Obejdeme se v budoucnosti bez hackerů?

O počítačích, svobodě a soukromí.
Jak to bylo dřív?
Hackeři – počítačová elita nebo underground?

Alena Šolcová,
FIT ČVUT v Praze

Hackeři právě dnes

- Dnes odpovídá pojem „hacker“ zvídavému jedinci, který
  usiluje o hlubší porozumění přístroji nebo programu a
  hledá jejich meze a nedostatky.
- Od ostatních lidí, kteří se spokojují s tím, že umí přístroj nebo program použít,
  se hackeři liší tím,
  že se snaží proniknout do základů.
- Jsou to většinou experti ve svém oboru.

Protohackeři

- Za protohackery můžeme považovat např.
  ty, kteří se pokusili v roce 1878,
  dva roky **po vynálezu telefonu A. G. Bella**
  proniknout do telefonního systému,
  jen proto, aby poznali, jak systém funguje.

- Z dnešního pohledu můžeme označit
  „hackery“ i **kryptology, kteří prolomili Enigmu**
  v době II. světové války.

Hackeři působí kdekoliv

1878
Vynález telefonu a hackeři

- Počítačoví hackeři existují stejně dlouho jako počítače. Jejich existence sahá dokonce ještě dále, až do 19. století.

- V roce 1878, pouze 2 roky po vynálezu telefonu **Alexandrem Grahamem Bellem**, se skupina mladíků snažila proniknout do telefonního systému New Yorku.
- **Důvod?**
  Chlapci se velice zajímali o to, jak telefonní systém funguje, a vytvářeli vlastní spojení a přímá volání. Ve skutečnosti se pokoušeli „hacknout“ systém, aby zjistili, jak pracuje.

50. -60. léta a „hacks“

- Na přelomu 50. a 60. let 20. století byly počítače velice odlišné od toho, jak je známe dnes.
- V těchto letech mnoho společností a univerzit používalo tzv. sálové počítače. Udržovat a provozovat tyto stroje stálo tisíce dolarů a programátoři museli bojovat o to, aby k nim měli přístup.
- Z těchto důvodů počítačoví programátoři začali hledat cesty, jak toho ze strojů dostat co nejvíce.
- Nejlepší a nejnápaditější programy, které byly vytvořeny, se začaly nazývat **„hacks“** - programy, které upravovaly a zlepšovaly provedení operačního systému nebo aplikace a umožňovaly tak, aby v kratším čase bylo dokončeno více úloh.

Osmdesátá léta
Hacker a opovrženíhodný?

- V 80. letech začal být výraz „hacker“ nepopulární a opovrženíhodný.

- Bylo to díky lidem,
  jako
  Kevin Mitnick, Kevin Poulen
  nebo **Vladimír Levin** etc.,
  kteří začali používat počítače a internet
  pro své podezřelé činnosti a výdělky.

Security hacker contra criminal hacker

- White hats
- Ethical hats
- Odhaluje slabost počítačových systémů a sítě

- Black hats
- „Black hat hacker“ (cracker) je ten, který narušuje počítačovou bezpečnost, např. ze škodolibosti nebo k osobnímu prospěchu.
- Tento typ hackera je také podstatou veřejného mínění, že všichni hackeři jsou kriminálníci.
- Crackeři pronikají do zabezpečených sítí s úmyslem zničit data nebo vyřadit síť z provozu.

„White hat hackeři“

- „White hat hackeři“ nenapadají zabezpečení s úmyslem způsobit újmu
- Takový hacker tak může zkoumat jen vlastnosti a zabezpečení operačního systému.
- White-hat hackeři pracují často v týmech nazvaných **„sneakers“**, **„red teams“** nebo **„tiger teams“**.

Píšťalka a telefon

- **1971** - Počítačový nadšenec **John Draper** objevil, že píšťalka přibalovaná do dětských vloček produkuje přesně tón o 2600 hertzích, který je potřeba k otevření telefonní linky.
  Začal pořádat zdarma dlouhé a daleké hovory. Zvolil si přezdívku **„Kapitán Crunch“** a za několik let takto uskutečnil stovky hovorů.

Modré skříňky a jablka

- **1975** - Dva členové **Homebrew Computer Club of California** začali vyrábět „modré skříňky“, zařízení založené na Draperově objevu.
- Tyto skříňky produkovaly různé tóny, a pomáhaly tak lidem hacknout telefonní systém.
- Tito dva členové se jmenovali **Steve Wozniak** a **Steve Jobs.** V roce 1977 založili firmu Apple Computers.

60 úspěšných prolomení

- **1983** - Jedno z prvních zatčení hackerů.
  FBI zatkla šestnáctileté hackery z Milwaukee, kteří byli známí jako „414s“.

- Mladíci byli obviněni
  z více jak 60 nezákonných proniknutí
  do počítačových sítí.
  Jeden hacker byl zbaven obvinění, ostatní dostali podmíněné tresty.

2600: The Hacker Quaterly

- **1984 - Eric Corley**
  začal publikovat časopis nazvaný

„2600: The Hacker Quarterly“,

který se rychle stal hlavním zdrojem informací pro telefonní a počítačové hackování.

Zpráva o průniku na nástěnce

- 1987 - **Herbert Zinn,** sedmnáctiletý student známý pod přezdívkou **„Shadow Hawk“,** byl zatčen a obviněn z proniknutí do AT&T počítačové sítě.
- **S tímto průnikem se chlubil na elektronické nástěnce.**
- Policie situaci popsala takto: „Tento mladík byl jen několik kroků od průniku do firemní centrální telefonní ústředny, což mohlo mít za následek výpadek národní telefonní sítě a komunikačního systému.“

Virus a bezpečnostní díra v UNIXu

- **1988** - **Robert Morris,** vysokoškolský student z Cornell University, vypustil po internetu **samorozmnožující se vir**, který využíval bezpečnostní díru v systému UNIX.
  Vir infikoval přes 6000 systémů (zhruba jednu desetinu internetových počítačů v té době) a na dva dny tak shodil celou síť.
  Morris byl posléze zatčen a odsouzen k tříletému podmíněnému trestu, 400 hodinám veřejně prospěšných prací a 10 tisícům dolarů pokuty.

Špionáž a KGB

- **1989** - Pět západoněmeckých počítačových uživatelů bylo zatčeno a obviněno ze špionáže poté, co správce UC Barkley objevil stopy jejich průniku do amerických vládních a univerzitních počítačových systémů.
- **Hackeři byli zodpovědní za prodej informací a software do KGB.**
- Tři byli usvědčeni a odsouzeni, ale ani jeden z hackerů nestrávil žádný čas za mřížemi.

90. léta
přístup k heslům a informacím

- **1990** - Čtyři členové spolku hackerů z jihovýchodu USA, známého jako **„Legion of Doom“,** byli zatčeni za krádež technické specifikace pro BellSouth 911 pohotovostního telefonního systému.
  Hackeři byli obžalováni z krádeže přístupových jmen, hesel a adres do počítačové sítě, tedy informací, které mohly potenciálně narušit nebo zastavit pohotovostní službu v USA.
  Tři hackeři by shledáni vinnými a byl jim udělen trest odnětí svobody od 14 do 21 měsíců.
  Bylo jim také nařízeno zaplatit skoro čtvrt milionu dolarů za způsobené škody.

- **1991** - General Accounting Office prozradila, že během války v Perském zálivu **skupina holandských mladíků pronikla do počítačové sítě ministerstva obrany.**
  Získala tak přístup k „citlivým“ informacím o válečných operacích, včetně informací o vojácích a armádních zaměstnancích, o množství materiálu, které bylo posláno do Perského zálivu a o vývoji některých zbraňových systémů.

Manipulace reklamní soutěže

- **1993** - **Kevin Poulsen** s dalšími dvěma hackery použili počítače ke zmanipulování reklamní soutěže ve třech rádiích v Los Angeles.
- Ovládli telefonní linky do rádia a zajistili si tak, že projde pouze jejich volání.
- Vyhráli 2 Porsche, 20 tisíc dolarů a dva zájezdy na Havajské ostrovy.
- Později byli všichni tři chyceni.

Pronikl do sítě NASA a rozbrečel se

- **1994** - Dva hackeři, známí jako **„Data Stream“** a **„Kuji“,** pronikli do několika stovek počítačových sítí, včetně **NASA a Korejského jaderného výzkumného institutu.**
- Po zdlouhavém pátrání detektivové ze Scotland Yard nakonec zatkli „Data Stream“.
- Byl to šestnáctiletý chlapec, který se při zatýkání rozbrečel.

Citlivá čísla na internet

- Pracovník **British Telecom** pronikl
  do počítačové sítě,
  která obsahovala množství velice „citlivých“
  telefonních čísel,
  včetně královnina, ministerského předsedy
  Johna Majora a několika dalších velice
  tajných armádních čísel.
  Všechna tato telefonní čísla rozeslal po internetu.

Proniknutí do Citibank

- **1995** - Ruský hacker **Vladimír Levin**
  byl zatčen v Británii po údajném použití svého počítače k proniknutí do počítačové sítě Citibank. Odtud převedl peníze na různé účty po celém světě.
  Přesná částka ukradených peněz není známa. Odhaduje se na 3,7 - 10 miliónů dolarů.
  Levin byl vydán do USA, kde byl odsouzen ke třem letům vězení a pokutě 240 tisíc dolarů.

Legenda – Kevin Mitnick

- Legendární počítačový hacker **Kevin Mitnick** byl zatčen v Raleigh v Severní Karolině a obviněn z několika bezpečnostních přestupků, jako je nelegální kopírovaní počítačového softwaru, proniknutí do různých sítí a odcizení soukromých informací, **včetně 20 tisíc platných čísel kreditních karet.**
- Strávil 4 roky ve vězení.

Čtvrt miliónu průniků do dat ministerstva USA

- **1996** - General Accounting Office vydala prohlášení,
  že se hackeři v roce 1995 pokusili
  více než 250 000krát proniknout
  do souborů ministerstva obrany USA.

- **Okolo 65 procent pokusů bylo úspěšných.**

30 000 virů na internetu

- **1998** - Symantec AntiVirus Research Center, jedna z hlavních firem v oblasti ochranného a antivirového software, oznámila, že

existuje asi 30 tisíc virů,
které jsou v oběhu na internetu.

Přerušil komunikaci mezi letadly a věží

- Poprvé federální žalobce obvinil mladistvého z počítačového hackování poté, co zastavil **komunikační systém Bell** na letišti ve Worcesteru, Mass.
- Chlapcův útok přerušil komunikaci mezi letadly a kontrolní věží na více jak 6 hodin.
- Naštěstí se nepřihodila žádná nehoda.
- Chlapec byl odsouzen ke dvěma rokům podmíněně, 250 hodin veřejných prací a zaplacení pokuty 5 tisíc dolarů.

Kontrola satelitního systému

- Členové hackerské skupiny nazývané **„Master of Downloading“** prohlásili, že pronikli do sítě Pentagonu a ukradli software, díky němuž mohou kontrolovat vojenský satelitní systém.
- Vyhrožovali tím, že tento software prodají teroristům.

- **Pentagon** popřel, že software je tajný nebo že by dovoloval hackerům kontrolu nad satelity.
- Později ale připustil, že došlo k odcizení méně tajných informací.

Na přelomu tisíciletí

- **1999** - Během května a června řada vládních i jiných internetových stránek - včetně amerického senátu, Bílého domu a americké armády, padla za oběť útokům hackerů.
  Hackeři vždy změnili úvodní stránku tajemnými zprávami, které se rychle vymazaly.

  V listopadu norská skupina hackerů, nazývaná **MoRE (Master of Reverse Engineering)**, crackla klíč k dekódování ochrany kopírování DVD. Skupina vytvořila DVD dekódovací program, který byl rozesílán zdarma po internetu.
- **2000** - Firma Symantec AntiVirus Research Center odhadla, že se každou hodinu po internetu rozšíří nový počítačový vir.

  V únoru bylo za 3 dny hacknuto velké množství tehdy velice populárních webových stránek, včetně Yahoo, Buy.com, Amazon.com, CNN.com a eTrade.

  Byli hacknuty **pomocí „Denial of Service“, který zahltil webové servery ohromným počtem dotazů.**

Májový pozdrav „I love you“

- V květnu 2000 se rozmohl vir **„I Love You“**. Objevil se nejprve na Filipínách a potom se rozšířil za několik hodin do celého světa. **Způsobil škodu zhruba 10 miliard dolarů, většinou kvůli ztraceným souborům a nefunkčním počítačům.**
- **2001** - V květnu skupina čínských hackerů pronikla do několika amerických vládních sítí, včetně Bílého domu a CIA.
- Webové stránky Microsoft v USA, Velké Británii, Mexiku a Saudské Arábii byly dočasně narušeny pomocí „Distributed Denial of Service“.

Kevin Mitnick

- Nejslavnější hacker všech dob Kevin Mitnick
- Vyzbrojen klávesnicí je prý nepřítelem státu číslo 1…alespoň takto se vážně o Kevinu Mitnickovi vyjádřil jeden soudní prokurátor. FBI se zase bála, že hvízdáním do telefonního sluchátka by prý zase mohl odpálit jaderné nosiče. Kevin Mitnick byl a pořád je nesmrtelná hackerská hvězda!
- Dnes je Condorovi – krycí hackerská Mitnickova přezdívka - 53 let a již se trochu zklidnil. Stojí totiž na světlé straně a vlastní společnost Mitnick Security Consulting, která se specializuje na systémové zabezpečení přesně proti takovým lidem, k jakým kdysi patřil on.
- Kromě vedení vlastní firmy, psaní knih o svém životě a o tom, co se vše naučil, mimo jiné také přednáší na různých konferencích, v televizních a rozhlasových pořadech, a to o nebezpečí hackingu, sociálním inženýrstvím a metodách tzv. phreakingu – nabourávání se do telefonních linek.

Stručně o životě génia a vizionáře

- Jedni ho přímo k smrti nenávidí a druzí v něm vidí génia a vizionáře.
- Mitnick asi dnes největší žijící hackerská VIP mediální celebrita všech dob,
- A pozor:
  FBI v 90. letech minulého století o něm rozhlašovala, že se jedná nejnebezpečnějšího muže v celé Americe.

We´ve got ticket to ride

Sociální inženýrství

- Dle oficiálních pramenů historie hackingu se prý jednalo o první moment použití metody tzv. sociálního inženýrství – psychologicky vedené manipulace s lidmi pro získání cenných informací. Na střední škole své vrozené komunikační schopnosti pro sociální inženýrství naplno začal rozvíjet s partou stejně smýšlejících jedinců v oblasti phreakingu.
- Poslouchal cizí hovory a získával citlivá osobní data a údaje.

Hackerské kousky s klávesnicí– dokonce i IBM?

- Po střední škole šel studovat dále informatiku do centra Los Angeles na **Computer Learning Center.**

- Zde se mu třeba podařilo **získat přístupová práva k počítačům velké společnosti IBM,** taktéž ukradl zdrojové kódy operačních systémů počítačové firmy DEC.

První soud a éra největší slávy

- V roce 1988 je Kevinovi je 25 let a stojí poprvé u soudu. Vypadá to s ním bledě.
- Ale to by nebyl vychytralý Mitnick, kdyby nevymyslel něco pikantního na svou obhajobu. U soudu prohlásil, **že je nadměrně závislý na hackingu a nemohou ho soudit ani dát do vězení, ale do léčebného sanatoria.**
- Soudní verdikt nakonec zněl nakonec takto: 8 měsíců v samovazbě a 3 roky kontrolního dohledu.
- Jenže to by nebyl Mitnick, kdyby zase po chvíli klidu nevymyslel něco zajímavého - být na útěků před kontrolou federálů.

Mitnick – obětní beránek?

- 15. února 1995 v Raleigh v Severní Karolíně FBI nasazuje Mitnickovi želízka, ale tentokrát už soudy neobalamutí. Stal se jedním z prvních odsouzených hackerů na světě a soud mu vyměřil pokutu ve výši 300 dolarů, i když mu nebylo prokázáno vlastní obohacení.
- Mitnicka pomohl FBI vystopovat systémový expert a fyzik z Kalifornie Tsutomu Shihomura, který poté s pomocí novináře Johna Markoffa napsal o celé akci knihu **Takedown** (česky i film **Nebezpečný kód**).
- Za dva roky po chycení Mitnicka v Severní Karolíně napsal jiný kalifornský novinář Jonathan Littman knihu **The Fugitive Game: Online With Kevin Mitnick** s trochu odlišným příběhem od Takedown. Celý případ Mitnicka byl diskutabilní, už jen z důvodu, že soud neprokázal žádné obohacení.

V konspiračních kruzích padly i názory, že USA chtěla jen na

Které firmy hacknul, ne snad ne?

- Na začátku 90. let – se mu i díky masivní mediální podpoře začalo připisovat mnoho činů, které ani technicky vzato nešly provést, jako například **slavné nabourání se do systému NORAD, která neměla v tu dobu připojení k žádné externí síti apod.**

- Ale na druhou stranu existuje i seznam firem, které opravdu hacknul – **Motorola, NEC, Nokia, Sun Microsystems či Fujitsu Siemens.**

Po pěti letech

- Po pěti letech vězení svoboda a výměna klávesnice za pero
- V roce 21. ledna 2000 byl Kevin Mitnick propuštěn na podmínku se zákazem "surfování" na internetu po dobu tří let a zákazem používat mobilní telefony.
- Soud také Mitnickovi zakázal napsat jakoukoli knihu o jeho životě a zkušenostech z oboru po dobu sedmi let od propuštění na svobodu.
- Ale to, že Mitnick už celebritou a miláčkem novin zůstal, na tom se nic nezměnilo. Svědčí o tom i to, že jeho první oficiální návštěva webových stránek byla v roce 2003 živě vysílaná v televizi.
- Ve stejném roce se poprvé objevil i u nás v Praze při představení své první knihy **Umění klamu.**

Kevin Mitnick

Zkušenosti v knihách

- Zprávu o něm tehdy vydal i ČRo Radiožurnál, mimo jiné o tom, že Mitnickovi nikdy nešlo o to něco ukrást.
- U knih Mitnick - kromě své aktivní a legální podnikatelské činnosti - zakotvil, protože za dva roky později vydal druhou publikaci **The Art of Intruison** (volně přeloženo jako **Umění nežádoucího pronikání**) a
- V roce 2011 konečně autobiografii **Ghost in the Wires: My Adventures as the World's Most** Wanted **Hacker.**

Hackerská etika

- Steven Levy: **Hackers: Heroes of the Computer Revolution,** 1984.

- Kniha je proslavená souborem estetických a etických imperativů.
- Povinností hackera sdílet svou odbornost (open-source kódy) s ostatními a usnadnit přístup k informacím všude, kde je to možné.
- Vyplývá to z historie – v 70. letech minulého století bylo zvykem, že počítačoví experti mezi sebou sdíleli zdrojové kódy. Zisky firem plynuly především z prodeje hardwaru, software býval přibalován zdarma.

Etičtí hackeři

- Etičtí hackeři také věří v decentralizaci a považují vládní či korporátní byrokracie za nefunkční, zkažené systémy.
  Nesoudí ostatní hackery na základě pohlaví, rasy nebo věku, ale ryze dle hackerských dovedností.
  A pevně věří, že počítače mohou naše životy změnit k lepšímu.
  Přestože by se mohli nabourat do systémů velkých firem a získané informace ošklivě zneužít, nikdy to neudělají.

Počátky komunity hackerů

- Počátky této komunity jsou spojené se známým MIT v Cambridge, Mass., a datují se do šedesátých let 20. století.
- Hackeři se výraznou měrou podíleli na vzniku hnutí za „svobodný software“ i za současnou podobu internetu.

Dobří hackeři

- Slovo „hacker“ je dnes chápáno značně rozsáhle. Ustálilo se na označení schopného programátora, jehož chytré řešení problému je dobrým „hackem“. Proces řešení je obvykle označován jako „hacking“.
- Hackeři jsou odborně velmi zdatní uživatelé internetu, kteří dokáží překonat mnohé nástrahy a využít nejrůznější mezery a skulinky k provedení něčeho, co „není zcela standardní“.
- Důležitá je přitom jejich motivace a podstata jejich „nestandardních“ činů. Klasický hacker nemusí mít skutečně zlé úmysly, spíše mu jde o to, aby si ověřil svou odbornou zdatnost, aby ukázal, co umí.
- V novinářské praxi se obvykle pojmem „hacker“ označuje ten, kdo se pokouší vlámat do počítačového nebo síťového systému násilím, ilegálně, a nějak ho poškodit nebo zneužít. Výstižnější je však používat v takových případech pojem „cracker“, „crack“ a „cracking“.

  Je zřejmé, že úspěšným crackerem může být i dobrý hacker. **Ale vůbec není pravda, že každý hacker musí být nutně crackerem.**
- V praxi ale toto jemné rozlišení není bráno příliš v úvahu a termínem „hacker“ je nepříliš správně označován i „cracker“, neboli i ten, kdo má skutečně zlé úmysly.

Současnost

- V současnosti není známější hackerské skupiny než **Anonymous.** Ta dokonale splňuje definici grey-hat hackera. Členové Anonymous jsou přesvědčeni, že činí dobro, ale nikoho se na nic neptají. Vyznávají stejné hodnoty jako například WikiLeaks – odmítají cenzuru, a vyznávají transparentnost, svobodu a demokracii. Neštítí se ostře zaútočit na ty, kteří stojí na opačné straně. Když Visa, MasterCard, Paypal a další firmy v roce 2010 pozastavily kvůli nátlaku politiků dobrovolné příspěvky na chod WikiLeaks, Anonymous spustili tzv. Operation Payback. Série DDoS útoků zcela vyřadily webové stránky MasterCard, Visa a citelně zpomalily služby PayPal.
- Neméně zajímavé je uskupení **Syrian Electronic Army.** To samo o sobě tvrdí, že podporuje vládu syrského prezidenta Bašára al-Asada, ač není jasné, zda je organizace přímo spojená s vládou. Vymezují se proti politické opozici, západním zpravodajským organizacím a skupinám pro lidská práva. Využívají spamming, malware, phishing i DDoS útoky. Dokonce znetvořili významné webové stránky jako BBC News, The Daily Telegraph nebo The Washington Post. Podobně jako Anonymous věří, že dělají, co je správné.
- **O white-hat hackerech** se tak často nepíše, ale patří mezi ně i velmi významné osobnosti IT – spoluzakladatel Applu **Steve Wozniak**, tvůrce World Wide Webu **Tim Berners-Lee** nebo autor jádra operačního systému Linux **Linus Torvald** jsou skvělými ambasadory, kteří hackingu dělají dobré jméno. Jen u nich média zatím nenarazila na žádnou skandální kontroverzi.