With this poster, we present our SSH Intrusion Detection System named SSHCure: it is the first IDS capable of distinguishing successful attacks from unsuccessful attacks, thus detecting actual compromises. As powerful as SSH is to administrators, as attractive it is to anyone with malicious intents. Measurements showing more than 700 attacks on NRENs per day emphasize this. This number is also the source of the main problem in existing detection systems: while 699 of these attacks are typically unsuccessful and therefore not interesting to network administrators or CSIRT members, a single successful one is. And its consequences possibly include severe damage to the target hosts themselves, others hosts in the network, or even the network itself: an NREN should be informed as quickly as possible when this happens, so adequate actions can be undertaken.

In SSHCure, we implement a detection algorithm based on flow export technologies, i.e. NetFlow and IPFIX. A flow-based approach offers clear performance benefits over packet-based approaches in large-scale networks. The packet payloads are not available in flow data, making it more privacy preserving, while the loss of information (in comparison to a packet-based approach) is limited due to the encrypted nature of SSH. We show however, that flow data offers sufficient information to perform accurate detection. Moreover, flow export technologies are widely available on high-end networking devices. SSHCure is a plugin for NfSen – a flow collector for NetFlow and IPFIX, used by many in the NREN community – and therefore easy to install and use within all kinds of networks. The adoption of SSHCure underlines this, as it is currently deployed at several large commercial ISPs, CERTs and NRENs. All of these types of organizations need to be able to act swiftly when a compromise has been observed, and SSHCure is designed to support in that: the web-interface offers clear insight on the situation, including detailed information on both attacker and targets, comprehensible visualisations of network flows, and raw flow data for extensive analysis if needed. This is backed up by a flexible notification system, and (currently under development) integration with incident reporting systems via standard protocols (e.g. IODEF or X-ARF).

SSHCure, available via Sourceforge [1], has been in development for 2.5 years, and is still actively being developed and supported. The first prototype was presented at the Autonomous Infrastructure, Management and Security conference (AIMS) in 2012 [2], and promising results were achieved. With the latest available version, we performed extensive validation using datasets from both campus and backbone networks. Results show detection rates up to 100%.

By presenting our poster at TNC, we hope to expand our audience and explain how NRENs can benefit from SSHCure in their operations.

References
