Technische Universität München
Lehrstuhl für Netzarchitekturen und Netzdienste
Prof. Dr. Georg Carle

Thesis (B.Sc./M.Sc.)

Looking for SSH Phishers, compromised hosts and weak keys

Motivation

The Secure Shell (SSH) is a protocol on the Application Layer that is used to establish secure channels between two hosts on the Internet. It is most commonly used for remote login to UNIX machines. However, it can in principle also be used to secure any other protocol.

In December 2008, it turned out that a bug in the Debian Linux distribution had caused a large number of hosts to use insecure keys. Even now, not all administrators seem to have woken up to the problem. In December 2009, another curious incident was reported. Someone had registered a large number of “typo domains” like tu-munchen.de and installed SSH daemons to capture incoming connections – useful to retrieve passwords from unsuspecting users. This was feasible because SSH is commonly used with a Trust On First Use model where the first connection to a new host is considered secure and the host key then stored for later comparison. Unfortunately, many users seem not to react to sudden changes in the host key.

In this work, we will analyse the threats that are due to these incidents. We will **conduct scans** of a plentitude of Internet hosts and we will **monitor traffic streams** for weak host keys.

Your Task

Your task consists of the following two steps.

First, you will implement a scanner that uses openssh to scan a wide range of hosts and stores their host keys in a database. We have already implemented a tool that will help you generate typo domain names. The scan will be executed several times.

Second, you will use our local traffic monitor to find out how often weak keys are still used, and by whom (which source network, destinations, etc.).

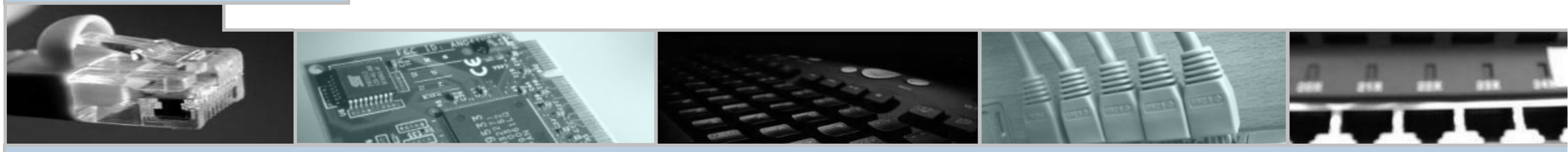
The result of your work will be both a report on the state of SSH security as well as a tool set that helps with assessing SSH security in the local network.

Requirements

We will program in Python and C++, so some programming skill and some knowledge of the languages is useful. Also, you might have to inspect SSH packets with wireshark and optimise our monitoring tool. Above everything, however, we appreciate **passion**: we want someone who enjoys his work and is motivated to participate in our research.

Keywords

OpenSSH, Network Security



Ralph Holz, Marc Fouquet, Lothar Braun
holz@net.in.tum.de, braun@net.in.tum.de