Zdeněk Říha
Fakulta informatiky
Masarykova universita
Botanická 68a, 602 00 Brno

POSUDEK DIPLOMOVÉ PRÁCE

Datum: 15. 6. 2014

Student: Ondřej Guettner

Vedoucí DP: Václav Matyáš

Oponent DP: Zdeněk Říha

Název: Group key agreement in Android-based mobile devices

Posudek:

Předložená diplomová práce se věnuje problematice skupinových protokolů pro domluvu na klíči. V souladu se zadáním práce se student věnuje také problematice získávání entropie.

V práce se student nejprve obecně zabývá získáváním entropie, dále se věnuje skupinovým protokolům pro domluvu na klíči. V těchto částech student prokazuje dobré pochopení problematiky, popisuje a srovnává jednotlivé protokoly.

Následně student podává úvod do problematiky OS Android a v kapitole 4 popisuje implementační část diplomové práce, diskutuje možnosti získávání entropie v OS Android a dále popisuje svou implementaci, včetně aspektů uživatelského rozhraní a bezpečnostních aspektů.

Práce je zpracována velice pečlivě. Student odvedl dobrou práci, vůči které nemám výraznějších připomínek.

Po jazykové (práce je psána anglicky) a typografické stránce je práce v pořádku. Práce s literaturou je odpovídající.

Hodnocení:

Doporučuji práci uznat jako práci diplomovou a navrhuji hodnocení **A**.

Zdeněk Říha
(oponent)