ROZDZIAŁ 7

Zastosowania kryptografii

Wprowadzenie

Do tej pory zakładaliśmy, że nasze algorytmy kryptograficzne są wykorzystywane w celu zapewnienia poufności. Mają one jednak dużo więcej zastosowań. Zawsze gdy wykorzystujemy kryptografię, ważne jest, byśmy sprawdzali, czy pomaga nam ona osiągnąć nasze zamierzone cele. Oto przykład niewłaściwego wykorzystania kryptografii.

W 1983 roku studio MGM wyprodukowało film zatytułowany *Gry wojenne*. Stał się on kultową produkcją, która zwróciła uwagę na niebezpieczeństwa związane z hakowaniem. Jedno ze streszczeń opisuje go w następujący sposób: „Los ludzkości spoczywa w rękach nastolatka, który przypadkowo dostaje się do taktycznego komputera Departamentu Obrony". Otwierająca scena pokazuje nastolatka włamującego się do systemu komputerowego swojego uniwersytetu i zmieniającego oceny swojej dziewczyny[10]. W tamtym czasie wiele uniwersytetów przechowywało wyniki egzaminów w bazach danych, do których można było uzyskać zdalny dostęp. Nie powinno zaskakiwać, że fakt zagrożenia wyników nieupoważnionymi manipulacjami pokazanymi w filmie był

[10] W rzeczywistości główny bohater filmu był jeszcze uczniem szkoły średniej, a opisana scena nie otwierała filmu, ale następowała nieco później. Bohater nie musiał też w zasadzie włamywać się do szkolnego komputera, bo udało mu się wcześniej podejrzeć potrzebne hasło [przyp. tłum.].

dla nich źródłem obaw i sprawił, iż chciały prowadzić odpowiednie zabezpieczenia.

Jedna z propozycji polegała na zaszyfrowaniu ocen każdego studenta. Nie przybliżało to jednak do osiągnięcia celu, a zrozumienie dlaczego jest zarówno ważne, jak i interesujące. Łatwo dostrzec, co udaje się osiągnąć dzięki zaszyfrowaniu ocen. W rezultacie nikt, kto włamał się do bazy danych, nie zobaczy stopni żadnego pojedynczego studenta. Zamiast tego włamywacz dostrzeże pozbawione znaczenia dane dołączone do każdego nazwiska. Niestety, niekoniecznie powstrzyma to hakerów przed konstruktywną zmianą stopni. Jeśli haker ma słabe oceny, ale wie, że jakiś konkretny student ma dobre stopnie, zmienił po prostu pozbawione znaczenia dane przy swoim nazwisku w taki sposób, by były identyczne z tymi powiązanymi z nazwiskiem prymusa. Oczywiście jeśli nie zna dokładnie stopni tego drugiego studenta, nie będzie też znać swoich własnych. Wie jednak, że teraz ma oceny pozwalające mu zdać. Nie jest to odpowiedź na wszystkie problemy. Zauważmy również, że w tym konkretnym przykładzie algorytm nie został złamany. Nie został nawet przypuszczony na niego atak. Użytkownik po prostu nie przeanalizował poprawnie problemu.

Nazwisko	Zaszyfrowane stopnie
Dobry	13AE57B8
Zły	2AB4017E

→

Nazwisko	Zaszyfrowane stopnie
Dobry	13AE57B8
Zły	13AE57B8

ALBO NAWET TAK

Nazwisko	Zaszyfrowane stopnie
Dobry	2AB4017E
Zły	13AE57B8

Przypuśćmy teraz, że zamiast szyfrować jedynie stopnie, uniwersytety zaszyfrowały całą bazę danych. Czy to pozwoliłoby osiągnąć cel w postaci powstrzymania hakera przed zmianą stopni? W tym wypadku zaszyfrowanie całej bazy danych znaczyłoby, że cały plik byłby niezrozumiały dla hakera. Jednak nawet wówczas mogłoby to nie wystarczyć do zabezpieczenia przed hakerem usiłującym zmienić stopnie. Przypuśćmy na przykład, że każda linia pliku reprezentuje nazwisko oraz stopnie jakiegoś studenta. Gdyby studenci uczestniczący w zajęciach wyświetlali się w porządku alfabetycznym, atak omawiany w poprzednim akapicie nadal byłby możliwy.

Nim skupimy się na tym, jak kryptografia mogłaby zostać wykorzystana w celu ochrony przechowywanej informacji przed zmanipulowaniem, zatrzymajmy się i rozważmy, czy naprawdę jest takie ważne, czy ktoś mógłby zmienić stopnie przechowywane w jakiejś konkretnej bazie danych. Jasne, że stanowi rzecz absolutnie kluczową, by studenci byli nagradzani właściwymi stopniami. Jeśli baza danych, która uległa zmianie, nie jest jedynym dostępnym rejestrem, wtedy student mógłby nie odnieść żadnych korzyści ze zmiany stopni w tym konkretnym rejestrze. Kluczowe wymaganie jest prawdopodobnie takie, że powinien istnieć jakiś mechanizm ostrzegający wszystkich autoryzowanych użytkowników, iż oceny zostały zmienione. Tak więc może być tak, że zapobieżenie zmianom nie jest kluczowe, jeśli tylko zmiany mogą zostać wykryte. Może to znaczyć, że autoryzowani użytkownicy są ostrzegani przed tym, by nie polegać na tej bazie danych i by zawsze odwoływać się do głównego rejestru. W wielu sytuacjach wymagana jest detekcja nieuprawnionych zmian, a nie zapobieganie zmianom.

Osiągnięcia kryptografii są powszechnie wykorzystywane dla zagwarantowania detekcji nieuprawnionych zmian w dokumentach. Tak naprawdę – przynajmniej w wypadku sektora komercyjnego – nie służy ona już głównie do zapewniania poufności. Poza

tradycyjną ochroną prywatności kryptografia wykorzystywana jest, by zagwarantować:

- *ochronę integralności danych*: zapewnić, że informacje nie zostały zmienione w sposób nieuprawniony lub za pomocą nieznanych środków;
- *umożliwienie uwierzytelnienia*: potwierdzenie tożsamości jakiegoś podmiotu;
- *uwierzytelnienie pochodzenia danych*: potwierdzenie źródła informacji;
- *niezaprzeczalność*: zapobieganie zaprzeczeniu (zwykle przez twórcę) treści informacji i/lub jego tożsamości.

Istnieje rzecz jasna sporo standardowych (niekryptograficznych) sposobów ochrony danych przed przypadkowym zniekształceniem, na przykład przez użycie kontroli parzystości lub bardziej wyrafinowanego kodowania korekcyjnego. Jeśli jednak wymagana jest ochrona przed rozmyślną zmianą, wtedy techniki te mogą nie wystarczyć, ponieważ zależą jedynie od informacji dostępnych publicznie. Każdy kto z premedytacją zmieniałby informację, zaszyfrowałby odpowiednio zmienioną wiadomość, tak by zmiana pozostała niewykryta. Dlatego w celu ochrony przed rozmyślną zmianą trzeba posłużyć się pewnymi wartościami znanymi jedynie nadawcy i (być może) odbiorcy, takimi jak klucz kryptograficzny.

Zastosowanie algorytmów symetrycznych dla zapewnienia poufności

Zidentyfikowaliśmy już pewne potencjalne ryzyka związane z bezpieczeństwem, które pojawiają się, gdy szyfr blokowy wykorzystywany jest do zaszyfrowania danych w trybie ECB. Jest na przykład możliwe, że ktoś, kto zna korespondujące bloki tekstu jawnego i szyfrogramu, może zmanipulować bloki szyfrogramu i skonstruować