

## [SR] Rozwiązania zadań 1 i 3 z listy 9

**Zadanie 1.** Mechanizmy, które przydadzą się budowniczym aplikacji, która uwzględnia czynnik powiązań końcowych:

- Mechanizm do wyliczania sum kontrolnych dla podanego ciągu bitów. Jest potrzebny, ponieważ przy zapisywaniu danych, na jednostce, z której chcemy rozpocząć przesył danych, potrzebujemy zapisywać wszystkie dane wraz z wyliczonymi sumami kontrolnymi. Przykładem takiego mechanizmu może być, omawiany na wykładzie, algorytm kryptograficzny MD5.
- Mechanizm do obsługi potwierdzania powrotnych sum kontrolnych i ewentualnego powtórnego przesyłania danych. Przykładowy mechanizm mógłby numerować fragmenty danych, które chcemy przesłać, a następnie, po odebraniu sumy kontrolnej, potwierdzać poprawność danych lub przesyłać ponownie dany fragment danych, być może z pewną informacją o niepowodzeniu w przesyłaniu, w celu identyfikacji etapu przesyłu, który powoduje jego niepoprawność działania.

**Zadanie 3.** Przykładowe wytyczne, które stałyby się częścią polityki bezpieczeństwa aplikacji do przeprowadzania egzaminów:

1. Wprowadzenie kont dla użytkowników do logowania do aplikacji. Użytkownicy niezalogowani nie mają dostępu do aplikacji.
2. Podział kont użytkowników na dwa rodzaje:
  - a. konta administratorskie - dla nauczycieli, umożliwiając wprowadzanie do aplikacji arkuszy egzaminacyjnych, etc.,
  - b. konta użytkowników - dla uczniów, takie konta mają ograniczony dostęp do aplikacji, tylko do swoich egzaminów.
3. Zapewnienie szyfrowania wgrywanych arkuszy egzaminacyjnych, a także rozwiązań przesyłanych przez uczniów w celu uniemożliwienia wykradnięcia danych przez osoby trzecie, czyli intruzów.
4. Zabezpieczenie plików PDF z arkuszami egzaminacyjnymi specjalnymi, indywidualnymi dla każdego pliku, znakami wodnymi, niewidocznymi dla użytkownika, które pozwoliłyby na identyfikację sprawcy wycieku arkusza.
5. Dodatkowe zabezpieczenie czasowe do dostępu do podstrony z arkuszami egzaminacyjnymi. Uczeń, nawet mimo znajomości ścieżki do podstrony z arkuszem egzaminacyjnym, nie jest w stanie pobrać podstrony poza ustalonymi przez nauczyciela godzinami egzaminu.