Network security – an updated perspective

Gulshan Kumar* and Krishan Kumar

Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India

(Received 21 October 2013; final version received 15 February 2014)

Network security is a specialized field consisting of the provisions and policies to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources as well as ensuring their availability through proper procedures. Many security devices are being developed and deployed to defend against cyber threats and to prevent unintended data breaches. In spite of all these efforts, the “golden age” of cyber crime continues, as organizations around the world continue to suffer data breaches and security attacks. What kinds of threats we are facing today? How these threats are to be dealt with? The goal of this paper is to communicate an updated perspective of network security for organizations, and researchers in the field and present some recommendations to tackle the current situation of security threats.

Keywords: cyber attacks; data breaches; intrusions; network security; security intelligence; security threats

1. Introduction

In the present era, there is an enormous growth of the Internet in terms of its usage and resources. Almost all major commercial organizations, educational institutes, governments and individuals are dependent upon the Internet for providing their services. Most of the commercial organizations exchange information with their collaborators and clients through the Internet. Educational institutes are uploading study materials and research findings over the Internet for the speedy propagation of the information. Governments provide information to the citizens through the Internet. Individuals use the Internet for accessing the information, online shopping and communicating with others through emails and social networking, etc. Thus, the Internet provides a platform to run the services and to store sensitive information of commercial organizations, educational institutes and governments. Internet also caters to the needs of individuals by providing appropriate information and a medium of communication. Therefore, smooth running of the Internet and maintaining integrity, availability and confidentiality of the sensitive information over the Internet are the most important aspects of the growth of the information-based organizations (Kumar, Kumar, & Sachdeva, 2010a).

However, presence of configuration errors and vulnerabilities in the most popular softwares provide numerous chances for malicious users to mount a variety of attacks to disrupt services and integrity of sensitive information over the Internet called cyber attacks. A cyber attack is a deliberate exploitation of computer systems, technology-dependent networks and enterprises (Kim, Kim, & Park, 2014). The cyber attacks use malicious code to alter computer code, logic or data resulting in destructive consequences, that can compromise information security. Zero-day (unknown) vulnerabilities are potentially more harmful, associated with newly published program or web services (Schneider, 2012). Such vulnerabilities may be visible for days or weeks until patched and offers more chances for attackers to exploit them. For example, most infections today occur through “exploit kits,” “infecting users” computers through a vulnerability without their knowledge. For example, more than 90% of these are through Java vulnerabilities in browsers (PandaLabs, 2013). The recent attacks on Microsoft, Apple, Facebook and Twitter used Java. Most “Police Virus” infections managed to reach victims’ computers due to outdated versions of Java. Network, server and client mis-configuration offers another avenue for hacking. Network elements, such as routers and home gateways, come with a default administrator password, passwords that often never change. Hackers with access to a router can cause all traffic through it to be sent through their own servers, allowing “man in the middle” attacks. Similarly, misconfigured servers can allow hackers to disable or modify websites, inserting code of their own choosing. Such code is usually intended to steal data from associated databases.

In the present scenario, network security devices consist of one or more security functions, including firewall, intrusion prevention/detection systems (IPS/IDS), data loss prevention (DLP) and content security filtering functions —

*Corresponding author. Email: gulshanahuja@gmail.com

© 2014 The Author(s). Published by Taylor & Francis.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The moral rights of the named author(s) have been asserted.
e.g. anti-spam, antivirus or URL filtering (Schneider, 2012). Anyone who works in security knows that nothing is 100% secure (PandaLabs, 2013). No doubt, a number of preventative measures may work well most of the time. Yet there will always be weak points, a new vulnerability, human errors, etc. which may finally facilitate one of the thousands of attacks to which these companies/individuals are constantly subjected.

This new war of advanced threats and attacks will remain to continue (Schneider, 2012). As sensitive information about various organizations stored in data centers, servers, PCs and mobile phones is ever increasing. The list of security threats is also increasing with new kinds of more advanced and complicated attacks. Emerging trends – including cloud computing, user mobility and BYOD – have further complicated matters, increasing the attack surface while diminishing the effectiveness of traditional perimeter defenses (Potts, 2012). Nowadays, the industry faces the challenges of fast changing trends of attacking the Internet resources, inability of conventional techniques to protect the Internet resources from a variety of attacks, and biases of individual techniques toward specific attack class(es). Developing effective techniques, security policies and enforcing them are necessary for securing valuable Internet resources from attacks.

This paper provides an analysis of recent network security events and today’s most prominent attacks that occurred in organizations worldwide, with examples of published incidents, followed by recommendations on how to protect against such assaults. It describes how security risk will evolve in the near future. Finally, it concludes that only the concept of security intelligence along with user training can defend these cyber threats.

2. Security threats

The dependence of the information-based organizations and individuals over the Internet is increasing day by day. However, most of the popular softwares contain vulnerabilities and configuration errors which are not only technically difficult, but also economically costly to be solved. These vulnerabilities and easy access to Internet resources are exploited by the intruders to misuse the Internet resources and launch influential attacks against them (Kumar et al., 2010a; Ramamohanarao et al., 2007; Schneider, 2012) such as the Denial of Service (DoS) (Peng, Leckie, & Ramamohanarao, 2007; Sachdeva, Kumar, Singh, & Singh, 2009) and Information attacks (Patcha & Park, 2007). The sheer volume of vulnerabilities revealed every year is overwhelming (as depicted in Figure 1), as more than 5000 new ways for hackers to cause damage and access systems were discovered in 2012 alone (Checkpoint, 2013). Figure 2 demonstrates that the most popular products used by organizations were also the most susceptible to cyber attacks. Oracle, Apple and Microsoft were the most vulnerable system vendors in 2012. Research at Check point software technologies show that 75% of hosts in organizations were not using the latest software versions (e.g. Acrobat Reader, Flash Player, Internet Explorer, Java Runtime Environment, etc.) (CheckPoint, 2013). This means that these hosts were exposed to a wide range of vulnerabilities that could have been exploited by hackers. Their research also shows that 44% of hosts in organizations were not running the latest Microsoft Windows Service Packs. Service packs usually include security updates for the operating system. Not running the latest versions increases security risk.

It is also highlighted by Panda labs in their annual report of the year 2012 that over the last few years, the number of Trojans in circulation has been constantly increasing (as depicted in Figure 3) (PandaLabs, 2012). In 2010, they accounted for more than half of all Malware created (56%), in 2011 they rose spectacularly to 73.31%, whereas in 2012
they reached 76.57%. Worms came second (11.33% compared with 8.13% in 2011), whereas viruses dropped to third place at 9.67% compared with 14.24% in 2011. It is observed that Trojans dominated the ranking at 76.56% of infecting the computers. It seems that cyber-crooks have managed to infect more computers with Trojans this year than in previous years. In 2011, the percentage of Trojan infected computers were 66.18%, so there has been a 10 point rise in this respect. One of the reasons for this growth is the increased use of exploit kits such as black hole, which are capable of exploiting multiple system vulnerabilities to infect computers automatically without user intervention. In addition to these factors, availability of free user friendly attack tools like Stacheldraht, Tribe, Trinoo, Mstream, etc. over the Internet made cyber attacks even simpler and easier. Lastly, the “Facebook phenomenon” and our passion with mobile devices have increased the attack surface available for cyber crooks to exploit (Potts, 2012). Today, everyone is on Facebook, from tweens to grandparents. As the number of mobile-connected devices has exceeded the number of people on earth by the year 2012. Consequently, the number of the attack incidents over the Internet is increasing day by day, as large scale and diverse nature of data breaches and other network attacks took center stage (Cert, 2012; Verizon, 2013). Motives for these cyber crimes appear equally diverse like (Kumar et al., 2010a; Schneider, 2012; Verizon, 2013):

- **Theft of data**: It consists of not only financial data, such as credit card numbers, passwords but also customer lists, intellectual property, and product development and marketing plans.
- **Loss of time**: It takes a great deal of time to recover from an attack, or even from the suspicion of an attack. Data may need to be recovered, or reconstructed and systems may need to be checked extensively.
- **Monetary loss**: This is often preceded by the theft of data.
- **Disabled or crippled services**: Protesters and some agencies may seek to disable offending websites. Hackers may be purely malicious in their intent.
- **Legal exposure**: Any of the previous items may expose an enterprise to lawsuits for loss of data or money entrusted to them.

It is observed that out of total data breaches occurred in 2012 worldwide, 37% of breaches are of financial organizations, 24% of breaches of retail environments and restaurants, 20% of network intrusions involved manufacturing, transportation, and utilities, and 20% of network intrusions hit information and professional services firms (Verizon, 2013). Cyber crooks performed these data breaches by using various tricks such as hacking, stolen credentials, installing Malware, physically attacking the systems, etc. It is reported by the Verizon in their annual report of 2013, 52% of breaches occurred in 2012 used some form of hacking, 76% of network intrusions exploited weak or stolen credentials, 40% incorporated Malware, 35% involved physical attacks, 29% leveraged social tactics and 13% resulted from privilege misuse and abuse (Verizon, 2013).

Cyber crooks used various methods of attack to gain entry into the system network. These are referred to as attack vectors. Figure 4 lists some of the more prevalent attack vectors, with the corresponding percentage of organizations that suffered from them. Memory corruption, buffer overflow and DoS topped the list of most popular attack vectors (CheckPoint, 2013). Traditionally, these security attacks and their risk is being classified into worms, virus,
Advanced persistent threats (APT): APT also known as targeted attacks are the most sophisticated and long-term attacks that work toward a specific pre-determined goal. APTs are unlikely to be detected by traditional security systems, placing governments, enterprises, small businesses and even personal networks at risk. In a survey conducted by the Ponemon Institute, 83% of IT and security practitioners said they believed their organizations had been the target of advanced threats (Goodchild, 2010). Some of the more prominently discussed APTs include Operation Aurora and Operation Shady remote access Trojan (RAT). In APT attacks, the typical first action is to perform reconnaissance to gather intelligence on the target system (CheckPoint, 2013). Then attackers make an initial intrusion into the target’s network to open a back door which allows them to persistently remain in the network. This is usually accomplished by infecting a host with a bot which allows the attacker to communicate with the infected host without being detected. The attacker then strives to gain further access into the network and compromise even more nodes. After reaching the target, the attacker can further exploit the infected host to collect data or cause damage remotely while remaining undisclosed indefinitely. APTs are extremely personal, targeted and backed by high levels of motivation. Motives behind APTs include:

- stealing trade secrets or government information for competitive advantage, espionage or warfare,
- infiltrate and controlling critical systems,
- making a political statement as in the case of hacktivists through Distributed Denial of Service (DDoS) attacks and/or data theft,
- unauthorized bank and credit card transactions,
- advance fees, as in the Nigerian scam (now originating from many countries) that requests money to cover the transfer of millions of “unclaimed” funds and
- product sales from scareware and web-based enticements.

Highly sophisticated Malware designed for APTs are Stuxnet, Duqu, Flame and Red October (Virvilis & Gritzalis, 2013). There is no question on the capability and effectiveness of these threats as Stuxnet has appeared to have slow down Iran’s nuclear program for four years. While other ones have operated silently for a long time, stealing a huge amount of information from sensitive environments. A number of such attack incidents occurred in the recent past. Some of such incidents are as described below:

**South African Postbank scam:** The first mayor cyber crime of 2012 took place in South Africa, as hackers got away with about $6.7 million from South African Postbank (PandaLabs, 2012). The robbery took place over three days, from 1 January to 3 January. The hackers, who had planned the attack for months, used stolen login details from a Postbank teller to transfer the stolen money into multiple bank accounts that were opened across the country.

**Police Virus Scam:** One of top threats in 2012 has undoubtedly been a new Malware that infected hundreds of thousands of computers around the world using fear and blackmailling techniques to extort money from computer users (PandaLabs, 2012).

**Social networks-based attacks:** Facebook continues its reign as the number one social networking site but it is also a favorite target of cyber crooks. In January 2012, a worm was discovered that had stolen over 45,000 Facebook login credentials (PandaLabs, 2012). Researchers fear that the criminals used these “infected” accounts to send links to people’s Facebook friends, spreading the computer worm further.

Social networking site LinkedIn had 6.5 million user passwords stolen and leaked online. Fortunately enough, however, these passwords were not stored in plain text files, but were encrypted.

In March 2012, it was revealed that Michael Jackson’s entire back catalogue had been stolen from Sony Music, including some previously unreleased material. This follows last year’s attacks on Sony that exposed personal data from more than 100 million accounts at Sony Online Entertainment and the PlayStation Network.

Nissan Motor Company fell victim to a breach of employee information. The attackers compromised user IDs and passwords, which seems to indicate that the Malware was designed for industrial espionage.

In September 2012, it was revealed that Adobe had also been attacked by hackers. In this case, the attackers were not interested in stealing customer data, but in accessing one of the company’s internal servers to be able to sign their Malware with a valid digital certificate from Adobe.

**Eurograbber attack:** It is a sophisticated multi dimensional attack took place in 2012 stealing an estimated 36+ million Euros from more than 30,000 bank customers in multiple banks across Europe (CheckPoint, 2013). Entirely transparent to users, online banking customers had no idea that they were infected with trojans, that their online banking sessions were being compromised, or that the funds were stolen directly out of their accounts. Once the Eurograbber...
trojans were installed on both devices, the bank customers’ online banking sessions were completely monitored and manipulated by the attackers. Even the two-factor authentication mechanism used by banks to ensure online banking security was circumvented and was actually used by the assailants to authenticate their illicit financial transfers. Further, the Trojans used to attack mobile devices were developed for both the Blackberry and Android platforms in order to attack a wider range of victims.

Insiders’ attacks: It is observed that insiders were responsible for 48% of data breaches in 2009, and of that percentage, 90% were the result of deliberate and malicious activity (Verizon, 2012). Insider threats originate from within an organization as opposed to coming from an outside perpetrator. Often the attacker has been a trusted entity – employee, contractor, partner, etc. – who has been granted access to the internal network. Methods used to conduct insider threats vary widely, but intentions are mostly malicious, often involving the theft of valuable information to make a profit. Since they occur within the network and by privileged users, insider attacks are not easily thwarted by traditional security measures, which are geared towards detecting attacks from the outside. By far the most high-profile insider attack in recent history is the WikiLeaks/Bradley Manning affair. Unfortunately, the insider threat will continue to grow as a concern over the next few years.

However, data leakage is not always caused by cyber criminals (Checkpoint, 2013). It can happen unintentionally by the actions of well intentioned employees. A classified document may be mistakenly sent to the wrong person, a sensitive Document might be shared. On a public site or a work file may be sent to an unauthorized home email account. These scenarios may inadvertently happen to anybody, with devastating results. Loss of sensitive data can lead to brand damage, compliance violations, lost revenue or even hefty fines.

Many incidents of attacks from insiders occurred in the recent past. Some of major incidents are:

In April 2012, Texas A&M University unintentionally sent an email with an attachment containing 4000 former students’ social security numbers, names and addresses to an individual who subsequently notified the university of the mistake (PandaLabs, 2013).

In October 2012, in the UK Stoke-on-Trent City Council was fined 120,000 after a member of its legal department sent emails containing sensitive information to the wrong address (PandaLabs, 2013). Eleven emails intended for a lawyer working on a case were sent to another email address due to a typing mistake.

Japan’s newspaper Yomiuri Shimbun fired one of its reporters in October 2012 for accidentally sending sensitive investigative information to the wrong recipients (PandaLabs, 2013). The reporter meant to send some of his research findings to his colleagues via email, but instead, he sent the messages to several media outlets, disclosing the identities of his sources.

Employees misuse or abuse attacks: With over 900 million users on Facebook, and nearly 75% of companies currently allowing employee-owned smart phones and/or tablets to be used at work, employee misuse and abuse is a problem that is not going away anytime soon (Potts, 2012). If employees feel that their organization’s policies are restricting their access to resources that they need to be happy in the workplace, they will often try to cheat the system. The new rise in BYOD environments is further complicating this issue, making it difficult for IT administrators to properly secure every new device that enters the network.

Fully automated attacks: Although they are still in use, “driveby” automated attacks, or traditional viruses and worms, have definitely been trending down over recent years, and will continue to do so (Potts, 2012). Automated attacks are designed and set loose by the attacker with the hope that the Malware will propagate automatically with little to no direct management by the author. The author’s primary interest is in notoriety rather than financial gain, similar to the motivation behind defacement of a train carriage or highway overpass. Automated attacks are the easiest type of attack to defend against, as they are indiscriminate, loud and easily detected with conventional security technologies. The primary concern with automated, indiscriminate attacks is business downtime and loss of worker productivity. A good example of a traditional worm is SQL Slammer, which did little but congest servers and wreak havoc on the Internet.

Social networking and other vulnerabilities: The increasing use of social media presents a real security threat to any company or institution (Conrad, 2012). It is nearly impossible to keep employees from disclosing company information via channels such as Facebook, Twitter or online forums. Even a seemingly innocuous remark, like: “We surprised the boss for his birthday today” can potentially provide valuable information to a hacker (a birthdate, for example, can be used to crack a password or for social engineering). Recent attacks indicate that hackers are shifting from regular emails to social networks as their preferred Malware distribution channel. For example, in August 2012, hackers used Twitter and Facebook social engineering techniques to distribute Malware (Checkpoint, 2013). Using a compromised Twitter account, the hacker sent the following message to all of the account’s followers. “Exactly what were you doing inside this film (Facebook – URL) wow disturbing.” The URL pointed to a Facebook app which required “Twitter Login.” The login screen was actually a web server owned by the hacker that was used to harvest the recipient’s Twitter credentials. The hacker can repeat the process by using the newly hacked Twitter accounts to steal even more passwords. The hacker can also use the stolen credentials to access other services.
such as Gmail, Facebook, etc. Even worse, stolen personal credentials can be used to log into bank accounts or business-related services such as salesForce.

User-involved attacks: Innocent computer users are involved in most security breaches. The most frequent methods include (Schneider, 2012):

- **Email**: In addition to spam, emails can contain attachments that are malicious executable programs or links to infected websites. This is currently the primary initial infection vector used to compromise computers that have Internet access. The emails are often part of phishing campaigns, using social engineering tricks to lure victims to infected sites. And these campaigns are frequently targeted at specific industries.
- **Web**: Those same client-side vulnerabilities are exploited by attackers when users visit infected websites. Simply accessing an infected website is all that is needed to compromise the client software programs.
- **Instant messaging (IM)**: IM programs now provide mechanisms for passing executable programs and web links, providing a means of infecting computers and revealing information.
- **Peer-to-peer (P2P)**: P2P environments are often used to share software, which may be similarly infected.
- **Gaming**: Social interaction with other players may invite email or IM communications.
- **Software updates**: Software vendors are increasingly updating their software over the Internet, using web pages or dedicated, resident programs. Malicious parties may substitute their own software, or infect the updates before they are downloaded.

**DoS attacks**: DoS and DDoS attacks are the oldest methods of disabling IP networks. While those methods are well known and have been studied for years, they continue to remain one of the most effective ways to impact the performance of IP networks or services, or completely restrict or prohibit access to a network, service or application for legitimate users. By definition, the intent of a DoS/DDoS attack is to partially restrict or completely deny access of legitimate users to resources provided by a victim’s network, computer or service. When this attempt is initiated from a single host, the attack is called a DoS attack. Although DoS attacks can be successfully mounted using a single host with limited resources, the majority of the attacks requires a group of malicious hosts that flood the victim’s network with an overwhelming amount of attack packets.

3. **Future trends**

We have seen what has happened in the recent past: Malware creation records the highest number of Trojans ever, attacks in social networks, cyber crime and cyber war everywhere. What do we have to expect for the near future?

Nowadays, cyber threat is no longer a threat, it is a daily reality. These threats continue to grow. They must be understood for addressing them so that tenets of information security are adhered. The important tenets of information security includes confidentiality, integrity and availability (Kumar et al., 2010a). By understating the motivation behind various cyber attacks, we can more clearly present the future trends of cyber attacks. The cyber attacks can be broadly classified into four categories described as below (depicted in Figure 5) (Hilbert, 2013):

**1) Cyber crime**:

The cyber crimes in the near future are enriched with the terms like cyber fraud, stealing, phishing and other malicious behaviors. Generally, cyber crimes refer to the malicious activities to block, read or interfere with cyber services. Multiple information security tenets including confidentiality, integrity and availability may be compromised during this type of cyber attack. Here, the motivations of cyber criminals include gaining economic benefit, compromising cyber infrastructure (e.g. in cyber warfare) and self satisfaction. The cyber criminals use stolen identity of victims, perform online extortion, spamming, phishing, etc. as attack vectors to commit cyber crimes. Most of cyber crimes committed in the real world are committed through online computers. Generally, the aim of cyber criminals is to gain access of victims’ computers, online resources and credentials. Once they gain access to victims’ resources by any means, then compromised resources can be used to perform any malicious activity. For example, booming e-commerce or online business lures cyber criminals. Cyber criminals can use Malware tools to commit economic crimes, such as stealing credit cards and social security numbers, and electronic money. Flaws in the software used for e-commerce or online services provide numerous chances for cyber crimes in the economy.

Cyber crimes go on daily in the real world and will continue to take place because of huge profits behind them and the availability of cyber tools to commit these crimes.

**2) Cyber espionage**:

The cyber espionage involves stealing the information. The information can be stolen by the cyber criminals to gain access to a computer system or
network. Here, cyber criminals may disturb confidentiality and integrity of the information of the systems. Generally, criminals work for a long time to gain control or access of the system and viewing the online information and other security policies in place. These criminals are generally technically sound people and are difficult to be detected. The attack vector in this category of cyber attack are not so simple. The attack method can be to target the employee of the organization, spreading of Malware designed for specific activities, and exploiting BYOD policy of the organization. Some of the important methods of performing such attacks are as described below:

**APT:** We learnt from the recent network security scenario that there are targeted, highly motivated attackers (Potts, 2012). It is expected to see the high-profile attacks continue in the future. While the APT will remain number one.

**Growth of Malware:** For two decades, the amount of Malware has been growing dramatically (PandaLabs, 2012). The figures are stratospheric, with tens of thousands of new Malware strains appearing everyday and therefore, this sustained growth seems very far from coming to an end. Despite security forces being better prepared to combat this type of crime, they are still handicapped by the absence of borders on the Internet. A police force can only act within its jurisdiction, whereas a cyber crook can launch an attack from country A, steal data from citizens of country B, send the stolen data to a server situated in country C and could be living in country D. This can be done in just a few clicks, whereas coordinated action of security forces across various countries could take months. For this reason, cyber criminals are still living their own golden era.

**Malware for Mac:** Cases like Flashback, which occurred in the recent past, have demonstrated that not only is Mac susceptible to Malware attacks but that there are also massive infections affecting hundreds of thousands of users (PandaLabs, 2012). Although the number of Malware strains for Mac is still relatively low compared with Malware for PCs, we expect it to continue to rise. A growing number of users added to security flaws and lack of user awareness (due to over-confidence), mean that the attraction of this platform for cyber crooks will continue to increase next year.

**Mobile Phone Malware:** As an Android’s market share continues to grow, the motivation for cyber crooks to target the platform also increases (PandaLabs, 2012). In September 2012, Google announced that it had reached the incredible figure of 700 million Android activations. Although it is mainly used on Smartphones and tablets. Its flexibility and the fact that you do not have to buy a license to use it are going to result in new devices opting to use Google’s operating system. Its use is going to become increasingly widespread, from televisions to all types of home appliances, which opens up a world of possible attacks as yet unknown.

In fact, we learned that Google, tired of the malicious apps found in Play Store, has started analysing apps before putting them in their catalog in order to detect anomalous behavior (PandaLabs, 2012). According to their own sources, they have managed to reduce malicious app downloads by 40%. Unfortunately, despite these efforts, criminals continued to target the Android mobile platform through apps not always accessible through Play Store. This was the case of Bmaster, a RAT on the Android platform that tried to pass itself off as a legitimate application. We also saw Trojans exclusively designed to steal data from infected devices: from call and text message records to users’ contact lists. Android is potentially exposed to far more security risks than its biggest competitor (iPhone and its iOS), as it allows users to get their apps from anywhere. However, using the official Android marketplace is no security guarantee either, as it has also been targeted by cyber crooks luring users into installing Trojans disguised as legitimate apps. Something which, by the way, has also happened to Apple’s App Store, but to a lesser extent than in Google’s Play Store.

It is shown in reports of security experts that no company is immune to cyber espionage attacks (Hilbert, 2013). Sensitive information of companies is shared in some way to others, so it need to be protected from cyber espionage attacks.

3) Cyber warfare:

Cyber warfare is aimed to disable or destroy the computer systems. Generally, a cyber-based program known as cyber weapon is developed to target the system. This type of attack disrupts the availability, and/or integrity of the system. The motive behind these attacks can be diverse. These attacks can be carried out by governments, military or other technically sound people who want to be famous in the world.

Software vulnerabilities remain the main target of cyber criminals as per previous practices (PandaLabs, 2012). It is undoubtedly the preferred method of infection for compromising systems transparently, used by both cyber criminals and intelligence agencies in countries around the world. In 2012, Java, which is installed on hundreds of millions of devices, was repeatedly compromised.
Table 1. Cyber attacks and information security tenets.

| Security tenet/attack type | Cyber crime | Cyber espionage | Cyber warfare | Cyber activism |
|----------------------------|-------------|-----------------|---------------|---------------|
| Confidentially             | ✓           | ✓               |               |               |
| Integrity                  | ✓           | ✓               | ✓             | ✓             |
| Availability               | ✓           |                 |               |               |

and used to actively infect millions of users. Adobe is at the second place for containing vulnerabilities in its most popular applications (like Acrobat Reader, Flash, etc.). Because of their multiple security flaws, it is one of the favorite tools for massively infecting users as well as for targeted attacks. Although we may think that home users are exposed to the highest risk, remember that updating applications, which is essential for protecting against these types of attacks, is a very complex process in companies, where updating all computers must be coordinated. At the same time, it is essential to ensure that all the applications used in a company work correctly. This makes the update processes slow, which opens a window that is exploited to steal information in general and launch targeted attacks in search of confidential data.

Numerous incidents of attacks in this category have taken place in recent years. It ranges from the Russian invasion of Georgia (2008) to the employment of Stuxnet (the computer worm which disrupted Iranian nuclear enrichment in 2010), is the first instance of a computer network attack known to cause physical damage across international boundaries), Duqu (a targeted Malware detected in September 2011), and Flame (a targeted information stealing Malware detected in May 2012), the hacking of Tibetan exiles by GhostNet to the international cyber espionage ring known as shadow networks (Shakarian, Shakarian, & Ruef, 2013). Today, cyber war has moved to the forefront of many national agendas.

4. Cyber activism:
Cyber activism is the newest class of cyber crime. It is a way of using Internet-based socializing and communication techniques to create, operate and manage activism of any type. It uses social networking tools and platforms to share and broadcast mottos and messages, and to interact with netizens. These platforms include Twitter, Facebook, LinkedIn, YouTube and other popular and niche social networks, along with email, IM and other online collaboration tools.

The e-activists use social engineering techniques for sharing information (PandaLabs, 2012). Tricking users into collaborating to infect their computers and steal their data are an easy task, as there are no security applications to protect users from themselves. In this context, use of social networks (Facebook, Twitter, etc.) where hundreds of millions of users exchange information, on many occasions personal data, makes them the preferred hunting ground for tricking users. Particular attention should be paid for Skype, which after replacing Messenger, could become a target for cyber criminals.

Depending on the cause or need of the e-activist, cyber activism can be used for various purposes, such as awareness creation, gathering and organizing followers and initiating reactions. For example, e-activists use e-petitions digitally signed by a number of followers before they are sent to government and legislative authorities. But, for malicious users and technically sound people it is not enough. They protest their companies, redirect a huge amount of traffic to the company website (DoS attack), make a large number of request to company server to fail them, extract personal information of company’s administrators to embarrass them and access company policies to damage company reputation and much more. The integrity of information is compromised in this type of attack (Hilbert, 2013).

Table 1 summarizes the various cyber attacks and information security tenets that may be compromised.

4. Recommendations
Network security is vital in order to prevent financial loss, protect customers and limit brand damage. Malware threats and security breaching tactics are continuing to grow, multiply and evolve (Schneider, 2012). We can no longer just buy various tools to protect each mechanism of launching an attack – anti-virus, anti-spam, anti-phishing, etc. (Potts, 2012). Today, we must instead think about the various forms of attack in terms of the motivation behind them to determine how best to protect our assets. We must move away from thinking that technologies that block attacks at the perimeter, or use signatures to detect Malware, are enough to keep us safe.

In the present scenario, technology alone is not enough to provide security to our valuable Internet resources. There is unfortunately no single, silver bullet solution to ensure safety from all potential threats (Denman, 2012). But by integrating multi-layered security throughout the network, you can at least stand a good chance of identifying and
isolating attacks before they spread. Combine this with powerful intrusion prevention, protocol and behavior analysis, application control, vulnerability management and all the other defenses found in some next-generation firewalls, and we will greatly reduce your exposure to such threats. Of course, these layers of protection are only effective when enabled, so if we own such a device, our most important task today could be to double check that every protection layer is enabled. We need to harmonize various layers of protection to fight against potential security threats.

It is evident that the use of best practices would have significantly raised the bar on attackers and limited the impact of the Malware (Virvilis & Gritzalis, 2013). However, it appears that even in a sensitive environment a small subset of protection mechanism was implemented. Even, current antivirus and IDSs are lacking in the detection of APTs. Detection techniques process a huge amount of audit data containing non-relevant and redundant features leading to extra computational overhead. The extra computational overhead leads to loss of real-time capability of IDSs. Employment of appropriate feature selection techniques along with AI-based techniques may reduce computational overhead (Kumar & Kumar, 2011, 2012; Kumar, et al., 2010a; Kumar, Kumar, & Sachdeva, 2010b).

So, there is an acute need to consider architecture of IDSs and their detection techniques.

In order to avoid increasing data losses due to insiders’ attacks, it is recommended to implement an automated corporate policy that catches such incidents before the data leaves the organization. Such solutions are called Data Loss Prevention (DLP). Content-aware DLP products have a broad set of capabilities and present organizations with multiple deployment options. Before deploying the DLP solution, organizations need to develop a clear DLP strategy with concrete requirements such as: What is considered to be confidential information? Who can send it? and so forth.

In a nutshell, we need to take care of the security policy and users. A security policy meeting the requirements of the concerned organization must be well defined to prevent cyber attacks. The policy must clearly state the ways for doing various operations in a secure manner. Special care must be taken to protect networks against operating system and application vulnerabilities. The users must be involved in the security of the concerned organizations. As they are responsible for using and sharing sensitive data of organizations. They must be provided training regarding various threats to their organizations and how their precautions can help to prevent the attacks. They must be aware of the technologies and latest trends of conducting cyber attacks. They must be aware of the security policy and must adhere to it. Organizations must ensure enforcement of security policy to prevent real security threats.

We believe there must be a change of focus in providing security from proprietary products to an integrated approach comprising latest multiple techniques along with proper education to the users.

5. Conclusions

The present time itself is full of challenges in the world of network security. Everything seems to indicate that the number of threats that users will have to face will continue to grow, so now more than ever protection is essential: having a good security policy, keeping security products (like antivirus, antis oppress) up to date, using common sense, educating the users, and enforcing the security policy are the best ways to avoid falling victim to the powerful social engineering ploys and tricks used by cybercrooks (PandaLabs, 2012).

Nevertheless, apart from all these attacks, there has also been good news in the fight against cybercrime: Interpol has announced they are planning to open a “Global Cybercrime Center” in Singapore in 2014 to improve global cooperation among law enforcement.

References

Cert (2012). Cert/cc statistics. http://www.cert.org/stats/
CheckPoint (2013). Check point 2013 security report January (2013). Retrieved September 23, 2013, from http://www.checkpoint.com/campaigns/security-report/
Conrad, J. (2012). Seeking help: The important role of ethical hackers. Network Security, 5, 5–8.
Dennman, S. (2012). Why multi-layered security is still the best defence. Network Security, 3, 5–7.
Goodchild, J. (2010). Study: Advanced threats a growing problem for security. PCWorld 30 June 2010. Retrieved September 23, 2013, from www.pcmag.com/businesscenter/article/200243/study advanced threats a growing problem for security.html
Hilbert, E. (2013). Living with cybercrime. Network Security, 11, 15–17.
Kim, Y., Kim, I., & Park, N. (2014). Analysis of cyber attacks and security intelligence. In James J. (Jong Hyuk) Park, H. Adeli, N. Park & I. Woungang (Eds.), Mobile, ubiquitous, and intelligent computing, Lecture Notes in Electrical Engineering, Vol. 274 (pp. 489–494). Berlin, Heidelberg: Springer.
Kumar, G., & Kumar, K. (2011). The need for an information theoretic aproach for feature selection. Security and Communication Networks, 5(2), 178–185. doi:10.1002/sec.303
Kumar, G., Kumar, K., & Sachdeva, M. (2010a). The use of artificial intelligence based techniques for intrusion detection: A review. Artificial Intelligence Review, 34(4), 369–387.
Kumar, G., Kumar, K., & Sachdeva, M. (2010b). An empirical comparative analysis of feature reduction methods for intrusion detection. International Journal of Information and Telecommunication Technology, 1(1), 44–51.
PandaLabs (2012). 2012 annual report pandalabs. Retrieved September 23, 2013, form http://press.pandasecurity.com/wp-content/uploads/2013/02/PandaLabs-Annual-Report-2012.pdf
PandaLabs (2013). Pandalabs quarterly report January – March 2013. Retrieved September 23, 2013, form http://press.pandasecurity.com/wp-content/uploads/2010/05/Pandalabs-Quarterly-Report.pdf
Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks, 51*(12), 3448–3470. doi:10.1016/j.comnet.2007.02.001

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, 39(1), Article 3. doi:10.1145/1216370.1216373

Potts, M. (2012). The state of information security. *Network Security, 2012*(7), 9–11.

Ramamohanarao, K., Gupta, K., Peng, T., & Leckie, C. (2007, December 16–20). The curse of ease of access to the internet. In P. McDaniel & S. K. Gupta (Eds.), *Information Systems Security, Third International Conference, ICISS 2007 Proceedings*, Delhi (pp. 234–249). Berlin Heidelberg: Springer.

Sachdeva, M., Kumar, K., Singh, G., & Singh, K. (2009, March 6–7). Performance analysis of web service under ddos attacks. *Proceedings of International Advance Computing Conference (IACC)*, Patiala, India (pp. 1002–1007). New York: IEEE.

Schneider, D. (2012). The state of network security. *Network Security, 2012*(2), 14–20.

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach*. Maryland Heights: Syngress Publishing.

Verizon (2012). The 2012 data breach investigations report. Retrieved September 23, 2013, from www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Verizon (2013). The 2013 data breach investigations report. Retrieved September 23, 2013, from www.verizonenterprise.com/resources/reports/rp_data-_breach-investigations-repor t-2013_en_xg.pdf

Virvilis, N., & Gritzalis, D. (2013, September 2–6). The big four—what we did wrong in advanced persistent threat detection? *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, Regensburg (pp. 248–254). New York: IEEE.