

Brian W. Kernighan

JAK POROZUMĚT DIGITÁLNÍMU SVĚTU

**Vše, co potřebujete vědět o internetu,
bezpečnosti a soukromí**

argo / dokořán



Brian W. Kernighan

JAK POROZUMĚT DIGITÁLNÍMU SVĚTU

**Vše, co potřebujete vědět o internetu,
bezpečnosti a soukromí**

ARGO / DOKOŘÁN

Brian W. Kernighan

JAK POROZUMĚT DIGITÁLNÍMU SVĚTU

**Vše, co potřebujete vědět o internetu,
bezpečnosti a soukromí**

© 2017 Princeton University Press

Translation © Petr Holčák, 2019

Všechna práva vyhrazena. Žádná část této publikace nesmí být rozmnožována a rozšiřována jakýmkoli způsobem bez předchozího písemného svolení nakladatele.

Druhé vydání v českém jazyce (první elektronické).

Z anglického originálu *Understanding the Digital World.*

What You Need to Know about Computers, the Internet, Privacy, and Security přeložil Petr Holčák.

Odpovědný redaktor Zdeněk Kárník.

Redakce Marie Černá.

Obálka a sazba Michal Puhač podle návrhu Pavla Růta.

Vydalo v roce 2020 nakladatelství Dokořán, s. r. o.,

Holečkova 9, Praha 5, dokoran@dokoran.cz, www.dokoran.cz,

jako svou 1037. publikaci (318. elektronická).

ISBN 978-80-7363-977-8

Věnováno Meg

OBSAH

Předmluva		9
Úvod		15
I. ČÁST	Hardware	21
	1. Co je v počítači?	26
	2. Bity, bajty a reprezentace informací	40
	3. Uvnitř CPU	57
	Shrnutí k hardwaru	72
II. ČÁST	Software	75
	4. Algoritmy	79
	5. Programování a programovací jazyky	93
	6. Softwarové systémy	118
	7. Učíme se programovat	140
	Shrnutí k softwaru	153
III. ČÁST	Komunikace	155
	8. Sítě	162
	9. Internet	180
	10. World Wide Web	206
	11. Data a informace	231
	12. Soukromí a bezpečnost	256
IV. ČÁST	Celkové shrnutí	275
Poznámky		283
Slovník		291
Rejstřík		301

PŘEDMLUVA

Od podzimu 1999 učím na Princetonské univerzitě studijní předmět nazvaný „Počítače v našem světě“. Název kurzu je trapně mlhavý, musel jsem ho ale vymyslet během pěti minut a pak už jej bylo těžké měnit. Vedení kurzu se pro mě stalo velkou zábavou a takřka vždy mi přináší potěšení.

Můj kurz je založen na skutečnosti, že počítače a výpočetní technologie jsou všude kolem nás. Některé počítačové technologie vidíme kolem sebe na první pohled: každý student má daleko výkonnější počítač, než byl sálový počítač IBM 7094, který stál několik milionů dolarů, zabíral celou jednu velikánskou klimatizovanou místnost a v roce 1964, kdy jsem na Princetonu zahájil doktorské studium, sloužil celému kampusu.¹ Každý student má také mobilní telefon, jehož výpočetní výkon je rovněž mnohem vyšší než výkon počítače z roku 1964. Každý ze studentů, stejně jako významný podíl světové populace, má i vysokorychlostní přístup k internetu. Každý z nich na internetu vyhledává informace, nakupuje a k udržování kontaktu s rodinou a přáteli používá elektronickou poštu, textové zprávy a sociální síť.

To je však jen část počítačového ledovce, jehož většina se nalézá pod povrchem. Nevidíme a obvykle nemyslíme na počítače, které se ukrývají v různých spotřebičích, automobilech, letadlech a všudypřítomných elektronických přístrojích, které už bereme jako samozřejmost – fotoaparátech, hudebních přehrávačích, tabletech, navigacích GPS, herních konzolích. Ani se příliš nepozastavujeme nad tím, do jaké míry na výpočetních technologiích závisí naše infrastruktura: telefonní síť, televizní vysílání, řízení letového provozu, energetické síť, bankovníctví a finanční služby.

Většina lidí do tvorby těchto systémů přímo zapojena není, počítačové technologie ale mají velký vliv na každého z nás a někteří o nich musí činit významná rozhodnutí. Nebylo by lepší, kdybychom počítačům rozuměli lépe? Vzdělaný člověk by o nich měl znát alespoň základní věci: co počítače umí a jak to dělají; co dělat vůbec neumí a co je pro ně dnes nesmírně těžké; jak vzájemně komunikují a co se při tom děje; měl by také znát celou řadu způsobů, jimiž počítačové technologie a komunikace ovlivňují svět kolem nás.

Všudypřítomná povaha počítačových technologií nás zasahuje nečekanými způsoby. Čas od času se sice dovídáme o nárůstu sledování pomocí elektronických systémů, na vpády do našeho soukromí a nebezpečí krádeže identity, zřejmě si ale neuvědomujeme, do jaké míry šíření těchto praktik umožňují počítačové a komunikační technologie.

V červnu 2013 spolupracovník americké Národní bezpečnostní agentury (NSA) Edward Snowden vynesl a předal novinářům dokumenty, které odhalovaly, že NSA rutinně monitoruje a shromažďuje obrovské množství údajů o elektronické komunikaci – telefonických hovorech, elektronické poště, používání internetu – takřka každého na světě, zvláště však amerických občanů, včetně těch, kteří pro svou zemi žádnou hrozbu nepředstavují. Snowdenovy dokumenty rovněž ukázaly, že své občany špehují i ostatní země, v Británii například agentura zvaná Vládní komunikační ústředí (GCHQ), což je tamní obdoba NSA. Zpravodajské agentury spřátelených zemí si své informace sice obvykle vzájemně vyměňují, neplatí to ale o všech datech, takže německé zpravodajce tak trochu zaskočilo, když se dozvěděli, že NSA odposlouchávala mobilní telefon německé kancléřky Angely Merkelové.

Rovněž firmy pilně monitorují, co děláme na síti i ve skutečném světě, a každému z nás tím dál zužují možnost zůstat v anonymitě. Dostupnost ohromného množství dat umožnila rapidní pokrok v rozpoznávání řeči a jejím převádění na text, v rozpoznávání obrazu a překladech mezi jazyky, stálo nás to ale hodně z našeho soukromí.

Také zločinci se v útocích na data a databáze výrazně zlepšili. Rozmohla se vloupání do elektronických systémů firem a vlád a ve velkých množstvích se odcizují informace o zákaznících a zaměstnancích, které se pak často používají k podvodům a krádežím identity. Běžné jsou i útoky na jednotlivce. Byly doby, kdy stačilo ignorovat e-maily od údajných nigerijských princů či jejich příbuzných a mohli jsme zůstat na síti vcelku v bezpečí, nyní jsou ale cílené útoky mnohem rafinovanější a staly se jedním z nejobvyklejších způsobů napadání firemních počítačů.

Komplikované jsou i otázky jurisdikce čili soudní pravomoci a příslušnosti. Evropská unie rozhodla, že velké internetové vyhledávače musí zajistit „právo být zapomenut“, to znamená, že obyčejní lidé mohou po provozovatelích těchto vyhledávačů požadovat, aby byli vyloučeni z výsledků vyhledávání. EU to nařídila firmám, které ukládají data o jejich občanech na serverech v EU, nikoli však v USA. Tato pravidla samozřejmě platí jen v EU, v jiných částech světa je to jinak.

Další vrstvu složitosti přidává rychlé rozšíření modelu cloud computing, kdy si jednotliví uživatelé a firmy nechávají ukládat svá data na serverech vlastněných společnostmi Amazon, Google, Microsoft a řadou dalších a tyto servery jim také dodávají výpočetní operace, které potřebují. Data už nejsou přímo u svých majitelů, ale u některé z třetích stran, které mají jiné cíle, jinou odpovědnost a zranitelnost, a v různých jurisdikcích mohou čelit různým právním požadavkům.

Nastává také překotný růst „internetu věcí“, trendu připojovat k internetu všechny možné typy zařízení. Nejvýmluvnějším příkladem jsou samozřejmě mobilní telefony, k síti se ale připojují i automobily, bezpečnostní kamery, domácí

spotřebiče a různé ovladače, lékařské přístroje a velká část infrastruktury, jako je řízení letového provozu nebo energetické soustavy. Tendence připojovat k internetu všechno, co je kolem nás, bude díky neoddiskutovatelným výhodám této praxe pokračovat, je s ní však bohužel spojena i řada rizik, protože zabezpečení většiny těchto zařízení je mnohem slabší než bezpečnost vyspělých počítačových systémů.

Jedním z mála účinných nástrojů obrany proti tomu všemu je kryptografie, která nám umožňuje udržovat data a komunikace v bezpečí a soukromí. Silná kryptografie ale čelí ustavičným tlakům. Vládám se nelíbí, že by jednotlivci, firmy nebo teroristé mohli komunikovat zcela v soukromí, takže se často objevují návrhy na to, aby kryptografické mechanismy měly povinně otevřená „zadní vrátka“, která by úřadům umožňovala prolamovat šifry, samozřejmě s „patřičnými zárukami“ a jen „v zájmu národní bezpečnosti“. I kdyby to bylo motivováno dobrými úmysly, je to velmi špatný nápad, protože slabá kryptografie pomáhá nejen našim přátelům, ale i našim protivníkům.

To všechno jsou některé z problémů a otázek kolem počítačových technologií, o něž by se měli zajímat všichni, včetně mých univerzitních posluchačů nebo příslovečných mužů a žen z ulice, bez ohledu na jejich zázemí či vzdělání.

Studenti v mém kurzu nestudují technické obory – nejsou to inženýři, fyzici ani matematici. Jsou to angličtináři, politologové, historici, klasičtí filologové, ekonomové, muzikologové i teoretici umění, takže jde o úžasný průřez humanitními obory. Na konci kurzu by měli být schopni přečíst a pochopit novinový článek o počítačové technologii, získat z něj více než dosud a možná i poznat, kde není příliš přesný. Obecně vzato bych chtěl, aby moji studenti a čtenáři přistupovali k technologiím s poučenou skepsí, aby věděli, že jsou často velmi užitečné, nejsou ale lékem na všechno; na druhé straně by měli vědět, že technologie mohou mít někdy neblahé následky, že ale žádným vysloveným zlem nejsou.

Pozoruhodná kniha Richarda Mullera *Physics for Future Presidents*² (Fyzika pro budoucí prezidenty) se pokouší vysvětlovat vědecké a technické pozadí významných problémů, s nimiž se musí potýkat političtí vůdci – jaderné hrozby, terorismu, energetiky, globálního oteplování a dalších podobných věcí. Něco o těchto tématech by měli vědět i dobře informovaní občané bez ambicí vstoupit do velké politiky. Mullerův přístup je dobrou metaforou toho, čeho bych zde chtěl dosáhnout i já: „Výpočetní technologie pro budoucí prezidenty.“³

Co by měl budoucí prezident vědět o výpočetních technologiích? Co by měl o počítačích znát slušně informovaný člověk? Nějakou představu o tom má každý: zde je ta moje.

Výpočetní technologie sestávají ze tří základních technických oblastí – hardwaru, softwaru a komunikací. Na tomto rozdělení je vystavěna také struktura naší knihy.

Hardware je fyzická, hmatatelná část technologií; jsou to počítače, které vidíme a můžeme se jich dotýkat, máme je ve svých domovech a kancelářích a nosíme si je ve svých telefonech. Co je uvnitř počítače, jak to funguje, jak je to postaveno? Jak počítač ukládá a zpracovává informace? Co jsou to bity a bajty a jak je používáme, aby se z nich stala hudba, filmy a cokoli dalšího?

Software, což jsou instrukce, které počítačům říkají, co mají dělat, je naopak v podstatě nehmotný. Co můžeme vypočítat a jak rychle? Jak počítačům sdělíme, co mají dělat? Proč je tak těžké je přimět, aby fungovaly správně? Proč je často tak těžké je používat?

Komunikace spočívají v tom, že počítače, telefony a další zařízení spolu rozmlouvají, a někdy pak nechávají přes internet, web, e-mail a sociální sítě spolu mluvit i nás. Jak všechny tyto komunikační prostředky fungují? Jejich výhody jsou jasné, jaká jsou ale rizika, zvláště pro naše soukromí a bezpečnost, a jak můžeme tato rizika zmírnit?

K této trojici bychom měli připojit *data*, což jsou všechny informace, které jsou hardwarem a softwarem shromažďovány, ukládány a zpracovávány a jež jsou komunikačními systémy posílány kolem světa. Něco z nich jsou data, jimiž přispíváme do těchto systémů dobrovolně – ať už si rizika uvědomujeme, nebo ne – když na web posíláme texty, fotografie nebo videa. Zbytek jsou osobní informace o nás, a ty se obvykle shromažďují a sdílejí bez našeho vědomí, natož pak souhlasu.

Ať prezident či kdokoli jiný, o světě počítačových technologií by něco měl vědět každý, protože tyto technologie se dotýkají nás osobně. I kdybychom žili a pracovali jakkoli daleko od technických vymožeností, s technologiemi a lidmi, kteří s nimi umí pracovat, vždy nějak přijdeme do styku. Vědět něco o tom, jak tyto přístroje a systémy fungují, je velká výhoda, i kdyby měla spočívat jen v tom, že poznáme, kdy nám prodejce nebo servisní linka neříká celou pravdu. Nevědomost zde může dokonce přímo uškodit. Kdo neví, co jsou viry, phishing a podobné hrozby, podlehne jim snadněji. Pokud nevíte, jak ze sociálních sítí unikají, nebo se dokonce cíleně vysílají informace, o nichž jste si mysleli, že jsou soukromé, pravděpodobně budete o sobě na síti odhalovat mnohem více, než byste chtěli. Pokud nevíte nic o honbě komerčních subjektů za využitím všeho, co se dozvěděly o vašem životě, vzdáváte se svého soukromí v podstatě zadarmo. Pokud nevíte, proč je riskantní přistupovat ke svému osobnímu bankovnímu účtu v kavárně nebo na letišti, hrozí vám krádež peněz nebo totožnosti. A ignorovat narušování našeho osobního soukromí vládou přináší velká nebezpečí.

Kniha se obvykle čte od začátku do konce, možná ale raději zalistujete dopředu k tématům, která vás zajímají nejvíc, a zpět se vrátíte později. Můžete třeba začít pasážemi o sítích, mobilních telefonech, internetu, webu a otázkách soukromí, které začínají kapitolou 8; možná se budete muset podívat o něco

zpět, abyste plně porozuměli detailům, většina výkladu je ale srozumitelná i bez toho. Můžete přeskakovat cokoli, kde se vyskytuje příliš mnoho čísel, například pasáže o fungování binárních čísel v kapitole 2, nebo ignorovat detaily programovacích jazyků v několika dalších kapitolách. V poznámkách na konci uvádím svoji oblíbenou literaturu a jsou tam i odkazy na zdroje a užitečné dodatky. Na závěr přikládám slovníček, který podává stručné definice a vysvětlení důležitých technických termínů a zkratk.

Každá kniha o počítačích může rychle zastarat a tato není žádnou výjimkou. Její první vydání vyšlo dlouho předtím, než jsme se dozvěděli o rozsahu sledování NSA. Nejnovější vydání jsem aktualizoval zejména v částech týkajících se soukromí a bezpečnosti, jelikož tato témata prošla v posledních letech prudkým vývojem. Také jsem se snažil vyjasnit některé méně srozumitelné části a vypustil jsem či nahradil zastaralé pasáže. I přesto se může stát, že v době, kdy knihu budete číst, už některé věci platit nebudou. Stejně jako u prvního vydání jsem se i zde snažil jasně označit to, co má trvalejší hodnotu; zbytek si můžete ověřovat na webové stránce knihy kernighan.com, která nabízí aktualizace, opravy, dodatečný materiál a podobně.

Mým cílem je, aby čtenář této knihy plně ocenil úžasné možnosti výpočetních technologií a pochopil, jak fungují, odkud přicházejí a kam by mohly v budoucnu směřovat. Během čtení by si rovněž mohl osvojit užitečný způsob uvažování o světě. Pevně v to doufám.

PODĚKOVÁNÍ

Jsem hluboce zavázán všem svým přátelům a kolegům, kteří mi při psaní knihy poskytli velkorysou pomoc a rady. Jon Bentley stejně jako u prvního vydání pečlivě přečetl několik pracovních verzí a každou stránku okomentoval; kniha je nyní díky jeho příspěvkům mnohem lepší. Cenné návrhy, kritické postřehy a upozornění na chyby v celém rukopisu mi poskytovali i Swati Bhattová, Giovanni De Ferrari, Peter Grabowski, Gerard Holzmann, Vickie Kearnová, Paul Kernighan, Eren Kursun, David Malan, David Mauskop, Deepa Muralidharová, Madeleine Planeix-Crockerová, Arnold Robbins, Howard Trickey, Janet Vertesiová a John Wait. Pomohly mi také rady, které mi dali David Dobkin, Alan Donovan, Andrew Judkis, Mark Kernighan, Elizabeth Linderová, Jacqueline Mislowová, Arvind Narayanan, Jonah Sinowitz, Peter Weinberger a Tony Wirth. Bylo mi potěšením spolupracovat s pracovní skupinou nakladatelství Princeton University Press – Markem Bellisem, Lorraine Donekerovou, Dimitrim Karetnikovem a Vickie Kearnovou. Všem jim za to děkuji.

Jsem vděčný rovněž princetonskému interdisciplinárnímu středisku Center for Information Technology Policy, kde jsem si mohl užívat dobrou společnost,

zajímavé debaty a každý týden obědy zdarma. A děkuji báječným studentům svého kurzu, jejichž talent a nadšení mě stále překvapují a inspirují.

PODĚKOVÁNÍ K PRVNÍMU VYDÁNÍ

Jsem hluboce zavázán všem svým přátelům a kolegům, kteří mi při psaní knihy poskytli velkorysou pomoc a rady. Zvláště jsem vděčen Jonu Bentleymu, který podrobně okomentoval takřka každou stránku několika mých pracovních verzí. Clay Bavor, Dan Bentley, Hildo Biersma, Stu Feldman, Gerard Holzmann, Joshua Katz, Mark Kernighan, Meg Kernighanová, Paul Kernighan, David Malan, Tali Moreshetová, Jon Riecke, Mike Shih, Bjarne Stroustrup, Howard Trickey a John Wait velmi pečlivě pročetli konečné pracovní verze, poskytli mi mnoho užitečných návrhů a ušetřili mě některých velkých chyb. Za cenné komentáře děkuji také Jennifer Chenové, Dougu Clarkovi, Stevu Elgersmovi, Avi Flamholzovi, Henrymu Leitnerovi, Michaelu Liovi, Hughovi Lynchovi, Patricku McCormickovi, Jacqueline Mislowové, Jonathanu Rochellovi, Coreymu Thompsonovi a Chrisu Van Wykovi. Doufám, že poznají místa, kde jsem jejich rady poslechl, a nevšimnou si těch několika, kde jsem to neudělal.

David Brailsford mi díky svým těžce nabytým zkušenostem dodal mnoho prospěšných rad k formátování textu. Greg Doench a Greg Wilson mi velkoryse radili s publikováním. Za fotografie jsem zavázán Gerardu Holzmannovi a Johnu Waitovi.

V akademickém roce 2010–2011, kdy jsem psal první pracovní verze této knihy, byl mým hostitelem na Harvardu Harry Lewis. Jeho rady a zkušenosti s vedením obdobného kurzu byly pro mě neocenitelné, stejně jako jeho poznámky k řadě hrubých náčrtů. Škola inženýrských oborů a aplikovaných věd při Harvardově univerzitě a Berkmanovo centrum pro internet a společnost mi poskytly kanceláře a další zařízení, přívětivé a podnětné prostředí a také (ano, to existuje!) pravidelné obědy zdarma.

Zejména jsem vděčný stovkám studentů, kteří se přihlásili do kurzu „Počítače v našem světě“. Jejich zájem, nadšení a přátelství jsou pro mě stálým zdrojem inspirace. Doufám, že až budou za pár let řídit celý svět, bude se jim hodit něco z toho, čemu jsem je naučil.

ÚVOD

„Dostatečně pokročilou technologii nelze odlišit od magie.“

Arthur C. Clarke: *Zpráva o třetí planetě*, 1972

V létě 2015 jsme si se ženou vzali dlouhou dovolenou a téměř tři měsíce jsme strávili cestováním po Anglii a Francii. Pronajali jsme si auto, koupili si jízdenky na vlak a zamluvili hotely ve velkých městech i chalupy na samotách, a to vše pouze prostřednictvím internetu. Před dokončením rezervací jsme si vždy prohlédli okolí a místní zajímavosti na on-line mapách a službě Google Street View. Na neznámých místech jsme se orientovali pomocí map a navigace v mobilních telefonech, kontakt s příbuznými a přáteli jsme udržovali přes e-mail a Skype, často jsme posílali fotografie a tu a tam i videa; pomocí mobilních telefonů jsem takřka denně několik hodin pracoval na jedné knize se svým spoluautorem v New Yorku. E-mail jsem si párkrát zkontroloval i v době, kdy jsme pluli lodí a nacházeli se uprostřed Atlantiku.

Na to si asi řeknete: „No a co? Nedělá to snad každý?“ A až na neobvykle dlouhou dovolenou a plavbu lodí asi budete mít pravdu. V dnešním světě je to úplně běžné. Je téměř magické, jak snadné a pohodlné je zařizovat si své věci bez prostředníků a udržovat kontakt s blízkými i daleko od domova. Všechny tyto technologické systémy jsou už tak samozřejmé, že na ně často ani nemyslíme, přestože se naše životy díky nim výrazně a velmi rychle změnily.

Na naší dovolené jsme k pronájům ubytování nepoužívali webovou službu Airbnb, i když bychom mohli. Airbnb byla založena v roce 2008, nyní působí ve 190 zemích a uživatelé přes ni inzerují kolem jednoho a půl milionů nabídek. Airbnb měla velký dopad na hotelové podnikání v řadě měst – ceny jsou na ní často nižší a její technologie obchází zavedený regulační rámec, který se něčemu takovému ještě nestihl přizpůsobit.

Nepoužívali jsme ani přepravní službu Uber, protože jet taxíkem jsme potřebovali jen párkrát, ale využívat jsme ji také mohli (a náš londýnský taxikář si přivydělával jako řidič Uberu). Uber vznikl v roce 2009 a své služby nyní provozuje ve více než 60 zemích. Podnikání Uberu má významný dopad na odvětví taxislužby v mnoha velkých městech – stejně jako Airbnb má často nižší ceny než běžné taxislužby a jeho technologie rovněž obchází stávající regulaci, která se tomu přizpůsobuje jen velmi pomalu.

K udržování kontaktu s blízkými jsme nepoužívali ani aplikaci WhatsApp, i když i tu jsme využívat mohli, ale Skype, který byl pro nás lepší. WhatsApp byla