RIPPS: Rogue Identifying Packet Payload Slicer Detecting Unauthorized Wireless Hosts Through Network Traffic Conditioning

CHAD D. MANO, ANDREW BLAICH, QI LIAO, YINGXIN JIANG,
DAVID A. CIESLAK, DAVID C. SALYERS and AARON STRIEGEL
Department of Computer Science & Engineering, University of Notre Dame

Wireless network access has become an integral part of computing both at home and at the workplace. The convenience of wireless network access at work may be extremely beneficial to employees, but can be a burden to network security personnel. This burden is magnified by the threat of inexpensive wireless access points being installed in a network without the knowledge of network administrators. These devices, termed *Rogue Wireless Access Points*, may allow a malicious outsider to access valuable network resources, including confidential communication and other stored data. For this reason, wireless connectivity detection is an essential capability, but remains a difficult problem. We present a method of detecting wireless hosts using a local RTT metric and a novel packet payload slicing technique. The local RTT metric provides the means to identify physical transmission media while packet payload slicing conditions network traffic to enhance the accuracy of the detections. Most importantly, the packet payload slicing method is transparent to both clients and servers and does not require direct communication between the monitoring system and monitored hosts.

Categories and Subject Descriptors: C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Network Communications*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms: Management, Measurement, Security

Additional Key Words and Phrases: Network Security, Rogue Systems, Traffic Conditioning

1. INTRODUCTION

Computer security is a critical component of business operations for companies ranging from small businesses to international conglomerates. The threat of a malicious intruder forces network administration personnel to devote a significant portion of time to the detection of unauthorized users and the securing of network resources. Success is dependent on the vigilant deployment of security devices such

Author's address: C. D. Mano, Utah State University, Department of Computer Science, A. Blaich, Q. Liao, Y. Jiang, D. A. Cieslak, D. C. Salyers, A. D. Striegel, University of Notre Dame, Department of Computer Science and Engineering, Notre Dame, IN 46556.
This research was supported in part by the National Science Foundation through the grant CNS03-47392.