potrestán a v roce 2000 byl propuštěn na podmínku. Dnes se mimo jiné zabývá přednáškami o bezpečnosti právě v souvislosti se sociálním inženýrstvím. Jeho kniha *Umění klamu* vyšla v překladu i v České republice [6].

Školení o sociotechnikách

Sociotechnické útoky patří mezi velmi úspěšné. Zopakujme si, že útočník nemusí mít ani tolik odborné znalosti, jako spíše být milý, schopný empatie, dobrý herec apod. Bezpečnostní politika každé organizace by měla počítat s možností sociotechnických útoků, vhodné jistě je i školení pracovníků v bezpečnosti informačních technologií včetně informací o sociotechnikách a jejich nebezpečnosti. To platí i pro školství; já sama o dané problematice velmi často školím pedagogy z různých typů škol a mám z této oblasti řadu poznatků. Jako ukázku uvádím dále tři reálné příklady ze školní praxe.

Správce IT z jedné školy po absolvovaném kurzu o bezpečnosti poslal všem svým kolegům mail, ve kterém je požádal o poskytnutí jejich hesla do školního systému a použil historku ... došlo k incidentu, je nutno opravit systém. Všichni!! mu odpověděli a heslo mu poslali. Oslovil je ze svého soukromého mailu a jak známo, každý si můžeme udělat konto se jménem kohokoliv jiného. Při mém školení nevěřil tomu, že bude úspěšný. Poté mi napsal, jak to bylo neuvěřitelně snadné.

Další pedagog během výuky informatiky na střední škole (šlo o učňovský maturitní obor) věnoval celou vyučovací hodinu tomu, aby své patnáctileté studenty (chlapce) poučil o nebezpečích internetu a upozornil je na to, že bezhlavě posílat někomu, koho neznáme, údaje o sobě, není rozumné. Předem si přichystal na seznamce fingovaný profil vhodně vyvinuté blondýnky, pocházející ze stejného města, jako byla ona střední škola. Po bezpečnostním školení studenty vhodně vmanévroval právě k prohlédnutí seznamky, kde při zadání filtru (věk, příslušné město) mezi jinými byl profil oné vyvinuté blondýnky. Poté nechal studentům pár minut volno na samostatnou práci. Na onen fingovaný inzerát odpověděla velká část studentů hned při hodině, další pak doma. Teprve poté, co jim začal při další hodině předčítat jejich odpovědi „pro blondýnku", si uvědomili, že na internetu skutečně nikdy nevíme, kdo je „na druhé straně".

Studenti jedné školy provedli phishingový útok na pedagogy. Škola má svůj informační systém pro vypisování konzultací, zadávání známek a další pedagogickou činnost. Útok opět spočíval v žádosti znovu se přihlásit do systému, „který měl určité problémy a je nutno znovu ověřit přihlašovací údaje". Byli obesláni pedagogové všech zaměření kromě informatiků, úspěch byl veliký, studenti získali řadu dvojic jméno a heslo.

Z těchto příkladů je vidět, je nutno uživatele nejen školit, ale pak i prakticky vyzkoušet jejich odolnost proti podobným útokům. Je to nakonec i v jejich zájmu.

Pro získání podrobnějších informací o podobných nebezpečích je možno se inspirovat např. na stránkách projektu Safer internet [7], který se věnuje právě nebezpečí na Internetu pro děti a mládež, a kde je možno načerpat řadu poznatků, motivovat děti soutěžemi apod.

Literatura

[1] http://business.center.cz/business/pravo/zakony/trestni_zakon
[2] http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.asp?c=A091117_171036_sw_internet_pka
[3] http://www.nic.cz/page/312/o-domenach-a-dns/
[4] http://www.nic.cz/page/513/o-dnssec/
[5] http://www.mcafee.com/us/resources/reports/rp-security-journal-fall-2008.pdf
[6] *Mitnick, Kevin, D.*: Umění klamu. Nakladatelství Helion, Glivice Polsko, 2003.
[7] http://www.saferinternet.cz/