Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

Biological Systems and Models in Information Security

Julie J.C.H. Ryan, *George Washington University*, and Daniel J. Ryan, *National Defense University*

Abstract – The term virus is widely used for one type of malicious code affecting computer systems and networks. Such usage suggests the mental picture of malicious code as a disease infecting computers and implies that information security can use a medical paradigm for protecting against those diseases. In fact, using the concepts of biological systems and models can inform, guide and inspire information security as it seeks to understand, prevent, detect, interdict and counter threats to information assets and systems. The biological approach is especially useful in enabling quantitative risk management and informing management decisions in information security. Statistical analyses are used to evaluate treatment protocols in medicine. Nonparametric models can estimate probabilities of improved longevity due to different drug protocols. Another approach views the risks of patients dying from various causes as competing risks and determines the correlation coefficients of different treatments to longevity. Since the times and causes of death in such studies are uncorrelated, the hazards associated with each risk are proportional. A similar proportional hazards approach can be usefully applied in information security by defining the risks of compromises of confidentiality, integrity and availability as competing to destroy information assets. By correlating system survival times to use of specific design enhancements and security countermeasures, as well as to system exposure based on choice of operational functionality, guidance can be obtained for making investments in information security.

Index terms – Information security; models; statistical analysis; failure time analysis

Julie J. C. H. Ryan, Assistant Professor, Engineering Management and Systems Engineering Department, School of Engineering and Applied Science, George Washington University, Washington, DC 20052, jjchryan@gwu.edu; Daniel J. Ryan, Professor of Systems Management, Information Resources Management College, National Defense University, Washington, DC 20319, ryand@ndu.edu. Opinions expressed in this paper are those of the authors and do not represent positions of George Washington University, the Information Resources Management College, the National Defense University, the Department of Defense, or the United States Government.

I. Introduction

The first computer viruses appeared in the early 1980's, although self-replicating programs had been described in science fiction even earlier. [1] Fred Cohen did research on self-replicating code as early as 1983, although he credits his advisor Leonard Adleman with coining the term "computer virus", from the Latin for poison, for such programs. Dr. Cohen wrote his first paper on the subject in 1984 [2] and published his dissertation exploring self-replicating programs in 1986 [3] at the University of Southern California. He described a computer virus as "a program that can 'infect' other programs by modifying them to include a possibly evolved version of itself." [2] Such a definition is not inclusive of other types of malicious code, such as digital worms, which are self-replicating but do not infect other programs, but it has served for many years as a useful biologically-informed model of computer viruses.

Viruses and worms were not the only biological models used in investigating information security threats. Agricultural models have been employed that treat malicious programs as "pests" modeled on the pests that infest plants. [4] Others apply epidemiological models to malicious code. [5] Some researchers have attempted to model the human immune system and apply their model to protecting information infrastructures against malicious code. Stephanie Forrest, Stephen Hofmeyr and Anil Somayaji of the University of New Mexico, explored analogies to immunology in trying to develop robust approaches to information security. [6] Anil Somayaji, in his Ph.D. dissertation, investigated homeostatic mechanisms that organisms use to stabilize their internal environment and followed that approach in slowing or stopping computer security attacks. [7] The general background of this approach is outlined by Damaris Christiansen. [8]

Biological models, and medical models in particular, have recently proven useful for information security in risk management and in the evaluation of proposed investments in information security, both of which depend

ISBN 1-933510-96-8 ©2008 CISSE

on having knowledge of the probability distributions associated with successful attacks on information assets and systems. Unfortunately, little real data is available upon which we can rely to estimate the required probability distributions. [9, 10] We have to collect the data we need and use sampling theory to arrive at statistically valid estimations of the probability distributions we need.

II. Medical Models and Information Security

Just as the medical community studies groups of patients by statistically analyzing the observed results of using different drugs and different protocols, [11, 12, 13, 14] the statistical methods that have been developed to investigate medical protocols are applicable to information infrastructures, where computer systems are dealt with as patients, hackers and malicious programs are diseases, technological countermeasures are drugs, and information security policies, practices and procedures are treatment protocols. To derive statistically valid estimations of the underlying probability distributions, we collect and analyze failure time data – that is, we observe the operation of the information infrastructure and record *inter alia* the times at which systems within the infrastructure fail and the causes of those failures. Analyses of such data can yield non-parametric estimates of the probability distributions related to successful attacks. [15] We may also record a variety of supplementary information concerning characteristics of the systems we observe, comprising an explanatory variable that can subsequently be analyzed to assess the relationship of those characteristics to security. [16]

Studies of failure time data and associated explanatory variables can be *observational* (or *epidemiological*) studies of the entire information infrastructure or a representative sub-infrastructure based on concurrent measurements (a *cross-sectional* study), of samples of individual systems followed prospectively (a *cohort* study), or of several samples with retrospective measurements (a *case-control* study). Alternatively, we can use a randomized controlled trial to study two or more parallel, randomized cohorts of systems, one of which (the *control group*) receives no security enhancements, and the others of which are enhanced by the proposed investment or investments in information security. Randomized controlled trials are ideal for evaluation of proposed investments in new information security practices, procedures or technologies, and can provide a quantitative method for understanding the security status of systems and networks, and for analyzing the relationships between security policies, practices, procedures and technologies and the loss against which their use seeks to avoid. Population-based epidemiological studies cannot support conclusions about causal relationships between system characteristics and security effectiveness. However, because we control possibly intervening factors through randomization, a randomized controlled trial can support conclusions concerning causal relationships among investments and security effectiveness. [11, pp. 5-7]

Systems and networks fail over time for a variety of reasons: they wear out, suffer from design or manufacturing defects, or are subjected to environmental or intrinsic stresses that lead to degraded performance or failure. Generic hazards facing organizations include natural disasters, technological disasters, product defects or failures in quality control, operational errors, criminal activity, lawsuits, damaging rumors, and the death or departure of key personnel. For the purposes of this paper, we are most concerned with the cases where their compromise or destruction is the result of an attack by malevolent individuals or groups, even if the attack is by undirected malicious code, rather than failures due to unintentional acts or to the class of problems usually described as failures of reliability, although we recognize that some of the risk abatement strategies that can be employed to protect against malevolent threats also offer some degree of protection against unintentional human acts or failures of system or component reliability, and vice versa. Consequently, in this paper, *failure time* means the time at which a system succumbs to an attack by malicious or malevolent individuals or groups. The extent to which a system must succumb before being counted a failure depends upon the purpose of the study. Significantly degraded performance may be studied as well as complete failure. How much degradation would be required to count as significant is also part of the experimental design.

We also need to be careful to define our collectable data in ways that preserve the independence of the data sets we collect, since independence is an assumption often applicable to the statistical methods we use. Information assets are characterized by requirements for confidentiality, integrity, and availability. Such requirements are not necessarily independent if carelessly defined. We therefore specify the requirements as follows:

- Confidentiality is a requirement imposed on access to the contents of a body of information because knowledge of the contents is to be limited to only a specified set of individuals or processes. Available, accurate data may have its confidentiality compromised if someone who is not an intended recipient reads it.

- Integrity is a requirement imposed on access to data for the purpose of limiting the set of individuals or

processes that can modify or destroy the data. Data integrity assures the recipient that the sender is known, assures the sender that the recipient is known, $S(t) = \exp\{-H(t)\}$. and both that the data has not been changed while in transit between them. Data may be readily available and uncompromised with respect to its confidentiality, yet suffer degraded integrity due to illicit modification.

- Availability is a requirement imposed on finite delays in delivery of requested data in order to ensure that a licit requestor receives the data in a timely manner. Permissible delays in delivery are normally stated in terms of time intervals. Data may be safe from disclosure, illicit modification or destruction and yet not be available when needed, as when a system's performance is degraded in a denial of service attack. Even though destruction of data surely affects its availability, we treat destruction as an integrity issue rather than an availability issue so that our requirements are independent. [16]

One problem in collecting and analyzing failure time data follows from the fact that the distributions in such studies are rarely normal, usually exhibiting a greater or lesser degree of right skew. Another problem in collection and analysis of failure time data arises when systems being studied can no longer be tracked in the study, either because they have disappeared or because the study is finished with the systems having yet to fail, or which fail due to reasons unrelated to the purposes of the study. An example of the latter might be a system that fails due to a reliability problem unrelated to information security (e.g. disk failure). When systems are lost to the study for such reasons, they are said to be *right-censored*. The statistical methods used in studies like those proposed here have to be adjusted to allow for the presence of right-censored data.

III. Applying the Models

Having dealt with these problems in our experimental design, we can collect failure time data and use it to calculate estimates of the *survival function* $S(t) = \Pr\{T>t\} = 1 - F(t)$, where $F(t)$ is the *failure distribution*. The *probability density* $f(t)$ associated with $F(t)$ is

$$f(t) = \frac{dF(t)}{dt} = \frac{d[1-S(t)]}{dt} = -\frac{dS(t)}{dt}, \text{ and the}$$

instantaneous risk of failure at t is given by the *hazard function*

$$h(t) = \lim_{\delta \to 0+} \Pr(t \le T < t+\delta \mid T \ge t)/\delta .$$

Obviously, $h(t) = \frac{f(t)}{S(t)}$ and the cumulative hazard function $H(t) = \int_0^t h(u)du$ satisfies $S(t) = \exp\{-H(t)\}$.

Non-parametric estimators for $S(t)$ due to Kaplan and Meier, and another from Nelson and Aalen, are available. [15] Log-rank and Wilcoxon tests are available to compare the survival functions of two groups in order to test the hypothesis that the underlying probabilities of failure are due to chance rather than improved security. [14, pp. 42ff.]

Alternatively, we may wish to evaluate the influence of a variety of environmental and system characteristics on failure rates. Cox [17] developed a semi-parametric approach that assumes that systems that enjoy investments in (hopefully) enhanced information security will survive proportionally longer than those that do not enjoy the advantage of such investments. Thus, $h(t) = k \cdot h_0(t)$, where k is the constant of proportionality. If we use $\exp(\boldsymbol{\beta}'\mathbf{x})$ as the constant of proportionality, where $\boldsymbol{\beta}$ and $\mathbf{x}$ are vectors with $\mathbf{x}$ being the explanatory variables being investigated and $\boldsymbol{\beta}$ the vector of coefficients of the explanatory variables, than the coefficients tell us the extent to which each explanatory variable contributes to the improved longevity (if any) of the "improved" systems (obviously, if there was no improvement, or worse some degradation resulted, following an investment in what was hoped would be improved information security, the investment was ill-considered). If there is more than one possible cause of failure, the model can be adjusted to evaluate the relative risk of failure due to each possible cause, an approach called *competing risks* by statisticians.

The difference between the integrals of our the survival functions with and without the investment, $S(t)$ and $S_0(t)$ respectively, makes a nice metric for measuring the effectiveness of a proposed investment in information security. [15] Better yet, if we can establish a value function that tells us the impact of a successful attack on our information assets or systems, we can combine the impacts and their probabilities to get expected losses with and without the advantage provided by a proposed investment. The net benefit of the proposed investment is the difference in expected losses less the cost of the investment. [15]

IV. Conclusions

Biological models inform and guide our understanding of information security threats and countermeasures. Medical models in particular have proven extremely useful in elucidating the nature of self-replicating malicious code. Now medical approaches to understanding the hazards posed by diseases and the efficacy of proposed drug and treatment protocols are beginning to be applied to information security risk management. By collecting and analyzing failure time data in samples of systems within an information infrastructure, we can estimate the probabilities of failures due to various information security attacks on our information assets and systems. Comparing the survival functions for protected and unprotected samples allows us to quantitatively compare the survival (hence failure) rates for the different samples and to perform hypothesis tests to determine if statistically significant results advantages are being obtained for the protected versus unprotected samples. Assigning explanatory variables to each system in the samples allows us to evaluate the contribution to enhanced security of each of several characteristics of our systems and their operational environments. Assigning a value function to information assets and systems further allows us to measure the risk we face in terms of expected losses with and without proposed investments in information security, enabling quantitative risk management for information security.

V. References

[1] David Gerrold, *When HARLIE was One*, 1972; John Brunner, *Shockwave Rider*, 1975.

[2] Fred Cohen, "Computer Viruses: Theory and Experiments", (1984) found at http://all.net/books/virus/index.html. See also, Fred Cohen, "Computer Viruses: Theory and Experiments", Computers and Security 6 (1987) 22-35.

[3] Fredrick B. Cohen, *Computer Viruses*, (1986) Ph.D. dissertation, University of Southern California.

[4] S. K. Jones and Clinton E. White, Jr., ``The IPM Model of Computer Virus Management," *Computers & Security,* vol. 9, 1990, pp. 411-418.

[5] W. H. Murray, ``The application of epidemiology to computer viruses," *Computers & Security,* vol. 7, pp. 130-150, 1988.

[6] Stephanie Forrest, Stephen Hofmeyr and Anil Somayaji, "Computer Immunology," *Communications of the ACM*, Vol. 40, No. 10 (Oct., 1997), p. 88ff.

[7] Anil Somayaji, Operating system stability and security through process homeostasis, (2002) Ph.D. dissertation, University of New Mexico.

[8] Damaris Christiansen, "Beyond Virtual Vaccinations: Developing a Digital Immune System in Bits and Bytes," *Science News*, Vol. 156, No. 5, July 31, 1999, p. 76. (1999) On-line at http://www.sciencenews.org/pages/sn_arc99/7_31_99/bob2.htm

[9] Julie J.C.H. Ryan and Theresa I. Jefferson, "The Use, Misuse, and Abuse of Statistics in Information Security Research," *Managing Technology in a Dynamic World*, Proceedings of the 2003 American Society for Engineering Management Conference, October 15-18, 2003, St. Louis, Missouri, pp. 644-653.

[10] Julie J.C.H. Ryan, Information Security Practices and Experiences in Small Businesses, (2000) D.Sc. dissertation, George Washington University. On-line at http://www.pirp.harvard.edu/pubs/pdf-blurb.asp?id=493.

[11] John M. Lachin, *Biostatistical Methods: The Assessment of Relative Risks*, John Wiley & Sons, New York (2000).

[12] John D. Kalbfleish and Ross L. Prentice, *The Statistical Analysis of Failure Time Data*, 2nd Ed., Wiley, Hoboken, NJ (2002).

[13] Terry M. Therneau and Patricia M. Grambsch, *Modeling Survival Data: Extending the Cox Model*, Springer, New York (2000).

[14] David Collett, *Modelling Survival Data in Medical research*, 2nd Ed., Chapman & Hall/CRC, Boca Raton (2003).

[15] Julie J. C. H. Ryan & Daniel J. Ryan. (November, 2006) "Expected Benefits of Information Security Investments", *Computers and Security*, Vol. 25, Issue 8. Amsterdam: Elsevier. Pages 579-588.

[16] Julie J. C. H. Ryan and Daniel J. Ryan, "Proportional Hazards in Information Security, *Risk Analysis: An International Journal*, Vol. 25, No. 1, 2005, pp. 139 - 147.

[17] Cox, D. R., "Regression models and life tables (with discussion)," *J. R. Statist. Soc*. B 34, 1972.