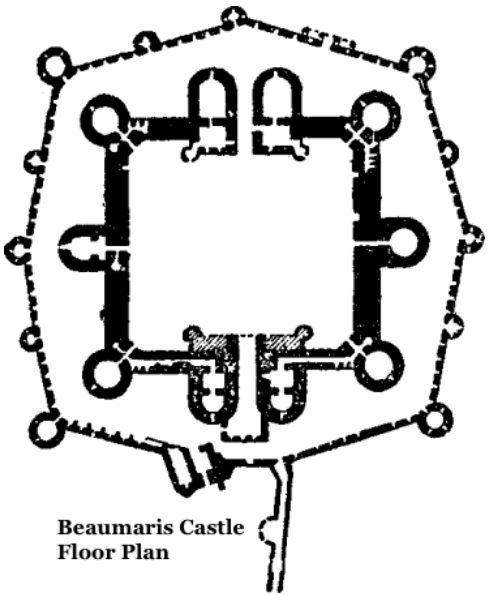
Demote those Security Bugs with a Hardened System Profile

Presentation Outline

Context: Operational Environment

- Organizational Ethics
  - Policies
  - Controls
  - Monitoring
- Insider Threats
  - Education and Training
- Untrusted Networks
  - Can you have a "trusted" system?
- Minimal Attack Surface
  - Complexity
- Default Deny
- *Defense-in-Depth*
- Reduce Exposure
  - Compartmentalization
  - Least Privelege
  - Insecure-Bootstrap Principle
- Input Validation

Defense-in-Depth



The principle of defense-in-depth is that layered security mechanisms increase security of the system as a whole. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system.

Proactive vs. Reactive

Example: Potential 0-day Kernel Exploit

Mishandled Object References in Kernel Keyring - A 0-day local privilege escalation vulnerability has been identified by the perception point research team. It has been reported that a vulnerability in the keyring facility possibly leads to a local privilege escalation.

- CVE 2016-0728
  - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0728
- Original Report
  - http://tinyurl.com/2016-0728

Typical Vendor Responses:

- RedHat, MRG 2 and RHEL 7
  - https://bugzilla.redhat.com/show_bug.cgi?id=1297475
- Gentoo Linux (gentoo-sources, all stable versions)
  - https://bugs.gentoo.org/show_bug.cgi?id=572384
- Suse Enterprise 11 and below
  - https://www.suse.com/security/cve/CVE-2016-0728.html

Hardened response - hardened-sources with default settings (in particular CONFIG_PAX_REFCOUNT) significantly reduces the effect of this issue to a local DoS rather than a privelege escalation.

What is PAX?

PAX Kernel Patches and User Tools

Hardened Toolchain

What Does PAX Do?

Resources

Hardened Project

- https://wiki.gentoo.org/wiki/Hardened/Introduction_to_Hardened_Gentoo
- https://wiki.gentoo.org/wiki/Hardened/Introduction_to_Position_Independent_Code
- https://wiki.gentoo.org/wiki/Hardened/PaX_Quickstart
- https://wiki.gentoo.org/wiki/Hardened/Grsecurity2_Quickstart
- https://wiki.gentoo.org/wiki/Hardened/Grsecurity_Trusted_Path_Execution
- https://wiki.gentoo.org/wiki/Hardened/Toolchain
- https://wiki.gentoo.org/wiki/Hardened/GNU_stack_quickstart
- https://wiki.gentoo.org/wiki/Hardened/Textrels_Guide
- https://wiki.gentoo.org/wiki/Hardened/PaX_Utilities
- https://wiki.gentoo.org/wiki/Hardened/Overview_of_POSIX_capabilities
- https://wiki.gentoo.org/wiki/Hardened/Position_Independent_Code_internals

Subprojects

- https://wiki.gentoo.org/wiki/Project:Hardened_musl
- https://wiki.gentoo.org/wiki/Project:Hardened_uClibc
- https://wiki.gentoo.org/wiki/Project:Integrity
- https://wiki.gentoo.org/wiki/Project:RSBAC
- https://wiki.gentoo.org/wiki/Project:SELinux

References and Specifications

Huang, Olson and Moore, Lightweight Communications and Marshalling for Low-latency Interprocess Communication. MIT CSAIL Technical Report, 2009.

Lorenz Meier, Petri Tanskanen, Lionel Heng, Gim Hee Lee, Friedrich Fraundorfer, and Marc Pollefeys. Pixhawk: A micro aerial vehicle design for autonomous flight using onboard computer vision. Autonomous Robots (AURO), 2012.

License and Thanks!

Author: Stephen L Arnold
Contact: answers@vctlabs.com

Revision: 0.1
Date: 2016-02-11T22:40:06,716796648-0800