The modeling of a digital forensic readiness approach to WLAN digital forensics

Sipho Ngobeni, HS Venter & Ivan Burke

sngobeni@csir.co.za, hventer@cs.up.ac.za, iburke@csir.co.za

Information and Computer Security Architecture Research Group (ICSA)

Department of Computer Science

University of Pretoria

Abstract

Over the past decade, wireless mobile communication technology based on IEEE 802.11 Wireless Local Area Networks (WLANs) has been adopted worldwide on a large scale, resulting in the increase of the wireless users. However, as the number of wireless users soars, so does the possibility of cyber crime over WLANs, where cyber criminals deliberately and actively break into WLANs with the intent to cause harm or eavesdrop on sensitive information. To respond to cyber crime in wireless environments, WLAN digital forensics is seen as not only a counterproposal but as a solution to the rapid increase of cyber crime in WLANs. The key issue impacting WLAN digital forensics is that, it is an enormous challenge to intercept and preserve all the communications generated by the communicating mobile devices and conduct a proper digital forensic investigation. Thus, WLANs are not forensically ready. In other words, currently one cannot gather enough evidence that can be used for subsequent digital forensic purposes. To attend to this issue, this paper proposes a Wireless Forensic Readiness Model (WFRM) with the capability of monitoring, logging and preserving wireless network traffic to be used in a subsequent digital forensic investigation. A prototype implementation of the WFRM is then presented as a proof of concept.