# The Identification of Information Sources to aid with Critical Information Infrastructure Protection

Jean Mouton
Academy of Computer Science and Software Engineering
University of Johannesburg
Johannesburg, South Africa
Email: ujitstudent@gmail.com

Ian Ellefsen
Academy of Computer Science and Software Engineering
University of Johannesburg
Johannesburg, South Africa
Email: iellefsen@uj.ac.za

***Abstract*—Providing Critical Information Infrastructure Protection (CIIP) has become an important focus area for countries across the world with the widespread adoption of computer systems and computer networks that handle and transfer large amounts of sensitive information on a daily basis. Most large organisations have their own security teams that provide some form of protection against cyber attacks that are launched by cybercriminals. It is however often the case that smaller stakeholders such as schools, pharmacies and other SMEs might not have the required means to protect themselves against these cyber attacks. The distribution of relevant and focused information is an important part of providing effective protection against cyber attacks. In this paper some of the existing mechanisms and formats in which information related to software security vulnerabilities are provided to the public are discussed and reviewed. Providing focused and relevant information can enable smaller stakeholders such as SMEs that have a limited set of skills and expertise to limit their risk of exposure to cyber attacks.**

***Index Terms*—Critical Information Infrastructure, Critical Information Infrastructure Protection, Vulnerability Information Sources, CVEs, CVSS, CSIRT, C-SAW Team.**

## I. Introduction

Critical Information Infrastructure Protection (CIIP) has become an important focus for countries across the world with the widespread adoption of computer systems and networks. These computer systems handle and transfer large amounts of sensitive information on a daily basis. The sensitive information, systems and networks are increasingly becoming the targets of cybercriminals that seek to gain financially from interception, alteration, or disruption of these information infrastructures [1].

The traditional view of CIIP will often only take into account large companies or governmental entities that have a primary economic stake in a country. The scope and nature of Internet connectivity has changed how Small and Medium Enterprises (SMEs) and individuals communicate and interact with large national structures to the extent that cyber threats are no longer only the concern of large economic entities. It is now the case that many countries are acknowledging the role of SMEs and individuals in CIIP strategies [2].

The level of actionable knowledge of cyber threats between different communities of SMEs can vary greatly. This is problem is compounded by information relating to cyber threats or software vulnerabilities that might not be in a digestible format to allow CIIP stakeholders gain the full benefit of this information [3]. Furthermore, the amount of information unrelated to a stakeholders computing environment might limit the efficacy of relevant information [4].

This paper aims to discuss the role of collection, filtering and distributing focused information has towards Critical Information Infrastructure Protection efforts. It also aims to discuss how the use of existing information sources, formats and mechanisms can be used to improve and address CIIP towards smaller stakeholders and developing countries that are not always sufficiently covered by existing CIIP efforts.

## II. Critical Information Infrastructure Protection

Critical Information Infrastructure (CII) are the computer systems, networks and other related infrastructures that could have a negative impact on the society or economy if disrupted [5], [6]. These critical systems provide services that support the daily operations of a country and can include online voting, water supply management, electricity supply management and many other services that use sensitive information that could be targeted by cybercriminals [5]. Critical Information Infrastructure Protection (CIIP) can be considered as the provision of support to maintain the normal operations of critical systems or assisting in the recovery of these systems in the event of a computer security incident that caused disruption in the operation of these systems [5]. Larger organisations such as government institutes and corporations often have some form of security team that provide support services in the event of a computer security incident.

A computer security incident can be considered to be the exploitation of some software vulnerability or system configuration that could lead to a compromise of the security of a computer system or network [7]. These computer security incidents are the result of successful attacks launched by cybercriminals to exploit some vulnerability that is present in software or system configuration that could be used to gain unauthorised access to systems.

Computer Security Incident Response Teams (CSIRTs) are some of the most common CIIP structures found in practice

and serves as some of the primary mechanisms used to protect a wide range of stakeholders. In the following section CSIRTs are introduced as a mechanism that is used to provide CIIP services to stakeholders.

## III. Computer Security Incident Response Teams

Computer Security Incident Response Teams (CSIRTs) are Critical Information Infrastructure Protection (CIIP) structures that are aimed at providing incident handling services to their constituencies [8]. A CSIRT constituency is made up of customers that make use of the teams incident handling services and can include groups of individuals, organisations and government bodies [8], [9].

The first CSIRT like structure CERT/CC (Computer Emergency Response Team Coordination Centre) was established as a result of the Morris worm incident in 1988 [10]. CERT/CC was introduced to coordinate security support efforts and respond to computer network emergencies [10], [11].

In the next section the services that a CSIRT provides are introduced.

### A. CSIRT Services

The services that a CSIRT provides to its constituency must at least include some form of incident handling services [11]. Incident handling services are services used to resolve or assist in the process of resolving of computer security incidents that occur [8]. The type of services that a CSIRT provides is dependant on the amount of resources, staff, the technical expertise, and knowledge that the staff that make up the teams have [11].

There are four main categories of services that CSIRTs provide to their constituency: Reactive, Proactive, Artefact Handling, and Security Quality Management Services [12]. Reactive services normally come into play when a security incident is identified and needs to be addressed. Incident handling services fall into the Reactive Services category and as mentioned above is a minimum service required to be provided by any CSIRT instance.

CSIRTs often provide additional services that are not directly used to resolve computer security incidents but are rather focused on the prevention of these computer security incidents [8]. Proactive and Security Quality Management services focus on prevention of computer security incidents rather than addressing them after they occurred [12]. Preventative and educational type services are some of the additional services that a CSIRT provides to its constituency and are normally grouped into the Proactive Services category. These services can include tasks such as educating staff on best security practices; analysis and identification of vulnerabilities in the software and hardware on the constituencies systems; providing advice and information to aid with addressing and resolving identified vulnerabilities [8].

An important part of the CSIRT service provision is the distribution of focused and relevant information that is required to ensure effective services to the constituency that it serves.

The organisational structure that a CSIRT uses is dependent on the constituency that it serves, in the next section we will discuss three general types of CSIRTs that are commonly found.

### B. CSIRT Organisation

There are several types of CSIRTs found in practice that differ according to their operational environment. The three general types of CSIRTs are Internal or Private CSIRTs, National CSIRTs, and Coordination CSIRTs [7].

Internal or Private CSIRTs are usually established by an organisation to provide incident handling services that are focused on the establishing entity's protection requirements. The following are some examples of the entities that would establish a Internal or Private CSIRT: universities, banks, federal agencies, military institutes, and manufacturing companies [7], [11]. It is also important to mention that these are the smallest instances of CSIRTs and that Internal CSIRTs provide the most focused services to the constituencies that it serves.

National CSIRTs operate on higher level than Internal CSIRTs and are normally established by a government to provide incident handling services to the country as a constituency rather than an organisation or other smaller body [7]. The goals of National CSIRTs include the coordination of incident handling services within a country, analysing and combining vulnerability and incident information from lower level CSIRTs, Internal CSIRTs, providing communication links between constituencies, and facilitating trusted communication between constituencies [13]. National CSIRTs therefore play an important role as coordinators of information, communications and services within a country. JPCERT/CC is an example of a National CSIRT that provides incident handling services to Japan [7].

Coordination CSIRTs operate on the highest level of the CSIRT organisation hierarchy and their constituency is made up of other CSIRTs such as Internal and National CSIRTs and possibly other CIIP instances [11], [14]. Some of the roles of Coordination CSIRTs include the facilitation of communication, information transfer, and supporting service sharing between constituencies that are not located within the same country's borders [14]. Coordination CSIRTs are therefore primarily tasked with providing assistance services to other lower operational level CSIRTs. Their role in interchanging information in the CSIRT hierarchy is vital to ensure effective coordination of CIIP efforts. The United States Computer Emergency Readiness Team (US-CERT) is an example of a Coordination CSIRT instance [7].

Figure 1 illustrates the hierarchy of the three different CSIRTs discussed above as well as an example of the communication and information transfer paths between the different types of CSIRTs.

### C. CSIRTs and Smaller Stakeholders

Internal CSIRTs are normally established by a parent organisation in order to cater for their specific protection needs and their operations and services are closer to those of a private

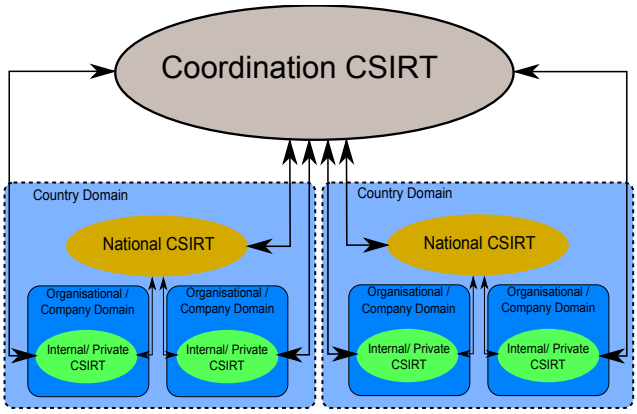



Fig. 1. This figure illustrates a conceptual representation of the different types of CSIRTs and how they could be organised. The communication paths are indicated by the arrows. The different operational domains that different CSIRT bodies will operate in are also illustrated by the diagram [7], [9].

security team [7]. Smaller stakeholders such as SMEs would find that it is infeasible to establish their own Internal CSIRTs because of the financial and technical requirements that are associated with the establishment of a CSIRT instance [15].

Larger CSIRTs such as National and Coordination CSIRTs in general have a larger constituency than that of the Internal CSIRTs and provide incident handling services to a larger constituency. Smaller stakeholders can form part of the constituency served by these large CSIRT instances although there are several factors can influence the adequacy of the services they receive. In general Coordination CSIRTs play an assisting role when it comes to providing incident handling services to their constituency and therefore is not a suitable candidate for providing protection to these smaller stakeholders [7]. National CSIRTs are focused on providing incident handling services to a country as a whole and the services that they offer might be to general and possibly to high level to cater to the specific needs of individuals and SMEs.

CSIRTs service provision are therefore not adequate to serve the needs of smaller stakeholders that have inadequate financial means to establish their own Internal CSIRT instance or similar structure. Developing countries often also do not have the technical expertise and financial means required to establish CSIRTs because of the lack of skills and limited government budget towards CIIP [9].

In the following section we discuss an alternative CIIP structure proposed by Ellefsen and von Solms to aid with CIIP in developing countries and extending protection services to smaller stakeholders.

## IV. C-SAW Teams

Community-orientated Security, Advisory, and Warning (C-SAW) Teams are Critical Information Infrastructure Protection (CIIP) structures that have been proposed to provide a low-cost start-up and operational solutions [9]. The primary goal of these CIIP structures are to provide protection, incident handling, services to smaller stakeholders and developing or industrialised countries [16], [9]. According to Ellefsen and von Solms [9] these C-SAW Teams are focused on providing incident handling services to communities. These communities are the equivalent of constituencies discussed in the CSIRT section, however Ellefsen and von Solms [9] distinguishes communities from constituencies by pointing out that communities contribute more to the operations of C-SAW Teams than conventional constituencies. Communities can be considered to be the individuals, organisations, or governmental bodies that are geographically related and have similar computer security concerns [9].

The C-SAW Team CIIP structure will form part of the primary focus of this paper as it is the CIIP structure that will be analysed as part of the discussion on CIIP Protection towards smaller stakeholders and developing countries.

### A. C-SAW Team Services

The services that a C-SAW Team will provide to the community that it serves must at least include some form of incident handling service. Providing incident handling services is a fundamental requirement for any CIIP structure and therefore must also be provided by C-SAW Teams [9]. Vulnerability Management services have been identified as the second service type that C-SAW Teams are expected to provide to their communities [9]

Incident handling services as discussed in section III-A, are concerned with handling and responding computer security incidents and can be considered as reactive services. Vulnerability Management services are concerned with the collection of vulnerability information and reports related to software and hardware that is used by the community members; identifying the presence of these vulnerabilities; analysing the resulting effects of these vulnerabilities; and devising a strategy to resolve or manage these vulnerabilities [12]. Vulnerability Management services are a part of the proactive services that a C-SAW will provide to its community.

It is vitally important that C-SAW Teams remain cost effective during their operation and that they provide an adequate level of service to the community that they serve. Therefore Vulnerability Management and Incident Handling Services have been identified as the minimal services that C-SAW Teams must include in their service provision in order to satisfy and maintain the requirements of cost effectiveness and adequate levels of service [9].

In the next section C-SAW Team Construction is discussed.

### B. C-SAW Team Construction

The services and organisation of a C-SAW Team are dependant on the constituency or community that it serves and are also important to the construction of a C-SAW Team instance.

Ellefsen and von Solms [9] provides several attributes that are required in order to construct a successful C-SAW Team instance. These attributes are: community orientated, autonomous, geographically and domain independent, and open design. A discussion on these attributes follows.

An important factor that will contribute to the successful operation of C-SAW Teams will be the active involvement

of community members in order to ensure effective and successful provision of CIIP services to the communities [9]. It must also be noted however that the community will not be responsible for the daily operations of the C-SAW Team, but instead will play a part in providing supporting functions [9]. Community members will be vitally important to C-SAW Teams as they will be contribute a large amount of information in the form of solutions, advice, best practices, and discussions on computer security incidents that could be used to solve computer security incidents. [9]

The ability of a C-SAW Team to operate autonomously is the ability of a C-SAW Team to operate independently from other CIIP structures. These C-SAW Teams must therefore still be able to provide services without the need of assistance from other C-SAW Teams or CIIP structures. This attribute will also include the C-SAW Teams ability to operate without the reliance on a single communication medium which could be important in developing countries that have unreliable electricity supplies and telecommunications mediums [9].

The geographically independent attribute was proposed to ensure that C-SAW Teams operate effectively in their operational environment. It focuses on the ability of C-SAW Teams to focus on their assigned communities, and the communities to identify their corresponding C-SAW Team and lastly it ensures that no two C-SAW Teams overlap in providing services to a single community [9].

Domain independence is concerned with C-SAW Teams focusing on certain related types of community members. This will allow the C-SAW Team to operate more effectively because the computer security incidents that they will encounter will have a higher probability of being similar to incidents encountered and resolved earlier because of the similarities in the operational domain [9].

The Open Design attribute of C-SAW Teams is concerned with encouraging community members to share information that could be used to address computer security incidents. The C-SAW Team must provide a single point of contact to allow the multitude of different community members to share information [9].

These attributes have been identified to aid with the successful establishment of a CIIP solution that will aid smaller stakeholders and developing countries. In the next section an analysis of C-SAW Teams follows.

### C. C-SAW Team Role

The primary role of a C-SAW Team is to provide incident handling services to the community that it serves. Figure 2 illustrates the role that a C-SAW Team serves towards its community. A C-SAW Team acts as an intermediary between external CIIP structures and its community filtering and distributing focused information related to system vulnerabilities and computer security incidents as required.

In the following section some of the common Computer Vulnerability Information sources are discussed.

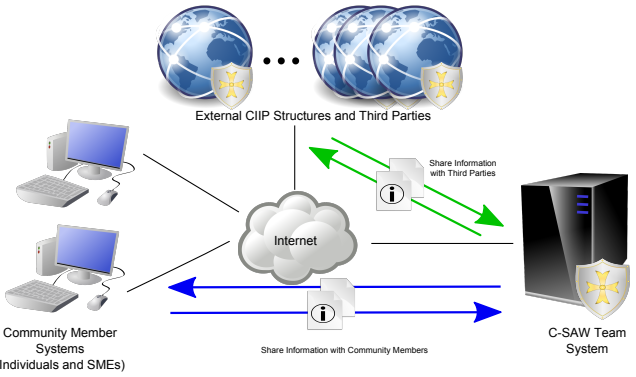



Fig. 2. This figure illustrates the role of a C-SAW Team in providing incident handling services and information sharing between the constituencies and external CIIP structures. The C-SAW Team will normally act as a filter for protection information that is passed down from larger CIIP structures to focus and simplify information [9].

## V. Vulnerability Information Sources

In this section we will introduce some of the parties that are responsible for identifying and address computer security vulnerabilities and distributing security related information.

There are large amounts of security vulnerabilities encountered in modern software and this can be attributed to the lack of proper security practices that are employed during the design and development processes that are used when software is being created [17]. In order to address these software vulnerabilities software vendors and other third parties provide information and patches to resolve or address these vulnerabilities. These software vendors and third parties often provide mechanisms that allow customers and other third parties to report the security vulnerabilities that they have encountered.

There are numerous sources that are focused on discovering computer software vulnerabilities and distributing this information to interested parties. These sources include software vendors, researchers, and other third parties such as CSIRTs or vulnerability database providers [18]. The information that is shared with customers and security teams can be provided in a variety of ways which include webpages, RSS feeds, and eMails. The variety of mechanisms promotes access to publicly available security related information.

In the following section we will introduce some software vendors and the mechanisms that they use to distribute security related information.

### A. Software Vendors

Software Vendors usually develop and maintain a large portion of popular software that are targeted by cybercriminals. In popular software products such as Adobe Flash Player [19], and Oracle Java [20] several vulnerabilities are reported annually [21]. It is therefore the responsibility of these software vendors to resolve these vulnerabilities in order to protect their customers from possible attacks. Many large software vendors have security teams that are tasked with addressing and resolving software vulnerabilities. These software vendors also often provide some form of a reporting mechanism that

can be used to report these vulnerabilities. In the following paragraph Microsoft is briefly discussed to provide more insight to the role that a software vendor fulfils towards the addressing of software vulnerabilities.

Microsoft a large and well know software vendor has several efforts focused towards addressing vulnerabilities identified in their software. The Microsoft Security Response Center is responsible for identifying, researching, and resolving security incidents and vulnerabilities related to Microsoft products [22]. Microsoft also makes use of the Technet Security Bulletin mechanism to relay information to IT professionals and customers. The security bulletins contain information about the security vulnerabilities, frequently asked questions, and possible workarounds to help IT professionals to address security vulnerabilities [22]. The information provided is aimed at improving the overall security of customer systems and address vulnerabilities. The Windows Updates mechanism shipped with the popular Windows operating system is commonly used to distribute security updates to address vulnerabilities related to Microsoft Products.

### B. Vulnerability Researchers and other Third Parties

Software Vendors usually are not the only parties that identify and address software vulnerabilities that are identified in software products. It is often the case that security bodies, such as CSIRTs mentioned above, have teams of researchers that are focused on identifying and resolving of security vulnerabilities in software that are used by their constituencies. These researchers after identifying the vulnerabilities will in most cases inform the respective software vendors about the vulnerabilities that have been found. If a solution is immediately obvious, the research teams will also provide this information to the software vendors in order to reduce the time to resolve the vulnerability. The vulnerabilities will not be made publicly available directly after their discovery in order to allow the software vendor to resolve the software vulnerability before it is published, this is know as Responsible Disclosure [23].

### C. Security Vulnerability Related Information

Security vulnerability related information usually have a set of common sections that form part the information provided. These common sections includes a description of a security vulnerability, a list of the software that is affected by the security vulnerability and possible solutions or workarounds in order to mitigate the risks posed by the vulnerability.

The security vulnerability related information are normally exposed through several mechanisms which can include websites, XML files, RSS feeds, mailing lists and other mechanisms that might require special software or a subscription in order to gain access to the information.

In the next section the Common Vulnerabilities and Exposures (CVE) format is discussed, this format is used consolidate several sources of computer vulnerability information in order to improve distribution.

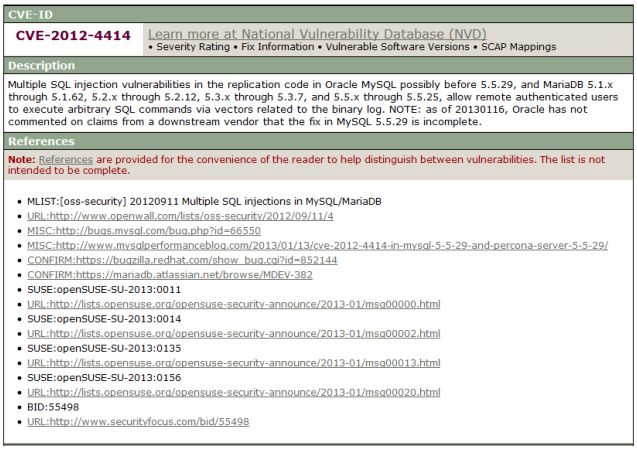
## VI. Common Vulnerabilities and Exposures

Initially software vendors and other third parties released security related information through their own mechanisms and layouts which lead to an increased complexity in the process of keeping track of the vulnerabilities that affected a interested party's systems. The CVE (Common Vulnerability and Exposure) format was developed to improve the distribution of computer security vulnerabilities and exposure information [24]. The CVE format achieves this through providing a common layout through which this information can be made available to interested parties. CVE identifers are distributed through a list or dictionary that is publicly available on the CVE List website that is managed and updated by the MITRE Corporation. In the next section a discussion on CVE identifiers follows.

### A. CVE identifiers

A CVE-ID (CVE identifier) is a common identifier that has been assigned to a security vulnerability or exposure that has been encountered where the related information is publicly available [24]. The role of CVE identifiers are not to provide information about security vulnerabilities or exposures, such as fixes for the vulnerability, but rather to provide a collection of the relevant information through references (links) to other information sources [24].

CVEs commonly consist out of three main elements [24]. The first element of the CVE identifier is the unique number that has been assigned to the CVE identifier. The second part is a brief description of the security vulnerability or exposure that the CVE is assigned to. The last part of the CVE identifier is links or references to information regarding the security vulnerability or exposure which could include methods that have been proposed to fix the security vulnerability or exposure. Figure 3 provides and example of the common CVE layout.


CVE-ID

CVE-2012-4414 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Multiple SQL injection vulnerabilities in the replication code in Oracle MySQL possibly before 5.5.29, and MariaDB 5.1.x through 5.1.62, 5.2.x through 5.2.12, 5.3.x through 5.3.7, and 5.5.x through 5.5.25, allow remote authenticated users to execute arbitrary SQL commands via vectors related to the binary log. NOTE: as of 20130116, Oracle has not commented on claims from a downstream vendor that the fix in MySQL 5.5.29 is incomplete.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MLIST:[oss-security] 20120911 Multiple SQL injections in MySQL/MariaDB
- URL:http://www.openwall.com/lists/oss-security/2012/09/11/4
- MISC:http://bugs.mysql.com/bug.php?id=66550
- MISC:http://www.mysqlperformanceblog.com/2013/01/13/cve-2012-4414-in-mysql-5-5-29-and-percona-server-5-5-29/
- CONFIRM:https://bugzilla.redhat.com/show_bug.cgi?id=852144
- CONFIRM:https://mariadb.atlassian.net/browse/MDEV-382
- SUSE:openSUSE-SU-2013:0011
- URL:http://lists.opensuse.org/opensuse-security-announce/2013-01/msg00000.html
- SUSE:openSUSE-SU-2013:0014
- URL:http://lists.opensuse.org/opensuse-security-announce/2013-01/msg00002.html
- SUSE:openSUSE-SU-2013:0135
- URL:http://lists.opensuse.org/opensuse-security-announce/2013-01/msg00013.html
- SUSE:openSUSE-SU-2013:0156
- URL:http://lists.opensuse.org/opensuse-security-announce/2013-01/msg00020.html
- BID:55498
- URL:http://www.securityfocus.com/bid/55498

Fig. 3. This figure provides an example of the layout of a CVE identifier entry for a MySQL vulnerability [25]. This includes the CVE-ID number at the top left, a description of the CVE-ID entry, and a list of references that relate to the CVE-ID entry.

### B. CVE Overview

The Common Vulnerability and Exposure (CVE) effort is widely used and over a 100 products and services are "CVE compatible " and there are more than 70 organisations contribute information to the CVE identifiers effort [26]. The large number of data sources that provide software vulnerability information results in a wider scope and increased relevance of the information that is provided by the CVE identifiers. It must however be pointed out that the information that is provided by these CVE identifiers and their references require a certain amount of information security expertise and might not be comprehensible to the average computer user. There are however a number of websites that will explain certain specialised terms and will provide additional information to help inexperienced users to understand some of the specialised information [24].

CVE identifiers are not used to provide information about security vulnerabilities and their solutions, but are rather used as a gateway to this information through the provision of links or references to the relevant information. Therefore it helps interested parties keep track of security vulnerability related information by providing a single point to which the user can return to find updates on the information related to the security vulnerability and alternative solutions [24].

There are currently over 54000 CVE entries that form part of the CVE list and this is by no means a complete list of all the software vulnerabilities that have been identified. The information provided by the CVE list must be publicly available vulnerability information, thus this source of vulnerability information will never provide a complete list of security information to interested parties. Another contributing factor is that it is often implausible for small software vendors and development companies to address vulnerabilities in their software because of the cost related to analysing software.

The "CVE List" is a large initiative that plays a substantial role in providing security vulnerability related information. Although CVEs do not provide all the possible references to all the information related to security vulnerabilities they do provide references to a substantial amount of information. The CVE related operations can therefore be considered worthwhile initiatives that aid with the reduction of publicly known security vulnerabilities found in widely used software.

In the next section a discussion of the Common Vulnerability Scoring System (CVSS) follows that is a framework that was devised in order to prioritise security vulnerabilities.

## VII. Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is an open framework proposed to provide a standardised method to score security vulnerabilities [3]. The CVSS is an open framework and the characteristics used to calculate the vulnerability score are available publicly making it easier to evaluate the resulting score.

There are many security vulnerabilities that are identified on a regular basis, the problem is presented while assessing which vulnerability takes priority over other vulnerabilities when it comes to addressing the most severe. This is where the CVSS can be used through providing a common severity rating making it simpler to identify vulnerabilities that pose the largest potential risk [3]. In this section, version 2.0 of the CVSS is assumed.

### A. CVSS Scoring Metrics

The CVSS vulnerability score consists out of three metric groups: Base, Temporal, and Environmental metrics [3].

Every metric group has a subset of metrics that are used to calculate the resulting value for that metric group [3]. The subset of metrics are determined by evaluating several factors such as risk, availability, integrity, etc.

After the factors that influence the vulnerability are evaluated, values are assigned to each of the subset of metrics that make up the metric groups. The values for each of these metrics are assigned numerical values and these numerical values are input into predefined equations used to evaluate each of the corresponding metrics. After the evaluation of the equations, a numerical value for each of the subset metrics are determined [3]. The numerical values for the subset metrics are then input into another set of predefined equations, used to calculate a corresponding numerical value for each of the metric groups. These numerical values for the three metric groups (Base, Temporal, and Environmental) makes up the overall CVSS vulnerability score [3].

The precise details about the metrics, equations, and methods used to evaluate the CVSS scores are beyond the scope of this document, please refer to the document [3] for more information about the CVSS framework.

### B. CVSS Analysis

The CVSS framework can be an effective tool used by CIIP instances and security teams to evaluate the risk posed by computer security vulnerabilities. The ability to prioritise computer security vulnerabilities that pose an immediate threat over other vulnerabilities that are less likely to be exploited is an important task. This will allow the CIIP instances and security teams to address threats that have a higher priority before considering threats that are less likely to be targeted and therefore pose a lower risk. The overall result of the effective use of prioritising computer security vulnerabilities will result in an improved level of security service provision in the constituency's operational environment.

CVSS Scores also form part of the content of CVE entries in order to provide some form of a vulnerability impact rating that could help security staff to identify the risks posed by vulnerabilities described in the CVE entries. CVEs however only include 'base scores'. The National Vulnerability Database however offers an additional service called the 'CVSS score calculator' that allows interested parties to calculate a temporal score and environmental score for a CVE entry.

In the following section the relationship between vulnerability information and CIIP efforts is discussed.

## VIII. Vulnerability Information and CIIP efforts

The vulnerability information that CIIP structure makes use of to support their operations is vitally important to the successful execution of these operations. Focused and relevant information are required to ensure effective use of this information during CIIP service provisions. There must also be a clearly defined process that is used to evaluate the relevance of the information to a computer vulnerability or computer security incident.

CVEs and the corresponding CVSS scores can be used to identify and evaluate the vulnerabilities that are present on community members systems. The CVE entries also provide responding parties with a starting point from where information related to specific security vulnerability can be identified and used during the resolution process. In the following section a model is introduced that is aimed at supporting C-SAW Team service provision efforts.

## IX. Model-Driven Solution

The C-SAW Team CIIP structure is a conceptual structure that proposes the use of community involvement in order to aid with CIIP service provision towards smaller stakeholders and developing countries. In the following sections a prototype system that will assist with CIIP efforts towards smaller stakeholders and developing countries will be discussed.

### A. Defining the Model

The system will consist out of three main components: a client-side component, an analysis component and communication component. Figure 4 illustrates the different components that will form part of the proposed system as well as the information flow between the different parties.

The client-side component is aimed at collecting information about the software that is installed on the community members systems. This information will then be relayed back to the analysis component for further processing.

The analysis component will be used to analyse the information retrieved from the community systems and identify possible computer security vulnerabilities or configurations. The component will make use of the security vulnerability information feeds during the analysis of the community member systems to aid with the identification of vulnerabilities.

The final component will be used to facilitate communication between community members, C-SAW Team operators and Third Parties. This component will provide a forum that will allow community members to discuss and share advice about security vulnerabilities and incidents. The communication component will play a vital role in the provision of CIIP services to the community members as it will be the mechanism used to distribute focused and relevant information to the community in the event of computer security incident.

Although most of the information distribution and collection will be automated the C-SAW Team operators will still play a vital role in this model as the operators will be responsible for overseeing the CIIP service provision efforts and the distribution of information.

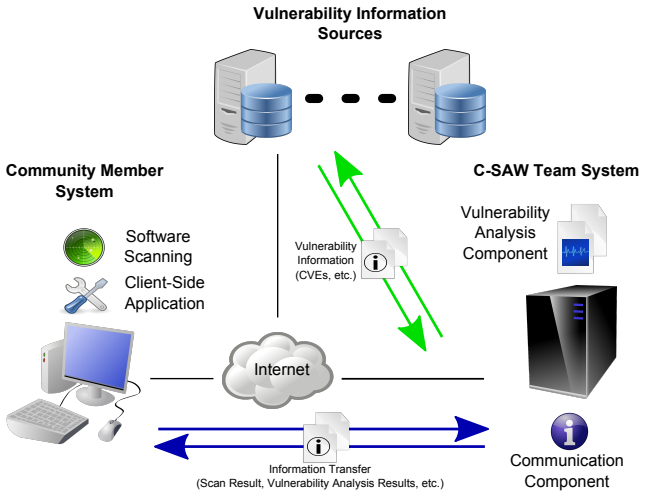



Fig. 4. This figure illustrates the different components that will form part of the system that is aimed at supporting CIIP towards smaller stakeholders and developing countries. The green arrows illustrate the information transfer between the C-SAW Team and vulnerability information sources. The blue arrow illustrates the information transfer between the C-SAW Team and the community members. (By Author)

### B. Supporting CIIP Efforts

CVEs combined with CVSS scores can provide vital information that could aid the process to resolve security vulnerabilities. Smaller stakeholders and developing countries often lack the required knowledge, expertise and experience to make use the security related information such as CVEs. The proposed system is focused on the process of collecting and distribution of focused and relevant information to the community. This distribution process will include a step that makes the information comprehensible to community members that might not be able to make use of the information collected directly from the security feeds. The C-SAW Team members will play a vital role in ensuring that the information is usable as well as to offer support and advice on how to make use of the information.

Making effective use of the combined body of knowledge that can be extracted from the community members is also an important function that the C-SAW Team system must provide. This function will be provided through a forum that will allow community members to discuss and provide advice on security related topics. This function will only be available to registered community members to ensure that the information is handled in a safe manner to encourage openness and sharing.

The proposed system will provide support to CIIP efforts towards smaller stakeholders and developing countries through collecting information about the community member systems such as software packages that have been installed and their version information. This information can then be linked to information gathered from vulnerability information sources such as CVEs augmented with version information. Relevant information can than be provided to the interested stakeholders which could include steps to solve or mitigate the impact of these vulnerabilities.

Providing focused and relevant information can enable smaller stakeholders such as SMEs that have a limited set of skills and expertise to limit their risk of exposure to cyber attacks. The aim of this proposed system is to provide community members with information that will allow them to limit their exposure to cyber attacks.

## X. Conclusion

The aim of this paper was to identify sources of vulnerability information that can be used as part of CIIP service provision to smaller stakeholder and developing country communities. This paper identified and discussed some of the mechanisms and sources that provide security related information to resolve security vulnerabilities and limit the exposure to cyber attacks. The paper has also introduced a proposed solution that is aimed at providing CIIP to developing countries and smaller stakeholders that might not be covered by existing CIIP structures.

Several sources of information have been identified that include software vendors, research teams and other third parties. There is an abundance of information that could be used to limit security vulnerabilities resulting in an overall reduced risk of exposure to cyber attacks. CVEs provide a standardised format that is widely used to address and resolve vulnerabilities. The problem comes in during the distribution of the information to affected parties and to ensure that this information is compressible and usable.

Future work and ongoing work consists of the realisation of a prototype system that will aid community members and C-SAW Teams to extract the full benefit from available vulnerability information sources. Future work also includes defining a process to collect, simplify and distribute vulnerability related information to interested parties. The development and realisation of a system of this type is essential to ensure that SMEs and individuals can securely participate in an ever expanding and global cyber environment.

## XI. Acknowledgement

This paper is based upon work that is financially supported by the National Research Foundation (NRF). The opinions expressed in this paper are those of the authors.

## References

[1] Microsoft. (2011, May) Malware research and response at microsoft. Microsoft. [Online]. Available: http://www.microsoft.com/en-us/download/details.aspx?id=26644

[2] UK Government, "The uk cyber security strategy." 2011, [Accessed 2 April 2013]. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[3] FIRST, "A complete guide to the common vulnerability scoring system version 2.0," website, 2007, [Accessed 2 April 2013]. [Online]. Available: http://www.first.org/cvss/cvss-guide.pdf

[4] Symantec, "Internet security report," 2011, [Accessed 2 April 2013]. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

[5] Estonian Information Systems Authority, "Critical information infrastructure protection ciip - estonian information systems authority," Website, February 2011, [Accessed 12 April 2013]. [Online]. Available: https://www.ria.ee/CIIP/

[6] B. Hammerli and A. Renda, "Protecting critical infrastructure in the eu. ceps task force report, 16 december 2010," p. 106, December 2010. [Online]. Available: http://aei.pitt.edu/15445/

[7] CERT/CC, "Cert®/cc: Computer security incident response team faq," Website, CERT/CC, n.d., [Accessed 12 April 2013]. [Online]. Available: http://www.cert.org/csirts/csirt_faq.html

[8] ENISA, "What is a csirt? - enisa," Website, n.d., [Accessed 11 April 2013]. [Online]. Available: http://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt

[9] I. D. Ellefsen and S. H. von Solms, "Critical information infrastructure protection for developing countries," Ph.D. dissertation, University of Johannesburg, November 2011.

[10] Cyber Defense Institute Inc. Csirt setup service — services — cdi - cyber defense institute, inc. Website. Cyber Defense Institute, Inc. [Accessed 12 April 2013]. [Online]. Available: http://www.cyberdefense.jp/en/services/csirt.html

[11] M. J. West-Brown, D. Stikvoort, K. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 2nd ed., ser. Handbook (Carnegie Mellon University. Software Engineering Institute). Carnegie Mellon University, Software Engineering Institute, April 2003. [Online]. Available: http://www.cert.org/archive/pdf/csirt-handbook.pdf

[12] ENISA. Enisa - services. Website. ENISA. [Accessed 22 July 2012]. [Online]. Available: http://www.enisa.europa.eu/activities/cert/support/guide2/annex/services

[13] G. Killcrece. (2004, August) Steps for creating national csirts. CERT Coordination Center, Carnegie Mellon University. Pittsburg, Pennesylvania. [Accessed 12 April 2013]. [Online]. Available: www.cert.org/archive/pdf/NationalCSIRTs.pdf

[14] I. D. Ellefsen and S. H. von Solms, "Critical information infrastructure protection in the developing world," in *Critical Infrastructure Protection IV*, ser. IFIP Advances in Information and Communication Technology, T. Moore and S. Shenoi, Eds. Springer Boston, 2010, vol. 342, pp. 29–40. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-16806-2_3

[15] J. Harrison and K. Townsend, "An update on warps. enisa quarterly review," December 2008. [Online]. Available: http://www.warp.gov.uk/downloads/enisa_quarterly_12_08.pdf

[16] I. D. Ellefsen and S. H. von Solms, "C-saw: Critical information infrastructure protection through simplification," in *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*, ser. IFIP Advances in Information and Communication Technology, J. Berleur, M. Hercheui, and L. Hilty, Eds. Springer Boston, 2010, vol. 328, pp. 315–325. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-15479-9_30

[17] T. Wilson, "Why can't johnny develop secure software?" [Website], June 2010, [Accessed 2 May 2013]. [Online]. Available: http://www.darkreading.com/applications/why-cant-johnny-develop-secure-software/225700320

[18] MITRE Corporation. (2012, December) Cve - cve numbering authorities. Website. The MITRE Corporation. [Accessed 6 March 2013]. [Online]. Available: http://cve.mitre.org/cve/cna.html

[19] Adobe Systems Incorporated, "Adobe - install adobe flash player," [Online]. [Online]. Available: http://get.adobe.com/flashplayer/

[20] Oracle, "Java se overview - at a glance." [Online]. Available: http://www.oracle.com/technetwork/java/javase/overview/index.html

[21] Symantec, "2013 internet security threat report," vol. 18, April 2013. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[22] Microsoft, "Microsoft security :: Microsoft security response center (msrc) — security engineering," n.d., [Accessed 14 May 2013]. [Online]. Available: http://www.microsoft.com/security/msrc/whatwedo.aspx

[23] S. Frei, D. Schatzmann, B. Plattner, and B. Trammell, "Modeling the security ecosystem-the dynamics of (in) security," in *Economics of Information Security and Privacy*. Springer, 2010, pp. 79–106.

[24] MITRE Corporation. (2012, December) Cve - frequently asked questions. Website. The MITRE Corporation. [Accessed 6 March 2013]. [Online]. Available: http://cve.mitre.org/about/faqs.html

[25] MITRE Corporation, "Cve – cve-2012-4414," Website, August 2012. [Online]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4414

[26] MITRE Corporation. (2013, February) Cve - compatible products and services. Website. The MITRE Corporation. [Accessed 6 March 2013]. [Online]. Available: http://cve.mitre.org/compatible/compatible.html