Mechanismy zabezpečení OS Android s využitím jazyka Kotlin

Student Bc. Lukáš Balaževič se ve své diplomové práci soustředí na popis bezpečnostních mechanismů v rámci operačního systému Android OS. Z pohledu řešené problematiky je práce aktuální, jelikož je zajištění zabezpečené komunikace v případě mobilních zařízení klíčovým požadavkem.

Teoretická část práce se soustředí na obecný popis vývoje mobilních zařízení a operačního sytému Android. Dále jsou diskutovány kryptografické protokoly, kdy jsou přiloženy ukázkové implementace pro jednotlivé kryptografické operace. Student provedl implementaci na vybraných mobilních zařízeních (chytré telefony a hodinky), což považuji za přínosné pro praktické ověření náročnosti jednotlivých kryptografických mechanismů. Přestože student provedl rozsáhlé testování, v textu práce bohužel nejsou dosažené výsledky dostatečně popsány. Z pohledu formálního členění teoretické části lze také vytknout nekoncepční návaznost jednotlivých sekcí či podsekcí, a to zejména v kapitole č. 2.

Praktická část práce popisuje návrh a implementaci aplikace SecNote jakožto kompletního řešení, které demonstruje ukázku implementace bezpečnostních mechanismů v Android OS. Konkrétně je pozornost zaměřena na zabezpečenou komunikaci mezi mobilním zařízením a vytvořeným cloudovým systémem. Z pohledu samotné implementace jsou splněny požadavky zadání, kdy jsou zahrnuty mechanismy pro: (i) biometrické ověření, (ii) časově omezené přihlášení, (iii) identitu uživatele, (iv) digitální podpis požadavků, (v) šifrování a dešifrování a (vi) vytvoření zabezpečeného komunikačního kanálu.

Z pohledu formálního zpracování je práce na průměrné úrovni. V případě teoretické části je obtížné pochopit textový popis, jelikož text ne vždy vhodně odkazuje na vložené diagramy. Obtížné porozumění je také dáno absencí vysvětlení zkratek. V textu se dále objevuje řada překlepů, nepřesných formulací či typografických chyb. Z pohledu zadání práce byly splněny veškeré body, nicméně získané výstupy nejsou dostatečně okomentovány.

Na základě výše uvedeného hodnotím práci stupněm B / 83 bodů a doporučuji k obhajobě.

Otázky oponenta:

Otázka č.1: Vysvětlete hlavní rozdíly mezi programovacím jazykem Java a Kotlin.

Otázka č.2: Programovací jazyk Kotlin je takzvaně null safe. Vysvětlete hlavní výhody tohoto přístupu.

Otázka č.3: Objasněte, z jakého důvodu byl využit gRPC protokol.

Otázka č.4: V závěru práce je zmíněna možnost využití mTLS. Objasněte rozdíly mezi TLS a mTLS.