International Workshop on Cyber Security, Trust and Privacy

网络空间安全、信任及隐私国际研讨会（International Workshop on Cyber Security, Trust and Privacy）将于2018年6月5日在西安电子科技大学新科技楼1012会议室召开。由网络与信息安全学院闫峥教授主持，受邀参加研讨会的专家学者包括美国弗吉利亚理工大学讲席教授、IEEE Fellow Wenjing Lou，芬兰赫尔辛基大学教授Valtteri Niemi，芬兰阿尔托大学教授Raimo Kantola，美国亚利桑那州立大学教授Yanchao Zhang，美国亚利桑那大学副教授Ming Li以及美国宾汉姆顿大学助理教授Yan Wang。

International Workshop on Cyber Security, Trust and Privacy **5 June, 2018** **Room 1012, New Science Building 新科技楼 1012**	
Session 1 Security, Trust and Privacy in IoT	
9:00-9:05	**Welcome and Introduction of the Workshop** Dr. **Zheng Yan**, Xidian University, China
9:05-10:05	Invited Talk: **The Internet of Things and its Security Challenges** Dr. **Wenjing Lou**, Virginia Tech, US
10:05-11:05	Invited Talk: **Security and Privacy in the Networked World: Some Challenges and Solutions** Dr. **Yanchao Zhang**, Arizona State University, US
11:05-12:05	Invited Talk: **Secret-Free Trust Initialization for Internet-of-Things Devices** Dr. **Ming Li**, University of Arizona, US
Session 2 Security, Trust and Privacy in 5G	
14:30-15:30	Invited Talk: **Cooperative Security for 5G and the Internet** Dr. **Raimo Kantola**, Aalto University, Finland
15:30-16:30	Invited Talk: **Identity and location privacy in 5G** Dr. **Valtteri Niemi**, University of Helsinki, Finland
16:30-17:30	Invited Talk: **Low-cost Fine-grained Human-Computer Interaction Using Heart Rate Sensor in Wearables** Dr. **Yan Wang**, SUNY Binghamton University, US

ISN 国家重点实验室

综合业务网理论及关键技术 国家重点实验室

State Key Laboratory of Integrated Services Networks

The Internet of Things and its Security Challenges

报告人：**Prof. Wenjing Lou**

Virginia Tech, America

报告时间：**2018年6月5日(周二)上午9:05**

报告地点：北校区新科技楼 **1012**会议室

Abstract: Internet of Things (IoT) is an emerging technology that has drawn a lot of attention in recent years. Things in IoT can take a wide variety of forms, from simple RFIDs attached to merchandises, smart thermostats installed in the classrooms, implantable medical devices on the patients, to video cameras on top of light poles, and automobiles with built-in sensors. The explosive deployment of IoTs has pushed the boundary of the cyber-world to be tightly intertwined with our physical world. The IoT enables the exchange of information in a variety of application scenarios, each having unique characteristics and requiring unique performance guarantees, and together they bring potentially tremendous benefits to us- home automation, environmental monitoring, health and lifestyle, smart cities, just to name a few.

Some significant risks go along with the potential benefits of the IoT. As we add devices to our cloths, bodies, homes, and environments, more personal information will be collected. Some information is deeply sensitive. As devices are more closely connected with our physical world and some are capable of taking actions, data security and device security become critically important. Last year, IoT devices have also been exploited to launch the largest DDoS attack in history to disrupt the Internet services.

A secure and trustworthy IoT is not an easy task. It demands multiple lines of defense from different layers to thwart attacks from both the physical world and cyberspace. It also requires the integration of security and privacy mechanisms into computing and networking functions. In this talk, I will introduce the network architecture and unique characteristics of IoT systems. I will then focus on unique security and privacy challenges in the IoT. Many of the security and privacy problems are very challenging and call for interdisciplinary expertise from a number of technical domains.

Bio: Wenjing Lou is the W. C. English Professor of Computer Science at Virginia Tech and a Fellow of the IEEE. She holds a Ph.D. in Electrical and Computer Engineering from the University of Florida. Her research interests cover many topics in the cybersecurity field, with her current research interest focusing on privacy protection techniques in networked information systems and cross-layer security enhancement in wireless networks.

Prof. Lou is currently on the editorial boards of IEEE Transactions on Dependable and Secure Computing, ACM/IEEE Transactions on Networking, IEEE Transactions on Mobile Computing, and Journal of Computer Security. She is the Steering Committee Chair of IEEE Conference on Communications and Network Security (IEEE CNS), which is a conference series in IEEE Communications Society (ComSoc) core conference portfolio and the only ComSoc conference focusing solely on cybersecurity.

ISN国家重点实验室，移动互联网安全111基地，网络与信息安全学院，国际合作与交流处

IEEE COMMUNICATIONS SOCIETY Xian Chapter

开放 流动 联合 竞争

综合业务网理论及关键技术 国家重点实验室
State Key Laboratory of Integrated Services Networks

Security and Privacy in the Networked World: Some Challenges and Solutions

报告人：**Prof. Yanchao Zhang**
Arizona State University, America

报告时间：**2018年6月5日(周二)上午10:05**

报告地点：北校区新科技楼 **1012**会议室

Abstract The human society is highly dependent on networked communications and also vulnerable to ever-growing cyber security and privacy threats. In this talk, I will first give a high-level overview of our recent cyber security research in multiple directions, such as online social networks, dynamic spectrum sharing, mobile device security, and indoor navigation. Then I will introduce EyeTell, our latest result published in the 2018 IEEE Symposium on Security and Privacy. In EyeTell, we propose a novel video-assisted attack that can infer a victim's keystrokes on his touchscreen device from a video capturing his eye movements.

Bio: Yanchao Zhang is a professor in the School of Electrical, Computer and Engineering at Arizona State University. He holds a Ph.D. in Electrical and Computer Engineering from the University of Florida. His primary research is on security and privacy issues in computer and networked systems, with current focus areas in emerging wireless networks, mobile crowdsourcing, Internet-of-Things, social networking and computing, wireless systems for disabled people, big data analytics, wearable computing, edge computing, mobile health, and AI.

Prof. Zhang has been on the editorial boards of IEEE Transactions on Mobile Computing, IEEE Wireless Communications, IEEE Transactions on Control of Network Systems, and IEEE Transactions on Vehicular Technology. He received the US NSF CAREER Award in 2009 and chaired the 2015 NSF Workshop on Wireless Security, the 2016 ARO Workshop on Trustworthy Human-Centric Social Networking, and the 2017 IEEE Conference on Communications and Network Security.

ISN国家重点实验室，移动互联网安全111基地，网络与信息安全学院，国际合作与交流处

IEEE COMMUNICATIONS SOCIETY Xian Chapter

开放 流动 联合 竞争

综合业务网理论及关键技术 国家重点实验室

State Key Laboratory of Integrated Services Networks

Secret-Free Trust Initialization for Internet-of-Things Devices

报告人：**Prof. Ming Li**

University of Arizona, America

报告时间：**2018年6月5日(周二)上午11:05**

报告地点：北校区新科技楼 **1012**会议室

Abstract: With the proliferation of personal wireless devices in the Internet-of-Things (IoT), such as mobile phones, wearable devices and smart home sensors, it becomes more and more critical to secure the communications among them by establishing initial trust (authenticated secret key establishment). The major challenge, is the lack of pre-shared secrets among IoT devices that are deployed in an ad hoc manner. In addition, personal devices are likely to be constrained in hardware interfaces and computational resources. Existing techniques such as device pairing usually need auxiliary secure channels or user interfaces that may not be present, and require significant human effort.

In this talk, we take a different "in-band" approach to establish initial trust without prior secrets, which is done purely using the wireless channel and with little human support. The key idea is to assure message integrity protection and authentication by detecting or preventing signal manipulation (or man-in-the-middle) attacks in the wireless channel. We first present HELP, which is a novel physical layer primitive that can detect any message modification with the aid of a co-located helper device that injects random authentication signals. HELP enables us to securely pair new devices with the hub with little extra effort. Then we introduce VERSE, another primitive that prevents signal manipulation using three or more devices as simultaneous verifiers, whose security is derived from basic signal propagation properties and geometrical constraints. VERSE enables secure pairing of a group of devices with the hub at the same time. Finally, we introduce the SFIRE protocol, which authenticates new devices with a moving helper based on received signal strength ratio, and can be implemented on commercial-off-the-shelf devices. Our schemes can resolve important challenges in IoT trust establishment, by eliminating default passwords, the need of public key infrastructure, while satisfying the efficiency and scalability requirements. Finally, I will discuss some future research directions in this area.

Bio: Ming Li is an Associate Professor in the Department of Electrical and Computer Engineering of University of Arizona. He was an Assistant Professor in the Computer Science Department at Utah State University from 2011 to 2015. He received his Ph.D. in ECE from Worcester Polytechnic Institute in 2011. His main research interests are wireless and cyber security, with current emphases on cross-layer optimization and machine learning in wireless networks, security and privacy of the Internet-of-Things and dynamic spectrum sharing, privacy-preserving data analytics, and security in cyber-physical systems including autonomous vehicles.

Prof. Li has been on the editorial boards of IEEE Transactions on Wireless Communications, and IEEE Wireless Communications Letters. He received the NSF Early Faculty

ISN国家重点实验室，移动互联网安全111基地，网络与信息安全学院，国际合作与交流处

IEEE COMMUNICATIONS SOCIETY Xian Chapter

开放　流动　联合　竞争

综合业务网理论及关键技术 国家重点实验室

State Key Laboratory of Integrated Services Networks

Cooperative Security for 5G and the Internet

报告人：**Prof. Raimo Kantola**
Aalto University, Finland

报告时间：**2018年6月5日(周二)下午 14:30**

报告地点：北校区新科技楼 **1012**会议室

Abstract: The prevailing attitude in current Internet security is “everyone for himself”. Sharing of knowledge in these matters is fragmented and poorly developed. In cooperative security, good guys form trust domains share evidence of misbehaviour and try to defend against the attackers with joint efforts. The cooperation is automated using suitable protocols and other systems. To help the cooperation, an ISP or any other customer network operator/admin has an important role in aggregating and processing evidence and sharing the results with others. In our implementation of the concept we use Customer Edge Switching (CES) which is still a research concept. When used, hosts are behind CES nodes that are generalised NATs and cooperative firewalls that form a chain of trust on a required level of trust from host-to-firewall to firewall-to-host. All flows are admitted based on a policy match at both ends of the communication path. Policies are per user/host. Upon detection of misbehaviour, a CES node can immediately delegate the restraining responsibility of the malicious or suspected host to the remote edge. The hypothesis is that the security engine is generic for most use cases but that the security can be tailored by modifying the policy management system to the use case such as Mobile Broadband or Industrial Internet. Besides the constructive work, we have looked at the motivation to cooperate as well as the adoption of trust management in a wide area context using game theory. We propose to use the CES concept first to defend ultra-reliable services in 5G against all attacks. The implementation follows SDN principles, so firewalling capacity is largely taken from the cloud. Customer Edge switching allows deployment one network at a time. For this purpose, it includes a Realm Gateway (RGW) which combines a destination side NAT (DNAT) with a DNS leaf node and admits dynamically flows from legacy Internet hosts to hosts in a private address space (such as a smart phone in Mobile network). Besides SDN, the implementation heavily relies on Linux capabilities.

Compared to the state of the art, CES adapts the Internet to the era when majority of the end devices are wireless and battery powered. It also provides a step-wise improvement of security by offering several automatic means of attack mitigation.

Bio: Raimo Kantola is a professor of Networking Technology at Aalto, Dept. of Communications and Networking. After some 15 years at Nokia Switching Systems in R&D, Product Marketing and Research in positions from SW designer to Department Head, Kantola joined TKK in 1996 as a pro tem professor and was tenured in 2005. His recent research is in the area of trust management and cooperative security for the Internet and 5G. At the moment the work is done in the contexts of 5G, Software Defined Networking and the Industrial Internet.

ISN国家重点实验室，移动互联网安全111基地，网络与信息安全学院，国际合作与交流处

IEEE
COMMUNICATIONS
SOCIETY
Xian Chapter

开放 流动 联合 竞争

综合业务网理论及关键技术 国家重点实验室

State Key Laboratory of Integrated Services Networks

Identity and location privacy in 5G

报告人：**Prof. Valtteri Niemi**

University of Helsinki, Finland

报告时间：**2018年6月5日(周二)下午15:30**

报告地点：北校区新科技楼 **1012**会议室

Abstract: Based on several years of preliminary work for 5G security, the 3GPP started to write the first standard specification one year ago. Now the security specification for the first phase of 5G is almost complete. Many things have changed in 5G security but mostly because the system itself has changed compared to the earlier generations. However, there are also purely security-motivated enhancements. One example is protection of user identity and location privacy against active attackers (IMSI catchers). We review some of the reasons that led to this improvement, in spite of the fact that the protection does not come without cost. Then we present different mechanisms that could provide the protection and compare them with a long list of different criteria.

The protection mechanism for 5G phase 1 has already been chosen in 3GPP. On the other hand, many of the highly promoted properties of 5G, e.g. low latency and support for massive number of IoT devices, have been postponed to phase 2 in 3GPP. This means that the specification work for these properties is just starting. It is discussed whether it is to be expected that 5G phase 2 security specification work could include further enhancements of identity and location privacy.

Bio: Valtteri Niemi is a Professor of Computer Science in University of Helsinki and leads the Secure Systems research group. Earlier he has been a Professor of Mathematics in two other Finnish universities: University of Vaasa during 1993-97 and University of Turku during 2012-2015. Between these two academic positions Niemi served for 15 years in various roles at Nokia Research Center and was nominated as a Nokia Fellow in 2009. At Nokia, Dr. Niemi worked for wireless security, including cryptological aspects and privacy-enhancing technologies. He participated 3GPP SA3 (security) standardization group from its beginning and during 2003-2009 he was the chairman of the group. He has published more than 80 scientific articles and he is a co-author of four books and more than 30 patent families.

ISN国家重点实验室，移动互联网安全111基地，网络与信息安全学院，国际合作与交流处

IEEE COMMUNICATIONS SOCIETY Xian Chapter

开放 流动 联合 竞争

综合业务网理论及关键技术 国家重点实验室
State Key Laboratory of Integrated Services Networks

Low-cost Fine-grained Human-Computer Interaction Using Heart Rate Sensor in Wearables

报告人：**Dr. Yan Wang**
SUNY Binghamton University, America

报告时间：**2018年6月5日(周二)下午16:30**

报告地点：北校区新科技楼 **1012**会议室

Abstract We subvert the traditional understanding of Photoplethysmography (PPG) and open up a new direction of the utility of PPG in commodity wearable devices, especially in the domain of human-computer interaction of fine-grained gesture recognition. We demonstrate that it is possible to leverage the widely deployed PPG sensors in wrist-worn wearable devices to enable finger-level gesture recognition, which could facilitate many emerging human-computer interactions (e.g., sign-language interpretation and virtual reality). While prior solutions in gesture recognition require dedicated devices (e.g., video cameras or IR sensors) or leverage various signals in the environments (e.g., sound, RF or ambient light), we introduce the first PPG-based gesture recognition system that can differentiate fine-grained hand gestures at finger level using commodity wearables. Our innovative system harnesses the unique blood flow changes in a user's wrist area to distinguish the user's finger and hand movements. The insight is that hand gestures involve a series of muscle and tendon movements that compress the arterial geometry with different degrees, resulting in significant motion artifacts to the blood flow with different intensity and time duration. By leveraging the unique characteristics of the motion artifacts to PPG, our system can accurately extract the gesture-related signals from the significant background noise (i.e., pulses), and identify different minute finger-level gestures. Extensive experiments are conducted with over 3600 gestures collected from 10 adults. Our prototype study using two commodity PPG sensors can differentiate nine finger-level gestures from American Sign Language with an average recognition accuracy over 88%, suggesting that our PPG-based finger-level gesture recognition system is promising to be one of the most critical components in sign language translation using wearables.

Bio: Yan Wang joins SUNY Binghamton University as an Assistant Professor in Department of Computer Science since Aug. 2015. He received his Ph.D. degree in Electrical Engineering from Stevens Institute of Technology advised by Prof. Yingying Chen. His research interests include Mobile and Pervasive Computing, Smart Healthcare, Internet of Things, and Cyber Security and Privacy. His research is supported by National Science Foundation (NSF). He is the recipient of the Best Paper Award from IEEE SECON 2017 and ACM AsiaCCS 2016. He is the Winner of ACM MobiCom Student Research Competition, 2013. His research has been reported in numerous media outlets including IEEE Spectrum, Yahoo Tech, MIT Technology Review, CNN, Fox News Channel, Wall Street Journal, and National Public Radio.

ISN国家重点实验室，移动互联网安全111基地，网络与信息安全学院，国际合作与交流处

IEEE COMMUNICATIONS SOCIETY Xian Chapter

开放 流动 联合 竞争