Measuring Security Threats with Honeypot Technology

Maximillian Dornseif Thorsten Holz Juliane Mathes Ingo Weisemöller
Laboratory for Dependable Distributed Systems
RWTH Aachen University

Abstract: *Honeypots* are electronic baits, i.e. network resources (computers, routers, switches, etc.) deployed to be probed, attacked and compromised. Honeypots run special software which permanently collects data about the system behavior and greatly aids in post-incident computer and network forensics. Several honeypots can be assembled into networks of honeypots called *honeynets*. Through the wealth of data collected by them, honeynets are considered a useful tool to learn more about attack patterns and attacker behavior in real networks.

Traditionally, information security has been purely defensive. Examples for the defensive mechanisms used in order to protect communication networks include firewalls, intrusion detection systems (IDS) and encryption. The strategy follows the classical security paradigm of „Protect, Detect and React“: Try to *protect* the network as best as possible, *detect* any failures in the defense, and then *react* to those failures. The problem with this approach is that the attacker has the initiative, being always one step ahead.

Honeypots – „a security resource whose value lies in being probed, attacked, or compromised“ – are a new approach in security research which attempt to change the defensive procedures. The primary purpose of a honeypot is to proactive gather information about security threats that exist in communication networks. A honeypot provides a real system with applications and services for attackers to interact with, but it has no production value. It is extensively monitored, all network traffic is captured and all information is logged. Since it has no production value, any interaction with a honeypot implies malicious or unauthorized activity and one can gain information about security threats in this manner. Therefore, honeypots can be used as electronic baits to attract attackers and study their behavior. In contrast to previous work in this area which collected data in an ad-hoc, post-incident manner, honeypots offer a more systematic approach to study attack patterns and general vulnerability assessment.

Honeynets placed inside the security perimeter usually do not only have a zero false positive rate but also have the ability to easily detect behavior patterns being very hard to detect with traditional, perimeter centered security systems.

Work by Thorsten Holz was supported by the Deutsche Forschungsgemeinschaft (DFG) as part of the Graduiertenkolleg „Software for mobile communication systems“.

To investigate the usefulness of honeynet technology and provide a solid scientific foundation for further work on honeynets, we have deployed a honeynet at RWTH Aachen University within the Laboratory for Dependable Distributed Systems.

We developed the idea of honeypots further and use them to measure security threats in communication networks. The classical setup for honeypots is a so called *honeynet*, a network consisting of several honeypots. Each honeypot is a real computer system with some usually old version of an operation system and some service like a Web- or FTP-server. It is extensively monitored with the help of a kernel module and all information flow in the network is captured via a so-called *honeywall*. Deployment is eased by virtual honeynets, in which a virtual machine like VMware is used to run a honeynet on a single host.

We devised some other forms of honeypot technology, to broaden the scope of data gathered by the honeynet approach:

- *HoneyDSL* – a DSL router with added honeypot capabilities.

  Incoming connection are redirected to simulated services. Break-in attempts on this services are recorded and gathered at a central server. HoneyDSL creates the capability to not only monitor attacks which occur to home users while surfing but also to analyze unwanted traffic reaching VPN-connected home office users. By analyzing in principle legitimate traffic like HTTP we also might correlate events like visits of certain websites or download of certain programs and illegitimate network activity. Such analysis of user initiated traffic is faced with serious technical but also privacy-related problems which need further research.

- *hProbe* – a quasi-transparent inline device adding honeynet capabilities to arbitrary networks.

  It is placed in front of an existing network and can claim unused IP addresses but also unused ports on addresses used by machines in the network behind the hProbe.

- *distHoneysty* - infrastructure for zero maintenance deployment of arbitrary many honeypots.

  distHoneysty offers the possibility to easily deploy hundreds of honeypots geographically dispatched and maintained by different organizations. Special care is taken so that the exact configuration of the whole system can be recreated for every point back in time and to keep clear trust boundaries.

- Advanced monitoring methods to monitor intruders actions in more detail while being less detectable. Such technologies would be based on specialized hardware which also could be used for forensic purposes.

A major challenge of our further research is to get an understanding why the results of our honeynet differ that much from the results published by the operators of other honeynets. The methods outlined above will provide us with a much more diverse view on the Internet.