MONTAVISTA SOFTWARE

Application Note:

Implementing NIST's Zero Trust Architecture with MontaVista Linux-based Resilient Embedded Systems

Introduction

With a history of more than 20 years, **MontaVista Software** is proud to be empowering millions of devices across industries worldwide. Some of the world's leading companies like Ericsson, Nokia, Mavenir and Grundfos have integrated **MontaVista's Carrier Grade eXpress (CGX) Linux** into their core technical system to utilize its design which emphasizes robustness, connectivity, and security in mission critical Telco Platforms, Medical Technology Systems, and Global, Resilient Industrial and Robotic Manufacturing environments.

This document discusses the concept of **Zero Trust Architecture (ZTA)** and shows how MontaVista can help our partners implement a **ZTA** for their mission-critical applications according to the guidelines from the **National Institute of Standards and Technology (NIST)**, part of the U.S. Department of Commerce. The reader is expected to have some familiarity with the **NIST SP 800-207** document.

The primary solution we present here is MontaVista's CGX Linux, since it commonly provides an operating environment base for our customer programs.

Solution Description

As discussed in the **NIST SP 800-207** document, ZTA is not a set of methods, but a set of principles, or tenets, that if followed create a more secure system. These tenets need application to a system to create the requirements to secure the system.

The requirements require tools to implement. Below we discuss the tenets and their applications. The NIST's document goes into more depth about what these tenets are. Here we focus on what needs to be done to meet these tenets.

1. All data sources and computing services are considered resources.

This requires modeling your system to know all the resources in the system and how they are accessed and by whom they are accessed. Modeling can be formal or informal, but needs to be done to discover where you need these tenants applied. Modeling should consider the internal and external threats the system might encounter, both from humans and from automated systems.

2. All communication is secured regardless of network location.

Here the central tenant of ZTA comes into play. All access to all resources must be secured. The network no longer has a perimeter where things inside it are open. Nothing is open. Once you have a model of your system, you can use it to determine everything that needs to be secured.

CGX provides many tools for this purpose. It has TLS libraries like OpenSSL or mbed that can be used for base security. It has tools like stunnel for securing connections for programs that don't do this by default. And it has various higher-level tools for securing HTTP connections through various web servers and SSH for login type services.

Many things that may not be obvious at first, including DNS, NTP, and DHCP, also need to be secured. And CGX has tools for these purposes.

3. Access to individual enterprise resources is granted on a per-session basis.

No. “Once you are trusted you are always trusted.” Again, the modeling should make clear the places that need to be access controlled and secured.

The best practice authentication comes through Public Key (PK) cryptography. And the same tools that facilitate secure connections provide authentication through PK.

4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

This tenet introduces the concept of dynamic policy: Policy for access control may depend on dynamic system state. Network operators or even software in the system may discover things happening dynamically and that can change access control. For instance, a network monitoring system may discover an active port scan and temporarily disable access to resources from that IP address.

SELinux is one solution in CGX that provides the fine-grained access control for principle of least privilege. MontaVista always suggests an approach where a system administrator configures the minimal capabilities available to accessible applications to limit exposure if compromised. Though powerful, SELinux can be challenging to implement, especially in systems with limited resources. MontaVista has experience implementing SELinux in heavily constrained systems.

In addition, this tenant requires dynamic automated configuration of the system, which has to, of course, be secured.

MontaVista provides NETCONF/RESTCONF interfaces with the clixon application. It delivers a standards-based modular modeling language based interface to configuration accessed through SSH or TLS. The fluentbit tool for log aggregation can also do log analysis and take actions based on system activity.

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

In order to implement tenant 4, a system has to have information about its operational state.

Good news is that CGX offers samhain, suricata, and many other tools for measuring the network and local system integrity.

6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

More of an operation philosophy than something a tool can help with, but as per the modeling and ZTA principles, no interface inside the system or into the system can be accessed without proper authentication. No exceptions.

7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Beyond just the network and local system monitoring done by each part of the system through the tools mentioned in tenant 5, the system logs and application logs need to be sent to upstream enterprise systems that can collect and analyze all the information, looking for possible issues and perhaps seeing issues before they become a problem. Local analysis may also be done and local measures taken, too.

CGX delivers fluentbit for receiving logs from many sources, possibly filtering and acting on logs, and aggregating those logs to many different enterprise monitoring systems.

Summary

This document has discussed the tenants of ZTA at a high level and some of the tools MontaVista's CGX Linux brings to the table to meet the requirements that will be generated by modeling. Other documentations from MontaVista will discuss how to do modeling, how to take that modeling and apply it to discover requirements, and how to take those requirements and the available tools to meet the security goals of the system.

In addition, MontaVista has a Secure Gateway product that provides a complete turn-key secure system, following the ZTA principles and implementing other security principles such as trusted boot, over-the-air (OTA) updates, mandatory access control (MAC), VPNs, and firewalling, as a base platform for developing applications. All these security tools are available on base CGX, but the Secure Gateway provides a pre-integrated platform with all though already configured and thought through.

Further, MontaVista's supported Kubernetes solution, MVKube, runs seamlessly on this platform and on devices inside networks the gateway protects. As a versatile solution, MVKube allows customers to run their existing Kubernetes cluster applications with professional support and security configuration or turn to our experts for an end-to-end cluster deployment service.

If you are looking for a secure, reliable, and connected OS platform, MontaVista's CGX Linux meets all of these demands and more. Harness MontaVista's CGX Linux and unique expertise for your next-gen resilient and scalable embedded applications today!

Please visit www.mvista.com and/or contact us at sales@mvista.com for more information on our Products and Solutions.

MontaVista Software, LLC, is a leader in embedded Linux commercialization.

For over 20 years, MontaVista has been helping Linux developers get the most out of open source by adding commercial quality, integration, hardware enablement, expert support, and the expert resources of the MontaVista development community. Because MontaVista customers enjoy faster time-to-market, more competitive device functionality, and lower total cost, more devices have been deployed with MontaVista than with any other Linux.

For more information about MontaVista, visit http://www.mvista.com

Media Contact:
MontaVista Software LLC | E: pr-contact@mvista.com | T: +1 (669) 777-6841

**Linux® is a registered trademark of Linus Torvalds in the United States and other countries.*
MontaVista® is a registered trademark of MontaVista Software, LLC.
All other names mentioned are trademarks, registered trademarks or service marks of their respective owners.