CONFIDENTIALITY, INTEGRITY AND AVAILABILITY AS CONSTRUCTS FOR CYBER SECURITY SIMULATION

Mark Rounds, College of Business and Economics, College of Business and Economics
University of Idaho, Moscow ID 83843, 208-885-4199, mrounds@uidaho.edu
Norman Pendegraft, College of Business and Economics, College of Business and Economics
University of Idaho, Moscow ID 83843, 208-885-7157, norman@uidaho.edu

ABSTRACT

The Confidentiality, Integrity and Availability triad is a model designed to guide policies for information security in an organization. Examination of several major cyber-attacks against businesses suggests that the costs of criminal attacks against confidentiality and accessibility are increasingly absorbed as the costs of doing business. On the other hand, attacks against the integrity of data seem to be having a significant effect on system value. The cases are used to inform a production function model of system value.

Keywords: Confidentiality, Integrity, Availability, Security, Simulation

INTRODUCTION

This paper extends an ongoing program of simulation research aimed at modeling the economics of information systems under attack. Such simulations attempt to model the impact of attacks on the system. Heretofore we have considered attackers to be homogeneous. In order to relax that assumption, it is necessary to consider various attack vectors. The Confidentiality, Integrity, and Availability triad (CIA) offers a simple way to structure that investigation. Here we ask whether the CIA model offers enough value to justify its use in simulation studies. The remainder of the paper is organized as follows. First we examine some background of the CIA model. Then we look at a number of prominent information security cases and categorize them using the CIA model. We illustrate the value of the cases by using them to justify certain assumption in an analytical model proposed elsewhere. Finally, we discuss the implications of our findings.

BACKGROUND

The CIA model has been used for a number of years to categorize problems that affect the use of information technology. Confidentiality refers to limiting access to data to only those who are authorized to use it. Integrity refers to the accuracy of data. Access refers making data and systems available to authorized users when needed [3], [6]. Simonds, Sandilands, and Van Exert [21] discuss this model as a method to categorize attacks against an information system, but they do not look at the effectiveness of these attacks as a category. Kotenko and Stepashkin [10] use the CIA model as a starting point for comparing threats against a system using attack graphs but don't compare the aspects of the CIA model as a categorization systems specifically for the type of threats involved. Later work, such as Khan, et. al., [8] describe the impact of security threats in terms of the CIA model, but don't use it as a taxonomy for the threats themselves.

CASES

We examined a number of high profile events, and summarize them below.

Attacks on confidentiality

Espionage by nation states is common, but frequently not made public [13]. Nor is the impact easy to evaluate. The recent attack on the OPM [12] widely believed to have been executed by China, is a case in point. In the Battle of Midway [24], a small espionage success resulted in a major naval victory.

In contrast, criminal attacks on confidentiality have become part of the expected cost of business. In May 2017 Equifax, which provides credit information for the banking industry was hacked and 143 million users were exposed. Credit card data for an additional 290,000 were also exposed [17]. Stock priced dropped sharply and by September 2017 was down 18.4% [16] suggesting that consumers expect the hacks and so far, the negative effects have not seriously impacted them.

Marketing firms seem to place a high value on personal information, but consumers don't seem to care [20], [25]. The Cambridge Analytica Episode seems to show that there is little impact to the company from exposure of this information as the downward move of Facebook's stock price was small in magnitude and of short duration [16].

These cases suggest that loss of confidentiality has limited downside except in the national security realm.

Attacks on integrity

During the 2008 Russian-Georgian war, Russian cyber operatives successfully took over the OSInform New Agency and used it to spread disinformation. They also were able to hack the controls for the Baku-Tbilisi-Ceyhan Pipeline causing an over pressure and explosion. These actions contributed materially to the eventual Russian victory [22].

In 2010, the Chinese Government demanded that they be allowed to censor the content and monitor communications activity. The Chinese government also made several attempts to access the accounts of dissidents. Ultimately, Google decided to leave the market space rather than submit to the requirements [23] as Googles concern about their data integrity meant they couldn't afford to be active in China.

In 2010, it became known that a nation state, likely the US or Israel, had unleashed a worm on the Iranian nuclear program that cause the centrifuges that were used to refine uranium to spin themselves to failure, also an attack against integrity. Since then, there have been other attacks that have kept the Iranian nuclear program from succeeding [11].

In 2014, the ACFE estimated organization typically lose 5% of revenues each year due to fraud. Since fraud is commonly hidden by data integrity attacks, this suggest that integrity is a serious issue. [1]

Vandalism attacks, seem to have little impact. While the number of attacks is on the rise and the tools available for detecting and combating this attacks continue to improve, the effect seems to

be less and less as time goes on [4]. Indeed, few of these attacks have a commercial motive, most being delivered for political or social reasons. The results are disappointing if you're a hacker. Policies are very rarely changed and if the victim is a commercial entity, there is very little change in stock price or sales [16]. It isn't a surprise therefore that the number of defacement attacks has been on the decline since 2013 [14].

Attacks on accessibility

Attacks on the accessibility occur in the banking industry in the guise of Denial of Service attack. This directly impacts the amount of new data generate and access to same. In the era of on-line banking, the threat to the industry is great. In the past these attacks were mainly the product of Hacktivists, but now, the focus is on extorting money from the banks [19]. The banks were, until recently, paying high ransoms to keep their on-line enterprises open suggesting that the long term effects. Now however, the tools have made it possible to mitigate or limit the threat and people accept the risk.

Ransomware attacks are also attacks against data accessibility. Hard drives are locked down and encrypted with a notice that a ransom must be paid have access to your data. The success rate is high as the alternative threat if the ransom is not paid is destruction of the data within a few (usually 48) hours [5].

In 2016, an internet of things DDOS attack on the Rio Olympics. This was a sustained attack for months and peaked at 540 Gbps [2]. With the help of a consulting firm, they were able to keep their site up and functional. Five Russian banks were targeted by a coordinated DDOS attack for over two days. The banks were able to stay open and on line. [9].

CASE IMPLICATIONS

Criminal attacks on confidentiality and accessibility appear to be having less impact and seem to be evolving into another cost of doing business. This is not to suggest that they are unimportant or should be ignored, merely that they seem to be controllable. On the other hand, nation state efforts seem to be more serious. Thus, we conclude that there is as fundamental difference between criminal attacks using these vectors and acts of war or espionage. Integrity attacks seem to remain serious threats to information systems. Even there, steps are being taken to mitigate that risk. For example, Amazon has enabled two factor identification to help mitigate the threat to integrity posed by identity theft [15].

ILLUSTRATION

These insights have implications for researchers trying to model these interactions. To illustrate the value of this result to a modeler, we apply it to the model suggested in Pendegraft & Rounds [18]. That paper suggests a Cobb Douglas production function to evaluate the impact of attacks on C, I, and A.

$$V(C, I, A) = C^{\alpha}\ I^{\beta}\ A^{\gamma} \qquad Eq1$$

where

C>0 is the level of privacy, I>0 is the integrity, and A>0 is the accessibility or quantity of data, and, α,β, and $\gamma > 0$

One of the advantages of the model is that it allows for concave or convex responses to changes in C, I, & A depending on the value of the exponents. Commonly, production functions are thought to be concave, i.e. have decreasing returns to scale. Here, we suggest that that is indeed the case for many attacks. In other cases, however, convex reflecting increasing returns to scale. In those cases even a small attack may result in a large loss. See Figure 1.

The cases presented here suggest that the model would be different for different organizations. For example, for commercial economic data you might have $\alpha<1$ resulting in a concave value function with respect to α, and for national security cases it may be that $\alpha>1$ which gives a convex function.

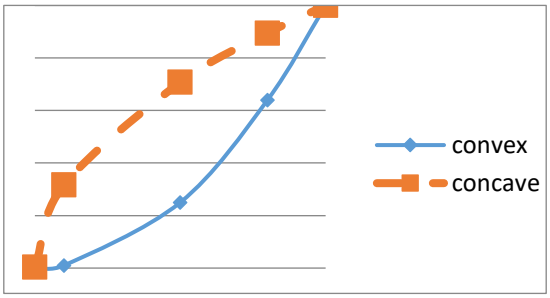

Figure 1

DISCUSSION

These conclusions were initially surprising to us as the current academic thinking on these issues was that the attackers were winning this war [7]. It seems that the defenders are making progress. While, we believe that more empirical work needs to be done to confirm our, admittedly anecdotal, observations, the results have three implications of interest.

First, this has already changed the authors' thinking on how to teach security related subjects as the emphasis will move from a life and death defense process to cost control.

Second, there is also a potential impact on how policies are determined for businesses when dealing with security threats. The focus will be on cost reduction rather than an amorphous threat. Of course, the situation will have to be monitored for change.

Finally, returning to the question that motivated the study, the analysis suggest that the CIA model continues to be useful in simulating infosec problems. We hope to use it in subsequent simulation studies.

REFERENCES

[1] AFCE, Report to the Nation on Occupational Fraud and Abuse, http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf, retrieved 20 Sept 2018.[2] Bisson, D., The five most Significant DDoS Attacks of 2016, Tripwire, Nov, 29, 2016,

https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/5-significant-ddos-attacks-2016/, downloaded September 12th, 2018

[3] Evans, D., Bond, P., & Bement, A. Standards for Security Categorization of Federal Information and Information Systems. National Institute of Standards and Technology, Computer Security Resource Center. 2004

[4] Das, A. K., Nguyen, Q. T., & Thomas, S., Entertaining whilst defacing websites: Psychological games for hackers. Issues in Informing Science and Information Technology, 14, 219-227, 2017

[5] Furhlinger, J., The 5 biggest ransomware attacks of the last 5 years, CSO, Aug 1st, 2017, downloaded Aug 29th, 2018.

[6] Gilliam, D. P. Managing information technology security risk. Software Security Theories and Systems, 2003, 3233, 296-317. doi: 10.1007/978-3-540-37621-7_16

[7] Harmandeep Singh Brar and Gulshan Kumar, "Cybercrimes: A Proposed Taxonomy and Challenges," Journal of Computer Networks and Communications, vol. 2018, Article ID 1798659, 11 pages, 2018. https://doi.org/10.1155/2018/1798659.

[8] Khan M., Anwar M.W., Azam F., Samea F., Shinwari M.F., A Model-Driven Approach for Access Control in Internet of Things (IoT) Applications – An Introduction to UMLOA. In: Damaševičius R., Vasiljevienė G. (eds) Information and Software Technologies. ICIST 2018. Communications in Computer and Information Science, vol 920. Springer, Cham

[9] Kitten, T., "DDoS Attacks Against Banks Increasing: Financial Institutions Seek New Ways to Mitigate the Risks", Bank Info Security, August 24th, 2015.

[10] Kotenko I., Stepashkin M., Attack Graph Based Evaluation of Network Security. In: Leitold H., Markatos E.P. (eds) Communications and Multimedia Security. CMS 2006. Lecture Notes in Computer Science, vol 4237. Springer, Berlin, Heidelberg

[11] Kushner, D., The Real Story of Stuxnet: How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program, IEEE Spectrum, 26, February, 2013

[12] Levine, M., and Date, J., "22 Million Affected by OPM Hack, Officials Say," ABC News, July 9, 2015, http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731.

[13] Mahvi A.J., Strategic Offensive Cyber Operations: Capabilities, Limitations, and Role of the Intelligence Community. In: Kosal M. (eds) Technology and the Intelligence Community. Advanced Sciences and Technologies for Security Applications. Springer, Cham 2018

[14] Maggi, F., Balduzzi, M., Flores, R., Gu, L., and Ciancaglini, V., Investigating Web Defacement Campaigns at Large, ASIACCS '18 Proceedings of the 2018 on Asia Conference on Computer and Communications Security, Incheon, Republic of Korea — June 04 - 04, 2018

[15] Moynihan, T., How to Enable Amazon's Two Step authentication, Wired, Nov 19th, 2015, https://www.wired.com/2015/11/amazon-two-step-authentication/ downloaded September 12th, 2018

[16] Nasdaq Prices retrieved 7/25/2018

[17] Nuska, A., "Equifax Stock Has Plunged 18.4% Since It Revealed Massive Breach", Fortune, September 11th, 2017

[18] Pendegraft, N. & Rounds, M., A Confidentiality, integrity, accessibility production function for Infosec evaluation using Cobb Douglas, Working paper, 2019.

[19] Romagna, Marco & Hout, Niek Jan., Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats. Conference: Conference: 27th Virus Bulletin International Conference, 2017, At Madrid, Spain, Volume: 1

[20] Shonenshine, J., "Here are five reasons Facebook will continue tumbling" Business Insider, April 2, 2018.

[21] Simmonds A., Sandilands P., van Ekert L., An Ontology for Network Security Attacks. In: Manandhar S., Austin J., Desai U., Oyanagi Y., Talukder A.K. (eds) Applied Computing. AACC 2004. Lecture Notes in Computer Science, vol 3285. Springer, Berlin, Heidelberg

[22] Shakarian, P., The 2008 Russian Cyber Campaign against Georgia, Military Review, November-December 2011

[23] Tan, J. & Tan, A.E., Business Under Threat, Technology Under Attack, Ethics Under Fire: The Experience of Google in China, Journal of Bus Ethics 110: 469. 2012 https://doi.org/10.1007/s10551-012-1494-0

[24] Truscott, J., Code breakers: Inside the shadow world of signals intelligence in Australia's two Bletchley Parks [Book Review] [online]. Australian Defence Force Journal, No. 203, 2017: 105-106.

[25] Wills, J., "7 Ways Amazon Uses Big Data to Stalk You (AMZN)" Investopedia, Septenber 7th, 2016, Downloaded July 26th, 2018)