Mathematical Model of Distributed Vulnerability Assessment

Kálmán Hadarics
hadarics@uniduna.hu
Secudit, University of Dunaújváros
Veszprém, Dunaújváros, Hungary

Krisztina Győrffy
gyorffyk@upcmail.hu
Secudit
Veszprém, Hungary

Dr. Bálint Nagy
nagyb@uniduna.hu
University of Dunaújváros
Dunaújváros, Hungary

Dr. László Bognár
drbognar@gmail.com
University of Dunaújváros
Dunaújváros, Hungary

Dr. Anthony Arrott
aarrott@checkvir.com
Secudit
Veszprém, Hungary

Dr. Ferenc Leitold
fleitold@secudit.com
Secudit
Veszprém, Hungary

Abstract

Electronic information systems are used in nearly every area of life today. Besides computers smart and IoT devices turn up. However, when IT systems are used online there are cyber-threats too. The so called cyber criminals can steal unauthorised data and credentials by means of malicious codes or can have a harmful effect on IT security. If we want to observe the protection of an IT system and infrastructure against threats we must consider several relevant relating parameters. Three factors are identified in the applied model of cyber-threats – Distributed Vulnerability Assessment (DVA):

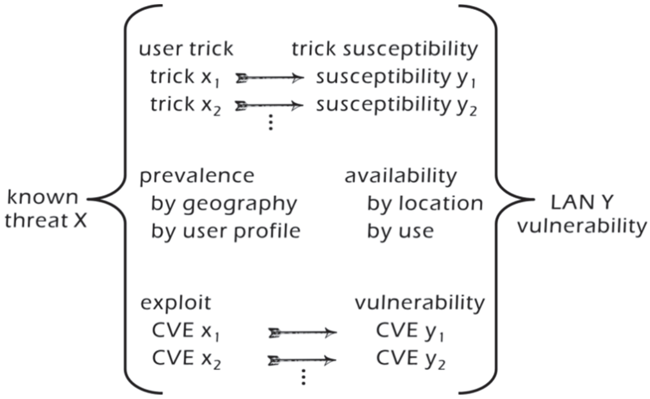
1. characteristics and prevalence of harmful cyber-threats;
2. vulnerabilities of IT infrastructure and its processes;
3. vulnerabilities deriving from users' behaviour.

There is further information of the models used for assess the risk of threats in [6] and [7].

Using a metric, the impact of a threat typical of a given infrastructure can be determined with a mathematical model. This metric means the probability of at least one threat attacking successfully at least one device in the IT infrastructure used by the given users. All available information must be considered in the case of the three cornerstones for the operation of the model. Such information is the prevalence, the necessary hardware and software elements or the demanded user activity. In the case of user behaviour, the most important characteristic is when and how the user uses the IT devices, to what extent he tends to open e-mail attachments or visit unknown web sites. In the case of IT infrastructure what hardware or software elements are present or absent and how they affect the operation of the observed harmful code.

This, obviously, relates to the protection systems installed on the devices of the IT infrastructure.

DVA provides a LAN-by-LAN measurement of cyber-attack vulnerability. The vulnerability of both the specific LAN users and LAN IT infrastructure are assessed for individual known threats and aggregated across the current threat landscape relevant to the particular LAN. The integrated cyber-attack vulnerability of a particular LAN is evaluated based on the prevalence and effectiveness of current known threats; the current susceptibility of LAN users; and the current penetrability of LAN IT infrastructure.



Assessed separately for each threat at each LAN

Using our mathematical approach the integrated vulnerability is decomposed and distributed to the contributing elements of individual user susceptibility, individual IT infrastructure elements, and the individual protecting cybersecurity services and applications. From the DVA results, vulnerability is quantitatively attributed to the various internal contributing components (e.g., user identities, ports, protocols, protection layers). This allows different contributing components to be assessed using comparable metrics (e.g., user security awareness vs. infrastructure patch condition vs. efficacy of anti-malware). DVA allows information security managers to pose and compare the results of "what if" queries to see the vulnerability reduction of various available options that might not otherwise be quantitatively comparable (e.g., investment in employee security awareness programs vs. hardening IT infrastructure vs. adding additional cybersecurity applications and services. The framework, formulae, and relevant examples of applying DVA to single LAN and multiple LAN enterprise networks are described.

This paper describes our model capable of determining the metric of threats. The paper includes the applied mathematical formulae to present the practical application of the model.

Keywords: distributed vulnerability assessment, continuous penetration testing, cybersecurity vulnerability metrics, user susceptibility to cyber-attack social engineering.

1 Introduction

To succeed, a malware attack directed against a protected target network requires successful execution of the malicious code by the protected IT with sufficient authorized user facilitation to subvert the network security. Minimally, user facilitation may be as simple as having the endpoint device powered on and connected to the Internet. Cybersecurity metrics have tended to focus on protected IT (e.g., ongoing penetration testing) [11] and malicious activity (e.g., breach detection testing) [4]. User behaviour cybersecurity metrics are less developed [2], although network traffic monitoring provides rich opportunities for their development (e.g., NetFlow/IPFIX). In addition to passive monitoring, interactive metrics can also be deployed, for example, probing user responses with fake phishing [1].

From a defender viewpoint, successful malicious attacks can be conceptually represented as occurring at the intersection of malicious activity acting on protected IT infrastructure, facilitated by sufficient authorized user behaviour. This conceptual framework builds on the operational formulation used by NSS Labs [5,12]. It is intended as a practical and convenient simplification of a more rigorous and complete treatment of attack surfaces [10]. Here we are focused exclusively on human-interactive endpoints (IT) as opposed to the security architecture of embedded systems (IoT, OT) [14]. For our purposes here, three distinct but highly interactive sources of vulnerability are considered:

1. Malicious activity by those who would subvert network capabilities for their own gain in violation of intended trusted relationships within the protected IT network;
2. Disruptive and dangerous IT behaviours by network users (e.g., employees, customers, suppliers) in using IT network capabilities; and
3. Unprotected vulnerabilities in the IT network infrastructure.

The most critical vulnerabilities in IT networks lie at the intersection of these three areas. Addressing these vulnerabilities requires sufficient visibility, scrutiny and discrimination to observe, understand, and take effective action to mitigate them.

Visibility of present and emerging vulnerability is most effectively achieved by vigilance in an ongoing risk analysis that combines observations in each of the three areas (Figure 1).

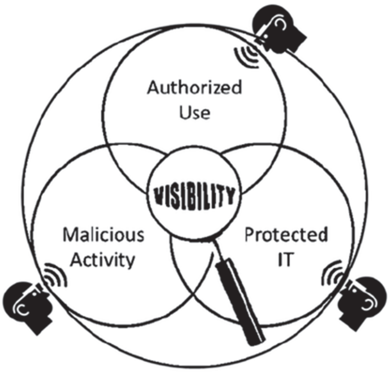


Figure 1: Components and contributing factors to IT network vulnerability can be segmented into three areas each of which has its own sets of methods and tools for visibility, scrutiny, and discrimination.

Visibility into information transaction vulnerabilities that threaten the wellbeing of an enterprise is a necessary but, by itself, completely insufficient requirement for enterprise cybersecurity. Vulnerability assessment may be thought of as the outermost layer in the ongoing provision of enterprise cybersecurity. The succeeding layers include: vulnerability detection, vulnerability remediation, security incident preparedness, security incident detection, and security incident response (Figure 2).

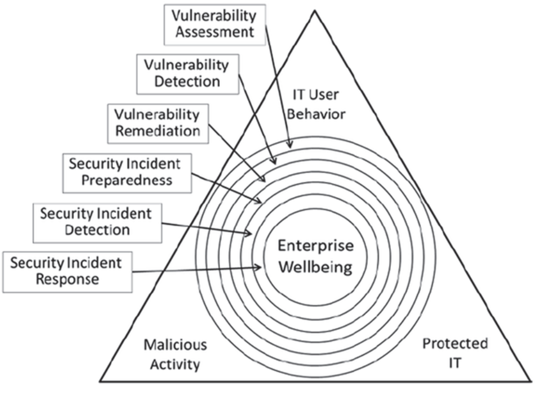


Figure 2: Vulnerability assessment is placed within the context of overall cybersecurity contribution to enterprise wellbeing.

To effectively contribute to enterprise wellbeing, vulnerability management requires practical and useful correlation of the various and highly interactive sources of vulnerability. The analogous requirement for security incident response is typically satisfied by security event information management systems (SEIM) [13]. For vulnerability management, we have adopted what we define as the Triunal Model of Cybersecurity Vulnerability. Derived from earlier formulations [8,9], the triunal model decomposes vulnerability assessment into three contributing sources, or triunes: i) malicious activity; ii) unprotected IT; and iii) facilitating adverse user behaviour. Within each contributing source, specific contributing factors are identified and characterized (e.g., social engineering and exploits within the malicious activity triune). The model provides a basis for correlating and combining contributing factors into an integrated view of specific vulnerabilities.

2 Malicious activity by threat actors

We first consider malicious activity by those who would subvert network capabilities for their own gain in violation of intended trusted relationships within the protected IT network. Cybersecurity in this area is largely achieved through prevention, detection, and deflection of malware attacks using commercially-available automated software applications and appliances.

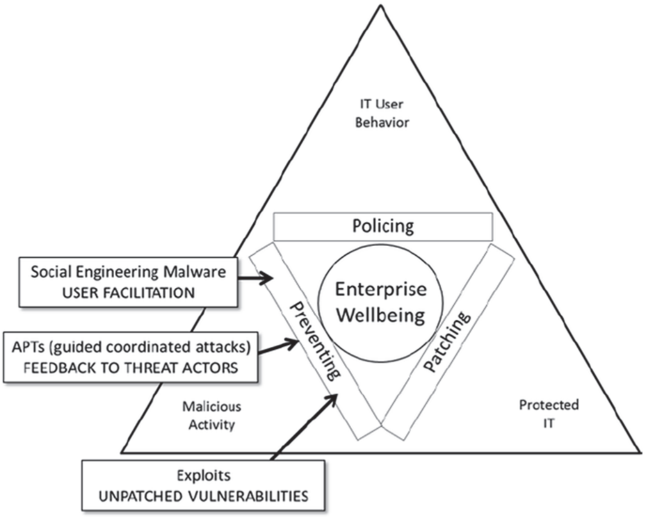


Figure 3: Typical sources of malicious activity vulnerabilities.

Malicious activity typically focuses on attack prevention weaknesses in the target victim's IT network and usage in the form of: (i) user facilitation (social engineering malware); (ii) feedback to threat actors from within the organization network (guided coordinated attacks, aka APTs); and (iii) malicious exploits of known & unknown vulnerabilities (Figure 4). Available methods for measuring vulnerabilities include malware susceptibility testing, breach detection testing, and exploit advance warning.

3 Deployed IT network vulnerabilities

Secondly, we consider unprotected vulnerabilities in an enterprise's deployed IT network infrastructure. This includes both the traditional concept of a walled network with controllable gateways as well as all the extended networks that interpenetrate the enterprise network (largely due to mobility and cloud services) [3]. Cybersecurity in this area is largely achieved through vigilant IT network maintenance and effective operation including up-to-date patching and upgrading of component IT infrastructure.

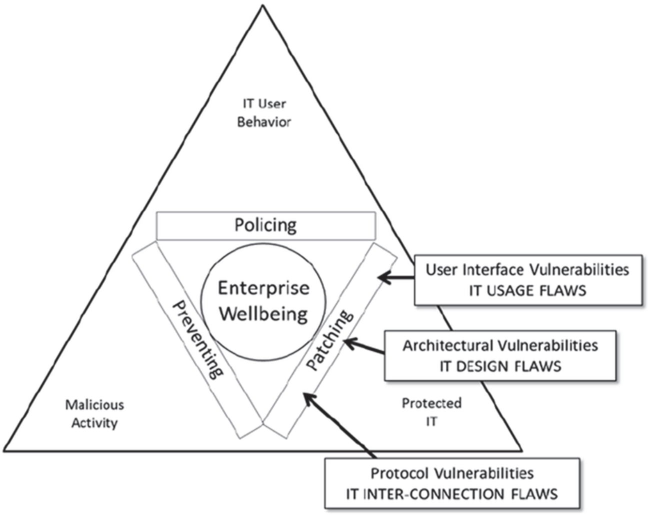


Figure 4: Typical sources of IT infrastructure vulnerabilities.

Unprotected IT infrastructure vulnerabilities typically appear as system and applications patching shortcomings in the form of: (i) user interface vulnerabilities (IT usage flaws); (ii) IT architectural vulnerabilities (IT design flaws); (iii) protocol vulnerabilities (IT interconnection flaws) (Figure 5). Available methods for measuring IT infrastructure vulnerability include penetration testing, application security testing, and port scanning.

4 User behaviour vulnerabilities

Finally, we consider vulnerabilities due to disruptive and dangerous IT behaviors by the users of enterprise IT network capabilities. Cybersecurity in this area is largely achieved through policy which is implemented and maintained primarily through training, security awareness, identity privilege management, and user behavior monitoring.

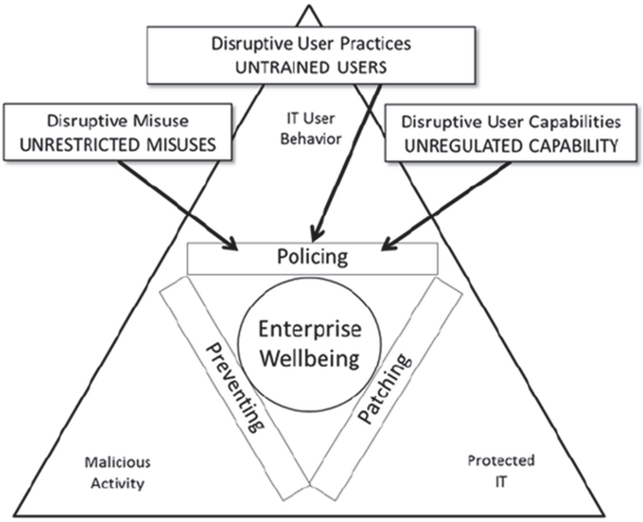


Figure 5: Typical sources of IT infrastructure vulnerabilities.

Disruptive and dangerous usage of IT networks typically appears as anomalies in baseline (normative) user behaviours in the form of: (i) unrestricted misuses; (ii) untrained and naïve user behaviours; (iii) unregulated user capabilities (Figure 6). Available methods for measuring IT user behaviour vulnerabilities include access control testing, user proficiency assessment, and behaviour anomaly detection

5 Combining sources of vulnerability

Let’s start with some definitions:

L: set of all available threat landscapes (eg.: World, Europe, USA, Hungary, …)
T$_{all}$: set of all possible malware
T$_l$: set of all possible malware inside $l \in L$, $T_l \subset T_{all}$
U: set of all users
I: set of all possible devices

P: set of all available protections
UT: set of all possible user tricks used by any malware in T

An integrated measure of vulnerability can be derived accounting for all three sources (attacker ingenuity, infrastructure weakness and adverse user behaviour). For any given threat or class of threats for which the requisite IT infrastructure vulnerability and user facilitation is known, we can obtain a best estimate of:

1. The probability that an attacker will use a particular threat or class of threats against the enterprise (p_{prev}):

$$p_{prev}(t,l) = \frac{number\ of\ computers\ infected\ by\ \boldsymbol{t}\ inside\ \boldsymbol{l}}{number\ of\ all\ comupters\ inside\ \boldsymbol{l}}$$

   where $t \in T_l$ and $l \in L$. Note, that p_{prev} can be based on a measurement or estimation and must be related to a time interval (ΔT).

2. The probability that the enterprise's IT infrastructure will allow the attack to be carried out successfully (p_{device}):

$$p_{prot}(t,p)$$

$$= \frac{number\ of\ successfull\ attempts\ of\ \boldsymbol{t}\ thru\ the\ protection\ \boldsymbol{p}}{number\ of\ all\ attempts\ of\ \boldsymbol{t}\ thru\ the\ protection\ \boldsymbol{p}}$$

   where $t \in T_l$, $l \in L$ and $p \in P$;

$$p_{device-prot}(t,i) = \min_{for\ all\ p\ protecting\ i} p_{prot}(t,p)$$

   where $t \in T_l$, $l \in L$ and $i \in I$;

$$p_{device-elements}(t,i) = \begin{cases} 1, if\ t\ can\ work\ on\ i \\ 0, if\ t\ can\ not\ work\ on\ i \end{cases}$$

   where $t \in T_l$, $l \in L$ and $i \in I$;

$$p_{device}(t,i) = p_{device-elements}(t,i) \cdot p_{device-prot}(t,i)$$

   where $t \in T_l$, $l \in L$ and $i \in I$;

3. The probability that users of the enterprise's IT infrastructure will provide sufficient facilitation for the attack to succeed (p_{user}):

$$p_{usertrick}(t,ut) = \frac{number\ of\ attempts\ of\ \boldsymbol{t}\ where\ t\ used\ \boldsymbol{ut}}{number\ of\ all\ attempts\ of\ \boldsymbol{t}}$$

where $t \in T_l, l \in L, ut \in UT$;

$$p_{user-usertrick}(u,ut) = \frac{number\ of\ successfull\ attempts\ of\ \boldsymbol{ut}\ on\ \boldsymbol{u}}{number\ of\ all\ attempts\ of\ \boldsymbol{ut}\ on\ \boldsymbol{u}}$$

where $u \in U$, $ut \in UT$;

$$p_{user}(u,t) = 1 - \prod_{for\ all\ ut\ used\ by\ t} (1 - p_{usertrick}(t,ut) \cdot p_{user-usertrick}(u,ut))$$

where $u \in U$, $t \in T_l, l \in L$, $ut \in UT$;

These three probabilities (p_{prev}, p_{device}, p_{user}) can be combined to obtain an overall probability of malicious success, (provided each relevant combination of attack, user, and component of IT infrastructure is accounted for) [6]. The (p_{prev}, p_{device}, p_{user}) values are related to a given threat, a given user and a given device. The aggregated vulnerability would be a metric of the whole organization related to all of the users, all of the devices and all of the possible threats.

$$p_s(l) = 1 - \prod_{for\ all\ t,u\ and\ i} (1 - p_{user}(t,u) \cdot p_{device}(t,i) \cdot p_{prev}(t,l))$$

where $u \in U$, $t \in T_l, l \in L$, $i \in I$;

In this chapter, we assumed the followings:

- the attacker usage of the given threat, the IT infrastructure allowance and the user acceptance are different from each other;
- all of the attack attempts are independent from each other;

- the computer usage behaviours of all users are the same and equal to the average usage in the organization;
- the calculated $p_s(l)$ value is related to the same ΔT interval as the original p_{prev} was related to.

6 The contribution of users' computer usage

In the chapter 5 we assumed that the computer usage behaviours of all users are the same and equal to the average usage in the organization. In fact, it is not true: the behaviours of users are usually different. Now let us examine how can we handle the different computer usage.

Let us define the probability of the successful attack as p_0. So, it is related to a piece of an attack attempt. If the attacker is able to attack multiple times (*n* times), then the probability of at least one attack attempt is successful:

$$p_n = 1 - (1 - p_0)^{n}$$

Using this formula, if

$$p_n = 1 - (1 - p_0)^{n} \text{ and}$$

$$p_m = 1 - (1 - p_0)^{m}$$

and they are related to *n* and *m* attack attempts, then

$$p_m = 1 - (1 - p_n)^{m/n}$$

On the other hand, if we assume that the number of attack attempts are in proportion with the time interval available for the attacker, then

$$p_{T1} = 1 - (1 - p_{T2})^{T1/T2}$$

where p_{T1} and p_{T2} are the probabilities of at least one successful attack attempt has occurred in the time interval T1 and T2. We can use this approach in two ways:

- if we are looking for the vulnerability of an organization related to another time interval,
- if a particular user uses a computer for other time interval than the average users.

On the other hand, computer users may have other modification element as well. Let us assume that there are to main attack vectors: malicious emails and malicious urls. If there is a user that open emails/open new urls in the browser with much more frequency than the average, then, of course it should be related to a much dangerous user. This is because this user enables much more attempts for the attacker. If he/she open twice more new urls, it results twice more attempts. So, let us define the following user related value for each threat (it can be identical for threats of the same threat type):

$$\mu(t,u) = \frac{number\ of\ attempts\ of\ \boldsymbol{t}\ are\ enabled\ by\ the\ user\ \boldsymbol{u}}{number\ of\ attempts\ of\ \boldsymbol{t}\ are\ enabled\ by\ the\ average\ user}$$

Using the mentioned approaches, we can make changes in the equation in chapter 5:

$$p_s(l) = 1 - \prod_{for\ all\ t,u\ and\ i} (1 - p_{user}(t,u) \cdot p_{device}(t,i) \cdot p_{prev}(t,l))^{k(t,u)}$$

where $u \in U$, $t \in T_l$, $l \in L$, $i \in I$ and

$$k(t,u) = \frac{T}{\Delta T} \cdot \frac{T_u}{T_{average}} \cdot \mu(t,u)$$

where

ΔT is the base time interval where the prevalence values are related to,

T is the time interval we would like to estimate the vulnerability for,

T_u is the time interval when the given user uses the computer in a time unit,

$T_{average}$ is the time interval when the average user uses the computer in the same time unit and

$\mu(t,u)$ is a constant related to each pair of threat and user defined above.

7 Summary

A non-independent three-dimensional framework of malicious activity, user behaviour, and IT infrastructure can be used to assess the vulnerability of a specific organization to successful malicious attack from its current surrounding cyber-threat landscape. The method utilizes three sources of information: external cyber-threat intelligence ("security intelligence"), organization IT infrastructure weakness ("penetration testing"), and the susceptibility of the organization's IT users to facilitating cyber-attacks ("user behaviour"). The method allows the measured sources of vulnerability to be systematically combined into a metric of overall vulnerability which can be decomposed into comparable contributing relative vulnerabilities from each source. The method quantifies the evolution of relative vulnerabilities over time, separately measures the vulnerability of individual departments (LANs) and to specific classes of cyber-threats (e.g., ransomware, phishing). In addition, the method predicts the consequences of potential remedial actions ("What ifs?"), thus aiding cyber-security decision-making specific to an organization's unique situation.

References

[1] CHAPMAN M.T. (2015), "Advanced Persistent Testing: How to fight bad phishing with good." PhishLine, http://www.phishline.com/advanced-persistent-testing-ebook

[2] CHAPMAN, M.T. (2013), "Establishing metrics to manage the human layer." ISSA Security Education Awareness Special Interest Group.

[3] COLON OSORIO, F.C., and A. Arrott (2016), "Fabric of security - changing our theory and expectations of modern security". Proceedings of Eastern European eGov Days Conference, EEGOV, Budapest, Hungary.

[4] EDWARDS, S.E., R. Ford, and G. Szappanos (2015), "Effectively testing APT defenses". Virus Bulletin Conference, Prague, Czech Republic.

[5] FREI, S. (2013), "Vulnerability threat trends." NSS Labs, Austin, Texas, http://nsslabs.com

[6] LEITOLD, F., A. Arrott and K. Hadarics (2016), "Quantifying cyber-threat vulnerability by combining threat intelligence, IT infrastructure weakness, and user susceptibility" 24th Annual EICAR Conference, Nuremberg, Germany.

[7] LEITOLD, F., A. Arrott, and K. Hadarics (2016), "Automating visibility into user behaviour vulnerabilities to malware attack" Proceedings of the 26th Virus Bulletin International Conference (VB2016), pp. 16-24, Denver, USA.

[8] LEITOLD, F and K. Hadarics (2012), "Measuring security risk in the cloud-enabled enterprise." Malicious and Unwanted Software (MALWARE), 7th International Conference on Malicious and Unwanted Software, pp: 62-66, ISBN: 978-1-4673-4880-5.

[9] LEITOLD, F. (2010), "Security Risk analysis using Markov Chain Model." 19th Annual EICAR Conference, Paris, France. 2010.

[10] MANDHATA P.K., J.M. Wing, (2010), "An Attack Surface Metric". IEEE Transactions on Software Engineering.

[11] PWNIE EXPRESS. (2014), "Vulnerability assessment and penetration testing across the enterprise". Whitepaper, http://www.pwnieexpress.com

[12] SHAH P, Phatak V, Scipioni R, inventors (2003), "Adaptive intrusion detection system." United States patent application US 10/443,568. 2003 May 22.

[13] SUAREZ-TANGIL G., E Palomar, A Ribagorda, Y Zhang. "Towards an intelligent security event information management system", http://www.seg.inf.uc3m.es/papers/2013nova-AIS-SIEM.pdf

[14] URIBEETXEBERRIA R., MG Eskola, L Trono, S Galileo, JN Movation, L de Celis Acorde, A Morgani, ES Selex, R Baldelli, IE Tecnalia, NP Hai, "New embedded systems architecture for multi-layer dependable solutions", http://www.newshield.eu/wp-content/uploads/2013/11/NSHIELD-D8.6_Build_Secure_Systems_with_SHIELD_v2.pdf