Operations & Management Area Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 30, 2012

S. Karavettil
ASTA Ventures, Inc.
B. Khasnabish
ZTE USA, Inc.
N. So
Tata Communications
W. Dong
Tektronix Communications
June 28, 2012

Security Framework for Virtualized Data Center Services
draft-karavettil-vdcs-security-framework-04.txt

Abstract

This document discusses the requirements and technology gaps related to security in the virtualized data center services (VDCS). The objective is to ensure end-to-end security for various types of carrier services built on virtualized infrastructure. The issues covered in this draft are focused on confidentiality and integrity of the services in the virtualized environment; including but not limited to infrastructure (IaaS), platform (PaaS), and application (SaaS) services. This draft also takes into account transient nature of identity, resources and connectivity in the virtualized environment.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 30, 2012.

Table of Contents

1. Introduction 4
2. Terminology and Abbreviation 5
3. Problem Statement and Examples 6
3.1. Virtualized Carrier Services Users 6
3.2. Data, Information and Knowledge Base Security Problem . . 6
3.3. Lack of mandatory Application Security in Protocol 8
4. Other Gaps in Existing Implementations & New Requirements . . 10
4.1. Systems Security Gaps & New Requirements 10
4.2. Network Security Gaps & New Requirements 10
4.3. Mobile Security Gaps & New Requirements 11
4.4. Physical Security Gaps & New Requirements 12
4.5. Operations & Management Security Gaps & New Requirements 12
4.6. Other New Requirements 13
5. Work Item for Consideration 15
5.1. Applications & Services 15
5.2. Infrastructure Operations & Management 15
6. Case Study 16
7. Security Considerations 17
8. Conclusion 18
9. Acknowledgement 19
10. IANA Considerations 20
11. References 21
Authors' Addresses 22

1. Introduction

The VDCS Security Framework is a reference framework to build secure and interoperable services on top of a virtualized infrastructure. Currently there are a variety of infrastructure equipments (servers and network equipments), and operational management software (hypervisors and provisioning/monitoring applications) and software-as-a-service that are proprietary in nature; therefore, causing service interoperability issues and creating security gaps.

Developing protocol standards around virtualized services and the supporting infrastructures is an integral part of the overall end-to-end security assurance. This draft proposes a security framework and the associated requirements for Protocols, Profiles, Network Interfaces, Operations and Management, and Application Interfaces(APIs) in an environment where virtualized resources are shared among a variety of public and private subscribers/clients seamlessly.

The current applications and services using existing protocols (e.g., HTTP) that are in need of security measures in a multi-tenant virtualized environment are described. Similarly gaps in security implementation of inter-working protocols (e.g., inter-domain BGP, MPLS) among virtualized network infrastructure resources are identified here.

These help design, develop and provide secure, inter-operable and on demand integrated self-service applications and services for users from various vendors. This also helps to reduce human interventions

in provisioning and management of resources in a more standardized manner.

2. Terminology and Abbreviation

- CSA: Cloud Security Alliance
- CSF: Cloud Security Framework
- CSP: Cloud Service Provider
- CSRF: Cross-Site Request Forgery
- DCOPS: Data Center Operations
- DPI: Deep Packet Inspection
- ETSI: European Telecommunications Standards Institute
- GRC: Governance, Risk & Compliance
- HIPAA: Health Insurance Portability and Accountability Act
- LDAP: Lightweight Directory Access Protocol

- SQL: Structure Query Language
- OWASP: Open Web Application Security Project
- PCI: Payment Card Industry
- SDO: Standards Development Organizations
- SOX: Sarbanes Oxley
- VDCS: Virtualized Data Center Services
- VDI: Virtual Desktop Infrastructure
- VM: Virtual Machine
- VPN: Virtual Private Network
- XSS: Cross-Site Scripting

3. Problem Statement and Examples

The applications in virtualized carrier infrastructure often follow the Client-Server model. The Server is typically a Virtual Machine (VM) hosting various applications while performing the computing and storage functions on top of generic server hardware. The client is a remote machine connecting to the VM via virtual connection(s).

In this case, security means protecting the information (data and content) in an on demand self service multi-tenant virtualized infrastructure and communication between the client and virtual host from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

3.1. Virtualized Carrier Services Users

Security impacts all service users. User identity security and verification needs to occur in a synchronized fashion along the service path end-to-end. Understanding who the users are is the critical first step in understanding the security landscape. Here is the list of the users that the security framework has to consider.

- Consumers
  - Internet Application Services Users (Internet consumers across various internet applications)
  - Enterprise Users (across various Organizations of Enterprise)
  - Regulation & Compliance Auditors
  - Investigators & Forensic Experts
- Publishers
  - Developers
  - System Administrators, Network Administrators
  - Management Users

3.2. Data, Information and Knowledge Base Security Problem

Data, information, and knowledge represent three levels of abstraction. Data on its own carries no meaning. For data to become information, it must be interpreted and take on a meaning. When that information is interpreted and used practically to fulfill a purpose, it becomes knowledge.

The types of data include:

- Live
  - Web Application Form Data (Structured)
  - Audio

    * Video

- Archive
    * Database Data Structures
    * Files
        + Data - PDF, DOC, Excel, etc
        + Voice archive
        + Video Archive
    * Emails, Logs (unstructured)

Information security has to be developed to manage the lifecycle of data, including data security while in use, in motion or at rest within a virtualized infrastructure environment.

- Data/content/media (e.g. videos) authenticity
    * Association and identification of data to its owner (user, enterprise consumer, service provider, location, etc) and access privileges.
- Data while in use
    * Isolation of data while in use by the computing resources.
    * Management of the data usage based on access privileges of the users, enterprise consumer, and service providers.
- Data in motion
    * Restricting the data transmission across geographical boundaries based on government regulations or enterprise policies and configurations defined during self-service setup.

- Data at rest (monitoring and management)

* Data isolation in a multi-tenant environment to protect against side attack (across tenants) or admin attacks.

* Data migration managed as defined by enterprise/government policies.

* Deletion, loss/leakage, and location of data.

In traditional data center, data/content migrates from machine to machine and from storage devices to storage devices frequently, both in normal operations as well as during backup/restore processes. Some of the data that are deemed sensitive for security or regulatory reasons can be isolated and controlled through dedicated physical devices for storage/access, therefore relatively easy to secure. However, in a virtualized environment, VMs are set up, relocate, shut down dynamically on demand. The traditional physical-device-based isolation is no longer sufficient in the new paradigm.

Data residing in a cloud environment shall go through the same create/read/update/delete (CRUD) lifecycle as in all other cases. While the create/update of data are easily abstracted and handled by the cloud platform, the destruction of data in the cloud may be tricky, especially for security/regulatory compliance purposes. Often in these cases, cloud service providers must demonstrate complete destruction of data taking into account of the virtual machine migration and remote data center backups. Some of the data destructions may be conditional based on other factors, such as legal time limits. Therefore, there must be a data lifecycle management function in the cloud framework based on policies defined by the users that shall govern the create/read/update/delete/migrate functions of data.

3.3. Lack of mandatory Application Security in Protocol

HTTP is the most widely used application layer protocol. It functions as a request-response protocol in the client-server computing model.

A Web service is a method of communication between two electronic devices over a network. Web service is most widely implemented on top of HTTP protocol. There are specifications defined for Web Services like WS-Interoperability (WS-I), WS-Security, WS-Addressing, WS-Policy, WS-Reliable Messaging, etc.

The web services specifications has not yet been widely adopted in the application implementations, thus leaving security as a choice up

to the developers of the organizations developing various applications.

With the lack of mandatory security requirements there may be significant security gaps in these application implementations. Few use cases are mentioned here to exemplify the problem:

The user identity and their session state management within an application context are not mandated or controlled at the protocol level thus leading to broken user session and authentication hijacking issues from the client side.

There is also identity and access management problem due to a lack of standards, as the applications used by enterprises are spread between private and public cloud providers, the users have to be single-signed on and authorized with appropriate privileges to access these resources. A requirement to support multi-factor authentication among multiple cloud providers would significantly enhance the security of the application implementations.

Another significant aspect that can be addressed at the HTTP protocol level is by making it mandatory to perform data input validation and escaping of data to the browser to protect against attacks. This will be important in maintaining data integrity without the use of other API during application development. This helps to protect against security vulnerabilities like Cross-Site Scripting (XSS), Cross-Site Request Forgery and Injection (LDAP, SQL).

4. Other Gaps in Existing Implementations & New Requirements

These topics are mentioned here to address the completeness of the security framework where privileged users shall access or use the on demand self-service to run these applications & services in a tenant isolated and inter-operable virtualized environment. These may be elaborated later as seen fit in the context of IETF protocol gaps.

4.1. Systems Security Gaps & New Requirements

The inter-operability and information exchanges between systems in the organization domains across an enterprise or across related enterprises are affected due to lack of proper protocol, profile definitions and raises security concerns with certain approaches.

Transport channel encryption is a widely deployed security implementation. While this practice helps avoid man in the middle attack it prevents detection of malicious attacks that has got into the system from the client side browser.

Another challenge in todays' implementations and new requirements for developing interoperable solutions in a virtualized environment are key management in a client/host (cloud user and cloud provider) architecture spread across multiple providers. All the key exchange between enterprise and cloud shall be secured and protected. The system shall be able to support the end users (consumers, or enterprise) to hold the encryption keys and integrate with their existing key management. When they withdraw the encryption keys from the cloud, customers data in the cloud become inaccessible or unreadable. It shall be protected from side attack and admin attack such as snapshot VM to get the encryption keys. The system should be able to support standard key management protocols between encryption entity in the cloud and key manager in the enterprise domain such as KMIP.

These days with multi-platform devices, insufficient restrictions on virtualized resources access over the network increases exposure to attack from viruses, spyware, etc. These may also facilitate undesired access to cloud based virtualized resources. Host-based

firewalls do not obviate the need for network-based firewalls in the virtualized environment.

4.2. Network Security Gaps & New Requirements

- Develop security at the Protocol to accommodate various needs of the virtual infrastructure environments and applications running in that environment.

- Protect the channel using VPN enables secure communication between the client and the host.

- Cloud customers depend on functional networks to access their resources, and because networks are often not under the control of customers, there is a risk that the cloud may not be reachable.

- Network virtualization layer 3 firewalls will need enhancements to support to protect the perimeter from intruders, role-based access control policies to protect in flight traffic within the perimeter and intrusion detection and prevention.

- Connectivity resources (bandwidth) allocation for routing, VLAN and other network configuration to handle multiple customers.

4.3. Mobile Security Gaps & New Requirements

With the proliferation of mobile devices and the applications that are developed to serve the needs of consumers with better user experience it's becoming critical to protect the privacy and security of these users during the physical loss of these devices.

The data center operations infrastructure including the networks need becoming more and more application aware through deep packet inspection (DPI) this in turn leads to interesting privacy and regulatory compliance issues. The data in motion when flowing through the network may be analyzed for better application awareness but should be done with a short memory span and no data in temporary store to avoid legal ramifications.

Managing the identity of the user accessing a mobile device is critical to the safety and privacy of the user content. In addition

there're high chances for private data falling into the wrong hands via removable media access or local blue tooth connections that are not turned off.

In some instances where the mobile devices are physically lost it may be helpful to track the device to see if it's in hands of someone or retrieve important data from it remotely and destroy the content on the device for safety.

Another important requirement would be the ability to seamlessly provide content to authenticated and authorized users on their mobile platform during transit across various networks (from various network providers) without disruption of service. This content may also be viewed by authorized user via various display channels and be able to switch seamlessly from the mobile device in their hands or in their automobile across to their television or home personal computer.

Governance and regulatory compliance requires that certain sensitive data be managed within certain boundaries though the user and mobile device may be across the geographic boundaries. This is very common application in the healthcare industry.

Few security requirements in the mobile area include:

- End-point security (protect against removable media)
- Protect against Bluetooth Connections Access
- Encryption of data
- Protect session during service mobility
- Locating the mobile device and ability to break it
- Location awareness for data store irrespective of the mobility of source

4.4. Physical Security Gaps & New Requirements

- Access control - What is the basis for trusting the human cloud operators?

- Common operational picture that provides integrated view of various alarms, alerts and notifications from various physical devices like video surveillance cameras, motion sensors, access control card readers, etc.

- Role-based and privilege-based access to video surveillance content and alarm notifications.

- Perimeter security of the virtualized data center operations and provide real-time insight into security issues to the provider and to the enterprises using their services.

- Business hours based security monitoring of provider assets.

4.5. Operations & Management Security Gaps & New Requirements

- Discovery of network nodes both physical and virtual and their access privileges (for example using SNMPv3), their locations in a virtualized infrastructure spread out physically.

- Ability to manage both physical network resources and virtual network resources through a consistent Network Management console.

- Management of configurations across various systems, network equipments.

- Need clarity on security control roles and responsibilities.

- Backup and recovery of information (import/export across multiple CSPs).

- Business continuity and disaster recovery - how to maintain continuity of operations if cloud providers fail?

- Business continuity and disaster recovery - how to maintain continuity of operations by having redundancy across multiple service providers?

- Management & Configuration Security

- Governance, Risk & Compliance

    * Clear certification and accreditation guidelines

    * Clear e-discovery guidelines

    * Cloud audit assurance and log sensitivity management

    * Need for clarity on how 800-53-style control guides can work for the cloud

    * Need clear privacy guidelines

    * Lawful interception needs in the cloud virtualized service environment.

4.6. Other New Requirements

- Inter-operability across various vendor products that spans across the Client or Host layers.

- Multi-Cloud Services integrated application at different CSPs.

- Inter-Cloud Information Exchange between CSPs.

- Visibility for Customers - ability for customers to observe the health of their VM instance and general status of their workloads.

- Control for Customers during self service - ability for customers to maintain effective control their workloads even though the protection mechanisms and even locations of workloads may not be

known to customers.

- Protect virtual machines, network traffic, actual/residual data, and other resources of a tenant against unauthorized access by another tenant.

- Provide normal availability to tenants incase of failure of other tenant application, protect their data, and their identities.

- Computer Resource Allocation Services- ability to allocate System, Computing, Storage, Network resources in a virtualized

infrastructure environment.

5. Work Item for Consideration

The various applications and interworking protocols developed by the IETF MAY need to be extended or profiled to support the security

requirements of virtualized services and infrastructure environment.

5.1. Applications & Services

The most widely used protocol that is in use today for application & services development areas HTTP have been considered for the applications in the virtualized environment. The protocol may have to be profiled or extended with significant changes to be ready to handle the security requirements in a virtualized environment.

5.2. Infrastructure Operations & Management

The various security parameters related to operations and management of virtualized network resources in multiple administrative domains may need to be defined. The results of monitoring may need to be exchanged periodically to support the private and public virtualized domains and infrastructure in order to maintain the expected end-to-end security.

6. Case Study

Will be added in future. Looking forward to contributions in this area.

7. Security Considerations

This document discusses security for virtualized environment.

8. Conclusion

Over the last decade the times have changed from the exponential growth of the internet and the associated advances in technologies to the large scale adoption of connected devices.

With this advancement we are seeing the rapid rise in security threats and vulnerabilities to today's application and infrastructure.

It is time to take a look at existing protocols, API's not only for todays application and infrastructure but also to tackle the rising threats due to the use of same technologies and protocols for the virtualized applications and infrastructure environment development.

These shall not only cause security and interoperability problems, but may also negatively impact further development of protocols and services in this very important area of virtualized applications and networking infrastructure environment. IETF is the best organization to address these issues.

9. Acknowledgement

The authors would like to thank Zachary Zeltsan for his valuable review and comments on this document.The authors would also like to thank Tony Rutkowski for his useful suggestions on the document.

10. IANA Considerations

This document has no actions for IANA.

11. References

[CSA] "Cloud Security Alliance".

[ETSI] "European Telecommunications Standards Institute".

[ITU-T] "ITU-T Focus Group on Cloud Computing (FG Cloud), WA 1-3 Cloud security", June 2012.

[NCCRA] "NIST Cloud Computing Reference Architecture".

[NCSA] "NIST Cloud Security Architecture", June 2012.

[NIST] "National Institute of Standards and Technology".

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[SCIM] "System for Cross-Domain Identity Management", June 2012.

[draft-ietf-opsawg-firewalls-00.txt]
Baker, F., "On Firewalls in Internet Security", June 2012.

[draft-so-vpn-o-cs-00.txt]
So, N., "Draft Requirement and Framework for VPN-Oriented Cloud Services", March 2011.

[draft-wei-nvo3-security-framework-00.txt]
Wei, Y., "NVO3 Security Framework", June 2012.

Authors' Addresses

Suren Karavettil
ASTA Ventures, Inc.
32 Hatikva Way

Chelmsford, MA 01863
USA

Phone: +001-978-857-5461
Email: surenck@gmail.com

Bhumip Khasnabish
ZTE USA, Inc.
18 Patterson Road
Lexington, MA 02421
USA

Phone: +001-781-752-8003
Email: vumip1@gmail.com

Ning So
Tata Communications
2613 Fairbourne Cir.
Plano, TX 75082
USA

Phone: +001-972-955-0914
Email: ning.so@tatacommunications.com

Wei Dong
Tektronix Communications
3033 President Bush Hwy
Plano, TX 75075
USA

Phone: +001-469-330-4000
Email: wei.dong@tek.com