o książce

Minęły już ponad dwa lata, odkąd zacząłem pisać tę książkę. Początkowo chciałem, aby stanowiła ona wprowadzenie do wszystkich wartych poznania kwestii związanych z tym rodzajem kryptografii, który wykorzystywany jest w prawdziwym świecie. Jest to jednak zadanie niemożliwe do wykonania. Żadnej dziedziny nie da się podsumować w jednej książce. Z tego powodu musiałem zachować równowagę między tym, jak wiele szczegółów chciałem przedstawić czytelnikom i jak szeroki obszar chciałem objąć. Mam nadzieję, że pod tym względem okażemy się zgodni. Jeśli szukacie praktycznej książki, która nauczy was kryptografii implementowanej i wykorzystywanej przez przedsiębiorstwa i produkty, i jeśli jesteście ciekawi, jak kryptografia w prawdziwym świecie działa pod powierzchnią, ale nie szukacie podręcznika zawierającego wszystkie szczegóły implementacji – ta książka jest dla was.

KTO POWINIEN PRZECZYTAĆ TĘ KSIĄŻKĘ

Oto lista typów osób, które moim zdaniem skorzystałyby na lekturze tej książki (proszę jednak, byście nikomu nie dawali się szufladkować).

Studenci

Jeśli studiujecie informatykę, bezpieczeństwo lub kryptografię i chcecie nauczyć się czegoś o zagadnieniach kryptograficznych w kształcie, w jakim są wykorzystywane w prawdziwym świecie (np. ponieważ celujecie w pracę w tej branży lub chcecie w ramach pracy naukowej zajmować się zagadnieniami stosowanymi), wtedy w mojej ocenie jest to podręcznik dla was. Dlaczego? Ponieważ, jak wspomniałem w przedmowie, dawno temu byłem takim studentem i napisałem taką książkę, jaką chciałbym mieć wtedy pod ręką.

Osoby zawodowo zajmujące się kwestiami bezpieczeństwa

Gdy nauczałem kryptografii stosowanej, większą część mojej grupy studenckiej stanowiły osoby zajmujące się testami penetracyjnymi, konsultanci, inżynierowie i architekci zajmujący się kwestiami bezpieczeństwa, a także osoby piastujące inne, związane z nimi stanowiska. Z tego powodu materiał ten został udoskonalony za sprawą wielu pytań, jakie otrzymałem, próbując wyjaśnić skomplikowane zagadnienia kryptograficzne osobom niebędącym kryptografami. Jako że sam jestem osobą zawodowo zajmującą się bezpieczeństwem, książkę tę ukształtowały również kryptografia uprawiana przeze mnie w ramach audytów prowadzonych dla wielkich przedsiębiorstw oraz błędy, które przy okazji poznałem.

Twórcy oprogramowania bezpośrednio lub pośrednio wykorzystujący kryptografię

Książce tej kształt nadały również liczne rozmowy, jakie odbyłem z klientami i współpracownikami, którzy w większości nie zajmowali się zawodowo ani kwestiami bezpieczeństwa, ani kryptografią. Dziś coraz trudniej jest tworzyć kod, nie dotykając zupełnie zagadnień kryptograficznych. Z tego względu pewna doza zrozumienia tego, z czego się korzysta, jest konieczna. Książka ta umożliwia takie zrozumienie, wykorzystując przykłady kodu w różnych językach programowania, a tym, których temat zaciekawi, zaoferuje jeszcze więcej.

Kryptografowie ciekawi innych obszarów

Książka ta stanowi wprowadzenie do kryptografii stosowanej, która przydaje się osobom takim jak ja. Pamiętajcie, że napisałem ją przede wszystkim dla siebie. Jeśli udało mi się dobrze wykonać robotę, kryptograf teoretyk powinien móc szybko zrozumieć, jak wygląda świat kryptografii stosowanej; inny, pracujący nad szyfrowaniem symetrycznym, dzięki lekturze odpowiedniego rozdziału powinien umieć prędko podłapać zagadnienia związane z wymianą kluczy zabezpieczaną hasłem; z kolei trzeci, pracujący z protokołami, powinien umieć szybko i gruntownie zrozumieć kryptografię kwantową – i tak dalej.

Osoby kierujące pracami inżynierskimi oraz menedżerowie produktu, którzy chcą zrozumieć więcej

Ta książka próbuje również odpowiedzieć na pytania, które uważam za bardziej zorientowane na produkt: jakie są kompromisy i ograniczenia różnych podejść? W jakie ryzyko się pakujecie? Czy ta ścieżka pomoże wam postąpić zgodnie z regułami? Czy musicie zrobić to i to, aby pracować z rządem?

Żądne wiedzy osoby, które chcą zrozumieć, o co chodzi w prawdziwym świecie kryptografii

Nie musicie należeć do żadnego z typów, które wymieniłem, aby przeczytać tę książkę. Wystarczy, że jesteście ciekawi kryptografii stosowanej w prawdziwym świecie. Pamiętajcie, że nie uczę historii kryptografii i nie uczę podstaw informatyki, więc powinniście

przynajmniej słyszeć już coś o kryptografii, nim zabierzecie się do lektury książki takiej jak ta.

Zakładana wiedza – dłuższa wersja

Czego będzie nam trzeba, by wycisnąć z tej książki tyle, ile się da? Powinniśmy wiedzieć, że ta książka zakłada, że dysponujemy podstawowym rozumieniem tego, jak działa nasz laptop oraz Internet i że przynajmniej słyszeliśmy coś o szyfrowaniu. Książka ta traktuje o kryptografii w prawdziwym świecie i ciężko będzie umieścić rzeczy w kontekście, jeśli nie korzystamy swobodnie z komputera i nigdy wcześniej nie słyszeliśmy słowa „szyfrowanie".

Zakładając, że co nieco wiemy o tym, w co się pakujemy, bardzo pomogłoby, gdybyśmy wiedzieli, czym są bity i bajty, i gdybyśmy widzieli kiedyś operacje bitowe takie jak XOR, przesunięcie w lewo czy inne, a może nawet z nich korzystali. Jeśli tak nie jest, czy powinniśmy dać sobie spokój z tą książką? Nie, ale możliwe, że tu i tam trzeba będzie zatrzymać się na kilka minut i trochę pogooglować przed powrotem do lektury.

Tak naprawdę bez względu na to, jak wysokie są nasze kwalifikacje, w trakcie lektury od czasu do czasu trzeba będzie się zatrzymać i poszukać dodatkowych informacji w Internecie – czy to dlatego, że zapomniałem zdefiniować jakieś słowo przed jego użyciem (wstyd!), czy też dlatego, że mylnie założyłem, że już je znacie. Tak czy inaczej, nie powinien to być duży kłopot, ponieważ tak dobrze, jak tylko potrafię, staram się wyjaśniać różne wprowadzane przeze mnie pojęcia, tak jak tłumaczyłbym je pięcioletniemu dziecku.

I wreszcie – gdy używam słowa *kryptografia,* nasze mózgi prawdopodobnie myślą o matematyce. Dodatkowo, jeśli na tę myśl nasze twarze wykrzywiają się w grymasie, powinno nas ucieszyć, że nie musimy się tym zanadto przejmować. W tej książce chodzi o wyrobienie w sobie przenikliwości pozwalającej na intuicyjne zrozumienie tego, jak to wszystko działa, stąd na ile tylko jest to możliwe, stara się ona unikać matematycznych szczegółów.

Oczywiście skłamałbym, gdybym powiedział, że w powstanie tej książki matematyka nie miała żadnego wkładu. Nie da się uczyć o kryptografii bez matematyki. Moje stanowisko jest takie: dobra znajomość matematyki będzie pomocna, ale jej brak nie powinien przeszkadzać w lekturze większej części tej książki. Niektóre fragmenty mogą wydać się nieprzyjazne bez pogłębionej znajomości matematyki; chodzi konkretnie o ostatnie rozdziały (14 i 15) poświęcone kryptografii kwantowej i kryptografii następnej generacji. Nie ma jednak rzeczy niemożliwych i zawsze można przejść przez te rozdziały dzięki sile woli, googlując informacje o mnożeniu macierzy oraz innych zagadnieniach, których można nie znać. Jeśli zdecydujecie się je pominąć, upewnijcie się, że nie pominiecie rozdziału 16, ponieważ jest on wisienką na torcie.

Jak uporządkowana jest ta książka: mapa drogowa

Książka ta jest podzielona na dwie części. Pierwsza z nich powinna zostać przeczytana od początku do końca. Obejmuje ona większość składników kryptografii: rzeczy, których koniec końców będziemy używać jak klocków Lego, by zbudować bardziej złożone systemy i protokoły.

- Rozdział 1 stanowi wprowadzenie do prawdziwego świata kryptografii i daje nam pojęcie, czego będziemy się uczyć.
- Rozdział 2 omawia funkcje skrótu, fundamentalny dla kryptografii algorytm wykorzystywany do tworzenia unikatowych identyfikatorów na podstawie ciągu bajtów.
- Rozdział 3 omawia uwierzytelnianie danych i to, w jaki sposób możemy upewnić się, że nikt nie zmodyfikował naszych wiadomości.
- Rozdział 4 omawia szyfrowanie pozwalające dwojgu uczestników ukryć swoją łączność przed obserwatorami.
- Rozdział 5 stanowi wprowadzenie do wymiany kluczy pozwalającej na wynegocjowanie z kimś wspólnego sekretu w interaktywny sposób.
- Rozdział 6 opisuje szyfrowanie asymetryczne, pozwalające wielu osobom na zaszyfrowanie wiadomości kierowanej do jednej osoby.
- Rozdział 7 poświęcony jest podpisom – kryptograficznym odpowiednikom tradycyjnych podpisów wykorzystujących papier i pióro.
- Rozdział 8 omawia kwestię losowości, a także sposoby na zarządzanie naszymi sekretami.

Druga część tej książki poświęcona jest systemom zbudowanym z poniższych składników.

- Rozdział 9 uczy, w jaki sposób szyfrowanie i uwierzytelnianie wykorzystywane są do zabezpieczania połączeń pomiędzy maszynami (za sprawą protokołu SSL/TLS).
- Rozdział 10 opisuje szyfrowanie od końca do końca (ang. *end-to-end encryption*), w którym tak naprawdę chodzi o to, w jaki sposób ludzie tacy jak my mogą sobie wzajemnie zaufać.
- Rozdział 11 pokazuje, w jaki sposób maszyny uwierzytelniają ludzi i w jaki sposób ludzie mogą pomóc maszynom w ich wzajemnej synchronizacji.
- Rozdział 12 wprowadza w powstający świat kryptowalut.
- Rozdział 13 rzuca światło na kryptografię sprzętową, czyli urządzenia, które można wykorzystać w celu ochrony kluczy przed ekstrakcją.

Są również dwa rozdziały dodatkowe: rozdział 14, poświęcony kryptografii postkwantowej oraz rozdział 15, dotyczący kryptografii następnej generacji. Te dwa obszary zaczynają torować sobie drogę do produktów i firm, czy to dlatego, że stają się coraz istotniejsze, czy dlatego, że stają się coraz praktyczniejsze i wydajniejsze. Choć nie będę was osądzać, jeśli pominiecie te dwa rozdziały, musicie przeczytać rozdział 16 (ostatnie

słowa), nim odłożycie tę książkę na półkę. Rozdział 16 podsumowuje różne wyzwania i różne lekcje, o których każda osoba zajmująca się kryptografią od strony praktycznej (czyli również my, gdy skończymy już tę książkę), musi stale pamiętać. Jak ujął to wujek Ben znany z przygód Spider-Mana: „Z wielką mocą wiąże się wielka odpowiedzialność".

Kilka słów o kodzie

Książka ta zawiera wiele przykładów kodu źródłowego zarówno w postaci ponumerowanych listingów, jak i znajdujących się w jednym wierszu ze zwykłym tekstem. W obu wypadkach kod źródłowy jest sformatowany krojem o stałej szerokości, `takim jak ten`, aby odróżnić go od zwykłego tekstu. Czasami kod jest również pogrubiony, aby wyróżnić ten, który zmienił się w stosunku do poprzednich kroków w rozdziale, np. gdy nowa funkcja zostaje dodana do istniejącej linii kodu. W wielu wypadkach oryginalny kod źródłowy został przeformatowany; dodaliśmy podziały na wiersze i przerobiliśmy wcięcia, aby dostosować je do miejsca dostępnego na stronie książki. W rzadkich wypadkach nawet to nie wystarczyło i na listingach pojawiły się znaczniki kontynuacji wiersza (➥). Dodatkowo, gdy kod źródłowy jest opisany w tekście, zamieszczone w nim komentarze często były usuwane z listingów. Adnotacje do kodu towarzyszą wielu listingom i wyróżniają ważne zagadnienia.