Capitol v. Thomas
Expert witness report by Dr. Yongdae Kim, Ph.D.

March 3, 2009

1 Overview

This report addresses the overall problem of identifying computers remotely through the Internet, the nature and extent of material errors in the expert witness report and testimony of plaintiff expert witness Dr. Jacobson, the nature and extent of inconsistencies in the evidence provided by MediaSentry, and of alternate explanations for evidence presented by the plaintiff. All these issues will be addressed in my testimony.

2 Alternative explanations for evidence presented at the trial

2.1 Summary

The FastTrack network, and the KaZaA software in particular, presents a large unknown to the academic community. There have been very few studies of the network, the behavior of its users, and the security of the underlying protocols. Moreover, the availability of "custom" (altered) KaZaA clients such as KaZaA Lite [2] suggests that it is possible to design a custom FastTrack client that could affect the functionality of the network in unpredictable ways. Combined with the lack of rigor and opacity of MediaSentry's methods, the ability to track the activity of an individual computer participating in the network is uncertain. There are many alternative explanations that conflict with MediaSentry's claim of a particular computer being involved in copyright infringement, including Internet misconfiguration and/or instability, malicious activity of other Internet users or providers, malicious activity by software installed on the defendant's computer, or potential faults in MediaSentry's information-gathering software and a lack of error checking controls.

2.2 Existing knowledge about the KaZaA network

In terms of measurement, peer-to-peer (P2P) technology is relatively new, and not a great deal of information exists about the specific behavior of any given network. Even less is known about KaZaA than other networks since the software and protocols are entirely proprietary. More recent protocols have also cooled any academic interest in the FastTrack network. With the exception of a few studies [16, 17] consulted for this report, not much information exists about the FastTrack network, the behavior of its users, or the KaZaA Media Desktop software. Therefore, making scientifically-based statements about the behavior of a particular user of the FastTrack network is difficult to impossible.

MediaSentry claims to have much experience in identifying individual committing copyright infringement. However, they insist that their methods are proprietary and thus cannot be subject to scrutiny by an impartial third party. No academic studies exist of their internal investigative techniques, methods, software, data collection practices, or even employee training in retaining collected data in a way that would allow for it to be used as evidence at a trial. While this report will address specific methodology questions at a later time, it suffices to say for the moment that MediaSentry's claims of their ability to record activity on the FastTrack network and identity individual computers used to commit copyright infringement are not only unproven, but highly unlikely to be accurate. Combined with the incentive to accuse as many users as possible due to both the supposed deterrent effect on file sharing and the likely per-user compensation scheme that may exist between the Recording Industry Association of America (RIAA) and MediaSentry, their allegations are highly suspect.

2.3 Ability to identify users from the actions traced back to personal computers

As much as we would like to be able to determine the identity of a computer used to perform any given action on the Internet, such technology does not exist – no method of identification is foolproof. Nothing exemplifies this better than banking and credit card web sites, which use any combination of browser "cookies", SSL certificates, custom image tagging, Flash- and JavaScript-based login systems, and even custom software installed on end-users' computers. However, the number of attacks where users are duped into believing that a random malicious computer is their bank's web site (called "phishing" attacks) has not decreased, bur rather increased in recent years. Moreover, the interaction between the bank's and user's computers takes place over a mature and well-understood protocol with built-in security features (SSL/TLS). Therefore, it would be quite difficult to determine the identity of a computer communicating over a protocol that uses untested or no encryption, is proprietary in nature, and has had no significant academic or other impartial review.

Due to the plaintiff's own allegations that peer-to-peer networks are nothing more than havens for illegal activity, we would expect anyone committing copyright infringement or other crimes to want to mask their trail when using these systems. This is especially true during the RIAA's highly-publicized legal campaign against copyright infringers. Malicious users have great incentive to attempt to either hide or displace blame for their actions onto a third party. Additionally, while malicious users have significant resources and knowledge at their disposal, few typical Internet users have the skill to protect themselves form these threats, and few Internet service providers (ISPs) worry about the security of their users.

2.4 Vulnerabilities of Internet-connected personal computers

A miscreant wishing to cover his or her tracks on the Internet has many options, the most likely of which is direct exploitation of one or more computers owned by a third party. Those computers can then be used for activity that the malicious party would not want linked to his or her Internet account. The average uninfected "life expectancy" of an Internet-connected computer running the Microsoft Windows XP operating system without any security updates ("patches") is as low as 4 minutes [15]. Since all Windows XP systems attempt to connect to the Internet immediately upon installation/first boot, and since it requires some time to download all security updates from Microsoft (which, for a newly-installed Windows XP system, can measure in gigabytes, with a typical Internet connection only capable of handling a few megabytes per second), it would not be surprising that any given Internet-connected Windows XP computer be infected with any number of pieces of "malware" (software malicious to the user of the computer on which it is installed).

By way of example, we present the following statistics concerning security advisories about software that was present, or was alleged to be present, on the defendant's computer. Note that advisories are vulnerabilities that are known *at the time*. Other vulnerabilities may have existed that had been reported in later years, or not at all. Occasionally software companies will repair multiple vulnerabilities with a single update, without informing their clients about the specific vulnerabilities a given update is meant to address. Thus, vulnerability statistics give strictly a lower-bound on the vulnerability of a given system or collection of software.

Statistics for Windows XP Home Edition, 2003-2005:

- 2003: of 29 advisories, 34% were highly critical, 41% were remotely exploitable, 21% remained unfixed, 46% allowed for system-level (maximal) access
- 2004: of 28 advisories, 36% were highly critical, 75% were remotely exploitable, 22% remained unfixed or only partially patched, 50% allowed for system-level (maximal) access
- 2005: of 36 advisories, 28% were highly critical and 34% extremely critical, 19% remained unfixed, 61% were remotely exploitable, 55% allowed for system-level (maximal) access

To date, 13% of all Windows XP Home advisories remain unfixed [10].

Statistics for Internet Explorer version 6, 2003-2005:

- 2003: of 24 advisories, 35% were highly critical and 12% extremely critical, 100% were remotely exploitable, 12% remained unfixed or only partially patched, 35% allowed for system-level (maximal) access
- 2004: of 35 advisories, 26% were highly critical and 14% extremely critical, 97% were remotely exploitable, 27% remained unfixed or only partially patched, 50% allowed for system-level (maximal) access
- 2005: of 17 advisories, 35% were highly critical and 12% extremely critical, 35% remained unfixed, 100% were remotely exploitable, 36% allowed for system-level (maximal) access

To date, 26% of all Internet Explorer version 6 advisories remain unfixed [10].

Statistics for KaZaA version 2, 2003-2005:

- 2003: of 2 advisories, 50% were highly critical, 50% remained unfixed, 100% were remotely exploitable, 50% allowed for system-level (maximal) access
- 2004: of 1 advisory, 100% were highly critical, 100% remained unfixed, 100% were remotely exploitable, 100% allowed for system-level (maximal) access

To date, 75% of all KaZaA 2.x advisories remain unfixed [10].
Similar statistics can be provided for other software.

It is possible that that a remote attacker, exploiting a Windows or other software vulnerability to obtain access, would use someone's computer to download or store music. The computer could have also been used to send SPAM or serve hostile Internet content.

Windows passwords do not protect the computer from tampering, and offer only minimal resistance to even a mildly knowledgeable adversary with either local or remote access to the computer. It is also likely that Ms. Thomas routinely left herself logged in without locking her screen. Even assuming that Ms. Thomas was consistent in logging out of her account when not in use, weak passwords[1] would make breaking in trivial. Moreover, passwords do not protect against exploitation of software vulnerabilities.

2.5 IP and MAC address spoofing and hijacking

An alternative method of appearing to be someone else on the Internet is to spoof their IP address through a number of means. Many of them are enumerated below, some including historical examples.

Using unprotected wireless access point

A neighbor or anyone passing by an unsecured ("open") wireless access point may connect and use the associated Internet account either for simple access or for more nefarious reasons. People who wish to engage in illegal activity often look for unprotected wireless network access points from which to connect to the Internet. This is usually quite effective in hiding their tracks, and leads investigators to the owner of the wireless access point.

Spoofing the modem MAC and/or IP address

Spoofing an IP address and even MAC address on the same Charter network segment is trivial, if Charter provides cable-based Internet service. While DSL subscribers have dedicated (private) paths from their DSL modems to the DSL provider substation, cable-based Internet subscribers "share" paths in a given part of the network with their neighbors. Sometimes this shared traffic is filtered by the cable modem, sometimes it is not. Even if filtering is in place, it is usually trivial to reprogram the modem. Traffic over local network segments tends to be unencrypted, and thus all information from one customer is visible to all others. This could lead to spoofing to either obtain free Internet service, to disguise the source of illegal activity, or frame a user of the service for another user's actions. If Ms. Thomas' computer was usually turned on, this sort of spoofing

[1] Passwords that are easily guessable based on the knowledge of a person (such as their child's name), passwords composed of fewer than six or eight characters, passwords that only contain lower-case letters are all considered weak (easy to guess).

may have caused problems with Charter's internal network management. It is more likely for this to happen when Ms. Thomas' computer is off.

BGP spoofing

IP addresses, or entire IP segments can be stolen outright. This usually occurs by accident, but can be done with malicious intent. The security and stability of IP address assignment and Internet routing infrastructure in general is quite precarious.
Some specific historical examples of misconfiguration are as follows:

- 1997 AS7007 misconfiguration incident "broke" the Internet by overwhelming routers with useless messages [14]
- 2006 Con-Ed incident resulted in temporary, and possibly malicious, reassignment of a number of important Internet "prefixes" (address blocks) [21]
- 2008 Pakistan Telecom incident purposely attempted to block access to YouTube from within the country, but instead caused traffic to YouTube to be diverted to Pakistan [11]
- 2009 Czech router misconfiguration incident triggered by two Cisco[2] IOS[3] bugs "broke" the Internet by causing many routers to repeatedly connect and disconnect, flooding neighboring routers with control messages [23, 22]

Examples of malicious usage of Internet routing infrastructure:

- Hijacking of "black" IP space – malicious users will "announce" ownership of unassigned IP addresses. This imposes minimal to no instability on the routing infrastructure of the Internet.
- Hijacking of temporarily unused space – malicious users will announce ownership of IP addresses they know to be idle (either the computers connected to them are turned off or the addresses are not used by their rightful owner). This imposes minimal to no instability on the routing infrastructure of the Internet.
- Hijacking of used space – malicious users will announce "better" paths to a given IP address or block of addresses. Depending on the skill of the adversary, this situation may be stable but routing results may differ based on source/destination points. While this imposes some instability (or at least unexpected behavior), it is difficult to prevent or stop this type of attack.

Most providers do not sanity-check announcements from other providers, making all of the attacks above easy to carry out and difficult to detect. There is no technological means currently in use to stop IP spoofing, although theoretical solutions exist. Manual intervention is needed to contain the problem at most ISPs, and the problem source must correct the problem in order to achieve a permanent solution. The latter usually required contacting the problem source directly if they do not realize they have caused this event.

[2] A large router manufacturer
[3] Cisco's router operating system

An attacker wishing to appear as coming from a given IP address can announce a route to that address that is more specific than other routes ("prefix hijacking") [18]. This situation would cause more than one computer connected to the Internet to have the same IP address, contrary to Dr. Jacobson's testimony. While a traceroute would show the path to the attacker rather than the victim of spoofing, the traceroute provided by MediaSentry is not time-stamped – it could have been collected at any time before or after the alleged infringement. The date of data collection is thus unknown, and may bear no relationship any logs collected by MediaSentry at the time of the alleged infringement.

A "man-in-the-middle" malicious framing attack can be mounted using BGP spoofing, and the attacker would show up in a traceroute. Any of the entities located on the Internet path between MediaSentry and the alleged file sharer could have perpetrated this attack [20]. Unfortunately, we do not know if the intermediaries in MediaSentry's traceroute were the intermediaries at the time of the alleged infringement due to the previously-mentioned lack of a timestamp in the traceroute file.

2.6 Other malicious framing

A KaZaA super node would have the ability to frame any of its child nodes, since it keeps their song indexes and replies to search requests with the metadata, as well as the child node IP address. A malicious super node could return successful search results, then point the searcher to a confederate who pretends to be a child node, offering songs for download. These downloaded songs may either be "garbage", may have correct metadata but garbage data, or may be entirely correct. Moreover, the availability of "custom" (altered) KaZaA clients such as KaZaA Lite [2] suggests that it is possible to design a custom FastTrack client that could affect the functionality of the network in unpredictable ways.

The following are excerpts from one of the few papers examining the possibility of malicious framing of arbitrary Internet-connected devices for copyright infringement and the success and failure rates of entities like MediaSentry [19]:

- "Copyright holders utilize inconclusive methods for identifying infringing BitTorrent users. We were able to generate hundreds of DMCA takedown notices for [computers] under our control . . . that were not downloading or sharing any content."

- "To sample our results, based on the inconclusive nature of the current monitoring methods, we find that it is possible for a malicious user (or buggy software) to implicate (frame) seemingly any network endpoint in the sharing of copyrighted materials. We have applied these techniques to frame networked printers, a wireless (non-NAT) access point, and an innocent desktop computer, all of which have since received DMCA takedown notices but none of which actually participated in any P2P network."

- [Attack] possibilities include man-in-the-middle (both at the IP and overlay level) and malware present on the victim's computers.

2.7 Defendant's hard drive

Dr. Jacobson provided only minimal details on the status of security and virus/spyware protection of the defendant's hard drive. Nor was there any mention whether any malware infections were found on the drive. This issue requires further study to determine the actual vulnerability of that computer to threats from the Internet, and I am continuing my investigation. The results will be provided as soon as practicable.

3 Problems with Dr. Jacobson's expert witness report

3.1 Summary

Dr. Jacobson's expert witness and supplemental reports contain multiple factual errors and mis-statements of fact regarding the technologies relevant tothis case, and show evidence of faulty logic in making conclusions. Dr. Jacobson not only does not consider *any alternative explanations* for the log data provided by MediaSentry other than what is alleged by the plaintiff, but also fails to definitively bridge the gap between the evidence presented by MediaSentry and the identity of the computer used in the alleged infringement.

3.2 Postal system analogy

Dr. Jacobson draws the dubious analogy between the postal system and the Internet. This analogy is not only flawed in several respects, but provides the illusion of intuitive understanding of Internet technologies that is simply false. If we were to use that analogy, we must first assume that all letters travel in fully transparent envelopes. Second, that there are several postal stations between source and destination, and the postmaster at each station can re-write the letter in any way without being detected.[4] Furthermore, the postmaster at any intermediate location the letter visits would be able to write a new letter from scratch and send it to a destination, faking the return address. All letters in response to the forged letter would be intercepted by our malicious postmaster, while the person on the other side of the exchange believes themselves to be corresponding with a person at another address altogether. This is called the "man-in-the-middle" (MITM) attack. This report has already mentioned the possibility that such an attack was carried out.

The analogy between networks and zip codes is also lacking, since it does not convey the ability of malicious postal operators to steal a chosen zip code and redirect all mail bound for addresses contained within it, nor does it allow for the potentially malicious movement of addresses between zip codes. Finally, it does not allow for the outright creation of zip codes, complete with fictitious addresses. All these events are difficult to detect and even more difficult to prevent.

The purpose of the above description is not to confuse anyone, but rather to show that the analogy Dr. Jacobson provided is dangerous in the sense that it conveys a great simplicity and determinism to the way the Internet works. This is not the case, and so we must drop this analogy

[4] This is not strictly true when cryptographic end-to-end integrity checks are in place, but we are dealing with generalities for now.

altogether lest it affects our thinking about the *actual* technologies involved in this case. Therefore, let us drop the faulty analogy and move on.

3.3 (non)Uniqueness of IP addresses

The statement that IP address assignments must be unique throughout the Internet is simply false. Contrary to Dr. Jacobson's insinuations that IP address assignments are somehow enforced, most Internet providers do not check whether someone on their network is sending traffic from IP addresses that do not belong to that provider. Additionally, malicious providers may advertise ownership of IP addresses that are either unassigned, are assigned to other providers but are not in use, or are both assigned to others and in use. Although IP address allocation *is* handled by centralized entities (in a hierarchical fashion), it is sometimes unclear who "owns" a given IP address at any given time [12, 13]. This report has already mentioned the manner in which IP addresses can be rendered non-unique through hijacking.

Throughout his expert report, Dr. Jacobson makes a number of unfounded logical leaps. For instance, he continually refers to users, Internet-connected computers, and IP addresses interchangeably. For instance, in section 13, Dr. Jacobson states that a user is identified by his or her IP address. This is not correct. In addition to the possible non-uniqueness of IP addresses mentioned above, a single IP address may be the location of a network address translation (NAT) device or a company firewall and web proxy, which allows a single Internet-visible IP address to be shared among many computers. Additionally, many computers come with software and hardware to share Internet access with other devices by providing NAT functionality themselves, without any additional physical devices. In short, while an IP addresses identifies an Internet *end-point*, the Internet is a hierarchical entity. The very word "Internet" implies a collection of many networks. Thus an Internet-visible IP address may be a single device, or a gateway to another network with a few, or dozens, or hundreds, or thousands of devices.

In his expert witness report, Dr. Jacobson states that a computer with a given IP address contained many copyrighted music files. In fact, what MediaSentry's logs show is file metadata, and no more than 11 (out of 1702) actual files which were downloaded and examined by a listener and can be definitively said to contain music. Dr. Jacobson concludes that music found on the *defendant's* computer was downloaded from the Internet. There is no evidence that files on the defendant's hard drive were downloaded from the Internet, but rather evidence points to them being "ripped" from CDs the defendant owns. So, Dr. Jacobson's conclusions are unfounded since no link between music files, an IP address, or a computer was conclusively shown.

3.4 "The" KaZaA share directory

Dr. Jacobson makes frequent references to *the* share directory. However, this is a mis-statement. While a single share directory exists, all directories added to KaZaA as directories containing media files will be shared by default, and therefore any remote user viewing a "shared" directory will be viewing the contents of a number of directories, not all of them necessarily meant to be shared by the user. KaZaA can be used as a media player, but in order to use it as such, media directories must first be added to a list in the KaZaA preferences. All files on that list are shared by default.

There is no evidence that the files observed by MediaSentry were consciously placed in a "shared" directory or willfully offered for distribution. Dr. Jacobson draws an analogy between putting music in a shared folder of a file-sharing application and publishing a list of songs and advertising that everyone is welcome to a copy. A more apt analogy is leaving music by an open window, so that anyone peeking in may come inside and copy a given piece of music. The user in question may not realize that the music is visible to others, and may not expect any copying to take place. In short, any publication of lists of owned music may simply be accidental.

4 Problems with MediaSentry procedures

4.1 Summary

There is currently no impartial information regarding the operating details of MediaSentry's software or staff. The company is not known to hold a private investigator license in any state [3, 4, 5, 6, 7, 8, 9], and there is no evidence that it employs staff who are familiar with procedures for gathering evidence for a trial. Furthermore, MediaSentry's faulty data collection has lead to multiple embarrassing episodes, such as lawsuits brought against persons who did not have Internet accounts at the time of the alleged infringement, persons whose homes were in a state of ruin at the time of the alleged infringement, and persons who do not even own computers [1]. There are multiple reports from service providers about requests for release of information about IP addresses which are not even owned by the provider in question [12, 13]. In light of this evidence of improper error checking and lack of transparency, it is impossible to place any trust in evidence or testimony from MediaSentry.

4.2 Proper collection and storage of evidence

Any of the information MediaSentry provided can be manufactured with no prior knowledge and without using the KaZaA network (except for the username/IP address match). Of the 6 exhibits provided by MediaSentry (logs and screenshots), 4 do not record the date they were collected. There is no indication that any rigorous storage process, as behooves evidence to be used in a trial, was used to store the data, and no indication of any kind of internal procedures or review designed to uncover errors in data collection software. I am not aware of any impartial external review of MediaSentry's collection procedures, and there are multiple reports of errors made by MediaSentry in determining the network-level identities of copyright infringers.

4.3 Reports of false copyright infringement notices from MediaSentry

There are two distinct time periods when the "unisog" mailing list[5] held discussions about reports of copyright infringement inbound from MediaSentry. Of 23 network administrators commenting on the matter, 3 reported receiving legitimate notices and 13 reported receiving anywhere

[5] "The unisog mailing list is intended for university and other academic institution system operators to discuss security issues specific to the academic environment."

from a single notice to a large number of notices that could not have been correct, since the IP addresses referenced were either not routable from the open Internet, were not in use at the time, belonged to computers that were offline at the time of the alleged incident, or were not even assigned to the organizations receiving the complaints [12, 13]. One of the discussions took place in January 2005 – very near to the time of the defendant's alleged file sharing activity [13]. These discussions indicate that MediaSentry's methods are lacking even the most basic of error control and mitigation procedures. This is especially troubling since the majority of persons contacting MediaSentry about the problem received no response. It is possible that MediaSentry has since corrected the particular errors that caused those reports to be generated. It is likewise possible that the errors are persistent and represent a complete lack of internal controls at MediaSentry. Without a systematic impartial review, we can never know.

4.4 KaZaA-reported IP address and possible IP spoofing

The KaZaA-reported IP address is not evidence that the machine running KaZaA is not behind a NAT device. KaZaA software includes technology that allows it to bypass firewalls and NATs, mainly through the use of super nodes. A super node can easily supply the KaZaA client with its externally-visible IP address. I could not verify this as I do not have source code access to the KaZaA client, nor could I get access to a functioning version to observe its behavior. Data collection is ongoing and results will be provided as soon as practicable.

Relating to improper evidence collection procedures, we are unable to determine if the traceroute submitted by MediaSentry was performed at the time of the alleged infringement, as no date appears in the data file. If the traceroute was collected at a different time, it would not show any evidence of IP spoofing that may have occurred at the time of the alleged infringement.

5 Conclusion

From the material considered in this report, I conclude that there is not one but numerous possible explanations for the evidence presented during this trial. Throughout the report I demonstrate possibilities not considered by the plaintiff's expert witness in his evaluation of the evidence. Additionally, the plaintiff's expert witness made numerous mis-statements as to the technologies involved in this case, as indicated above, and failed to to draw a reliable conclusion connecting the defendant's computer with the alleged copyright infringement activities. Moreover, MediaSentry has a strong record of mistakes when claiming that particular IP addresses were the origins of copyright infringement. Their lack of transparency, lack of external review, and evidence of inadequate error checking procedures puts into question the authenticity and validity of the log files and screenshots they produced.

6 Author's qualifications

(See Appendix A)

7 Full disclosure

I have been asked by the defending counsel for my opinion on alternative explanations of evidence presented by the plaintiff and the accuracy of the technical statements made by the plaintiff's witnesses, and to testify at the trial regarding my findings. These services are rendered for a flat fee of $3,000 provided by the Free Software Foundation (FSF).

8 Materials consulted

The documents considered in the preparation of this report includes the following:

Uncited documents

- Virgin Records, et al v. Thomas court transcript
- All Virgin Records, et al v. Thomas plaintiff exhibits
- Virgin Records, et al v. Thomas affidavit and expert report of Dr. Doug Jacobson, Ph.D., CFCE
- Virgin Records, et al v. Thomas supplemental declaration and expert report of Dr. Doug Jacobson, Ph.D., CFCE
- Forensic copy of defendant's hard drive

Cited Documents

[1] Index of litigation documents. http://recordingindustryvspeople.blogspot.com/2007/01/index-of-litigation-documents.html.

[2] KaZaA Lite. http://www.zeropaid.com/kazaalite/.

[3] Pike & Fischer Internet & Law Regulation. http://www.ilrweb.com/viewILRPDF.asp?filename=arista_does1-21_080204DeftsSupplementalMemorandum.

[4] Pike & Fischer Internet & Law Regulation. http://www.ilrweb.com/viewILRPDF.asp?filename=michigan_mediasentry_080222.

[5] Pike & Fischer Internet & Law Regulation. http://www.ilrweb.com/viewILRPDF.asp?filename=umg_delcid_070601AnswerCounterclaims.

[6] Pike & Fischer Internet & Law Regulation. http://www.ilrweb.com/viewILRPDF.asp?filename=lava_amurao_080128DeftsInLimineMotMemoLaw.

[7] Pike & Fischer Internet & Law Regulation. http://www.ilrweb.com/viewILRPDF.asp?filename=lava_amurao_080128DeftsMotExcludeMediaSentryDeposeOppenheimCompelExpenseDiscov.

[8] Pike & Fischer Internet & Law Regulation. http://www.ilrweb.com/viewILRPDF.asp?filename=arista_does1-17_071128ReplyMemorandum.

[9] Pike & Fischer Internet & Law Regulation. http://www.ilrweb.com/viewILRPDF.asp?filename=arista_does1-17_071128ReplyAffidavit.

[10] Secunia advisories - vulnerability information - secunia.com. http://secunia.com/advisories.

[11] YouTube Hijacking: A RIPE NCC RIS case study. http://www.ripe.net/news/study-youtube-hijacking.html.

[12] unisog – UNIversity Security Operations Group. http://lists.sans.org/pipermail/unisog/2004-April/, April 2004.

[13] unisog – UNIversity Security Operations Group. http://lists.sans.org/pipermail/unisog/2005-January/, January 2005.

[14] Vincent J. Bono. 7007 explanation and apology. http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html.

[15] Lorna Hutcheson. Survival time on the Internet. http://isc.sans.org/diary.html?storyid=4721.

[16] Jian Liang, Rakesh Kumar, and Keith W. Ross. The KaZaA overlay: A measurement study. *Computer Networks*, 2005.

[17] Jian Liang, Rakesh Kumar, Yongjian Xi, and Keith W. Ross. Pollution in P2P file sharing systems. In *INFOCOM*, 2005.

[18] Christian McArthur and Mina S. Guirguis. Stealthy IP prex hijacking: Don't bite off more than you can chew. In *SIGCOMM*, 2008.

[19] Michael Piatek, Tadayoshi Kohno, and Arvind Krishnamurthy. Challenges and directions for monitoring P2P file sharing networks–or–why my printer received a DMCA takedown notice. In *HotSec*, 2008.

[20] Alex Pilosov and Tony Kapela. Stealing the Internet: An Internet-scale man in the middle attack. In *Defcon*, 2008.

[21] Todd Underwood. Con-Ed steals the 'Net. http://www.renesys.com/blog/2006/01/coned-steals-the-net.shtml.

[22] Earl Zmijewski. Longer is not always better. http://www.renesys.com/blog/2009/02/longer-is-not-better.shtml.

[23] Earl Zmijewski. Reckless driving on the Internet. http://www.renesys.com/blog/2009/02/the-flap-heard-around-the-worl.shtml.

Signature and date

Date: 03/02/2009

Signature: Yongdae Kim

A Author's qualifications

Yongdae Kim

Work Address:

Department of Computer Science & Engineering
University of Minnesota
4-192 EE/CS Building, 200 Union St. SE
Minneapolis, MN 55455
Phone: (612) 626-7526
Fax: (612) 625-0572
Email: kyd@cs.umn.edu
URL: http://www.cs.umn.edu/~kyd

EDUCATION

Ph.D	**Computer Science, University of Southern California.** May 2002. Thesis Title: *Group Key Agreement: Theory and Practice* Thesis Advisor: Gene Tsudik and B. Clifford Neumann
M.S.	**Mathematics, Yonsei University, Seoul, Korea**, Feb. 1993 Advisor: Chul Kim
B.S.	**Mathematics, Yonsei University, Seoul, Korea**, Feb. 1991

RESEARCH INTERESTS

General	Network and Distributed System Security, Applied Cryptography
Current Focus	Peer-to-peer systems: Secure and robust routing, Accounting, Access Control Mobile and Wireless Ad-hoc Networks: Secure routing, Key management Sensor Networks: Secure routing, Key management, Physical Security Internet: Secure routing Storage Systems: Confidentiality and Integrity, Access control Applied Cryptography: Group Key Management, Digital Signatures, Timed-release Cryptography

WORK EXPERIENCE

9/2008 – Present	**Department of Computer Science, University of Minnesota, Twin Cities** Associate Professor
7/2006 – 6/2008	**Department of Computer Science, University of Minnesota, Twin Cities** McKnight Land-Grant Professor
8/2002 – 8/2008	**Department of Computer Science, University of Minnesota, Twin Cities** Assistant Professor
1/2001 – 7/2002	**Department of Information and Computer Science, University of California at Irvine** Visiting Researcher
9/1998 – 12/2000	**Department of Computer Science, University of Southern California** Graduate Research Assistant
2/1993 – 8/1998	**Electronics and Telecommunication Research Institute**, Daejon, Korea Member of Research Staff

AWARDS AND HONORS

7/2006	**McKnight Land-Grant Professorship** Award University of Minnesota, Twin Cities
3/2005	**NSF CAREER Award**

PHD STUDENTS

Chunhui Shi	current
Denis Foo Kune	current
Hun J. Kang	
Eugene Vasserman	Coadvisor: Nick Hopper
Peng Wang	Thesis: *Secure Routing for Distributed Hash Table*, Spring 2008
Vishal Kher	Thesis: *Secure Authorization and Accounting for Distributed Storage*, Oct. 2007
Mark Shaneck	Thesis: *Privacy Preserving Nearest Neighbor Search and its Applications* (Coadvisor: Vipin Kumar), Jul. 2007
Joengmin Hwang	Thesis: *In-Situ Modeling on Sensing Coverage and Location Proof* (Coadvisor: Tian He), Jul. 2007
Ivan Osipkov	Thesis: *Securing Decentralized Peer-to-Peer Systems*, May. 2007

MS STUDENTS

J. Tyra	*Security of Kad Distributed Hash Table*, current
K. Mahadevan	*Self Diagnosing Sensor Networks*, Fall, 2007
S. Hong	*Encrypted File System*, Fall, 2006
J. Kim	MCS, Spring, 2006
K. Do	*Group Key Management with Flash Crowd*, Summer, 2004
B. Pokorney	*Group Key Management*, Spring, 2004

TEACHING

CSci 5471 **Modern Cryptography**

Designed in 2003, Offered four times. This course serves as a graduate-level introduction to cryptography, covering fundamental mathematical concepts of cryptography, application of cryptography to computer systems. The course requires students to do an independent group research project as well as problem solving assignments and exams.

CSci 8271 **Security and Privacy in Computing**

Designed in 2003, offered three times, The intent of this course is to prepare students to do research in the field of security, by surveying the fundamental papers in the area and teaching the major techniques employed by modern security research. The course requires students to do an independent group research project as well as assignments and exams.

CSci 5271 **Introduction to Computer and Network Security**

Co-designed with Nick Hopper. Offered twice by Nick Hopper. This rigorous graduate course introduces students to principles of computer security and surveys a wide range of topics, including software security, operating systems security, cryptography, and network security. Students complete a course project along with several programming and non-programming homework designed to supplement the lecture topics.

REFEREED JOURNAL PUBLICATIONS

1. J. Hwang, T. He, **Y. Kim**, *Secure Localization with Phantom Node Detection*, Ad Hoc Networks, Elsevier, 2007.

2. J. Cheon, N. Hopper, **Y. Kim**, I. Osipkov, (alphabetical order. Main author of the paper is I. Osipkov.) *Provably Secure Timed-Release Public Key Encryption*. ACM Transactions on Information Systems Security, 2007.

3. A. Jaiswal, **Y. Kim**, M. Gini, *Design and implementation of a secure multi-agent marketplace*, Electronic Commerce Research and Application, Volume 3, Issue 4, Winter, Elsevier Science, 2004

4. Y. Amir, **Y. Kim**, C. Nita-Rotaru, G. Tsudik, *On the Performance of Group Key Agreement Protocols*, ACM Transaction on Information and System Security, Vol. 7, No. 3, Aug. 2004.

5. Y. Amir, **Y. Kim**, C. Nita-Rotaru, J. Schultz, J. Stanton, G. Tsudik, *Robust Contributory Key Agreement in Secure Spread*, IEEE Transaction on Parallel and Distributed System, Vol. 15, No. 5, May 2004.

6. **Y. Kim**, A. Perrig, G. Tsudik, *Communication-Efficient Group Key Agreement*, IEEE Transaction on Computers, Vol. 53, No. 7, Jul. 2004.

7. **Y. Kim**, A. Perrig, G. Tsudik, *Tree-based Group Key Agreement*, in ACM Transaction on Information and System Security, Vol. 7, No. 1, Feb. 2004.

8. **Y. Kim**, F. Maino, M. Narasimha, K. Rhee, G. Tsudik, *Secure Group Key Management for Storage Area Networks*, IEEE Communications Magazine, Vol. 41, No. 8, Aug. 2003.

9. S. Park, **Y. Kim**, and K. Kim, *On the Security of Lin-Chang-Lee Public Key Cryptosystem*, Journal of the Korean Institute of Information Security and Cryptography, 1996.

REFEREED CONFERENCE AND WORKSHOP PUBLICATIONS: Major

1. B. Kang, E. Chan-Tin, C. Lee, J. Tyra, H. Kang, C. Nunnery, Z. Wadler, G. Sinclair, N. Hopper, D. Dagon, and **Y. Kim**, *Towards Complete Node Enumeration in a Peer-to-Peer Botnet*, ACM Symposium on Information, Computer & Communication Security (ASIACCS 2009)

2. P. Wang, J. Tyra, T. Malchow, **Y. Kim**, N. Hopper, D. Foo Kune, and E. Chan-Tin. *Attacking the Kad Network*, at SecureComm 2008.

3. V. Kher and **Y. Kim**, *Building Trust in Storage Outsourcing: Secure Accounting of Utility Storage*, IEEE International Symposium on Reliable Distributed Systems (SRDS), 2007

4. J. Hwang, T. He, **Y. Kim**. *In-Situ Sensing Area Modeling for Wireless Sensor Networks*, ACM Conference on Embedded Networked Sensor Systems (SenSys), 2007.

5. I. Osipkov, E. Vasserman, N. Hopper and **Y. Kim**. *Combating doublespending using cooperative P2P systems*, 2007 IEEE Conference on Distributed Computing Systems (ICDCS), 2007.

6. J. Hwang, Y. Gu, T. He, and **Y. Kim**. "Realistic Sensing Area Modeling". IEEE Infocom 2007 Minisymposia, August 2007.

7. J. Hwang, T. He, and **Y. Kim**. "Detecting Phantom Nodes in Wireless Sensor Networks". IEEE Infocom2007 Minisymposia, August 2007.

8. I. Osipkov, P. Wang, N. Hopper and **Y. Kim**. *Robust Accounting in Decentralized P2P Storage Systems*. In *Proceedings of the 26th IEEE Conference on Distributed Computing systems (ICDCS)*, 2006.

9. J.-H. Cheon, N. Hopper, **Y. Kim** and I. Osipkov. *Authenticated Key-Insulated Public Key Encryption and Timed-Release Cryptography*. In *10th Conference on Financial Cryptography and Data Security*, February 2006.

10. D. Du, D. He, C. Hong, J. Jeong, V. Kher, **Y. Kim**, Y. Lu, A. Raghuveer, S. Sharafkandi, *Experiences in Building an Object-Based Storage System based on the OSD T-10 Standard*, NASA/IEEE Conference on Mass Storage Systems and Technologies 2006.

11. V. Kher, E. Seppanen, C. Leach, **Y. Kim**, *SGFS: Secure, Efficient and Policy-based Global File Sharing (Short Paper)*, NASA/IEEE Conference on Mass Storage Systems and Technologies, 2006.

12. P. Wang, **Y. Kim**, V. Kher, T. Kwon, *Strengthening Password-Based Authentication Protocols Against Online Dictionary Attacks*, ACNS 2005.

13. H. Yoon, J. Cheon, **Y. Kim**, *Batch Verifications with ID-Based Signatures*, ICISC 2004.

14. J. Hwang, **Y. Kim**, *Revisiting Random Key Pre-distribution Schemes for Wireless Sensor Networks*, 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04).

15. **Y. Kim**, D. Mazzochi, G. Tsudik, *Admission Control in Collaborative Groups*, 2nd IEEE International Symposium on Network Computing and Applications (NCA-03), Massachusetts, USA, April, 2003.

16. S. Lee, **Y. Kim**, K. Kim, D. Ryu, *An Efficient Tree-Based Group Key Agreement Using Bilinear Map*. ACNS 2003

17. Y. Amir, **Y. Kim**, C. Nita-Rotaru, G. Tsudik, *On the performance of Group Key Agreement Protocols*, The 22nd International Conference on Distributed Computing Systems (IEEE ICDCS 2002)

18. **Y. Kim**, A. Perrig, G. Tsudik, *Communication-Efficient Group Key Agreement*, In Proceedings of IFIP TC11 Sixteenth International Conference on Information Security (IFIP/SEC 2001), Kluwer Academic Publishers, June 2001

19. Y. Amir, **Y. Kim**, C. Nita-Rotaru, J. Schultz, J. Stanton and G. Tsudik, *Exploring Robustness in Group Key Agreement*, In Proceedings of The 21st International Conference on Distributed Computing Systems (IEEE ICDCS 2001), IEEE Press, April 2001

20. **Y. Kim**, A. Perrig, G. Tsudik, *Simple and Fault-tolerant Group Key Agreement Scheme*, In Proceedings of the 7th ACM Conference on Computer and Communications Security (ACM CCS 2000), ACM Press, Nov. 2000

21. Y. Amir, G. Ateniese, D. Hasse, **Y. Kim**, C. Nita-Rotaru, T. Schlossnagle, J. Schultz, J. Stanton and G. Tsudik, *Secure Group Communication in Asynchronous Networks with Failures: Integration and Experiments*, In Proceedings of The 20th International Conference on Distributed Computing Systems (IEEE ICDCS 2000), IEEE Press, April 2000

22. **Y. Kim**, S. Lee, and S. Park, *On the Design of Stream Ciphers and a Hash Function Suitable to Smart Card Application*, In Proceedings of CARDIS, Smart Card Research and Advanced Application: Second International Conference, Amsterdam, September, 1996.

OTHER REFEREED CONFERENCE AND WORKSHOP PUBLICATIONS

1. M. Shaneck, **Y. Kim**, V. Kumar, *Privacy Preserving Nearest Neighbor Search*, IEEE International Workshop on Privacy Aspects of Data Mining, December 2006

2. V. Kher and **Y. Kim**, *Securing Distributed Storage: Challenges, Techniques, and Systems*, StorageSS'05. (invited paper)

3. M. Shaneck, K. Mahadevan, V. Kher, and **Y. Kim**. Remote Software-based Attestation for Wireless Sensors. ESAS 2005.

4. T. Shon, **Y. Kim**, C. Lee, J. Moon, *A Machine Learning Framework for Network Anomaly Detection using SVM and GA*, 6th IEEE Information Assurance Workshop, 2005.

5. V. Kher, **Y. Kim**, *Decentralized Authentication Mechanism for Object-based Storage Devices*, Security in Storage Workshop 2003 (SISW), Washington D.C., Nov. 2003.

6. A. Jaiswal, **Y. Kim**, M. Gini, *Security Model for a Multi-Agent Marketplace*, The Fifth International Conference on Electronic Commerce (ICEC 03), Pennsylvania, Sep. 2003

7. **Y. Kim**, G. Tsudik, *Admission Control in Peer Groups*, Large-Scale Network Security Workshop – New Directions in Scalable Cyber-Security in Large-Scale Networks: Deployment Obstacles, Virginia, Mar. 2003,

8. **Y. Kim**, F. Maino, M. Narasimha, G. Tsudik, *Secure Group Services for Storage Area Networks*, 1st International IEEE Security in Storage Workshop (SISW 2002), Dec. 2002

9. G. Ateniese, O. Chevassut, D. Hasse, **Y. Kim** and G. Tsudik, *The Design of a Group Key Agreement API*, In Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX 2000), IEEE Computer Society Press, 2000

10. S. Park, S. Chee, K. Kim, **Y. Kim**, and S. Lee, *How to Use Exponent Permutations in Cryptography: Classifications and Applications*, In Proceedings

of International Conference on Cryptology and Information Security, ROC, December, 1996.

Technical Reports

1. P. Wang, N. Hopper, I. Osipkov, and **Y. Kim**, *Myrmic: Secure and Robust DHT Routing*, UMN DTC Research Report 2006/20, November 2006.
2. V. Kher, E. Seppanen, C. Leach, and **Y. Kim**, *SGFS: Secure, Efficient and Policy-based Global File Sharing,* UMN DTC Research Report 2006/8, April 2006.
3. M. Shaneck, V. Chandola, H. Liu, C. Choi, G. Simon, E. Eilertson, **Y. Kim**, Z-L Zhang, J. Srivastava, V. Kumar, *A Multi-Step Framework for Detecting Attack Scenarios*, UMN CS 06-004
4. I. Osipkov, **Y. Kim**, A. Tripathi, *Fighting Freeloaders in Decentralized P2P File Sharing Systems*, UMN CS 04-004
5. V. Kher and **Y. Kim**, *Decentralized Authentication Mechanisms for Object-based Storage Devices,* UMN DTC Research Report 2003/14, December 2003.

INVITED LECTURES

1. *Attacking the Kad Network*, University of Minnesota, Sep. 2007
2. *Securing Peer-to-peer Systems*, University of Southern California, Apr. 2007
3. *Securing Peer-to-peer Systems*, John Hopkins Univ., Apr. 2007
4. *Securing Peer-to-peer Systems*, Penn State Univ., Apr. 2007
5. *Securing Peer-to-peer Systems*, Purdue Univ., Apr. 2007
6. *Securing Peer-to-peer Systems*, Istituto Superiore Mario Boella, Mar. 2007
7. *Securing Peer-to-peer Systems*, IBM Zurich, Mar. 2007
8. *Securing Peer-to-peer Systems*, University of Milan, Mar. 2007

9. *Securing Peer-to-peer Systems*, Technische Universität München, Mar, 2007

10. *Myrmic: Secure and Robust DHT Routing*, Department of Computer Science, UC Irvine, 2006

11. *Integrated Infrastructure for Secure and Efficient Long-Term Data Management*, HEC-IWG File Systems and I/O R&D Workshop, 2006

12. *Securing Cooperative P2P Systems*, CyLab Seminar, CMU, 2006

13. *Differentiating Anomaly from Irregularity in Sensor Networks: A Closed-Loop Approach*, Special workshop on WSN security and privacy, organized by ARO and CMU, 2006

14. *Secure Group Services for Storage Area Networks*, IRTF GSEC Research Group, Minneapolis, Minnesota, Nov. 2003

15. *Group Key Agreement*, CSE Colloquium, University of Minnesota, Nov, 2002 Korea, Jul, 2002

16. *Group Key Agreement: Theory and Practice*, CIS Colloquium, University of Oregon, Feb, 2002

17. *Group Key Agreement: Theory and Practice*, Penn State University, Mar, 2002.

18. *Group Key Agreement: Theory and Practice*, Texas A&M University, Mar, 2002.

19. *Group Key Agreement: Theory and Practice*, University of Arizona, Mar, 2002.

20. *Experimental Performance of Five Notable Key Agreement Protocols for Dynamic Peer Groups*, IRTF GSEC (The Group Security) Research Group, Salt Lake City, Utah, Dec, 2001

21. *Group Key Agreement*, Guest Lecture in “Cryptography and Computer Security” course (ICS 268), UC Irvine, Oct, 2001

22. *Introduction to Block Ciphers*, Guest Lecture in “Cryptography and Computer Security” course (ICS 268), UC Irvine, Oct, 2001

23. *Group Key Agreement: Theory and Practice*, Korean Information Security Agency, Seoul, Korea, Sep. 2001

24. *Group Key Agreement*, Guest Lecture in "Advanced Topics in Cryptography" course (ICS 280), UC Irvine, May, 2001

25. *Multicast Security*, National Security Research Institute, Taejon, Korea, Aug. 2000

GRANT: External

1. PI, KISA (Korean Information Security Agency), *Detecting, Monitoring and Mitigating Peer to Per Botnet*, $70,000; 08/01/08 - 02/28/09.

2. Co-PI, NSF award CNS-0709048, *CRI: IAD Research Infrastructure for Emerging Networked Systems and Applications*, $200,000; 09/01/07-08/31/09, with Zhi-Li Zhang (PI), Abhishek Chandra, Nick Hopper, Arindam Banerjee.

3. Co-PI, NSF award CNS-0716025, *CT-ISG: Building Trustworthy Cooperative P2P Systems*, $200,000; 09/01/07-08/31/10, with Nick Hopper (PI) and Zhi-Li Zhang.

4. PI, DHS Phase II, *STTR: Network-Based Boundary Controllers*, $224,999; 06/01/2007 – 05/31/2009, Prime: ATCorp.

5. PI, DHS, *STTR: Network-Based Boundary Controllers*, $33,001; 10/02/06-04/01/07, Prime: ATCorp

6. Co-PI, NSF award CCF-0621462, *Integrated Infrastructure for Secure and Efficient Long-Term Data Management*, $599,790; 09/15/06-08/31/09, with Andrew Odlyzko (PI) and David Lilja

7. Co-PI, NSF award DUE-0621324, *UMSSIA: University of Minnesota Summer School on Information Assurance*, $199,979; 11/1/06-10/31/08, with Zhi-Li Zhang (PI) and Nick Hopper.

8. PI, *Secure Wireless Sensing for Industrial Applications II*, Honeywell International Inc., $33,668, 08/29/2005 – 05/28/2006

9. co-PI, *SIMON: Simulation and Modeling for Networked Storage System*, ONR Phase II, $180,000, 07/01/2005 – 12/31/2006

10. PI, *CAREER: Reconsidering Security for Networked Storage and File Systems*, NSF, $400,000, , 03/01/2005 – 02/28/2010
REU Supplement, NSF, $12,000, 03/15/2007 – 02/29/2008

11. PI, *Design of Efficient Group Key Management*, National Security Research Institute, Korea, $100,000, 01/01/2005 – 06/30/2005

12. PI, *Intelligent Storage Consortium-ETRI*, ETRI, Korea, $45,000, 10/01/2004 – 12/31/2004

13. PI, *Secure Wireless Sensing for Industrial Applications I*, Honeywell International Inc., $32,700, 08/24/2004 – 05/29/2005

14. PI, *SIMON: Simulation and Modeling for Networked Storage System*, ONR Phase I, $33,250, 07/01/2004 – 07/31/2005, Prime: ATCorp

15. PI, *Multiple-Security Multimedia Collaboration Environment (MMCE)*, (with Zhang), ONR, $28,869, 01/01/2004 – 06/30/2004, Prime: ATCorp

16. co-PI, *Situational Awareness Analysis Tool for Aiding Discovery of Security Events and Patterns*, Advanced Research and Development Activity (ARDA), $800,000, 09/24/2003 – 05/31/2005, with Vipin Kumar (PI), Jaideep Srivastava and Zhi-Li Zhang.

17. PI, *Secure and Efficient File Sharing using Secure Spread*, Johns Hopkins US/Air Force Research Lab., $32,776, 07/01/2003 – 08/31/2003

GRANT: Internal

1. PI, *Practical security for emerging networked systems*, McKnight Land-Grant Professorship Award, $90,000, 07/01/2006 - 06/30/2008

2. PI, *New Approaches to Timed-Release Cryptography and their Applications*, University of Minnesota Grant-in-aid, $21,738, 01/01/2005 – 06/30/2006

3. PI, *Secure Admission Control in Peer Groups on the Internet*, University of Minnesota (Grant-in-Aid), $18,357, **Selected as Exemplary Proposal**, 06/01/2003 – 05/31/2004

SOFTWARE

1. coreFS
   - Faculty: Yongdae Kim
   - Student: Vishal Kher, Matt Kokotovich (ugrd), Eric Seppanen (ugrd), Cory Leach (ugrd)
   - A very basic user-level network file system built on top of FUSE (`http://fuse.sourceforge.net/`).
   - Goal: to give file system developers some form of basic distributed file system, which can be later modified as per the implementor's requirement.
   - This is not a file system to be deployed in practice as is; rather, it is for the programmers/students to extend it as they wish for research and education purposes.
   - Released open-source on Mar. 2007.
   - Available from `http://www.cs.umn.edu/research/sclab/coreFS.html`
   - *Number of downloads: 175*
2. OSD ANSI T10 Standard Reference Implementation
   - Faculty: Yongdae Kim, David Du
   - Students: Dingshan He, Jaehoon Jeong, Vishal Kher, Yingping Lu, Aravindan Raghuveer, Sarah Sharafkandi, and 6 more students
   - OSD (Object-based Storage Device) is an ANSI (American National Standards Institute) standard developed by storage industry. UMN provides a reference implementation so that industry can develop other required component of the system.
   - Released open-source on Apr. 2007.

- Available from `http://sourceforge.net/projects/disc-osd/`.
- *Number of downloads: 128*

3. CLQ_API 1.0
   - PI: Gene Tsudik
   - CLQ_API is a group key agreement API that implements four major group key agreement algorithms.
   - The whole implementation was done by Yongdae Kim.
   - Available from `http://sconce.ics.uci.edu/cliques/download.html`.
   - Number of downloads has not been tracked.

4. Secure Spread 2.1.0
   - PI: Yair Amir, Gene Tsudik
   - Secure Spread integrates security services with reliable group communication. This implementation was done by 4 graduate students and 2 PIs under Secure Spread project funded by DARPA. CLQ_API is one of the core components of the Secure Spread library.
   - Available from `http://www.cnds.jhu.edu/research/group/secure_spread/`.
   - *Number of downloads: 1074*

CONFERENCE/WORKSHOP ORGANIZING COMMITTEES

- Editorial Board on Journal of Computing Science and Engineering (Korea Information Science Society), 2007 – Present
- IEEE Infocom 2007 NSF Student Travel Grant Committee Chair
- Local Steering Committee, Third Annual Workshop on Economics of Information Security (WEIS 04)
- Editorial Board on Journal of Korea Institute of Information Security & Cryptology, 2002 – Present

CONFERENCE/WORKSHOP PROGRAM COMMITTEES

- IFIP SEC, 2008
- IEEE Symposium on Security and Privacy, 2008
- ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2008
- ACM StorageSS, 2007
- ACM Workshop on Scalable Trusted Computing, 2007
- IEEE Symposium on Security and Privacy, 2007
- IEEE International Workshop on Trust, Security, and Privacy for Ubiquitous Computing (TSPUC) 2007
- IEEE International Conference on Distributed Computing Systems (ICDCS) 2006
- IEEE Infocom 2006
- IEEE SecureComm 2006
- IEEE International Workshop on Trust, Security, and Privacy for Ubiquitous Computing (TSPUC) 2006
- European Workshop on Security and Privacy in Ad Hoc and Sensor Networks, 2006
- ACM SASN 2005
- IEEE SecureComm 2005
- European Workshop on Security and Privacy in Ad Hoc and Sensor Networks, 2005
- ACM StorageSS 2005
- Asiacrypt 2004

- ICISC (International Conference on Information Security and Cryptology) 2004
- IEEE International Security In Storage Workshop (SISW) 2002 – 2005
- 2003 International Conference on Parallel Processing (ICPP) 2003
- International Workshop on Information Security Applications (WISA) 2002 – 2005

PANEL/REVIEWER

- NSF Panel member, 2003, 2005, 2006
- Journal reviewer: IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, IEEE/ACM Transactions on Network, IEEE Transactions on Mobile Computing, IEEE Transactions on Wireless Communications, ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Software Engineering

DEPARTMENTAL SERVICE

- CSE Research Opportunity Committee: 2007 – present
- CSE Strategic Positioning Committee: 2006 – 2007
- CSE Research Opportunity Committee: 2005 – 2006
- CSE Graduate Admission Committee: 2004 – 2005
- Assisted in the review of faculty candidates in security, 2003-current.

SUPPLEMENTAL STATEMENT

The NSF and Homeland Security both sponsor a “Scholarship for Service” (SFS) program that gives large (around $2.5M/4 years) grants to departments to fund scholarships for MS students to study computer security (students who receive these scholarships are then obligated to work in a federal agency or national lab for two years). Along with Nick Hopper, Zhi-Li Zhang and Jaideep Srivastava, I have been working to secure a SFS grant. This effort included:

- In December 2005, applied to NSA for the "Center of Academic Excellence in Information Assurance Education" designation, which is a prerequisite for SFS grants. The first step of this application is to obtain a certification from the Committee on National Security Standards stating that security courses at UMN meet NSA standards. This certification was obtained in December 2005. The Center of Excellence application was approved in March 2006.

- From November 2005 - January 2006, developed and submitted the proposal "MISS: Minnesota Information Security Scholarship" ($2.8M; 9/1/2007 – 8/31/2011) to NSF, along with Zhi-Li Zhang and Nick Hopper. The proposal, to support a total of 30 Master's students to study information security in the department, was declined but received a competitive rating; we plan to revise and resubmit in 2008.

- In February 2006, submitted the revised proposal "UMSSIA: University of Minnesota Summer School for Information Assurance," ($199,979; 11/1/2006 – 10/31/2008) a proposal to educate regional instructors at 4-year and minority-serving institutions at a two-week summer session. The proposal was funded and we offered UMSSIA 2007 was held in June 2007 in cooperation with DTC and OITSec.