APPLICATIONS ON TOP OF DNA CENTER: NETWORK SECURITY SCORE BY NETWORK APPLICATION SEGMENTS

Swami Anantha
Santosh Patil
Byju Pularikkal
Sourav Chakraborty

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
Anantha, Swami; Patil, Santosh; Pularikkal, Byju; and Chakraborty, Sourav, "APPLICATIONS ON TOP OF DNA CENTER: NETWORK SECURITY SCORE BY NETWORK APPLICATION SEGMENTS", Technical Disclosure Commons, (June 25, 2018) https://www.tdcommons.org/dpubs_series/1279

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.
APPLICATIONS ON TOP OF DNA CENTER: NETWORK SECURITY SCORE BY NETWORK APPLICATION SEGMENTS

AUTHORS:
Swami Anantha
Santosh Patil
Byju Pularikkal
Sourav Chakraborty

ABSTRACT

Techniques are provided to quantify the security impact of network vulnerabilities (e.g., hardware, software, configuration, etc.) on network applications running in the network and vice versa. The security impact quantification may be calculated by combining the vulnerability reach index (i.e. how far in the network does the impact of a vulnerability extend) with the security breach probability (i.e. the probability of accessing the network elements belonging to one network application from another network application).

DETAILED DESCRIPTION

One of the main tasks of network operators today is ongoing monitoring of the network for security vulnerabilities. If a vulnerability is found, a fix is implemented to remove or reduce the vulnerability. There are a number of network applications or technology segments such as IoT, Guest WiFi, or software defined access (SDA) that are overlaid on the network being monitored. When a security vulnerability is detected in one of the network elements in the network, the network operator has to determine which network applications would be impacted due to this security vulnerability. This is a non-trivial task that is often time consuming and potentially error prone.

If there is a security threat due to a specific type of IoT device, the network operator can determine which IoT applications would be impacted. However, if the affected IoT devices are connected to the same router that supports WiFi services, it is a non-trivial task to determine which WiFi applications would be impacted due to this security breach.
Similarly, when a new network application is being overlaid on the network or network element configuration changes are being made for a network application in the network, it would be beneficial to understand the security impacts of the network application configuration changes on the rest of the network and network applications. In these scenarios, to assess security impacts, a network administrator must understand overlaps between the network applications and implications of such overlaps, which may be complex and difficult to discern.

The present techniques provide an automated mechanism to determine network vulnerability impacts on network applications and vice versa. Generally, the techniques include: collecting and maintaining the network topology and configurations of the network elements that constitute each network application running on the network; identifying the network overlaps between network applications based on the network topology and configurations; and for each connection between network applications in the overlapping network segments, identify the security mechanism that regulates data access over the connection, and calculate the Security Breach Probability (SBP), which describes how probable it is to evade or circumvent a security mechanism.

As examples, if a WiFi network and an IoT network use the same subnet on a router, then there is no security mechanism at the overlap connection and then the SBP is 1. If a WiFi network and an IoT network use two different subnets on the same router which has a strong configuration password, then there is a reasonable security mechanism at the overlap connection and the SBP is 0.2. If a WiFi network and an IoT network use two different subnets on the same router having a strong configuration password but uses a WAN router without a firewall, then even though there is a reasonable security mechanism at the overlap connection, the router itself is vulnerable and hence the SBP is 0.5.

The Enhanced Vulnerability Reach Index (EVRI) can be calculated for each network element that determines how far a security vulnerability in the network element extends into the network. The Vulnerability Reach Index (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 VLAN and/or subnet. The Enhanced Vulnerability Reach Index adds the number of network elements that can be accessed across an overlap connection, weighted by the SBP of the overlap connection. Once the EVRI has been calculated for
each network element, it is possible to calculate the probability of a vulnerability in one network application to move across to another network application. Similarly, it is possible to calculate the Security Vulnerability Potential (SVP) of making a configuration change in a network element, and adding new network applications to a network.

Thus, present techniques include calculating the SBP of an overlap connection, calculating the Enhanced Vulnerability Reach Index of each network element by including the SBP weights, and calculating the SVP of making configuration changes in the network.

Example calculations follow.

---

**Figure 1**

In reference to *Figure 1*, the following assumption are made. The guest WiFi network is on a separate subnet and VLAN. Strong login security at the switch and WAN routers has been implemented. The SBP of WAN routers is 0.1. The total number of network elements in the network is 13. Based on this information, a simple SVP calculation may be performed:

- VRI of Guest Network = \( NE_{Guest} = 4 \)
- EVRI of Data Center Network = \( SBP_{DataCenter} \times NE_{DataCenter} = 0.1 \times 5 = 0.5 \)
- EVRI of Private Network = \( SBP_{Private} \times NE_{Private} = 0.1 \times 4 = 0.4 \)
- Baseline SVP = \( 4 + 0.5 + 0.4 = 4.9 \)
SVP may be normalized on the baseline SVP of the guest WiFi feature. Normalization of SVP without any vulnerabilities is 4.9/13 = 0.37.

In reference to Figure 2, the following assumption are made. A guest WiFi is misconfigured, so that there is a strong possibility to access the private network from the guest network. Therefore, SBP_{Private} is 0.8. Additionally, strong login security at switch and WAN routers has been implemented. The SBP of WAN routers is 0.1. A simple SVP calculation may be performed:

- VRI of Guest Network = NE_{Guest} = 4
- EVRI of Data Center Network = SBP_{DataCenter} * NE_{DataCenter} = 0.1 * 5 = 0.5
- EVRI of Private Network = SBP_{Private} * NE_{Private} = 0.8 * 4 = 3.2
- SVP = 4 + 0.5 + 3.2 = 7.82

The normalized SVP is 7.82/13 or 0.6.
In reference to Figure 3, the following assumptions are made. The guest WiFi is misconfigured, so there is a strong possibility to access the private network from the guest network. Also, \( SBP_{\text{Private}} = 0.8 \). A software vulnerability in the data center WAN firewall is present. Strong login security has been implemented at the switch and WAN routers, and \( SBP \) of WAN Routers = 0.1. A simple SVP calculation may be performed:

- \( \text{VRI of Guest Network} = NE_{\text{Guest}} = 4 \)
- \( \text{EVRI of Data Center Network} = SBP_{\text{DataCenter}} * NE_{\text{DataCenter}} = 0.8 * 5 = 4 \)
- \( \text{EVRI of Private Network} = SBP_{\text{Private}} * NE_{\text{Private}} = 0.8 * 4 \)
- \( \text{SVP} = 4 + 4 + 3.2 = 11.2 \)

The normalized SVP is \( 11.2/13 \) or 0.86.

In summary, the techniques provided herein include an automated mechanism to determine network vulnerability impact on network applications and vice versa. The security impact quantification may be calculated by combining the VRI with the SBP.