SR20. Zadania i ćwiczenia (bezpieczeństwo)

1. Jakie mechanizmy usług w zakresie bezpieczeństwa można by udostępnić w systemie rozproszonym budowniczym aplikacji, którzy przy projektowaniu systemu uwzględniają wyłącznie czynnik powiązań końcowych[1].

2. Czy w metodzie RISSC całe bezpieczeństwo można skoncentrować na bezpiecznych serwerach, czy nie?

3. Załóżmy, że poproszono Cię o opracowanie aplikacji rozproszonej, która umożliwi nauczycielom organizowanie egzaminów (nie mówimy o egzaminie 22 czerwca). Podaj co najmniej trzy wytyczne, które stałyby się częścią polityki bezpieczeństwa w takiej aplikacji.

4. Czy w protokole uwierzytelniania, pokazanym na rys. 9.6[2] (plansza 54), byłoby bezpiecznie połączyć komunikaty 3 i 4 w komunikat $K_{A,B}(R_B,R_A)$?

5. Dlaczego na rys. 9.9 (plansza 58) nie jest konieczne, aby centrum rozprowadzania kluczy (KDC) miało pewność, że rozmawia z Ają, kiedy otrzymuje ono zamówienie na klucz tajny, który Aja będzie użytkować wspólnie z Benkiem?

6. Co można zarzucić pomysłowi zrealizowania jednorazówki w postaci znacznika czasu?

7. W komunikacie 2 protokołu uwierzytelniania Needhama-Schroedera bilet jest zaszyfrowany za pomocą klucza tajnego, używanego wspólnie przez Aję i centralę KDC. Czy to szyfrowanie jest niezbędne?

8. Czy możemy bezpiecznie tak zmodyfikować protokół na rys. 9.13 (plansza 64), aby komunikat 3 składał się tylko z R_B?

9. Wymyśl prosty protokół uwierzytelniania, używający podpisów w kryptosystemie z kluczem jawnym.

10. Załóżmy, że Aja chce wysłać Benkowi komunikat m. Zamiast szyfrować m za pomocą Benkowego klucza publicznego, K_B^+, generuje ona klucz sesji $K_{A,B}$ i wysyła komunikat $[K_{A,B}(m), K_B^+(K_{A,B})]$. Dlaczego jest to schemat zazwyczaj lepszy? (*Wskazówka*: rozważ kwestie wydajności).

11. Jak można wyrazić zmianę ról w tablicy kontroli dostępów?

12. Jak są zrealizowane listy kontroli dostępów w systemie plików UNIX?

13. W jaki sposób przedsiębiorstwo może wyegzekwować używanie bramy pośrednika Sieci i powstrzymać swoich użytkowników przed bezpośrednim dostępem do zewnętrznych serwerów WWW?

14. Spoglądając na rys. 9.24 (plansza 76), określ, w jakim stopniu użycie odniesień do obiektów Javy w charakterze uprawnień rzeczywiście zależy od języka Java.

15. Wymień kilka zalet i wad używania do zarządzania kluczami serwerów scentralizowanych.

16. Protokołu wymiany kluczy Diffiego-Hellmana możemy też użyć do ustanowienia wspólnego klucza tajnego między trzema stronami. Wyjaśnij, jak to zrobić.

17. W protokole wymiany kluczy Diffiego-Hellmana nie ma uwierzytelniania. Wykorzystując tę właściwość, intruz Cyryl (złośliwa osoba postronna) może łatwo wtargnąć w proces wymiany kluczy między Ają a Benkiem i zrujnować bezpieczeństwo. Wyjaśnij, jak mogłoby do tego dojść.

18. Podaj prosty sposób odwoływania uprawnień w systemie Amoeba.

19. Czy ograniczanie żywotności klucza sesji ma sens? Jeśli tak, to podaj przykład, jak można to osiągnąć.

---

[1] Ang. *end-to-end argument*, zob. //web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf; pojęcie to jest również wspomniane w p. 5.2.2, w wydaniu polskim.

[2] Jeśli nie zaznaczono inaczej, numery rysunków odnoszą się do podręcznika angielskiego S&T 2017.

20. Jaką rolę odgrywa znacznik czasu w komunikacie 6 na planszy 87 (rys. 8.38 w wydaniu polskim) i dlaczego należy go szyfrować?

21. Uzupełnij rys. 8.38 (wydanie polskie), dodając komunikację związana z uwierzytelnieniem Ai i Benka.

22. Rozważ komunikację między Ają i serwerem uwierzytelniającym AS, jak w systemie SESAME. Na czym polega różnica — jeśli w ogóle jest jakaś — między komunikatem $m_1 = K^+_{AS}[K_{A,AS}[dane]]$ a $M_2 = K_{A,AS}[K^+_{AS}[dane]]$?

23. Zdefiniuj przynajmniej dwa różne poziomy niepodzielności transakcji w elektronicznych systemach płatności.

24. Kupujący w systemie pieniędzy elektronicznych powinien raczej poczekać jakiś czas, zanim użyje pieniędzy, które podjął z banku. Dlaczego?

25. Anonimowość sprzedającego w systemie płatniczym jest często zakazana. Dlaczego?

26. Rozważ elektroniczny system płatności, w którym kupujący wysyła gotówkę do (zdalnego) sprzedającego. Podaj tabelę podobną do tabel użytych na rys. 8.44 i 8.45 (wydanie polskie), wyrażającą ukrywanie informacji.

20-06-13 zpl..iiuwr, na podstawie podręczników Tanenbauma i Steena