Anomaly Detection on Smartphones

Aubrey-Derrick Schmidt*

* Technische Universität Berlin, DAI-Labor,
Ernst-Reuter-Platz 7, 10587 Berlin, Germany
aubrey.schmidt@dai-labor.de

This abstract outlines my ongoing research in the field of smartphone anomaly detection. Malware, e.g. like virus, worms, and Trojan horses, have been threats to computer systems for many years and it was only a question of time when the first malicious software writers would get interested in smartphone platforms, such as Symbian OS. In 2004, the first articles about malware for smartphones [1] appeared saying that the next generation of targets are mobile devices. Since then, the number of malwares increased every month, and variants for various platforms appeared [2].

Commercially available countermeasures to smartphone malware suffer from weaknesses since they rely on signature lists or static rules. Additionally, the currently used signature-based approaches leave user exposed to the malware threat until the signature is available where Builygin [3] showed that in worst case a MMS worm targeting random phone book numbers can infect more than 700,000 devices in about three hours. Therefore, it is crucial to detect malware presence and activity as fast as possible. Monitoring-based anomaly detection systems can be a valuable addition to signature-based approaches for achieving this since they do not rely on signatures and can indicate suspicious activity in real-time. Although still suffering from high false-alarm and low detection quality several approaches showed the functionality of such systems, e.g. [4].

My current research focuses on creating and evaluating host-based anomaly-detection systems for smartphones. First results show that these cannot be fully independent from remote systems analyzing the monitored data since capabilities, like CPU power and availlable memory, are still very limited. But as these capabilities are steadily increasing, I expect *capable* devices to be released in the next two years. Especially devices running open platforms, e.g. Android or OpenMoko, are of special interest since they provide full access to the operating system, which is necessary for implementing an effective host-based anomaly detection system. Therefore, an initial monitoring client will be developed on Android for showing its usability for implementing low-level security tools. The main problems that have to be handled are: decreasing device resource usage, decreasing false positive rates of the detection, and increasing detection quality. Furthermore, applicability of already existing Linux tools. e.g. Snort, Nagios, or OSSEC, will be checked.

References

[1] D. Dagon, T. Martin, and T. Starner, "Mobile phones as computing devices: The viruses are coming!" *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 11–15, 2004.

[2] A. Schmidt and S. Albayrak, "Malicious software for smartphones," Technische Universität Berlin, DAI-Labor, Tech. Rep. TUB-DAI 02/08-01, Feb. 2008, `http://www.dai-labor.de`.

[3] Y. Bulygin, "Epidemics of mobile worms," in *Proceedings of the 26th IEEE International Performance Computing and Communications Conference, IPCCC 2007, April 11-13, 2007, New Orleans, Louisiana, USA*. IEEE Computer Society, 2007, pp. 475–478.

[4] A.-D. Schmidt, F. Peters, F. Lamour, and S. Albayrak, "Monitoring smartphones for anomaly detection," in *MOBILWARE 2008, International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*, Insbruck, Austria, 2008.