Linux Kernel Security: Overview of Security Features and Hardening

Webinar Q&A Document
February 25, 2021

1. **Are the settings used in the presentation the recommended values?**

   Yes, everything presented will enhance your kernel security. It's ultimately up to you to determine if the cost of using the option is too great for your system (too much added CPU overhead, too much maintenance burden, etc.).

2. **Where can I see the default value of the option?**

   The default value is in the kernel source's many Kconfig files. If you look at a sample Kconfig file (https://github.com/torvalds/linux/blob/master/drivers/i2c/Kconfig), you'll see some of them say "default y". This means they are defaulted to yes (on).

3. **NXP offers (patched) kernels as part of its BSPs and with it, a default config. Would you consider it safe to deviate from the hardware vendor BSP kernel default config by enabling/disabling certain options?**

   Yes, the patched kernels have not been hardened as much as possible. They try to give a decent universal configuration, but there's definitely more that can be set to increase security.

4. **There was no mention of iptables or network hardening. Are there any recommended settings for improving network related security?**

   The upcoming webinar, "Linux System Hardening: Securing your embedded device from the risk of being compromised," being held on May 6th (https://www.timesys.com/software-services/software-development-training/self-directed/webinars/), will cover parts of network and system hardening best practices.

5. **What performance hits will you take with the memory protections enabled?**

   There is some inherent overhead added to the CPU in terms of additional CPU instruction cycles. The holistic impact depends on too many variables to say specifically, such as how much memory protection, processor speed, use cases, etc. It's best to see what the impact is by profiling it on your system/board.

6. **From a kernel security point of view, are there any settings or configurations that can be done at run time?**

   Yes, these are called system controls and they can be modified via the sysctl tool. This is briefly discussed one slide later on in the presentation. https://linux.die.net/man/8/sysctl

7. **Configuration settings are during building kernel, but how can I check post configurations?**

   You can use the following command on a running operating system to see what has been set:

   ```
   $ cat /proc/config.gz | gunzip -c
   ```

8. **What is meta-security in Yocto? Is it useful?**

   meta-security is a collection of generic security tools ranging from penetration testing to hardening tools to implement aspects of Linux security.

   The Timesys tools are complementary to meta-security and enhance the security of your BSP while making it easy to use. In addition to the tools available in the Timesys Yocto layer, it specifically implements Secure By Design features such as secure boot, chain of trust, data encryption, secure OTA, and system hardening for the NXP BSP which are not available in the meta-security layer.

9. **Is this specific to Arm architecture?**

   While this presentation covers kernel hardening concepts for both Arm and x86, the tools we have developed can report hardening options specific to Arm.

10. **What's the difference between CVE scan results from Vigiles and Yocto's own cve check? Is it that Vigiles takes into account the actual kernel config?**

    The Yocto cve check tool relies on the NVD database which is subject to various inaccuracies when it comes to CPE data (affected versions and products). The limitations of Yocto's cve check solution is discussed here: https://elinux.org/images/0/0a/Open-Source-CVE-Monitoring-and-Management-V3.pdf.

    Vigiles uses a curated database with multiple sources reviewed by Timesys' Security team, thus reducing false positives by 75+% while increasing coverage by 40+% compared to open source tools. In addition, Vigiles is a complete end-to-end vulnerability management tool that includes:

    - Intelligent filters based on attack vectors, severity, architecture, kernel/u-boot config
    - Information on fixes / mitigation
    - Email notification for new vulnerabilities
    - Team collaboration for assessing CVEs, sharing reports, managing products
    - Complete workflow management for tracking releases, comparing reports, Jira integration and more.

    In summary, Vigiles is a tool geared toward reducing time and effort managing vulnerabilities while enhancing the security of your product. You can find more details at: https://www.timesys.com/security/vigiles-vulnerability-management-patch-monitoring/options-pricing/.

11. **Is VigiShield open source?**

    VigiShield is a product offering from Timesys that is currently only available for purchase. However, if you are interested in a sample report for kernel hardening, please contact security@timesys.com.

12. **Does the Timesys Vigiles tool also work with Android builds?**

    The kernel hardening checker part is applicable to both Android and Linux kernel. The Vigiles vulnerability monitoring and management tool works out of the box for Yocto / Buildroot. For Android, the end user is required to generate a software bill of materials (SBOM) which can then be uploaded to Vigiles to get a list of vulnerabilities.

13. **How does Vigiles compare to Black Duck?**

Vigiles is optimized for embedded systems, and it saves 75+% time/effort in managing vulnerabilities by reducing false positives compared to Black Duck. It does so by:

- Using highly accurate, curated vulnerability data specific to Linux open source components,
- Integrating with the Yocto build system, enabling Vigiles to track already patched vulnerabilities and
- Filtering out vulnerabilities not applicable based on Linux/U-Boot config.

Vigiles was developed with the embedded developer workflow in mind, so it makes vulnerability monitoring for Yocto easy. To learn more about generic binary scanners vs. Vigiles, visit https://www.timesys.com/security/evaluating-vulnerability-tools-embedded-linux-devices/.

14. **Where can I find the Timesys tools discussed?**

Vigiles can be found at https://github.com/TimesysGit/meta-timesys, and it also comes pre-integrated with your NXP BSP.

For kernel hardening and DAC check tools, please contact security@timesys.com.

15. **Is "linuxlink.timesys.com" open to public?**

Yes, anyone can register on linuxlink.timesys.com for a free Vigiles account and generate security reports, access Vigiles documents, videos, and sample reports.

16. **Is there a detailed, in-depth video tutorial available for security by design?**

Past webinars which cover various Secure by Design topics can be viewed at: https://www.timesys.com/software-services/software-development-training/self-directed/webinars/

If you're interested in in-depth hands-on training on these topics, please contact sales@timesys.com.

https://www.nxp.com/support/support/nxp-engineering-services/vigiles-software-keeping-your-linux-bsp-secure:VIGILES

https://community.nxp.com/community/oss-security-maintenance