**Student Name: Nina Nguyen**

**Date:**

**Topic: Security Hacking Privacy**

**Article:** [**Internet Security Protection in Personal Sensitive Information**](https://ieeexplore-ieee-org.proxy.seattleu.edu/document/7016972)

**Citation: Y. Wang, C. Li and N. Cheng, "Internet Security Protection in Personal Sensitive Information," 2014 Tenth International Conference on Computational Intelligence and Security, Kunming, 2014, pp. 628-632.**

**Summary of Article:**

Personal information is one of the most important things about a person. And most activities can be done online these days with that personal information so it’s important that we know how to secure that. Some risks were covered by the authors, such as, OpenSSL “heart bleed” loophole that caused the leakage of private key, password, server configuration, and source code. Currently, there are a few ways personal information is being leaked; from the individual’s own disclosure, from a business leaking or hacked, and internet security loopholes. The authors went on to introduce systems and procedures for both internal network and external network that protect personal information. An experiment was done to show how one can apply the mentioned procedure to internal internet.

**Article Purpose:**

The purpose of the article was to share different approaches on securing the internal internet and external internet. To protect personal information on the internal side, the author mentioned Document Security Management System, Water Box System to allow detailed audit report, Access Control, and Real Time Encrypt/Decrypt Technology. As for the external side of the internet, the authors discussed Protocol Security (Application Layer, Transport Layer, Network Layer), Web Application Security, and Database Security. For Database, the authors suggest deploying database security audit system to auditing database. For example, if social engineering data is detected, the aforementioned measures will kick in to protect sensitive information from falling into the wrong hands.

**Methodology**

The experiment wasn’t much an experiment in my opinion. The authors took all the mentioned strategies about internal internet security and applied it to a file system because they believe that is the most vulnerable. All operations on the file and folders will be recorded through information audit technique. The system has role-based access through RBAC model. The files and folders are encrypted/decrypted with operations. Every action could be traced back. The authors showed screenshot of an audit trail of how this could be implemented but there was not much on whether this was real or not. There was no mentioned about where the screenshots came from, but I like the idea of securing the data on the internal side of the coin since users can be unpredictable.

**Conclusion**

Personal information can be jeopardized anytime from the source, the transmission, the storage, and interaction with external applications. The authors proposed a model which combined protocol security, web application security, database security, encrypt/decrypt, etc. to overcome security deficiencies.

**Article Strengths:**

The article did a great job with explaining the systems recommended for the internal internet network and how it will help files and folders protect personal information. For example, the water box system was described in detailed along with a structure model on how the water box system works. From pre-prevention, mid-protection to after-auditing. The external network security was also discussed, from protocol security on the different OSI model to database security. I thought this was very helpful especially for readers that does not have a lot of knowledge about security and how it works on different layers.

**Article Weaknesses:**

I think the experiment/methodology was really weak overall. It mentioned about applying audit trail and locking down access to databases but there was not much on how it was done or how efficient the process will be. When I hear audit, to me it’s a long process with a lot of documentation and logs. Not sure how feasible it will be in an environment that’s constantly making transactions. There was no comparison about testing this methodology versus normally secured database. So I’m not sure how secure this would actually be or how adding an audit process will affect the speed of any read/write actions.

**Recommendation:**

There was no recommendation in the article.

**Checklist:**

Number of Authors: 3

Number of Citations of Article: 12

Number of Citations to other articles: 1

Methodology Explained (Yes/No): Yes

Technology Explained (Yes/No): Yes

Experiments and Data Reviewed (Yes/No): No

Conclusion Exist (Yes/No): Yes

Recommendations Exist (Yes/No): No