An Architecture to Enable Intelligent Cyber security Information Exchange and Resources Pooling Worldwide

Ebot Ebot Enaw[1],Djoursoubo Pagou Prosper[2]

[1]Department of Computer Science, National Advanced School of Engineering,
Yaounde, P.O Box 8390, Cameroon,

[2]Department of Computer Science, National Advanced School of Engineering,
Yaounde, P.O Box 8390, Cameroon,

Abstract

Over the past couple of years, our society has become very dependent on the Internet and ICT making it a major driver of economy growth. However, with the wide adoption of ICT and the Internet, new threats have emerged in the cyberspace called cybercrimes which cause severe security issues for companies, governments and even individuals. Given that on one hand, borders are not well defined and enforced in the digital world as in the real world, and that on the other hand, cyber-attacks are becoming more intelligent and coordinated, a highly collaborative environment has to be established between all the stakeholders namely Computer Incident Response Team (CIRT), Internet Service Provider (ISP), IT managers, Security solutions providers (antivirus, firewall, SIEM, etc) and end users in order to successfully fight against cybercrime. Therefore, in a bid to address this security concern, we propose an efficient solution to facilitatethe sharing of cybersecurity related informations between stakeholders (CIRT, IT manager, security solutions providers, ISP, end users, etc.), as well as intelligence and resources pooling, we design an architecture that leverages several standards (IODEF, CVSS, RID, CVE, CPE) and concepts like peer-to-peer networks and machine learning.

Keywords: *cybersecurity, IODEF, peer-to-peer network.*

1. Introduction

ICT and Internet have established an environment where borders are not well defined and enforced and the notion of distance is no longer an issue. This new landscape plays an important role in the spread of cyberthreats: A hacker located in country A can attack a government system located in country B by controlling zombies machines of a private company located in country C through a proxy located in country D. Managing this kind of attacks from detection to treatment requires that all the stakeholders involved (CIRT, ISP, IT managers, security solution editors) collaborate in an efficient, rapid, intelligent and secure way. Numerous standards have been developed to deal with vulnerabilities specifications and scoring (CVE, CVSS), assetspecifications (CPE), incidents information sharing (IODEF), etc, but unfortunately they only address abstract formats cybersecurity information should conform to, not the interactions between stakeholders much less intelligence and resources sharing or pooling. Moreover, they are neither harmonized nor interoperablesincethey were supported by different organizations like MITRE and IETF.Also, they are not inclusive enough to enable the collaboration of all the stakeholders.

In a bid to address and tackle these shortcomings, in this paper we propose a new architecture that will leverage the standards already developed, and the concepts like webservices, peer-to-peer and machine learning to develop a solution that will permit on the one hand a secure, rapid and intelligent collaboration between stakeholders, and on the other hand intelligences and resourcespooling.

2. Related work

Some research has been done on topics related to this issue namely [1] that presents a practical approach aimed at building a platform that will enable a national CIRT to develop and disseminate security bulletins customized to IT assets of local private and public companies. Their architecture leverages standards like CVE, CVSS, CPE, XML and is made up of four (04) major components: vulnerability collector that collects rough vulnerabilities information from vendors and incident response team ; IT asset collector which collects information related to IT assets of public and private companies ; security bulletin managers which map vulnerabilities to IT asset and design security bulletins customized to public and private companies ; Alert that disseminates security bulletins and security alerts through email, SMS and XML. A prototype of a system developed in JAVA that implements this architecture was also presented as well as some outputs and results.

[2] presents the Cyber Threat Intelligence (CTI) concept and proposes an approach to manage a CTI project based on three standard processes defined by the PMBOK namely “Develop project charter”, “Develop Preliminary Project Scope Statement” and “Scope *Definition*”. It states that a CTI project should leverage some standards and tools related to cybersecurity such as Real-time Inter-network Defense (RID), Incident Object Description and Exchange Format(IODEF), Trusted Automated eXchange of Indicator Information(TAXII), Traffic Light Protocol (TLP), Vocabulary for Event Recording and Incident Sharing (VERIS) which are presented briefly in their document.

[3] first presents a list of formats and protocols developed to standardize the exchange of cybersecurity related information between several stakeholders. It then focus on the Structured ThreatInformation Expression language (STIX) and presents in detail its main components which are:Observables, Indicators, TTPs, ExploitTargets, Incidents,CoursesOfAction, Campaigns, and ThreatActors. Finally, it illustrates the STIX language through a scenario featuring exchange of incident information and log data output by IDS/IPS sensor of a company targeted by a Dos DNS attack.

[4] proposes an architecture based on ontologies and XML to enable easy location and access to cybersecurity informations stored in scattered servers.Their architecture is made up of four major components: *Discovery Client*that retrieves cybersecurity information by communicatingwith one or more arbitrary Discovery Servers ; *Discovery Server* provides assistances to find proper InformationSource to *Discovery Clients* by communicating withmultiple Registries, aggregating information from them, andthen delivering the aggregated information to the *Discovery Client*;*Registry* managesan internal registry that contains the metadata of *Information Sources* by communicating with them ;*Information Source*provides cybersecurity information that is described in XMLformat by communicating with Registries. It finally presents a prototype of their system that is developed in Java and executed on Linux Centos.

[5] advocates the need for a globallycommon format and framework for cybersecurity informationexchange, which will eventually minimize the disparityof cybersecurity information availability on a globalscale and presents CYBEX as the solution. This article presents in details the major components of the CYBEX framework namely: *Information Description*, *Information Discovery*, *Information Query*, *Information Assurance* and *Information Transport*.

3. Research problem

Given the ever-growing impact of the Internet on the global economy and the surge in more sophisticated and coordinated cyber-threats, the establishment of a collaborative environment between different stakeholders is highly needed. In fact, whether for preventive or curative purposes, stakeholders need to interact:

- When an asset is under attack, the IT manager of that asset has to handle the attack and carry out investigations. In this process, interactions need to be carried out between local and remote CIRTs, ISP, and even the vendors of the security solutions deployed inside the victim’s company ;

- In order to prevent cyberattack, IT managers need to identify the vulnerabilities their systems are exposed to and implement the corresponding patches. To that effect, they need to interact with CIRT, security solutions vendors, etc.

Though some protocols have been developed to standardize some of these interactions, they only define the format the cybersecurity information should conform to not the interaction between stakeholders, they are heterogeneous and supported by different organizations, and they handle interactions between some stakeholders only.

Therefore in this paper, we propose a unified architecture that will permit a flexible, secure and intelligent collaboration of all the stakeholders.

This system will leverage existing protocols (IODEF, CVE, CVSS,etc) and concepts like webservices, peer-to-peer file sharing, machine learning, NoSQL, etc.

4. Description of some cybersecurity’s information standards

4.1 CVE

[1] CVE is a dictionary of publicly known information security vulnerabilities and exposures managed by the MITRE organization.

CVE assigns a unique identifier to each vulnerability called CVE-ID or CVE names or CVE number or CVEs.

The syntax of this identifier is as follows:

CVE prefix + Year + Arbitrary digits where Year represents the year when the ID were assigned to a particular vulnerability, and “arbitrary digits” represents any digits assigned to the vulnerability.

CVE-ID are assigned by CNA (CVE Numbering Authority). CNA request CVE-ID pool from MITRE and uses the pool to assign CVE-ID numbers to researchers and information technology vendors for inclusion in first-time public announcements of new vulnerabilities.

CVE has become very popular as it has been adopted by many entities including vendors, Computer Incident Response Team and vulnerability assessment service.

4.2 CVSS

[1] The Common Vulnerability Scoring System is a free and open standard under the responsibility of Forum of Incident Response and Security Teams (FIRST) that

provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics.

The base metric group represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments. This contains six metrics: Access Vector, Access Complexity, Authentication that captures how the vulnerability is accessed and whether or not extra conditions are required to exploit it and Confidentiality impact, Integrity impact, Availability impact which measure how a vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability.

The temporal metric group represents the characteristics of a vulnerability that change over time but not among user environments. It contains three metrics: exploitability, remediation level and report confidence.

The environmental metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment. This group contains five metrics: collateral damage potential, target distribution, confidentiality requirement, integrity requirement and availability requirement.

Generally, the base and temporal metrics are specified by vulnerability bulletin analysts, security product vendors, or application vendors because they typically have better information about the characteristics of a vulnerability than do users. The environmental metrics, however, are specified by users because they are best able to assess the potential impact of a vulnerability within their own environments.

This framework has been adopted by many entities namely: vulnerability bulletin providers, software application vendors and researchers.

4.3 IODEF

The Incident Object Description Exchange Format (IODEF) is a format derived from XML to standardize the exchange of computer security information between Computer Security Incident Response Teams (CSIRTs) and parties that have an operational responsibility of remediation or a watch-and-warning over a defined constituency (ISP, bank incident response team). Its XML schema allows for the representation of computer security incidents data like: attack methodology, incident impact, actions performed to handle the incident, systems and devices involved in the attack, services running on those systems, time when the incident was discovered as well as the contact of persons that handle the incident, etc. However, in an effort to provide to IODEF the support for existing protocols such as CVE, CVSS, CEE,CAPEC, CVRF, CWE, CWSS, OCIL, OVAL, XCCDF and XDAS the MILE group develop an extension to IODEF called IODEF-SCI.

4.4 CYBEX Framework

The Cybersecurity Information Exchange Framework (CYBEX) is a framework developed by the ITU (International Telecommunication Union) as the recommendation ITU-T X.1500 in an effort to enable coherent, comprehensive, global, timely, and assured exchange of cybersecurity information. It has been designed to be a flexible and evolutive framework so as to support new technologies and applications like smart grid and cloud computing. This framework is based on two (02) main pillars:

- Structuring cybersecurity information for exchange purposes: This pillar is aimed at developing standards for structuring “cybersecurity information” so that stakeholders share informations easily. These cybersecurity informations are grouped in clusters: “Weakness, vulnerability and state exchange”, “Event, Incident, and Heuristics Exchange”, “policy exchange”, “evidence exchange”, “identification and discovery”, “identity assurance”, that leverages protocols like Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), Common Weakness Scoring System (CWSS), Open Vulnerability and Assessment Language (OVAL), eXtensible Configuration Checklist Description Format (XCCDF), Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), Asset Reporting Format (ARF),Common Event Expression (CEE), Incident Object Description Exchange Format (IODEF), Common Attack Pattern Enumeration and Classification (CAPEC), Malware Attribution Enumeration and Characterization Format (MAEC), Traffic Light Protocol (TLP), ETSI TS102232, ETSI TS102657, 3GPP TS23.27;
- Enabling information exchange: This pillar provides methods and mechanisms which can be used to identify and locate sources of cybersecurity information, types of cybersecurity information, specific instances of cybersecurity information, methods available for access of cybersecurity information as well as mechanisms to secure the exchange of information. It proposes the attribution of OID to cybersecurity information, organization and policy and introduces Cybersecurity Information Query Language (CYIQL) which is a query language derived from XML for requesting information commonly exchanged by Computer Incident Response Teams (CIRTs) about computer security incidents. As security mechanisms it proposes technologies like Trusted Platform Module (TPM) and digital certificates;

4.5 SCAP

The Security Content Automation Protocol (SCAP) is a standard created by the National Institute of Standards and Technology (NIST) to provide an automated, standardized approach to perform security operations such as verifying the presence of patches, checks for known vulnerabilities, verifying security configuration settings, and generating reports that link low-level settings to high-level requirements, examining systems for signs of compromise. It is a set of specifications that standardize the format and nomenclature by which security products exchange software flaws and security configuration information.It is made up of three (03) major components:

- Enumerations: This component entails nomenclatures and dictionaries for security and product-related information. It leverages standards like CVE, CPE and CCE;
- vulnerability measurement and scoring: This component provides specifications for measuring the characteristics of vulnerabilities and generating scores based on those characteristics. It leverages the CVSS standard ;
- Expression and checking languages: This component provides an Extensible Markup Language (XML) schema for specifying checklists, generating checklist reports, and specifying the low-level testing procedures used by the checklists. It leverages standards like OVAL and XCCDF.

4.6 RID

Real-time Inter-network Defense (RID) is a framework developed to enable easy exchange of data between stakeholders (CIRT, ISP, etc) when handling information security incidents. RID messages can be communicated between stakeholders to report or investigate any type of incident and allow for actions to be taken. It supports natively IODEF and provides four (04) main message type: Report, query, request, acknowledgement and result. To provide security, RID leverages existing security mechanisms such as XML encryption and signature, public key infrastructure (PKI), etc.

5. Peer-to-Peer File sharing network

It is a network made up of nodes (peers) which are end-users computers and that allow for the sharingof files and data among them. This type of network has become popular over the past decade and permits users to download video, music and other files easily. Many tools and technologies exists namely Bitorrent and edonkey. To enable the sharing of data between the peers, two main architectures have been designed:

- Centralized tracking: In this architecture, when a peer wants to share a file, he first splits it intoa number of identically sized pieces and generates the hash of individual pieces. He then creates a torrent file that contains the URL of the tracker and an "info" section, containing (suggested) names for the files, their lengths, the piece length used, and a SHA1 hash code for each piece, all of which are used by clients to verify the integrity of the data they receive. The tracker maintains a list of the peers that hold the file shared so that when someone needs to download the file in question, he will just open the torrent file with a P2P client which will connect to those peers to get pieces of the files which will be reconstructed later to make the original file.

- Decentralized tracking: In this architecture which is also called “trackerless”, each peer plays the role of the tracker. One of the most prominent technology of decentralized tracking is DHT (Dynamic Hash table). In this technology, a keyspace containing the possible hash values of files is built and subdivided into segments and ownership of each of these segments is assigned to peers. When a peer connects to a P2P network, it automatically gets IP addresses of some peers so that when the client will try to download a file, he will send the hash of the pieces of this file to the peers which will route it to the closer peers (in terms of distance between the keys) until it reaches the peers that hold the specific piece. This will be done for all the pieces of the file to download.

Though decentralized tracker provides a more reliable architecture as it can handle the loss of a tracker, Centralized tracker offers an environment where the owner of the file can control who downloads its files as well as gather statistics easily.

6. Our Solution

6.1 Methodology

In an effort to design an efficient architecture that will enable easy and intelligent security information sharing between stakeholders, we leverage concepts of peer-to-peer file sharing, machine learning and standards related to cybersecurity’s information exchange that were described in previous sections. Our architecture relies on a P2P network with controllers that play almost the same role as that of the trackers in the P2P file sharing architecture. All communication between the modules use webservices and XML

The methodology used to design this architecture consists of the following steps:

1. Identify the different stakeholders and the information they need to share as well as the operations they need to perform ;
2. Define the protocols and standards used to exchange those information ;
3. Develop the module that will permit the identified stakeholders to exchange information ;

6.2 Identification of stakeholders

The major stakeholders that intervene in our architecture are:

- End user: End users should receive alerts whenever a new vulnerability is discovered. They should be able to report an incident easily ;

- IT security manager of company: The IT security manager should be able to gather in real time all the vulnerabilities that target the IT asset of his company, their risk level as well as the latest news related to cybersecurity. He should also be able to report an incident as well as interact with other entities (CIRT, ISP) to handle this incident ;

- Computer Incident Response Team: The CIRT should be able to interact with other entities (CIRT, ISP) when handling incidents. It should be able to report incidents and vulnerabilities, disseminate security bulletins and compute statistics.

- Security vendors: They should be able to make available their products, patches and updates. They should have a way to interact and assist in real time their customers who are undergoing an attack;

6.3. Identification of standards

In our architecture we adopted the following standards:

- CVE for vulnerability enumeration
- CPE for assets enumeration
- MAEC for malware enumeration
- CVSS for evaluating the score of vulnerabilities
- IODEF-SCI: for exchanging security incident information
- TLP for defining the level of confidentiality of information

6.4. Description of the components of the architecture

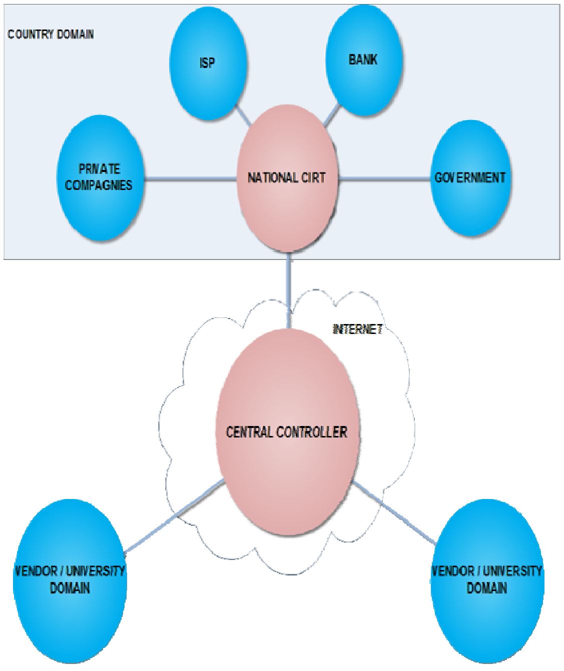

Fig1: global architecture

As depicted in the figure above, the architecture we propose is a hierarchical P2P network made up of a central controller that interconnects domains. There are two types of domains: country's domain and vendor/university domain. Each domain is a P2P network with a domain controller that acts as the gateway for others domains.

6.4.1 Country Domain

The country domain encompasses the national CIRT of a country and its constituencies namely the ISP and the public and private companies of the country. The national domain is a peer to peer network where the national CIRT plays the role of the domain controller. It is worth mentioning that each of these constituencies can be a subdomain with a domain controller also. For efficiency purposes, we propose that the country's domain controller server should be hosted in the national IXP (Internet eXchange Point) for countries that have an IXP. The modules deployed in the constituencies of a country's domain are described in the following sections.

6.4.1.1 National CIRT's module

This module is made up of seven (07) main components:

- Cryptographic key management: This component acts as a certification authority since it delivers certificates to all the constituencies (ISP, private/public companies). It holds a certificate signed by the certificate of the central controller which it uses to sign the certificates it delivers. It carries out all the functions of a certification authority including creation, renewal and revocation of certificates. The certificates issued to the constituencies are used to secure communication between them through the TLS protocol ;

- Client Manager: This component holds the database of the client (constituencies) as well as their state (connected or disconnected). It also collects information pertainingto the IT assets of the different constituencies using the CPE format ;

- Collector: This component collects vulnerabilities and news related to IT assets of the constituencies of a national domain from other CIRT and security vendors. The vulnerabilitiescollected conform to the CVE format;

- NAT transversal: Enable the initial setup of a direct communication between entities of the country domain located behind NAT devices through hole punching technique ;

- Incidents manager: This component that relies on IODEF-SCI protocol, is in charge of enabling the exchange of information when handling incidents. When a constituency of the national domain is undergoing an attack, it notifies the CIRT which will coordinate in real time the treatment of the incident with the assistance of other entities like ISP and CIRT of other countries. This module also implements machine learning algorithms to analyze past cases of synchronized attacks or zero day and then collects and analyzes incidents' descriptions stemming from diverse sources in the country domain in a bid to detect synchronized attacks or zero day. ;

- Digital forensic manager: Usually, when a cybercrime is committed, investigators have to collect and analyze the digital evidences. However a lot of countries especially those of developing countries do not have a well-equipped forensic lab or digital forensic experts that can analyze digital evidences. Therefore, a system that enables CIRTs that do not have a well-equipped forensic lab to send a copy of the evidences collected to other well-equipped CIRT for analysis purposes is necessary ;

- Search engine: This module keeps a copy of the metadata of all the data available in the database of the constituencies of a national domain with the ID of the constituency that owns the data so that when an entity requests a data, this module will respond with the ID of the constituency that holds therequested data and the requester will then establish a link with that constituency to download the data in question. It also acts as a gateway to all data stored outside the national domain.

This module uses a NoSQL database to store all its data.

6.4.1.2 Client's Module

This module is installed in ISP, private and public companies of a country and enables them to perform the following operations:

- Request assistance to treat an incident and interact with other entities such as CIRT and other ISP. It leverages the IODEF standard ;

- Gather customized security bulletin containing vulnerabilities that targets their assets as well as links to download the patches and fixes from security vendors' repositories ;

- Keep a directory of all the IT assets of the client (ISP, public/private company) in the CPE format as well as their interconnection ;

- Compute the CVSS score of vulnerabilities targeting the IT assets of the client considering the role each asset plays as well as their interconnections ;

- Receive latest news on specific subject in cybersecurity;

- Request information related to cybersecurity (security product, statistic, vulnerabilities, threat, etc.).

6.4.3 Central controller

This module is the core of our architecture. It carries out the following operations:

- Keeps and stores in its database all the metadata of data and information storedin all the stakeholders databases so that when en entity located in a domain requests an information, that request is first transmitted to the controller of thesaid domain and if it is not available in the local domain, the request is forwarded to the central controller which will identify the domain where that information is store. It will then requests from that domain's controller the identity of the entity that holds the information and returns it back to the requester ;

- Enables pooling of resources when handling incidents: When an entity notices a security incident and submits it to its domain controller, the domain controller will submit it to the central controller which based on artificial intelligence and machine learning techniques will analyze the incident’s description and locate the “best” resources and entities that could be helpful in treating the incident in question. These entities will then share their resources and knowledgeto treat the incident ;
- Acts as the root certification authority and in so doing signs, revokes and renews certificates of domain controller and vendors ;
- Enables the initial setup of a direct communication between entities located behind NAT devices through the*hole punching* technique;
- Produces statistics related to cybersecurity at the global level.

6.4.2 Universities and Vendor domain

IT products and security solution vendors and universities/research center have an important role to play in the fight against cybercriminality. This module enables them to perform the following actions:

- Publish patches and updates in a standardized way and make them available to customers easily ;
- Enable the collaboration and exchange of information and knowledge between vendors ;
- Make their knowledge and resources (malware detection mechanisms, malware signatures, etc) available when handling attacks ;
- Guarantee interoperability between their vendor’s products: today, when a security solution (antivirus, firewall, IDS, IPS, etc.) is deployed in an information system, thesaid information system can only be protected from malwares or attacks their security solutions recognize. Unfortunately, all the security solutions cannot detect or protect from all types of threats since some threats might be detected by one security solution and not be detected by others. Therefore, it is essential to define a standard format for vendor to develop security solutions so that different security solutions can share threat signatures or protection mechanisms. This module leverages the standards: MAEC (Malware Attribute Enumeration and Characterization) and MMDF (Malware Metadata Exchange Format).

7. Case Study

Although our architecture enables all the stakeholders to collaborate and share information related to various cybersecurity topics namely: incidents, vulnerabilities, news and digital investigations, in this section we will illustrate the interactions between the various stakeholders in a situation where a company is victim of a cybersecurity incident as depicted in figure 2 below.

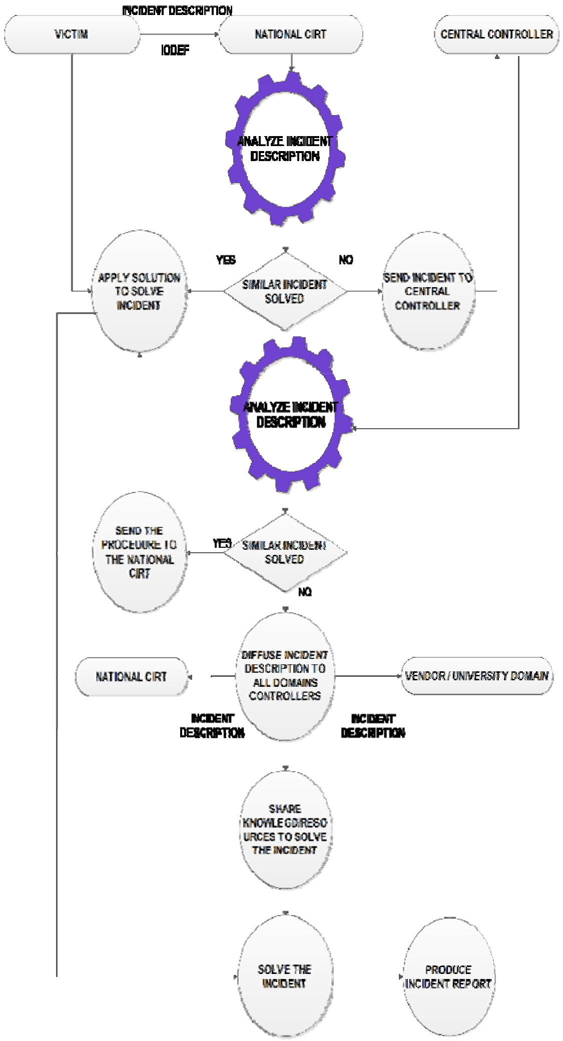
INCIDENT DESCRIPTION
VICTIM
IODEF
NATIONAL CIRT
CENTRAL CONTROLLER
ANALYZE INCIDENT DESCRIPTION
YES
NO
APPLY SOLUTION TO SOLVE INCIDENT
SIMILAR INCIDENT SOLVED
SEND INCIDENT TO CENTRAL CONTROLLER
ANALYZE INCIDENT DESCRIPTION
SEND THE PROCEDURE TO THE NATIONAL CIRT
YES
SIMILAR INCIDENT SOLVED
NO
NATIONAL CIRT
DIFFUSE INCIDENT DESCRIPTION TO ALL DOMAINS CONTROLLERS
VENDOR / UNIVERSITY DOMAIN
INCIDENT DESCRIPTION
INCIDENT DESCRIPTION
SHARE KNOWLEGDIRESOURCES TO SOLVE THE INCIDENT
SOLVE THE INCIDENT
PRODUCE INCIDENT REPORT

Fig 2: Incident handling interactions between stakeholders

1. Whenever a victim identifies a cybersecurity incident,itsends the incident's description to the national CIRT of its country in the IODEF format ;
2. The national CIRT analyses the incident's description and using artificial intelligence algorithms, it tries to figure out whether similar incidents have been solved in the past. If so, it will first send the victim the procedure undertaken to solve the past incident, secondly it will collaborate with the victim to solve the said incident and finally it will produce the incident's report ;
3. If the national CIRT cannot identify in its database similar past incidents, it will forward the incident's description to the central controller ;
4. The central controller will analyze the incident's description and using artificial intelligence algorithms, it will try to figure out whether similar incidents occurred and were solved in the past. If so, it will send, the procedure undertaken to solve the past incident to the national CIRT of the victim;
5. If the central controller doesn't find similar incidents, it will first broadcast the incident description to all main domain controllers (vendor/universities domain controller, national CIRT) and then it will create a virtual group where all stakeholders can share knowledge and pool their resources to solve the incident ;
6. When the incident is solved, the national CIRT of the victim will produce and store the incident's report. This report will be used for subsequent similar incident and also will enable the vendor to develop products or patches to handle future occurrences of the incident in question.

8. Conclusion and future work

Due to the ever growing importance of ICT and Internet in our daily life, the diversity of IT and security products' vendors,coupled with the fact cyber-attacks are becoming more intelligent and coordinated, there is a need to build a platform where all the stakeholders can collaborate and exchange information and experiences in order to curb cybercrimes.

A number of formats and protocols have been designed to standardize the way some types of cybersecurity's information are kept but they didn't address the whole issue of cybersecurity's information and experience sharing as well as the pooling of resources of stakeholders.

Therefore, in this paper we propose a new architecture inspired by Peer-to-Peer file sharing network. Our architecture is hierarchical and is made up of a central controller and different domains. Each domain has a set of actors or constituencies and a domain controller that acts as a gateway to other domains. Each stakeholder can establish a direct or Peer-to-Peer connection with another stakeholder and security is provided through digital certificates. The domain controller is not involved in the communication between stakeholders, it intervenes only in the initial setup of the peer-to-peer link. The data exchanged between stakeholders conform to the existing formats and protocols namely CVE, IODEF, etc. Domain controllers and Central controller do not store all the data exchanged, they only keep metadata of these data and a mapping between metadata and data's owner so that when a stakeholder requests a particular data, he will receivethe address of the owner of the data and the requester will establish a direct connection with thedata's owner. Domain and Central controller also implements some artificial intelligence and machine learning techniques that do permit them to identify a set of "best" entities and resources that could be put together to handle a particular incident.

One of the most important achievements of this architecture is that it allowsfor fluid and intelligent communication between stakeholders when treating an incident and enables interoperability and integration between security tools.

Although this paper has set the building blocks of an architecture that will enable stakeholders to share information and joint their efforts and experiences to curb cybercriminality in an intelligent way, much remains to be done. Therefore, future work can include the specification of these building blocks and the development of prototypes of a system that will implement this architecture so as to evaluate its pragmatism and applicability.

References

[1] Dr Ebot Ebot Enaw , Djoursoubo Pagou Prosper, "A system for collecting security alerts and diffusing customized security bulletins " in *International Journal of Advanced Computing, Vol. 3 (2) , 27-34,* 2014.

[2] Greg Farnham, Kees Leune, "Tools and Standards for Cyber Threat Intelligence Projects" *SANS Institute, 2013.*

[3] Julius Barath, "Protocols for exchange of cybersecurity information" Security and Protection of Information conference, 2013.

[4] Takeshi Takahashi, Youki Kadobayashi, Yuuki Takanoy, "Linking Cybersecurity knowledge: Cyberecurity information discovery mechanism " in Annual Computer

Security Applications Conference poster session, 2012.

[5] Anthony Rutkowski,Youki Kadobayashi, Inette Furey, Damir Rajnovic,Robert Martin, Takeshi Takahashi "The Cybersecurity Information Exchange Framework", ACM SIGCOMM Computer Communication Review Volume 40 (5), 2010

Biography

Dr. EBOT EBOT ENAW obtained his B.Eng hons degree from Liverpool University in Electronic Engineering in 1989. He later obtained an M.Eng degree in Telecommunication Engineering from The University of Manchester England in 1991. He returned home where he was recruited in the University of Yaounde I, as an assistant lecturer. He pursued his university studies and obtained a PhD in Computer Sciences from the National Advanced School of Engineering of the University of Yaounde I, where he is currently a senior lecturer. His area of specialization include: computer network security, cryptography and formal specification and verification; theorem proving and model checking. He has published many research articles in peer-reviewed international journals. In 2006 he was appointed Director General of the National Agency for Information and Communication Technologies Cameroon, a position he occupies till date. Major activities of the agency include amongst others: securing the Cameroon cyberspace through three key services: Computer Incidents Response Team (CIRT), Public Key Infrastructure (PKI) and Computer Security Audits.
Dr.EBOT EBOT ENAW may be reached at ebotenaw@yahoo.com

DJOURSOUBO PAGOU Prosper obtained his Master degree in Computer science engineering from the National Advanced School of Engineering of the University of Yaounde I in 2009. He holds several certifications in networking and cybersecurity namely CCNA, CCNP, CEH, ECSA, CHFI. In 2013, he was appointed subdirector of the National Computer Incidents Response Team (CIRT) of Cameroon, a position that he occupies till date.