Introduction

Goal
- To break the isolation property of System Virtual Machines. Examine whether processes running on a guest OS can usefully profile activity on other guest OSes or the host OS without having to raise their own privilege level.

State of the Art
- System Virtual Machines are becoming the norm in large scale server environments.
- The Xen project has been getting more and more credit from the community and is now one of the leading virtualization projects.
- The Xen architecture is composed of a Hypervisor, a privileged domain (the dom0) and a range of unprivileged domains (the domUs).
- Attacks aimed at raising privileges by exploiting dom0 vulnerabilities or at backdooring/profiling the system from inside dom0 have already been presented.

Breaking Isolation
- We identified three design issues that can be exploited to break the isolation property and attack other guests. They allow to us to:
  - Count the number of live guests on the same physical host and discover their domain identification.
  - Know exactly whenever a target domain is performing a set of actions like booting, shutting down, or reclaiming memory.
  - Identify the IP address of domains running on the same physical host.
  - Play Intrusion and Evasion tricks against a NIDS (Network Intrusion Detection System) running on dom0.

Advanced DHCP attacks
- The vulnerabilities described can be used to improve the traditional DHCP spoof attack.
- The time of the attack can be precisely chosen (no need to have a rogue DHCP always on).
- The transaction ID can be predicted and thus the race “won in advance”.
- All our attacks have been implemented in a single, highly automated tool: xenophobia.
- The Xen code is well structured, easy to read and designed with security in mind (the number of lines in the hypervisor code has decreased with each release!).
- The presented DHCP attack works only in a specific (but quite common) network configuration: guests must have a static MAC address.
- The checksum attack applies to paravirtualized guests. HVM (Hardware-assisted virtualized) guests that use paravirtualized network drivers may be vulnerable too.

The xenophobia tool

Conclusion
- The Xen code is well structured, easy to read and designed with security in mind (the number of lines in the hypervisor code has decreased with each release!).
- The presented DHCP attack works only in a specific (but quite common) network configuration: guests must have a static MAC address.
- The checksum attack applies to paravirtualized guests. HVM (Hardware-assisted virtualized) guests that use paravirtualized network drivers may be vulnerable too.

Further Information
- The Xen security team has been notified of the issues and potential solutions have been proposed.
- Contact: Enrico Perla (perlae@tcd.ie) or Stephen Farrell (stephen.farrell@cs.tcd.ie)

M.Sc. in Computer Science
(Networks and Distributed Systems)