International Journal of Security and Its Applications
Vol. 4, No. 1, January, 2010

On the Potential of Limitation-oriented Malware Detection and Prevention Techniques on Mobile Phones

[1]Qiang Yan, [2]Robert H. Deng, [3]Yingjiu Li, and [4]Tieyan Li

[1,2,3]School of Information Systems, Singapore Management University
{qiang.yan.2008, robertdeng, yjli}@smu.edu.sg
*[4]Institute for Infocomm Research, A*STAR, Singapore*
litieyan@i2r.a-star.edu.sg

Abstract

The malware threat for mobile phones is expected to increase with the functionality enhancement of mobile phones. This threat is exacerbated with the surge in population of smart phones instilled with stable Internet access which provides attractive targets for malware developers. Prior research on malware protection has focused on avoiding the negative impact of the functionality limitations of mobile phones to keep the performance cost within the limitations of mobile phones. Being different, this paper investigates the positive impact of these limitations on suppressing the development of mobile malware. We study the state-of-the-art mobile malware, as well as the progress of academic research and industrial effort against mobile malware. Our study shows that the functionality limitations of mobile phones should be considered as advantages as they have significant impact on shrinking the living space of mobile malware. From this perspective, we propose and analyze three potential limitation-oriented techniques for effective malware detection and prevention on mobile phones.

Keywords: *Mobile Security; Malware; Limitation-oriented Protection.*

1. Introduction

Malware is one of the most well-known security threats to mobile phones, which comes from the concern about privacy disclosure from the mobile phones as more and more people carry them all the time and store more and more sensitive information on them. The malware targeting mobile phones (called mobile malware) develops slowly in the past five years since the first proof-of-concept mobile malware "Cabir" was proposed in 2004[1]. Until now, the total number of mobile malwares is known to be hundreds, which is a small number as compared to millions of PC malwares[2]. Nonetheless, mobile malware causes serious public concern as the population of mobile phones is much larger than the population of PCs. According to Gartner, worldwide mobile phone sales total 269.1 million units in the first quarter of 2009[3], while worldwide PC shipments only reach 292 million units in the whole year of 2008[4]. A large scale outbreak of mobile malware could be more serious than the outbreaks of PC

[1] Viruslist, http://www.viruslist.com/en/analysis?pubid=200119916
[2] Symantec, http://www.symantec.com/business/theme.jsp?themeid=threatreport
[3] Gartner, http://www.gartner.com/it/page.jsp?id=985912
[4] Gartner, http://www.gartner.com/it/page.jsp?id=1040020

malware that we have seen in the past decades. The recent rapid functionality enhancement of mobile phones driven by the population surge of smart phone platforms is expected to increase the security threat from mobile malware. The enhanced functionalities such as faster Internet access and standardized programming APIs provide an ideal breeding ground for malware development.

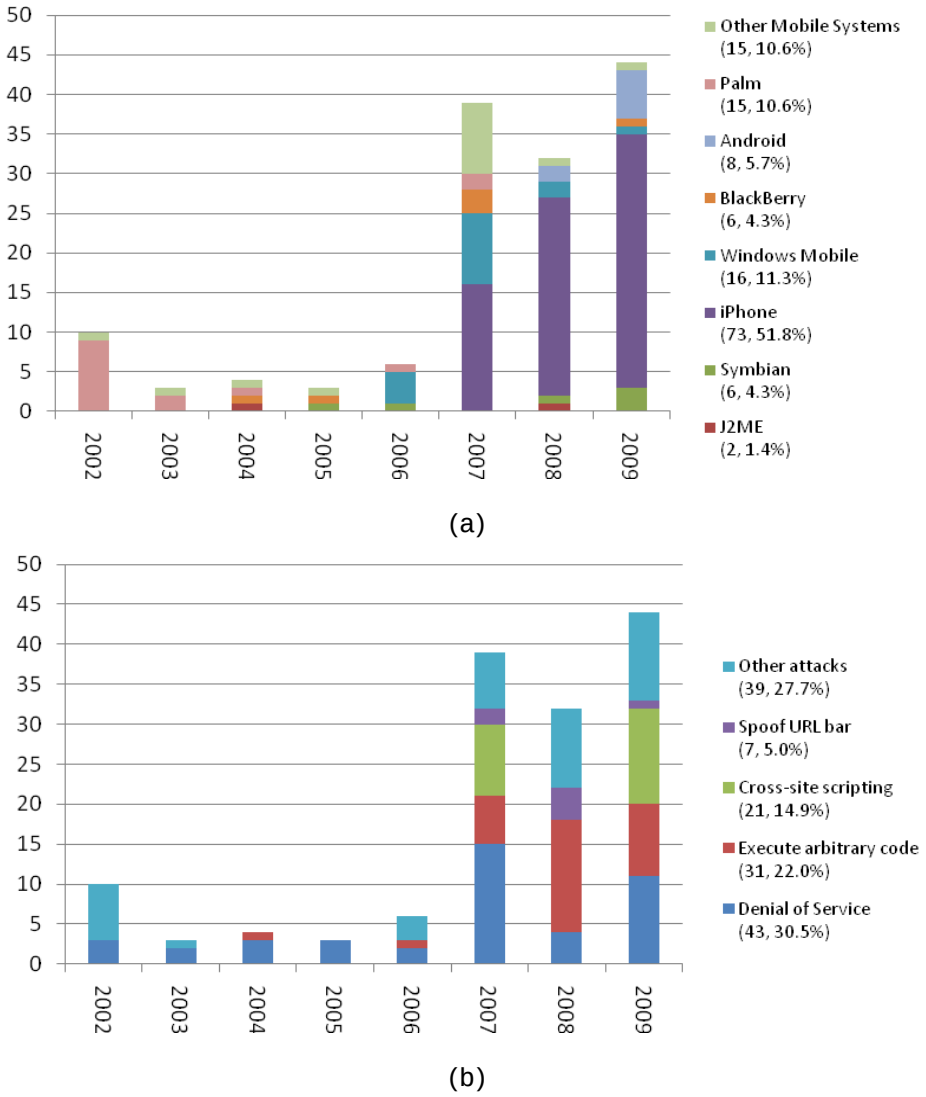


Figure 1. Distribution of software vulnerabilities on (a) mobile systems and (b) attack types in Common Vulnerabilities and Exposures database. Each bar describes the number of vulnerability records for each mobile system or attack type in each year. The numbers after the legend text are the sum and percentage of the record number from 2002 to 2009. Note: The attack types are classified based on the description of vulnerability records. If the description of a vulnerability record contains both "execute arbitrary code" and "denial of service", it will be classified into "execute arbitrary code"

Prior research [1,2,3,4] on malware protection has focused on avoiding the negative impact of the functionality limitations of mobile phones. The major efforts are to keep the performance cost within the limitations of mobile phones. Although the energy-efficiency criterion and other capability restrictions limit the effectiveness of complex malware protection solutions, they also limit the power of mobile malware. The positive impact of these functionality limitations could be one of the major reasons to explain the slow development of mobile malware in the past five years.

To understand the impact of the functionality limitations of mobile phones, this paper studies the state-of-the-art mobile malware, and the progress of academic research and industrial effort against mobile malware. Our study shows that the functionality limitations of mobile phones have significant impact on suppressing the development of mobile malware. From this perspective, we propose and analyze three potential limitation-oriented techniques for effective malware detection and prevention on mobile phones.

2. State-of-the-Art Mobile Malware and Countermeasures

2.1. State and Trends on Mobile Malware

Due to lack of sufficient number of wild malware samples, we investigate the state of mobile malware based on the vulnerability records in Common Vulnerabilities and Exposures (CVE) database[5]. Figure 1(a) shows the distribution of software vulnerabilities on mobile systems in the CVE database retrieved at July 25, 2009. It can be observed that the number of vulnerability records increases dramatically after the rise of the smart phone platform. Especially iPhone contributes to half of the number of the vulnerability records in its first two-and-a-half years.

From the distribution of attack types shown in Figure 1(b), until 2007, Denial of Service is still the dominant attack type that can be exploited from the known vulnerabilities (50.0%). This explains that most mobile malware in the past is only able to affect the availability of a mobile phone such as application crash and device reset. Only a few of mobile malware targeting at special mobile phones is able to launch advanced attacks such as distributed denial of service for some specific phone numbers (Redbrowser Trojan, 2006) [5]. Unfortunately, the functionality limitations for mobile malware are significantly relaxed after the release of smart phone platforms. This trend brings more serious vulnerabilities that allow mobile malware to execute arbitrary code. The percentage of its vulnerability record number is raised from 7.7% to 22.0% in the past three years. Moreover, the availability of standardized programming APIs on smart phone platforms and faster Internet access via 3G and WiFi make it easier for malware development and propagation.

Nowadays, still a significant barrier for the known mobile malwares is that user interaction must be involved for those non-crash-purpose malwares. None of today's mobile malwares are able to install stealthily without the users accepting the standard security warnings [6]. Social engineering techniques, such as pretending to be a theme, a system patch, or a game installation, are widely used to tempt users to run malwares on mobile phones. So the interest of mobile malware is largely dependent on the market share of mobile phones. The latest cell-phone malwares report from F-Secure [6] indicates that, until 2007, 364 out of 373 malwares are designed for the most popular mobile OS, Symbian (47.1% market share in Q4 2008[6]),

[5] CVE database, http://cve.mitre.org
[6] Smartphone Market Share, http://en.wikipedia.org/wiki/Smartphone

which however has only six vulnerability records in the CVE database until 2009. The most popular infection mechanism is still user download (373 cases). The rapid market growth of iPhone will make it the next attractive target for malware development.

2.2. Academic Research against Mobile Malware

The academic research on mobile malware detection began later as mobile malware developed slowly in the past few years. Less than ten samples of wild mobile malwares including Cabir, Mabir, Commwarrior, and Lasco are available to academic researchers. Most researchers designed their own artificial malware to evaluate their protection solutions [1,7]. Existing research on mobile malware detection focuses on tailoring the traditional signature-based detection techniques to the resource-constrained computation environment on mobile phones. Bose et al. [1] introduced a signature scheme that characters high-level program behaviors to reduce the cost of real time monitoring and signature comparison. Cheng et al. [2] bypassed the resource limitations by presenting a firewall solution between cellular network and Internet to filter suspicious data stream.

Except traditional signature-based malware detection, recent research also starts new attempts to prevent the threat of mobile malware. Zhang et al. [3] and Muthukumaran et al. [4] investigated the integrity measurement based malware prevention that enforces lightweight mandatory access control to prevent malicious program behaviors. The major challenge of this approach is to automatically define sound rules without involving considerable human labor. Kim et al. [7] and Liu et al. [8] examined power anomaly monitoring that detects mobile malware by observing the extra power consumption caused by malicious behaviors. The major obstacle for this technique is the difficulty in accurately quantifying and modeling power consumption for multitask mobile platforms.

2.3. Industrial Effort against Mobile Malware

The industrial effort against mobile malware mainly comes from anti-virus vendors and mobile OS providers.

Most anti-virus vendors offer the mobile versions of their anti-virus software. We examined the latest specifications of mobile anti-virus software from ESET, F-Secure, Kaspersky, McAfee, Norton, and Trend Micro. The core technique used in these solutions is still traditional signature-based detection techniques that monitor execution traces and file accesses. For these products, the major challenges, besides the constrained resources of mobile phones, also come from social engineering, which may tempt users to skip the warning provided by anti-virus software. Once malware is launched, anti-virus software could be neutralized due to weak runtime privilege control on mobile systems.

The efforts from mobile OS providers mainly focus on enhancing the privilege control of mobile OS. The privileges on latest Symbian OS are defined as capabilities of a program[7]. To access a certain capability, a program must be signed by a certificate that is authorized with the corresponding privilege. These capabilities allow the Symbian OS to enforce fine-grained access control for the functionalities provided by the platform APIs. Mobile malware is not able to gain a high privilege as long as the high privilege certificate is not disclosed to malware developers. Some linux-based smart phone platforms such as MontaVista also

[7] Symbian Signed, http://www.symbiansigned.com

provide similar privilege control mechanisms by incorporating miniaturized version of SELinux[8].

3. Potential Limitation-oriented Techniques for Effective Malware Detection and Prevention on Mobile Phones

The key challenge for existing malware protection techniques on mobile phones is to satisfy the functionality restrictions. The minimal functionality requirement for a mobile malware is usually much lower than that of an anti-malware solution. It is difficult to narrow this gap as an anti-malware solution has to defend all possible intrusion locations while a mobile malware only need to find one breakthrough point. So the current functionality enhancement on mobile phones tends to give more power to mobile malware than to anti-malware solutions, which is expected to raise the threat of mobile malware rather than lowering the threat.

Since the functionality limitations of mobile phones have succeeded in suppressing the development of mobile malware in the past few years, we should not only consider their negative impacts that the power of existing solutions has to be weaken as these solutions have to be slimed to satisfy the functionality limitations. Instead, we should also consider them as the advantages that can be taken to design more effective anti-malware solutions. Based on this idea, we present the following three potential limitation-oriented techniques for effective malware detection and prevention on mobile phones.

3.1. Monitoring Power Consumption

Battery power consumption is one of the major limitations of mobile phones that limit the complexity of anti-malware solutions. It also brings the challenge for mobile malware as all critical behaviors for malware propagation such as accessing WiFi or Bluetooth consume significant battery power [7]. Any malicious behaviors caused by mobile malware also involve extra power consumption. Mobile malware cannot hide these malicious behaviors if the power consumption of normal behaviors can be accurately quantified. As one of the most coarse-grained features that characterize program behaviors, the cost of real time power consumption monitor is negligible [7,8]. These factors make power consumption monitoring a potential direction for effective malware detection. Figure 2 illustrates an example of mobile malware detection by monitoring power consumption.

The preliminary works have been done for this direction. The first known research by Jacoby and Davis [9] proposed a malware detection technique based on the assumption that greedy malwares keep repeating the power consuming behaviors like scanning adjacent Bluetooth devices. These repeating behaviors will result in certain dominant frequencies shown in frequency-domain data transformed from the collected time-domain data of power consumption. The malwares are identified from these certain dominant frequencies. Recent work by Kim et al. [7] proposed another detection technique by comparing the compressed sequences of the power consumption value in each time interval. Liu et al. [8] defined a user-centric power model to estimate the power consumption based on the number or the duration of the user actions, such as, the duration of Call, the number of SMS, and etc. Their work uses machine learning techniques to generate rules for malware detection.

[8] MontaVista, http://www.mvista.com

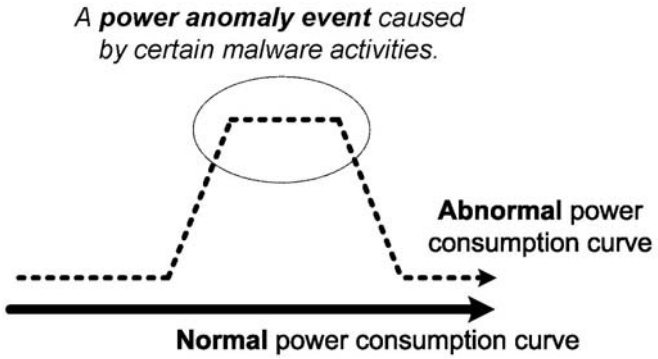


Figure 2. Example of mobile malware detection by monitoring power consumption. The activities of mobile malware are detected based on power anomaly events

These works have shown that power anomaly is an effective indicator for suspicious activities on mobile phones. To identify the causes of these activities is still a challenge for power-based malware detection as the power consumption for normal behavior is yet to be accurately quantified. Another challenge is that existing mobile phones is not able to provide sufficient precision for power consumption measurement without involving extra measuring devices like an oscilloscope.

3.2. Increasing Platform Diversity

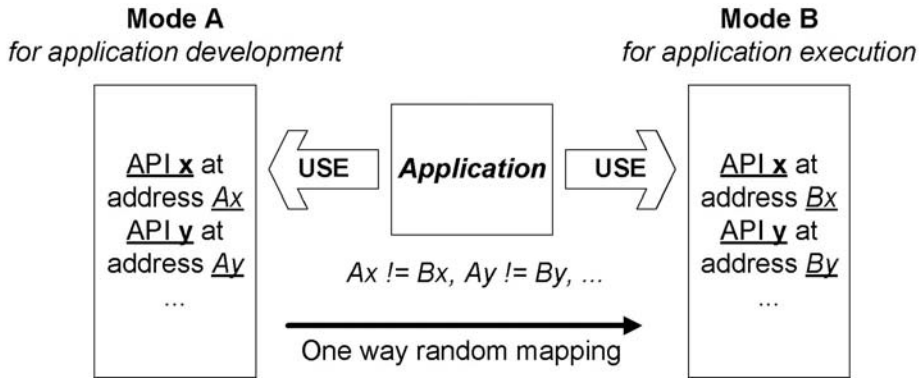


Figure 3. Example of dual mode design. The intrusion of mobile malware is prevented by self diversity after randomizing the programming APIs

Platform diversity that mainly represents as lack of standardized programming APIs was one of major obstacles for deploying applications on different mobile phone models. It also limits the scope of victim mobile phones for a certain mobile malware. It is very difficult if not impossible for a mobile malware to use a limited-size payload to infect a large number of mobile phones with completely different programming APIs. This platform diversity is decreasing with the population of smart phones as device manufacturers prefer to deploy only

a few smart phone platforms for all their mobile phones to increase the usability and extensibility.

The key idea to increase platform diversity of smart phone platform is to use a dual mode design for application execution and development. The diverse programming APIs that are specific to each individual mobile phone are used for application execution to prevent the intrusion of mobile malware. The standard programming APIs are used for the application development. During the installation, a user switch the mobile phone into a bridge phrase that maps the standard programming APIs to the diverse programming APIs. Without the confirmation of users, a mobile malware is not able to learn the mapping for the diverse programming APIs that are currently used in the mobile phone. Figure 3 demonstrates an example of dual mode design.

The major challenge for this approach is to secure the mapping information for legitimate applications and the bridge phrase that maps the standard programming APIs to the diverse programming APIs. The established mapping should be updated periodically, such as update the mapping during each mobile phone startup, to mitigate the threat that mobile malware learns the correcting mapping incidentally.

3.3. Enforcing Hardware Sandbox

Hardware capability limitation subject to manufacture cost was another major limitation that makes it difficult to extend the applications of mobile phones beyond telephony. It also suppresses the damage that can be caused by mobile malware. For example, the weak connectivity of traditional mobile phones makes that the best propagation methods for mobile malware were via Bluetooth and MMS. Although Internet is more attractive as it is necessary for mobile malware to propagate globally, the stable Internet access with sufficient bandwidth was not available. This is one of the major reasons that no large-scale outbreak has been observed until now. But these hardware capability limitations are being eliminated. More new hardware features such as WiFi and GPS have been integrated with the latest mobile phones.

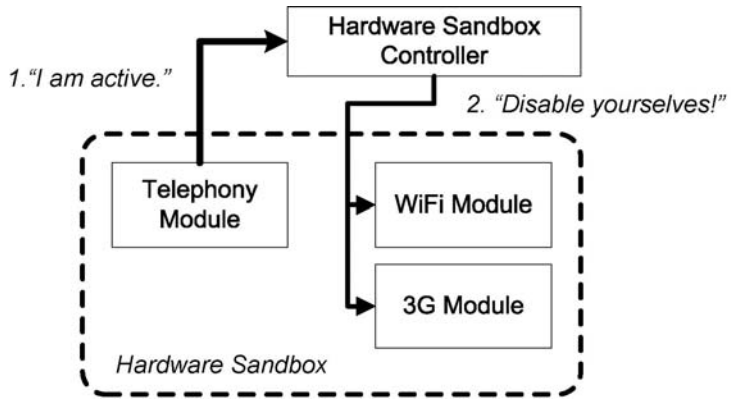


Figure 4. Example of hardware sandbox application. Real time wiretapping via Internet is prevented as all hardware modules required for Internet access are disabled during a phone call

The key idea to mitigate the threat from hardware capability enhancement is to enforce hardware sandbox that controls the access to the hardware. This hardware access control should be enforced by hardware sandbox rather than software sandbox like Symbian Signed. It is because the prevailing social engineering attacks may tempt users to bypass the protection of software sandbox. This is driven by the fact that the majority of interesting applications on mobile phones is provided by third party software developers who usually do not provide the certificates to prove their legitimacy. Hardware sandbox is able to provide a baseline protection even when the whole software system has been compromised by mobile malware, which cannot be provided by software sandbox. The basic principle to design a hardware sandbox is to disable the dangerous hardware components when sensitive applications such as telephony are running. Figure 4 illustrates an example of using hardware sandbox to prevent real time wiretapping via Internet.

The major challenge for hardware sandbox is to define flexible rules to guarantee the baseline protection while imposing minimal influence on normal usage of mobile phones. Disabling hardware components is not necessary if fine-grained access controls are available from hardware sandbox. Certain physical buttons on mobile phones can be used to switch among the protection levels to increase the usability of hardware sandbox. The remaining challenges are to provide an effective implementation and to securely store and update access control rules. These two challenges may be solved by incorporating a trusted platform module for mobile devices. However, such a hardware product is still not available until now [3].

4. Conclusion

In this paper, we investigated the impact of functionality limitations of mobile phones on the development of mobile malware. Through a survey on the state-of-art mobile malware, as well as the progress of academic research and the industrial effort against mobile malware, our study shows that the functionality limitations of mobile phones have a positive impact on suppressing the development of mobile malware. Based on this analysis, we proposed three potential limitation-oriented techniques for effective malware detection and prevention on mobile phones after considering these limitations as the advantages. The major challenges for these potential techniques are identified in this work and more technical details will be provided in our future work.

References

[1] Bose, A., Hu, X., Shin, K.G., Park, T.: Behavioral detection of malware on mobile handsets. In: Proceeding of the 6th international conference on Mobile systems, applications, and services. (2008) 225-238

[2] Cheng, J., Wong, S.H., Yang, H., Lu, S.: Smartsiren: virus detection and alert for smartphones. In: Proceedings of the 5th international conference on Mobile systems, applications and services. (2007) 258-271

[3] Zhang, X., Aciicmez, O., Seifert, J.P.: Building efficient integrity measurement and attestation for mobile phone platforms. In: Proceedings of the First International Conference on Security and Privacy in Mobile Information and Communication Systems. (2009)

[4] Muthukumaran, D., Sawani, A., Schiffman, J., Jung, B.M., Jaeger, T.: Measuring integrity on mobile phone systems. In: Proceedings of the 13th ACM symposium on Access control models and technologies. (2008) 155-164

[5] Bose, A., Shin, K.G.: On mobile viruses exploiting messaging and bluetooth services. In: Securecomm and Workshops. (2006) 1-10

[6] Hypponen, M.: State of cell phone malware in 2007. invited talk at the 16th usenix security symposium, boston, http://www.usenix.org/events/sec07/tech/ (2007)

[7] Kim, H., Smith, J., Shin, K.G.: Detecting energy-greedy anomalies and mobile malware variants. In: Proceeding of the 6th international conference on Mobile systems, applications, and services. (2008) 239-252

[8] Liu, L., Yan, G., Zhang, X., Chen, S.: Virusmeter: Preventing your cellphone from spies. In: Proceedings of the 12th International Symposium On Recent Advances In Intrusion Detection. (2009)

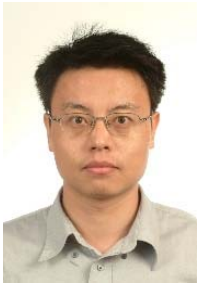
[9] Jacoby, G., Davis, N.: Battery-based intrusion detection. In: Proceedings of the Global Telecommunications Conference. (2004)

Authors

Qiang Yan is currently a Ph.D. student in the School of Information Systems at Singapore Management University. He received his B.Eng. and M.Sc. in Software Engineering from Fudan University, China, in 2006 and 2009. His current research areas include RFID security, mobile security, and system security.

Robert H. Deng received his B.Eng from National University of Defense Technology, China, his M.Sc. and Ph.D. from the Illinois Institute of Technology, USA. He has been with the Singapore Management University since 2004, and is currently Professor, Associate Dean for Faculty & Research, and Director of SIS Research Center, School of Information Systems. Prior to this, he was Principal Scientist and Manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. He has 26 patents and more than 200 technical publications in international conferences and journals in the areas of computer networks, network security and information security. He served as general chair, program committee chair and member of numerous international conferences. He received the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006.

Yingjiu Li is currently an Assistant Professor in the School of Information Systems at Singapore Management University. He received his Ph.D. degree in Information Technology from George Mason University in 2003. His research interests include RFID system security, data applications security, and information security management. He has published over 60 technical papers in the refereed journals and conference proceedings. Yingjiu Li is a senior member of the ACM. The URL for his web page is http://www.mysmu.edu/faculty/yjli/



Tieyan Li is currently a research scientist at Institute for Infocomm Research (I2R, Singapore). He obtained his dual B.Sc. degrees in 1994 at NanKai University, China and his Ph.D. degree in 2003 at School of Computing, National University of Singapore. He has been with I2R since Oct. 2001, and is active in academic security research fields with tens of journal and conference publications and several patents. Prior to this, he had solid working experiences on practical system developments such as networking, system integration and software programming. Currently his areas of research are in applied cryptography and network security, as well as security issues in RFID, sensor, multimedia and tamper resistant hardware/software, etc. Dr. Li has served as the associate editor, PC member and reviewer for a number of security conferences and journals.