

Design of Campus Network Security System Based on Network Information Security

Taiwo Onitiju

CNT 4504 - Computer Networks

Professor: Scott Kelly

University of North Florida

Due Date: November 22nd 2024

1 Introduction:

In this article “**Design of Campus Network Security System Based on Network Information Security**” written by a researcher, he dives into the urgent need for more complex and efficient security frameworks in school campus network systems [1]. Due to the nature of school networks being open for collaborative work, they face vulnerabilities to cyber-attacks which as more complex hacking methods and network assault tools are developed, worsens the issue. The author of the paper’s main objective is to offer a multi-layered security framework that protects the campus network from these threats while still allowing for the performance of the networks purpose which is operation of research and educational work on campus.

The research conducted by the author to create the proposed framework involved investigating the architectural and practical demand of a campus network to be fully protected using a guide method of WPDRRC (Warning, Protection, Detection, Response, Recovery, Counterattack) security model. This model that makes use of preventive and responsive techniques to strengthen networks against invasion was created by Chinese intellectuals to meet their demands of network security in China [1].

Previous research on network information security was reviewed and served as the backbone for the author’s paper. The constraints of conventional two-layer security methods i.e. a firewall and antivirus combination which mainly protected certain layers in the OSI model was investigated in more detail. Intrusion detection, how human factors affect network security, and studies in relation to network security management were also reviewed. Overall, this substructure served to create a more advanced security model that makes use of both specialized and regulatory techniques to improve campus network security.

2 Ideas Presented:

The focal point of the article revolves around the creation of a more advanced security system within campus networks. Weak points of these networks are highlighted by the author such as the networks dependency and acceptance of shared resources which make them an easy target to various cyber-attacks such as data breaches or malicious attacks. To combat these issues, the paper offers 3 key ideas:

2.1 Restrictions of Conventional Security Measures

The paper does an appraisal on traditional two-layer security defenses which include a firewall and an antivirus software, deeming them as insufficient. Firewalls, while effective at filtering and blocking traffic at the network layer, fails in protecting the application and transport layers of the OSI model [1]. Antivirus software on a similar note, depend on frequent updates and fail to catch up to emerging threats such as zero-day attacks. This highlights the need for a multi-layered and dynamic change to campus network security.

2.2 WPDRRC Security Model

As I discussed earlier, the author of the paper proposed a WPDRRC model as the backbone for his multi-layered and dynamic security system. This model is comprised of 6 interconnected sections:

- **Warning:** This involved anticipating the emergence of a malicious attack and estimate the level of threat in real time monitoring.
- **Protection:** Using a layered defense system combining emergency response with log analysis and security hardening, software, data security, and the overall network is secured
- **Detection:** Using an Intrusion Detection System (IDS) and other vulnerability scanners available, system weak-points as well as external threats can be identified.
- **Response:** Combining Alarms, real-time tracking, and audits of each security sub-framework, an emergency response plan is provided to lower the impact of incidents.
- **Recovery:** Measures are provided to restores systems to normal operations post an attack. These measures include data recovery and system recovery.
- **Counterattack:** Retaining information regarding the attacker's attack pattern and tactic, catching criminals in accordance with the law as well as launching a counterattack when needed can be achieved.

2.3 Human Factors

The paper also discusses the vital role personnel from system administrators to end users play in maintaining network security. A low to lack of knowledge on the importance of network security among staff and users is stated as a huge risk. Offering training sessions as well as laying operational standards are given to help prevent this issue.

3 Research Findings:

Vulnerabilities and inherent obstacles to campus networks were investigated in the paper. The author analyzed existing campus network systems and identified key weak-points. Multiple cyber-attack scenarios were simulated such as data interception, compromising systems, among others. Lastly, key performance detectors were gauged such as rate of detection, recovery speed, and response time; to estimate how efficient the established security system was [1].

The data collected in the paper included:

- How accurate threats were identified by the system.
- Logs of system maintenance, downtime, and rate of success in restoring normal operations post an attack.
- Time to start the emergency scenario in the case of a breach.

- Feedback and survey data from campus network users

the author concluded based on the data and results drawn that there is an immediate need to upgrade campus network security and their proposed WPDRRC model would be effective in creating a more secure and strong network environment [1].

4 Lesson Learned:

Post reading of this article, I gained an understanding on campus network security and how unaware I was on how vulnerable I may have been. The paper offered the simple layout a campus network security can be made up off due to their open and shared nature which further led me to consider other similar networks such as airport Wi-Fi networks and how easily susceptible to attacks they likely are. Luckily, the papers proposed WPDRRC model offered relief in the possibility of a more effective network security framework [1].

Overall, this article gave me an understanding on the need for a multi-layered system for defense that could not only be applied to campus networks but to other areas in our increasingly digital and interconnected world.

References

- [1] J. Zhang, “Design of campus network security system based on network information security,” in *2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*. Dalian, China: IEEE, 04 2022, pp. 1194–1197.