## 计算机网络作业——学术研究追踪

姓名：周宝航 专业：计算机科学与技术 学号：2120190442

1. 文章名称：Evolution and Trends in IoT Security

作者：[Roman-Castro Rodrigo](http://xueshu.baidu.com/s?wd=author%3A%28Roman-Castro%20Rodrigo%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson), [Lopez Javier](http://xueshu.baidu.com/s?wd=author%3A%28%20Lopez%20Javier%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson), [Gritzalis Stefanos](http://xueshu.baidu.com/s?wd=author%3A%28%20Gritzalis%20Stefanos%20%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson)

刊物信息：Computer, 2018, 51(7):16-25

日期：31 July 2018

摘要：The amount and diversity of devices that integrate connection capabilities continues to grow, and both the public and private sectors continue to explore various application areas and paradigms that involve these connected objects. Yet as the IoT field evolves, so too must its security capabilities. This article presents an analysis of IoT security issues and an overview of the current and future trends in this area.

1. 文章名称：Two-Factor Fuzzy Commitment for Unmanned IoT Devices Security

作者：Dooho Choi, Seung-Hyun Seo, Yoon-Seok Oh, Yousung Kang

刊物信息：IEEE Internet of Things Journal

日期：17 May 2018

摘要：To create an environment for IoT devices, securely, it is necessary to establish a cryptographic key for those devices. Conventionally, this key has been stored on the actual device, but this leaves the key vulnerable to physical attacks in the IoT environment. To solve this problem, several research studies have been conducted on how best to conceal the cryptographic key. Recently, these studies have most often focused on generating the key dynamically from noisy data using a fuzzy extractor or providing secure storage using a fuzzy commitment. Thus, far, all of these studies use only one type of noisy source data, such as biometric data or physical unclonable function (PUF). However, since most IoT devices are operated in unmanned environments, where biometric data is unavailable, the method using biometric data cannot be utilized for unmanned IoT devices. Although the method using PUF is applied to these unmanned devices, these are still vulnerable against physical attacks including unintended move or theft. In this paper, we present a novel way to use the fuzzy commitment on such devices, called two-factor fuzzy commitment scheme. The proposed method utilizes two noisy factors from the inside and outside of the IoT device. Therefore, although an attacker acquiring the IoT device can access the internal noisy source, the attacker cannot extract the right key from that information only. We also give a prototype implementation for ensuring the feasibility of our two-factor fuzzy commitment concept by utilizing the image data and PUF data for two noisy factors.

1. 文章名称：End-to-End Trust and Security for Internet of Things Applications

作者：[Bhattarai, Sulabh](http://xueshu.baidu.com/s?wd=author%3A%28Bhattarai%2C%20Sulabh%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson" \t "_blank)，[Wang, Yong](http://xueshu.baidu.com/s?wd=author%3A%28%20Wang%2C%20Yong%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson" \t "_blank)

刊物信息：Computer, 2018, 51(4):20-27

日期：27 April 2018

摘要：Many Internet of Things (IoT) devices utilize the cloud to store data and synchronize with one another. Because data breaches can occur anywhere en route to the cloud, ensuring end-to-end trust and security for IoT applications is critical. The authors propose a novel 3D threat model for the IoT and discuss nine security and privacy challenges as well as several ways to mitigate risks.

1. 文章名称：TRIFECTA: Security, Energy Efficiency, and Communication Capacity Comparison for Wireless IoT Devices

作者：[Sen, Shreyas](http://xueshu.baidu.com/s?wd=author%3A%28Sen%2C%20Shreyas%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson" \t "_blank)，[Koo, Jinkyu](http://xueshu.baidu.com/s?wd=author%3A%28%20Koo%2C%20Jinkyu%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson" \t "_blank)，[Bagchi, Saurabh](http://xueshu.baidu.com/s?wd=author%3A%28%20Bagchi%2C%20Saurabh%29%20&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_f_para=sc_hilight%3Dperson" \t "_blank)

刊物信息：IEEE Internet Computing, 2018, 22(1):74-81

日期：07 March 2018

摘要：The widespread proliferation of sensor nodes in the era of the Internet of Things (IoT), coupled with increasing sensor fidelity and data acquisition modality, is expected to generate 30+ Exabytes of data per month by 2020. Since most of these IoT devices will be wirelessly connected at the last few feet, wireless communication is an integral part of the future IoT scenario. The ever-shrinking size of unit computation (Moores law) and continued improvements in efficient communication (Shannons law) are expected to harness the true potential of the IoT revolution and produce a dramatic societal impact. However, reducing the size of IoT nodes and the slow improvement in energy storage density leads to reduced energy availability. Moreover, smaller size and less energy means fewer resources available for securing IoT nodes, making the energy-sparse low-cost leaf nodes of the network prime targets for attackers. In this article, we survey six prominent wireless technologies with respect to three dimensions: security, energy efficiency, and communication capacity. We point out the state of the art, open issues, and the road ahead for promising research

1. 文章名称：Penetration Testing in the IoT Age

作者：Chung-Kuan Chen, Zhi-Kai Zhang, Shan-Hsin Lee, Shiuhpyng Shieh

刊物信息：Computer, 2018, 51(4):82-85

日期：27 April 2018

摘要：Internet of Things (IoT) objects offer new services but also pose new security threats. Due to the heterogeneity, large number, and resource constraints of these objects, new penetration testing tools and techniques are needed to complement defensive mechanisms.

1. 文章名称：LogSafe: Secure and Scalable Data Logger for IoT Devices

作者：Hung Nguyen, Radoslav Ivanov, Linh T.X. Phan, Oleg Sokolsky, James Weimer, Insup Lee

刊物信息：2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE Computer Society, 2018.

日期：28 May 2018

摘要：As devices in the Internet of Things (IoT) increase in number and integrate with everyday lives, large amounts of personal information will be generated. With multiple discovered vulnerabilities in current IoT networks, a malicious attacker might be able to get access to and misuse this personal data. Thus, a logger that stores this information securely would make it possible to perform forensic analysis in case of such attacks that target valuable data. In this paper, we propose LogSafe, a scalable, fault-tolerant logger that leverages the use of Intel Software Guard Extensions (SGX) to store logs from IoT devices efficiently and securely. Using the security guarantees of SGX, LogSafe is designed to run on an untrusted cloud infrastructure and satisfies Confidentiality, Integrity, and Availability (CIA) security properties. Finally, we provide an exhaustive evaluation of LogSafe in order to demonstrate that it is capable of handling logs from a large number of IoT devices and at a very high data transmission rate.

1. 文章名称：IoT as a Land of Opportunity for DDoS Hackers

作者：Natalija Vlajic, Daiwei Zhou

刊物信息：Computer, 2018, 51(7):26-34

日期：31 July 2018

摘要：In 2016, Mirai showed the destructive potential of a botnet composed exclusively of Internet of Things devices. To evaluate the current state of anti-DDoS (distributed denial-of-service) protection for such devices, the authors studied webcams—discovered by Shodan—and found that most have little to no firewall protection and, as such, are vulnerable to future direct and reflective DDoS attacks.

1. 文章名称：A Framework for Efficient and Secured Mobility of IoT Devices in Mobile Edge Computing

作者：Sufyan Almajali, Haythem Bany Salameh, [Moussa Ayyash](https://ieeexplore.ieee.org/author/37296098200), [Hany Elgala](https://ieeexplore.ieee.org/author/37396369500)

刊物信息：the Third IEEE International Conference on Fog and Mobile Edge Computing (FMEC 2018). IEEE, 2018.

日期：31 May 2018

摘要：Mobile Edge Computing (MEC) provides an efficient solution for IoT as it brings the cloud services close to the IoT device. This works well for IoT devices with limited mobility. IoT devices that are mobile by nature introduce a set of challenges to the MEC model. Challenges include security and efficiency aspects. Achieving mutual authentication of IoT device with the cloud edge provider is essential to protect from many security threats. Also, the efficiency of data transmission when connecting to a new cloud edge provider requires efficient data mobility among MEC providers or MEC centers. This research paper proposes a new framework that offers a secure and efficient MEC for IoT applications with mobile devices.

1. 文章名称：Efficient Design of a Novel ECC-Based Public Key Scheme for Medical Data Protection by Utilization of NanoPi Fire

作者：Dariush Abbasinezhad-Mood, Morteza Nikooghadam

刊物信息：IEEE Transactions on Reliability, 2018:1-12

日期：17 July 2018

摘要：Investigating the literature reveals the fact that the key management protocols play a vital role in protecting the security and privacy of medical data in telecare medical information systems. Recently, Tseng et al. have proposed an interesting elliptic curve cryptosystem (ECC) based self-certified key management scheme that can yield secure channel for the communications of secure sensors (cluster members) and access point (cluster head). After careful consideration, we found that their scheme suffers from the cluster head impersonation, replay, and key replicating attacks. In addition, in the secure session phase, there are some errata and a point multiplication that is undefined in the ECC and hence is mathematically incorrect. Finally, yet importantly, their presented scheme has been adopted for a similar application by other authors with the same problem. Therefore, in this paper, we first try to elaborate the existing errata and security threats. Second, we propose a modified version, which is free from the challenges of their scheme. Eventually, we propose a novel anonymous ECC-based self-certified two-factor key management scheme that not only provides the desired security features, but also has much better efficiency than several recently-published schemes, such as the presented one by Tseng et al. Our formal security verification and proof besides the efficiency analysis support our claim.

1. 文章名称：Personal PIN Leakage from Wearable Devices

作者：Chen Wang, Xiaonan Guo, Yingying Chen, Yan Wang, Bo Liu

刊物信息：IEEE Transactions on Mobile Computing, 2018, PP(99):1-1

日期：March 1 2018

摘要：The proliferation of wearable devices, e.g., smartwatches and activity trackers, with embedded sensors has already shown its great potential on monitoring and inferring human daily activities. This paper reveals a serious security breach of wearable devices in the context of divulging secret information (i.e., key entries) while people are accessing key-based security systems. Existing methods of obtaining such secret information rely on installations of dedicated hardware (e.g., video camera or fake keypad), or training with labeled data from body sensors, which restrict use cases in practical adversary scenarios. In this work, we show that a wearable device can be exploited to discriminate mm-level distances and directions of the user's fine-grained hand movements, which enable attackers to reproduce the trajectories of the user's hand and further to recover the secret key entries. In particular, our system confirms the possibility of using embedded sensors in wearable devices, i.e., accelerometers, gyroscopes, and magnetometers, to derive the moving distance of the user's hand between consecutive key entries regardless of the pose of the hand. Our Backward PIN-Sequence Inference algorithm exploits the inherent physical constraints between key entries to infer the complete user key entry sequence. Extensive experiments are conducted with over 7,000 key entry traces collected from 20 adults for key-based security systems (i.e., ATM keypads and regular keyboards) through testing on different kinds of wearables. Results demonstrate that such a technique can achieve 80 percent accuracy with only one try and more than 90 percent accuracy with three tries. Moreover, the performance of our system is consistently good even under low sampling rate and when inferring long PIN sequences. To the best of our knowledge, this is the first technique that reveals personal PINs leveraging wearable devices without the need for labeled training data and contextual information.

1. 文章名称：Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing Based Smart Health

作者：Hong Liu, Xuanxiao Yao, Tao Yang, Huansheng Ning

刊物信息：IEEE Internet of Things Journal, 2018:1-1

日期：04 June 2018

摘要：Along with an integration of wearable devices, wireless communications and big data in the smart health, biomedical data is collected referring to multiple associated patients during interactions. Due to communication channel openness and data sensibility, privacy preservation become increasingly noteworthy in the edge and cloud hybrid computing-based healthcare applications. In this paper, a cooperative privacy preservation scheme is designed for wearable devices with identity authentication and data access control considerations in the space-aware and time-aware contexts. In the space-aware edge computing mode, secret sharing and MinHash-based authentication is designed to enhance privacy preservation along with similarity computing without revealing sensitive data. In the time-aware cloud computing mode, ciphertext policy attribute-based encryption is applied for fine-grained access control, and bloom filter is used to achieve efficient data structure without privacy exposure. The GNY logic-based security formal analysis is performed to prove theoretical correctness, and the proposed scheme achieves cooperative privacy preservation for wearable devices in smart health with communication overhead and computation cost.

1. 文章名称：Securely Connecting Wearables to Ambient Displays with User Intent

作者：Xiaohui Liang, Ronald Peterson, Daivd Kotz

刊物信息：IEEE Transactions on Dependable and Secure Computing, 2018:1-1

日期：28 May 2018

摘要：Wearables are often small and have limited user interfaces, hence they often wirelessly interface with a personal smartphone or a personal computer to relay information from the wearable for display. In this paper, we envision a new method LightTouch by which a wearable can establish a secure connection to an ambient display, such as a television or computer monitor, based on the user's intention to connect to the display. Such connections must be secure to prevent impersonation attacks, must work with unmodified display hardware, and must be easy to establish. LightTouch uses standard RF methods for communicating the data to display, securely bootstrapped with a key shared via a brightness channel between the low cost, low power, ambient light sensor of a wearable and the screen of the display. A screen touch gesture is adopted by users to ensure the modulation of screen brightness can be accurately and securely captured by the ambient light sensor. We further propose novel on-screen localization and correlation algorithms to improve security and reliability. Through experiments we demonstrate that LightTouch is compatible with current display and wearable designs, easy-to-use (5-6 seconds), reliable for connecting displays (98\% success connection ratio), and secure against impersonation attacks.

1. 文章名称：Efficient and Provably Secure Distributed Signing Protocol for Mobile Devices in Wireless Networks

作者：Yudi Zhang, Debiao He, Sherali Zeadally, Ding Wang, Kim-Kwang Raymond Choo

刊物信息：IEEE Internet of Things Journal, 2018:1-1

日期：14 August 2018

摘要：Rapid advances in wireless communications, hardware/software, and Internet technologies have contributed to an exponential growth in the number of users accessing the Internet using mobile, wearable or other Internet of Things devices. Identity-based signature schemes have been widely applied to enforce user authorization and validate user messages in mobile wireless networks. However, the user’s private key used to generate signatures is prone to leakage because the key is being stored on the mobile device. Several ( t, n ) threshold secret sharing schemes have been proposed to address the issue. One limitation is that the private keys in most of those schemes have to be recovered on a single device when generating signatures, so that the user who holds the device can sign any message without the participation of other users. To address the recovery limitation, we propose an efficient and secure two-party distributed signing protocol for the identity-based signature scheme in the IEEE P1363 Standard, where two users can generate a valid signature without recovering the whole private key. We formally prove its security under a nonstandard assumption. We also implemented our proposed protocol using the MIRACL Cryptographic software development kit. The experimental results obtained show that the time it takes for two general Android devices to generate a signature is about 709.53 ms.

1. 文章名称：Guest Editorial Special Issue on Trust, Security, and Privacy in Crowdsourcing

作者： Zheng Yan, Kai Zeng, Yu Xiao, Thomas hou, Pierangela Samarati

刊物信息：IEEE Internet of Things Journal, 2018, 5(4):2880-2883

日期：09 August 2018

摘要：The recent proliferation of mobile devices such as smartphones and wearable devices has given rise to crowdsourcing Internet of Things (IoT) applications, such as urban mobility monitoring, virtual/augmented reality, smart city management, and indoor floor plan reconstruction and mapping. Various data collected by mobile devices with small or big volumes can be further processed, analyzed, and mined in order to support multifarious promising services with intelligence.

1. 文章名称：Privacy in the Internet of Things for Smart Healthcare

作者：Daojing He, Ran Ye, Sammy Chan, Mohsen Guizani, Yanping Xu

刊物信息：IEEE Communications Magazine, 2018, 56(4):38-44

日期：13 April 2018

摘要：With the rapid development of wearable biosensors and wireless communication technologies, various smart healthcare systems are proposed to monitor the health of patients in real time. However, many security problems exist in these systems. For example, a password guessing attack can compromise IoT devices, leading to invasion of health data privacy. After giving an overview of security threats of healthcare IoT, this article studies security vulnerabilities of password building and presents a password strength evaluation method that takes into account users' personal information.