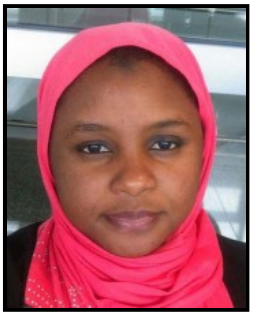

Other

Towards a More Resilient Android Malware Fingerprinting

Aisha Ali-Gombe

Louisiana State University

Digital Media Center 1034
April 21, 2017 - 10:30 am

Abstract:
The rapid increase in mobile malware over the years has been of great concern to the security community. Encroaching on user's privacy, malicious apps increasingly exploit various sensitive data on mobile devices. The information gathered by these applications is sufficient to uniquely and accurately profile users and to cause tremendous personal and financial damage.
Android malware are often created by injecting malicious payloads into benign applications. They employ code and string obfuscation techniques to hide their presence from antivirus scanners. Recent studies have shown that common antivirus software and static analysis tools are not resilient to such obfuscation techniques. To address this problem, we develop a robust fingerprinting approach that can deal with complex obfuscation with a high degree of accuracy.

Our approach, called ***OpSeq***, scores similarity as a function of normalized opcode sequences found in sensitive functional modules as well as app permission requests. This combination of structural and behavioral features results in a distinctive fingerprint for a malware sample, thereby improving our model's overall recall rate. We tested our prototype on 1,192 known malware samples belonging to 25 different families, 359 benign apps, and 207 new obfuscated malware variants. The empirical results show that ***OpSeq*** can correctly detect known malware with an F-Score of 98%.

Speaker's Bio:

Aisha Ali-Gombe is currently a postdoctoral researcher at Center for Computation and Technology at the Louisiana State University. She has completed her Ph.D. requirements in Computer Science at the University of New Orleans awaiting formal graduation in May 2017. During her Ph.D. studies, Aisha has worked in various areas of cyber security and digital forensics including code fingerprinting, malware analysis, privacy policy enforcement techniques and memory & database forensics. She has published and presented her work in conferences such as CODASPY, PPREW, WiSec and AAFS. She is a recipient of TotalFinaElf Undergraduate Merit Scholarship, Nigeria.

Center for Computation & Technology
2003 Digital Media Center • Telephone: +1 225/578-5890 • Fax: +1 225/578-8957