计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20190404
57(4):836-846,2020

基于区块链的网络安全威胁情报共享模型

黄克振[1,2] 连一峰[1] 冯登国[1] 张海霞[1] 刘玉岭[1,2] 马向亮[1,2]
[1](中国科学院软件研究所可信计算与信息保障实验室 北京 100190)
[2](中国科学院大学 北京 100049)
(huangkezhen@tca.iscas.ac.cn)

Cyber Security Threat Intelligence Sharing Model Based on Blockchain

Huang Kezhen[1,2], Lian Yifeng[1], Feng Dengguo[1], Zhang Haixia[1], Liu Yuling[1,2], and Ma Xiangliang[1,2]
[1](*Trusted Computing and Information Assurance Laboratory*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100190)
[2](*University of Chinese Academy of Sciences*, *Beijing* 100049)

Abstract In the process of increasing cyber security attack and defense confrontation, there is a natural asymmetry between the offensive and defensive sides. The CTI (cyber security threat intelligence) sharing is an effective method to improve the responsiveness and effectiveness of the protection party. However, there is a contradiction between the privacy protection requirements of CTI sharing and the need to build a complete attack chain. Aiming at the above contradiction, this paper proposes a blockchain-based CTI sharing model, which uses the account anonymity of the blockchain technology to protect the privacy of CTI sharing party, and at the same time utilizes the tamper-free and accounting of the blockchain technology to prevent the "free-riding" behavior in CTI sharing and guarantee the benefit of CTI sharing party. The one-way encryption function is used to protect the private information in CTI, then the model uses the encrypted CTI to build a complete attack chain, and uses the traceability of the blockchain technology to complete the decryption of the attack source in the attack chain. The smart contract mechanism of the blockchain technology is used to implement an automated early warning and response against cyber security threats. Finally, the feasibility and effectiveness of the proposed model are verified by simulation experiments.

Key words cyber security; cyber security threat intelligence; attack chain; privacy protection; blockchain

摘 要 在不断加剧的网络安全攻防对抗过程中,攻防双方存在着天然的不对称性,网络安全威胁情报共享利用是一种有效提高防护方响应能力和效果的手段.然而威胁情报共享利用中的隐私保护需求与构建完整攻击链的需求之间存在矛盾.针对上述矛盾点,提出一种基于区块链的网络安全威胁情报共享模型,利用了区块链技术的账户匿名性和不可篡改性,使用单向加密函数保护情报中的隐私信息,基于加密后的情报构建完整攻击链,借助区块链的回溯能力完成攻击链中攻击源的解密.最后,通过实验验证了该模型的可行性和有效性.

关键词 网络安全;网络安全威胁情报;攻击链;隐私保护;区块链

中图法分类号 TP391

收稿日期:2019-06-11;**修回日期**:2019-09-18

基金项目:国家自然科学基金项目(U1836211);公安部技术研究计划项目(2018JSYJA08)
This work was supported by the National Natural Science Foundation of China (U1836211) and the Ministry of Public Security Technology Research Projects (2018JSYJA08).

近年来,网络技术日益翻新,同时带来了日趋复杂的网络攻击方法或手段,如零日漏洞利用、高级可持续性威胁(advanced persistent threat, APT)、社交工程等.由于信息的不对称性,安全防护方在复杂系统安全攻防的"速度之争"中处于天然的劣势(如图 1 所示,根据 Verizon 公司 2018 年的报告,攻击者可以在分钟级别的时间内攻陷 87%企业的网络系统,而 68%的企业在数月后才会发现企业的网络系统被入侵).面对复杂的攻击形式和严重的攻击后果,依靠个人或单个组织的技术力量仅能获得局部的攻击信息,无法构建完整的攻击链,更无法准确有效地预防攻击者.网络安全威胁情报共享利用作为一种"以空间换时间"的技术方式,可以及时利用其他网络中产生的高效威胁情报提高防护方的应对能力,缩短响应时间,从而形成缓解攻防对抗不对称态势的长效机制[2].

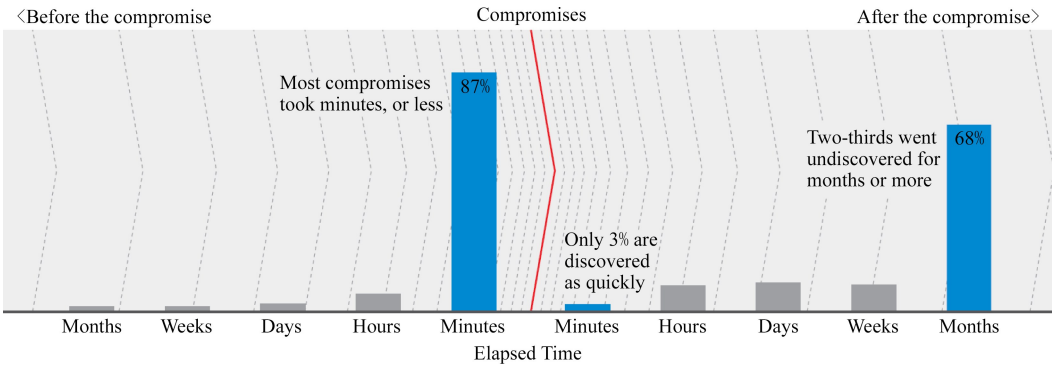

Fig. 1 2018 data breach investigations report[1]

图 1 2018 年数据泄露调查报告[1]

信息共享可能会导致隐私信息的泄露,网络安全威胁情报共享也不例外,现实社会中已经发生因隐私信息泄露导致企业经济或名誉损失[3],进而影响企业参与网络安全威胁情报共享积极性的案例.针对网络安全威胁情报共享中的隐私保护问题,文献[4-7]从保护情报共享组织身份信息、保护情报利用成员身份信息和改进 STIX(structured threat information expression)共享标准中隐私泄露等方面进行研究,在隐私保护方面取得了有效的进展.但是严格的隐私保护也阻碍了完整攻击链的推理构建工作.例如某银行 IP 地址为 12.1.2.3 的服务器被恶意代码 M 攻陷成为了 C2(command and control)服务器,该银行为了保护隐私信息,发布了泛化的威胁情报:恶意代码 M 攻击银行服务器,攻陷的服务器承担 C2 服务器职能,那么分析人员就无法利用 12.1.2.3 进行攻击链的推理分析,即无法构建完整攻击链,所以需要提出一种既能满足隐私保护需求,又能利用威胁情报进行推理分析并构建完整攻击链的网络安全威胁情报共享模型.

本文针对隐私保护和威胁情报利用之间存在的矛盾点,提出一种基于区块链的网络安全威胁情报共享模型,该模型利用区块链的账户匿名性保护威胁情报共享方和利用方的身份信息;利用加密保护的威胁情报构建完整攻击链,并对攻击链中的威胁源借助区块链的回溯能力完成解密;利用智能合约对潜在攻击目标自动发出预警响应.

1 相关工作

研究人员已经在网络安全威胁情报共享框架或模型、网络安全威胁情报共享中的隐私保护、区块链在信息共享中的利用等方面开展了诸多研究,为本文工作提供了基础和借鉴.

在网络安全威胁情报共享方面,Zhao 等人[8]讨论了网络安全信息共享的必要性并提供了共享信息类型指南,定义了社区网络安全威胁警报级别并讨论了不同警报级别对信息共享造成的影响,提出了一种协同的信息共享框架,进而阐述了共享过程中可能遇到的安全、可信、隐私等问题和未来的研究方向.Goodwin 等人[9]借助微软在基础设施安全管理方面的经验,分析了信息共享的历史背景,阐述了信息共享在模型、方法和机制等方面的分类,最后对基于协作式的信息共享、隐私保护和交换方法提出了建议.上述研究工作都充分肯定了网络安全威胁情报共享的必要性,也提出了隐私保护的需求,但是未能给出行之有效的隐私保护方法或措施.

在威胁情报共享中的隐私保护方面,Vakilinia 等人[4]为了保护共享威胁情报的组织机构的身份

信息,利用可聚合的盲签名(基于 BBS+签名方案)机制,提出了具有注册、共享、论证和奖励功能的网络安全信息共享框架.Badsha 等人[5]为了防止威胁情报共享过程中隐私信息可能泄露给不信任的参与者或黑客,提出了基于同态加密的网络安全威胁情报共享和利用框架.Martinelli 等人[6]分析了 STIX 网络安全威胁情报共享标准中可能的隐私信息泄露问题,并利用改进的数据共享协议尝试解决隐私信息泄露问题.上述研究工作都从单方维度起到了隐私保护作用,但不能同时保护情报共享方、情报使用方和情报涉及其他方的隐私信息.

在区块链技术与信息共享相结合方面,Peterson 等人[10]将区块链应用到医疗档案共享交换方面,在保护患者隐私的同时实现了数据的共享.Kang 等人[11]将区块链应用于车载边缘计算和网络数据共享中,取得了一定的效果.Rawat 等人[12]提出了基于区块链的 iShare 框架,参与 iShare 框架的成员间仅可分享网络安全防护的方案或概述,并利用博弈论对框架内可能的恶意行为进行了分析.区块链技术在其他行业信息共享方面的研究工作已经取得了一定进展,但是这些研究成果无法直接应用于网络安全威胁情报的共享;而 iShare 框架仅能够共享网络安全防护方案,未涉及威胁情报信息的共享工作.

针对已有研究工作存在的局限性,本文构建了基于区块链的网络安全威胁情报共享模型.该模型利用区块链的账户匿名性和统一的单向加密函数,充分保护情报共享方、使用方和情报涉及其他方的隐私信息,同时,可以对加密后的威胁情报进行关联分析,构建完整攻击链,提高安全防护的效率和能力.

2 基于区块链的威胁情报共享模型

如表 1 所示,区块链的去中心化、账户匿名性、开放性、自治性、不可篡改性和智能合约机制等特点或功能,可以满足网络安全威胁情报共享中的隐私保护、根据贡献值进行奖励、威胁情报可追溯、自动预警响应等需求,其中:

1) 区块链的匿名性由比特币地址生成过程决定,比特币地址由一系列编码算法和散列算法对椭圆曲线的公钥进行运算生成.

2) 区块链的可追溯性由区块链构造过程决定,$Block(N)=\mathrm{Hash}(tp(N),Merkle(N),Block(N-1),nounce)$,其中 $tp(N)$ 表示时间戳,$Merkle(N)=\mathrm{Hash}(Tx(N))$ 表示包含已有交易的 *Merkle* 根,*nounce* 表示随机数.

3) 智能合约在满足合约条件时可触发交易,即

$$is\_execute=\begin{cases}\mathrm{True},\ x\in conditions\ \text{or}\\ \quad x=conditions;\\ \mathrm{False},\ \text{otherwize.}\end{cases}$$

Table 1 Compare Cyber Security Threat Intelligence (CTI) Sharing Requirements and Blockchain Features

表 1 网络安全威胁情报共享需求与区块链特点对比

Serial Number	CTI Sharing Requirements	Blockchain Features
1	Privacy Preservation	Decentralized Technology and Account Anonymity
2	Rewarding	Distributed Ledger Technology, Openness and Autonomy
3	Traceability	Tamper-free
4	Automating Cyber Security Early Warning and Response	Smart Contract

鉴于此,本文提出一种基于区块链的网络安全威胁情报共享模型.

2.1 定义

在阐述本文的模型和算法之前,先给出相关的定义.

定义 1. 一元类网络安全威胁情报(*OneCti*).主要包括网络安全威胁指示器(indicator of compromise, IoC)或威胁对象(threat object)类型情报,如电子邮件、IP 地址、域名、恶意代码、组织、域名所有者、攻击者等.使用四元组〈*tp*,*type*,*value*,*label*〉描述,其中 *tp* 表示时间戳,*type* 表示元素类型($type\in\{ip,domain,email,campaign,attacker,\cdots\}$),*value* 表示元素值,*label* 表示元素标签;如〈2019-05-16T10:00:00,ip,12.6.5.3,C2〉表示在 2019-05-16T10:00:00 检测到 IP 地址 12.6.5.3 为 C2 服务器.

定义 2. 二元类网络安全威胁情报(*TwoCti*).主要包括网络安全事件类型情报,使用七元组〈*tp*,$type_1$,$value_1$,*rel*,$type_2$,$value_2$,*desc*〉描述,其中,*tp*,$type_i$,$value_i$ 与 *OneCti* 中的 *tp*,*type*,*value* 含义相同,*rel* 表示 2 元素间的关系($rel\in\{connect,inject,scan,\cdots\}$),*desc* 表示该情报相关的描述信息;如〈2019-05-16T10:00:00,ip,12.6.5.3,connect,

ip,13.5.6.6,connect server〉表示 2019-05-16T10:00:00 时,IP 地址为 12.6.5.3 的服务器连接了 IP 地址为 13.5.6.6 的服务器.

定义 3. 网络安全情报共享交易(*STrans*).指组织机构共享网络安全威胁情报给威胁情报中心,威胁情报中心对威胁情报验证、评估后给予一定奖励(*reward*)并返回情报共享凭证(*ticket*)的过程,使用六元组〈tp,O_{acc},C_{acc},*reward*,*SEnc*(C_{pub_k},*Cti*),*ticket*〉描述,其中 tp 表示时间戳,O_{acc},C_{acc} 分别表示组织机构和网络安全威胁情报中心的区块链账户地址,*SEnc*(C_{pub_k},*Cti*)表示使用威胁情报中心的公钥 C_{pub_k} 加密的威胁情报.

定义 4. 网络安全威胁情报图.指使用单向加密的网络安全威胁情报元素值组成的有向图,用 $G=\langle V,E,L,R\rangle$ 描述.其中,V 表示 IP、域名、邮箱等元素值的单向加密密文;如果 $u,v\in V$ 间存在二元类网络安全威胁情报,构成一条从 u 到 v 的有向边,则 $(u,v)\in E$;L 是节点 $v\in V$ 的标签 *label* 的集合;R 是节点间关系 *relation* 的集合.

定义 5. 网络安全情报分析交易(*ATrans*).指组织机构向威胁情报中心提出威胁情报分析需求,情报中心将组织机构提供的威胁情报与情报库中的情报关联分析后,返回分析结果或威胁处置建议(*result*)并收取一定情报使用费用(uf)的过程,使用六元组〈tp,O_{acc},C_{acc},uf,*SEnc*(C_{pub_k},*Cti*),*SEnc*(O_{pub_k},*result*)〉描述,其中 tp,O_{acc},C_{acc},*SEnc*(C_{pub_k},*Cti*)的含义与 *STrans* 中的含义相同,*SEnc*(O_{pub_k},*result*)表示使用组织机构公钥 O_{pub_k} 加密的情报分析结果 *result*.

2.2 模型描述

如图 2 所示,基于区块链的网络安全威胁情报共享模型使用八元组〈*Org*,*Center*,*BlockNet*,*CtiDB*,*Cti*,*Trans*,*SC*,*Operation*〉表示,其中:

1) *Org* 表示组织机构,能够共享和使用网络安全威胁情报;模型中有 N 个组织机构 Org_i($1\leqslant i\leqslant N$),每个组织机构 Org_i 作为区块链的节点,拥有区块链账户地址 O_{acc},组织机构在网络安全威胁情报共享和使用过程中均以 O_{acc} 的形式出现,能够有效保护组织机构的身份信息.

2) *Center* 表示网络安全威胁情报分析中心,具有分析网络安全威胁情报的功能,是推理构建完整攻击链不可或缺的可信第三方;拥有区块链账户地址 C_{acc}.

3) *BlockNet* 表示区块链网络,由 *Org* 和 *Center* 组成.

4) *CtiDB* 表示网络安全威胁情报库,能够存储网络安全威胁情报.在该模型中网络安全威胁情报库中的情报均为加密情报 Hash(*Cti*),能够有效防止情报中隐私信息的泄露.

5) *Cti* 表示网络安全威胁情报(*Cti*∈{*OneCti*,*TwoCti*}),本文主要讨论一元类和二元类网络安全

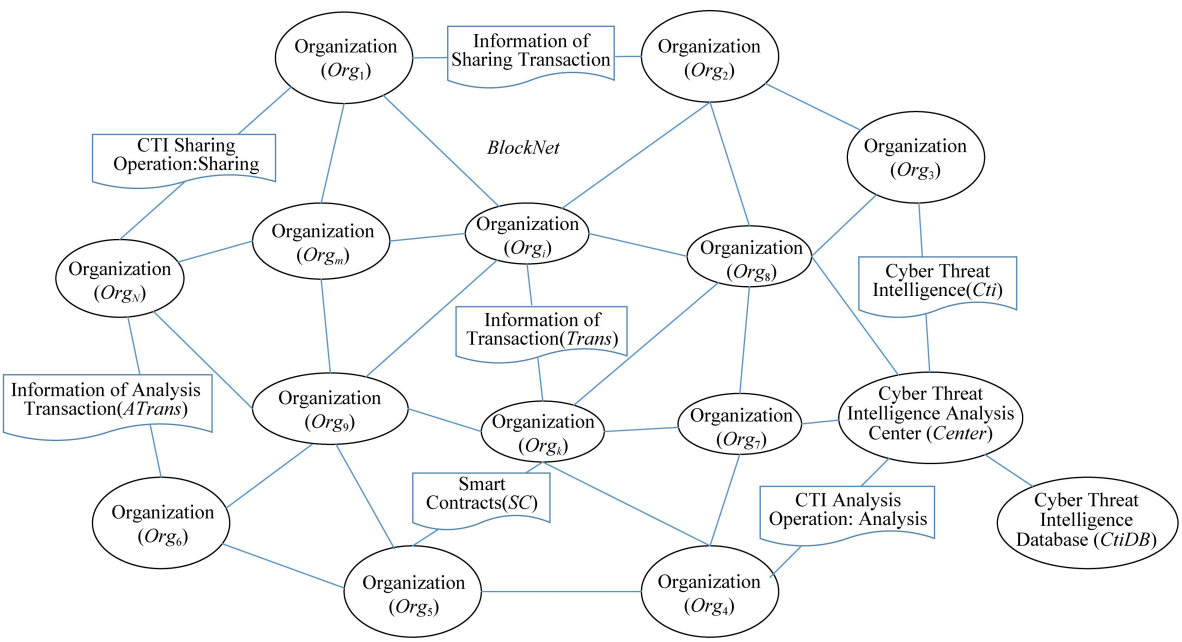

Fig. 2 Cyber security threat intelligence sharing model based on blockchain

图 2 基于区块链的网络安全威胁情报共享模型

威胁情报,其他多元类网络安全威胁情报可以拆分为多个二元类或一元类网络安全威胁情报的组合.

6) $Trans$ 表示区块链上的交易信息,包括网络安全威胁情报共享交易和网络安全威胁情报分析交易,即 $Trans\in\{STrans,ATrans\}$.

7) SC 表示组织机构创建的智能合约,由创建者账户地址 O_{acc}、触发条件 $condition$、预警响应措施 $response$、情报使用费用 uf 组成,使用四元组 $\langle O_{acc},condition,response,uf\rangle$,当 $Center$ 在情报分析推理中发现满足智能合约触发条件 $condition$ 时,就执行预警响应措施 $response$,并从智能合约的创建者账户 O_{acc} 中扣除费用 uf.

8) $Operation$ 表示主体 Org, $Center$, $CtiDB$, $BlockNet$ 间的动作操作,包括情报节点注册(registry)、威胁情报共享(sharing)、情报评估(evaluate)、威胁情报分析(analysis)、交易广播(broadcast)、情报存储(store)、情报提取(get)和智能合约创建(create)等.如图 3 所示,组织机构 Org_1 与 $Center$ 间进行情报共享时,不同的主体间会涉及 sharing, get, evaluate, store, broadcast 等多种动作操作.

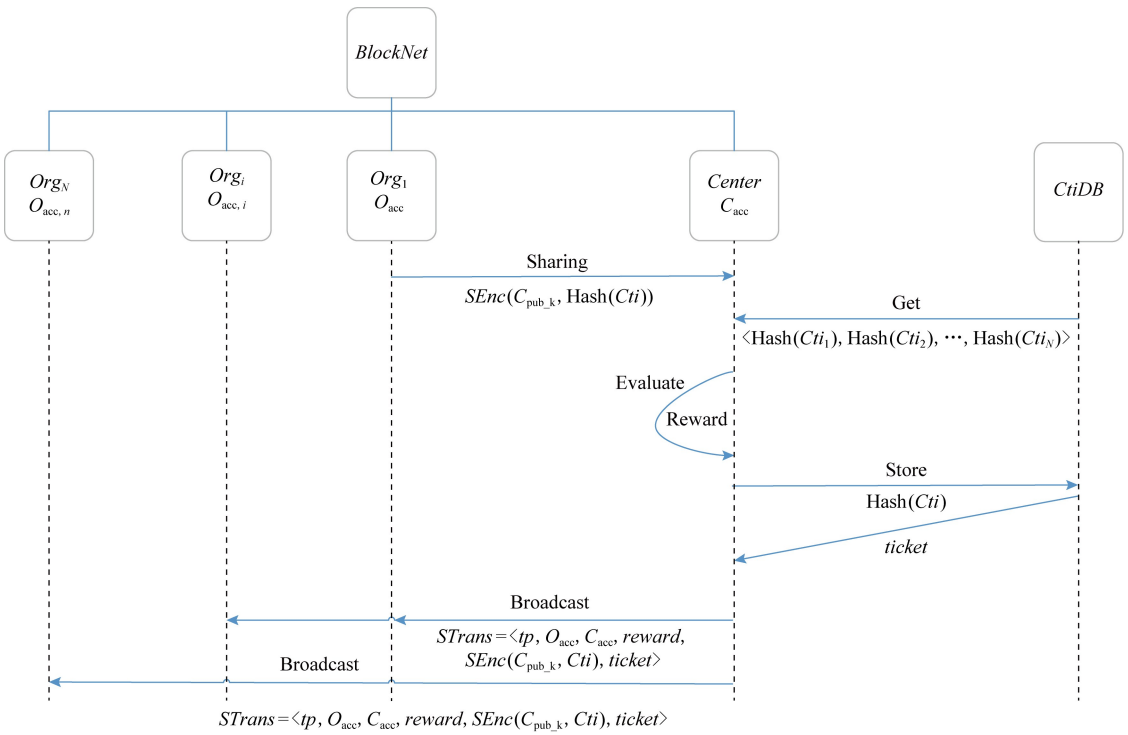

Fig. 3 Operations in cyber threat intelligence sharing

图 3 情报共享过程中主体间的动作操作

3 情报节点注册算法(INRA)

为了保证情报节点的可信度和保护情报共享、利用中的隐私信息,本文引入如算法 1 所示的情报节点注册算法 INRA,组织机构尝试加入威胁情报区块链并成为情报节点,需要向网络安全威胁情报中心进行注册,注册过程依赖标准加密体系完成,其中,非对称加密由三元组 $\langle G_{sig},SEnc,SDec\rangle$ 组成:G_{sig} 产生公私密钥对,$SEnc$ 为非对称加密算法,$SDec$ 为非对称解密算法;单向加密函数使用 H_{alg} 表示.具体来说,算法 1 的行②~④组织机构 Org 产生接收威胁情报中心 $Center$ 返回情报的公私密钥对(O_{pub_k}, O_{pri_k}),并将 O_{pub_k} 发送给威胁情报分析中心 $Center$;行⑤~⑨$Center$ 产生接收组织机构提交情报的公私密钥对 C_{pub_k}、C_{pri_k} 和单向加密函数 H,为了验证 O_{pub_k} 是否被篡改,利用 Org 的公钥 O_{pub_k} 加密 C_{pub_k},将公钥的密文和明文发送给 Org;行⑩~⑮Org 利用自身私钥解密获得 C_{pub_k1},并判断与明文 C_{pub_k} 是否相等,如相等,完成情报交换时的加密密钥的协商和单向加密算法的指定.该算法为线性算法,时间复杂度在 $O(1)$ 范围内.

算法 1. 情报节点注册算法 INRA.

输入:组织机构区块链账户 O_{acc}、威胁情报分析中心账户 C_{acc};

输出:组织机构情报接收公钥 O_{pub_k}、威胁情报

分析中心情报接收公钥 C_{pub_k}.

① *inra* (O_{acc},C_{acc})
② 组织机构执行:
③ O_{pub_k},O_{pri_k}=G_{sig}();
/* 生成公私密钥对 */
④ send O_{pub_k} to C_{acc};
⑤ CTI 分析中心执行:
⑥ C_{pub_k},C_{pri_k}=G_{sig}();
⑦ H=H_{alg}(); /* 指定单向加密算法 */
⑧ PK^{sig}_{Center}=$SEnc$(O_{pub_k},C_{pub_k});
⑨ send H,PK^{sig}_{Center},C_{pub_k} to O_{acc};
⑩ 组织机构执行:
⑪ C_{pub_k1}=$SDec$(O_{pri_k},PK^{sig}_{Center});
⑫ if C_{pub_k1}==C_{pub_k}
⑬ return O_{pub_k},C_{pub_k},H;
⑭ else
⑮ return None;
⑯ end if

4 情报数据记账算法(IDAA)

为了保证情报共享社区的良性发展,避免情报节点出现只利用情报,不共享情报的“搭便车”行为[13],本文设计了如算法 2 所示的情报数据记账算法 IDAA,该算法实现组织机构与网络安全威胁情报中心的情报共享,并将共享情报加密后记入区块链,方便后续的威胁源追溯解密,同时又引入奖励机制,鼓励情报节点积极共享情报.首先,组织机构提交加密的网络安全威胁情报 $SEnc$(C_{pub_k},Cti)(Cti=〈tp,$type$,H($value$),$label$〉‖〈tp,$type$,H($value$),rel,$type$,H($value$),$desc$〉);然后,如算法 2 中的行②~⑥所示,情报分析中心在收到提交情报后进行解密、评估和存储,其中威胁情报的价值评估主要依据与已有情报的关联度进行评价;最后,如算法 2 中的行⑦⑧所示,C_{acc}将情报共享交易信息广播至整个区块链网络,完成情报共享的记账操作.

算法 2. 情报数据记账算法 IDAA.

输入:情报收到时间 *receive_time*、组织机构账户 O_{acc}、威胁情报中心账户 C_{acc}、非对称加密算法加密的情报消息 $SEnc$(C_{pub_k},Cti)、威胁情报中心私钥 C_{pri_k};

输出:接收成功 True 或接收失败 False.

① *idaa*(*receive_time*,O_{acc},C_{acc},$SEnc$(C_{pub_k},Cti),C_{pri_k})
② *enc_msg*=$SEnc$(C_{pub_k},*Cti*);
③ *msg*=$SDec$(C_{pri_k},*enc_msg*);
④ *reward*=*evalue_cti*(*msg*); /* 评估威胁情报价值 */
⑤ if *store*(*msg*,*CtiDB*)
⑥ *ticket*=*CtiDB.find*(*msg*).*index*;
⑦ *strans*=(*receive_time*,O_{acc},C_{acc},*reward*,*enc_msg*,*ticket*);
⑧ *broad_to_blockchain*(*strans*); /* 区块链中广播交易信息 */
⑨ return True;
⑩ else
⑪ return False;
⑫ end if

5 基于情报图的分析交易算法(IGATA)

为了有效地使用情报节点共享的网络安全威胁情报,本文引入算法 3 所示的基于情报图的分析交易算法 IGATA,该算法实现组织机构与网络安全威胁情报中心间的情报分析,并将情报线索和情报结果记入区块链.具体来说,首先,行②~⑰网络安全威胁情报中心与已有的情报进行相互关联,构建网络安全威胁情报图;然后行⑱~⑳利用标签传播算法推理威胁情报元素的标签,行㉑利用拓扑排序算法构建攻击链;最后根据攻击链和元素标签,借助区块链的追溯功能,解密单向加密的网络安全威胁元素值,返回分析需求发起方,并将分析交易信息写入区块链.

算法 3. 基于威胁情报图的分析交易算法 IGATA.

输入:加密的威胁情报 *msg*、威胁情报库 *CtiDB*;

输出:情报标签列表 *label_list*、攻击链 *attack_chain*.

① *igata*(*msg*,*CtiDB*)
② init graph G;
③ *hash_value_list*=*get_hash_value*(*msg*);
④ for *hash_value* in *hash_value_list*
⑤ if *hash_value* not in G
⑥ G.*add*(*hash_value*);
⑦ end if
⑧ end for
⑨ for v in G
⑩ *two_cti*=*CtiDB.find_two_cti*(v);

```
⑪      for item in [two_cti.src_value, two_cti.dst_value]
⑫        if item ! =v and item not in G
⑬          G.add (item);
⑭          G.L[item]=CtiDB.find_one_cti (item).label;
⑮        end if
⑯      end for
⑰    end for
⑱    for hash_value in hash_value_list
⑲      label_list.append(label_propagation (G, hash_value));
⑳    end for
㉑    attack_chain=top_sort(G);
㉒    atrans = construct_atrans(msg, label_list, attack_chain);
㉓    broad_to_blockchain(atrans);
㉔    return label_list, attack_chain.
```

算法 3 的时间复杂度分析:算法 3 的主要时间消耗在情报图的构建过程中,假设构建完成的情报图节点数有 n,有向边为 m,*CtiDB* 采用键值对的形式数据库存储或云存储,存取时间为 $O(1)$,那么,构建情报图的时间复杂度为 $O(n^2)$,标签传播算法的时间消耗小于 $O(m)$,攻击链构造过程时间消耗为 $O(n+m)$,则总的时间复杂度接近 $O(n^2)$.

6 基于智能合约的预警响应算法(SERA)

鉴于网络安全攻防对抗的时间不对称性,如何提高防护方的响应速度成为了攻防对抗的一个重点.为了提高情报区块链网络内预警响应的速度,本文模型中引入基于智能合约的预警响应机制,如算法 4 所示.首先,行②~④组织机构将需要重点防护的系统在区块链上创建智能合约,并广播整个区块链网络;然后,行⑥~⑨网络安全威胁情报中心在分析情报时,对与组织机构创建的智能合约相关的威胁情报进行分析,如有符合智能合约触发条件的威胁情报,模型自动触发智能合约,并执行其中的预警响应流程或措施,并将分析转化为网络安全威胁情报分析交易信息广播情报区块链网络.

算法 4. 基于智能合约的预警响应算法 SERA.

输入:智能合约创建者账户地址 O_{acc}、智能合约条件 *condition*、预警响应措施 *response*、支付的费用 uf;

输出:满足智能合约条件的威胁情报 *Cti*.

```
① sera(msg, CtiDB)
②   组织机构执行:
③     sc=create_sc(condition, response, uf);
④     broad_to_blockchain(sc); /* 情报区块链网络内广播智能合约 */
⑤   CTI 中心执行:
⑥     if Cti match condition
⑦       execute(response);
⑧       atrans=construct_atrans(Cti);
⑨       broad_to_blockchain(atrans);
⑩       return SEnc(O_pub_k, Cti);
⑪     end if
```

7 实验评估

为了验证评估上述威胁情报共享模型的效果,本文设计了如图 4 所示拓扑结构的网络,其中 16.1.5.20,16.1.5.23,16.1.5.26,16.1.5.29,16.1.5.30 构成区块链网络,16.1.5.20 承载网络安全威胁情报分析中心功能,网络安全威胁情报库存储于使用 ownCloud 搭建的云存储上.

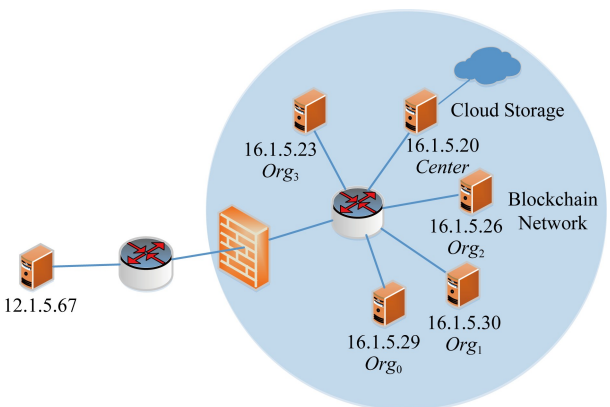

Fig. 4 Topology of network example

图 4 网络拓扑

本文参照杀伤链(侦查跟踪、武器构建、载荷投递、漏洞利用、安装植入、命令与控制和目标达成)[14]设计了如图 5 所示的模拟攻击场景:2019-05-26T10:00:00,攻击者 Alice 利用 IP 为 12.1.5.67 的服务器攻陷 Org_0 企业的 IP 为 16.1.5.29 的服务器,并投放恶意代码载荷 M_0,进而利用 16.1.5.29 作为跳板攻陷了 16.1.5.30 服务器,投放了恶意代码载荷 M_1(M_0 的变种);恶意代码 M_0 利用自身的传播机制,传播至 IP 为 16.1.5.26 的服务器;在 2019-05-

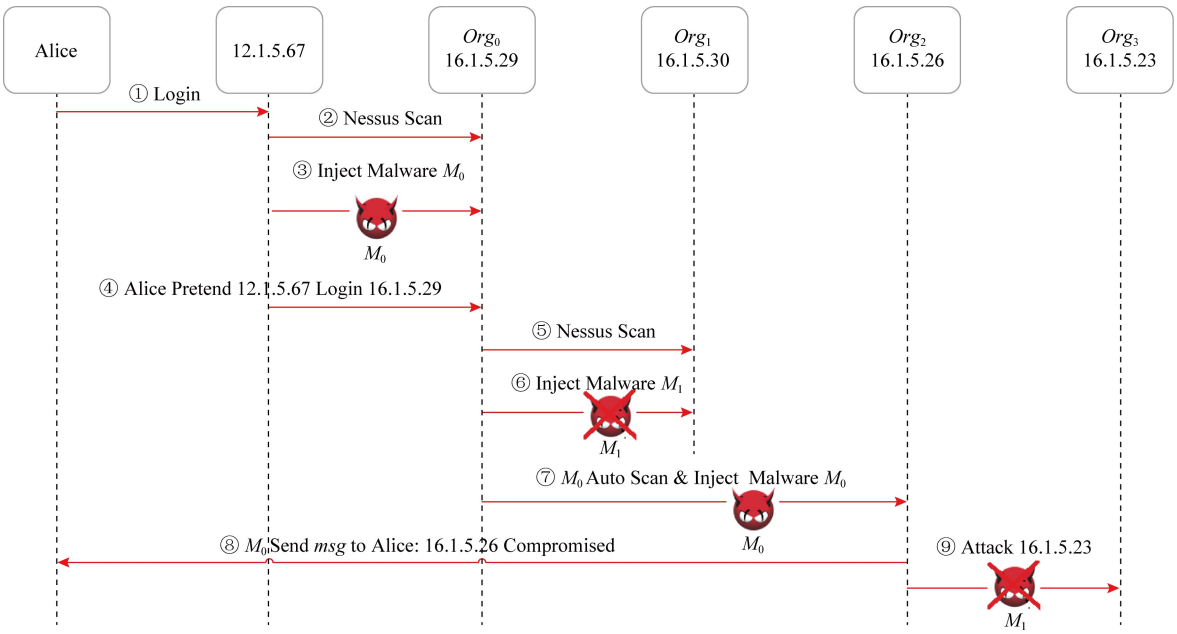

Fig. 5 Cyber attack data flow

图 5 攻击数据流

27T01:00:00,攻击者 Alice 收到新的僵尸机器 16.1.5.26 上线后,借助该机器攻陷了企业 Org_3 的 16.1.5.23 的服务器,并投放了恶意代码载荷 M_1.

Org_1 在区块链网络上创建了如图 6 所示的智能合约,只要满足条件:$ip \in \{SHA256(16.1.5.23), \cdots, SHA256(16.1.5.29)\}$ &$label = C2$,就执行函数 *send_email*("org1_admin@163.com")向服务器管理员发送告警信息.

为了满足模型需求,在实验评估中,本文非对称加密采用 RSA 算法,对称加密采用 AES 算法,单向加密采用 SHA256 算法.按照模型设计,本文中 IP 信息在情报共享时都以 SHA256(IP)的形式出现,即如表 2 中 SHA256(IP)的值所示,避免了情报中 IP 信息的泄露;同理域名、邮箱和姓名等亦采用该方法.社区内网络安全威胁情报共享时参照 STIX 标准,为了方便阐述,采用如表 3 的形式进行表示.如图 7 所示,首先,各组织机构 *Org* 向网络安全威胁情报中心 *Center* 注册;然后,Org_1 创建如图 6 所示

```
constract EmergencyCons{
    address public owner;
    bool public locked;
    uint public reward;
    string[] public conditions;

    function EmergencyCons(){
        owner=msg.sender()
        reward=msg.value
        locked=false;
        //add conditions
        conditions.push("62acd8afd97b6edf66e55fde96e4e03ec657de103541e679f6e13fbbf2eaefa4");
        conditions.push("0b2dd7f6cd1980521800ba5cafc08df4567dbbfe9a6c5cec89bcfeae4e017eb5");
        conditions.push("ec79018f878f26704ad240689a75802b3d098432b6262183b6d3b1a870fabe0a");
        conditions.push("a5d64e021f1bed445deaeab0a8a09e8e56855fbd83b27dc2dbde402a26031f36");
    }

    function(){
        if (msg.sender==owner){
            if (locked) throw;
            owner.send(reward);
            reward=msg.value;
        }else if (msg.data.length>0){
        if (locked) throw;
        for(uint i=0;i<conditions.length;i++)
        {
          if (msg.data["ip"]==conditions[i]&&msg.data["label"]=="C2"){
              msg.sender.send(reward);
              send_email("com1_admin@163.com");// send email to admin
              locked=true;
              break;
              }
        }
        }
    }
}
```

Fig. 6 Smart contract of Org_1

图 6 Org_1 智能合约

的智能合约;随后,Org_0 向网络安全威胁情报中心共享第 1 条网络安全威胁情报,因为满足智能合约的触发条件 SHA256(16.1.5.29)∈{SHA256(16.1.5.23),…,SHA256(16.1.5.29)}&$label$=C2,系统则向 Org_0 发送威胁源请求(因 SHA256(16.1.5.29)涉及隐私信息,Org_0 选择不解密 IP 地址,但返回不涉及隐私性的恶意代码 M_0 的行为和应急处置方法)并触发 Org_1 的智能合约执行,向 16.1.5.30 的管理员发送告警信息.最后,当 Org_3 发出〈2019-05-27T01:00:00,ip,SHA256(16.1.5.26),None〉网络安全威胁情报分析需求时,系统借助已有的网络安全威胁情报构建情报图,并利用标签传播算法计算出 SHA256(16.1.5.26)的标签为 C2,同时构建可能的完整攻击链:SHA256(12.1.5.67)→SHA256(16.1.5.29)→SHA256(16.1.5.26),并利用区块链对 SHA256(12.1.5.67)进行解密得到 12.1.5.67.

Table 2 IP and SHA256(IP) Cross-reference

表 2 IP 与 SHA256(IP)对应表

Org/Attacker	IP	SHA256(IP)
Alice	12.1.5.67	558692953c968a26a7187824a229d63be84753a4a0acace95982e1bbb2761a7b
Org_0	16.1.5.29	62acd8afd97b6edf66e55fde96e4e03ec657de103541e679f6e13fbbf2eaefa4
Org_1	16.1.5.30	0b2dd7f6cd1980521800ba5cafc08df4567dbbfe9a6c5cec89bcfeae4e017eb5
Org_2	16.1.5.26	ec79018f878f26704ad240689a75802b3d098432b6262183b6d3b1a870fabe0a
Org_3	16.1.5.23	a5d64e021f1bed445deaeab0a8a09e8e56855fbd83b27dc2dbde402a26031f36

Table 3 Cyber Threat Intelligence Sharing List

表 3 情报共享列表

Serial Number	Organization	CTI
1	Org_0	〈2019-05-26T10:00:00,ip,SHA256(16.1.5.29),C2〉
2	Org_0	〈2019-05-26T10:00:00,ip,SHA256(12.1.5.67),connect,ip,SHA256(16.1.5.29),"src ip connect target ip"〉
3	Org_2	〈2019-05-26T11:00:00,ip,SHA256(16.1.5.29),scan,ip,SHA256(16.1.5.26),"M_0 malware scan server"〉

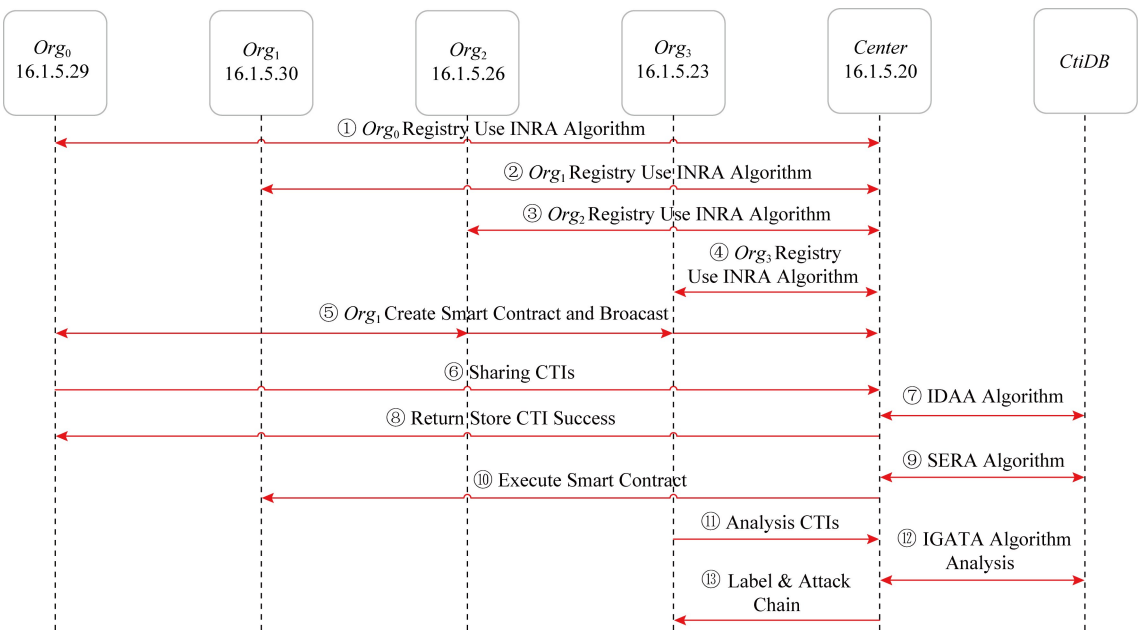

Fig. 7 Cyber threat intelligence data flow

图 7 威胁情报数据流

上述过程验证了本文基于区块链的威胁情报共享模型可以在保护情报隐私的同时构建完整攻击链.为了进一步证明本文模型的有效性,本文从开源情报收集的 2 010 条情报信息中提取出 15 条完整

攻击链,并将涉及的 30 个 IP 地址映射至 16.1.5.10～16.1.5.29 地址段内进行实验.30 个 IP 分别为 4 个 C2 IP、11 个攻击 IP、15 个攻击目标 IP.图 8 给出了在其他类型标签 IP 已成为情报节点的情况下,某类型标签 IP 成为情报节点的占比对成功构建攻击链的影响,可以看出当 C2 IP 成为情报节点时,威胁情报共享更有利于完整攻击链的构建.

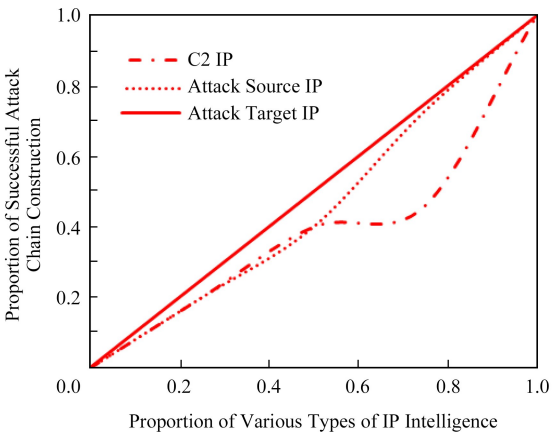

Fig. 8 The impact of different types of IP CTI node on the successful construction of the attack chain

图 8 不同类型标签 IP 情报节点对成功构建攻击链的影响

为了进一步评估本文模型在情报共享过程中隐私保护的情况,本文从情报共享方、情报利用方、情报涉及第三方的隐私保护强度方面同已有的典型模型进行了分析和模拟实验,实验结果如图 9 所示,其中纵轴表示隐私保护强度,根据表 4 中隐私保护算法的破解难度设定隐私保护强度;横轴表示情报共享中需要保护的隐私(即情报共享方隐私、情报利用方隐私和情报涉及第三方隐私)和综合隐私保护评价指标(根据三方隐私保护各种对情报共享的重要性,采用式(1)加权平均的方法计算).

$$f=0.5s_{\mathrm{s}}+0.3s_{\mathrm{u}}+0.2s_{\mathrm{t}}, \tag{1}$$

其中,s_{s} 表示情报共享方隐私保护强度;s_{u} 表示情报利用方隐私保护强度;s_{t} 表示情报涉及第三方隐私保护强度.

图 9 中,文献[4]提出的方案较好地解决了情报共享方的隐私保护问题,但是该方案对情报利用方和情报涉及的第三方隐私保护不足;文献[5]保护了情报利用方的隐私,但保护强度仍低于本文对情报利用方的保护强度;文献[6]主要保护了情报涉及的第三方隐私,其采用方式与本文第三方隐私保护的方式类似,所以保护强度基本相同;从图 9 中可以得出本文提出的借助区块链匿名机制保护情报共享方隐私和情报利用方隐私及利用单向加密算法保护情报涉及第三方隐私的方案从综合隐私保护强度上具有明显的优势.

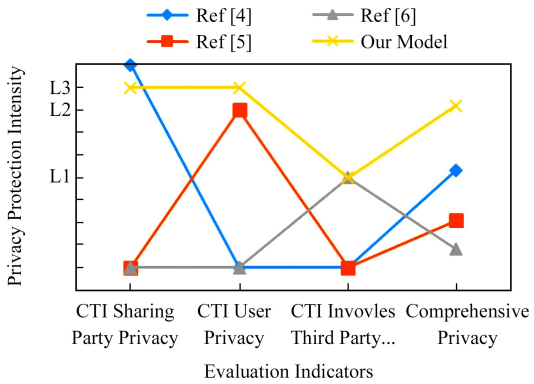

Fig. 9 Comparison among our model and others

图 9 本文模型与其他模型的比较

Table 4 Encryption Algorithm Crack Time Complexity List

表 4 加密算法破解时间复杂度列表

Encryption Algorithm	Crack Time Complexity	Reference	Symbolic
RSA	$O(n^3)$, $n=\mathrm{lb}\,N$ and $N=pq$	Ref [15]	L3
Homomorphic Encryption	$O(2^{(k-1)p})$	Ref [16]	L2
Hash	$O(2^n)$		L1

8 总 结

本文针对当前网络安全威胁情报共享过程中隐私保护和攻击链构建之间存在矛盾的问题,提出了一种基于区块链的网络安全威胁情报共享模型,利用区块链技术的去中心化和匿名性特点,既保护网络安全威胁情报共享参与组织和涉及组织的隐私信息,又便于推理分析完整的网络攻击链;利用区块链的回溯能力对攻击链中的威胁源进行追溯还原;利用智能合约机制实现针对网络威胁的自动预警响应.最后,本文通过模拟实验,验证了模型的可行性和有效性.

参 考 文 献

[1] Widup S, Spitler M, Hylender D, et al. 2018 verizon data breach investigations report, 11th edition [R]. New York: Verizon Communications, 2018

[2] Juan A G, Costin R, Kurt B. Threat predictions for 2018 [R]. Moscow: Kaspersky Security Bulletin, 2018

[3] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks [J]. Computers & Security, 2018, 72: 212-233

[4] Vakilinia I, Tosh D K, Sengupta S. Privacy-preserving cybersecurity information exchange mechanism [C/OL] // Proc of the 2017 Int Symp on Performance Evaluation of Computer and Telecommunication Systems (SPECTS). Piscataway, NJ: IEEE, 2017 [2019-04-30]. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8046785

[5] Badsha S, Vakilinia I, Sengupta S. Privacy preserving cyber threat information sharing and learning for cyber defense [C] //Proc of the 9th IEEE Annual Computing and Communication Workshop and Conf (CCWC). Piscataway, NJ: IEEE, 2019: 0708-0714

[6] Martinelli F, Osliak O, Saracino A. Towards general scheme for data sharing agreements empowering privacy-preserving data analysis of structured CTI [M] //Computer Security. Berlin: Springer, 2018: 192-212

[7] de Fuentes J M, González-Manzano L, Tapiador J, et al. PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing [J]. Computers & Security, 2017, 69: 127-141

[8] Zhao Wanying, White G. A collaborative information sharing framework for community cyber security [C] //Proc of the 2012 IEEE Conf on Technologies for Homeland Security (HST). Piscataway, NJ: IEEE, 2012: 457-462

[9] Goodwin C, Nicholas J P, Bryant J, et al. A framework for cybersecurity information sharing and risk reduction [R]. Washington: Microsoft Corporation, 2015

[10] Peterson K, Deeduvanu R, Kanjamala P, et al. A blockchain-based approach to health information exchange networks [C/OL] //Proc of the NIST Workshop Blockchain Healthcare. Gaithersburg, Maryland: ONC/NIST, 2016 [2019-04-30]. https://oncprojectracking.healthit.gov/wiki/display/TechLabI/Use+of+Blockchain+in+Healthcare+and+Research+Workshop

[11] Kang Jiawen, Yu Rong, Huang Xuming, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks [J]. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670

[12] Rawat D B, Njilla L, Kwiat K, et al. iShare: Blockchain-based privacy-aware multi-agent information sharing games for cybersecurity [C] //Proc of Int Conf on Computing, Networking and Communications (ICNC). Piscataway, NJ: IEEE, 2018: 425-431

[13] Al-Ibrahim O, Mohaisen A, Kamhoua C, et al. Beyond free riding: Quality of indicators for assessing participation in information sharing for threat intelligence [J]. arXiv preprint arXiv:1702.00552, 2017

[14] Yadav T, Mallari R A. Technical aspects of cyber kill chain [C] //Proc of Int Symp on Security in Computing and Communication. Berlin: Springer, 2015: 438-452

[15] Boneh D. Twenty years of attacks on the RSA cryptosystem [J]. Notices of the AMS, 1999, 46(2): 203-213

[16] Gu Chunsheng. Fully homomorphic encryption from approximate ideal lattices [J]. Journal of Software, 2015, 26(10): 2696-2719 (in Chinese)
(谷春生. 近似理想格上的全同态加密方案[J]. 软件学报, 2015, 26(10): 2696-2719)

Huang Kezhen, born in 1988. PhD candidate. His main research interests include network security situation and cyber threat intelligence.

Lian Yifeng, born in 1974. PhD, professor. His main research interests include network and system security evaluation.

Feng Dengguo, born in 1965. PhD, professor. His main research interest is information security.

Zhang Haixia, born in 1981. PhD, associate professor. Her main research interests include network information security.

Liu Yuling, born in 1982. PhD, associate professor. His main research interests include network security situation and security assessment.

Ma Xiangliang, born in 1986. PhD. His main research interests include information security and side channel attack.