An Empirical Analysis of Android Banking Malware
Andi Fitriah A.Kadir, Natalia Stakhanova, Ali A.Ghorbani
Faculty of Computer Science, University of New Brunswick

ABSTRACT
In general, any financial operation on the mobile platform potentially exposes a user to a variety of threats including data leakage, theft and financial loss. Driven by financial profits, banking malware leverages user’s cluelessness, openness of mobile platforms, and a lack of security measures. In this work, we aim to give insight into mobile banking malware and explore unique characteristics of its communication patterns. Given popularity of Android platform, in this work we focus on Android banking malware detected since the first appearance of Android platform in 2008. Through static and dynamic analysis combined with visualization, we analyze patterns of benign and malicious URLs employed by malware, their common characteristics, encoding trends, and the relationships with other types of malware. Through our study, we reveal methods (e.g., hidden encryption techniques) currently adopted by attackers to avoid detection. As a part of this study, we compile and offer to the research community a dataset containing 973 samples representing 10 Android banking malware families.

CONCLUSION
1. Behavioral similarity of Android banking malware (DGA, encryption, URLs)
2. Evolution of Android banking malware (become sophisticated over time)