MODELLING CYBER ATTACKS

Farida Chowdhury[1]and Md Sadek Ferdous[2]

[1]Department of Computer Science &Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh

[2]Electronics and Computer Science, University of Southampton, Southampton, UK

ABSTRACT

In this article, we present a model of cyber attacks which can be used to represent a cyber attack in an intuitive and concise way. With ever-increasing popularities of online services, we have seen a growing number of cyber attacks targeted towards large online service providers as well as individuals and the IoT devices. To mitigate these attacks, there is a strong urge to understand their different aspects. Creating a model is a widely used method towards this goal. Unfortunately, the number of models for cyber attacks is pretty low and even the existing models are not comprehensive. In this paper, we aim to fill this gap by presenting a comprehensive cyber attacks model. We have used this model to represent a wide range of cyber attacks and shown its applicability and usefulness. We believe that our model will be a useful tool for the formal analysis of cyber attacks.

KEYWORDS

Cyber Attacks, Modelling, Security.

1. INTRODUCTION

With the ever-increasing demand for online services, more and more financial transactions, consisting of highly sensitive financial and personal information, are carried out online. Furthermore, we are heading towards a direction where a plethora of IoT (Internet-of-Things) devices will get connected to the Internet. These IoT devices comprise of a wide variety of hardware ranging from small devices envisioned to be used within a smart home environment to large Cyber-Physical devices to be used for protecting national infrastructures. All these scenarios present a lucrative economic incentive for the attackers to carry out cybe attacks. This is evident from large scale attacks against a number of large online service providers such as Amazon,Ebay, Yahoo, Sony and so on [1, 2, 3, 4, 5]. In a recent cyber attacks, a huge number of IoT devices have been compromised to launch a large scale Distributed Denial of Service attack[4].

To mitigate these attacks, there is a strong urge to understand their different aspects. Towards this goal, a popular approach among the researchers is to categorise and analyse cyber attacks using a taxonomy. This has resulted in a number of taxonomies created using different criteria [6, 7, 8, 9]. Even though very popular, a taxonomy can barely be used to represent a cyber attack in a concise way and to understand its different characteristics.

Creating a comprehensive model would be a much more effective approach in order to understand and represent a cyber attack. Unfortunately, the number of models for cyber attacks is pretty low and even the existing models fail to embody all the required properties of a cyber attack. In this paper, we aim to feel this gap by presenting a comprehensive model of a cyber attack that captures a wide range of properties associated with a cyber attack.

Contribution

The major contributions of this article are:

- A comprehensive model of a cyber attack encoding its different characteristics.

DOI: 10.5121/ijnsa.2017.9402

- A taxonomy of cyber attacks based on the motivations of an attacker.
- Modelling a variety of major cyber attacks according to the presented model and thetaxonomy.
- Showcasing the applicability and the usefulness of the presented model by illustrating two examples.

Structure

The paper is structured as follows. The related work is presented in Section 2. In Section 3, we present the model of a cyber attack. Next, a taxonomy of different cyber attacks is presented in Section 4. Then, we model different cyber attacks utilising our model in Section 5, Section 6 and Section 7. We discuss the usefulness of our model by presenting two examples in Section 8 and finally, we conclude in Section 9 with a direction of future work as well.

2. Related Work

Understanding cyber attacks from different perspectives is crucial in order to mitigate them. Towards this vein, a popular research topic is to create, present and analyse different cyber attacks using a taxonomy based on a range of criteria. There are a number of research papers which eitherpresent a novel taxonomy based on new criteria or survey and analyse the existing taxonomies to identify their strengths and weaknesses as well as to identify the gaps in them. These works provide a solid foundation towards understanding different cyber attacks which is essential to model them. That is why, at first, we analyse a few works on the taxonomy of cyber attacks in different domains.

In [6], the authors have presented a dimension based taxonomy. The authors have utilised four different dimensions where the first dimension consists of different attack vectors. In the second dimension, the authors have considered the attack targets to create a taxonomy whereas the third dimension considers different vulnerabilities. Finally, in the fourth dimension, attack payloads are considered. Moreover, the authors have also analysed and compared a few other similar taxonomies.

Supervisory Control and Data Acquisition (SCADA) systems are an integrated component of any crucial critical infrastructure as well as cyber-physical systems. In recent years, SCADA systems have been increasingly targeted for different cyber attacks. In [7], authors have presented a taxonomy of cyber attacks in SCADA systems. Their main motivation in presenting the taxonomy is to highlight common traits among the attacks and to identify unique challenges for securing such systems. In a similar vein, the authors in [8] have presented another taxonomy of different cyber attacks based on a different set of criteria. Similarly, in [9], the authors have presented a taxonomy of network attacks as well as a taxonomy of attack tools. In addition, a comprehensive survey of different attack and defence tools and systems have been presented.

There are a few other works presenting different taxonomies of attacks. They are briefly discussed below:

- An analysis and comparison of different taxonomies within the domain of social engineering has been presented in [10].
- The authors in [11] have presented a taxonomy of a wide range of attack methods in Peer-to-Peer networks.
- A taxonomy of threats in Cloud-of-Things has been presented in [12].

Next, we explore a few works which focus on modelling (mathematically or analytically) different threats, security attacks and other related issues. A formal way for modelling information security attacks has been presented in [13]. The model utilises attack trees to represent a security attack. This attack tree is then used to identify attack patterns. The authors argue that modelling based on attack trees and attack patterns will be helpful to identify common yet recurring attack traits which could be utilised to mitigate such attacks.

In [14], a formal language, called Correlated Attack Modeling Language (CAML), has been presented to model a multistep cyber attacks scenario. CAML supports a modular functionality where each module can represent an attack inference and therefore, multiple modules can be linked together to represent multistep attack scenarios. In addition, CAML is equipped with a library of predicates which are used to describe different system properties, states and events. Their motivation is similar to the motivation of this paper. However, unlike their work, our focus is on the representation of the attack itself.

Petri nets have been utilised to model cyber-physical attacks within the domain of smart-grid in [15]. The authors argue that petri nets are more expressive in comparison to attack trees to represent any attack. However, modelling a large scale cyber-physical system requires a significant manual input to create the petri net. To address this limitation, the authors have proposed a hierarchical method to create large petri net by combining a number of small petri nets. A petri net can provide an excellent visual representation of attacks, however, their main shortcoming is that they do not encode different significant properties of an attack.

There are other works, as presented in [16, 17, 18, 19], which discuss and present a threat model in lifelogging, mathematical representation of identity and trust issues. Even though they are not strictly related to the scope of current paper, we have drawn motivations on how to model an attack from these works.

In essence, there is not any work presenting a comprehensive model of a cyber attack. To the best of our knowledge, this article presents the first attempt to model a cyber attack comprehensively by encoding its different properties.

3. ATTACK MODELLING

Let us assume that Adenotes the set of attackers while$V$ denotes the set of victims. The set of cyber attacks is denoted using $ATTACK$.

A victim can be a single person or an organisation. We denote the set of persons and organisations as U and O respectively and define V as follows.

$$V \triangleq \{U \cup O\}$$

Furthermore, we denote the set of systems as$S$. We assume that every system is either owned or operated by a person or an organisation. Every system has many processes which are different computing programs running in the system [20]. We denote the set of processes as$P$. Every system is connected to another system using the network, consisting of different routers, bridges, switches, hubs and so on. Without specifying too much granularities regarding these components of a network, we consider it as a single entity. We use the notation$N$ to denote the set of networks. Finally, every system, in reality different programs in the system, handles data which are also transmitted between different systems using a network. We denote the set of data with$D$.

According to our model, every attack is originated from an attacker$a$ (where$a \in A$) and is aimed towards a single target or a set of targets. The target can be data, a process, a system or a network. We denote the set of targets with$T$ which is defined in the following way:

$$T \triangleq \{D \cup P \cup S \cup N\}$$

Via the target, each attack attempts to victimise a person or an organisation, generally labelled as the$victim$. We model this relationship using the following notation:

$$a \mapsto \tau \rightsquigarrow v$$

where, $a \in A, \tau \subseteq T$ and $v \in V$.The notation$\mapsto$ represents the direction of the attack whereas the notation $\rightsquigarrow$ is used to point out the respective victim.

Every cyber attacks is launched using a channel. We consider three types of channels: *visual*, *network* and *hybrid* channel. A visual channel allows an attacker to visually inspect a victim or a system, collect sensitive information and then launch an attack by physically accessing a system. A network channel, on the other hand, allows an attacker to inspect a victim or a system remotely in order to collect sensitive information and then launch an attack over a network. Finally, a hybrid channel allows an attacker to visually inspect a victim or a system in order to collect sensitive information and then launch an attack targeting the system or the victim remotely over a communication network. We use the notationVIS to denote the visual channel, $NET$to denote the network channel andHYB to denote the hybrid channel. Combining these three channels, we define the set of channels (denoted using$C$) in the following way:

$$C \triangleq \{VIS \cup NET \cup HYB\}$$

Every computing system that is connected to the Internet leverages a conceptual model of layers in order to communicate with another system. In our model, we utilise the TCP/IP Protocol model, also known as the $DARPA$ model [21]. According to the TCP/IP protocol model, there are four layers: Network Interface layer (denoted asNIL), Internet layer (denoted as IL), Transport layer (denoted asTL) and Application Layer (denoted asAL). Each cyber attack usually targets a specific layer to launch a successful attack. However, there might be some attacks which might target multiple layers. Combining these four layers, we define the set of layers (denoted using L) in the following way:

$$L \triangleq \{NIL \cup IL \cup TL \cup AL\}$$

Each attack has an associated probability of being successful. We denote the probability of an attack withp_{attack}. In essence, the probability of an attack determines its severity. If an attack has a higher probability of being successful, it is considered to be more severe than another attack having a lower probability. In our model, we consider three different types of severity: $low, medium$ and $high$. The severity of an attack is defined as a function denoted as $severity$and is defined as:

$$severity: ATTACK \longrightarrow \{low, medium, high\}$$

To concretise the severity of an attack, we utilise two different thresholds of probability, $\alpha$and β, where αdenotes a high probability threshold and β denotes a relatively low probability threshold in the threshold spectrum. Therefore, the severity of an attack is concretised in the following way for any$attack \in ATTACK$:

$$severity(attack) = \begin{cases} severe, & if\ p_{attack} > \alpha \\ medium, & if\ p_{attack} \geq \beta p_{attack} \leq \alpha \\ low, & if\ p_{attack} < \beta \end{cases}$$

Since, the probability thresholds effectively can be enumerated using different concrete values (e.g.$\alpha = 70\%$ and so on) in different situations, we have restricted ourselves from assigning a concrete numerical value for the thresholds.

We differentiate between two types of attacks: active and passive [8]. An active attack (denoted as $ACTIVE$) enables an attacker to modify, misconfigure or disrupt a target (e.g. modifying a process, system or data; disrupting a communication channel and so on) whereas a passive attack (denoted as$PASSIVE$) allows an attacker to observe a target without modifying it. With these two types, we define the types (denoted as $TYPE$) of an attack as follows:

$$TYPE \triangleq \{ACTIVE \cup PASSIVE\}$$

Finally, we define an attack ($attack \in ATTACK$) as the following tuple consisting of the attack relation, the channel, the layer it utilises and its associated severity along with the type:

$$attack \triangleq \langle a \mapsto \tau \rightsquigarrow v, c, l, s, type \rangle$$

where, $a \in A, \tau \subseteq T, v \in V, c \in C, l \subseteq L, s \subseteq severity(attack)$ and $type \in TYPE.$

4. Attack Taxonomy based on Motivations

An attacker initiates an attack with a concrete motivation. Here, we have identified three different types of motivations: *footprinting*, *launching* and *trace removal*. We have utilised these motivation to propose a novel taxonomy of attacks. Unlike any previous taxonomies, the taxonomy presented here is based on these motivations; each of which isdescribed below.

Footprinting

Footprinting, also known as *information gathering* [9], can be defined as the systematic use of tools and techniques by an attacker to create a complete security profile of a victim. The security profile consists of information with respect to the target, such as process, layer, network and the system, of the victim. The collected information is used to identify any vulnerability within the target of the victim.

Launching / Compromisation / Gaining access

After gathering enough information about the target and identifying vulnerabilities within them, the attacker aims to compromise the target by launching more severe attacks which exploit the identified vulnerabilities. The main motivation is to get hold of credentials or to compromise the target victim for gaining access to the system. Once the attacker gains access to the system, he/she can exploit the system anyway possible. The attacker can steal sensitive information, install malicious software such as a key-logger or rootkit or even abuse the system to attack another system belonging to another victim.

Trace removal.

After abusing the access to carry out malicious activities, the attacker attempts to modify the system in order to eradicate any trace (history) of the attacker compromising and accessing the system. This step is carried out to ensure that any sign of the system being compromised remains unnoticed.

Next, we present a taxonomy of attacks by classifying them based on these motivations (Figure 1). In the next section, we present the attacks belonging to a particular category and model each corresponding attack using the model presented in Section 3.

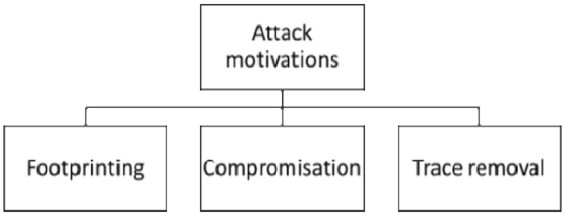

Figure 1: Taxonomy of attacks based on motivations.

5. Footprinting

There are a wide range of footprinting attacks which can be categorised according to their underlying mechanism. Based on these mechanisms, a taxonomy of footprinting attacks is proposed in Figure 2. Each of these attacks is presented below according to their mechanism and modelled using our mathematical model. It is to be noted that the attacks presented here are indirect in nature, meaning that none of these can be used to launch an attack with any devastating implication.

5.1. Social Engineering

Humans are often regarded as the weakest link in any information security system [22]. The social engineering is the process of exploiting the weakest link, the people, in the system with illegitimate motivations. It can be defined as an attacker's use of multitude methods, such as personal interviewing techniques, research skills and trickery/deception, to communicate, deceive and consequently, extract sensitive information regarding a victim from the victim or from the people who are close to the victim such as the victim's employees, partners or customers [23]. It is considered as one of the most primitives yet one of the most successful ways to gather unauthorised information which can be leveraged at a later stage of an attack [24, 25, 26]. There are several mediums by which an attacker initiate a social engineering attack such as via telephone, via an email message, a television commercial, a web-based mechanism or countless other mediums which might provoke human reactions.

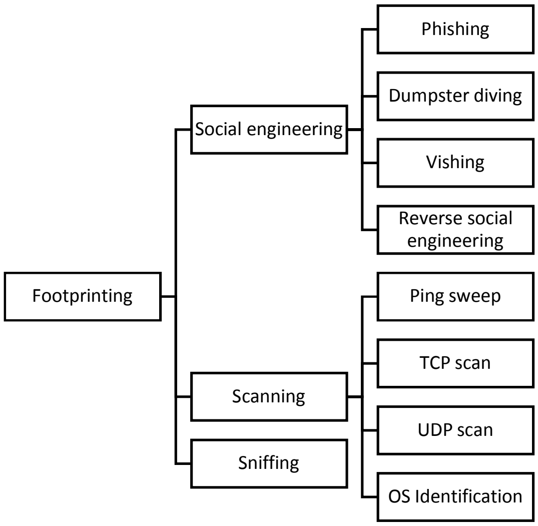

Figure 2 : Taxonomy of footprinting attacks.

There are several attacks that can be categorised under the umbrella of social engineering. Some of these attacks can be leveraged for the footprinting process whereas the others can be directly exploited to carry out more direct attacks. Here, we only describe those attacks which are used for footprinting. The attacks are presented and modelled below [27,10].

Phishing

Phishing is a kind of social engineering attack which is defined as follows [27].

> "*Phishing is the attempt to acquire sensitive information or to make somebody act in a desired way by masquerading as a trustworthy entity in an electronic communication medium. They are usually targeted at large groups of people. Phishing attacks can be performed over almost any channel, from physical presence of the attacker to websites, social networks or even cloud services.*"

There are different modes of phishing attacks: Deceptive Phishing, Spear Phishing, Whaling, Pharming, Dropbox Phishing, Google docs phishing and so on [27].
Phishing is denoted as$Phishing$ and modelled in the following way:

$$Phishing \triangleq \langle\, a \mapsto \{D, S\} \rightsquigarrow u, NET, \{AL\}, \{low, severe\}, PASSIVE\, \rangle$$

The explanation for modelling this attack in the above manner is as follows:

- A phishing attack targets critical user information (data) which can be used to compromise a system. That is why the target is$D$ and$S$.

- Such an attack is carried out via the Internet and hence, the modelled channel is NET.
- Similarly, the attack occurs through an application interface (e.g. via email, website, etc.) and therefore, the layer is modelled with AL
- The severity of the attack depends on what information is captured. For example, if only innocuous information such as a username or date of birth is captured, it can hardly be abused to compromise a system and hence, it has a low severity. On the other hand, if the attacker can capture both username and password or any credit card information, it might have severe consequences and that is why it can be modelled as$severe$.
- Finally, this is a passive attack as this does not actively compromise a system, rather information captured via this attack is used to launch an active attack. Hence, it is modelled as$PASSIVE$.

Dumpster diving

The dumpster diving is the process of scavenging through the dumpster with the hope to find sensitive information [27,28]. Without considering the implication, documents are sometimes discarded in the dumpster which might contain several pieces of crucial information regarding employees, memos and even printed/hand-written sensitive information, such as a password. The main motivation of the attacker is to find such crucial information to carry out more direct attacks, e.g. compromising a system or a specific user account, in the subsequent step. We denote this attack with DD and model in the following way:

$$DD \triangleq \langle\, a \mapsto \{D,S\} \rightsquigarrow u, VIS, \{AL\}, \{low, medium\}, PASSIVE \,\rangle$$

The explanation is similar to what presented before and hence, it has been skipped for brevity.

Vishing

Vishing, also known as Voice Phishing, is the method of utilising a rogue Interactive Voice Response (IVR) system to simulate a legitimate IVR system of an important institution (e.g. a bank) in a convincing manner [10, 29]. The ultimate motivation is to trick the victim to release sensitive information.The vishing attack is denoted withVS and modelled in the following way:

$$VS \triangleq \langle\, a \mapsto \{D,S\} \rightsquigarrow u, NET, \{AL\}, \{low, medium\}, PASSIVE \,\rangle$$

Reverse social engineering

In the traditional mode of any social engineering attack, an attacker initiates the interaction by the process described above. However, in the reverse social engineering attack, the attacker presents a problematic scenario to the victim as well as impersonates someone that the victim trusts in order to address the problem [27, 30]. This would allow the attacker to gain the trust of the victim which could be abused to collect sensitive information to be leveraged at the subsequent step of the attack.

We denoted this attack with RSE and model as follows:

$$RSE \triangleq \langle\, a \mapsto \{D,S\} \rightsquigarrow u, HYB, \{AL\}, \{low, medium\}, PASSIVE \,\rangle$$

5.2. Scanning

All the footprinting methods discussed above require the attacker to interact with the victim to collect sensitive information. However, information with respect to the network and the system of the victim, such as employee names and phone numbers, IP address ranges, DNS servers, and mail servers, also represents a valuable source of information. Interestingly, such information can be collected via remote methods without any direct interaction with the victim. Scanning is the process to facilitate the collection of such information. There are a variety of scanning tools and techniques available, some of which are listed next.

- **Ping sweep:** The basic and the most primitive scanning technique is *Ping sweep*. It is based on sending an automated ping request on a range of IP addresses and network blocks to determine if the target systems are alive [31, 32, 33].

- **TCP scan:** TCP scan is the process of probing and determining open TCP ports which are associated with different network services that the attacker can exploit [34]. There are different ways it can be carried out. For example, the scanning process can probe for normal TCP connections (*TCP Connect Scan*) or employ advanced stealth scans that probe for half-open connections to prevent them from being logged (*TCP SYN Scan* or *TCP FIN scans*).

- **UDP Scan:** In this process, a UDP packet is sent to the target port of the target machine [34]. Most machines will respond with an ICMP *"destination port unreachable"* message, indicating that no service is active on that port. However, if no message is received, an attacker can deduce the port is open and a service is utilising the port. It should be noted that the UDP scanning process is not as reliable as the TCP scan as UDP is a connectionless protocol. Therefore, the accuracy of this method depends on which system and network resources have been utilised.

- **OS Identification:** Once an attacker identifies the ports and the corresponding services running in the target machine using the scanning methods described above, the attacker, then, tries to determine the type of Operating System (OS) within the target system. Different OS have different responses with respect to different queries. The attacker will match those queries with a predetermined *QUERY-REPLY* profile to determine the target OS.

We denote all the scanning attacks with SCN and model as follows:

$$SCN \triangleq \langle\, a \mapsto \{S, N\} \rightsquigarrow u, NET, \{IL, TL, AL\}, \{low, medium\}, PASSIVE\, \rangle$$

5.3. Sniffing

Sniffing is a method by which an attacker can compromise the security of a network in a passive fashion [42]. To initiate this attack, an attacker captures and analyses all network packets to retrieve some useful information. For this, an attacker utilises a tool called Sniffer which can capture packets in a network and analyse them to identify sensitive information, such as authentication information consisting of usernames and passwords. We denote this attack using $SNIFF$ and model it in the following way:

$$SNIFF \triangleq \langle\, a \mapsto \{D, N\} \rightsquigarrow u, NET, \{NIL, IL, TL, AL\}, \{medium, high\}, PASSIVE\, \rangle$$

6. LAUNCHING

At this step, it is assumed that the attacker has been successful to gather a wide range of crucial information utilising different footprinting methods. Next, the attacker aims to launching different $ACTIVE$attacks abusing the gathered information. There are different launching attacks available at the disposal of the attacker. The taxonomy of these launching attacks is proposedin. Next, each of these attacks is briefly discussed and modelled according to our model.

6.1. Account scan

The simplest form of attacks for an attacker to launch is account scanning. For this, the attacker attempts to break in to all identified active network services (e.g. web service, FTP service, etc.) by checking:

- an account with no password,
- an account with the password same as the username, or "password",

- a default account that is shipped with the product/software,
- an anonymous FTP account,
- rlogin/rsh/rexec ports that may support less trusted logins.

We denote this attack with AS and model it as follows:

$$SCN \triangleq \langle\, a \mapsto \{S\} \rightsquigarrow u, NET, \{AL\}, \{low, medium\}, ACTIVE \,\rangle$$

6.2. Social Engineering

Here, we present the social engineering attacks which can be utilised for launching direct attacks. One example of a successful and common attack method is to simply call the helpdesk of an organisation and say something like this: *“Hi, this is Mr. X, the senior director of the organisation. I have to present something to the CEO, but I cannot log into server XYZ to get my notes. Would you please reset my password now according to my choice? I have to be in this meeting in 2 minutes.”*Nowadays, most corporations should have a policy for their helpdesk operators not to reset password as requested. However, an unsuspecting and ill-trained operatormight simply reset the password as requested. Once, the password is reset, the attacker can easily log in to the account and do whatever he likes. Next, we present some of the most widely-used such social engineering methods.

Waterholing. It refers to a targeted attack in which a website, supposedly to be of interest to the victim, is compromised and then malicious contents are injected by the attacker [27, 35]. Once the victim visits the website, the malicious contents are loaded and executed, thus enabling the user to compromise and then ultimately take control of an online account or even the system of the attacker. We model this attack in the following way whereWH represents the waterholing attack:

$$WH \triangleq \langle\, a \mapsto \{D, S\} \rightsquigarrow u, NET, \{AL\}, \{low, medium\}, ACTIVE \,\rangle$$

Baiting. Baiting is the process of luring the victim by drawing his attention using an object [27, 36]. The object could be a malware/trojan horse infected storage medium (e.g. a USB drive) which is intentionally left in a place that could be easily found by the victim. To increase the curiosity of the victim, the attacker often labels the object with tempting labels such as *confidential*. Out of curiosity, once the victim picks up the object and inserts into his system, the system gets infected with the malware/trojan allowing the attacker to have full access to the system. The attack method (denoted as BT) is modelled in the following way:

$$BT \triangleq \langle\, a \mapsto \{D, S\} \rightsquigarrow u, HYB, \{AL\}, \{low, high\}, ACTIVE \,\rangle$$

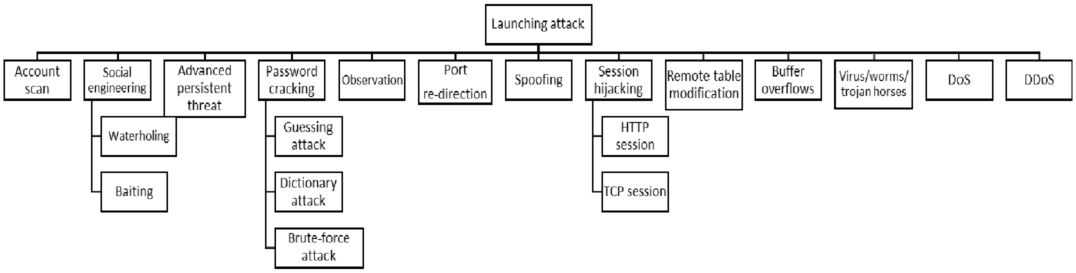

Figure 3: Taxonomy of launching attack

6.3. Advanced Persistent Threat

Advanced Persistent Threat (APT) refers to a long-term attack method employed by a group of attackers targeting specific organisations, governmental institutions, commercial enterprises in order to infiltrate the system for monetary or espionage purposes [27, 37, 38]. This is unlike other traditional attack methods where an attack is launched on a one-time basis. In APT, the attackers study, monitor and attack the target systems for a long period of time with a stay-low and slow approach so that the attacks remain unnoticed. Also, the attackers in APT are usually very well resourced and well organised. US National Institute of Standards and Technology (NIST) has formulated a comprehensive definition of APT combining its different characteristics [39]. The characteristics from this definition is presented below:

> *“The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.”*

We model APT, denoted asAPT in the following way:

$$BT \triangleq \langle\, a \mapsto \{D, S, N\} \rightsquigarrow o, HYB, \{IL, TL, AL\}, \{medium, high\}, ACTIVE \,\rangle$$

6.4. Password Cracking

If the attacker fails to compromise the target system using the account scanning or any of the social engineering methods, he might adopt a more direct exploitation approach to acquire the credentials (passwords) associated with the target systems. One of the most effective methods with this regard is the process of password cracking which can be carried out in one of the following ways.

Guessing attack

The simplest approach for password cracking is to guess the password. Many unaware users do not comprehend the necessity to maintain a secure difficult-to-guess password and hence, they often use passwords which can be easily guessed. A few examples of such easily guessable passwords are [40]:

- To use the word "password" as the password.
- The same password as the username.
- The real names as the passwords.
- The name of the children, spouse, pet, or car model as the passwords.
- Birthdays and birth places as passwords.
- Favourite colours, foods and places as passwords.

Understandably, this approach is more effective if the attacker personally knows the victim and has the knowledge of such information which is susceptible to password guessing.

Dictionary attack

In this attack, the attacker utilises a program or a script that tries different possible combinations of words in a dictionary along with some additional special characters (such as '\#', '\$', '_' and so on) often used in the beginning or in the end of a password [40]. The attacker usually possesses a copy of the English dictionary as well as foreign language dictionaries for this purpose. In addition, additional dictionary-like databases containing names and lists of common passwords are often used.

Brute-force attack

The brute-force attack, often resorted as the last step for the password cracking, requires an attacker to try all possible combinations of characters within the length of the password [40]. A short 4-letter password consisting of lower-case letters can be cracked in just a few minutes. However, a 7-character long password consisting of either upper or lower case letters would take 26^7(8,031,810,176) guesses. A combination of alpha-numerical characters along with casesensitivity and special characters would increase the complexity significantly that it might be impossible to crack within a reasonable period of time.

All these attacks are represented using a combined model in the following way where $PassCrack$ denotes the generic password cracking attack:

$$PassCrack \triangleq \langle\ a \mapsto \{D\} \rightsquigarrow u, HYB, \{AL\}, \{medium, high\}, ACTIVE\ \rangle$$

6.5. Observation / Shoulder surfing

Another primitive yet successful method to accumulate the password is by observation. One of the traditional problems in password-based security is that passwords must be long and difficult to guess. However, such passwords are often difficult to remember. Therefore, users often write them down somewhere. An attacker can often search a person's work site/desk in order to find passwords written on little pieces of paper usually hidden under the keyboard. An attacker can also train themselves to launch the shoulder surfing attack where they look over the victim's shoulder while the victim types in his password at the screen or keyboard [27].This attack is denoted as OBS and modelled as follows:

$$OBS \triangleq \langle\ a \mapsto \{D, S\} \rightsquigarrow u, VIS, \{AL\}, \{medium, high\}, ACTIVE\ \rangle$$

6.6. Port re-direction

Port re-direction can be defined as the process to direct network traffic destined for one port and redirect it to another host into another port [41, 8]. To gain access to a system, the attacker has to compromise the system. However, there might arise a situation where an intervening entity such as a firewall blocks any direct access to a target system. Resourceful attackers can find their way around these obstacles using the port redirection attack to gain access to any system behind a firewall. For this, the attacker listens to certain ports of a trusted host and forwards certain raw packets to a specified secondary target which might be behind a network firewall. We model this attack in the following way:

$$PortRedir \triangleq \langle\ a \mapsto \{S\} \rightsquigarrow u, NET, \{AL\}, \{medium, high\}, ACTIVE\ \rangle$$

6.7. Spoofing

A spoofing attack allows an attacker to falsify the identity of a trusted and authorised user so that the attacker can gain access to the system or the services [43, 44, 45]. It has different modes. In an IP spoofing attack, the attacker spoofs the source address of an IP packet in order to simulate that the packet has originated from a trusted computer and thereby, compromising any IP based authentication mechanism. In a DNS (Domain Name Service) spoofing attack, the attacker compromises a DNS server and modifies the DNS entry in such a way that a domain name is rerouted to an IP address belonging to a server controlled by the attacker. In an ARP (Address Resolution Protocol) spoofing attack, the attacker spoofs the association between MAC (Media Access Control) and IP address in a LAN in such a way that all traffic targeted for a trusted node are routed to the attacker node. These spoofing attacks are generally used to steal or alter sensitive information regarding the victim. However, these attacks are used to facilitate other attacks (e.g. Man-in-the-Middle and Denial-of-Service attacks) which will be described below. We denote Spoofing attack using$SPOOF$and model it in the following way:

$$SPOOF \triangleq \langle\ a \mapsto \{D, N\} \rightsquigarrow u, NET, \{NIL, IL, TL, AL\}, \{low, medium\}, ACTIVE\ \rangle$$

6.8. Session hijacking

Session hijacking is the process of taking over a connection which has either been established or is in the process of being set up [46]. In most cases, this would be connections for web applications, however, connections could belong to other protocols such as FTP, SMTP and so on. There are many advanced techniques to launch this attack. We present the most well-used session hijacking techniques below.

HTTP Session

The HTTP Session hijacking is targeted towards a web application [47, 48, 49]. Once a user is successfully logged in a web application, a session is created with a unique session identifier. Then, a session token is issued to the user containing the session identifier, indicating that the user logged in. This identifier is passed in different ways, such as via HTTP cookies, URL rewriting or hidden fields and is used in all subsequent interactions between the user and the web application. Once the session is established, the attacker can hijack the HTTP session by simply getting hold of this identifier which can be used to impersonate the user. This attack is represented using $HTTPSes$ and modelled in the following way:

$$HTTPSes \triangleq \langle\, a \mapsto \{D,P\} \rightsquigarrow u, NET, \{AL\}, \{low, medium\}, ACTIVE \,\rangle$$

TCP Session

A TCP session hijacking technique exploits one of the key features of the TCP/IP protocol [50]. Using different approaches, an attacker can insert malicious TCP packets into an already-established TCP session, thereby enabling commands to be executed on the remote host. The most effective time to hijack the session is after a session has been established between a server and a client and these entities trust each other. There are different ways to launch this attack. For example, an attacker can spoof IP packets (as described above) to insert packets containing malicious commands into the session. Another variant of a TCP session attack leverages a special form of attack called *Man-in-the-Middle (MITM)* [51]. In an MITM attack, the attacker places himself, using the ARP spoof attack, within an established connection between two entities in such a way that every packets transmitted between these entities go via the attacker, thus enabling to insert falsified packets to hijack a session. We model the TCP session attack in the following way where $TCPSes$ denotes the attack:

$$TCPSes \triangleq \langle\, a \mapsto \{D,P\} \rightsquigarrow u, NET, \{TL\}, \{low, medium\}, ACTIVE \,\rangle$$

6.9. Remote table modification

In a remote table modification attack, similar to an MITM attack, an attacker will try to modify the routing table of the target host in such a way that all packets flow through a system he controls. Preferably, an attacker will try to maliciously modify the routing tables remotely by targeting the Open Shortest Path First (OSPF) or the Border Gateway Protocol (BGP) which are used by most ISPs for exchanging route information with each other [52, 53]. A local version of this attack might try to spoof ICMP (Internet Control Message Protocol) packets so that the target host is tricked to route packets via the attacker's host. This works as many OSs have a default configuration which accepts ICMP redirects [51]. We model this attack in the following way whereRTM denotes the attack:

$$RTM \triangleq \langle\, a \mapsto \{D,P\} \rightsquigarrow u, NET, \{NIL, IL, TL, AL\}, \{low, medium\}, ACTIVE \,\rangle$$

6.10. Unexpected input/Buffer overflow

To interact with most of network and web-based applications, users are expected to provide different types of inputs in the forms of mouse click, keyboard typing or multi-modal touch. Handling these user inputs without proper care can introduce vulnerabilities which an attacker can exploit to launch different types of attacks. Many of these vulnerabilities occur due to a mistake in coding, lack of experience in writing secure code as well as undocumented anomaly. One of the most notorious attacks exploiting the unexpected input is the *Buffer Overflow* attack which is widely used by the attackers. In a buffer overflow attack, an attacker crashes or gains control of a specific program of a target host by overflowing the buffer of the program [6, 54, 55]. A common practice among the programmers is to allocate an arbitrary number of bytes for a buffer within a program which is often utilised to store user inputs. If the size of user input is larger than the allocated bytes for the buffer, a situation of buffer overflow occurs. When this happens, the program might crash. However, a resourceful attacker might input a carefully crafted data which includes malicious code. This triggers to overflow the buffer in such a way that the flow of the target program is diverted and then the malicious program is executed, thus allowing the attacker to compromise the program and ultimately the system.We model this attack (denoted by BO) in the following way:

$$BO \triangleq \langle\ a \mapsto \{D, P, S\} \rightsquigarrow u, NET, \{AL\}, \{medium, high\}, ACTIVE\ \rangle$$

6.11. Malicious programs: virus/worm/trojan horse

One major tool employed by the attacker is to exploit malicious programs known as viruses, worms or trojan horses. RFC 1135 defines a computer virus and worm in the following way [56]:

- **Virus:** *"A virus is a piece of code that inserts itself into a host, including operating systems, to propagate. It cannot run independently. It requires that its host program be run to activate it."*
- **Worm:***"A worm is a program that can run independently, will consume the resources of its host from within in order to maintain itself, and can propagate a complete working version of itself on to other machines."*

On the other hand, a *Trojan Horse* (or simple *trojan*) is disguised as a benign program which, once executed, can collect sensitive information from the target system [57]. To be most effective, an attacker normally combines a trojan with a virus/worm. The trojan helps the attacker to retrieve sensitive required information from the target system whereas the virus/worm helps to deliver that information through the network to the attacker.

Even though a virus, worm and trojan horse are different in nature and in their functionalities, we group them together under the category of malicious programs for simplicity. Then, we model an attack, denoted withMAL, involving a malicious program in the following way:

$$MAL \triangleq \langle\ a \mapsto \{D, S\} \rightsquigarrow u, NET, \{AL\}, \{medium, high\}, ACTIVE\ \rangle$$

6.12. Denial-of-Service (DoS)

A Denial-of-Service (DoS) attack is a special class of attacks in which the attacker does not attempt to gain access to the target system. Instead, the main motivation of launching this attack is to disrupt or crush the target system so that legitimate users, networks, systems, or other resources are denied to avail the services offered by the target system [58, 59]. Within this motivation, the attack may target to overload the process/service, the computing and storage resources or even attempt to forcefully shut down the part of the service/system. There are many ways these can be achieved. Next, we present a few ways.

- **Bandwidth consumption:** The most insidious form of DoS attacks is the bandwidth-consumption attack. In this attack, attackers will attempt to consume all available bandwidth to a particular network so that the target system becomes unreachable from other systems.
- **Resource starvation:** A resource starvation attack mostly focuses on consuming resources, such as CPU utilisation, memory and storage quotas, of the target host. An attacker generally is authorised to consume a certain amount of such resources. However,

he abuses the authorisation in order to consume additional resources in such as way other users cannot use them anymore and thereby denying access to the system.

- **Routing and DNS attacks:** A routing-based DoS attack is based on the idea that the attacker manipulates the routing table enabling the attacker to route the traffic of a victim to the attacker's system or to a black hole which is a network that does not exist and thus denying the victim to access the requested service. On the other hand, in a DNS-based DoS attack, an attacker compromises a DNS server to cache bogus DNS information so that traffic towards the target system is routed to the attacker's system and thereby denying other users to access services offered by the target system.

With tools readily available over the Internet, the attacker needs to possess little skills. That is why DoS attacks are currently on the rise. Also, as more and more traditional as well as innovative services are offered online with increasing popularities, the business motivations attached to these services carry a massive monetary value. If such services are disrupted, it often causes a significant amount of monetary loss to the corresponding business organisations. This has attracted the attackers to carry out DoS attacks with the sole purpose of causing significant monetary damages. The motivation of carrying out such an attack often involves scenarios where an organisation would like to inflict monetary damages to other competitive organisations. Moreover, there are personal as well as political vendettas that would drive an attacker to carry out such an attack.We denote a DoS attack usingDoS and model it in the following way:

$$DoS \triangleq \langle\, a \mapsto \{S, N\} \rightsquigarrow u, NET, \{IL, TL, AL\}, \{medium, high\}, ACTIVE \,\rangle$$

6.13. Distributed Denial-of-Service (DDoS)

A DoS attack is usually generated from a single source which, in reality, can cause any significant damage as the source also has limited resources to carry out such an attack. This has motivated an attacker to create a new form of attack called *Distributed Denial-of-Service* (DDoS). A DDoS attack enables the attacker to launch a DoS attack targeted towards a victim from a huge number of different sources [60, 61]. For this, the attacker needs to compromise as many systems as possible by leveraging the attack methods presented before. Such a compromised host is often referred to as a*Zombie*. Then, the attacker installs a specific DDoS tool which remains dormant and preserves a connection with the attacker. Upon receiving a signal from the attacker, the DDoS tool becomes active and participates in the DDoS attack along with other compromised zombies.

In recent years, there has been a steady rise on the number of DDoS attacks, targeted towards large online service providers or different countries [62]. With the prediction of a large number of IoT (Internet-of-Things) devices connected to the Internet in near future, it is feared that many of these IoT devices will be exploited to launch even larger type of DDoS attacks which might be difficult to contain. In fact, we have already seen a DDoS attack involving IoT devices [62].

We denote a Distributed DoS attack using$DDoS$ and model it in the following way:

$$DDoS \triangleq \langle\, a \mapsto \{S, N\} \rightsquigarrow u, NET, \{IL, TL, AL\}, \{medium, high\}, ACTIVE \,\rangle$$

7. Trace Removal

As a final step, the attacker tries to hide his activities just to ensure that the user/administrator of the system cannot trace any source of attack back to the attacker. For this, the attacker may subvert the logging/registry system to remove the captured logs or history of illicit activities [63]. We represent this attack usingTR and model it in the following way:

$$TR \triangleq \langle\, a \mapsto \{P\} \rightsquigarrow u, HYB, \{AL\}, \{medium, high\}, ACTIVE \,\rangle$$

8. Application

In this section we present a couple of applications of our model in order to illustrate the applicability and usefulness of the model. The first application illustrates how the model can be leveraged to create different types of categorisation and is presented in Section 8.1. On the other hand, the second application sketches how the model can be extended for other scenarios and is presented in Section 8.2.

8.1. Dimension-based categorisation

In Section 4, we have presented a taxonomy of cyber attacks based on the motivations of the attacker. Interestingly, the model presented here can be utilised to create different taxonomies, representing different categorisation, based on different aspects within the model. We exemplify a few such taxonomies below. Other categorisations can be easily created following these examples and hence, have been omitted for brevity.

Taxonomy based on channels

We can define a function called $taxonomy_{channel}$which, given a subset of different channels, returns a set of attacks which can be launched using those channels.

$$taxonomy_{channel}: \mathcal{C} \longrightarrow \mathcal{A}$$

Where,$\mathcal{C} \subseteq C$ and $\mathcal{A} \subseteq ATTACK$.

We can use this function to classify attacks based on channels. A few examples follow:

- The attacks which can be launched using the visual channel can be classified as:

  $$taxonomy_{channel}(\{VIS\}) = \{DD, PassCrack, OBS\}$$

- The attacks which can be launched using either the visual or the network channel can be classified as:

  $$taxonomy_{channel}(\{VIS, NET\}) = \{DD, PassCrack, OBS, Phishing, RSE, \dots\}$$

  Here, "..." indicates that there are other attacks belonging to this class which has been omitted for brevity.

Taxonomy based on layers

Similarly, we can define a function called $taxonomy_{layer}$which, given a subset of different layers, returns a set of attacks which can be launched in those layers.

$$taxonomy_{layer}: \mathcal{L} \longrightarrow \mathcal{A}$$

where, $\mathcal{L} \subseteq L$ and $\mathcal{A} \subseteq ATTACK$.

We can use this function to classify attacks based on layers. A few examples follow:

- The attacks which can be launched in the application layer (AL) can be classified as:

  $$taxonomy_{layer}(\{AL\}) = \{Phishing, DD, RSE, \dots\}$$

  Like before, "..." indicates that there are other attacks belonging to this class which has been omitted for brevity.

- The attacks which can be launched using either in the internet layer (IL) or in the transport layer (TL) can be classified as:

  $$taxonomy_{layer}(\{IL, TL\}) = \{SCN, APT, SNIFF, SPOOF, TCPSes, \dots\}$$

Likewise, "..." indicates that there are other attacks belonging to this class which has been omitted for brevity.

8.2. Modelling incident handling

An incident handling mechanism is a strategic process for any organisation to prepare itself with a series of steps in case a security incident in the form of cyber attacks occurs. It is a crucial strategy for any organisation to mitigate risks associated with cyber attacks. It consists of four phases [64, 65]:

- **Preparation:** In this phase, an organisation attempts to minimise the occurrence likelihood of any security incident by taking proactive measures such as deploying firewalls within the organisation's network, malware protection, access control mechanisms, real-time network monitoring and so on.
- **Attack detection and analysis:** Even with the deployment of an array of strong protective measures, there is always a probability for any cyber attack to occur. In this phase, the organisation aims to detect and analyse such an attack.
- **Incident response.** This phase aims to address and contain the identified cyber attack incident so that the associated risk can be minimised as much as possible by adopting a set of reactive approaches such as shutting down the infected system, changing the password of compromised account/system and so on.
- **Post-incident.** Finally, once the incident has been contained, it is required to reflect upon the newly identified attack so that protective measures can be fed back to the preparation phase. This is to ensure that the similar attack can be prevented at the initial stage in future.

We model the incident handling mechanism using as the following:

$$IncidentHandling \triangleq \langle\ Prep \biguplus DA \biguplus IR \biguplus PI \biguplus Prep \biguplus \ldots \rangle$$

Here,

- $Prep$ symbolises the *preparation* phase,
- DA symbolises the *attack detection and analysis* phase,
- IRsymbolises the *incident response* phase,
- PIsymbolises the *post-incident* phase,
- the symbol$\uplus$ denotes the sequence of operation and the$\uplus$ $Prep$ $\uplus$ ... indicates the feedback loop.

Within the scope of this article, we focus on theDA phase where the attack is detected and analysed. We can intuitively model this phase using the model of cyber attacks introduced in this article as follows:

$$DA \triangleq \langle \bigcup_{a \in ATTACK'} (detect \circledast analyse)^{a} \rangle$$

This essentially denotes that all attacks identified in this phase (denoted with $ATTACK' \subseteq ATTACK$) are required to be detected and analysed.

9. CONCLUSION

In this article we have presented a novel mathematical model of cyber attacks. Using this model, any cyber attack can be represented in a concise and intuitive way. The model encodes different essential properties of a cyber attack. For example, the model expresses the victim, the target entity for an attack, the channel and the layer used to launch the attack, the probable severity of the attack and the type of the attack. Then, we have introduced a novel attack taxonomy based on the motivations from the perspectives of attackers. We have also modelled each single identified attack using our model. Finally, we have showcased the applicability of the presented model in two scenarios.

The principle motivation of modelling cyber attacks according to our model is to prepare a solid foundation for a formal analysis of attacks within a system, organisation and network. Within this larger picture, modelling an attack is just one single component. The formal analysis will additionally need to consider how an attack can successfully exploitanyvulnerability, the threats associated with each attack and how such attacks can be mitigated. In this article, we have just shown how the incident handling mechanism can be modelled and how just one phase (attack detection and analysis) can be represented using our attack model. However, we have not explored the ways to model, represent and analyse other aspects of incident handling. The presented model can be utilised to model other aspects of incident handling. It will also be interesting to explore how the model can be combined with other existing attack formalising approaches which explore petri nets and attack trees.

REFERENCES

[1] Ben Quinn and Charles Arthur. “PlayStation Network hackers access data of 77 million users”. https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data. 26 April, 2011. Accessed: 14 February, 2017.

[2] Samuel Gibbs. “Ebay urges users to reset passwords after cyber attacks”.https://www.theguardian.com/technology/2014/may/21/ebay-urges-users-to-reset-passwords-after-cyber attacks. 21 May, 2014. Accessed: 14 February, 2017.

[3] Andrea Peterson. “The Sony Pictures hack, explained”.https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.7d8221627572. 18 December, 2014. Accessed: 14 February, 2017.

[4] KifLeswing. A massive cyber attacks knocked out major websites across the internet. http://uk.businessinsider.com/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10. 21 October, 2016. Accessed: 14 February, 2017.

[5] Cara McGoogan. “Yahoo hack: What you need to know about the biggest data breach in history”. http://www.telegraph.co.uk/technology/2016/12/15/yahoo-hack-need-know-biggest-data-breach-history/. 15 December, 2016. Accessed: 14 February, 2017.

[6] Simon Hansman and Ray Hunt. “A taxonomy of network and computer attacks”. Computers & Security, 24(1):31–43, 2005.

[7] Bonnie Zhu, Anthony Joseph, and Shankar Sastry. “A taxonomy of cyber attacks on SCADA systems”. In Internet of things (iThings/CPSCom), 2011, pages 380–388. IEEE, 2011.

[8] M Uma and GanapathiPadmavathi. “A survey on various cyber attacks and their classification”. IJ Network Security, 15(5):390–396, 2013.

[9] NazrulHoque, Monowar H Bhuyan, Ram CharanBaishya, DK Bhattacharyya, and Jugal K Kalita. “Network attacks: Taxonomy, tools and systems”. Journal ofNetwork and Computer Applications, 40:307–324, 2014.

[10] F MohdFoozy, Rabiah Ahmad, MF Abdollah, R Yusof, and MZ Mas'ud. “Generic taxonomy of social engineering attack”. 2011.

[11] Md Sadek Ferdous, Farida Chowdhury, and Md. Moniruzzaman. “A taxonomy of attack methods on peer-to-peer network”. In ICCIIS’ 07, p. 132–138. 2007.

[12] Md Sadek Ferdous, Raid Hussein, MadiniAlassafi, AbdulrahmanAlharthi, Robert Walters, and Gary Wills. “Threat taxonomy for Cloud of Things”. In Internetof Things and Big Data Analysis: Recent Trends and Challenges, volume 1, pages 149–191. United Scholars Publications, USA, 2016.

[13] Andrew P Moore, Robert J Ellison, and Richard C Linger. “Attack modeling for information security and survivability”. Technical report, DTIC Document, 2001.

[14] Steven Cheung, Ulf Lindqvist, and Martin W Fong. “Modeling multistep cyber attacks for scenario recognition”. In DARPA information survivability conferenceand exposition, 2003. Proceedings, volume 1, pages 284–292. IEEE, 2003.

[15] Thomas M Chen, Juan Carlos Sanchez-Aarnoutse, and John Buford. “Petri net modeling of cyber-physical attacks on smart grid”. IEEE Transactions on SmartGrid, 2(4):741–749, 2011.

[16] Md Sadek Ferdous, Gethin Norman, and Ron Poet. “Mathematical modelling of identity, identity management and other related topics”. In, SIN ’14, pages 9:9–9:16. ACM, 2014.

[17] Md Sadek Ferdous, Gethin Norman, AudunJøsang, and Ron Poet. “Mathematical modelling of trust issues in federated identity management”. In IFIP InternationalConference on Trust Management, pages 13–29. Springer International Publishing, 2015.

[18] Md Sadek Ferdous, Soumyadeb Chowdhury, and Joemon M Jose. “Privacy threat model in lifelogging”. In UBICOMP 2016, pages 576–581. ACM, 2016.

[19] M. S. Ferdous and R. Poet. “Formalising identity management protocols”. In 2016 14th Annual Conference on Privacy, Security and Trust (PST), pages 137–146.IEEE, Dec 2016.

[20] Terry Fleury, HimanshuKhurana, and Von Welch. “Towards a taxonomy of ‘attacks against energy control systems”. In International Conference on CriticalInfrastructure Protection, pages 71–85. Springer, 2008.

[21] “TCP/IP Protocol Architecture”. https://technet.microsoft.com/en-gb/library/cc958821.aspx. Accessed: 5 March, 2017.

[22] Bruce Schneier. “Secrets and lies: digital security in a networked world”. John Wiley & Sons, 2011.

[23] Markus Huber, Stewart Kowalski, Marcus Nohlberg, and Simon Tjoa. “Towards automating social engineering using social networking sites”. In CSE’09, volume 3, pages 117–124. 2009.

[24] Gregory L Orgill, Gordon W Romney, Michael G Bailey, and Paul M Orgill. “The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems”. In Proceedings of the 5th conference on Information technology education, pages 177–181. ACM, 2004.

[25] Tim Thornburgh. “Social engineering: the dark art”. In Proceedings of the 1st annual conference on Information security curriculum development, pages 133–135. ACM, 2004.

[26] EnkhboldNyamsuren and Ho-Jin Choi. “Preventing social engineering in ubiquitous environment”. In Future Generation Communication and Networking (FGCN2007), volume 2, pages 573–577. IEEE, 2007.

[27] Katharina Krombholz, HeidelindeHobel, Markus Huber, and Edgar Weippl. “Advanced social engineering attacks”. Journal of Information Security and applications, 22:113–122, 2015.

[28] Sarah Granger. “Social Engineering Fundamentals, Part I: Hacker Tactics”. https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics. December, 2001. Accessed: 7March, 2017.

[29] HananSandouka, Andrea J Cullen, and Ian Mann. “Social engineering detection using neural networks”. International ConferenceonCyberWorlds, 2009. CW’09. IEEE, 2009.

[30] DaneshIrani, Marco Balduzzi, DavideBalzarotti, EnginKirda, and Calton Pu. “Reverse social engineering attacks in online social networks”. In InternationalConference on Detection of Intrusions and Malware, and Vulnerability Assessment, pages 55–74. Springer, 2011.

[31] Lawrence Teo. “Port scans and ping sweeps explained”. Linux Journal, 2000(80es):2, 2000.

[32] Vladimir Gorodetski and Igor Kotenko. “Attacks against computer network: Formal grammar-based framework and simulation tool”. In International Workshopon Recent Advances in Intrusion Detection, pages 219–238. Springer, 2002.

[33] Ofir Arkin. “Network scanning techniques”. Publicom Communications Solutions, 1999.

[34] Marco De Vivo, Eddy Carrasco, Germinal Isern, and Gabriela O de Vivo. “A review of port scanning techniques”. ACM SIGCOMM Computer CommunicationReview, 29(2):41–48, 1999.

[35] Will Gragido. “Lions at the Watering Hole: The VOHO Affair”. http://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/. July, 2012.Accessed: 21 March, 2017.

[36] Steve Stasiukonis. “Social engineering, the USB way”. Dark Reading, 7, 2006.

[37] Colin Tankard. “Advanced persistent threats and how to monitor and deter them”. Network security, 2011(8):16–19, 2011.

[38] Ping Chen, LievenDesmet, and Christophe Huygens. “A study on advanced persistent threats”. In IFIP International Conference on Communications and Multimedia Security, pages 63–72. Springer, 2014.

[39] Joint Task Force Transformation Initiative et al. “Managing Information Security Risk: Organization, Mission, and Information System View”. 2011.

[40] Will Mitchell. “Password cracking”. http://web.cs.du.edu/~mitchell/forensics/information/pass_crack.html. Accessed: 21 Feb, 2017.

[41] Xin Sun, Ruben Torres, and Sanjay Rao. “DDoS attacks by subverting membership management in p2p systems”. In 3rd IEEE NPSec Workshop 2007, pages 1–6. IEEE, 2007.

[42] “CommonTypesof Network Attacks”. https://technet.microsoft.com/en-us/library/cc959354.aspx. Accessed: 21 March, 2017.

[43] Edward W Felten, Dirk Balfanz, Drew Dean, and Dan S Wallach. “Web spoofing: An internet con game”. Software World, 28(2):6–8, 1997.

[44] Matthew Tanase. “IP spoofing: an introduction”. Security Focus, 11, 2003.

[45] “Spoofing Attack: IP, DNS & ARP”. https://www.veracode.com/security/spoofing-attack. Accessed: 21 February, 2017.

[46] Martin Johns. “Session hijacking attacks”. Encyclopedia of Cryptography and Security, pages 1189–1190, 2011.

[47] MitjaKolšek. “Session fixation vulnerability in web-based applications”. Acros Security, 2002.

[48] Nick Nikiforakis, WannesMeert, Yves Younan, Martin Johns, and WouterJoosen. “Sessionshield: Lightweight protection against session hijacking”. In International Symposium on Engineering Secure Software and Systems, pages 87–100. Springer, 2011.

[49] “Session Hijacking Cheat Sheet”. http://resources.infosecinstitute.com/session-hijacking-cheat-sheet. January, 2015. Accessed: 15April, 2017.

[50] Shray Kapoor. “Session hijacking exploiting tcp, udp and http sessions”. www.infosecwriters.com/text_resources/pdf/SKapoor_SessionHijacking.pdf. 2006.

[51] Alberto Ornaghi and Marco Valleri. “Man in the middle attacks”. In Blackhat Conference Europe, 2003.

[52] Alex Kirshon, Dima Gonikman, and Gabi Nakibly. “Owning the routing table - new OSPF attacks”. BlackHat Briefings and Trainings USA+ 2011, pages1–18, 2011.

[53] Ola Nordström and ConstantinosDovrolis. “Beware of bgp attacks”. ACM SIGCOMM Computer Communication Review, 34(2):1–8, 2004.

[54] Crispan Cowan, Calton Pu, Dave Maier, Jonathan Walpole, Peat Bakke, Steve Beattie, Aaron Grier, Perry Wagle, Qian Zhang, and Heather Hinton. “Stackguard:automatic adaptive detection and prevention of buffer-overflow attacks”. In Usenix Security, volume 98, pages 63–78, 1998.

[55] Cowan, Crispin, F. Wagle, Calton Pu, Steve Beattie, and Jonathan Walpole. “Buffer overflows: Attacks and defenses for the vulnerability of the decade”. In DARPA Information Survivability Conference and Exposition, 2000. DISCEX'00. Proceedings, vol. 2, pp. 119-129. IEEE, 2000.

[56] Joyce K Reynolds. “The helminthiasis of the internet (rfc 1135)”, December 1989, 1989.

[57] “What is a Trojan Virus? – Definition”. https://usa.kaspersky.com/internet-security-center/threats/trojans#.WNwsIPnyvIU. Accessed: 17April, 2017.

[58] JelenaMirkovic, Sven Dietrich, David Dittrich, and Peter Reiher. “Internet denial of service: Attack and defense mechanisms” (radiaperlman computer networking and security). 2004.

[59] Christoph L Schuba, Ivan V Krsul, Markus G Kuhn, Eugene H Spafford, AurobindoSundaram, and Diego Zamboni. “Analysis of a denial of service attackontcp”. In Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on, pages 208–223. IEEE, 1997.

[60] Felix Lau, Stuart H Rubin, Michael H Smith, and LjiljanaTrajkovic. “Distributed denial of service attacks”. In IEEE International Conference on Systems, Man, and Cybernetics,pages 2275–2280. 2000.

[61] JelenaMirkovic, Janice Martin, and Peter Reiher. “A taxonomy of ddos attacks and ddosdefense mechanisms”. ACM SIGCOMM Computer Communication Review,34(2):39–53, 2004.

[62] David Bisson. “The 5 Most Significant DDoS Attacks of 2016”. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/5-significant-ddos-attacks-2016/. 29 November, 2016. Accessed: 17April, 2017.

[63] “How to Cover Your Tracks & Leave No Trace Behind on the Target System”. https://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-leave-no-trace-behind-target-system-0148123/. August, 2013. Accessed: 17April, 2017.

[64] NurulHidayah Ab Rahman and Kim-Kwang Raymond Choo. “A survey of information security incident handling in the cloud”. Computers & Security, 49:45–69,2015.

[65] Bernd Grobauer and Thomas Schreck. “Towards incident handling in the cloud: challenges and approaches”. In Proceedings of the 2010 ACM workshop on Cloudcomputing security workshop, pages 77–86. ACM, 2010.

Authors

Farida Chowdhury is an Assistant Professor at the department of Computer Science and Engineering of the Shahjalal University of Science & Technology, Bangladesh. She received her PhD degree at the Institute of Computing Science and Mathematics at the University of Stirling, Scotland. Her research interests focus on Network security, P2P networks, Pervasive computing, Next-Generation Wireless Networks, Wireless Sensor Networks, Internet of Things and Social Networks.

Md Sadek Ferdous is a Research Fellow at the Electronics and Computer Science of the University of Southampton. He holds a PhD in the area of Mobile Identity Management at the School of Computing Science of the University of Glasgow in 2015. His research interest includes Network Security, Distributed Ledger, Identity Management, Trust Management and Privacy Enhancing Technologies.