This research has been supported in part by European Commission
FP6 IYTE-Wireless Project (Contract No: 017442)

Brill Academic Publishers
P.O. Box 9000, 2300 PA Leiden
The Netherlands

Lecture Series on Computer and Computational Sciences

On Defining Security Metrics for Information Systems

A.H. Koltuksuz[1]

Department of Computer Engineering,
Faculty of Engineering,
Izmir Institute of Technology,
35430 Urla, Izmir, Turkey

1. Introduction

It is quite evident that the need for a security metrics grows rapidly as the security budgets are becoming demanding more than ever. Apart from already known security metrics for cryptosystems such as FIPS 140-1/2 we have SSE-CMM which stands for Systems Security Engineering-Capability Maturity Model. [1] A very good example to the efforts for creating the security metrics there is this one and a half year old security metrics consortium known as the “SECMET” [2]. There are other numerous security metrics projects going on. [3]

According to the International Systems Security Engineering Association the good metrics are those that are specific, measurable, attainable, repeatable, and time dependent. [4]

A security metrics model was defined to consist of three components which are

- the object being measured,
- the security objectives the object is being measured against, and
- The method of measurement. [3]

Although many models to create the security metrics have been proposed the question is whether it can be done or not. In other way of saying is it possible to define a security metric for the information systems?

The rest of this paper will try to answer the above question. In this regard, it is organized as follows; Section 2 will consider the security metrics rationale for cryptography. Section 3 discusses the problems of security metrics for the information systems. Conclusions will delineate the proposed answer.

2. Security Metrics Rationale for Cryptosystems

The Information Theory provides us with a measurement unit for syntactic information which is known as the entropy. The entropy is a measure of uncertainty of a random variable.

Definition. The entropy H(X) of a discrete random variable X is defined by

$$\mathrm{H(X)} = -\sum_{x} p(x)\log p(x)$$

[1] Corresponding author. Information Systems Strategy and Security Lab. of IZTECH. E-mail: ahmetkoltuksuz@iyte.edu.tr

This research has been funded in part by EU Commission. FP6 IYTE Wireless Project, Contract #017442.

And since the log is to the base 2, the entropy is expressed in bits. [5] This also means that the amount of information in a message is thus measured by the entropy of the message. Shannon defined the perfect security as

$$P_C(M) = P(M) \text{ where;}$$

$P_C(M)$ be the probability that a message M was sent given that C was received, with C=E(M), and
P(M) is the probability that message M will occur. [6] [7]

While the symmetrical cryptosystems are based on Shannon's Information Theory and thus have an explicit security metric as shown above, the asymmetrical cryptosystems bear the crypto secrecy which actually refers to the concept of intractability.

So far, we have demonstrated that we have a statistically/mathematically proven security metric only for symmetrical cryptosystems.

3. Security Metrics Problem

Defining a security metric for an information system other than the symmetrical cryptosystem is very hard due to fact that there is neither a mathematically proven theory nor any definition for semantic information. This furthermore means that we do not know what we are trying to measure. So now, some questions can be asked such as:

- What exactly is semantic information?
- How can we measure it? In what unit?
- Is it continuous or discrete?
- Is there any proof that it is discrete? Or continuous?
- Is it deterministic or stochastic?
- Would it be possible to process it in a finite state machine if it is continuous and/or stochastic?
- How many dimensions will be needed for the definitions if it is continuous?

4. A Solution Attempt

Although the above asked questions have been circulating around for sometime there seem no clear cut answers as yet. One possible answer as to why not might be due to fact that all of our attempts to define the unit for semantic information and even to define the information itself stems from three dimensional Euclidean geometry.

Trying to define information and/or knowledge in a three dimensional space as a scalar entity is not fruitful. And yet even though the fourth dimension is quite known since Riemann we have yet to include it in our definitions for information and/or knowledge. So the option left is to redefine information in a higher-dimensional space. Here the author's proposal is to conceive the information as a field and thus apply Riemannian tensor analysis to constitute the answers to questions aforementioned. Creating metrics for information security will be an easy task once and if this can be done.

Conclusion

The information and/or knowledge might be a field and if so it should be redefined in a higher-dimensional space by Riemannian tensors. Once it's proven that the information is not a scalar entity then creating security metrics will be possible through tensor analysis.

Acknowledgments

The author wishes to thank the anonymous referees for their careful reading of the manuscript and their fruitful comments and suggestions.

References

[1] SSE-CMM – Metrics; http://www.sse-cmm.org.

[2] SecMet: Security Metrics Consortium; http://www.secmet.org.

[3] S. Katzke, *Security Metrics*, Information Assurance Solutions Group, National Security Agency, USA, 2001.

[4] S. C. Payne, *A Guide to Security Metrics*, SANS Institute, 2002.

[5] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, USA, 1991.

[6] J. Seberry, J. Pieprzyk, Cryptography: An Introduction to Computer Security, Prentice Hall, USA, 1989.

[7] C. E. Shannon, Communication Theory of Secrecy Systems, *Bell Syst. Tech. J.*, **28**, 656-715(1949).