



Dorothy E. Denning



Západočeská Univerzita V Plzni
Katedra Kybernetiky
Semestrální práce - HKUI

Eliška Toncarová
31. semestr
15. února 2026

1 Životopis

1.1 Začátek života a akademická dráha

Dorothy E. Denning je americká vědkyně a světově uznávaná expertka na kybernetickou bezpečnost. V rámci svého výzkumu se zabývala oblastmi jako jsou kryptologie, bezpečnost dat a informační válka. Je známá pro některé inovace kybernetické bezpečnosti, lattice-based access control (LBAC) a intrusion detection systems (IDS). Doposud vydala 200 článků a 4 knihy. Proslavila se i mimo akademickou komunitu a to kvůli své účasti v soudním procesu *United States v. Riggs* a později kvůli aféře *Clipper Chip*. V roce 2012 byla uvedena do Síně slávy kybernetické bezpečnosti Spojených států amerických (National Cyber Security Hall of Fame) [4, 5].

Dorothy Elizabeth, rozená Robling, se narodila v roce 1945 ve městě Grand Rapids ve státě Michigan. Byla prostřední ze tří sester. Už jako dítě byla velice chytrá a talentovaná v matematice. Na základní škole pomáhala svému otci v jeho firmě a vydělala si tak na své první kolo. Na střední škole dokonce pro otce spravovala fakturování a vedení skladových zásob. Její středoškolský poradce si všiml jejího talentu a doporučil jí, ať se při vysokoškolském studiu zaměří na počítače, Dorothy ale tento návrh odmítla [5].

Získala stipendium na University of Michigan, kam nastoupila v roce 1963. V roce 1969 získala magisterský titul ve středoškolském učitelství matematiky. Během svých studií se náhodou dostala k programování, navzdory svému předešlému odporu. O letních prázdninách zůstala na univerzitě a pracovala jako sekretářka na oddělení radioastronomie. Jeden z profesorů si všiml, že Dorothy úspěšně provádí výpočty Dopplerových posunů na stolním kalkulátoru a doporučil jí, aby zkusila programování [5].

Programování Dorothy nadchlo. Později navíc v rámci praxe pro učitelství matematiky vyučovala děti na základní škole. Tento zážitek jí utvrdil ve změně oboru. Po získání magisterského titulu v roce 1969 nenastoupila do práce jako učitelka, ale pokračovala ve studiu, tentokrát se zaměřením na počítače [5].

Nastoupila na Purdue University na doktorské studium. Během prvního semestru se seznámila s Peterem Denningem, který vyučoval operační systémy. Padli si do oka a o dva roky později se vzali. Svoji disertační práci napsala na téma tok informací a v roce 1975 získala titul Ph.D. [4, 5].

Mezi nejznámější práce Denningové patří lattice-based access control (LBAC)

a intrusion detection systems (IDS). Model lattice-based access control představila ve článku *A Lattice Model of Secure Information Flow*. Denningová zavádí formální model, který popisuje, jak zabezpečit tok informací tak, aby nedocházelo k neautorizovanému úniku. Popisuje několik tříd informací (např. tajné, důvěrné). Hlavním záměrem je, aby nedocházelo k úniku dat z vyšších tříd do nižších. Denningová definuje množinu objektů (procesy či soubory), procesů (běžící programy) a dříve zmíněných bezpečnostních tříd a zavádí relaci "smí téct do", která určuje směr toku mezi třídami. Pokud jsou splněny požadavky reflexivity, tranzitivity, antisymetrie a pokud je zaveden operátor pro sloučení tříd, pak ze tříd vzniká mřížka (anglicky *lattice*) s nejnižší a nejvyšší třídou, což umožňuje jednotně formulovat bezpečnostní podmínky. Model poskytuje jednotný matematický rámec, ve kterém lze popsat a porovnat jednotlivé bezpečnostní systémy a klasifikovat je podle bezpečnostních cílů. Umožňuje nejenom řídit přístup k datům, ale zároveň řízení toku informací [1].

Další známou prací Denningové je systém detekce narušení (Intrusion Detection System - IDS). Denningová představuje obecný real-time model pro detekci narušení. Navrhuje odhalování narušení pomocí statistické detekce abnormalit v log souborech, jako jsou třeba neobvyklé časy přihlášení, místa, odkud se uživatel hlásí, nebo neobvyklá spotřeba zdrojů. Model sleduje auditní záznamy systému a porovnává současnou aktivitu se známými záznamy a obvyklým chováním. Model využívá 3 metriky: (1) Počítadlo událostí - proti auditním záznamům se porovnává třeba to, jestli odpovídá počet přihlášení za hodinu nebo například počet špatně zadaných hesel za minutu. (2) Měření intervalů - provnáváme jestli je stejná doba mezi přihlášeními. (3) Množství zdrojů - hledáme výchyly ve využití CPU, výchyly v počtu čtení záznamů nebo výchyly v počtu vytisknutých stran. Denningová ve článku zdůrazňuje, že takový systém by neměl nahradit dosavadní bezpečnostní řešení, ale pouze se stát další vrstvou obrany proti útokům [2].

V 70. letech došlo na poli kybernetické bezpečnosti k důležitému vývoji. Denningová a někteří další vědci správně predikovali, že kryptografie, která byla do té doby kontrolována vládou, se dostane i do soukromého sektoru. Velice jí zaujal článek z roku 1977 od Rivesta, Shamira a Adelmana, kteří navrhli praktickou implementaci kryptografie s veřejným klíčem - RSA šifru. Denningová v té době vyučovala předmět o počítačové bezpečnosti a uvědomila si, že doposud neexistuje žádná učebnice, která by se zabývala těmito novými objevy. Chopila se této příležitosti a knihu napsala sama. Učebnice *Cryptography and Data Security* byla vydána v roce 1982 a stala se standardem na

poli kybernetické bezpečnosti [5].

1.2 Veřejné vystupování

Kromě kybernetické bezpečnosti zaujala Denningovou i problematika počítačové grafiky a designu uživatelského rozhraní. V roce 1978 získala práci ve výzkumném centru zaměřeném na toto téma v Palo Alto. V této době se seznámila se Stevem Steinbergem, hackerem, který na internetu vystupoval pod přezdívkou Frank Drake [5].

Steinberg Denningovou ohromil. Velice ji zaujalo, že ačkoliv je hacker, tak přemýšlí nad problematikou soukromí a zodpovědnosti. S pomocí Steinberga získala kontakty na další hackery a začala s nimi dělat rozhovory. Jejich završením byl článek *Concerning Hackers Who Break into Computers*, který představila v roce 1990 na národní konferenci počítačové bezpečnosti ve Washingtonu. V tomto článku zveřejnila názor, že hackeři často chtějí spíš pomáhat než páchat škodu a mají vysoké standardy chování a vědcům by doporučila, aby s nimi častěji pracovali. Tento názor se mezi ostatními vědci setkal s těžkou kritikou. Článek byl označen za naivní a neprofesionální. Komunita hackerů naopak článek uvítala a Denningová si mezi nimi získala dobrou pověst [5].

Tyto sympatie ještě umocnilo to, že vystoupila na obranu studenta Craiga Niedorfa v soudním procesu *United States v. Riggs*. Neidorf byl student práv, který byl zároveň aktivní na hackerské scéně, kde vydával online magazín PHRACK. Denningová se stala poradkyní jeho právních zástupců. V rámci procesu byli Craig Neidorf a Robert Riggs obžalováni z neoprávněného přístupu a šíření dokumentů, které získali z počítačů firmy BellSouth, spadající pod AT&T. Podle obžaloby měl Riggs soubory ukrást a následně předat Neidorfovi, který je zveřejnil ve svém magazínu PHRACK. Riggs byl souzen ve státě Georgia a obdržel trest odnětí svobody v délce trvání 21 měsíců. Neidorf byl souzen ve státě Illinois. Jeho obhajoba tvrdila, že zveřejnění dokumentů nebylo nelegální na základě prvního dodatku ústavy. Denningová a John Neagle, nezávislý počítačový vědec, vystoupili jako expertní svědci obhajoby. Oba dosvědčili, že ukradené soubory v podobě, ve které je Neidorf šířil, neobsahovaly žádné citlivé informace a Neidorf se tedy ničeho nedopustil. I na základě jejich svědectví byl Neidorf osvobozen [3, 5, 7].

Bývalý kolega Denningové, Donn Parker, patřil mezi kritiky jejího článku o hackerech. Doporučil jí, aby se na problematiku podívala i z pohledu druhého tábora. Denningová proto začala navštěvovat i osoby, které proti

hackerům musely bojovat, například policii v Los Angeles, nebo prokurátorku Gail Thackery. Když se seznámila s případy reálných zločinů, byla nucena změnit názor. Zjistila, že její předešlé názory byly zcestné a většina hackerů jsou zločinci. Svůj předešlý článek a názory v něm odvolala. V roce 1995 vydala jeho redakci ve které tvrdila, že práci s hackery už nedoporučuje, protože práce s lidmi, kteří porušují zákony odměňuje špatné chování [5].

Do povědomí širší veřejnosti se dostala na začátku 90. let, kvůli své účasti v debatě o chystaném zákoně *Digital Telephony Bill*. V té době měli policie a tajné služby problém s uskutečňováním odposlechů, kvůli zlepšujícím se bezpečnostním technologiím. Nový zákon navrhoval, aby veškeré telefonní sítě byly povinně tzv. "wiretap-friendly", tedy aby na nich bylo možné provádět odposlechy. Denningová byla v té době oslovena magazínem *Discovery*, aby pro ně o chystaném zákoně něco napsala. Denningová se sešla s FBI a ostatními bezpečnostními složkami, aby zjistila jejich názor na věc. Jejich argumenty jí přesvědčili, že nová legislativa je nutná a stala se její podporovatelkou. Vláda tvrdila, že si chce pouze zachovat schopnost vykonávat odposlechy, ale odpůrci zákona věřili, že hlavním záměrem je používat více odposlechů, za nižší cenu a s méně technologickými překážkami [5].

V březnu 1993 vydala Denningová článek *To Tap or Not to Tap*, ve kterém vyjádřila podporu chystané legislativě a podpořila odposlechy. Článek vyvolal značný rozruch, protože Denningová byla doposud známá svou obranou hackerů. Denningová byla následně považována za jakéhosi "zběha" a začala čelit elektronickým útokům a urážkám [5].

O měsíc později, v dubnu 1993, se situace zkomplikovala. Národní bezpečnostní agentura (NSA) představila novou technologii jménem Clipper Chip. Jednalo se o šifrovací zařízení, které šifrovalo komunikaci a zároveň mělo jakési "zadní vrátka", která měla bezpečnostním složkám umožnit odposlech. Pokud by byly odposlechy povolené, státní složky by dostaly přístup ke klíči (nazývaném escrow key), který by zcela dešifroval komunikaci v daném kanále. Tyto klíče by byly vytvořeny během výroby čipu a následně skladovány ve státních zařízeních. Denningová dostala pozvánku, aby se stala součástí technického panelu kryptografů, kteří hodnotili výkonnost clipper čipu a hlavně šifrovací algoritmus čipu jménem Skipjack [5].

Po přezkoumání čipu se Denningová stala jeho výraznou zastánkyní a technologii začala veřejně podporovat. Odpůrci čipu ale nedůvěřovali, i proto že návrh vzešel od tajnůstkářské NSA. Algoritmus čipu, Skipjack, byl navíc utajován, což ve kritikách vyvolávalo nedůvěru. Kritika Denningové ještě vzrostla. Byla považována za jakéhosi nohsleda velkého bratra [5].

Jeden z jejích kritiků dokonce napsal kritickou bajku *Ruritania*. Ruritánie je malá spokojená země, do té doby, než policie začne vymýšlet šílené a nesmyslné zákony. Veřejnost je proti, ale nakonec je přesvědčí vědkyně Dorothy Quisling, která podporuje rozhodnutí policie. Ta díky podpoře vědkyně protlačuje stále drsnější zákony a Ruritánie se pomalu propadá do totality. Postava vědkyně Dorothy Quisling je napsaná podle Dorothy Denning [6].

Navzdory kritice zůstala Denningová neochvějnou podporovatelkou Clipper čipu a kvůli tomu dokonce získala přezdívku "Clipper Chick". Navzdory veškerým snahám se technologie neuchytila a i opětovné návrhy na její zavedení (Clipper II, Clipper III) byly veřejností rázně odmítnuty [5].

Dorothy E. Denning je nyní 80 let. Kauza Clipper čipu je už většinou veřejností zapomenuta, ale přínos Denningové zůstává. Za svůj život získala velké množství různých ocenění, například cenu Augusty Ady Lovelace, nebo cenu Harolda F. Tiptona. Dodnes je aktivní na akademické půdě. Působí na oddělení bezpečnostní analýzy na Naval Postgraduate School jako Emeritus Distinguished Professor [4].

Reference

- [1] Dorothy E Denning. A lattice model of secure information flow. *Communications of the ACM*, 19(5):236–243, 1976.
- [2] Dorothy E Denning. An intrusion-detection model. *IEEE Transactions on software engineering*, (2):222–232, 1987.
- [3] Dorothy E. Denning. The united states vs. craig neidorf: A debate on electronic publishing, constitutional rights, and hacking. *Communications of the ACM*, 34(3):24–32, 42–43, March 1991.
- [4] Department of Computer Science, Purdue University. Professor dorothea denning, June 2025. Last updated Jun 16, 2025. URL: https://www.cs.purdue.edu/about/womens-history/dorothea_denning.html.
- [5] Steven Levy. Clipper chick, September 1996. WIRED, Sep 1, 1996. URL: <https://www.wired.com/1996/09/denning/>.
- [6] Perry E. Metzger. Ruritania. http://www.brouhaha.com/eric/bad_laws/ruritania.html, 1999. A 2026 – 02 – 12.

- [7] The Phrack Staff. Phrack. <https://phrack.org/>, 1985. Electronic magazine written by and for hackers. First published November 17, 1985; accessed 2026-02-12.