SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2012; **5**:422–437
Published online 13 July 2011 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.331

REVIEW ARTICLE

A survey of cyber crimes

Yanping Zhang[1], Yang Xiao[1]*, Kaveh Ghaboosi[2], Jingyuan Zhang[1] and Hongmei Deng[3]

[1] Department of Computer Science, The University of Alabama, 101 Houser Hall, Tuscaloosa, AL 35487–0290, U.S.A.
[2] Centre for Wireless Communications, University of Oulu, Finland
[3] Intelligent Automation, Inc., 15400 Calhoun Drive, Suite 400, Rockville, MD 20855, U.S.A.

ABSTRACT

With the advancement of computer and information technology, cyber crime is now becoming one of the most significant challenges facing law enforcement organizations. Cyber crimes are generally referred as criminal activities that use computers or networks. An understanding of the characteristics and nature of cyber crimes is important in helping research communities find ways to effectively prevent them. Most existing research focuses more on attacks and attack models, including either actual attacks or imaginary/possible attacks over all layers of networks or computers, but there has been less work carried out on a comprehensive survey of cyber crimes. This paper provides a survey of cyber crimes that have actually occurred. First, cyber crimes in the digital world are compared with crimes in the physical world. Then, cyber crimes are categorized according to the roles of computers or networks. Furthermore, we also notice that some cyber crimes are actually traditionally non-cyber crimes that are facilitated by computers or networks. It is surprising that there are so many recurrent cyber crimes. More efforts are needed to protect people from cyber crimes.

KEYWORDS
MAC security; IDS; forensics

***Correspondence**
Prof. Yang Xiao, Department of Computer Science, The University of Alabama, 101 Houser Hall, Tuscaloosa, AL 35487–0290, U.S.A.
E-mail: yangxiao@ieee.org

1. INTRODUCTION

With the advancement of computer and information technology, cyber crime is now becoming one of the most significant challenges facing law enforcement organizations. The most important difference between a cyber crime and a physical crime is that a cyber crime always happens in the digital or virtual world; however, this difference does not separate these two types of crimes, and they sometimes involve each other.

In the physical world, crimes are unavoidable but can be minimized by all kinds of mechanisms, such as regulations, laws, legislation, police, and so forth. Similarly, we believe that cyber crimes are unavoidable and should be punished by regulations, laws, and so forth. However, in the digital world, related laws have yet to mature. There are still no sound laws to protect users from cyber crimes because of the relatively brief history of information technology and people's limited understanding of such crimes. Because of cyber crimes' existence in the digital world, it is difficult to make technical laws. Therefore, it is difficult to capture criminals and punish them. It is also difficult to collect evidence.

In the digital world, damages are always inflicted remotely and can only be noticed after a long time (or not at all). This type of damage is quite different from the obvious damages within physical society, such as personal injury or property loss. Information loss or damage is not always as obvious or observable as financial loss; so many attacks in the digital world are not easily detected. For example, many users or administrators do not realize that their computers and networks have been hacked or attacked. One reason for this is that a cyber crime is not restricted by physical access limitations (such as noticeable human injury or stolen articles). Instead, a cyber crime is stealthy. It can access a building via an unnoticeable wired or wireless link. Most damages in the physical world can only be caused by criminals at the scene, although there are some remotely conducted crimes, such as those conducted with missiles or other long-range weapons, which need financial and human resources and are therefore not easily accessible to normal criminals. However, in the digital world, criminals can potentially go anywhere in the world and commit crimes. Another reason is that computers and networks are all connected so that a skillful attacker can access them from anywhere in the world with much less effort than in physical crimes.

Due to the brief history of digital technology and networks, the achievement of functions (e.g., information management, computation, and communication) is always the main target instead of information security. When considering system hardware/software, network, and related services/programs, security schemes are not well designed. Cyber crime prevention, detection, and response have also yet to mature. Therefore, it is relatively easy to commit digital crimes.

Cyber crime generally is described as criminal activities that use modern information technology, such as computer technology, network technology, and so forth. There are all kinds of cyber crimes, including illegal access (such as hacking), illegal interception, data interference, systems interference, misuse of devices, forgery (ID theft), electronic fraud, and so forth [1].

Cyber crime is now becoming a serious concern. Many researchers put a great deal of energy into protecting society and human beings from cyber crimes. One recent study showed that a new cyber crime is committed every 10 s in Britain [2]. About 3.24 million attacks [2] were conducted by cyber criminals in 2006. Some online crimes have even surpassed their equivalents in the physical world. In the meantime, experts estimate that about 90% of the cyber crimes go unreported [2].

As a specialist in psychology at the University of San Francisco, S. McGuire once performed a study showing that most teenagers hack into and intrude computer systems only for fun and not to cause damage or harm [3]. It is quite often the case that parents cannot understand the motivations of teenage hackers. She conducted an anonymous study with more than 4800 students in the San Diego area and questioned them about their experience related to unauthorized operation of computer systems or network resources. As published at the American Psychological Association conference, the results are as follows [3]: the percentage of teenagers involved in software piracy is about 38%; the percentage of youngsters who admitted using information in other people's computers/Web sites is about 18%; the percentage of people who committed revisions in computers and files is about 13%; and the percentage of hackers causing harm or financial losses is about 10%. Most of the teenagers' illegal computer activities are driven by their curiosity or enjoyment of the experience [3].

Usually, the term cyber crime refers to criminal behavior carried out through a computer or network [4]. However, it is also applied to some traditional crimes committed with the help of computers or networks [4]. In the later sections of this paper, we will present a categorization of cyber crimes and explain each class with detailed examples.

It is important for the research community to deeply understand cyber crimes and to find ways to prevent them. Most existing research focuses more on attacks and attack models, covering either actual attacks or imaginary/possible attacks over all layers of networks or computers, but there has been less work carried out on a comprehensive survey of cyber crimes. Our motivation for writing this paper is to help people realize the comprehensive classifications and examples of cyber crimes. We expect that this paper can help reduce the number of cyber crimes listed in this paper significantly in the near future. In this paper, we provide a comprehensive survey of cyber crimes that have actually occurred. We compare cyber crimes in the digital world with crimes in the physical world. We also categorize cyber crimes according to the roles of computers or networks.

There are many related research studies in the following topics: various attacks and vulnerabilities [5–20], key management [21–36], traceback [37–40], elliptic curve cryptosystem [41–42] intrusion detection [44–50], radio frequency identification security [51–57], security in wireless networks [58–75], authentication [76–85], security in peer-to-peer networks [86–88], and other security issues [89–131].

The rest of this paper is organized as follows: in Section 2, we provide the classification of cyber crimes; in Section 3–7, we detail each category with examples; and we conclude the paper in Section 8.

2. CATEGORIES

The advance of computers and networks has greatly contributed to the spread of cyber crimes. According to the main roles of computers or networks played in the crimes, cyber crimes are categorized into the following six classes [3,132]. We draw this classification in Figure 1.

(1) *The computer or network is used as a tool in a criminal activity.* These are the cyber crimes in which computers or networks are used mainly as tools, including spamming and criminal copyright violations, especially those facilitated through peer-to-peer networks [132].
(2) *The computer or network is the target of a criminal activity.* These are the cyber crimes in which computers or networks are the targets of criminal activities, including unauthorized access (i.e., defeating access controls), malicious code, viruses, denial-of-service (DoS) attacks, and hacking attacks [3].
(3) *The computer or network is the place of a criminal activity.* These are the cyber crimes in which computers or networks are mainly the places of criminal activities, including theft of services (in particular, telecommunication frauds) and certain financial frauds [3].
(4) *Traditional crimes facilitated through the computers or the networks.* Many traditional crimes become more harmful when facilitated by the use of computers or networks. This category of crimes includes gullibility or social engineering frauds, such as phishing, identity theft, child pornography, online gambling, securities fraud, and so forth [132]. For example, cyber stalking is a traditional crime of harassment, but it follows out with different patterns when facilitated by computers and networks [132].
(5) *Other information crimes.* Additionally, there are also some information crimes, such as trade secret theft and industrial or economic espionage, which are

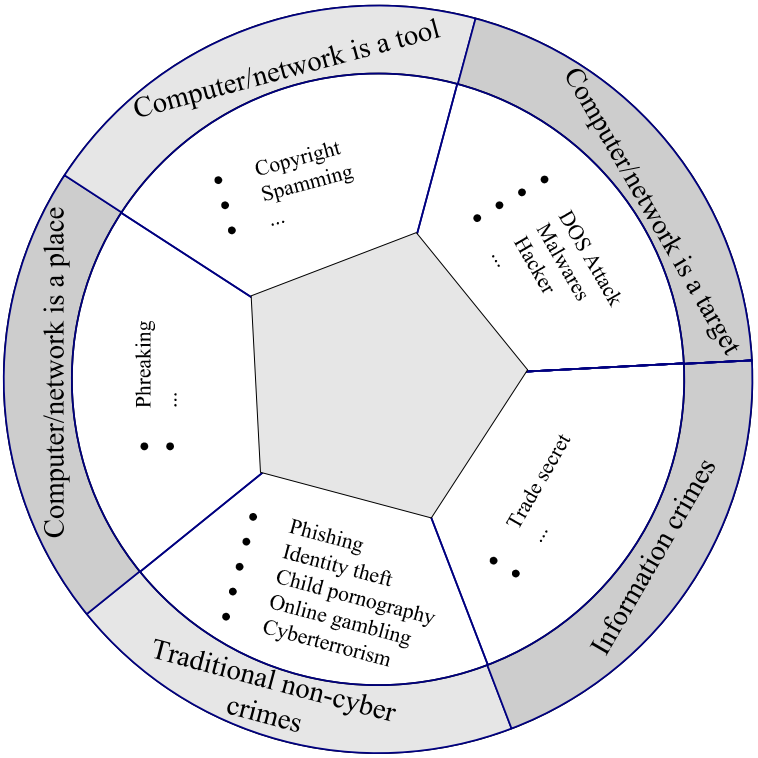

Figure 1. Categorization of cyber crime.

considered to be cyber crimes when facilitated by computers or networks [3].

In the following sections, we will detail each category of cyber crimes with examples.

3. AS A TOOL

3.1. Copyright

According to the definition in [133], "copyright is a legal concept, enacted by most governments, giving the creator of an original work exclusive rights to it with a limited time." Broadly speaking, it is "the right to copy", and the copyright holder achieves the right to be credited for the work, to decide who can use the work, who can perform the work, who can benefit from it, and other corresponding benefits [133].

Nowadays, it is very common to unlawfully download copyrighted materials and share recorded music with all kinds of audio files (like MP3), even though the American recording industry has brought about the demise of Napster and a series of infringement suits [134].

In the meantime, in some countries, people are illegally selling copyrighted materials, such as VCDs, CDs, and DVDs, by the roadside or night market.

In February 2007, the YouTube Web site was ordered by Viacom, Inc. to delete about 100 000 videos that were alleged to be clips of Viacom movies or TV shows [199].

In 2004, Novell was sued by the SCO Group (a software company) after Novell claimed its copyrights to the UNIX operating system and the UnixWare software were violated [135]. In August 2007, a court concluded that SCO's copyright claims were false and that Novell indeed had the UNIX copyrights [135].

3.2. Spamming

According to the definition in [136], spamming usually refers to the abuse of electronic messaging systems and the indiscriminate sending of unsolicited bulk messages [199]. Spamming is widely recognized as e-mail spams; however, it has been similarly abused in other approaches such as instant messaging, the Usenet newsgroup, Web search engines, blogs, wikis, mobile phone messaging, Internet forums, and junk fax transmissions [136].

Economically, spamming remains viable because, except for managing their list of e-mail addresses, there are no operating costs for advertisers, and it is difficult to hold senders accountable for their mass mailings [136]. As a result of its being easy and its low cost of entry, spammers and unsolicited e-mails are numerous. The cost of lost productivity, fraud, and so forth is high, and Internet service providers cope with it by adding extra capacity [136].

It is widely believed that the term "spam" originated with the 1970 Monty Python Spam sketch set in a café with Spam lunch meat included in nearly every item on its menu [200]. In that café, all the waiters recite the Spam-filled menu all

the time [200]. Then, a song was made because of a chorus of that song (Spam, Spam, lovely Spam… wonderful Spam), and then the word "SPAMming" became a popular word in that café. During World War II, Spam was a widely available meat product that did not require rationing. The Spam mentioned in the sketch is a reference to British rationing during that war period [200].

Spam can be used to spread all kinds of viruses and malicious software for identity theft, distributing some malwares, or worse. Examples of spammers are listed as follows.

Sanford Wallace and Cyber Promotions were once engaged in a string of lawsuits [136]. Although many of them were settled out of court, Sanford Wallace was part of the famous 1998 Earthlink settlement, and Cyber Promotions was put in bankruptcy [136].

In 1997, the Tennessee Supreme Court disbarred Attorney Laurence Canter for sending a great deal of spam propagandizing his law practice related to immigration [136].

In 2005, Florida Attorney General Charlie Crist sued Scott J. Filary and Donald E. Townsend of Tampa, Florida [137]. The two spammers violated the Florida Electronic Mail Communications Act [137]. They both received a penalty of $50 000. If any of the following situations existed, they would be charged an additional $1.1m penalty: the spamming was still spreading, the $50 000 went unpaid, or they provided dishonest financial statements [138].

In 2005, Nigel Roberts received junk e-mails in his personal account from the Channel Islands and won £270 in a suit against the sender, Media Logistics UK [139].

In January 2007, the Edinburgh Sheriff's Court granted Gordon Dick a decree against Transcom Internet Services Ltd. (Transcom) of Henley-on-Thames [140].

On 31 May 2007, Robert Alan Soloway, one of the world's top 10 spammers, was arrested. Soloway was prosecuted for 35 criminal counts, including mail fraud, wire fraud, e-mail fraud, aggravated identity theft, and money laundering [141].

In June 2007, two men were convicted of eight counts of sending enormous e-mail spam messages [136]. The two were required to pay $100 000 as a penalty, to pay $77 500 in compensation to AOL, and charged more than $1.1m in forfeitures [136].

4. AS A TARGET

4.1. Denial of service

A DoS attack or distributed DoS (DDoS) attack is a crime that renders computers or network resources inaccessible to their intended users or customers. Although DoS attacks may be via different means, motives, and targets, they generally include the concerted, malevolent efforts of a person or persons to make an Internet site or service unable to perform normally or even at all [142]. Criminals are always interested in sites or hosts related to high profile servers, such as banks, credit card payment gateways, and even domain name system (DNS) root servers [142].

As defined by the US Computer Emergency Readiness Team, symptoms of DoS attacks include the following [143]:

- unusually slow performance of network services (opening files or accessing Web sites),
- unavailability of a particular Web site or even any Web site, and
- an increasing number of spam e-mails.

One common type of DoS attack is saturating the target/victim's machine with external communications requests to make it inaccessible to its intended users. Subsequently, the victim host/server cannot provide services to its users or responds extremely slowly even though they become available [142]. A different kind of DoS attack is achieved by forcing the target/victim's computer(s) to reset, whereas another is to consume much of the computer(s)' resources [142]. Both activities aim at preventing the computer(s) from providing its intended service or preventing communications between the victim and the others [142].

In January 2001, http://www.register.com was attacked by a DNS using DNS servers as reflectors [144]. This attack was stopped until 1 week later. It made use of enormous DNS records that were from 1 year before the attack happened [144].

In two other cases, attackers performed DNS backbone DDoS attacks on the DNS root servers [145]. One occurred in October 2002, and as a result, 9 of the 13 root servers were put out of service; the other one was in February 2007 and disrupted two of the root servers [145]. The true motivations of the attackers were unclear. Generally, they aim to shut down the Internet service.

In February 2007, a hacker group named "RUS" attacked more than 10 000 online game servers, which included Return to Castle Wolfenstein (Activision, Santa Monica, CA, USA), Halo (Bungie, Inc., Bellevue, WA, USA), Counter-Strike (Valve Corp., Bellevue, WA, USA), and so forth [146]. More than a thousand computer units were involved, which were located in the republics of the former Soviet Union, with most being in Russia, Uzbekistan, and Belarus. Even now, there are still minor attacks [146].

A group that calls itself "Anonymous" made a DDoS attack in late January 2008 that targeted the Web site of Scientology as part of an anti-Scientology campaign called Project Chanology [147].

4.2. Malwares

According to the definition in [148], malware refers to software designed to penetrate or destroy a computer system without the knowledge of the owner. The word malware combines the words malicious and software [148]. As generally used by computer professionals, the expression refers to all kinds of software or program codes with hostile or intrusive purposes [148].

However, the term "malware" is seldom used by computer users, and many people are confused by the terms "malware" and "virus" [148]. The term "virus" is inappropriately used in common parlance to describe all

kinds of malware, but not all kinds of malware are actually viruses [148].

Software is considered malware only if the creator's intent is malicious [149]. There are many examples of malware, such as computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software [149].

4.3. Hacker

In the context of security, a hacker is someone who tries to explore systems or obtain unauthorized access to others' computers through specific skills or knowledge [150]. There are usually three kinds of hackers: black hat hackers, white hat hackers, and gray hat hackers [150]. What people always refer to with the term "hacker" is a black hat hacker that is malicious or criminal [150]. White hat hackers are ethical hackers, and those ambiguous in ethics are called gray hat hackers.

The first time "hacker" was used to describe the illegal activity of intruding into others' computer systems was in an article published in Newsweek in 1983 [151]. The article reported an incident in which dozens of computers were broken into by several teenagers who called themselves 414s [152]. From then on, several laws were passed related to "hack" criminals [153].

In the 1980s, Nahshon Even-Chaim (also known as Phoenix) attacked the US defense and nuclear research computer systems. He was captured in 1990 [150]. He was the first computer intruder prosecuted by evidence from remote computer intercepts [150].

Jonathan James was sentenced to prison at the age of 16 because he downloaded software related to the International Space Station's life sustaining elements, which was worth $1.7m. He became the youngest person imprisoned for cyber crime in the USA [154].

Adrian Lamo once intruded into several famous systems in 2003, including Microsoft, Lexis-Nexis, SBC, and so forth.

Before Kevin Mitnick became a public speaker, author, and so forth, he spent more than 4 years in jail and was once known as "The most wanted man in cyberspace" [154].

In fact, there are countless cyber criminals. For example, Robert T. Morris, who created the first worm when he was still a student at Cornell University [155]; Jason Burks, who is famous for writing malicious software [156]; Neidorg, who stole secret documents from BellSouth through online means [150]; Brian Scalcedo, who was sentenced to prison for 9 years in 2004 for hacking the Low's for credit card numbers used in transactions [157]; and Smith, who launched the Melissa Worm and was sentenced to prison in 1999 [150].

5. AS A PLACE

5.1. Phreaking

Phreaking is a slang term used to describe criminal activities related to phones. The word "phreak" is a combination of the words "phone" and "freak", and those individuals involved in "phreaks" are known as "phreakers" or "phone preaks" [158]. Such criminal activities are always related to those people working with or studying telecommunication systems, especially those familiar with public telephone networks and related equipments and systems [159].

In 1957, a blind 8-year-old boy named Joe Engressia found that a dialed phone recording would be stopped when whistling the fourth E above middle C, which has a frequency of 2600 Hz [160]. Later, the boy changed his name to "Joybubbles" and became skilled with perfect pitch [160]. In fact, the 2600-Hz frequency was a critical internal telephone company signal to control a trunk line and opened up almost limitless free use. However, the 8-year-old boy knew nothing about this even after he had done it, and he even made a call to the phone company to ask why the recordings stopped [160]. After that, he became quite interested in exploring telephone systems [160].

Other early phreaks, such as "Bill from New York", also started by wondering how phone networks worked [159]. "Bill" found that one of his recorders could also play a frequency of 2600 kHz [159]. John Draper, a friend of "Joybubbles", discovered another way to produce a tone with a frequency of 2600 kHz, which inspired the control of phone systems by single frequency (SF) controls [159].

As SF and its function are well known for certain phone routes, multi-frequency (MF) is the most common signaling control for long distance networks [161]. SF served this purpose until the publication of an article in the *Bell System Technical Journal* that described the methods and frequencies of inner-office signaling [161].

The most famous case of phreaking happened in the USA on 15 June 2006 [162]. The event is called "The end of MF phreaking", as it made attacks during the replacement of an N2 carrier with a T1 carrier in the USA [162]. The Northern Telephone Company of Minnesota located in Wawina Township, Minnesota [162], ran this exchange. Many phreakers from North America and all over the world made attacks during this event. A message board was set up on a specific number, and the most popular phreakers could be heard on the message board. The attacks lasted for more than a week, from several days prior to the official exchange date of 14 June 2006 [162].

6. TRADITIONAL NON-CYBER CRIMES FACILITATED BY COMPUTER AND NETWORK TECHNOLOGY

6.1. Phishing

In computing, phishing refers to attempts to criminally and fraudulently gain sensitive information, such as usernames, passwords, and credit card details, by means of some public entities that run on electronic systems, such as online banks, PayPal, and eBay [163].

Typically, phishing uses e-mail or instant messaging and directs users to enter their detailed information on the Web site [164]. Nowadays, efforts have been made to protect people from phishing, including legislation, user training, and technical measures.

The phishing technique has been used since 1987, and the first recorded phishing was in 1996, although the term existed on hacker-related print publications even earlier [163,165].

In these years, phishing-related reports increased dramatically. Recently, such crimes have been more likely to target customers of banks and payment services. E-mail is also a critical way to steal customers' sensitive information. Initially, phishers send e-mails indiscriminately to many people expecting some to respond. Thereafter, criminals determine which bank the users used and begin to send bogus e-mails, responsively.

Phishers also target social networks, through which they can gain a customer's personal information for identity theft [163]. It has been reported that such attacks have reached a success rate of over 70% [163].

6.2. Identity theft

Identity theft is a term used to describe fraud in which the criminal pretends to be someone else to steal money or get other benefits. It is also a crime for criminals to pretend to be someone else even if they do not steal an identity [166].

According to the US Federal Trade Commission, every year in the USA, approximately 10 million people are victims of identity fraud [167]. Mostly, such crimes are related to computer theft, loss of backups, or compromised information systems and are intended to reap financial benefits or to conceal illegal activities by using a legal identity [167]. Identity theft is also a habitual trick among terrorists [167].

As evidenced in a joint study by the Council of Better Business Bureau and Javelin Strategy & Research, approximately $50bn was lost by both consumers and businesses because of identity theft in the USA [167]. According to one home office committee, identity theft cost the British economy about $3.2bn in the UK in the last 3 years [168]. In the meantime, in Australia, the Securities Industry Research Center of Asia-Pacific estimates the cost at less than $1bn, whereas the Commonwealth Attorney-General's Department calculates it to be more than $3bn per year [167].

In May 2006, Standard Bank discovered that an international group of cyber criminals had cheated more than 50 customers, including both local and international customers [169]. The costs exceeded over several hundred thousand rands (1 rand = $US0.15) [169]. The criminals passed a Trojan virus to the customers' computers and captured bank information from them [169].

Also in May 2006, a study related to identity theft was presented by Mary Poquette at the "Secure 360"conference in the USA, which cited 31 cases with nearly 3.5 million people involved in personal data theft that occurred from 15 February 2005 to 8 April 2005 [169].

Another case included two individuals who were arrested on 30 October 2002 with dozens of French passports, revenue stamps, and laminated films [167]. They were also found to be working for terrorists, and they were sentenced to 5 and 8 years in prison in Paris on 9 July 2004 [167].

In the USA, a database of names of dangerous individuals is maintained by the National Counterterrorism Center with the purpose of detecting terrorists or criminals [170]. More than 325 000 names are included in the database; however, those names correspond to only 200 000 persons [170]. It is possible that an innocent person's name may be added to the list if the name was used by a criminal in an identity theft [170].

There was such a mistake in December 2004 [167]. A passenger on a Delta airline was on the no-fly list, and authorities rerouted the plane to a military base [167]. After several hours of examination, authorities found that the passenger was innocent and that they were the victim of identity theft [167].

6.3. Child pornography

Child pornography is the term used to describe the sexual abuse of children by means of pornographic material [171]. With the help of the Internet, it is quite easy to spread images and video.

Child pornography is illegal all over the world. Related production of such material is also prohibited [132]. The main reason that such criminal activities continue is the profit that can be generated from the sale of such images. Photographs and movies are still being produced and purchased. From a statement by the UK Children's charity NCH, child pornography cases have undergone a 1500% rise since 1988 [172]. As such, more and more children are becoming the victims of such crimes.

According to a review in 2008 [173], exposure to child pornography stimulates and provokes criminal sexual intentions that otherwise would have lie buried or was inaccessible [174]. Exposure to child pornography may heighten desires and motivate people to act on urges by lowering internal restraints [174]. Anonymity (or the belief that anonymity exists) may further loosen these internal restraints, such that the individual "practices" molestation in their imagination that is facilitated by still or moving images. This makes actual criminal sexual behavior with children more probable if the person was already sexually motivated toward children and creates new sexual interest in children [174]. The review article states that these are plausible hypotheses, while there is a lack of clarity as to the general applicability of these mechanisms [174].

The review article mentioned in the former paragraph further indicates that, when child pornography users go on to commit sexual offenses, the offenses are characterized by the exploitation of a relationship that is bent by the offender in the direction of sexuality and by the absence of violence [174]. The most common charges are statutory rape and other types of sexual crimes in which the victim has cooperated [174].

Additionally, some materials (such as images) related to child pornography are created artificially. In these cases, the children involved are not the actual persons. Therefore,

there is a dispute on whether such a form falls under the scope of child pornography.

6.4. Online gambling

Online gambling generally refers to gambling over the Internet. In the following, we will introduce some forms of online gambling, as well as some general issues [175].

In November 2002, sports betting with interstate electronic information transmissions was prohibited by the US Court of Appeals for the Fifth Circuit; however, there is a lower court ruling for the betting related to sports through the Internet [175].

Any possible form of online gambling is prevented in some states by special laws for online gambling [175]. Without a license, it is illegal for anyone to own an online game. However, there is currently no law on granting online gaming licenses in any state [175].

Online money laundering is the major concern of the US Department of Justice. Specifically, it is very difficult to trace online money laundering transactions [176].

In August 2004, the US Department of Justice sued an online portal for Internet gambling sites at Casino City. The complaint claimed that Internet gambling, which was the business of the Web site, was legal and should be protected by the First Amendment. The Web site also requested a declaration from the Court [177]. In February 2005, the case was dismissed by the US District Court for the Middle District of Louisiana [177].

David Carruthers, the CEO of BetonSports, was detained in Texas in July 2006 when he was changing planes on his way from London to Costa Rica [175]. BetonSports was a publicly traded company on the London Stock Exchange, which hosted sports betting and violated at least nine different Federal statutes, including 18 USC Sec. 1953 (Operation of an Illegal Gambling Business) [175]. Coincidently, in September 2006, the chairman of Sportingbet, Peter Dicks, was detained in New York City because he was running online games [178].

Problem gambling is also an important form of online gambling. In the USA, it was stated by the National Gambling Impact Study in 1999 that problem and pathological gambling may be exacerbated by a high-speed Internet game with instant gratification and highly protected privacy [179]. A review of previous research funded by the UK government reported that in a small-scale patient survey, only a minority of people would choose to visit legitimate land-based casinos and that most online gamblers are "problem" or "pathological" [180].

The UK Gambling Commission conducted a study, the *British Gambling Prevalence Survey 2007*,, which reported that only a small proportion of the adult population had gambling issues. This was the same result as in 1999 [181]. The survey also reported other proportions among the adult population, such as the percentage participating in spread betting (14.7%), fixed odds betting terminals (11.2%), and betting exchanges (9.8%) [181]. There was a drop in overall gambling compared with earlier years (62% in 1999 to 58% in 2007) [181].

When the former two surveys are combined, it is clearly suggested that the rapid growth of Internet gambling does not contribute to the increase in the number of problem gamblers [181]. In the meantime, the largely unsupervised electronic funds transferred for online gambling are alleged to be related to large-scale criminal money laundering [180].

6.5. Cyber stalking

As defined in [182], cyber stalking is stalking someone through the Internet or through other electronic means. It refers to an individual or group of individuals harassing another individual, group of individuals, or organization through the Internet or other communication technologies [182]. Behaviors intended to harass others, such as false accusations, monitoring, transmission of threats, identity theft, damage to data or equipment, solicitation of minors for sexual purposes, gathering information, and so forth, are all considered to be cyber stalking [182]. Harassment is considered to be an activity that, with the same information, a reasonable person would regard as sufficient to afflict another person [183].

Stalking is a criminal activity that consists of a series of continuous behaviors, and each of them may even be entirely legal in themselves [184]. As described by Lambèr Royakkers, stalking is the act of making a mental assault in which the victim's daily life is continuously and disruptively disturbed by the perpetrator [184]. The motivation of cyber stalkers is always to affect the lives of the victims directly or indirectly, mentally or physically [184].

The main factors of cyber stalking can be identified as follows:

False accusations: Many cyber stalkers aim to ruin the reputation of their victims and sometimes to make many other people oppose them [185]. In order to disgrace their victims, the cyber stalkers may apply all different kinds of media, such as newspapers, Bulletin Board System (BBS), chat rooms, Web sites, blogs, and so forth, to spread false information about the victims [185].

Attempts to gather information about the victim: The cyber stalker may try to approach the family or friends of the victim for detailed information about the victims [186]. They may also employ others to get the information they want or even to track the victims' online activities to steal related information [186].

Turning others against the victim: Sometimes, the cyber stalkers try to turn a third party against their victims for harassment purposes [182]. They may spread sham stories about the victims harming others and usually do so through the Internet [182]. They even post the contact information of the victims, such as their names, phone numbers, addresses, and so forth [182].

False victimization: This refers to crimes in which the cyber stalkers claim to be the victim and libel and stigmatize the true victims as cyber stalkers [182]. There have been many well-known cases of this phenomenon [182].

Attacks on data and equipment: The cyber stalkers may send viruses in an attempt to damage the victim's computer [182].

Ordering goods and services: The cyber stalkers order items or subscribe to magazines in the victim's name [182]. These purchases are often immoral things like pornography [182].

Arranging to meet: It seems that young people face a particularly high risk of having cyber stalkers who attempt to set up meetings [182].

The cyber stalkers use many methods to meet or target their victims, such as search engines, online forums, and, more recently, through online communities such as blogs and so on [187]. There are also other ways, including engaging in live chat harassment, flaming, or sending electronic viruses and unsolicited e-mails [187].

It is common for victims to be unaware of being stalked initially [187]. The cyber stalkers may attract victims by feeding their obsessions and curiosities. Then cyber stalkers may act more intensely by continuously sending messages to the victim [187].

Paige Padgett from the University of Texas Health Science Center conducted a study in 2007, which found that it was not safe for women to look for love online [188].

6.6. Cyber terrorism

With the intense development of information technology, the Internet has become more pervasive in all areas of human life. Under the threat of crimes committed in cyber space, individuals, social organizations, or even the whole Nation may be attacked [189]. Cyber space attackers do not face the inherent threat of injury or death that a physical attack would bring [189].

With the help of highly developed information technology, terrorists can attack networks or those which are electronic related [190].

After the September 11 attacks in 2001, cyber terrorism became a serious problem; a fact evidenced by reports of potential threats through all kinds of media [191]. Large attacks that use computer networks have become a popular discussion of the mainstream media. Such attacks could quite possibly occur with the purpose of threatening human lives or even causing nationwide panic [191].

Winn Schwartau and John Arquilla described many attacks, such as nuclear/mechanical plant attacks, in their popular books [189]. However, there is also much criticism over whether these attacks are realizable [191].

A significant number of people may be influenced by cyber terrorism, and a serious large-scale influence may also result [192]. Cyber terrorism can greatly damage countries' economies [192]. Internet-based businesses may also be affected by cyber terrorism [192].

When the computer systems at an Antarctic research station were hacked by some hackers in Romania, 58 scientists were involved and endangered [189]. However, the culprits were stopped before damage could actually be inflicted [189].

In 1999, North Atlantic Treaty Organization computers were attacked by hackers [193]. It was a DoS attack performed by hackers using flooding e-mails [193]. The attack was motivated by political purposes and e-mails containing political contents along with viruses bombarding many institutes and organizations [193].

More recently, a distributed DoS attack was initiated when the Estonian government tried to remove the Russian World War II memorial in May 2007 [189]. Some Web sites were inaccessible during the attack, especially the government Web sites [189]. People believed that the attack might have been related to Russian hackers and even the Russian government; however, no one was able to prove this [189].

Hackers attacked the Web site of Ukrainian president Viktor Yushchenko in October 2007. The Eurasian Youth Movement, a radical Russian nationalist youth group, claimed responsibility [194].

7. INFORMATION CRIMES

7.1. Trade secret

A trade secret is considered by a business to be some advantage over competitors or customers. The advantage can be in many different forms, such as formulas, practices, processes, designs, instruments, patterns, or compilations of information [195]. In some jurisdictions, terms such as "confidential information" or "classified information" are also used to describe such secrets [195].

A trade secret is some sort of information that [195]

- is generally unknown by the relevant portion of the public,
- confers to the holder some sort of benefit, and
- requires reasonable efforts to maintain its secrecy.

It is common for a company to require its employees to sign contracts promising not to disclose their technology and business secrets [196]. The holder of the trade secret owns a perpetual monopoly over the information under the protection of the law for confidential information [185]. However, without formal protection, the third party is legally able to independently duplicate and use the secret information once it is discovered [196].

A company always spends a great deal of time and money developing its own advantages for better performance in social competition. A company will not be able to well maintain its market dominance if its competitor shares the same knowledge [196]. Such secrets, regarded as "trade secrets" or "special knowledge", are also considered to be intellectual properties [196].

Generally, trade secrets are not as well protected as trademarks or patents by law [197]. There are already sophisticated state laws for protecting trademarks and patents, whereas trade secrets are not so well protected [197]. The biggest difference between trade secrets and trademarks/patents is that a trade secret is only protected when it is not disclosed [197].

Principally, trade secret protection can be indefinitely extended. This is a big advantage over the protection of patents, which are only effective and protected for a limited period [196]. A famous trade secret example is Coca-Cola, which has effectively protected its formula for many more years than a patent would have [198]. A common way to gain a competitor's trade secret is to conduct reverse engineering, and a patent will better withstand such a situation than a trade secret [196].

Historically, trade secrets existed during war so that advanced military technologies were protected from one's enemies [198]. However, in more recent times, they have been used more often to describe keeping industrial revolutionary technology secret [198].

Companies always try to discover each other's secrets, sometimes through lawful means such as reverse engineering and sometimes through less lawful means like industrial espionage [196].

8. CONCLUSIONS

With the great advance of computer technology, there now exist many different kinds of cyber crimes. Anyone could be attacked by a cyber criminal. Serious attacks happen every day, and we should have basic preparation and principles to protect ourselves. Awareness is the best defense. Individuals can also install firewalls to protect themselves from many attacks and can avoid installing unknown software.

In this paper, we categorized cyber crimes into several different classes and explained each category with detailed examples. The main purpose of the paper is to help people realize the threats and potential attacks and to learn from these attacks in order to better protect themselves.

ACKNOWLEDGEMENT

This work was supported in part by the US National Science Foundation (NSF) under grants CNS-0737325, CNS-0716211, CCF-0829827, and CNS-1059265.

REFERENCES

1. Moore R. Cybercrime: *Investigating High-Technology Computer Crime*. Anderson Publishing: Cleveland, Mississippi, 2005.
2. Cyber Crime Overview. 2008. Available from: http://cybercrimeindo.blogspot.com [accessed on 25 April 2010]
3. Cyber Forensics. 2008. Available from: http://www.santoshraut.com/forensic/cybercrime.htm [accessed on 25 April 2010]
4. Cyber Crimes. April 2008. Available from: http://theviewspaper.net/cyber_crimes [accessed on 25 April 2010]
5. Xiao Y. Editorial. *International Journal of Security and Networks* 2006; **1**(1/2): 1.
6. Englund H, Johansson T. Three ways to mount distinguishing attacks on irregularly clocked stream ciphers. *International Journal of Security and Networks* 2006; **1**(1/2): 95–102.
7. Karyotis V, Papavassiliou S, Grammatikou M, Maglaris V. A novel framework for mobile attack strategy modelling and vulnerability analysis in wireless ad hoc networks. *International Journal of Security and Networks* 2006; **1**(3/4): 255–265.
8. Jung E, Gouda MG. Vulnerability analysis of certificate graphs. *International Journal of Security and Networks* 2006; **1**(1/2): 13–23.
9. Jhumka A, Freiling F, Fetzer C, Suri N. An approach to synthesise safe systems. *International Journal of Security and Networks* 2006; **1**(1/2): 62–74.
10. Deng J, Han R, Mishra S. Limiting DoS attacks during multihop data delivery in wireless sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4): 167–178.
11. Evans JB, Wang W, Ewy BJ. Wireless networking security: open issues in trust, management, interoperation and measurement. *International Journal of Security and Networks* 2006; **1**(1/2): 84–94.
12. Hutter M, Plos T, Feldhofer M. On the security of RFID devices against implementation attacks. *International Journal of Security and Networks* 2010; **5**(2/3): 106–118.
13. Guo Y, Perreau S. Detect DDoS flooding attacks in mobile ad hoc networks. *International Journal of Security and Networks* 2010; **5**(4): 259–269.
14. Hu F, Dong D, Xiao Y. Attacks and countermeasures in multi-hop cognitive radio networks. *International Journal of Security and Networks* 2009; **4**(4): 263–271.
15. Ehlert S, Rebahi Y, Magedanz T. Intrusion detection system for denial-of-service flooding attacks in SIP communication networks. *International Journal of Security and Networks* 2009; **4**(3): 189–200.
16. Dalton II GC, Edge KS, Mills RF, Raines RA. Analysing security risks in computer and radio frequency identification (RFID) networks using attack and protection trees. *International Journal of Security and Networks* 2010; **5**(2/3): 87–95.
17. Hsu H, Zhu S, Hurson AR. LIP: a lightweight interlayer protocol for preventing packet injection attacks

in mobile ad hoc network. *International Journal of Security and Networks* 2007; **2**(3/4): 202 – 215.
18. Zhu Y, Fu X, Bettati R, Zhao W. Analysis of flow-correlation attacks in anonymity network. *International Journal of Security and Networks* 2007; **2**(1/2): 137–153.
19. Berthier R, Cukier M. An evaluation of connection characteristics for separating network attacks. *International Journal of Security and Networks* 2009; **4**(1/2): 110 – 124.
20. Xiao Y, Jia X, Sun B, Du X. Editorial: security issues on sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4): 125 – 126.
21. Franklin M. A survey of key evolving cryptosystems. *International Journal of Security and Networks* 2006; **1**(1/2): 46 – 53.
22. Araz O, Qi H. Load-balanced key establishment methodologies in wireless sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4): 158 – 166.
23. Teo J, Tan C, Ng J. Low-power authenticated group key agreement for heterogeneous wireless networks. *International Journal of Security and Networks* 2006; **1**(3/4): 226 – 236.
24. Ling H, Znati T. End-to-end pairwise key establishment using node disjoint secure paths in wireless sensor networks. *International Journal of Security and Networks* 2007; **2**(1/2): 109 – 121.
25. Hoeper K, Gong G. Preventing or utilising key escrow in identity-based schemes employed in mobile ad hoc networks. *International Journal of Security and Networks* 2007; **2**(3/4): 239 – 250.
26. Cheng Z, Chen L. On security proof of McCullagh – Barreto's key agreement protocol and its variants. *International Journal of Security and Networks* 2007; **2**(3/4): 251 – 259.
27. Kotzanikolaou P, Vergados DD, Stergiou G, Magkos E. Multilayer key establishment for large-scale sensor networks. *International Journal of Security and Networks* 2008; **3**(1): 1 – 9.
28. Zou X, Karandikar Y. A novel conference key management solution for secure dynamic conferencing. *International Journal of Security and Networks* 2008; **3**(1): 47 – 53.
29. Challal Y, Gharout S, Bouabdallah A, Bettahar H. Adaptive clustering for scalable key management in dynamic group communications. *International Journal of Security and Networks* 2008; **3**(2): 133 – 146.
30. Tripathy S, Nandi S. Secure user-identification and key distribution scheme preserving anonymity. *International Journal of Security and Networks* 2008; **3**(3): 201 – 205.
31. Ma L, Teymorian AY, Xing K, Du D. A one-way function based framework for pairwise key establishment in sensor networks. *International Journal of Security and Networks* 2008; **3**(4): 217 – 225.
32. Srinivasan A, Li F, Wu J, Li M. Clique-based group key assignment in wireless sensor networks. *International Journal of Security and Networks* 2008; **3**(4): 226 – 239.
33. Wu B, Wu J, Dong Y. An efficient group key management scheme for mobile ad hoc networks. *International Journal of Security and Networks* 2009; **4**(1/2): 125 – 134.
34. Chakrabarti S, Chandrasekhar S, Singhal M. An escrow-less identity-based group-key agreement protocol for dynamic peer groups. *International Journal of Security and Networks* 2009; **4**(3): 171 – 188.
35. Bettahar H, Alkubeily M, Bouabdallah A. TKS: a transition key management scheme for secure application level multicast. *International Journal of Security and Networks* 2009; **4**(4): 210 – 222.
36. Guo H, Mu Y, Zhang XY, Li ZJ. Enhanced McCullagh – Barreto identity-based key exchange protocols with master key forward security. *International Journal of Security and Networks* 2010; **5**(2/3): 173 – 187.
37. Hamadeh I, Kesidis G. A taxonomy of Internet traceback. *International Journal of Security and Networks* 2006; **1**(1/2): 54 – 61.
38. Pan J, Cai L, Shen X. Vulnerabilities in distance-indexed IP traceback schemes. *International Journal of Security and Networks* 2007; **2**(1/2): 81 – 94.
39. Korkmaz T, Gong C, Sarac K, Dykes SG. 8 Single packet IP traceback in AS-level partial deployment scenario. *International Journal of Security and Networks* 2007; **2**(1/2): 95 – 10.
40. Burt AL, Darschewski M, Ray I, Thurimella R, Wu H. Origins: an approach to trace fast spreading worms to their roots. *International Journal of Security and Networks* 2008; **3**(1): 36 – 46.
41. Finnigin KM, Mullins BE, Raines RA, Potoczny HB. Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks. *International Journal of Security and Networks* 2007; **2**(3/4): 260 – 271.
42. Wang H, Sheng B, Li Q. Elliptic curve cryptography-based access control. *International Journal of Security and Networks* 2006; **1**(3/4): 127 – 137.
43. Abbes T, Bouhoula A, Rusinowitch M. Efficient decision tree for protocol analysis in intrusion detection. *International Journal of Security and Networks* 2010; **5**(4): 220 – 235.
44. Wang X. The loop fallacy and deterministic serialisation in tracing intrusion connections through stepping stones. *International Journal of Security and Networks* 2006; **1**(3/4): 184 – 197.

45. Owens SF, Levary RR. An adaptive expert system approach for intrusion detection. *International Journal of Security and Networks* 2006; **1**(3/4): 206 – 217.
46. Liu Y, Comaniciu C, Man H. Modelling misbehaviour in ad hoc networks: a game theoretic approach for intrusion detection. *International Journal of Security and Networks* 2006; **1**(3/4): 243 – 254.
47. Scheirer W, Chuah M. Syntax vs. semantics: competing approaches to dynamic network intrusion detection. *International Journal of Security and Networks* 2008; **3**(1): 24 – 35.
48. Uphoff B, Wong JS. An agent-based framework for intrusion detection alert verification and event correlation. *International Journal of Security and Networks* 2008; **3**(3): 193 – 200.
49. Dong Y, Hsu S, Rajput S, Wu B. Experimental analysis of application-level intrusion detection algorithms. *International Journal of Security and Networks* 2010; **5**(2/3): 198 – 205.
50. Zhuang Z, Li Y, Chen Z. Enhancing intrusion detection system with proximity information. *International Journal of Security and Networks* 2010; **5**(4): 207– 219.
51. Huang S, Shieh S. Authentication and secret search mechanisms for RFID-aware wireless sensor networks. *International Journal of Security and Networks* 2010; **5**(1): 15 – 25.
52. Yang M. Lightweight authentication protocol for mobile RFID networks. *International Journal of Security and Networks* 2010; **5**(1): 53 – 62.
53. Leng X, Lien Y, Mayes K, Markantonakis K. An RFID grouping proof protocol exploiting anti-collision algorithm for subgroup dividing. *International Journal of Security and Networks* 2010; **5**(2/3): 79 – 86.
54. Mahinderjit-Singh M, Li X. Trust in RFID-enabled supply-chain management. *International Journal of Security and Networks* 2010; **5**(2/3): 96 – 105.
55. Imasaki Y, Zhang Y, Ji Y. Secure and efficient data transmission in RFID sensor networks. *Internaional Journal of Security and Networks* 2010; **5**(2/3): 119 –127.
56. Zhang X, Gao Q, Saad MK. Looking at a class of RFID APs through GNY logic. *International Journal of Security and Networks* 2010; **5**(2/3): 135 – 146.
57. Raad M. A ubiquitous mobile telemedicine system for the elderly using RFID. *International Journal of Security and Networks* 2010; **5**(2/3): 156 – 164.
58. Zheng J, Li J, Lee MJ, Anshel M. A lightweight encryption and authentication scheme for wireless sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4): 138 – 146.
59. Al-Karaki JN. Analysis of routing security-energy trade-offs in wireless sensor networks. *International Journal of Security and Networks* 2006; **1**(3/4): 147 – 157.
60. Oliveira LB, Wong H, Loureiro AAF, Dahab R. On the design of secure protocols for hierarchical sensor networks. *International Journal of Security and Networks* 2007; **2**(3/4): 216 – 227.
61. Wang W, Kong J, Bhargava B, Gerla M. Visualisation of wormholes in underwater sensor networks: a distributed approach. *International Journal of Security and Networks* 2008; **3**(1): 10 – 23.
62. Li F, Srinivasan A, Wu J. PVFS: a probabilistic voting-based filtering scheme in wireless sensor networks. *International Journal of Security and Networks* 2008; **3**(3): 173 – 182.
63. Hsiao Y, Hwang R. An efficient secure data dissemination scheme for grid structure wireless sensor networks. *International Journal of Security and Networks* 2010; **5**(1): 26 – 34.
64. Wang J, Smith GL. A cross-layer authentication design for secure video transportation in wireless sensor network. *International Journal of Security and Networks* 2010; **5**(1): 63 – 76.
65. Sun F, Shayman MA. On pairwise connectivity of wireless multihop networks. *International Journal of Security and Networks* 2007; **2**(1/2): 37 – 49.
66. Hu F, Rughoonundon A, Celentano L. Towards a realistic testbed for wireless network reliability and security performance studies. *International Journal of Security and Networks* 2008; **3**(1): 63 – 77.
67. Lin X, Ling X, Zhu H, Ho P, Shen X. A novel localised authentication scheme in IEEE 802.11 based Wireless Mesh Networks. *International Journal of Security and Networks* 2008; **3**(2): 122 – 132.
68. Kandikattu R, Jacob L. Secure hybrid routing with micro/macro-mobility handoff mechanisms for urban wireless mesh networks. *International Journal of Security and Networks* 2008; **3**(4): 258 – 274.
69. Kuo C, AC Perrig, Walker J. Designing user studies for security applications: a case study with wireless network configuration. *International Journal of Security and Networks* 2009; **4**(1/2): 101 – 109.
70. Watkins L, Beyah R, Corbett C. Using link RTT to passively detect unapproved wireless nodes. *International Journal of Security and Networks* 2009; **4**(3): 153 – 163.
71. Xu L, Chen S, Huang X, Mu Y. Bloom filter based secure and anonymous DSR protocol in wireless ad hoc networks. *International Journal of Security and Networks* 2010; **5**(1): 35 – 44.
72. Malaney RA. Securing Wi-Fi networks with position verification: extended version. *International Journal of Security and Networks* 2007; **2**(1/2): 27 – 36.
73. Richard AO, Ahmad A, Kiseon K. Security assessments of IEEE 802.15.4 standard based on X.805

framework. *International Journal of Security and Networks* 2010; **5**(2/3): 188 – 197.
74. Chen H, Guizani M. Editorial. *International Journal of Security and Networks* 2007; **2**(1/2): 1 – 2.
75. Sakarindr P, Ansari N. Adaptive trust-based anonymous network. *International Journal of Security and Networks* 2007; **2**(1/2): 11 – 26.
76. Mu Y, Chen L, Chen X, Gong G, Lee P, A Miyaji, *et al*. Editorial. *International Journal of Security and Networks* 2007; **2**(3/4): 171 – 174.
77. Tartary C, Wang H. Efficient multicast stream authentication for the fully adversarial network model. *International Journal of Security and Networks* 2007; **2**(3/4): 175 – 191.
78. Jiang Y, Lin C, Shi M, Shen X. A self-encryption authentication protocol for teleconference services. *International Journal of Security and Networks* 2006; **1**(3/4): 198 – 205.
79. Abdalla M, Bresson E, Chevassut O, Moller B, Pointcheval D. Strong password-based authentication in TLS using the three-party group Diffie – Hellman protocol. *International Journal of Security and Networks* 2007; **2**(3/4): 284 – 296.
80. Asadpour M, Sattarzadeh B, Movaghar A. Anonymous authentication protocol for GSM networks. *International Journal of Security and Networks* 2008; **3**(1): 54 – 62.
81. Memon N, Goel R. Editorial. *International Journal of Security and Networks* 2008; **3**(2): 79.
82. Scannell A, Varshavsky A, LaMarca A, de Lara E. Proximity-based authentication of mobile devices. *International Journal of Security and Networks* 2009; **4**(1/2): 4 – 16.
83. McCune JM, Perrig A, Reiter MK. Seeing-is-believing: using camera phones for human-verifiable authentication. *International Journal of Security and Networks* 2009; **4**(1/2): 43 – 56.
84. Laur S, Pasini S. User-aided data authentication. *International Journal of Security and Networks* 2009; **4**(1/2): 69 – 86.
85. Lee S, Sivalingam KM. An efficient one-time password authentication scheme using a smart card. *International Journal of Security and Networks* 2009; **4**(3): 145 –152.
86. Zhu B, Jajodia S, Kankanhalli MS. Building trust in peer-to-peer systems: a review. *International Journal of Security and Networks* 2006; **1**(1/2): 103 – 112.
87. Tsai K, Hsu C, Wu T. Mutual anonymity protocol with integrity protection for mobile peer-to-peer networks. *International Journal of Security and Networks* 2010; **5**(1): 45 – 52.
88. Schrader KR, Mullins BE, Peterson GL, Mills RF. An FPGA-based system for tracking digital information transmitted via peer-to-peer protocols. *International Journal of Security and Networks* 2010; **5**(4): 236 –247.
89. Shehab M, Bertino E, Ghafoor A. Workflow authorisation in mediator-free environments. *International Journal of Security and Networks* 2006; **1**(1/2): 2 – 12.
90. Kiayias A, Yung M. Secure scalable group signature with dynamic joins and separable authorities. *International Journal of Security and Networks* 2006; **1**(1/2): 24 – 45.
91. Ramkumar M, Memon N. Secure collaborations over message boards. *International Journal of Security and Networks* 2006; **1**(1/2): 113 – 124.
92. Hwu J, Hsu S, Lin Y-B, Chen R. End-to-end security mechanisms for SMS. *International Journal of Security and Networks* 2006; **1**(3/4): 177 – 183.
93. Chen Y, Susilo W, Mu Y. Convertible identity-based anonymous designated ring signatures. *International Journal of Security and Networks* 2006; **1**(3/4): 218–225.
94. Tan C. A new signature scheme without random oracles. *International Journal of Security and Networks* 2006; **1**(3/4): 237 – 242.
95. Li R, Li J, Chen H. DKMS: distributed hierarchical access control for multimedia networks. *International Journal of Security and Networks* 2007; **2**(1/2): 3 – 10.
96. Erdogan O, Cao P. Hash-AV: fast virus signature scanning by cache-resident filters. *International Journal of Security and Networks* 2007; **2**(1/2): 50 – 59.
97. Rabinovich P, Simon R. Secure message delivery in publish/subscribe networks using overlay multicast. *International Journal of Security and Networks* 2007; **2**(1/2): 60 – 70.
98. Chen Z, Ji C. Optimal worm-scanning method using vulnerable-host distributions. *International Journal of Security and Networks* 2007; **2**(1/2): 71 – 80.
99. Artan NS, Chao HJ. Design and analysis of a multi-packet signature detection system. *International Journal of Security and Networks* 2007; **2**(1/2): 122 –136.
100. Gu Q, Liu P, Chu C, Zhu S. Defence against packet injection in ad hoc networks. *International Journal of Security and Networks* 2007; **2**(1/2): 154 – 169.
101. Bhaskar R, Herranz J, Laguillaumie F. Aggregate designated verifier signatures and application to secure routing. *International Journal of Security and Networks* 2007; **2**(3/4): 192 – 201.
102. Michail HE, Panagiotakopoulos GA, Thanasoulis VN, Kakarountas AP, Goutis CE. Server side hashing core exceeding 3 Gbps of throughput. *International Journal of Security and Networks* 2007; **2**(3/4): 228 – 238.
103. Huang D. Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks. *International Journal of Security and Networks* 2007; **2**(3/4): 272 – 283.

104. Ray I, Poolsappasit N. Using mobile ad hoc networks to acquire digital evidence from remote autonomous agents. *International Journal of Security and Networks* 2008; **3**(2): 80 – 94.
105. Kilpatrick T, Gonzalez J, Chandia R, Papa M, Shenoi S. Forensic analysis of SCADA systems and networks. *International Journal of Security and Networks* 2008; **3**(2): 95 – 102.
106. Cronin E, Sherr M, Blaze M. On the (un)reliability of eavesdropping. *International Journal of Security and Networks* 2008; **3**(2): 103 – 113.
107. Okolica JS, Peterson GL, Mills RF. Using PLSI-U to detect insider threats by datamining e-mail. *International Journal of Security and Networks* 2008; **3**(2): 114 – 121.
108. Xu H, Ayachit M, Reddyreddy A. Formal modelling and analysis of XML firewall for service-oriented systems. *International Journal of Security and Networks* 2008; **3**(3): 147 – 160.
109. Bouhoula A, Trabelsi Z, Barka E, Benelbahri M. Firewall filtering rules analysis for anomalies detection. *International Journal of Security and Networks* 2008; **3**(3): 161 – 172.
110. Ma X, Cheng X. Verifying security protocols by knowledge analysis. *International Journal of Security and Networks* 2008; **3**(3): 183 – 192.
111. Li F, Xin X, Hu Y. ID-based threshold proxy signcryption scheme from bilinear pairings. *International Journal of Security and Networks* 2008; **3**(3): 206 – 215.
112. Hsieh C, Chen J, Lin Y-B, Chen K, Liao H, Liang C. NTP-DownloadT: a conformance test tool for secured mobile download services. *International Journal of Security and Networks* 2008; **3**(4): 240 – 249.
113. Sadowitz M, Latifi S, Walker D. An iris and retina multimodal biometric system. *International Journal of Security and Networks* 2008; **3**(4): 250 – 257.
114. Mayrhofer R, Nyberg K, Kindberg T. Foreword. *International Journal of Security and Networks* 2009; **4**(1/2): 1 – 3.
115. Soriente C, Tsudik G, Uzun E. Secure pairing of interface constrained devices. *International Journal of Security and Networks* 2009; **4**(1/2): 17 – 26.
116. Buhan I, Boom B, Doumen J, Hartel PH, Veldhuis RNJ. Secure pairing with biometrics. *International Journal of Security and Networks* 2009; **4**(1/2): 27 – 42.
117. Goodrich MT, Sirivianos M, Solis J, Soriente C, Tsudik G, Uzun E. Using audio in secure device pairing. *International Journal of Security and Networks* 2009; **4**(1/2): 57 – 68.
118. Suomalainen J, Valkonen J, Asokan N. Standards for security associations in personal networks: a comparative analysis. *International Journal of Security and Networks* 2009; **4**(1/2): 87 – 100.
119. Chen Z, Chen C, Li Y. Deriving a closed-form expression for worm-scanning strategies. *International Journal of Security and Networks* 2009; **4**(3): 135 –144.
120. Drakakis KE, Panagopoulos AD, Cottis PG. Overview of satellite communication networks security: introduction of EAP. *International Journal of Security and Networks* 2009; **4**(3): 164 – 170.
121. Bai L, Zou X. A proactive secret sharing scheme in matrix projection method. *International Journal of Security and Networks* 2009; **4**(4): 201 – 209.
122. Huang H, Kirchner H, Liu S, Wu W. Handling inheritance violation for secure interoperation of heterogeneous systems. *International Journal of Security and Networks* 2009; **4**(4): 223 – 233.
123. Rekhis S, Boudriga NA. Visibility: a novel concept for characterising provable network digital evidences. *International Journal of Security and Networks* 2009; **4**(4): 234 – 245.
124. Djenouri D, Bouamama M, Mahmoudi O. Black-hole-resistant ENADAIR-based routing protocol for Mobile Ad hoc Networks. *International Journal of Security and Networks* 2009; **4**(4): 246 – 262.
125. Yang M, Liu JCL, Tseng Y. Editorial. *International Journal of Security and Networks* 2010; **5**(1): 1 – 3.
126. Malliga S, Tamilarasi A. A backpressure technique for filtering spoofed traffic at upstream routers. *International Journal of Security and Networks* 2010; **5**(1): 3 – 14.
127. Wang H, Jia X. Editorial. *International Journal of Security and Networks* 2010; **5**(2/3): 77 – 78.
128. Sun L. Security and privacy on low-cost radio frequency identification systems. *International Journal of Security and Networks* 2010; **5**(2/3): 128 – 134.
129. Azevedo SG, Ferreira JJ. Radio frequency identification: a case study of healthcare organisations. *International Journal of Security and Networks* 2010; **5**(2/3): 147–155.
130. Rodrigues MJ, James K. Perceived barriers to the widespread commercial use of radio frequency identification technology. *International Journal of Security and Networks* 2010; **5**(2/3): 165 – 172.
131. Chen Z, Chen C, Wang Q. On the scalability of delay-tolerant botnets. *International Journal of Security and Networks* 2010; **5**(4): 248 – 258.
132. Bantekas I, Nash S. *International Criminal Law 2/E*, Routledge Cavendish: London, 2003. ISBN 1859417760. [retrieved on 20 June 2008]
133. Copyright. Available from: http://en.wikipedia.org/wiki/Copyright [accessed on 25 April 2010]
134. Copyright infringement. Available from: http://en.wikipedia.org/wiki/Copyright_infringement [accessed on 25 April 2010]
135. SCO-Linux controversies. Available from: http://en.wikipedia.org/wiki/SCO-Linux_controversies [accessed on 25 April 2010]

136. Spam (electronic). Available from: http://en.wikipedia.org/wiki/Spam_(electronic) [accessed on 25 April 2010]
137. Crist Announces First Case Under Florida Anti-Spam Law. Available from: http://myfloridalegal.com/newsrel.nsf/newsreleases/F978639D46005F6585256FD90050AAC9 [accessed on 25 April 2010]
138. Crist: Judgment Ends Duo's Illegal Spam, Internet Operations. Available from: http://myfloridalegal.com/__852562220065EE67.nsf/0/F08DE06CB354A7D7852570CF005912A2?Open&Highlight=0 [accessed on 25 April 2010]
139. Businessman wins e-mail spam case. Available from: http://news.bbc.co.uk/2/hi/europe/jersey/4562726.stm [accessed on 25 April 2010]
140. Leyden J. Scotsman wins £1,300 settlement against spammer. March 2007. Available from: http://forms.theregister.co.uk/mail_author/?story_url=/2007/03/02/scotland_spam_victory/ [retrieved on 25 April 2010]
141. One of world's top 10 spammers held in Seattle. Available from: http://www.msnbc.msn.com/id/18955115/ [accessed on 25 April 2010]
142. Yuval F, Uri K, Yuval E, Shlomi D, and Chanan G. Google Android: *A Comprehensive Security Assessment. In the proceeding of IEEE Security and Privacy*, Los Alamitos, CA, USA: IEEE Computer Society 2010; **8**(2): 35–44.
143. McDowell M. Cyber Security Tip ST04-015. United States Computer Emergency Readiness Team. 2008. Available from: http://www.us-cert.gov/cas/tips/ST04-015.html [retrieved on 2 May 2008]
144. January 2001 thread on the UNISOG mailing list. Available from: http://staff.washington.edu/dittrich/misc/ddos/register.com-unisog.txt [retrieved on 20 June 2008]
145. Naraine R. Massive DDoS Attack Hit DNS Root Servers. October 2002. Available from: http://www.esecurityplanet.com/trends/article.php/1486981/Massive-DDoS-Attack-Hit-DNS-Root-Servers.htm [accessed on 25 April 2010]
146. Subbulakshmi T, Mercy Shalinie S, and Ramamoorthi A. Detection and Classification of DDoS Attacks Using Machine Learning Algorithms, *European Journal of Scientific Research* 2010, **47**(3): 334–346.
147. Landers C, The Internets Are Going to War. January 2008. Available from: http://www.citypaper.com/digest.asp?id=15150.[accessed on 25 April 2010]
148. Available from: http://en.wikipedia.org/wiki/Malware [retrieved on 20 June 2008]
149. Penalty for Computer Contamination. Joint Commission on Technology and Science. Available from: http://jcots.state.va.us/2005 Content/pdf/Computer Contamination Bill.pdf [retrieved on 17 September 2010]
150. Sterling B. *The Hacker Crackdown Indypublish.com*: McLean, VA, 1993; Part 2(d):61.
151. Beware: Hackers at play. Newsweek, 5 September 1983: 42 – 46,**48** [retrieved on 20 June 2008]
152. Bailey D. Attacks on computers: congressional hearings and pending legislation. In *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 29 April–2 May 1984. IEEE Press: New York, 1984; 180–187.
153. Recognized hackers. April 2007. Available from: http://forums.zizula.com/index.php?topic=14.msg105#top [accessed on 25 April 2008]
154. Kehoe B.P. The Robert Morris Internet Worm. 2007. Available from: http://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html. Retrieved August 23, 2008. [accessed on 25 April 2010]
155. Jason Burks. Available from: http://www.answers.com/topic/jason-burks [accessed on 25 April 2010]
156. Convicted Computer Hackers. Available from: http://www.listafterlist.com/tabid/57/listid/8002/The+Web/Convicted+Computer+Hackers.aspx [accessed on 25 April 2010]
157. Sterling B. *The Hacker Crackdown*, Indypublish.com: McLean, VA, 2002: **39**.
158. Robson G.D. The Origins of Phreaking. Blacklisted! 411. April 2004. Available from: http://www.robson.org/gary/writing/phreaking.html. Retrieved 2008-06-21. [accessed on 25 April 2010]
159. Schenker L. Pushbutton Calling with a Two-Group Voice-Frequency Code, The Bell system technical journal 1960; **39**(1): 235–255. Available from: http://www.alcatel-lucent.com/bstj/vol39-1960/articles/bstj39-1-235.pdf
160. Phreaking. Available from: http://www.absoluteastronomy. com/topics/Phreaking [accessed on 25 April 2010]
161. Jagatic T, Johnson N, Jakobsson M, and Menczer F. Social Phishing. Communications of the ACM. October 2007. Available from: http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf [Retrieved on 3 June 2006]
162. Koon T. Phishing and Spamming via IM (SPIM). Internet Storm Center. 2006. Available from: http://isc.sans.org/diary.html?storyid=1905 [retrieved on 5 December 2006]
163. Felix J, Hauck C. System security: a hacker's perspective. *Interex Proceedings*, 1987; **1**: 6.
164. Identity theft. Available from: http://en.wikipedia.org/wiki/Identity_theft [retrieved on 25 April 2010]
165. Paget F. Identity Theft. McAfee White Paper January 2007. Available from: http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf

166. Leyden J. Trojans fuel ID theft boom. January 2007. Available from: http://www.theregister.co.uk/2007/01/16/mcafee_id_theft_trends/ [accessed 25 April 2010]
167. Paget F. Identity Theft. Available from: http://www.docstoc.com/docs/1080365/identity-theft [accessed 25 April 2010]
168. 325 000 names on terror list. Available from: http://www.news24.com/World/News/325-000-names-on-terror-list-20060215 [accessed 25 April 2010]
169. Finkelhor D. Current Information on the Scope and Nature of Child Sexual Abuse. *Future of Children* (Sum-Fall 1994); **4**(2): 31–53.
170. Hume M. Child porn is being 'normalised' by panic merchants. *The Times*. January 12, 2004.
171. Wolak J, Finkehor D, Mitchell K, Ybarra M. Online "Predators" and Their Victims. *American Psychologist* February 2008; **63**(2): 111–128.
172. Wolak J, Finkelhor D, Mitchell K, Ybarra ML. Online "predators" and their victims: Myths, realities, and implications for prevention and treatment. *American Psychologist* 2008; **63**(2): 111–128.
173. Online gambling. Available from: http://en.wikipedia.org/wiki/Online_gambling#cite_note-9 [accessed 25 April 2010]
174. Legality of online gambling. Available from: http://www.worldlawdirect.com/article/2010/legality-online-gambling.html [accessed 25 April 2010]
175. Humphrey C. Advertising Internet Gambling. Available from: http://www.gambling-law-us.com/Articles-Notes/advertising-online-casinos.htm
176. Arrest of Sportingbet Chairman. Available from: http://www.casinomeister.com/news/sept2006/online_casino_news2/ARREST_OF_SPORTINGBET_CHAIRMAN.php [accessed 25 April 2010]
177. Problem Gambling Information. Available from: http://www.npgaw.org/problemgamblinginformation/factsfigures.asp [accessed 25 April 2010]
178. Carozza D. Interview with Ros Wright: UK's Resolute Fraud-Fighting Advisor. July/August 2007. Available from: http://www.fraud-magazine.com/article.aspx?id=570 [accessed 25 April 2010]
179. Wardle H, Sproston K, Orford J, Erens B, Griffiths M, Constantine R, Pigott S. British Gambling Prevalence Survey 2007. Available from: http://www.rga.eu.com/data/files/070919_gambling_prevalence_survey_exec_summ.pdf
180. Bocij P. *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. Praeger, 2004; **14**.
181. Maughan L. What Is The Legal Definition Of Harassment? Available from: http://www.life123.com/career-money/career-development/harassment/definition-of-harassment.shtml [accessed 25 April 2010]
182. Royakkers L. The Dutch Approach to Stalking Laws. California Criminal Law October 2000 Vol.**3**. Available from: http://boalt.org/CCLR/v3/v3royakkers.PDF
183. Press S. Fighting Cyberstalking. Available from: http://www.jahitchcock.com/cyberstalked/skippress.htm [accessed 25 April 2010]
184. McFarlane L, Bocij P. An exploration of predatory behavior in cyberspace: Towards a typology of cyberstalkers. First Monday, September 2003; **8**(9).
185. Cyberstalking. Available from: http://www.ncvc.org/ncvc/main.aspx?dbName=DocumentViewer&DocumentID=32458 [accessed 25 April 2010]
186. Moravekj D. Social Networks - The Change of Communication Paradigm 2008. Available from: http://noebius.com/pdf/moravek-social-networks-part1.pdf
187. Baranetsky V. What is cyberterrorism? Even experts can't agree. Harvard Law Record, 2009. Available from: http://ww0w.hlrecord.org/news/what-is-cyberterrorism-even-experts-can-t-agree-1.861186 [accessed 25 April 2010]
188. Wickramarathna W. Defining cyber terrorism. Available from: http://www.i-policy.org/2009/07/defining-cyber-terrorism.html [accessed 25 April 2010]
189. Cyber Crime And Its Consequences: Introduction to Cyber Crime. Available from: http://airwebworld.com/articles/index.php?article=870#sdfootnote9sym [accessed 25 April 2010]
190. Cross M, Shinder DL. Scene of the Cybercrime. *Syngress*, 2008; **415**.
191. Cyberterrorism: What's The Worst Case Scenario? Available from: http://blog.zonealarm.com/2011/01/cyberterrorism-whats-the-worst-case-scenario.html [accessed on 25 April 2010]
192. Hackers Launch Massive Attack on Ukrainian President's Web Site. Available from: http://www.foxnews.com/story/0,2933,306438,00.html [accessed on 25 April 2010]
193. Kane S. Trade Secret. Available from: http://legalcareers.about.com/od/glossary/g/Tradesecret.htm [accessed 25 April 2010]
194. Trade Secret. Available from: http://en.wikipedia.org/wiki/Trade_secret [accessed 25 April 2010]
195. Trade Secret. Available from: http://www.absoluteastronomy.com/topics/Trade_secret [accessed 25 April 2010]
196. Pendergrast M. *For God, Country & Coca-Cola*. Basic Books: New York, 2000; **456**.
197. Perez JC. Viacom Demands Video Removal From YouTube. Available from: http://www.pcworld.com/article/128753/viacom_demands_video_removal_from_youtube.html [accessed 25 April 2010]
198. Spam (Monty Python). http://en.wikipedia.org/wiki/Spam_(Monty_Python) [accessed 25 April 2010]

199. Ollmann G. The phishing guide: understanding and preventing phishing attacks. Technical Info. 2006. Available from: http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf [retrieved on 10 July 2006]
200. Kirk J. Phishing scam takes aim at MySpace.com. IDG Network. 2006. Available from: http://www.pcworld.com/article/id,125956-page,1/article.html?RSS=RSS [retrieved from 2 June 2006]
201. Available from: http://www.nytimes.com/2007/07/19/us/19sex.html? [retrieved on 20 June 2008]
202. Available from: http://www.ecpat.net/fr/Ecpat_inter/projects/monitoring/WC1/child_porn.asp [retrieved on 20 June 2008]
203. Available from: http://www.guardian.co.uk/media/2006/jul/18/newmedia.gambling [retrieved on 20 June 2008]
204. Available from: http://www.usatoday.com/news/washington/2006-10-13-bush-bill_x.htm [retrieved on 20 June 2008]
205. Available from: http://www.house.gov/apps/list/hearing/financialsvcs_dem/ht060807.shtml [retrieved on 20 June 2008]
206. Available from: http://uk.reuters.com/article/InternetNews/idUKL3047306520070330 [retrieved on 20 June 2008]
207. Available from: http://www.bbc.co.uk/caribbean/news/story/2007/06/070620_antwto.shtml [retrieved on 20 June 2008]
208. Pendergrast M. *For God, Country & Coca-Cola*, Basic Books: New York, 2000.