BUILDING BLOCK

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

TRUSTED GEOLOCATION IN THE CLOUD

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of hardware and geolocation trust in the cloud through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Trusted Geolocation in the Cloud project, including background and challenge, goals, and potential benefits. If you would like to propose an alternative architecture or know of products that might be applicable to the challenge, please contact us at trusted-cloud-nccoe@nist.gov.

BACKGROUND

While cloud computing offers businesses and other organizations cost savings and flexibility, these shared resources can introduce security and privacy challenges. Enterprises that use cloud services want to be assured that:

- the cloud compute platform hosting their workload has not been modified or tampered with
- sensitive workloads on a multi-tenancy cloud platform are isolated within a logically defined environment from the workloads of competing companies
- workload migration occurs only between trusted clusters and within trusted data centers
- cloud servers are located in their preferred regions or home countries so that the cloud provider is subject to the same data security and privacy laws as the enterprise

CHALLENGE

Whenever multiple workloads are present on a single cloud server, there is a need to segregate those workloads so they do not interfere with each other, gain access to each other's sensitive data, or otherwise compromise the security or privacy of other workloads. As an example, consider two rival companies with workloads on a multi-tenancy cloud platform; each company would want to ensure that the server can be trusted to protect its information from the other company. Similarly, a single organization might have multiple workloads that need to be kept separate because of differing security requirements and needs for each workload, such as isolating a regulated workload from a public-facing workload.

Another concern with shared cloud computing is that workloads could move from cloud servers located in one country to servers in another country. Each country has its own laws for data security, privacy, and other aspects of information technology (IT). Because these laws may conflict with an organization's policies or mandates (e.g., laws, regulations), an organization may decide that it needs to restrict which cloud servers it uses based on its country.

GOALS

This project aims to demonstrate how to improve the security of cloud computing and accelerate the adoption of cloud computing technologies by establishing an automated hardware root of trust method for enforcing and monitoring geolocation restrictions for cloud servers. A hardware root of trust is an inherently trusted combination of hardware and firmware that maintains the integrity of the geolocation information and the platform. Once the cloud platform has been attested to be trustworthy and to comply with a defined geolocation policy, then other use properties can be instantiated to support additional security capabilities that are built on this foundational hardware root of trust. These capabilities can include restricting workloads to run on trusted hardware in a trusted location; restricting communications between workloads; ensuring workload data is protected at rest; applying security policies to workloads; and leveraging these capabilities across a hybrid cloud.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

BENEFITS

The potential business benefits of the solution explored by this project include:

- gain the benefits of dynamic cloud environments while still enforcing higher levels of protection for more critical or regulated workloads
- deploy and migrate cloud workloads between cloud servers within private and hybrid clouds
- detect unauthorized changes to the hypervisor/operating system or BIOS/UEFI in near-real-time
- ensure that the workloads are deployed to trusted platforms, thus reducing the chance of workload compromise
- ensure that the workloads are not migrated to a server in an unsuitable geographic location or non-regulated environment
- ensure that the workloads are decrypted on a server that meets the trust and geolocation or regulated workload policy
- meet the least privilege principle for network flow within a workload
- meet an industry sector-specific compliance framework by continuously enforcing and assessing the platform over the lifecycle of the cloud platforms and workloads

COMPONENT LIST

- commodity servers with hardware crypto module
- commodity network switches
- hypervisors
- operating systems
- application containers
- attestation server
- orchestration and management servers
- database servers
- directory servers
- software defined network
- data encryption and key management server
- cloud service

DOWNLOAD THE PROJECT DESCRIPTION

For more information about this project, visit: https://nccoe.nist.gov/projects/building-blocks/trusted-geolocation-in-the-cloud

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you are interested in contributing technology or expertise to this project, please email trusted-cloud-nccoe@nist.gov.