ATIP Report: Cyber Security Research in China

ATIP/China

ABSTRACT: The Chinese government has placed unprecedented importance on information security. In China, the developing trend to assure cyber security is adopting independent and controllable core technologies in an IT system, and various government funding agencies have been supporting cyber security research on fundamental theory and frontier technologies there. This report reviews major government research projects and introduces the leading research groups in the field of cyber security in China. Progress has recently been made in the areas of cryptography, web security, intrusion detection & attack analysis, cloud security, mobile security, and security of wireless sensor networks in China, and an overview of these research achievements is provided within.

KEYWORDS: Government S&T Policy / Funding, Information Technology / IT, Mathematics, Telecommunications / Networking

COUNTRY: China

DATE: June 5, 2015

REPORT CONTENTS

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
05 JUN 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
ATIP Report: Cyber Security Research in China	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ATIP,,PO Box 4510,,Albuquerque,,NM, 87196**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Chinese government has placed unprecedented importance on information security. In China, the developing trend to assure cyber security is adopting independent and controllable core technologies in an IT system, and various government funding agencies have been supporting cyber security research on fundamental theory and frontier technologies there. This report reviews major government research projects and introduces the leading research groups in the field of cyber security in China. Progress has recently been made in the areas of cryptography, web security, intrusion detection & attack analysis, cloud security, mobile security and security of wireless sensor networks in China, and an overview of these research achievements is provided within.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a REPORT **unclassified**	b ABSTRACT **unclassified**	c THIS PAGE **unclassified**	**Same as Report (SAR)**	**27**	

EXECUTIVE SUMMARY

- The Chinese government has placed unprecedented importance on information security, especially after Edward Snowden leaked aspects of the United States (US) National Security Agency's (NSA's) PRISM program. China established the Central Leading Group for Internet Security and Informatization in February 2014 as the country's highest government organization in charge of cyber security.
- Both the volume and sophistication of cyber attacks have been growing in China in recent years. The country's current information assurance system is not able to completely defend against all of the various types of cyber attacks.
- China faces challenges in management, technology, and human resources in addressing the cyber security issue.
- Adopting independent and controllable core technologies in IT systems is currently the developing trend in China's assurance of cyber security.
- Cyber security research on fundamental theory and frontier technologies is primarily supported by the Ministry of Science and Technology's (MOST's) High-Technology Research and Development Program (863 Program) and National Basic Research Program of China (973 Program), as well as a variety of programs of the National Natural Science Foundation of China (NSFC).
- Security research on emerging technologies has been funded as a priority in recent years, covering topics such as cloud computing, Internet of Things (IoT), and mobile systems and applications.
- Institutes of the Chinese Academy of Sciences (CAS) and some university research teams are leading research groups in the field of cyber security. Among them, the Institute of Information Engineering (IIE) of CAS is engaged in the most comprehensive research on cyber security.
- Information security research in China has not been conducted in a systematic way, and it primarily involves the application or improvement of existing technologies rather than original innovation.
- The overall level of Chinese information security research still lags behind the advanced

international level.

IMPACT & ASSESSMENT

With the growing volume and sophistication of cyber attacks in China, ongoing attention is required to protect sensitive business and personal information as well as safeguard national security. Adopting independent and controllable core technologies in IT systems is the developing trend for China's assurance of cyber security. In the meantime, security research on emerging technologies such as cloud computing and IoT as well as mobile systems and applications are receiving more financial support and widespread interest. Although the overall level of Chinese information security research still lags behind the advanced international level, some progress has been made by Chinese researchers in the areas of cryptography, web security, intrusion detection & attack analysis, cloud security, mobile security, and the security of wireless sensor networks.

1. INTRODUCTION

Cyber security, also referred to as IT security, focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, alteration, or destruction. Today, the Internet has become the major communication infrastructure of modern society - but the Internet's evolution has also spawned a rich complexity and vulnerability in its infrastructure. The adoption of new technologies and new business models such as cloud computing, big data, Internet of Things (IoT), and mobile Internet further increase the risks. Constant attention is required to protect sensitive business and personal information, as well as safeguard national security.

The Chinese government has placed unprecedented importance on information security, especially after Edward Snowden leaked aspects of the United States (US) National Security Agency's (NSA's) PRISM program. Adopting independent and controllable core technologies in IT systems is the developing trend in China to assure cyber security.

Various government funding agencies in China have supported cyber security research on fundamental theory and frontier technologies. This report reviews major government research projects and introduces the leading research groups in the field of cyber security. An overview of some recent research achievements in the areas of cryptography, web security, intrusion detection & attack analysis, cloud security, mobile security, and security of wireless sensor networks is provided within.

Note: This report uses a currency conversion rate of 1 Chinese Yuan Renminbi (RMB) = .163 United States Dollars (US$).

2. CURRENT STATUS OF CYBER SECURITY IN CHINA

The Chinese government has placed unprecedented importance on information security, especially after Edward Snowden leaked aspects of the US NSA's PRISM program. In February 2014, China established the Central Leading Group for Internet Security and Informatization headed by President Jinping XI. The group is designed to lead and coordinate information security and informatization work among different sectors, as well as draft national strategies, development plans, and major policies in this field. President XI said China must balance its

needs for both developing IT technologies and safeguarding cyber security, describing the two issues as “two wings of a bird and two wheels of an engine.”

China has been connected to the worldwide web for 20 years. By the end of 2014, China had 649 million Internet users and 557 million mobile Internet users. As the number of Internet users, digital applications, and data networks increase, so do the opportunities for exploitation.

According to a China Cyber Security Situation Annual Report released by China's National Computer Network Emergency Response Technical Team and Coordination Center (CNCERT/CC) in June 2014, the country’s capability to defend its basic networks such as telecommunications (telecom) carrier backbone networks has improved, but domain name systems remains the weak link concerning security. The annual report noted that the volume and sophistication of the following types of cyber attacks were growing in 2013:

- Hackers tampered with 24,034 web pages in China, including 2,430 government websites - up 46.7% and 34.9 % year-on-year, respectively.
- Built-in backdoor programs were detected in 76,160 domestic websites, including 2,425 government websites.
- A total of 30,199 phishing websites targeting China's growing online population were monitored, with 90.2% of these phishing websites being run on foreign severs. Chinese authorities state that US-based sites accounted for 53.4%.
- The China National Vulnerability Database (CNVD) reported 7,854 new vulnerabilities in 2013, including 2,607 (33.2%) high-risk vulnerabilities.
- The environment of the mobile Internet continues to deteriorate. The number of malicious software programs causing security incidents involving mobile terminals has increased 331.3% compared to 2012. Among the 702,861 malicious software modules detected by CNCERT, 99.5% of them targeted Android-based terminals.

However, China's current information assurance system is not able to completely defend all the different types of cyber attacks. China faces challenges in management, technology, and human resources in addressing the cyber security issue as follows.

1. Management

   Laws and regulations regarding information security lag behind the rapid development of IT technologies and applications. Government organizations that are in charge of information security lack a clear description of responsibilities.

2. Technology

   China's cyber security emergency response capability needs to be improved. At present, China lacks capacity in the following:

   - Monitoring unknown vulnerabilities and unknown attacks.
   - Accurate assessment of security status at the macro level.
   - Early warning of some specific security incidents.
   - Appropriate methods to retrieve sources of APT attacks.
   - Tracking attack incidents outside of China.
   - Timely decision-making on major emergency incidents.
   - Appraising the effectiveness of methods for handling emergencies.

In addition, the majority of network equipment and protection software used in China are imported. The lack of core IT technologies (such as CPU and OS) poses a threat to the nation's overall level of information security. Other previously published ATIP reports have discussed aspects of China's efforts to develop their own basic technologies in these areas.

3. Human Resources

The security awareness of staff members is usually weak. Multidisciplinary experts are urgently needed to work in the information security field.

3. MAJOR GOVERNMENT RESEARCH PROGRAMS

Cyber security research on fundamental theory and frontier technologies is primarily supported by the 863 and 973 programs of MOST as well as a variety of NSFC programs. The Ministry of Industry and Information Technology (MIIT) and the National Development and Reform Commission (NDRC) also support industry-related and application-oriented R&D in the field of cyber security.

3.1 High-Technology Research and Development Program (863 Program)

MOST's 863 Program supports emerging technologies and frontier technologies that have the potential to foster high-tech/new industries and create proprietary intellectual property (IP). Information security has been supported as a priority in both the 11th Five-Year Plan period (2006-2010) and the 12th Five-Year Plan period (2011-2015), with different research targets.

1. Funding Focus During the Period 2006-2010

- Public opinion analysis; warning technology and systems.
- Monitoring cyber security incidents; developing control technology and systems.
- Demonstrations of technical systems and applications using commercial cipher codes.
- Security testing and evaluation technology and systems.
- Platform technologies for trusted computing.
- Monitoring and management systems on Internet audio/video contents.
- Telecommunications security gateway systems.

2. Funding Focus During the Period 2011-2015

- Security sensing key technologies for IoT; simulation verification platform.
- High-confidence and controlling technology for cloud computing platforms.
- Security testing and security enhancing technology for smart terminals.

Some recent projects are summarized below.

1. Key technologies for secure sensing layer in Internet of Things (IoT), and simulation verification platform

   This project is being led by Prof. Jie HUANG at Southeast University with about 10 million RMB (~US$1.6 million) in funding from the 863 Program for a period of three years (2013-2016). This project studies the following topics:

   - Secure systems of sensing layers in IoT.
   - Lightweight encryption technology and authentication mechanisms.
   - Node stealth communications and secure routing technology for attack-resistant nodes.
   - Node distinguishing, privacy protection, and tolerant technologies for intrusive malicious nodes.
   - Building IoT secure application simulation platforms for critical areas and sectors.

2. Smart terminal security testing and security enhancing technologies

   The National Information Center of CAS, Beijing University of Technology (BUT), Hubei University of Police, and the first Branch of Beijing Municipal People's Procuratorate are jointly carrying out this three-year project (2014-2017), which consists of the following four research directions. Respective funding for each topic area is 3 million RMB (US$490K), 2 million RMB (US$327K), 2 million RMB, and 3 million RMB.

   - Security testing technologies for smart terminals.
   - Vulnerability detection and mining technologies for smart terminal applications.
   - Electronic forensic technologies for novel smart terminals.
   - System kernel security enhancing technologies for smart terminal.

3. High confidence and controlling technologies for cloud computing platform, and its supporting system

   This three-year project (2015-2018) includes the following research directions:

   - How to verify, audit, and evaluate the credibility of a cloud platform from the third party perspective.
   - Detection technologies for malicious behavior under a cloud computing environment.
   - Tracking the responsible party of cloud security based on information stream, and the associated control technologies.
   - Cloud data privacy protection technologies.
   - How to provide trusted services under a cloud computing environment, and demonstration applications.

3.2 National Basic Research Program of China (973 Program)

MOST's 973 Program supports both basic and applied research. During the 11th Five-Year Plan period (2006-2010), fundamental research on information security was funded as a priority. During the 12th Five-Year Plan period (2011-2015), information security under a

cloud environment was also funded as a priority. Some recent projects are summarized below.

1. Key mathematics problems in modern cryptography

   This five-year project (2013-2018) is being led by Prof. Xiaoyun WANG at Tsinghua University with participation from Peking University, the CAS Academy of Mathematics and Systems Science (AMSS), the University of Science and Technology of China (USTC), IIE of CAS, Nankai University, and Shandong University. Funding in the amount of 14 million RMB (~US$2.23 million) was allocated for the first two years, and 15.57 million RMB (~US$2.5 million) was allocated for the last three years. This project aims to make progress in the following areas: (1) sphere's lattice packing and covering, (2) rational point theory of elliptic curve, (3) solving finite-domain algebraic equation and provide cipher application solutions to different sectors.

2. Fundamental theory and methods on cloud computing security

   This five-year project (2014-2019) is being led by Prof. Hai JIN at Huazhong University of Science and Technology (HUST), with participation from both Wuhan University and IIE of CAS. Funding in the amount of 6.45 million RMB (~US$1.1 million) was allocated for the first two years, and funding for the last three years will be determined after a mid-term evaluation. This project aims to study three scientific problems: (1) how to construct cloud systems safely, (2) secure sharing of cloud-based services, and (3) security and control of cloud data.

3. Construction safety-critical software and quality assurance methods

   This five-year project (2014-2019) is being led by Prof. Jian ZHANG of the CAS Institute of Software (IOS). Funding in the amount of 6.91 million RMB (~US$1.13 million) was allocated for the first two years, and funding for the last three years will be determined after the mid-term evaluation. Safety-critical software refers to software used in the aerospace, transportation, finance, medicine, and national defense sectors. Disabling such software would cause catastrophic consequences such as casualties, financial loss, and environmental damage. This project consists of the following three subprojects: (1) software requirements and design: modeling and verification; (2) software testing and analysis; and (3) software operation surveillance and behavior prediction.

4. Fundamental theory and key technologies on detection and control of malicious behaviors in mobile applications

   This five-year project (2015-2020) is being led by Prof. Ming YANG ZHANG of Fudan University. Funding in the amount of 1.9 million RMB (~US$310K) has been allocated for the first two years, and funding for the last three years will be determined after the mid-term evaluation.

3.3 National Natural Science Foundation of China (NSFC) Programs

NSFC funds basic research. Trusted computing was supported as a priority area during the 11th Five-Year Plan period (2006-2010). Some of the projects related to information security that have recently been selected for funding are presented in Table 1 below.

Table 1: NSFC-Funded Projects Related to Information Security

No.	Name of Project	Organization	Funding (RMB)	Term
1	Trusted multi-party computation under distributed environment	Nanjing University	4 million	Jan. 2015-Dec. 2019
2	Privacy protection under wireless mesh network and key exchange	Hubei University for Minorities	800,000	Jan. 2015-Dec. 2018
3	Key technologies on wireless network interference-resistant protocol based on cross layers	Zhejiang University	830,000	Jan. 2015-Dec. 2018
4	Privacy protection under cloud computing environment and remote assessment technologies	China Academy of Telecommunication Research (CATR)	800,000	Jan. 2015-Dec. 2018
5	Risk assessment method on mobile malicious program based on APP web behavior tracking and feature learning	Nanjing University of Science and Technology	840,000	Jan. 2015-Dec. 2018
6	Web data stream-oriented unknown application protocol deduction technology	Institute of Information Engineering (IIE) of CAS	230,000	Jan. 2015-Dec. 2017
7	Theoretical model, architecture and its control mechanism of software defined network (SDN)	Tsinghua University	3.2 million	Jan. 2015-Dec. 2019
8	Security status analysis theories and methods for new communication networks	Shanghai Jiaotong University (SJTU)	3.6 million	Jan. 2015-Dec. 2019
9	Key theory and technology on dynamic trusted SDN firewall under cloud computing environment	Wuhan University	260,000	Jan. 2015-Dec. 2017
10	Key technologies on emergency response to computer virus	Hunan Police Academy	830,000	Jan. 2015-Dec. 2018
11	Novel encrypt algorithm for multimedia based on physical model	Chongqing University of Post and Telecommunications	530,000	Jan. 2015-Dec. 2018
12	Recognition model of hardware Trojans based on power consumption characteristics, and algorithm study	National University of Defense Technology (NUDT)	700,000	Jan. 2015-Dec. 2018
13	Authentication and encryption protocol design based on stream cipher architecture	IEE of CAS	800,000	Jan. 2015-Dec. 2018
14	Encryption of key-dependent clear text	IEE of CAS	810,000	Jan.2 015-Dec. 2018
15	Key technologies on position privacy protection of Internet of Things	IEE of CAS	830,000	Jan. 2015-Dec. 2018

No.	Name of Project	Organization	Funding (RMB)	Term
16	Lattice-based method in public-key cryptographic analysis and algebraic attack	IEE of CAS	800,000	Jan. 2015-Dec. 2018
17	Public key cryptographic theory and key technologies targeting characteristics of quantum computer	Wuhan University	3 million	Jan. 2014-Dec. 2018
18	Software vulnerability based on graph theory	Beijing Forestry University	750,000	Jan. 2014-Dec. 2017
19	Quantum authentication mechanism based on chaotic cryptographic system	Central South University	750,000	Jan. 2014-Dec. 2017
20	Forensics method for multimedia content	IEE of CAS	3 million	Jan. 2014-Dec. 2018
21	Optimization, security and information services of large-scale networked system	Xi'an Jiaotong University	6 million	Jan. 2013-Dec. 2015
22	Data security under cloud computing environment: theory and key technologies	Nanjing University of Information Science and Technology (NUIST)	2.75 million	Jan.2013-Dec.2017
23	Key technologies for privacy protection in the Internet of Things	Nanjing University of Post and Telecommunications (NUPT)	580,000	Jan. 2012-Dec. 2015

4. LEADING RESEARCH GROUPS

Cyber security research on fundamental theory and frontier technologies is primarily being conducted by CAS institutes and some university research teams, including the following:

- IEE of CAS (comprehensive cyber security research)
- IOS of CAS (trusted computing, test and evaluation)
- ICT of CAS (software security based on compiling technology)
- Prof. Huanguo ZHANG and his team at Wuhan University (trusted computing & cryptography)
- Prof. Xiaoyun WANG and her team at Tsinghua University and Shandong University (cryptography)
- Prof. Haixin DUAN and his team at Tsinghua University (web security & intrusion detection)
- Prof. Wenchang SHI and his team at Renmin University (security of OS and basic software)
- Profs. Jianwei PAN & Gangcan GUO's teams at USTC (quantum cryptography)
- Prof. Min YANG and his team at Fudan University (mobile security)
- Prof. Yan CHEN and his team at Zhejiang University (security of software defined networks and mobile systems)
- Prof. Jie HUANG and his team at Southeast University (security of wireless networks and IoT)

4.1 Institute of Information Engineering (IIE) of CAS

IIE of CAS was set up in 2011 by restructuring a few groups that engaged in information security research from IOS, ICT, and the CAS Graduate School. IIE performs research on fundamental theory and frontier technologies in IT and information security, and develops application technology and systems. It consists of six research laboratories, which are presented in Table 2 below along with their research interests and personnel.

Table 2: Research Laboratories at IIE of CAS

Lab No.	Lab History	Current Research Interests	Research Team
1	Founded as the State Key Laboratory of Information Security (SKLOIS) in 1989, affiliated with IIE in 2012	Cryptographic theory and technology, security protocols and systems, network and system security, countermeasures against threats, and security of IoT	More than 70 faculty members, including 12 research fellows and 12 associate research fellows; about 210 non-permanent researchers, including visiting scholars, post-docs, and graduate students
2	Founded as the National Engineering Laboratory for Content Security Technologies in 2008, affiliated with IIE in 2012	Information content recognition and understanding, information retrieval and public opinion computing, data mining and deep learning, network and system security, security defense for fusion networks, countermeasures to cyber attacks, mass data storage management, web information-processing architecture	More than 100 faculty members, including two research fellows and 18 associate research fellows
3	Founded as Data Assurance & Communication Security Research Center in 1989, affiliated with IIE in 2012	Network and system security, data security and cryptographic engineering, cryptography, secure protocols	43 faculty members, including seven research fellows and 13 associate research fellows; about 100 non-permanent researchers, including visiting scholars, post-docs, and graduate students
4	Founded as the Key Laboratory of Security Technology previously, and affiliated with IIE in 2012	Web security technology, mobile wireless network security technology, TEMPEST electromagnetic security technology, security risk assessment technology, location-based testing and evaluation of audio and optical information leaks, comprehensive electromagnetic protection, web infiltration testing and forensic technology	Over 50 faculty members, including three research fellows

Lab No.	Lab History	Current Research Interests	Research Team
5	New lab founded in 2013 after IIE was set up in 2012	Architecture of secure computer, System-on-Chip (SOC) and embedded systems, security of operating systems, trusted computing, cyberspace trust, cloud computing and cyber security, software defined networks, large-scale network sensing and control, mobile Internet and smart devices, content networks, future network and testing infrastructure	More than 70 faculty members, including 20 research fellows and associate research fellows; about 150 non-permanent researchers, including visiting scholars, post-docs, and graduate students
6	New lab founded in 2014 after IIE was set up in 2012	Cyberspace risk assessment, software vulnerability analysis, mobile and web security examination, penetration test (pentest) technology	About 50 faculty members

Among the six research laboratories, the State Key Laboratory of Information Security (SKLOIS) is conducting the most comprehensive research related to cyber security. The detailed research directions of SKLOIS are listed below.

1. Cryptography

- Cryptography-related mathematical theory
- Cryptographic algorithm design and analysis
- Cryptographic algorithm testing & assessment methods and implementation techniques
- Novel cryptographic theory and techniques (quantum cryptography, visual cryptography)

2. Security Protocols & Systems

- Formal analysis and verification theory of security protocols
- Complexity theory of security protocol, and its application
- Theory on multi-party secure computation protocol
- Design, analysis, and testing of practical security protocols
- Information security systems

3. Network and System Security

- Network security architecture
- Authentication, authorization, and responsibility definition theory and techniques
- Security techniques for trusted computing
- OS and database security
- Wireless and mobile communication security
- Trust system of cyberspace
- Security of smart terminals
- Security of IoT

4. Countermeasures against Threats

- Reverse analysis and controllable techniques
- Vulnerability analysis of networks and systems, and risk assessment
- Intrusion detection, forensics, surveillance, and emergency response
- Malicious code analysis and prevention technology
- Cyber attack technology
- Information hiding and digital IPR protection

4.2 Tsinghua University

There are two research groups engaged in cyber security research at Tsinghua University: (1) the Research Center on Cryptographic Theory and Technology led by Prof. Xiaoyun WANG, and (2) the Network and Information Security Lab (NISL) led by Prof. Haixin DUAN.

1. Research Center on Cryptographic Theory and Technology

Founded in December 2009, the center's research directions include:

- Cryptographic theory
- Mathematic problems of cipher
- Cryptographic technology and its applications
- Quantum cryptography and quantum computing
- Cyber security

The center's director, Prof. Xiaoyun WANG, is a leading researcher in the field of cryptography. She proposed the collision attack on the world's widely-used hash function standards MD5 and SHA-1. She also proposed a subkey recovery attack on Message Authentication Codes (MAC) ALPHA-MAC, MD5-MAC and PELICAN, as well as the distinguishing attack on HMAC-MD5. These efforts have had a major impact on new research on hash functions. The center's vice-director Prof. Xiangbing WANG has proposed practical decoy-state quantum cryptography protocols that increased the distance of quantum key distribution (QKD) using weak coherent light from 20 km to 120-150 km.

2. Network and Information Security Lab (NISL)

NISL is one of the labs within the Institute for Network Sciences and Cyberspace. Research directions of NISL include:

- Network secure architecture
- Security analysis of network protocol and intrusion detection
- Network security monitoring
- Malicious code analysis
- Anti-spam techniques

NISL has been conducting a number of projects funded by government programs, including the following:

- CNGI Project: Identification, Authentication and Credit Service System for Campus Networks based on Validated Source IP Addresses. PI: Prof. Jianping Wu, Prof. Haixin DUAN, 2009-2011.
- Key Projects in the National Science & Technology Pillar Program Sub-Program: Trusted Internet Security Service -- Public Key Infrastructure, PI: Prof. Haixin DUAN, 2009-2011.
- 973 Project: Internet Governance and Security Research based on Autonomy Management, PI: Prof. Jilong WANG, Prof. Haixin DUAN, 2009-2014.
- NSFC Project: Mechanism Analysis and Detection Methods of Drive-by Download Exploits, PI: Prof. Jianwei ZHUGE, 2011-2013.

4.3 Wuhan University

The Ministry of Education's Key Laboratory of Aerospace Information Security and Trusted Computing at Wuhan University was founded in 2008. It currently has 29 faculty members, including 11 professors and 10 associate professors. Researchers of this laboratory have been conducting theoretical, technical, and applied research in the following directions:

- Information security in aerospace: spatial information sphere model, semantic navigation, applied research of aerospace information security, and aerospace information simulation.
- Trusted computing: theory of trusted computing, trusted computing system architecture, trusted computing platform, trusted software, trusted networks, and applications of trusted computing.
- Cryptography: evolutionary cryptography, and automatic cipher design and analysis based on evolutionary cryptography.
- Cyber security: locate attacks from hackers and malicious codes, rapid response and forensic technology to cyber attacks, digital copyright protection and tracking, digital content forensic technology, covert communication and its detection, key technologies for disaster recovery.

One of the representative achievements of this laboratory is evolutionary cryptography, which was proposed by Prof. Huanguo ZHANG and Prof. Zhongping QIN's team. They introduced evolutionary computing into cryptography. Based on concepts of biological evolution, automatic cipher design and analysis could be realized, providing a new perspective to cryptography and forming a new type of cryptographic system.

4.4 Shandong University

The Key Laboratory of Cryptographic Technology and Information Security at Shandong University was planned in 2005 and officially approved by the Ministry of Education in 2007. Prof. Xiaoyun WANG has been the director of this laboratory since 2006 (she also holds a position at Tsinghua University - see section 3.2 above for more details). This laboratory currently has 42 faculty members, including 17 professors and 17 associate professors. Research directions include:

- Theory of cryptology
- Application of cryptography and security techniques

- Secure computation of number theory and algebra
- Security of networks and systems

5. RESEARCH PROGRESS

In China, information security research focuses on five areas: 1) cryptography, 2) network security, 3) information system security, 4) information content security, and 5) countermeasures against threats. With the increasing risks that accompany cloud computing, big data, IoT, and mobile systems, some basic research is also being conducted to address new threats in these areas. However, information security research in China has not been conducted in a systematic way, and it primarily involves applications of technology or improvement of existing technologies rather than original innovation. The overall level of Chinese information security research still lags behind the advanced international level. In the past, Chinese researchers have made some achievements in the area of theoretical studies of cryptography, trusted computing platforms (TCP), and WLAN Authentication and Privacy Infrastructure (WAPI) technology. Some of the papers recently published by Chinese researchers are summarized in this section.

5.1 Cryptography

- KDM-CCA Security from RKA Secure Authenticated Encryption

  Key dependent message (KDM) security is stronger than the traditional semantic security. It has extensive application value in protocol design, hard disk encryption, and fully homomorphic encryption. Since the plaintext message is dependent on the secret key of the encryption scheme, the construction of a KDM secure scheme under the standard model remained open until the first construction under the chosen plaintext attack (CPA) was proposed in 2008. However, the approach to achieve KDM-CPA security conflicts with the requirement of chosen ciphertext security (CCA). Although the existence of a KDM-CCA secure scheme was demonstrated by cryptographers in 2009, practical construction remains open. In 2013, Hofheinz proposed a CIRC-CCA secure encryption scheme, but such a scheme only guarantees KDM-CCA security with respect to selection functions. The main difficulty of constructing KDM-CCA secure schemes is that resolving the conflict between KDM and CCA requires a polynomial amount of entropy, while the secret key can only provide a linear amount of entropy. To resolve this problem, Hofheinz proposed a new tool called a “lossy algebraic filter” (LAF), which guarantees that the adversary cannot obtain excessive entropy by means of lossy. For the restriction of the mathematical structure, the technique based on LAF only allows the use of selection functions.

  Based on the previous research work on related key attacks (RKAs), Xianhui LU et al. at SKLOIS of IIE, CAS proposed a new solution to this problem: an entropy reuse technique based on the RKA secure authenticated encryption. The main concept behind their solution is reusing the entropy after linear re-randomizing. The proposed solution breaks through the limitation of the LAF and achieves KDM-CCA security with respect to affine functions.

  This paper was accepted by the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2015), which was held in Sofia, Bulgaria from April 26-30, 2015.

- Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers

  Differential cryptanalysis is one of the most well-known attacks on modern block ciphers, and a number of cryptanalytic techniques have been developed based on this concept. In comparison with the single-key model, the understanding of the security of block ciphers with regard to related-key differential attacks is relatively limited, although improvement has been made in recent years. For bit-oriented block ciphers such as PRESENT-80 and DES, methods proposed in previous research either cannot be used to search for actual (related-key) differential characteristics or are applicable only to ciphers with a linear key schedule. Siwei SUN et al. at IIE of CAS provided a method based on Mixed-Integer Linear Programming (MILP) that is capable of not only evaluating the security (obtain security bound) of a block cipher with respect to the (related-key) differential attacks, it can search for actual (related-key) differential characteristics, even when the key schedule algorithm of the block cipher is nonlinear.

  The researchers proposed two systematic methods to describe the differential property of an S-box with linear inequalities based on logical condition modeling and computational geometry, respectively. In one method, inequalities are generated according to some conditional differential properties of the S-box. In the other method, inequalities are extracted from the H-representation of the convex hull of all possible differential patterns of the S-box. For the second method, they developed a greedy algorithm for selecting a given number of inequalities from the convex hull. Using these inequalities combined with the MILP technique, SUN et al. proposed an automatic method for evaluating the security of bit-oriented block ciphers against the (related-key) differential attack with several techniques for obtaining tighter security bounds.

  They also developed a new tool for finding (related-key) differential characteristics automatically for bit-oriented block ciphers. Using this tool, they obtained new single-key or related-key differential characteristics for SIMON48, LBlock, DESL and PRESENT-128, which cover a larger number of rounds or have a larger probability than all previously known results. The methodology presented by the researchers at CAS is generic, automatic, and applicable to many bit-oriented block ciphers. This paper was accepted by the 20th Annual International Conference on the Theory and Application of Cryptology and Information Security (AsiaCrypt 2014), which was held in Kaoshiung, Taiwan from December 7-11, 2014.

5.2 Web Security

- When HTTPS Meets CDN: A Case of Authentication in Delegated Service

  Content Delivery Network (CDN) and Hypertext Transfer Protocol Secure (HTTPS) are two popular but independent web technologies, each of which has been well studied individually and independently. Jinjin LIANG et al. from the Institute for Network Science and Cyberspace at Tsinghua University conducted a systematic study on how these two work together. They examined 20 popular CDN providers and 10,721 of their customer websites using HTTPS. Their study revealed various problems with the current HTTPS practice adopted by CDN providers, such as widespread use of invalid certificates, private key sharing, neglected revocation of stale certificates, and insecure

back-end communication. While some of these problems are operational issues only, others are rooted in the fundamental semantic conflict between the end-to-end nature of HTTPS and the man-in-the-middle nature of CDN involving multiple parties in a delegated service. To address the delegation problem when HTTPS meets CDN, they proposed a lightweight solution based on the "DNS-based Authentication of Named Entities" (DANE), an emerging IETF protocol complementing the current Web PKI model. Their implementation demonstrated that it is feasible for HTTPS to work with CDN securely and efficiently. This work is expected to raise the awareness of this emerging problem within security and the CDN community, and stimulate further discussion among practitioners and researchers on more preferable solutions. This paper was accepted by the 35th IEEE Symposium on Security & Privacy (IEEE S&P 2014), which was held from May 18-21, 2014 in San Jose, California (US).

- Vetting SSL Usage in Applications with SSLINT

  Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols have become the security backbone of the Web and Internet today. Many systems, including mobile and desktop applications, are protected by SSL/TLS protocols against network attacks. However, numerous vulnerabilities caused by the incorrect use of SSL/TLS APIs have been uncovered in recent years. Such vulnerabilities, many of which are caused due to poor API design and a lack of experience on the part of the application developers, often lead to confidential data leaks or man-in-the-middle attacks. In order to guarantee code quality and logic correctness in applications that use SSL/TLS, a scalable automated approach for security analysis is needed.

  In a collaboration with researchers from Northwestern University in China and Columbia University (New York) and the University of Illinois at Chicago in the US, Boyuan HE et al. at Zhejiang University jointly designed and implemented SSLINT, a scalable automated system for detecting the incorrect use of SSL/TLS APIs. By using static analysis techniques, it is capable of performing automatic logic verification with high efficiency and good accuracy. To demonstrate the feasibility of their approach as well as advantages of SSLINT, HE and his colleagues applied it to one of the most popular Linux distributions - Ubuntu. They found 27 unknown SSL/TLS vulnerabilities in Ubuntu applications, most of which are also distributed with other Linux distributions. This paper was accepted by the 36th IEEE Symposium on Security & Privacy (IEEE S&P 2015), which was held in San Jose, California (US) from May 18-20, 2015.

5.3 Intrusion Detection and Attack Analysis

- Protecting Private Keys against Memory Disclosure Attacks using Hardware Transactional Memory

  Cryptography plays an important role in computer and communication security. In practical implementations of cryptosystems, the cryptographic keys are usually loaded into the memory as plaintext, and then used in the cryptographic algorithms. Therefore, the private keys are subject to memory disclosure attacks that read unauthorized data from RAM. Such attacks could be performed through software methods (e.g., OpenSSL Heartbleed) even when the integrity of the victim system's executable binaries is maintained. They could also be performed through physical methods (e.g., cold-boot attacks on RAM chips) even when the system is free of software vulnerabilities.

Le GUAN et al. at SKLOIS of IIE, CAS proposed a solution named "Mimosa" that protects RSA private keys against the above software-based and physical memory attacks. When the Mimosa service is in idle, private keys are encrypted and reside in memory as ciphertext. During the cryptographic computing, Mimosa uses hardware transactional memory (HTM) to ensure that (a) whenever a malicious process other than Mimosa attempts to read the plaintext private key, the transaction aborts and all sensitive data are automatically cleared with hardware mechanisms, due to the strong atomicity guarantee of HTM; and (b) all sensitive data, including private keys and intermediate states, appear as plaintext only within CPU-bound caches, and are never loaded to RAM chips.

According to CAS researchers, Mimosa is the first solution to use transactional memory to protect sensitive data against memory disclosure attacks. They have implemented Mimosa on a commodity machine with Intel Core i7 Haswell CPUs. Extensive experiments show that Mimosa effectively protects cryptographic keys against various attacks that attempt to read sensitive data from memory, and Mimosa only introduces a small performance overhead. This paper was accepted by IEEE S&P 2015.

- Security Architecture to Deal with APT Attacks: Abnormal Discovery

Facing the advanced persistent threat (APT), the existing security architecture cannot help users detect threats in a timely manner before serious economic losses have occurred. Based on an in-depth analysis of APT, Yuejin DU et al. at IIE of CAS proposed a theoretical defending framework, i.e., abnormal discovery, which is the prerequisite of defending policy and protective measures. Based on the theoretical framework of abnormal discovery, Yuejin DU et al. designed a security architecture named "Wizeye" (see Figure 1 below).

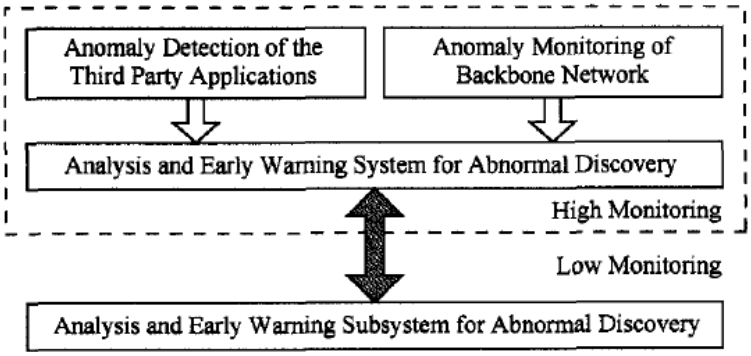

Figure 1. The framework of Wizeye

As shown in Figure 1, "low monitoring" refers to a subsystem targeting terminals. The low monitoring system is different from traditional security defense software, because it not only detects known threats, but unknown threats as well. "High monitoring" refers to a subsystem targeting sources and pathways. The high monitoring system can detect massive abnormalities in backbone networks and dig out malicious applications from sources. By combining the high and low monitoring systems, the Wizeye system can monitor and detect the APT from its source, pathway, and terminal.

So far, the high monitoring system has been deployed in China's National Cyber Security Center and used to monitor the backbone network. It is also used to detect abnormalities in app stores. For low monitoring, Yuejin DU and his colleagues developed a security-enhanced mobile operating system named “RayDroid” based on the Android platform. The RayDroid focuses on deep analysis of codes and threat detection based on correlative analysis of samples, since some threatening software are not necessarily traditional malicious codes. In the future, DU and his team will continue to improve the Wizeye system and try to use the high and low monitoring systems in practical applications. This paper was published in the *Journal of Computer Research and Development*, 51(7): 1633-1645, 2014 (in Chinese).

- Software Vulnerability Exploit Detection based on Illegal Control Flow Transfers Identification

  Software vulnerability is one major threat to the security of information systems. Although security mechanisms such as address space layout randomization (ASLR) and data execution protection (DEP) used in new OS have restrained attacks towards application software and system vulnerability, attacks by hijacking control flow still occur. To address such attacks under a new security environment, control flow integrity (CFI) testing and dynamic taint analysis were proposed by academia and API intercept technology was proposed by some security software vendors. However, the above-mentioned methods have different limitations. Minghua WANG et al. from the Laboratory of Trusted Computing and Information Assurance at IOS, CAS proposed an approach to detect exploits based on the identification of illegal control flow transfers.

  They proposed to construct the control flow safety outline (CFSO) first by performing both static and dynamic analyses. The control flow transfer out of the CFSO during the execution of programs is identified as abnormal control flow transfer, which might be an exploit attack. When a call/ret/jmp is about to execute, the target is checked according to the CFSO. The illegal control flow transfer is considered to be an exploit attack, and all of the subsequent attacking steps can be captured. The proposed method has higher accuracy and better operation efficiency than the traditional taint analysis method. It is also able to detect attacks that cannot be detected using the CFI method, such as JIT Spraying. The exploit detection prototype system based on the identification of illegal control flow transfers was tested through eight experiments targeting vulnerabilities in Microsoft (MS) Word, Internet Explorer (IE), and Adobe Flash Player. The experimental results showed that the proposed method had high accuracy, decent overhead, and could be applied to detect exploits online. This paper was published in the *Journal on Communications* 35(9): 20-31, 2014 (in Chinese).

- DDoS Attack Collaborative Detection System based on Information Entropy

  Distributed denial of service (DDoS) is one type of denial of service attack that is prevalent and causes great economic loss and damage. Since the methods of DDoS attacks are getting more diverse and intelligent, more sophisticated attack detection and defense technology are now required. However, the existing attack detection technologies also need to be improved in terms of timeliness and accuracy. With the goal of detecting DDoS in a real-time manner, Hong-tao SONG et al. from the College of Computer, National University of Defense Technology (NUDT) proposed a DDoS collaborative detection method based on information entropy.

The proposed detection system focuses on two aspects: local detection and global collaborative decision. In local detection, the suspicious summary matrix is generated based on information entropy and the clustering algorithm of subspace. Based on such a matrix, the local detection module is designed to preliminarily filter suspicious information. NUDT researchers adopted a Sketcher structure to store traffic data and optimize storage capacity, which helps realize real-time Internet traffic monitoring. In the global collaborative decision, all local suspicious information is integrated globally. An aggregation tree is constructed by a Distributed Hash Table (DHT) algorithm to share paths. A global decision module based on the collaborative work of all detecting nodes finally determines whether there are any DDoS attacks. The accuracy and timeliness of the proposed method were each tested in comparison with the existing single point detection method and centralized single point detection method, respectively. Testing results showed superior performance of the proposed method. This paper was published in the *Journal of Chinese Computer Systems* 36(1): 133-137, 2015 (in Chinese).

5.4 Cloud Security

- Fine-grained and heterogeneous proxy re-encryption for secure cloud storage

The cloud is an emerging computing paradigm, but the security issues associated with the cloud environment are considered to be a critical obstacle in its rapid development. When data owners store their data as plaintext in a cloud, they lose the security of their cloud data due to the potential of arbitrary accessibility, especially access by the untrusted cloud. One promising approach to protecting the confidentiality of data in the cloud is the data owners' encryption of data prior to storing it there. However, the straightforward employment of the traditional encryption algorithms cannot solve the problem well, since it is hard for data owners to manage their private keys if they want to securely share their cloud data with others in a fine-grained manner.

Peng XU et al. at the Services Computing Technology and System Laboratory of HUST proposed a fine-grained and heterogeneous proxy re-encryption (FH-PRE) system to protect the confidentiality of cloud data. The architecture of the proposed secure cloud storage is shown in Figure 2 below.

Suppose that data owners and data consumers belong to different cloud storage systems that are respectively equipped with the cryptographic primitives IBE and Elgamal. The proposed PRE system allows proxy to transform the IBE ciphertexts of data owners to new ciphertexts, and these new ciphertexts can be decrypted by the correlated Elgamal private keys of the data consumers. Thus, data consumers can share cloud data, even when they are in different cloud systems. Moreover, the proposed PRE system does not require data consumers to register in the same cloud system as the data owner. To realize fine-grained sharing of the data owners' cloud data, the proposed PRE system employs the same method as the previous work (called ITHJ08). It allows a data owner to assign a PTI for each of his cloud data and the generation of a re-encryption key. When receiving a re-encryption key, only proxy can reencrypt the ciphertexts that have the same type with the re-encryption key. In addition, a novel function is equipped in the proposed PRE system that allows the data owner to update old types of cloud data. This function provides more flexible access control of the data owners' cloud data than ITHJ08. Performance tests showed that the

proposed PRE has more efficient re-encryption and decryption processes. This paper was published in the *Journal of Chinese Science Bulletin* 59(32): 4201-4209, 2014.

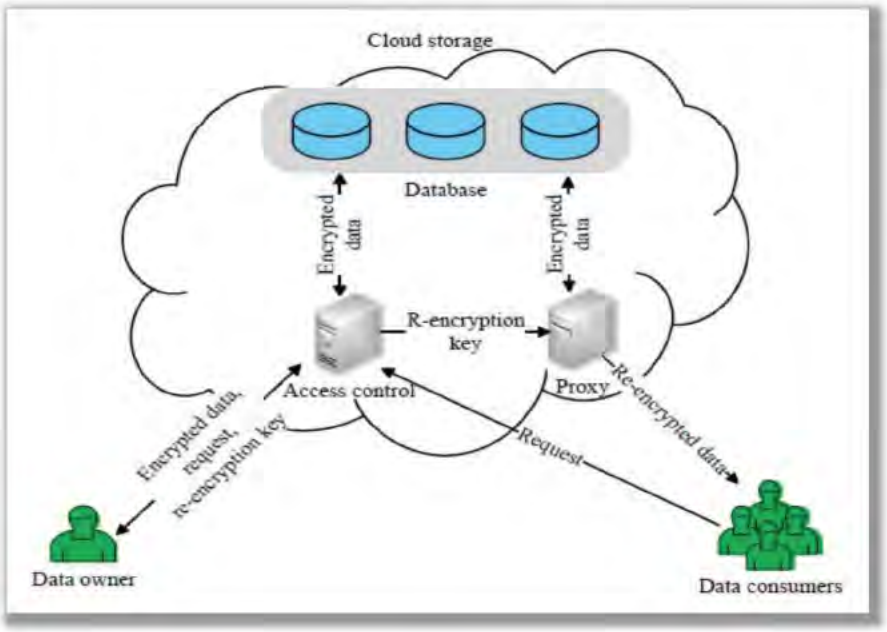
Cloud storage
Database
Encrypted data
Encrypted data
R-encryption key
Access control
Proxy
Encrypted data, request, re-encryption key
Request
Re-encrypted data
Data owner
Data consumers

Figure 2. Architecture of the FH-PRE based cloud storage

- Secure Application Model based on Identity Management under Cloud Computing Environment

  Under a cloud computing environment, multiple entities are involved, such as users, terminal equipment, virtual entities and physical entities, Infrastructure as a Service (IaaS) resources, Platform as a Service (PaaS) resources, and Software as a Service (SaaS) resources. To every user under the cloud computing environment, it is very dangerous to engage with any entity without knowing its identity. Thus, multi-entity identity management under the cloud computing environment must be addressed. However, previous research on identity management lacks either technical considerations about the cloud scenario or solutions to address the cloud resource's dynamics, virtualization, and management. Yazhe WANG et al. at SKLOIS of IIE, CAS proposed encoding multiple entities by a unified identification structure. They also proposed methods for the following: 1) distributed storage of entity identity, 2) privacy protection of multi-entity identity, and 3) security auditing based on identity association mapping. These proposed methods were implemented successfully, indicating entity identity management can be realized within the cloud computing environment. This paper was accepted by the International Conference on Future Computer and Communication Engineering (ICFCCE 2014), which was held in Tianjin, China from March 27-28, 2014.

5.5 Mobile Security

- DeepDroid: Dynamically Enforcing Enterprise Policy on Android Devices

  It is becoming a global trend for company employees equipped with mobile devices to access their company's assets. Besides enterprise apps, numerous personal apps from various untrusted app stores may also be installed on those devices. To secure the business environment, enforcing policies regarding what, how, and when certain apps can access system resources is required by enterprise IT. However, Android, the largest mobile platform, provides very restricted interfaces for enterprise policy enforcement.

  Xueqiang WANG et al. at the Data Assurance and Communication Security Research Center at IIE of CAS proposed a scheme named "DeepDroid," which is a dynamic enterprise security policy enforcement scheme on Android devices. Unlike existing approaches, DeepDroid is implemented by dynamic memory instrumentation of a small number of critical system processes without any firmware modification. The DeepDroid can be easily deployed on various smart phone platforms with a wide range of Android versions. Moreover, based on the context information extracted from Binder interception, a fine-grained policy can be enforced. CAS researchers developed a prototype of DeepDroid and tested it on various smart phones and Android versions. The experimental results showed that DeepDroid could effectively enforce enterprise resource access policies with negligible performance overhead. This paper was accepted by the 2015 Network and Distributed System Security Symposium (NDSS Symposium 2015), which was held from February 8-11, 2015 in San Diego, California (US).

- AppIntent: Analyzing Sensitive Data Transmission in Android for Privacy Leakage Detection

  Since Android phones often carry personal information, malicious developers have become interested in embedding code in Android applications aimed at stealing sensitive data. With known techniques in the literature, one may easily determine whether sensitive data is being transmitted out of an Android phone. However, transmission of sensitive data in itself does not necessarily indicate a privacy breach; a better indicator might be whether it was the device user's intention to transmit the data. When transmission is not the user's intention, it is more likely a privacy breach. The problem is how to determine whether or not the user intended to transmit the data.

  As the first approach to resolving this issue, Zhemin YANG et al. at Fudan University proposed a new analysis framework called "AppIntent." For each data transmission, AppIntent can efficiently provide a sequence of GUI manipulations corresponding to the sequence of events that led to the data transmission, thus helping an analyst to determine whether the data transmission is user-intended or not. The basic idea is to use symbolic execution to generate the aforementioned event sequence, but straightforward symbolic execution has been shown to be too time-consuming to be practical. A major innovation in AppIntent is leveraging the unique Android execution model to reduce the search space without sacrificing code coverage. The researchers at Fudan conducted an evaluation of AppIntent using a set of 750 malicious apps, as well as 1,000 of the top free apps from Google Play. The results show that AppIntent can effectively help separate the apps that truly leak user privacy from those that do not. This paper was accepted by the 20th ACM Conference on Computer and Communications Security (CCS 2013), which was held from November 4-8, 2013 in Berlin, Germany.

5.6 Security of Wireless Sensor Networks (WSNs)

- A Security Key Distribution Scheme based on Energy Efficiency for Hybrid Wireless Sensor Networks

  According to their function and structure arrangement, WSNs can be classified as either a flat network, hierarchical network, or a hybrid network. The hybrid network integrates structures of both flat and hierarchical networks. The flat structure is used between cluster heads or between the ordinary nodes, while the hierarchical architecture is used between cluster heads and the ordinary nodes. In the hybrid construct, the cluster heads are key nodes. If a cluster head were to be attacked, all of the nodes in the cluster would be compromised.

  Due to the low cost, limited resources, and large scale of WSN's, symmetric key-based key pre-distribution schemes are considered to be very suitable, but they cannot thoroughly solve the authentication or the resilience problems against physical capture. Some researchers have tried to improve the traditional public-key cryptography to meet the security requirements of the WSNs.

  Jie HUANG et al. at the Information Security Research Center of Southeast University developed a security mechanism for the hybrid WSNs. First of all, to create the hybrid network model, the number range of cluster heads is determined according to the change of the average path length, with the probability that the nodes are selected as

the cluster heads. Then, based on the characteristics of the hybrid WSNs, a novel security mechanism is proposed using the advantages of both symmetric and asymmetric cryptography. The proposed scheme can provide different security mechanisms for vital links and ordinary links, respectively. In order to balance the energy consumption across all nodes, a selecting cluster head algorithm is proposed to periodically rotate cluster heads among all nodes, and to compute the optimal frequency of transmitting data per round. The experimental results showed that the proposed scheme not only provides sufficient security, but also has the lowest energy overhead and sound connectivity. This paper was published in the *Journal of Security and Communication Networks* 7(8): 1189–1198, 2014.

6. CONCLUSION

The Chinese government has placed unprecedented importance on information security, especially after Edward Snowden leaked aspects of the US NSA's PRISM program. However, China's current information assurance system is not able to completely defend against all the possible types of cyber attacks, and China faces challenges in management, technology, and human resources in responding to the cyber security issue. Adopting independent and controllable core technologies in IT systems is the developing trend in China's assurance for cyber security.

Cyber security research on fundamental theory and frontier technologies is primarily supported by MOST's 863 and 973 Programs, as well as a variety of programs from NSFC. Security research on emerging technologies - such as cloud computing, IoT, mobile systems, and applications – have recently been funded as priorities. Institutes of the CAS and some university research teams are leading research groups in the field of cyber security. Among them, IIE is engaged in the most comprehensive research on cyber security. Information security research in China has not been conducted in a systematic way - it primarily involves applications of technology or improvement of existing technologies and lacks original innovation. The overall level of Chinese information security research still lags behind the advanced international level.

END OF REPORT


atip
asian technology
information program