IVDA: International Vulnerability Database Alliance

Chen ZHENG[1,2], Yuqing ZHANG[1,2*], Yingfei SUN[2], Qixu LIU[1,2]
[1]National Computer Network Intrusion Protection Center, GUCAS
[2]School of Information Science and Engineering, GUCAS
Beijing, PR China

***Abstract*—Vulnerability is one of the important factors that cause security incidents and has become a major international threat to network security. Previous work like Common Vulnerabilities and Exposures (CVE) and vulnerability databases has been offered to manage vulnerability. However, they have significant disadvantages in coverage and regional differences. International Vulnerability Database Alliance (IVDA) is proposed as an alliance model which consists of security organizations from different countries. IVDA provides systematic policies and standards to manage vulnerabilities of software in different languages, and achieves agreement with its members to enhance international cooperation and communication. The evaluation of IVDA shows that the international alliance is rational and effective in vulnerability disclosure.**

Keywords-Network Security; Vulnerability; CVE; IVDA

I. INTRODUCTION

Security vulnerability is extremely important for network security and even relates with international relations. As the range of software deployment grows large, a vulnerability which is discovered in a local application will soon affect systems in other countries. For example, Stuxnet is a computer worm, which targeted Iranian nuclear facilities and affected industry systems in many countries [1]. Vulnerabilities played a significant role in this attack and can be judged as the major cause of all the loss.

If vendors release patches for vulnerabilities promptly after discoveries, attacks using vulnerabilities will surely affect less systems. However, even Microsoft cannot ensure to produce prompt patches for all their products [2]. Attempts to resolve this dilemma have resulted in the development of vulnerability disclosure. The disclosure of a vulnerability is the revelation of a vulnerability to the public at large [3]. Many vulnerability databases are founded to provide advisories to vendors [4]. Nevertheless, users with different levels can only obtain useful data from particular databases for a number of reasons, the most important being the lack of international vulnerability disclosure standards. Another reason is the difficulty in identifying vulnerabilities from different databases in different counties.

Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS) are two widely used methods for vulnerability disclosure. Many databases have included CVE, which is designed to deal specifically with the diversity in identifiers. CVSS is a quantitative method by scoring vulnerabilities. However, given that they are designed for vulnerability disclosure in English speaking countries, the scope of these methods are limited and cannot match the evolving reality of international security vulnerability.

Although CVE benefits a lot in sharing data across separate databases and services, the shortcomings of CVE cannot be neglected. Firstly, it doesn't cover all the vulnerabilities of software in English speaking counties. Secondly, here comes the issue of languages. CVE contains most of vulnerabilities in English speaking regions but only covers a small part of vulnerabilities in non-English speaking areas. Thirdly, CVE is inefficient in identifying new types of vulnerabilities.

The International Vulnerability Database Alliance (IVDA) that we proposed in this paper will address these maladies. In IVDA, we involve security authorities and combine public resources so as to ensure stable data feeds. We present the basic idea for identifying vulnerabilities of software in different language by providing International Vulnerabilities Description (IVD), which has two status tags and rational management. We systematically extract minimum description fields that IVDA members will include in their vulnerability reports, and provide a general procedure in vulnerability disclosure that brings few changes in the original routines of IVDA members. To improve the vulnerability data exchanges under the alliance, we propose a worldwide Vulnerability Citation Index (VCI) and describe the policies based on this index. What's more, we propose a council to be in charge of IVDA, which formulates regulations and policies to support the routine of IVDA, reduce regional differences and be adaptive to the evolving reality. We also provide the basic implementation phases of IVDA and compare it with the previous work, which shows that IVDA is rational and available. In addition, possible avenues for expanding IVDA have been fully considered.

The rest of this paper is organized as follows. Section II introduces background and previous work whereas Section III discusses problems in current efforts. In Section IV, we describe the architecture and policies of IVDA in detail, and give the implementation steps. Section V compares IVDA with previous work and describes the potential problems, while Section VI presents the conclusion and future work.

II. BACKGROUND AND PREVIOUS WORK

A. Background

Vulnerability is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy [5]. Research in National Computer Network Intrusion Protection Center of

[*] Corresponding author. Tel./fax: +86 10 88256218. zhangyq@gucas.ac.cn

This work is supported by The National Natural Science Foundation of China (60970140).

978-0-615-51608-0/11 ©2011 EWI

TABLE I. AN OVERVIEW OF MAJOR VULNERABILITY DATABASES

Database Name	Record Count	Update Frequency	Description fields	Other security services
NVD	45672	Continuously updated, but not updated daily	17 items	None
SecurityFocus	43460	updated daily	14 items	Mailing lists
ISS X-Force Database	66639	Continuously updated	10 items	Papers, reports
OSVDB	70620	updated daily	12 items	Blogs, news

China (NCNIPC) shows vulnerabilities of various severities are disclosed continually across the entire cyber world [6].

B. *Vulnerability database*

Comparing with firewall, intrusion detection and other security measures, vulnerability disclosure is a much more proactive protection method.

In some English-speaking countries, especially in America and European countries, some famous vulnerability databases have been in service for years, such as NVD, Secunia, Security Focus, ISS X-Force, OSVDB, Vupen and so on. The data from four famous databases before April 11, 2011 are described in Table I. It is obvious that services of different databases differ from each other, for they have particular goal and procedure.

C. *Current industry standards*

Many efforts have been taken to develop reliable standards for vulnerability management, of which two widely used standards are CVE and vulnerability assessment method.

1) *Common Vulnerabilities and Exposures*

CVE is designed for providing a common identifier to identify vulnerabilities in different databases. CVE contains identifier number with status entry, brief descriptions, and some reference links. After assigning a potential vulnerability a CVE identifier with candidate status by a CVE Candidate Numbering Authority (CNA), vulnerability detail will be posted into CVE candidate list. If the vulnerability is verified by CVE Editorial Board, it will be then listed in CVE list [7].

2) *Vulnerability assessment methods*

The severity and priority of vulnerabilities can be observed by vulnerability assessment methods, which are classified into quantitative method or qualitative method. Historically, vendors use their own ways to rate vulnerabilities, without detailing criteria. Some further work, like CVSS v2.0 [8] and VRSS [9], is released and some of them have been used.

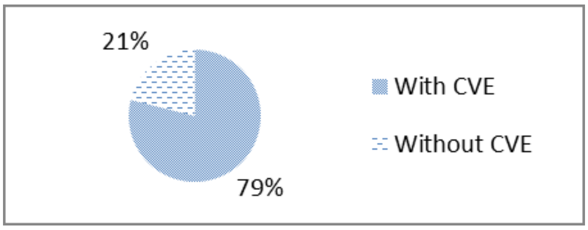

Figure 1. Vulnerability category by CVE in OSVDB

III. ANALYSIS OF CVE AND VULNERABILITY DATABASES

Since the number of vulnerability is large and still increases continuously, the previous work including vulnerability databases and CVE doesn't fit well with the reality. This section describes the disadvantages of previous work and discusses the reasons of them.

A. *Weakness of CVE*

1) *CVE doesn't cover all the vulnerabilities.*

a) CVE doesn't cover all the vulnerabilities of software in English speaking regions.

According to Fig.1, 21 percent of all the vulnerabilities are without CVE identifiers in OSVDB. It is a common issue in many security databases that a large amount of vulnerabilities are without CVE identifiers, which makes it hard for data exchanging or addressing among different databases. This fact will increase the complexity in vulnerability management.

b) Many vulnerabilities of software not in English language are not included by CVE.

CVE contains most of vulnerabilities in English speaking regions but only includes a small part of vulnerabilities in non-English speaking areas. Vulnerabilities excluded by CVE may sometimes make a tremendous impact on international network security. For example, there are 26 vulnerabilities announced publicly in Rising products, popular security software in China, but only 7 of the total are assigned CVE identifiers [10]. Given that the above example is very common in Chinese software, similar problems may also occur in other non-English software.

This problem arises from the operating mechanism of CVE. CVE mainly focuses on vulnerability reports from its official partners but not the ones from other organizations. While this might suffice most time, it may sometimes be critical to ignore the vulnerabilities announced in other databases. In addition, CVE is designed to identify vulnerabilities of widely deployed software in English speaking countries but has less concern about vulnerabilities in other languages.

2) *CVE is not adaptive to the new types of vulnerability.*

CVE shows inefficient in emerging types of vulnerability. XSS vulnerability, as a new Web vulnerability, has accounted for a large proportion of all the vulnerabilities. XSS vulnerability statistics from CVE and other three databases are given in Table II, in which CVE covers the least number.

3) *The number of CNAs is limited.*

CNAs are the main data feeds of CVE, and they can include CVE identifiers themselves in their initial vulnerability advisories. However, the participating CNAs consist of only fifteen organizations, including eleven software vendors, two third-party coordinators and two researchers [7]. The number of CNAs is too small to cover all the software vulnerabilities. Vulnerabilities in software which is not released by CNAs cost more time to get CVE identifiers. It's also a reason for many databases storing vulnerabilities without CVE identifiers.

4) *Duplicate of CVE identifiers*

The existence of duplicate CVE identifiers is vital, because it loses its credibility in identifying vulnerabilities. Although CVE takes measures to deal with the duplicate, duplicate CVE

TABLE II. XSS VULNERABILITY STATISTICS

CVE	OSVDB	X-Force	Xssed
6140	10951	9720	39249

identifiers are inevitable. Firstly, different security databases sometimes offer different descriptions for a single vulnerability, which would create a loophole to be recognized as different vulnerabilities. Secondly, different CNAs may assign CVE identifiers to a vulnerability at the same time. For example, CVE-2000-0744 is a duplicate of CVE-2000-0743 [11], and breaks completeness of CVE identifiers after being deprecated.

B. Regional differences in vulnerability disclosure

The mechanisms of vulnerability disclosure in non-English speaking countries are less developed than the ones in English-speaking countries. Although some non-English software's vulnerability are announced by local security communities or individuals, and even are covered in some famous vulnerability databases, the majority are still not well disclosed. Besides, many software vendors in non-English speaking countries just release patches quietly in later versions without announcing the necessity of patch deployment in software currently in use, which makes it impossible to protect against intrusions [4].

Take China as an example, plenty of vulnerabilities were discovered in Chinese applications, such as a code execution vulnerability in Baidu Soba Search Bar, which can be exploited to compromise systems of victims in many other countries [10]. However, vulnerability databases in China are established very late and the repositories of them just contain a section of vulnerabilities in Chinese software. Many famous vulnerability databases in English-speaking areas, like NVD, only contain the minority of Chinese software vulnerabilities. Some of them even have not collected any Chinese software vulnerability.

Vulnerabilities of random software in Chinese are provided in Fig.2. The vulnerability statistics are all the largest count collected respectively among English Vulnerability databases, Chinese Vulnerability databases, and CVE List. Most Chinese software vulnerabilities are stored in Chinese vulnerability databases without fully CVE identifiers. An exception is that English vulnerability databases contain vulnerabilities in Rising products much more than Chinese ones do. This finding supports the view that English vulnerability databases have much more developed vulnerability disclosure mechanisms but have less concern about vulnerabilities in other languages.

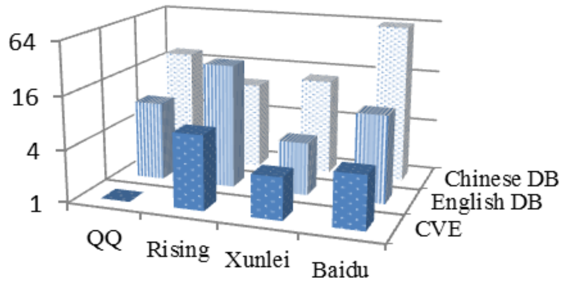

Figure 2. Chinese software vulnerability disclosure statistics

C. Diversity in vulnerability management procedure

The common vulnerability disclosure process contains five major steps: discovery, report, verification, evaluation, and announcement. The managing procedures of databases differ from each other. They offer different description fields in their reports. Some databases include CVSS to score vulnerability, but there are still many organizations use their own qualitative methods to rate the severity of vulnerability. There is also a lively debate about full disclosure and limited disclosure [12]. Consequently, a single vulnerability will have different description fields and publish time in different databases. It can be observed from Table I.

IV. ARCHITECHTURE AND IMPLEMENTATION OF INTERNATIONAL VULNERABILITY DATABASE ALLIANCE

Since the problems of previous work become the barriers for vulnerability disclosure, an international alliance including all the security authorities should be put on the agenda to improve vulnerability disclosure.

In this section, we propose an alliance model, International Vulnerability Database Alliance (IVDA), give an overview of the alliance architecture and then discuss in detail about the key work surrounding the alliance.

A. The goal of IVDA

The primary goal of IVDA is to integrate all the existing resources from major security vulnerability databases all over the world, expand the storages of current databases to cover vulnerabilities in different countries, increase data feeds of vulnerability information, and propose reliable and consistent vulnerability management standards to announce vulnerability information promptly and consistently. Through the efforts of alliance, we will aim to reduce the time of vulnerability disclosure, increase the concerns about the vulnerabilities in non-English software, maintain IVD identifiers, enable the emergency response measures handling emerging vulnerabilities, and enhance the sharing of vulnerability information. What's more, the alliance will become an effective platform among different databases, communities, vendors, and countries, which support robust information sharing and international standard discussing.

B. Architecture of IVDA

IVDA endorses all the security organizations, software vendors, vulnerability databases and communities to participate in the alliance. Four major roles that will be involved in IVDA are presented in Fig.3, including IVDA members, IVD Identifying Authorities (IIAs), IVDA Council, and Vulnerability Citation Index (VCI) department.

IVDA members are the most basic component of IVDA, which consist of security organizations from different countries. With coordination and communication, they share their efforts and participate in all the work provided by IVDA.

IIAs are some qualified IVDA members, who involve in the policy decision and will be responsible for IVDA. IIAs are mainly composed of software vendors, and they are allowed to assign IVD identifiers to vulnerabilities of their own software.

IVDA Council is a decision-making section that maintains the normal operation of the alliance. IVDA Council formulates general policies, audits qualifications of IIAs, verifies reports from IVDA members, maintains IVD identifiers and handles duplicate identifiers.

VCI department is dedicated to maintain VCI relying on the reports from IVDA members.

C. *Standards and policies of IVDA*

IVDA aims to develop a new vulnerability identification method to resolve the dilemma of the previous work. IVDA members manage vulnerability in a general procedure provided by IVDA, and then post their reports to IVDA. IVDA Council assigns IVD identifiers to the vulnerability, indexes the detail and forms the VCI for users to obtain latest data from different databases. These three relevant tasks are the preconditions for and the basis of each other.

1) *International Vulnerabilities Description (IVD)*

In order to identify vulnerabilities and avoid redundancy, IVDA designs IVD for identifying vulnerabilities of software in different languages. IVD's format is IVD-YYYY-NNNNNN, of which YYYY is a 4 decimal digit that represents the year of vulnerability disclosure and NNNNNN is a 6 decimal digit as the serial number of a vulnerability. There are also two additional status tags added to IVD identifiers, which respectively represent verification status and language field of a vulnerability. The language tag is determined by the software where the vulnerability occurs. The verification status tag contains four states: candidate, verified, fixed and misreport.

IVDA uses the following criteria to assign IVD identifiers. IVDA Council reserves a portion of IVD identifiers for every IIA. So when critical vulnerabilities of their own products emerge, all these representative IIAs can instantly announce their security advisories including IVD identifiers. The IVDA members which are not IIAs yet cannot include IVD identifiers to their announced vulnerabilities until they get feedbacks with IVDs from the alliance. After instant security advisories, IIAs and other IVDA members post the latest vulnerability information to the alliance. Receiving the reports from IVDA members, IVDA Council compares description fields of the vulnerability against the data in VCI to decide whether to update the original information or to take further verification. If the vulnerability has been included by VCI, the original data will be updated. If not, IVDA Council will assign to it a new IVD identifier after checking the validity of the vulnerability. To the reports from IIAs, IVDA Council will check the IVD identifier to determine whether this identifier has been used. If the IVD identifier already exists, further information will be compared against the earlier one. According to the results, IVDA Council will handle the duplicate identifiers or update the vulnerability information. If it's a new IVD, IVDA will index the vulnerability information in VCI. Eventually, IVDA posts the latest vulnerability data back to each IVDA member.

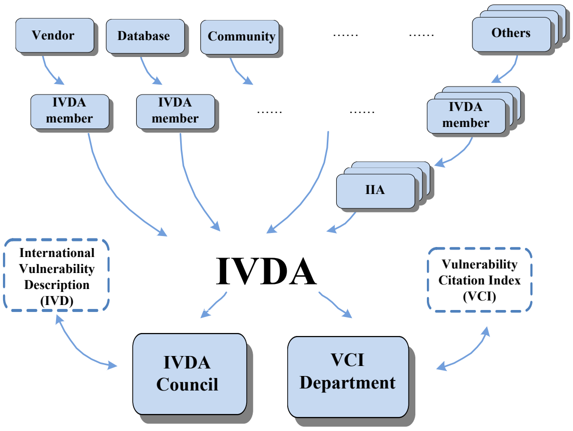

Figure 3. IVDA Architecture

IVDA Council takes the following basic approaches to handle duplication and conflict issues in IVD identifiers.

- If two vulnerabilities are assigned the same IVD identifier, the earlier one's IVD will be reserved, and the later one will be assigned another IVD identifier by IVDA Council.
- If a vulnerability has two IVD identifiers, the identifier that assigned for the longest period of time will be reserved.
- If two identifiers are assigned for the same time, the one which is assigned by the original vendor or firstly verified by IVDA Council will be reserved.

The purpose of this work is to resolve the existing diversity in the identifiers from different vulnerability databases and make full use of the current vulnerability disclosure channels. With IVD's facilitation for cross-linking with vulnerability databases, many other databases or security services will include IVD identifiers as a reference to help identifying vulnerabilities among databases. As IVDA members grow large, vulnerability announced to the public will be easily identified by searching its IVD identifier.

2) *International procedures for vulnerability management*

For vulnerability databases in different counties and regions, the vulnerability submitting and announcement should obey a basic standard. For example, when a vendor or vulnerability database collects vulnerability information from researchers, some necessary fields are required to make sure the facility of vulnerability verification and disclosure in a consistent process. IVDA encourages full disclosure, but also supports limited disclosure. IVDA Council requires that vulnerabilities posted to IVDA should contain the minimum description fields, and also allows IVDA members to include other additional fields in their own advisories. This policy will bring fewer changes to their own routines.

The minimum description includes the following thirteen fields: IVD, language, verification status, type, English name, publish time, update time, description, severity, exploit status, affect, solution, and original reference. IIAs should include IVDs in their reports, while common IVDA members don't have to. Most of the fields have already been included by many databases except IVD, language, verification status, English name and the original reference. These five description fields are specified by IVDA, of which the first three ones are used to address a unique IVD identifier. In the original reference field, databases include the reference where a vulnerability is first disclosed. The original reference is a vital field which is used to tell similar vulnerabilities and handle duplicate IVDs, while the English name field is for facilitating the index process of VCI. All these fields will be specified in the international procedures formulated by IVDA. With these descriptions of multiple dimensions, IVDA Council could distinguish different vulnerabilities which has similar feature effectively.

IVDA requires all the IVDA members to detail their criteria or processes and obey the basic procedure. The common vulnerability disclosure process provided by IVDA is given in Fig.4. It generally begins with posting a potential vulnerability to an IIA or an IVDA member. After existence check, duplicate reports will be abandoned. IIA verifies the validity of the vulnerability, and then publish on web site the security advisory including an IVD identifier with two status tags. As the IIA posts vulnerability information to IVDA with all fields required, vulnerability and its IVD identifier will get further verification and duplication handling. Eventually, vulnerability details will be indexed in VCI and posted back to IIAs helping the development of patches. The whole process is implemented in every IVDA members. And within this process, the latest data can be obtained from VCI to promote the accuracy in every step. This general procedure not only ensures efficiency and openness of IVDA routine, but also promotes the growth of immature vulnerability disclosure in some countries.

3) *Vulnerability Citation Index (VCI)*

Uniform data is necessary for efficient communication and documentation. With the effort of a series of standards and regulations released by IVDA, vulnerability will be disclosed in a common format. Vulnerability Citation Index (VCI) can be founded by integrating the vulnerability reports from IVDA members. It requires all the databases in this alliance provide English names and related descriptions for vulnerabilities.

When a vulnerability is announced on a database web site of an IVDA member, the vulnerability will be then posted to IVDA. After IVDA Council verified the vulnerability and assigned IVD identifier, VCI department indexes its English name, database identifier, IVD identifier and other necessary description fields.

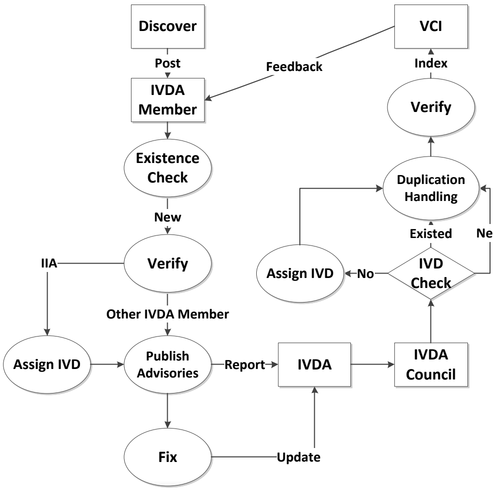

Figure 4. Vulnerability Management Flow

For the reason that many vulnerability databases may have overlapped portions, each vulnerability entry in VCI is added a field covering multiple database identifiers to reference the relevant databases. If a vulnerability has already been indexed in VCI, the vulnerability information in later post will be added to the existing entry. VCI allows users to identify any vulnerability database by which specific vulnerability has been cited, locate the vulnerabilities which have been reviewed most frequently, and address the databases which have covered certain vulnerabilities.

The vulnerability entry in VCI contains an IVD with status tags, along with multiple identifiers of particular databases. VCI will provide multiple search methods, like search by keywords, categories, or identifiers. A plenty of relevant vulnerabilities as the search result will be outlined in the order of customization. In brief, VCI provides an international interface to the latest critical vulnerabilities from different databases, and a direct way to choose the appropriate database for vulnerability detail.

4) *Analysis reports and emergency response services*

The alliance provides analysis reports and many other services for different regions and groups. IVDA also takes action to bring all the authority organization to anticipate in the discussion and implementation of international standards on vulnerability disclosure. When a new emerging vulnerability type appears, IVDA Council will give it an accurate description about its type, and provide a rating method in a very short time.

D. Implementation of IVDA

The actual implementation of IVDA is a phased process that needs data feeds, standard regulations and support of all the other security organizations. It is therefore necessary to draw up the major phases to facilitate the IVDA routine work.

The implementation begins with the primitive accumulation of the existing vulnerability data. The data is then processed into a common format, and is indexed in VCI, which is available on internet with IVD. After data accumulation, IVDA invites security authorities from different counties to participate. As IVDA members, they not only provide stable data feeds, but also expand the influence of IVDA by including IVD identifiers in their advisories. With scale spreading gradually, IVDA Council will be in charge of all the routine work. Eventually, IVDA along with all its members will be dedicated to the IVDA issues to ensure this open environment. Standards, policies and regulations provided by IVDA Council will also be improved to match the evolving reality.

V. Evaluation

In order to evaluate performance of IVDA in international vulnerability disclosure, we discuss in this section the process steps that vulnerabilities experience in IVDA, and then compare IVDA against the previous work.

Fig.4 illustrates the main process of a vulnerability report, of which most steps have been achieved in the original security organizations. The extra steps are the vulnerability detail exchanges and IVDA management. IVDA members' routines have no big changes as they only need to include a few more description fields of vulnerability, such as English name, IVD, and original reference. The general procedure will finish the diversity in vulnerability disclosure. IVDA members announce the vulnerability instantly as they receive the vulnerability reports from researchers. They don't have to wait until the patches are released. The time cost in vulnerability disclosure is reduced to the minimum. In contrast to CVE, IVDA involves more partners to participate in the alliance and requires multiple vulnerability data exchanges. Vulnerability disclosure in IVDA is much more consistent and timely, because all the vulnerabilities in an IVDA member include general description fields and have been verified for several times.

Additionally, as the IVDA grows large, vulnerabilities of software in non-English speaking countries can be searched in VCI promptly after it announced in their local IVDA members.

It can be observed from Table III that vulnerabilities in different databases contain different kinds of description fields. IVDA requires its IVDA members to disclose vulnerabilities covering thirteen basic fields, which provide comprehensive description for vulnerability. With these description attributes, formalized data can be easily obtained by automatic tools and help a lot in further verification by IVDA.

Comparing with CVE and famous vulnerability databases shows the advantages of IVDA in vulnerability disclosure.

- The coverage of IVDA is much larger. IVDA aims to identify all the vulnerabilities in different languages, and draws up a plan in VCI to expand the coverage of current vulnerability disclosure. With stable data feeds and rational IVD identifier spanning among countries gradually, IVDA will cover all the public vulnerability across the entire cyber world. IVDA also involves new emerging types of vulnerabilities. In contrast, CVE and most famous security databases mainly concern about the vulnerabilities of software in English speaking countries, and just covered a small part of new types of vulnerabilities.
- IVDA endorses all the security databases, vendors and community to participate and sort them by country. In contrast to only fifteen CNAs that CVE supports, IVDA has broader data feeds of potential vulnerability.
- CVE needs a year or more to verify some candidate vulnerability [7]. While IVDA allocates the work to members of the alliance to directly verify the potential vulnerability. It vastly reduces the workload of IVDA and the time cost in vulnerability verification.
- The distribution of IVD is strictly controlled by IVDA Council. Only IIAs directly include IVD identifiers in vulnerabilities of their own products whereas the other IVD identifiers are totally assigned by IVDA Council. This management policy reduces the risk of duplicate.
- IVDA ensures the integrity of vulnerability data by the general procedure, and resolves regional differences through efforts in international cooperation.

However, IVDA is still a model requiring consideration of multiple aspects. There are also some flaws in IVDA.

TABLE III. DESCRIPTION FIELDS STATISTICS

IVDA members	NVD	X-Force	OSVDB	Vupen
>=13	17	10	12	17

- IVD duplicate cannot be totally avoided. The basic approaches for handling duplication still need evolving.
- Vulnerability disclosure in non-English speaking area is still in the state of immaturity. It takes time to meet the requirements of IVDA.
- IVDA requires all databases to maintain English names for indexing vulnerabilities. However, searching in different languages to obtain relevant vulnerability data is more convenient for native users.
- The minimum description fields need to be optimized to distinguish similar vulnerabilities efficiently.

VI. CONCLUSION AND FUTURE WORK

The previous work like CVE was mostly used to manage vulnerabilities in English software, while IVDA proposed in this paper is a universal model aiming to contribute to the international network security. IVDA provides an open channel for security organizations to share their efforts across the world. When the alliance is implemented, not only vulnerability will have a common format after the general process, necessary communication will also be satisfied. So vulnerabilities in different languages can be searched either in local databases or through VCI. Vendors and governments can obtain the latest security alerts from IVDA to act in response to prevent secure incidents. The future work on IVDA will focuses on the implement issues, involving expanding IVDA members, optimization of minimum description fields, improving IVD duplicate handling, and the multiple language support in VCI.

REFERENCES

[1] R. McMillan, "Siemens: Stuxnet worm hit industrial systems", Computerworld, September 2010.

[2] G. Keizer, "Microsoft's bug reports fail to produce prompt patches", Computerworld, July 2010.

[3] Microsoft, "Software Vulnerability Management at Microsoft", July 2010.

[4] A. Takanen, P. Vuorijärvi, M. Laakso and J. Röning, "Agents of responsibility in software vulnerability processes", Ethics and Information Technology, vol. 6, no. 2, pp. 93-110, June 2004.

[5] Internet Engineering Task Force, "RFC 2828 Internet Security Glossary".

[6] NCNIPC, http://www.nipc.org.cn/

[7] CVE, http://cve.mitre.org/about/faqs.html

[8] P. Mell, K. Scarfone, S. Romanosky, "A complete guide to the common vulnerability scoring system version 2.0", June 2007. Available from: http://www.first.org/cvss/cvss-guide.html

[9] Q. Liu, Y. Zhang, "VRSS: A New System for Rating and Scoring Vulnerabilities", Computer Communications, Elsevier, vol. 34, no. 3, pp. 264-273, March 2011.

[10] ISS X-Force, http://xforce.iss.net/

[11] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0744

[12] J. P. Choi, C. Fershtman, N. Gandal, "Network Security: Vulnerabilities and Disclosure Policy", 2007