Cyber security: the Risk of Supply Chain Vulnerabilities in an Enterprise Firewall

Marshall A. Kuypers[*a], Greg Heon [a], Philip Martin [a], Jack Smith [a], Katie Ward [a], and Elisabeth Paté-Cornell [a]
Stanford University, Stanford, CA

Abstract: Cyber security is a critical concern for many organizations. One defense approach is to install firewalls, but their effectiveness is uncertain and the cheapest model may not be the best. One may try to inspect them for vulnerabilities that may have been introduced in the product's supply chain. Most existing models that quantify cyber risk do not address that issue, and the risk that corrupted components could be successfully inserted into a secure network is not directly considered other than by characterizing the supplier. We present a probabilistic risk analysis model for a firewall linking its parts to the different stages of production. We then evaluate the tradeoff between cost (system and inspection) and security by comparing two firewalls. We base our analysis on expert opinions, which we aggregate using the Delphi method. The model shows that in the illustrative case presented here, the value of information about the effectiveness of a firewall is actually worth little to a risk neutral decision maker. Therefore, inspecting firewalls for vulnerabilities may not be the most effective way to address the system's security. Gathering information by monitoring for warning signals of a cyber attack could be a beneficial alternative or complement.

Keywords: Cyber security, Supply chain, risk analysis

1. INTRODUCTION

The increased reliance on chip-based electronics has resulted in a greater risk to organizations of data destruction, corruption, or loss of confidentiality. Many organizations are constantly adding new hardware and software to information technology (IT) networks, but the security of new products is often taken for granted. Over the past five years, however, several companies have been compromised by an intentional vulnerability introduced in a product's supply chain. At this time, decision makers have a limited toolset to analyze risk from new products caused by non-secure supply chains. A common heuristic might be to use the national origin of the equipment as a discrimination factor, which is suboptimal. In this paper, we model an organization's decision to purchase an enterprise firewall using decision analysis and risk analysis to assess the likelihood of supply chain vulnerabilities. Quantifying the risk to an organization that a vulnerability has been introduced in its cyber defenses enables a clear breakdown of the costs and benefits of different firewalls. In this paper, we consider the option of inspecting these defenses for undetected vulnerabilities and we assess the value of these inspections.

2. Background

Supply chain attacks have increased in frequency and scope. One of the earliest examples occurred in Chicago in 1982, when several residents died after taking store bought Tylenol that had been laced with cyanide[†] [1]. In response to public alarm across the nation, the pharmaceutical industry developed tamper-proof seals and began analyzing supply chain security. Soon after, new supply chain threats emerged. The liquid in eye drop products was replaced with Hydrochloric acid and other medications were poisoned. Criminals also began targeting manufacturing processes. In 2006, McDonalds recalled promotional mp3 players that included spyware designed to steal users' passwords [3]. The GPS

[*] mkuypers@stanford.edu

[†] Authorities eliminated contamination during the manufacturing process as a cause since contaminated bottles came from two manufacturing plants in different states and only surfaced in Illinois. Authorities believe that someone tampered with the medicine shortly before the point of sale [2].

manufacturer Tom-Tom shipped malware infected devices in 2006, and Apple ironically shipped iPods infected with a PC virus [4]. Vulnerabilities were also introduced in the supply chains of flash drives, digital picture frames, external hard drives, and laptops, and customers purchased products that had been compromised before ever being used.

A particularly sophisticated supply chain attack occurred in 2008, when extra computer chips were covertly added to Mastercard credit card readers. These chips then transmitted credit card data to criminals overseas. According to Joel Brenner, a former US National Counterintelligence Executive, the vulnerability was introduced either during the manufacturing process in China or shortly thereafter, since the new card readers appeared to be in their original packaging when they arrived at stores for installation [5]. A small, wireless chip had been inserted behind the card reader's motherboard, which allowed the copied data to be sent to a server in Pakistan [5,6]. Mastercard resorted to sending teams to weigh each card reader, since virtually the only sign of tampered card readers was an extra 3 to 4 ounces in their weight [7]. An estimated $50M to $100M were lost as a result of the attack.

The possibility of the introduction of vulnerabilities by foreign adversaries through a supply chain gained new national attention in 2010, when Sprint was considering bids to upgrade its US telecommunications network [8]. Huawei, the world's second largest telecommunications and internet manufacturer, placed a bid that was estimated to save Sprint $800M in the first year alone [9]. Security concerns arose and a group of senators wrote a letter to national security officials pointing out that Huawei had repeatedly violated intellectual property rights and had ties to the Chinese government[‡] [10]. Huawei's bid was blocked and since then, Huawei has struggled to dispel fears about its products[§].

2.1. Related Work

As supply chain attacks have become more frequent and widespread, governments and organizations have been increasingly interested in the study of risk controls and mitigations. Supply Chain Risk Management (SCRM) is a well-studied area primarily focused on optimizing a supply chain against disruptions [13, 14]. The aftermath of events such as the September 11th attacks on the US and the 2011 earthquake and tsunami in Japan have shown the importance of robust supply chains to avoid production line shutdowns that can cost up to $10,000 per minute of downtime. However, the risk of an intentional introduction of vulnerabilities in specific products is considerably less studied.

Many researchers and organizations have addressed cyber security quantitatively with tools ranging from probabilistic risk analysis (PRA) to game theory [15]. The unique damage caused by cyber attacks includes the loss of physical equipment, network downtime, reputation damage, and other costs. They require new modeling approaches to fully capture the range of impacts. Initially, the complexity and uncertainty of losses led to simple measures of risk, such as Annual Loss Expectancy [16]. As the limitations of simple expectation methods were exposed, new probabilistic tools were developed [17, 18]. The Gordon-Loeb model demonstrated how economic analysis could be applied to the cyber domain for a variety of applications [19]. Buckshaw outlined a decision analysis framework to quantitatively evaluate information system designs [20]. Recently, there has been growing interest in attack trees, kill chains, and the optimization of IT resources [21, 22, 23]. Yet, very few models address security concerns about the supply chain, assuming instead that IT products and controls increase security without introducing additional risks. This problem is the focus of this paper.

At this time, interest in supply chain attacks is growing. In 2012, the White House released the "National Strategy for Global Supply Chain Security", which responded to earlier government studies calling for better management of supply chain risks [24]. The United States Government

[‡] The founder and CEO of Huawei, Ren Zhengfei, was a Major in the People's Liberation Army Engineering Corps.

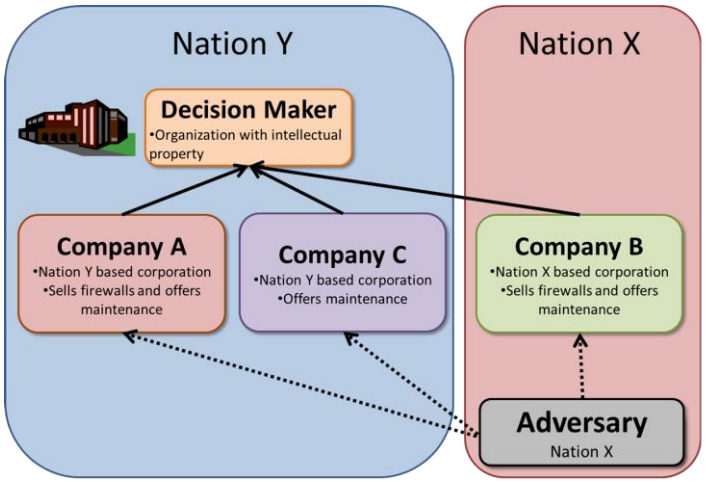
[§] In 2013, Huawei announced that it was not interested in the US market, although a month later, it announced plans to launch a smartphone in the US [11, 12].

Accountability Office has released several reports about risks in IT supply chains, and the National Institute of Standards and Technology has published best practices for businesses regarding supply chain risk management [25, 26, 27, 28]. Many organizations and researchers have also begun to call attention to supply chain attacks [29, 30]. Yet, little quantitative, risk-analytic work has been done in this area. The objective of this paper is to present a PRA for a firewall considering the possibility that vulnerabilities have been introduced in the different parts in the production process.

3. Model Formulation

To study the tradeoffs between price and security in IT products, we constructed an organization comparing two enterprise firewalls (see Figure 1). The client organization is located in nation state Y and owns valuable intellectual property (IP). This organization considers buying firewalls from two companies, A and B. Company A is publically owned, also based in nation state Y, and has a reputation for delivering high quality, secure products. Company B is privately owned and based in nation state X, which is an adversary of nation state Y. It is less well known and may have a less secure supply chain but cheaper products. The client organization must also purchase a maintenance plan from either the firewall's manufacturer, or from company C in nation Y. In spite of their reputations, companies A or C as well as company B, could be collaborating with nation state X, which may introduce vulnerabilities into their supply chains. The decision maker would like to analyze which firewall should be purchased, the value of additional information (e.g., through inspection) about the probability of a vulnerability, and what strategies could be used to secure the organization's IP.

Figure 1: Decision Model for the purchase of a firewall



3.1. Vulnerability Analysis

In order to narrow the scope of the analysis, we only model one specific vulnerability for this illustrative study. Firewalls contain a run configuration file, which lists the protocols, the open ports of the network, and the security controls of the machine. The run configuration file is thus valuable to attackers because it provides information about the network defenses and allows the adversary to launch more targeted, effective attacks. Accessing the run configuration file does not guarantee that the adversary will immediately steal or destroy data, but it increases the likelihood that it will compromise the client organization in the future. Therefore, the decision maker is concerned that a vulnerability that copies and sends the run configuration file to an adversary could be introduced in the firewall's supply chain. The nature of the run configuration file also provides a high degree of plausible deniability[**]. Also, firewalls typically maintain a certain configuration for months or years.

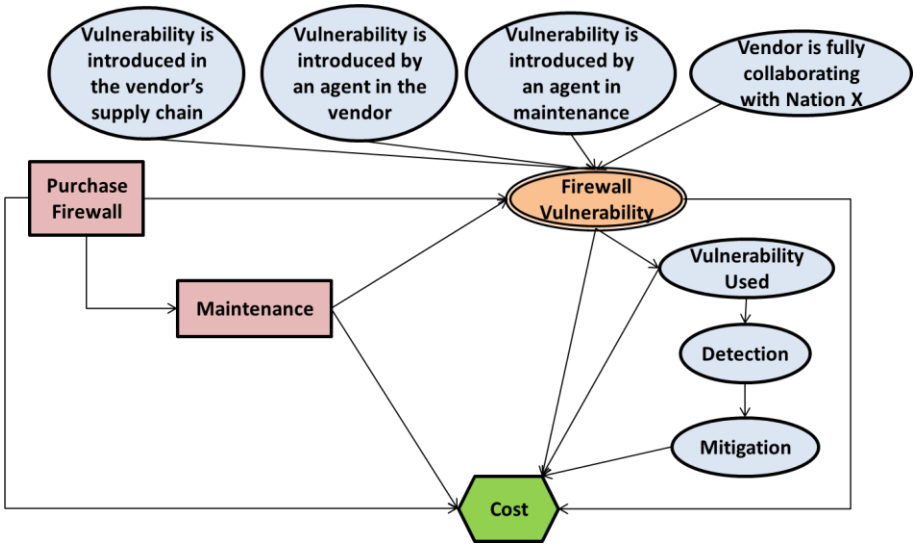
[**] The run configuration file is typically on the order of kilobytes, meaning a file transmission could blend into network traffic easily.

Therefore, the information obtained by the adversary about the network security would remain useful for a substantial length of time. This is the vulnerability described in the model presented here.

3.2. Decision Diagram

A decision diagram for the decision maker is shown in Figure 2. He/she will first choose a firewall and maintenance plan. If either of the producing companies is fully cooperating with the adversary nation X, the decision maker assumes that a vulnerability will be introduced with probability one, since it is technically feasible. If this collaboration does not occur, the adversary can attempt to introduce the vulnerability through company's vendors who supply materials such as chips, software, or other components of the firewall. The vulnerability could be introduced in the supply chain several tiers below the main supplier unless effective security practices are followed. The adversary may also introduce an agent into the company. An agent is defined here as a person or group of people directed by an adversary (forcefully or willfully) to implement a vulnerability in the client's system. The definition encompasses blackmail, bribery, and agent infiltration. Agents who attempt to plant the vulnerability may be unsuccessful due to security restrictions, or because it is not technically feasible in the particular production phase that they have infiltrated. Finally, the adversary may introduce the vulnerability through maintenance since code updates may not be as thoroughly tested as the original product.

Figure 2: Decision Diagram for the purchase of a fire wall



The decision maker, even if he/she is aware of a breach, may not know with certainty whether the adversary will actually use the vulnerability that was introduced. In this study, we assume that the run configuration file is always exploited if a vulnerability is introduced in it, but we include an uncertainty about its actual use, which would increase the probability its detection. An option for the decision maker is to inspect the system to try to detect intrusions.

3.3. Supply Chain Model

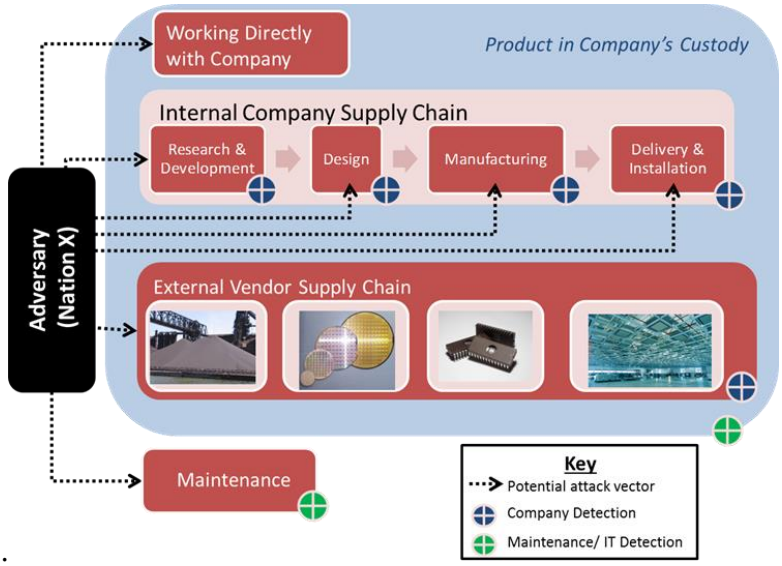
The probability that a vulnerability is successfully inserted in a product's supply chain depends on the stage at which it was introduced, the difficulty of insertion at different stages, and the likelihood that it is detected later in the manufacturing process. Our model of the supply chain for an enterprise firewall was developed to study how the likelihood of a successful insertion changes through the supply chain lifecycle, and the chances of detection through inspection of the product.

The structure and secrecy of IT supply chains makes this analysis difficult in practice. Most companies consider supply chain information to be proprietary, leading to a lack of publically available data on

the number of suppliers, their locations and the nature and frequency of attacks. Tiered suppliers make tracing components back to original sources difficult as well. Subcontractors are often nested several (often three) layers deep below the main contractor, making it difficult to track products' security. Multiple vendors may be involved in the manufacturing of the components[††]. Supply chains often overlap, but their lack of transparency makes the understanding of common risks nearly impossible[‡‡]. Villasenor presents a comprehensive overview of other challenges in assessing the overall security of a supply chain [30].

A firewall production lifecycle consists of several basic steps: research and development, design, manufacturing, and delivery/ installation[§§]. During this process, components from external vendors may be integrated into the product. Each of these phases presents an opportunity to introduce or detect a vulnerability. Figure 3 shows the possible attack vectors.

Figure 3: Supply Chain vulnerabilities



For a vulnerability to exist, it must be introduced in a phase *i* and not be discovered in any subsequent phase *p*. The probability *P(V)* that the vulnerability remains in the system into its operation is thus simple if one assumes independence of attempts to insert and detect vulnerabilities at different stages of the supply chain:

$$P(V) = \sum_{i=1}^{n} P(S_i)\left(\prod_{p=i}^{n}\left(1 - P(F_p)\right)\right)$$

in which:

$P(S_i)$ is the probability that a vulnerability is introduced in Stage *i*

$P(F_p)$ is the probability that a vulnerability is found in stage *p*

Decomposing the probability of a vulnerability introduction in different phases of the supply chain simplifies the data needed to populate the model by conditioning each event on the phase in the supply chain where it takes place.

3.4. Expert Probability Elicitation

[††] For example, a manufacturer may run out of a RAM chip made from vendor A and substitute a chip from vendor B.

[‡‡] For example, a CPU chip vendor may supply company A and company B with the same chip.

[§§] Note that the usage and disposal are not modeled, due to the limit scope of the model.

To populate the model with probability inputs, interviews were conducted with four experts with backgrounds ranging from network security to firewall manufacturing[***]. The Delphi method was used to obtain and integrate expert probability elicitations [32]. Each interview was prefaced with the list of definitions for each supply chain phase and two rounds of interviews were conducted, after which the responses were averaged and used as inputs to the model. Despite considerable efforts to make the questions unambiguous, experts often made implicit assumptions that led to probability estimations that differed by orders of magnitude. Eliminating ambiguities in the elicitation questions will thus be essential in future studies. A summary of the data obtained from the expert probability elicitation and other input data is contained in Table 1, for the comparison of two different firewalls (A and B) and two maintenance options for each (maintenance from supplier or from another firm C).

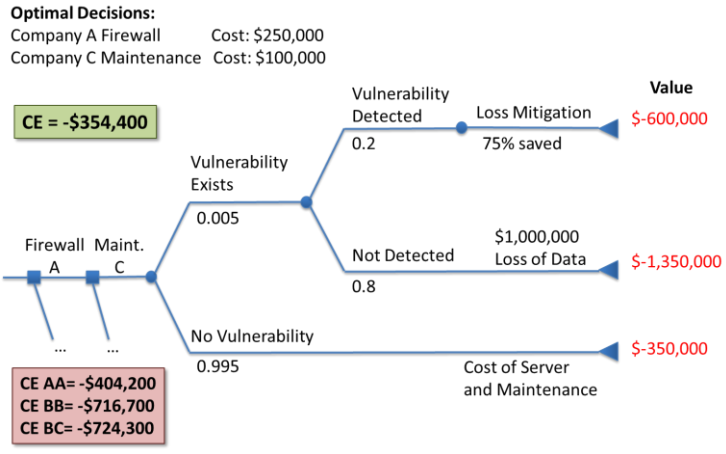
Table 1: Input data and firewall comparison: expert opinions on introduction of vulnerabilities

Options	Cost	Probability
Firewall A	$250,000	
Firewall B	$150,000	
Maintenance A (lifetime)	$150,000	
Maintenance B (lifetime)	$50,000	
Maintenance C (lifetime)	$100,000	
Run Configuration File Stolen	-$1,000,000	
Vul. in Firewall A, Maint. A		0.00513
Vul. in Firewall A, Maint. C		0.00518
Vul. in Firewall B, Maint. B		0.608
Vul. in Firewall B, Maint. C		0.558
Prob. Detection | Vul. AA		0.25
Prob. Detection | Vul. AC,BB, BC		0.20
% of Damages Mitigated | Detection		0.75

4. Decision Analysis for the Choice of a Vendor and Maintenance Operator

After the expert probability elicitation, the data were entered into a decision tree along with the costs defined in the original problem statement to determine the optimal choice of a supplier and of a maintenance company.

Figure 4: Decision Tree for the choice of supplier and maintenance organization



We found that in this illustrative case, the optimal decision for the client organization (assumed first, to be an expected value maximizer) is to buy company A's firewall and company C's maintenance

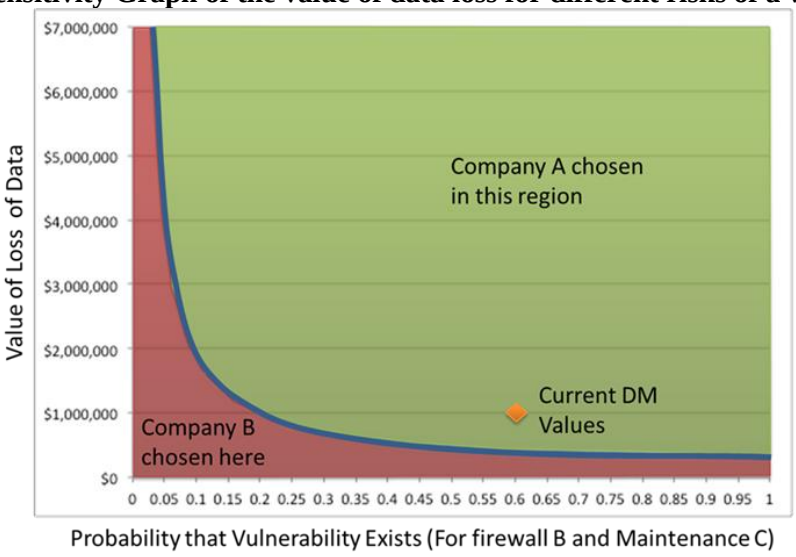
[***] More experts are needed to ensure accurate results, but four experts allowed an effective demonstration of the model for this illustrative scenario. For an example of the Delphi method applied to IT risk, see Herrmann [31].

(see Figure 4). A sensitivity analysis was performed for all input probabilities and different risk tolerance levels. It showed that the decision is fairly robust. The value of perfect information is found to be only $5,800 for a risk neutral decision maker.

4.1. Analysis

The decision between company A and company B is often simple if the client organization places a high value on losing data or if the probability of a vulnerability is significantly different between the two companies. These two metrics are compared in Figure 5. The analysis assumes that the price difference between the two firewalls is $100,000. Therefore, for the risk neutral decision maker, the expected loss due to the increased risk must be less than $100,000 for company B to be chosen. Figure 5 shows the tradeoff, which offers a simple way for decision makers to decide if more analysis is needed.

Figure 5: Sensitivity Graph of the value of data loss for different risks of a vulnerability



4.2. Inspection

Various controls have been proposed to reduce the probability that a vulnerability is successfully introduced in a supply chain. Most software comes with a checksum[†††], which detects code differences between the original source and the installed application. However, vulnerabilities introduced during the firewall software development would not be detected using checksums. Large organizations often rely on "many eyes" to detect vulnerabilities, claiming that it is infeasible for an adversary to maliciously tamper with their product. However, empirical evidence suggests that "many eyes" do not prevent vulnerabilities if they look for the same things, even in open source applications. For instance, enough incidents of malicious code insertion by disgruntled employees have occurred to raise doubt about an organization's ability to detect unauthorized insider activity[‡‡‡] [33, 34].

Given the uncertainty surrounding vulnerability insertions and the effectiveness of many proposed controls, a quantitative analysis of security measures is useful. One option is to inspect incoming products. Firewalls could be dismantled to look for suspicious components and executable files could

[†††] A checksum function works by computing a string of bits corresponding to the code. Standard algorithms of that type are very difficult to defeat by reverse engineering because any change in the original code will change the checksum value and alert a user that the code has been compromised. In a sense, it is almost a "tamper-evident" seal.

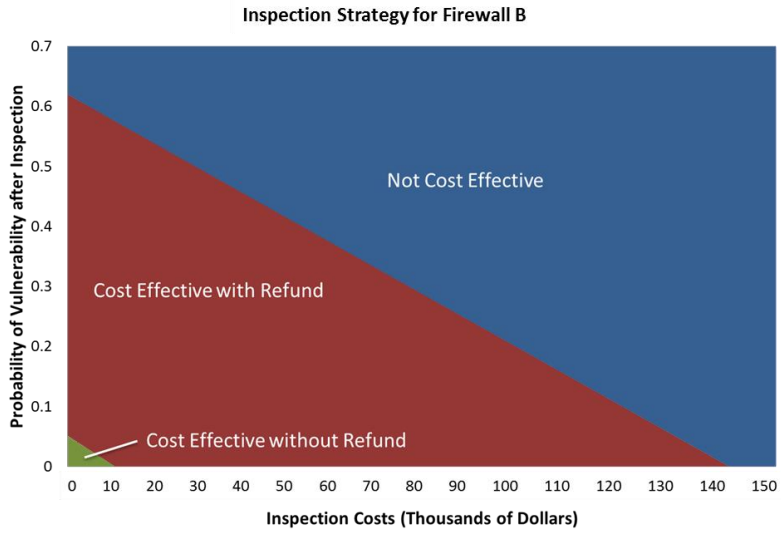
[‡‡‡] The frequent occurrence of "Easter Eggs", or secret features inserted into software or hardware such as a flight simulator in Excel 1997, also suggest that code development is not secure.

be reviewed for strange activity[§§§]. However, dismantling a firewall to look for hardware or software vulnerabilities is labor- and cost-intensive with uncertain outcomes. Our model can help a decision maker determine if products should be inspected and what investment in inspection is cost-effective.

If firewall B is purchased, a perfect inspection that finds all vulnerabilities is worth $142k to a risk neutral decision maker, assuming that a refund is given when vulnerabilities are found in a firewall. If refunds are not given, perfect inspection is worth only $12k. In reality, perfect inspection cannot reasonably be obtained. Instead, a decision maker should evaluate by how much the prior probability of a vulnerability in the product can be reduced by a given level of inspection. For example, if after spending $100k on inspection, the decision maker believes that the probability of a vulnerability in firewall B can be reduced from the prior of 0.608 to a posterior of 0.1, then the investment is cost-effective. However, given the complexity of the firewall hardware and software, if the decision maker thinks that a $100k inspection would only reduce the posterior probability of vulnerability detection to 0.4, then the inspection is not cost-effective. Figure 6 shows the cost-effective investment ranges for firewall B.

A decision maker might also decide to invest some amount of money to inspect firewall A. In this illustrative case and given the figures that were chosen, the probability of a vulnerability can only be reduced from the 0.005, which is the prior. The value of inspection is much lower: a perfect inspection value is only $2.2k.

Figure 6: Inspection Costs



5. CONCLUSION

Regarding the cyber security of supply chains and the benefits of inspection to detect vulnerabilities, there are many qualitative reports and best practice statements, but to the best of our knowledge, no quantitative tools have been proposed to help organizations mitigate that risk. Supply chain attacks are complex problems, involving dozens of manufacturers, hundreds of vulnerabilities, and thousands of components. The model presented in here involves only one attacker and one vulnerability. It can be expanded to include multiple adversaries and multiple attacks.

We start here from the observation that the frequency of cyber attacks related to information systems supply chains has increased over the past 30 years. One can reasonably assume that it is likely to continue to increase. Using data from expert probability elicitation, we modeled such a supply chain to calculate the probability that a successful vulnerability is introduced and undetected in a firewall at

[§§§] The source code, which contains comments and is designed to aid engineers in the analysis and verification of a code, is not included in most applications. The executable code is considerably more difficult to analyze.

each stage of its production lifecycle. We find that product inspection is rarely cost-effective, and we show how one can quantify and communicate the tradeoff between price and security using simple graphs. In comparing supply options, one should thus not count solely on the chances of detecting vulnerabilities through product inspection, but consider alternatives (or complements) such as signal monitoring, signature- or anomaly-based detection, and other warning systems to improve the security of organizations.

Acknowledgements

The authors would like to thank Steve Hurd, Alex Keller, and Matthew Daniels for their expertise and guidance for this paper. The authors also thank 4 anonymous experts who participated in the expert probability elicitation.

References

[1] K. A. Wolnik, F. L. Fricke, E. Bonnin, C. M. Gaston, and R. D. Satzger. *"The Tylenol tampering incident-tracing the source"*, Analytical chemistry 56.3, 466A-474A, (1984).
[2] M. Beck, M. Hagar, R. LaBreque, S. Monroe and L. Prout. *"The Tylenol Scare"*, Newsweek. 11 October 1982.
[3] C. Arthur. "*Get yer malware with fries, or on your new video iPod*," The Guardian. 18 October 2006.
[4] R. McMillan. *"Virus located in TomTom GPS systems*," InfoWorld. 29 January 2007.
[5] A. Modine. "*Organized crime tampers with European card swipe devices*", The Register. 10 October 2008.
[6] S. Gorman. "*Fraud Ring Funnels Data From Cards to Pakistan*", Wall Street Journal. 11 October 2008.
[7] H. Samuel. *"Chip and pin scam 'has netted millions from British shoppers',"* The Telegraph. 10 October 2008.
[8] J.S. Lublin and S. Raice. *"Security Fears Kill Chinese Bid in U.S,"* Wall Street Journal. 5 November 2010.
[9] S. Prasso. "*What makes China telecom Huawei so scary?"* Fortune. 28 July 2011.
[10] J. Kyle, C. Bond, R. Shelby, J. Inhofe, J. Bunning, J. Sessions, R. Burr, S. Collins. Letter to Secretary Geithner, Secretary Locke, Administrator Johnson, and Director Clapper. 18 August 2010.
[11] K. Hille and P. Taylor. "*Huawei 'not interested in the US any more"*", The Financial Times. April 23, 2013.
[12] C. Thompson. *"Huawei plans to tackle US market with huge new smartphone*," CNBC. 6 January 2013.
[13] S. Chopra and M. S. Sodhi. "*Managing risk to avoid supply-chain breakdown,"* MIT Sloan Management Review. (Fall 2004)
[14] C. S. Tang. "*Perspectives in supply chain risk management*," International Journal of Production Economics, 103.2, 451-488, (2006).
[15] H. Cavusoglu. S. Raghunathan, W.T. Yue. "*Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment",* Journal of Management Information Systems, Vol. 25, No. 2, pp. 281–304, 2008.
[16] K. J. Soo Hoo. "*How Much Is Enough? A Risk-Management Approach to Computer Security*", 2000.
[17] R. Bojanc, B. Jerman-Blazic, M. Tekavcic. "*Managing the investment in information security technology by use of a quantitative modelling*", Information Processing and Management, 48, 1031–1052, (2012).
[18] N. Xie. "*SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies*", Software Engineering Institute. 2004.
[19] L.A. Gordon and M.P. Loeb. "*The Economics of Information Security Investment*", ACM Transactions on Information and System Security, Vol. 5, No. 4, Pages 438–457, (2002).

[20] D.L. Buckshaw, G.S. Parnell, W.L. Unkenholz, D.L. Parks, J.M. Wallner, O.S. Saydjari. "*Mission Oriented Risk and Design Analysis of Critical Information Systems*". Military Operations Research, 10.2, 19-38, (2005).
[21] A. Roy, D.S. Kim, K.S. Trivedi. "*Cyber security analysis using attack countermeasure trees",* In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (p. 28). ACM. (2010)
[22] E.M. Hutchins, M.J. Clopperty, R.M. Amin. "*Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*", Leading Issues in Information Warfare & Security Research, 1, 80, (2011).
[23] R.A. Miura-Ko. "*Modeling and Mitigation of Information Technology Risks*," 2010.
[24] White House. "National Strategy for Global Supply Chain Security", 2012.
[25] G.C. Wilshusen et al. "*IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*", United States Government Accountability Office. March 2012.
[26] M.L. Goldstein et al. "*Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment*", United States Government Accountability Office. 21 May 2013.
[27] J. Boyens, C. Paulsen, N. Bartol, S.A. Shankles, R. Moorthy. *"Notional Supply Chain Risk Management Practices for Federal Information Systems*", National Institute of Standards and Technology. 2012.
[28] J. Boyens, C. Paulsen, N. Bartol, S.A. Shankles, R. Moorthy. "*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*", National Institute of Standards and Technology. 2013.
[29] J. Villasenor. "*Compromised By Design? Securing the Defense Electronics Supply Chain*", Brookings. 2013.
[30] R.J. Ellison, J.B. Goodenough, C.B. Weinstock, C. Woody. "*Evaluating and Mitigating Software Supply Chain Security Risks",* Software Engineering Institute. May 2010
[31] A. Herrmann. *"The Quantitative Estimation of IT-Related Risk Probabilities*." Risk Analysis, Vol. 33, 8, 1510-1538. (2012).
[32] H.A. Linstone and M. Turoff. "*The Delphi method: Techniques and applications*", 2002.
[33] G. Schryen. "*Security of open source and closed source software: An empirical comparison of published vulnerabilities",* (2009).
[34] J. Vijayan. "*Unix Admin Pleads Guilty to Planting Logic Bomb*", PC World. 21 September 2007.