密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2020, 7(1): 83–86

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

物联网安全技术专栏

物联网安全技术专栏序言 (中英文)

武传坤

临沂大学 信息科学与工程学院, 临沂 276000
通信作者: 武传坤, E-mail: chuankunwu@lyu.edu.cn

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000351

中文引用格式: 武传坤. 物联网安全技术专栏序言 (中英文)[J]. 密码学报, 2020, 7(1): 83–86. [DOI: 10.13868/j.cnki.jcr.000351]

英文引用格式: WU C K. Preface of security techniques in Internet of Things column[J]. Journal of Cryptologic Research, 2020, 7(1): 83–86. [DOI: 10.13868/j.cnki.jcr.000351]

Preface of Security Techniques in Internet of Things Column

WU Chuan-Kun

School of Information Science and Engineering, Linyi University, Linyi 276000, China
Corresponding author: WU Chuan-Kun, E-mail: chuankunwu@lyu.edu.cn

物联网的概念已经被提出 20 多年的时间了, 国内对物联网技术和产业的重视是在 2009 年之后. 从 2009 年开始, 国家在物联网相关领域无论从政策方面还是在资金方面都给予了高度的重视和支持. 物联网的概念经过最初的热捧阶段, 到之后的冷却阶段, 再到后来的逐步落地阶段, 物联网相关技术和产品慢慢从虚无缥缈发展到实实在在的产业应用. 物联网系统和技术不仅应用于许多行业领域, 也在不知不觉中走进人们的日常生活: 智能家居、智慧交通、智慧医疗、智慧城市, 都是人们生活中能感受到的物联网技术的产物.

同其他与网络相关的信息技术一样, 安全和隐私是物联网系统不可或缺的技术支撑. 然而, 虽然物联网技术和产业在飞速发展, 但物联网安全问题却像个气球一样, 飘得很高, 却只有一条细线落地. 一方面, 物联网安全问题是个看不见效果的问题, 在经济指标导向下不具有竞争力, 企业在物联网安全方面的投入看不到明显的效果, 这就导致企业对物联网安全领域的投入失去动力. 另一方面, 具有轻量级特性的物联网安全技术尚不成熟, 因此在物联网设备和物联网应用系统中, 物联网安全技术的应用非常有限.

随着物联网技术和产业规模的发展, 网络安全事件不可避免地会影响到物联网系统, 而物联网安全事件对社会造成的影响会更大. 2016 年 10 月份在美国东海岸发生的大规模分布式网络拒绝服务攻击 (DDoS) 事件, 开始了典型的物联网设备安全事件, 警醒了心存侥幸的物联网设备制造商: 站在自己的角度评估黑客的攻击能力, 可能要付出惨重的代价.

2017 年 6 月 1 日起, 国家《网络安全法》正式施行, 这标志着中国已进入依法治理网络, 依法保护网络安全的时代. 2019 年 10 月 26 日, 十三届全国人大常委会第十四次会议表决通过《密码法》, 该《密码

收稿日期: 2019-11-26 定稿日期: 2020-02-07

法》在 2020 年 1 月 1 日起正式施行. 这两项法律为密码技术对网络时代的安全保护支撑作用提供了强有力的政策保护, 也将促进相关领域的政策制定、产业投入、技术开发和应用推广.

在这样一个背景下, 我们有幸在《密码学报》组织一个《物联网安全技术专栏》, 旨在将有关专家近期在物联网安全领域的研究成果进行小规模的集中, 使物联网安全问题得到国内学者更多关注. 该专栏共收录 4 篇论文, 分别简介如下:

论文《物联网认证协议综述》, 介绍了物联网认证协议研究的背景以及近几年物联网认证协议的研究进展, 分析了物联网认证协议与传统计算机网络认证协议的不同, 指出了物联网认证协议中常用的技术和数学方法, 然后从用户与设备认证、设备与服务器认证、设备与设备认证三个方面来介绍物联网认证协议研究的最新研究成果, 最后讨论了物联网认证协议的未来研究方向.

论文《基于 Augur 的交易者身份管理方案研究》, 使用 Augur 的身份管理技术对区块链进行研究, 探索区块链应用的身份管理方案以及潜在风险, 并针对 Augur 的身份管理方案潜在风险和基于设计缺陷的攻击提出了一个基于信誉评估的安全解决方案. 该方案选取了 6 个信誉指标和 3 种信誉计算方法, 为交易者选择有效市场及其他 Augur 交易活动提供信誉依据.

论文《一种基于 PUF 的超轻量级 RFID 标签所有权转移协议》, 针对 RFID 标签所有权转移协议中存在的数据完整性受到破坏、物理克隆攻击、去同步攻击等多种安全隐私问题, 设计了一种基于物理不可克隆函数 (PUF) 的超轻量级 RFID 标签所有权转移协议. 所设计的协议无须引入可信第三方, 通过标签所有权的原所有者和新所有者之间的通信就可以完成所有权转移. 协议实现了 RFID 标签所有权转移之前的标签原所有者与标签之间的双向认证、所有权转移之后的标签新所有者与标签之间的双向认证. 论文通过对协议的安全性的形式化分析, 表明所设计的协议能够保证通信过程中交互信息的安全性及数据隐私性.

论文《物联网的 OT 安全技术探讨》, 介绍了操作安全 (OT 安全) 的概念, 论述了物联网的操作安全区别于传统信息网络安全的原因, 指出传统网络安全保护的主要是信息, 而操作安全保护的是控制. 物联网系统除了要保护信息安全外, 还需要对操作安全提供保护技术. 操作安全是信息转化为物理活动行为的安全问题, 其安全防护的目标与传统的信息安全保护不同, 但有许多类似的实现技术. 论文从操作安全的概念和操作安全保护技术的特点等方面予以分析, 并指出物联网的操作安全与传统信息安全的本质区别. 论文也列出了一些物联网领域有关 OT 安全的技术问题.

物联网安全技术专栏的以上几篇论文包括一篇综述性论文、两篇安全方案设计方面的论文和一篇对某些新概念进一步剖析方面的论文. 对物联网安全这个新颖和充满活力的领域来说, 还远远不能代表国内的研究现状. 无论如何, 希望这个专栏能吸引更多研究者对物联网安全领域的关注, 更好地推动物联网安全领域的研究, 进一步推动物联网安全技术的产业应用.

The concept of Internet of Things (IoT for short) has been proposed for over 20 years. The booming development of IoT techniques and industrial applications in China started from 2009. Since then, the China government has paid much attention and given much support both in policy making and financial support. The development of IoT has gone through the processes of concept proposal and initial interest, enthusiasm cooling down, and graduate applications. Now the IoT related applications cover a large variety of industries. The IoT techniques and applications have also been in our everyday life, such as smart home, smart transport systems, WIT120, and smart city.

As in other network related information technology, security and privacy in IoT systems are core components. However, irrespective of the repaid development of IoT techniques and industrial applications, the IoT security techniques are like balloons–flying in the sky with a thin string connected to the ground. The reasons for this situation include the following: on one hand, the IoT security has invisible effect, and is less attractive when financial figure is the most significant measure, hence industries do not have much interest in paying for the IoT security services, and the government has also been very careful in investigating to this field. On the other hand, many IoT security techniques need to have the feature of being lightweight, such techniques are far from being mature, and hence

the application of IoT security techniques to IoT applications has been very limited.

With the development of IoT techniques and IoT industries, network security events will inevitably affect the IoT application systems. IoT security events may have more serious social effect than traditional network security events. For example, in October of 2006, the US east coast experienced a large scale DDoS attack, where a large number of IoT devices are involved in the attack, which waken many manufactures of IoT devices who used to have a fluke mind of mot having IoT security problems so soon. The security event warns the IoT device manufactures that, painful price may have to be paid if the hackers' attack is underestimated.

In 2017, the "Network Security Law" has been put into effect, which indicates that China has come into the era when the networks are managed according to the law. In 2019, China has lunched the "Cryptography Law" which will take effect from 1st, January of 2020. These two laws provide strong policy support to the applications of cryptographic techniques in this networked word, and will further foster new policies, industry investigation, technology development, and applications.

In such a background, it is our owner to organize such a special column of "Security Techniques in Internet of Things" for the Journal of Cryptologic Research, aiming at collecting recent research results in the field of IoT security from relevant researchers, hence to attract more researcher pay attention to the IoT security. This special column includes 4 papers, they are introduced as follows:

The paper titled "A survey on authentication protocol for Internet of Things" introduces the background and some recent research progress of authentication protocols of Internet of things. The paper analyzes the differences between Internet of things authentication protocols and traditional computer network authentication protocols, summarizes the techniques and theoretical methods commonly used in IoT authentication protocols. It introduces some most recent research results of Internet of things authentication protocols from three aspects: authentication protocols between a user and an IoT device, between an IoT device and a server, and between IoT devices. Some future research directions are also discussed.

The paper titled "Research on trader identity management scheme based on Augur" studies the application of Augur's identity management techniques in blockchain applications, explores some potential risks of the identity management techniques in blockchain applications, and proposes a security solution based on reputation assessment for Augur's identity management scheme. The proposed scheme selects 6 credit indicators and 3 credit calculation methods to provide a credibility basis for traders to choose effective market and other Augur trading activities.

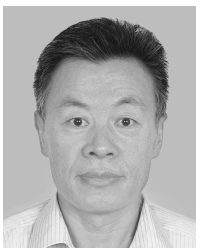
The paper titled "A PUF-based ultra-lightweight ownership transfer protocol for low-cost RFID tags" proposes an ultra-lightweight ownership transfer protocol for low-cost RFID tags based on the techniques of physically uncloneable functions (PUFs). The proposed protocol aims at various security and privacy issues such as data integrity destruction, physical cloning attacks, and desynchronization attacks in the RFID tag ownership transfer protocols. In the proposed protocol, the current owner and the new owner of an RFID tag can communicate directly to complete the ownership transfer, and does not need to rely on a trusted third party. The proposed protocol achieves mutual authentication between the current owner of the tag and the tag before the completion of the ownership transfer, and the mutual authentication between the new owner of the tag and the tag after the completion of the ownership transfer. Formal security analysis shows that the proposed protocol can ensure the security of interactive information and data privacy in the process of communication.

The paper titled "A primary study on the OT security of IOT" introduces the concept of operational security (OT security for short), discusses the necessity of OT security in IoT systems apart from information security (known as IT security). The OT security is a security technique in the process of converting information into physical actions, where the purpose of security protection is different from

that of traditional information systems. The paper points out some essential differences between the OT security and the traditional IT security. Some possible research topics about the OT security for IOT are listed.

The above mentioned papers in this special column of IoT security techniques include one survey paper, two papers about security protocol design, and one paper about further discussion of new concepts. For the new and active field of IoT security, these papers are far from being sufficiently representing the current research status in China. Nevertheless, it is hopped that this special column of the JCR can attract more researchers to pay attention to the field of IoT security, hence to promote the advances of IoT security research, and the industrial applications of IoT security techniques.

作者信息



武传坤 (1964–)，山东沂水人，教授，博士. 主要研究领域为密码学、认证协议、物联网安全、工业控制安全.
chuankunwu@lyu.edu.cn

WU Chuan-Kun (1964–), Ph.D., Professor. Research interests cover cryptography, network security, with special interest being in the areas of security techniques in Internet of Things and industrial control security.
chuankunwu@lyu.edu.cn