June 12, 2018

CONTEXT SENSITIVE NETWORK SECURITY SCORE

Swami Anantha

Byju Pularikkal

Santosh Patil

Sourav Chakraborty

CONTEXT SENSITIVE NETWORK SECURITY SCORE

AUTHORS:
Swami Anantha
Byju Pularikkal
Santosh Patil
Sourav Chakraborty

ABSTRACT

Techniques are described herein for quantifying a security impact of network vulnerabilities (e.g., hardware/software/configuration) on a network. The security impact quantification is calculated by weighting a configuration vulnerability score and an infrastructure security vulnerability score with a Vulnerability Reach Index (VRI). The VRI is an indication of the depth in the network of the impact of a vulnerability.

DETAILED DESCRIPTION

Currently, one of the main tasks of every network operator is to constantly monitor a network for security vulnerabilities and, eventually, to fix/address any identified vulnerabilities. In doing so, the network operator looks for vulnerabilities that may have been caused/introduced due to changes in the network. These vulnerabilities, for example, may be caused by updates that are regularly made to the network and network configuration. Such updates to the network may be made to support new applications/features/devices that are added, for example, to satisfy the needs of network consumers.

The network operator also looks at published security vulnerability notifications for different components in the network. The notifications are published with severity information for individual network elements (e.g., software/hardware). However, a security impact of the different components on the network has to be determined. For each security notification, the network operator determines whether the notification is applicable in the context of the network operator's network. The network operator also determines, for each security notification, the scope and priority/urgency for fixing the vulnerabilities associated with security notification in the context of the network operator's network.

The process to detect security vulnerabilities in the network, as well as to prioritize the scope, impact, and urgency of vulnerabilities associated with security notifications in the context of the operator's network, is complex and time consuming. Additionally, this process is potentially error prone. Moreover, it is undesirable for an operator to take the network offline for installation of a security patch that has limited/unknown impact.

Accordingly, techniques are described herein that address one or more problems associated with identifying, scoping, prioritizing and quantifying security vulnerabilities in the context of an operator's network. The presented techniques involve determining a security vulnerability score for a set of network elements, and the network as whole. More specifically, the presented techniques introduce the concept of “Vulnerability Reach,” which can be described as a determination (and potentially quantification) of how far into the network that a configuration vulnerability reaches. A mechanism is provided to create a prioritized list of network elements and vulnerabilities that are first addressed.

Techniques described herein are employed to calculate and present a quantifiable metric of security vulnerabilities of a network and/or part of a network (e.g., a site).

A network security vulnerability metric (NetSecScore) may be calculated. The NetSecScore may be calculated by identifying vulnerabilities in the network element configurations in the context of the network and network topology. Specifically, this may include calculating a security risk posed by a network element's configuration, which may depend on a location of the network element is in the network.

A configuration vulnerability score may be combined with the hardware, software and operating system (OS) vulnerabilities.

A security score may be weighted with a Vulnerability Reach Index (VRI). A VRI of a network element is a measure of how far a security vulnerability in a network element has reached into a network. The VRI of one or more network elements can be used to bound the impact of a security breach and hence prioritize its importance.

Quantifying security vulnerabilities in a network involves creating a Context Sensitive Network Secure Score (NetSecScore) by combining a Config NetSecScore and a Infra NetSecScore. The Config NetSecScore is calculated using, for example, network and network component configuration vulnerability parameters. The Infra NetSecScore is calculated using, for example, infrastructure vulnerability parameters.

A prioritized list of vulnerable network elements that need to be patched is created. The prioritized list may be created using the combined Config NetSecScore and Infra NetSecScore of each network element.

Calculating the Config NetSecScore and the Infra NetSecScore is described in more detail below. More specifically, calculating the Config NetSecScore may involve determining configuration related security vulnerabilities for each network element. The configuration related security vulnerabilities can be determined using the following parameters: network access; and/or client and Internet of Things (IoT) access.

Network access parameters may include a list of open ports. The list of ports may include ports that can be accessed by external components to access the network. For example, every port that is opened to allow external components to access the network is a potential security risk. The list of ports may also include ports that can be accessed by internal components to go out of the network. For example, every port that is opened to allow a tunnel creation is a potential security risk. This is because it allows internal access from the other side of the tunnel. Network access parameters may also include a strength of network device passwords. Network access parameters may also include an absence or presence of a firewall on a network element. An absence of a firewall on a network element with public interfaces is a security risk.

Client and IoT access parameters may include wired and/or wireless client access mechanisms. For example, open unsecured access by wired and/or wireless clients is penalized. Client and IoT parameters may also include wired and/or wireless client authentication mechanisms. For example, token based authentication is given a better security score than password based authentication. Client and IoT parameters may also include a strength of client access passwords.

The configuration related security vulnerabilities in a network element are used to create a Config NetSecScore for the network element. Each network component Config NetSecScore is weighted based on the network element's location in the network topology and how the network element is connected to the other network elements. In other words, each network component Config NetSecScore can be weighted using the following weights: Topology Location Weight; and/or Vulnerability Reach Index.

The Topology Location Weight may include a weight for internal devices. Internal devices are devices inside a private network (e.g., a switch inside a private network). Vulnerabilities on these devices pose a lower security risk. Therefore, these devices have a lower weight.

The Topology Location Weight may also include a weight for network access devices. These are devices at the edge of the network with public interfaces (e.g., a wide area network (WAN) router). Vulnerabilities on these devices pose a higher security risk. Therefore, they have a higher weight.

The Topology Location Weight may also include a weight for client and IoT access devices (e.g., an access point, an IoT device). Vulnerabilities on these devices pose a higher security risk. Therefore, they have a higher weight.

The VRI may be weighted by a security risk weight, which is added for a network element that has a high VRI. VRI of a network element is the number of network elements that can be reached in one or more hops from the network element via a common virtual land area network (VLAN) and/or subnet.

Calculating the Infra NetSecScore may involve determining infrastructure related security vulnerabilities of each network element. The infrastructure related security vulnerabilities of each network element can be determined using Network Infra parameters and Security Notification parameters.

The Network Infra parameters may include hardware authentication. For example, devices that have hardware security modules or secured chips with device authentication certificates and/or device authentication functionality pose less of a security threat. These parameters may also include hardware chipset vulnerability. For example, devices with chipsets that are susceptible to Meltdown and/or Spectre pose a higher security threat. The Network Infra parameters may also include software and/or operating system (OS) vulnerabilities.

The Security Notification parameters may include parameter values that are based on severity levels of security notifications (e.g., Product Security Incident Response Team (PSIRT) severity levels).

The infrastructure related security vulnerabilities in a network element are used to create an Infra NetSecScore for the network element. Each Network Component Infra

NetSecScore is weighted based on the following impacts: data access impact; data modification impact; and/or network usage disruption impact.

Data Access Impact may be indicative of whether the security vulnerability allows a hacker to access/collect network operator data. Network operator data may be, for example, data center records, network configuration, and/or operations data.

Data Modification Impact may be indicative of whether the security vulnerability allows a hacker to modify network operator data. Network operator data modification may be, for example, changing data center records, planting a trojan in the system, highjacking user accounts, etc.

Network Usage Disruption Impact may be indicative of whether the security vulnerability allows a hacker to cause network usage disruption. Network usage disruption may be, for example a denial of service (DDoS) attack.

Figures 1 and 2 below illustrate an overview of an example health score calculation.

Figure 1 illustrates an example of an overall health score calculation.

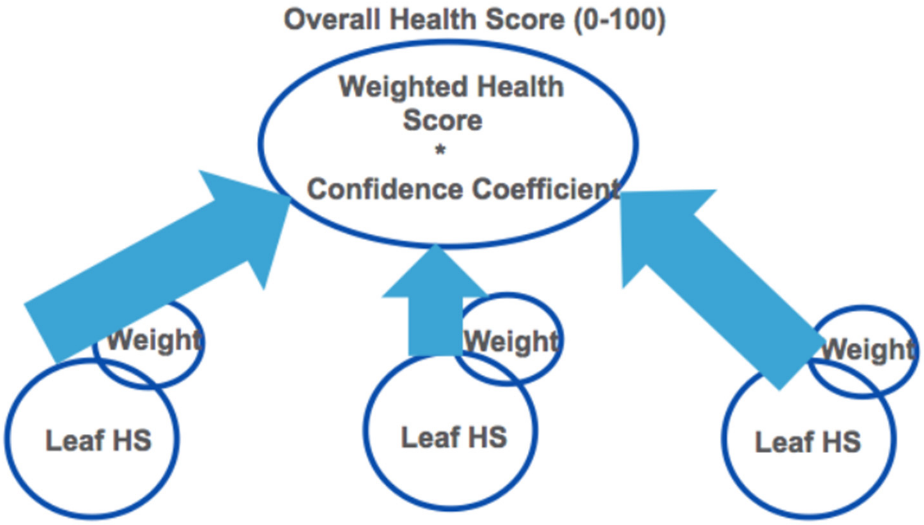

Figure 1

Figure 2 illustrates an example of a component health score calculation.

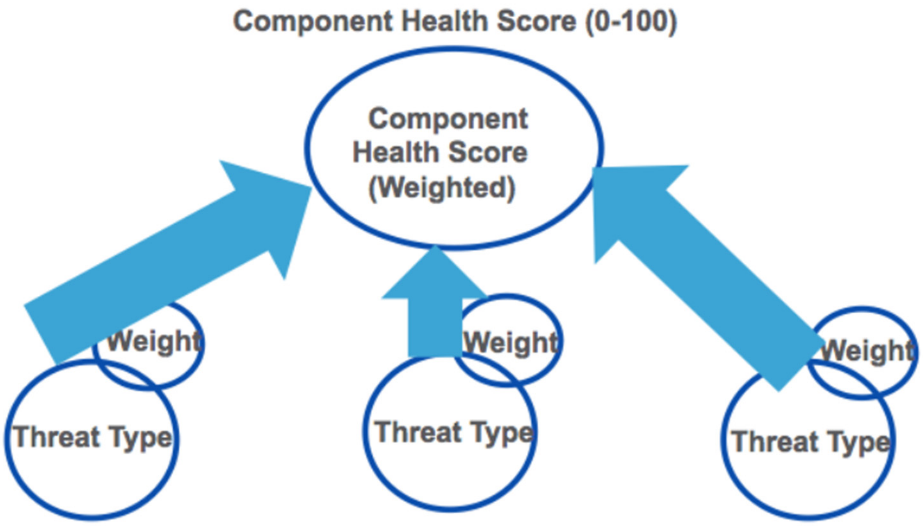
Component Health Score (0-100)
Component Health Score (Weighted)
Weight
Threat Type
Weight
Threat Type
Weight
Threat Type

Figure 2

The threat type category, for example, may be: Infected: 100%; Highly Vulnerable: 80%; Likely Vulnerable: 60%; Potentially Vulnerable: 20%; Safe: 0%.

The weights may be configurable. Weighted geometric mean may be used to calculate weighted health scores.

Kolmogorov-Smirnov test patterns may be used as a basis to validate threat distribution patterns between known and observed values to derive the confidence coefficient.

In summary, techniques are described herein for quantifying the security impact of network vulnerabilities (e.g., hardware/software/configuration) on the network. The security impact quantification is calculated by weighting the configuration vulnerability score and the infrastructure security vulnerability score with the Vulnerability Reach Index.