Practical Cryptography

Neil Ferguson / Bruce Schneier

Obálku neznám, možná je to umělec. záměr, nebo je to špatný, černý scan

Autoři šli ve své knize obdobným směrem jako Wenbo Mao v knize Modern Cryptography. Theory & Practice, kniha však neobsahuje zdaleka tolik formálního matematického aparátu, je napsána spíše volným stylem. Lze ji proto doporučit i širšímu okruhu čtenářů. Cílem autorů je dát řadu praktických informací o reálných kryptografických systémech a ukázat tak veřejnosti důležitost pojmu bezpečnost ("Jedna díra v plotě je zcela postačující"). V úvodu ke knize autoři charakterizují vývoj kryptografie (jako aplikované discipliny) v posledních deseti letech.

Kryptografie vstoupila do širšího povědomí na počátku devadesátých let jako prostředek pro zabezpečení internetu a byla do ní vkládána řada očekávání. Většina z nich se však podle autorů nenaplnila, uživatelé mají často falešný pocit bezpečí. Nemá to však co do činění s pojetím kryptografie ve smyslu ryzí matematické disciplíny. Jedná se o transformaci těchto teoreticky bezpečných modelů do konkrétní podoby v praktických aplikacích. V tomto smyslu hovoří autoři o kryptografii jako inženýrské disciplíně a v tomto smyslu si autoři kladou cíl objasnit inženýrům, jak využívat kryptografii pro dosažení praktické bezpečnosti.

-1 slovo děkuji

Bezpečnost (viz B.Schneier v jiné své knize: Secrets and Lies) je vždy směsí činností preventivních, detekčních a reakcí. Kryptografie patří do části preventivní a jejím cílem je, aby zbývající dva činitelé (detekce a reakce) nebyly příliš zatíženy.

Kniha se skládá ze čtyř hlavních částí a část úvodní (celkem 25 kapitol). V úvodních třech kapitolách se autoři věnují základním kryptografickým přístupům a pojmům (bezpečnost, útoky a útočníci, šifrování, autentizace, digitální podpisy, PKI atd.).

První část knihy (bezpečnost zpráv) je věnována symetrické kryptografii a problematice bezpečného kanálu. Zahajuje jí pojem blokové šifry, ale autoři hned přechází k rozboru typů útoků na takovéto šifry. Obdobným způsobem se autoři zabývají módy blokových šifer, hashovacími funkcemi a autentizačními kódy zpráv (MAC, Message Authentication Code). Následuje rozbor pojmu bezpečný kanál a rozbor otázek implementací (kryptografických modelů).

Druhá část se zabývá problematikou práce s klíči. Popisuje filosofie náhodného generování klíčů (přistupují zde i hluboké zkušenosti autorů v této oblasti) a v dalších kapitolách popisuje základní postupy asymetrické kryptografie (pojem prvočísla, Diffie-Hellmanovo schéma, RSA) a uvádí pojem kryptografického protokolu. Poměrně zeširoka je zde diskutována problematika těchto protokolů jak z hlediska jejich obecné bezpečnosti, tak i z hlediska bezpečnostních vlastností konkrétních implementací těchto protokolů.

Třetí část je věnována klíčovému hospodářství. Prvním pojmem, který zde autoři diskutují, je otázka získání spolehlivého zdroje času. Cílem této části je však ukázat na základní myšlenky filozofie PKI a na problémy spojené s praktickými implementacemi PKI. Pohled autorů charakterizuje např. název kapitoly 19: The Dream of PKI (Sen o PKI) - vysvětlují zde, proč něco takového jako je ideální PKI nemůže v reálném světě existovat. Jsou zde diskutovány otázky, jako je formáty certifikátů, doba praktické životnosti klíčů, problematika digitálních certifikátů atd. V 22. kapitole (poslední v této části) se autoři věnují celé řadě otázek spojených s praktickým uchováváním tajemství (lidská paměť, biometrické metody, single-sign-on, sdílené tajemství atd.). Závěrečná čtvrtá část knihy je věnována postupům při vytváření normativních dokumentů a otázkám patentů. Kniha je tedy určena spíše laikům v oblasti kryptografie - dává jim možnost nenásilnou cestou nahlédnout do její kuchyně. Vzhledem k hloubce a originalitě úvah autorů musí být kniha zajímavá i pro odborníky.

Jaroslav Pinkava
jaroslav.pinkava@pvt.cz

Titul: Practical Cryptography.
Autoři: Niels Ferguson, Bruce Schneier,
Vydalo: Wiley Publishing, Inc., 2003,
Hardcover ISBN: 0-471-22894-X, 70 USD,
Paperback ISBN: 0-471-22357-3, 50 USD.