

RDMA 协议应用及安全防护技术综述

刘雨蒙¹, 唐正梁¹, 路松峰^{1,2}, 朱建新¹, 刘运渠^{1,3}

(1. 华中科技大学网络空间安全学院工业互联网安全实验室, 湖北 武汉 430074; 2. 深圳华中科技大学研究院, 广东 深圳 518057;
3. 江苏为是科技有限公司, 江苏 苏州 215000)

摘要: 远程直接内容读写技术是一种有效提升数据传输速率、降低CPU占用率的通信方式, 在跨区域数据中心之间的转存、高性能计算、快速数据读写等领域起着重要的作用。然而, 作为新兴技术, RDMA 缺少得到业界广泛认同的安全方案, 目前, 随着大量 RDMA 应用逐渐从专用网络环境向一般以太网拓展, 关注其安全风险、为其设置一套在不影响传输效率的前提下保障安全性的防护措施是很有必要的; 此外, 由于采用了特殊的底层实现和协议设计, RDMA 技术不仅无法兼容现有的成熟安全方案, 还面临其他特殊安全风险挑战。为梳理 RDMA 攻防技术的发展, 向即将到来的 RDMA 技术的大规模应用提供安全保障: 以无线带宽协议和基于以太网的 RDMA 协议第2版为例介绍了 RDMA 技术及其实现原理, 调查了在相关场景下 RDMA 应用面临的安全风险, 总结了近年来 RDMA 安全领域的攻防研究进展, 汇总了能够应对这些安全风险的有效安全方案; 在证明其有效防御能力的基础上, 结合理论分析和实验数据, 对比了这些方案的优劣; 提出了 RDMA 攻防领域后续的改进方案和技术优化前景。

关键词: 远程直接内容读写; 无限带宽协议; 基于以太网的 RDMA 协议; 协议漏洞; 协议防护

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024022

Survey on RDMA protocol applications and security protection technologies

LIU Yumeng¹, TANG Zhengliang¹, LU Songfeng^{1,2}, ZHU Jianxin¹, LIU Yunqu^{1,3}

1. School of Cyber Science and Engineering, Laboratory of Industrial Internet Security, Huazhong University of Science and Technology, Wuhan 430074, China;

收稿日期: 2023-08-09; 修回日期: 2024-03-03

通信作者: 路松峰, lusongfeng@hust.edu.cn

基金项目: 2023年湖北省重大攻关项目 (No.2023BAA027); 湖北省重点研发计划项目 (No.2021BAA038); 深圳市科技计划基础研究项目 (No.JCYJ20210324120002006); 深圳市科技计划技术攻关项目 (No.JSGG20210802153009028)

Foundation Items: The 2023 Hubei Province Major Research and Development Project (No.2023BAA027), The Hubei Province Key Research and Development Program Project (No.2021BAA038), The Basic Research Project of Shenzhen Science and Technology Plan (No.JCYJ2021032412002006), The Shenzhen Science and Technology Plan Technology Research Project (No.JSGG20210802153009028)

引用格式: 刘雨蒙, 唐正梁, 路松峰, 等. RDMA 协议应用及安全防护技术综述[J]. 网络与信息安全学报, 2024, 10(02): 22-46.

Citation Format: LIU Y M, TANG Z L, LU S F, et al. Survey on RDMA protocol applications and security protection technologies[J]. Chinese Journal of Network and Information Security, 2024, 10(02): 22-46.

2. Research Institute of Huazhong University of Science and Technology, Shenzhen 518057, China;

3. Jiangsu Viscore Technologies Company Limited, Suzhou 215000, China

Abstract: The remote direct memory access (RDMA) technology, which has been effectively utilized to enhance data transfer rates and reduce CPU utilization, has played a significant role in various domains such as cross-regional data center transfers, high-performance computing, and rapid data read/write operations. However, despite its emerging status, RDMA has been lacking in widely recognized security solutions. With the expansion of RDMA applications from dedicated network environments to general Ethernet networks, the need to address the security risks faced by these applications has become imperative. A set of protective measures were established to ensure security without compromising transmission efficiency. Furthermore, the unique underlying implementation and protocol design of RDMA technology have resulted in incompatibility with existing mature security solutions and have led to the confrontation with specific security risks. The development of RDMA attack and defense technologies and the provision of security guarantees for the forthcoming widespread application of RDMA technology were elucidated. The principles of RDMA technology and its implementation were proposed, with examples drawn from the InfiniBand (IB) and the RDMA over converged Ethernet (RoCE) second edition protocols. The security risks faced by RDMA applications in relevant scenarios were investigated, and a summary of the research progress in the RDMA security field over recent years was provided. Effective security solutions addressing these risks were compiled and, after their defensive capabilities were proven, a comparison of their advantages and disadvantages was conducted through theoretical analysis and experimental data. Finally, improvement plans and prospects for technological optimization in the RDMA attack and defense field were proposed.

Keywords: remote direct memory access, InfiniBand protocol, RDMA over converged Ethernet, protocol vulnerability, protocol protection

0 引言

远程直接内存读写 (remote direct memory access, RDMA) 是一种通信技术, 允许在网络上对远程计算机或设备的内存进行直接、高速访问, 实现高效的数据传输, 同时减少 CPU 的介入^[1]。RDMA 技术之所以具备这些优势, 是因为 RDMA 通过网络把传输数据直接传入计算机的存储区, 从本地系统内存中快速移动到远端系统内存中而不对操作系统造成任何影响。RDMA 技术的实现基础是它所采用的特殊网络接口控制器 (RDMA network interface controller, RNIC)。在底层, 它与内存通过直接内存访问 (direct memory access, DMA) 技术或 PCIe 总线相连接并直接交换数据, 所以消除了外部存储器复制和上下文切换的开销, 因而能解放内存带宽和缩短 CPU 周期, 改进应用系统性能, 目前 RDMA 技术的速率可达 10~200 GB/s。

目前, RDMA 通信技术的具体实现主要是无线带宽 (InfiniBand, IB) 技术协议、基于以太网

的 RDMA (RDMA over converged Ethernet, RoCE) 协议和互联网广域 RDMA 协议 (Internet wide area RDMA protocol, iWARP)。其中 IB 协议由国际组织 IBTA (InfiniBand trade association) 提出, 从硬件级别保证了 RDMA 协议的高吞吐和低延时, 但缺点是实现需要特定型号的网络交换设备和不开源的 IB 协议来支持, 经济开销更大; RoCE 的实现基于以太网和用户数据报协议 (user datagram protocol, UDP), 只需要通信双方都搭载 RDMA 网卡, 基于现有网络链路即可进行 RDMA 通信^[2], 在泛用性上有优势; iWARP 基于传输控制协议 (transmission control protocol, TCP) 实现, 但是在性能上远远不及 IB 和 RoCE。本文主要讨论 IB 和 RoCE 的安全协议设计方案。

随着应用领域的不断扩大, RDMA 的安全问题也逐渐凸显。RDMA 技术最先出现在高性能计算 (high-performance computing, HPC) 社区, 用于对精度和延时等条件要求较为苛刻的科学计算。由于其出色的传输性能, RDMA 技术被逐渐拓展到更加开放的数据中心存储、分布式模型训

练等业务场景。而脱离特殊的科学计算等专网，在一般的以太网环境使用 RDMA 应用时，需要考虑面临的网络安全风险和其自身协议的安全机制漏洞。从传统网络安全风险分析视角看，RDMA 缺少很多通信协议必备的网络安全通信机制保护^[3]，此外，RDMA 协议还有一些独特的安全漏洞，如 RDMA 协议的通信序列号存在可被恶意利用的弱点^[4]，造成了欺骗攻击、侧信道攻击和信息窃取的可能性^[5]。

在对 RDMA 协议进行安全建模时，由于其在功能上对标的是 TCP，因此分析方法是可借鉴的。从宏观上看，对于一个网络环境下以客户端/服务器模型工作的通信协议而言，需要考虑的安全威胁包括拒绝服务、欺骗、信息泄露、篡改^[6]。评估一个通信协议的安全性时，通常从保密性、完整性、可用性 3 个角度出发。具体来说，缺失保密性或保密性低会导致信息泄露类问题，攻击方式包括明文嗅探^[7]和流量分析^[8]等，造成通信数据被窃取、隐私信息或行为习惯被分析^[9]等后果；缺失完整性或完整性低会导致欺骗和篡改类问题，攻击方式包括重放攻击、中间人攻击、通信数据被截获或修改^[10]等，造成攻击者恶意假冒，违法取得数据等后果；缺失可用性或可用性低会导致拒绝服务类问题，攻击方式主要是 DDoS 攻击^[11-12]，会导致系统无法提供可靠服务，性能低等问题。

在考虑 RDMA 安全性时，需要结合 RDMA 的特性，采用特殊的定制安全方案。虽然针对如何保障一个通信协议的安全性已经有了很多方案（如超文本传输安全协议（hypertext transfer protocol secure, HTTPS）、互联网安全协议（Internet protocol security, IPSec）等），但因为 RDMA 技术的特性，直接引入这些方案是不可行的。例如，RDMA 技术的优势是高速传输，引入目前成熟的 4 层以上加密机制等安全方案，会显著降低其速率^[13]。虽然已有的、被证实安全的非对称和对称加密算法（如 RSA 算法、DES 算法等）可以通过修改参数等方式改进这些算法的速率，但其计算速率仍然难以和 RDMA 匹配^[14-15]；除速率不匹配问题外，RDMA 还因为其工作在传输层，无法直接引入应用层的安全协议和工具。

随着智能网卡和软件卸载到网卡技术的出现，上述不兼容问题已经不再成为研究 RDMA 安全方案的障碍^[16]，这是引入 RDMA 安全机制并且不影响其原工作模式的最可靠方法。网卡卸载技术能有效提高通信协议效率，通过用户可编程的硬件平台现场可编程门阵列（field programmable gate array, FPGA）^[17-18]将安全方案卸载到智能网卡上，能在添加解密、MAC（message authentication code, 消息认证码）等安全防护措施的同时，尽量减少因此带来的通信中的延时增加^[19]。这些增加的可容忍延时是 RDMA 技术必须接受的，即使是在高吞吐的网络环境中，网络安全也是重要的技术支持。

目前，虽然针对 RDMA 安全的研究非常广泛，如风险及弱点分析、攻击设计和补救措施，但大部分研究是基于某项具体风险进行分析的，本文希望通过调研和总结，全面地了解 RDMA 安全特性的需求，总结 RDMA 的网络攻防主要手段，旨在帮助研究者和工业界形成通用的 RDMA 安全综合防护方案，为技术实现和优化做出贡献。

本文主要围绕 RDMA 的 IB 和 RoCE 第 2 版（RoCEv2）2 种主流 RDMA 实现协议的安全风险及其防护方案进行调研和整理，具体工作如下。

（1）梳理 RDMA 技术的相关基础知识，全面系统地介绍 RDMA 协议及其安全机制。

（2）参考其他网络通信协议的安全标准，对实际以太网环境下 RDMA 协议可能面临的威胁进行分类和阐述。

（3）调研总结国内外 RDMA 领域的相关研究，分析其贡献和不足。

（4）总结针对 RDMA 的 2 种主要实现协议的攻击方案，同时根据国内外研究人员的攻防实验数据，进行分析和对比。

（5）总结相关领域高速传输协议的主要安全机制，并展望 RDMA 安全协议在相关场景下未来的发展趋势，提出进一步的研究方向和思路。

1 RDMA 安全性分析

1.1 RDMA 技术概述

作为通信协议，RDMA 对标的是经典的

TCP/网际互连协议 (Internet protocol, IP) 协议栈, 但是 RDMA 主要用于高吞吐、低延时的大数据传输, 在电气模拟、地质勘探这类科学计算场景中会使用 RDMA 取代 TCP 协议栈^[20]。之所以 RDMA 协议能在速率和吞吐量上领先 TCP/IP, 是因为它具有独特的硬件支持, 传输数据流动中减少了很多非必要的延时。在典型 TCP/IP 协议栈的以太网通信过程中, 完整的通信流程是数据先从用户内存空间复制到内核区域, 内核将数据打包后通过直接信息存取 (direct message assess,

DMA) 推至网卡^[21]。采用 TCP/IP 协议栈的数据流如图 1 所示。

在使用 RDMA 技术的通信场景下, 数据不再需要双端 CPU 进行复制, 报文的组装和解析直接由硬件完成, 这样使数据收发绕过了内核, 并且不需要 CPU 参与, 不仅减轻了 CPU 的负担, 而且降低了任务因等待 CPU 排队和被 CPU 处理的延时^[22-23]。采用 RDMA 协议的数据流如图 2 所示。

TCP/IP 协议栈在收发过程中, 内核每次上下

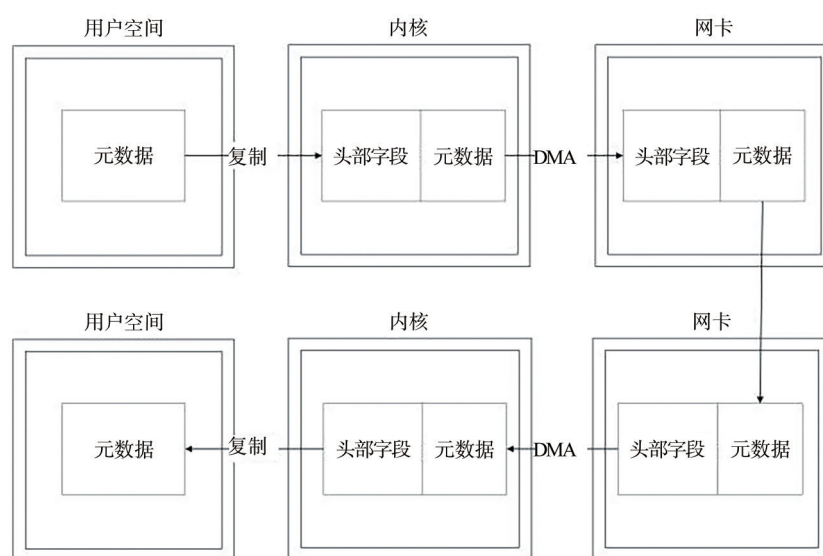


图1 采用TCP/IP协议栈的数据流
Figure 1 TCP/IP protocol stack data flow

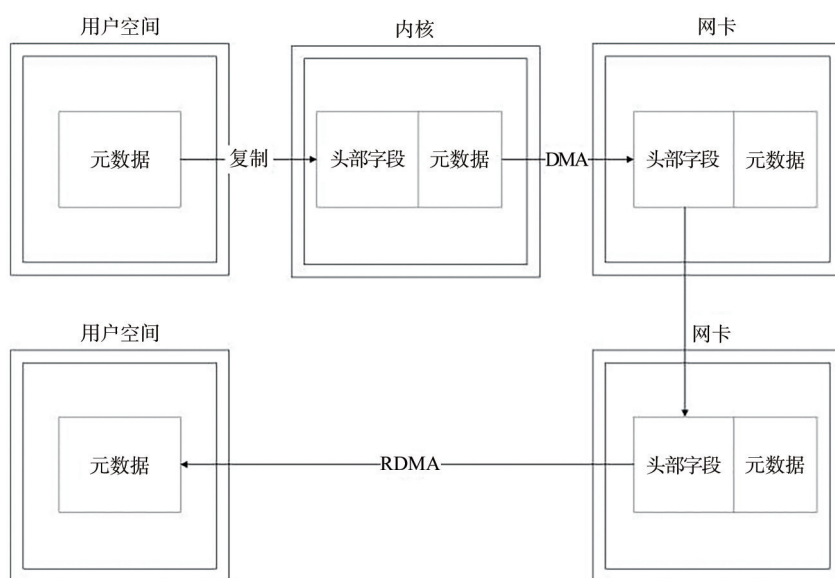


图2 采用RDMA协议的数据流
Figure 2 RDMA data flow

文切换都会带来 5~10 ms 延时，当网络流量达到 40 Gbit/s 左右时，使用 TCP/IP 的主机 CPU 占用率将接近 100%，而使用 RDMA 的主机 CPU 占用率在 5% 左右，延时降低至 10 ms 以下。

目前，RDMA 技术的具体实现方案包括 IB 协议^[24]、RoCE^[25]协议和 iWARP^[26] 3 种。本文主要介绍目前使用更为广泛的 IB 协议和 RoCE 协议。

IB 协议的全部架构由 IBTA 组织定义。IB 协议性能十分优秀，但企业要想使用 IB 协议，需要采用实现了 IB 协议的特殊网线、网卡和交换机等，且协议仍然是私有的，搭载了 IB 协议的设备无法与外界网络互通，加之基于 IB 协议的通信场景产生的经济开销较大，不利于科研工作和现实商业业务的展开。

iWARP 将 RDMA 封装在 TCP 上实现，借助 TCP 的可靠传输实现 RDMA，需要支持 iWARP 协议的特殊网卡，能够在标准以太网交换机上使用。但 TCP 需要考虑重传、拥塞控制等一系列复杂的控制机制，导致 iWARP 的速率远不及 UDP，因此目前 iWARP 使用的场景很少。

RoCE 能够支持更广泛的节点便利、经济地使用 RDMA，RoCEv2 协议在传输层支持 UDP，因此传统的线材、路由器也可以实现 RDMA 通信，尽管相较 IB 协议，RoCEv2 在性能上有所损失，但 RoCEv2 仍然是目前实现 RDMA 协议最便捷的备选方案。本文主要讨论 RoCEv2 和 IB 两种常见 RDMA 协议的安全防护方案。

下面介绍 RDMA 技术的一些基础概念，RDMA 基础概念释义如表 1 所示。

在 RDMA 处理具体通信任务的实体被称为 WQ，每个待处理的任务叫作工作队列元素。在发送或接收数据时，具体的读写任务会被添加到相应的工作队列中，RDMA 设备通过轮询这些工作队列来获取要处理的工作请求。WQ 按照其中任务的不同分为读任务队列和写任务队列，这 2 个队列分别称为 SQ 和 RQ。1 个 SQ 和 1 个 RQ 的组合叫做 QP。QP 是 RDMA 技术中通信的基本单元^[27]，每次通信在 RDMA 操作时的数据流实际上是通过 1 个本地的 QP 与远端的 1 个 QP 相关联而完成的。网络节点的每个 QP 都有 1 个唯一的编号，称为查询对号（query pair number, QPN），

通过 QPN 与路由头部可以唯一确定 1 个网络节点上的 QP。在实际通信中，1 个计算机节点上的 RDMA 应用进程会被分配若干个 QP，这些 QP 会与另一个远程计算机节点上的 QP 产生关联，QP 示意如图 3 所示。

表 1 RDMA 基础概念释义

概念英文缩写	中文全称	英文全称
WQ	工作队列	work queue
QP	队列对	queue pair
SQ	发送队列	send queue
RQ	接收队列	receive queue
CQ	完成队列	complete queue
write	远程直接内存写	RDMA write
read	远程直接内存读	RDMA read
RC	可靠连接	reliable connection
rKey	远程内存密钥	remote key
lKey	本地内存密钥	local key

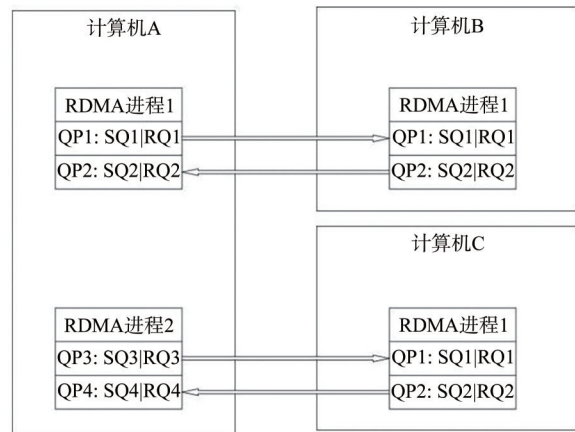


图 3 QP 示意
Figure 3 QP definition

当本端需要利用 RDMA 技术向远端写入一段信息时，进行 write 操作。在握手阶段，对端将计算机上某一片可用的内存地址和安全密钥告知本端，随后在本端进行 write 操作的过程中远端的 CPU 不会感知数据收发的过程。read 操作行为与 write 操作相似，对端获取到本端在握手阶段发送来的信息后，会将指定内存的相关信息和访问权限授予本端，在握手阶段结束后不需要对端 CPU 的参与。与传统网络编程中使用的 SEND 和 RECV 操作相比^[28]，write 和 read 操作解放了对

端的CPU占用,直接利用报文中携带的内存地址和相应的安全验证字段访问指定的内存。

无论是在以太网上传输的RoCEv2报文还是在专线专网下传输的IB报文都具有特殊规定的报文格式,具有独特的传输层结构,RDMA报文格式如图4所示。

由于IB协议是私有的未开源,因此本文主要讨论RoCEv2的报文格式。封装在UDP下的RoCEv2头部规定了RDMA的协议版本、服务类型和长度等信息。RoCEv2头部分为固定长度的RDMA头部和RDMA协议数据单元(RDMA protocol data unit, RPDU),其中RDMA头部包

含了rKey和QPN等信息。RDMA协议数据单元为具体的数据报文,包括发送数据的位置、大小和标志位等信息。RoCEv2头部的具体报文格式如图5所示。

1.2 RDMA通用安全机制

与TCP/IP协议栈相同的是,RDMA也提供了类似于TCP和UDP的服务类型,最常见的服务类型是可靠链接(reliable connection, RC)和不可靠数据包(unreliable data-gram, UD)。RC适用于对数据完整性和可靠性要求较高的场景,需要引入各种机制来保证可靠性,RC服务类型下每个节点与其他任意一个节点间通信时都需要

全局路由头部 (global routing header, GBH)	RDMA基本传输 头部 (basic transporting header, BTH)	RDMA头部 (RDMA header)	RDMA元数 据 (payload)	检验码 (checksum)
以太网头部 Ethernet (或IB头部 IBHeader)	工作队序列号 QPN	远程虚拟内存 地址addr		
IP头部 IPV4/IPV6	传输包序列号 PSN	远程密钥 r_key		
UDP头部 UDP		访问内存长度 data length		

图4 RDMA报文格式
Figure 4 RDMA message format

状态码 (OPCODE) 指出报文所 处操作状态 8 bit	solicited event (SE) 报文是否需 要回复标识 1 bit	MigReq 状态迁移 1 bit	pad count 填充长度 1 bit	transport header version IB传输版本 4 bit	partition key (P_KEY) 密钥值 4 bit
QPN 目的QPN 24 bit	ACK 标识报文是 否需要回复 1 bit	PSN 报文序列 号,用于控制 报文收发顺序 24 bit	pad 填充字段	payload 载荷	CRC 校验码 4 bit

图5 RoCEv2头部的具体报文格式
Figure 5 Message format of RoCEv2 header

各自维护一个不同的专用 QP，资源开销会更大；与之相比，在 UD 服务下，每个节点只需要维护一个 QP 即可完成对其他所有节点的通信。UD 服务的硬件开销小，并且节省存储资源，但缺点是可靠性和安全性较差。本文讨论的链接均为 RC 链接，即每个 RDMA 链接下，双端均有专用的 QP 用于维护通信，对数据完整性和可靠性要求较高，有着更加严格的报文字段检查机制^[25]。

1.2.1 报文格式与字段校验

RDMA 的通信流程可以分为握手阶段、传输阶段和结束通信阶段^[22]。数据包传输前双端机器会协商一些必要的节点信息，如工作消息队列序列号（work queue number, WQN）、数据包序列号（package sequence number, PSN）和 rKey 等。RC 链接下需要判断对端发来的数据包是否合法，有以下 5 个检查步骤。

(1) 数据包须通过循环冗余检验（cyclic redundancy check, CRC），以检查数据传输时数据包的比特是否被改变。

(2) 检查数据包携带的工作消息队列序列号。

(3) 检查数据包的序列号。

(4) 检查远端存储密钥。

(5) 检查虚拟地址。

检验不合法的数据包会被直接丢弃且没有确认字符（acknowledge character, ACK）响应。需要注意的是，在 RC 服务下，若对端发来的数据包涉及内存安全的重要字段（如 rKey 和虚拟地址）发生错误，服务器会直接断开这次链接^[24]。

1.2.2 内存区域 MR

在 RDMA 操作中一个很显而易见的问题是，单侧的内存安全由对侧决定，对侧的恶意操作可能形成劫持软件控制流^[29]，造成写入内存溢出和越权读取内存等后果。因此，需要将整体内存和被 RDMA 操作内存隔离起来。内存区域（memory region, MR）实现了这个功能，RDMA 应用在访问主机内存之前，需要向网卡请求注册一种称作 MR 的物理内存区域，MR 的映射表等会被复制到网卡内存，同时 RDMA 网卡会为每个 MR 分配 2 个密钥：rKey 和 lKey。rKey 用于提供对侧访问本侧内存时的权限，lKey 用于本地访问 MR。进行 RDMA 操作时，需要提供相应 MR 密钥才能成

功访问 MR。

MR 需要绑定 rKey 和 QP 编号使用，这些额外信息需要被存储在 RNIC 中占据一部分网卡空间。

1.2.3 保护域

考虑主机可能同时运行多个 RDMA 进程，每个 RDMA 应用由多个 QP 来实现功能，为了保证内存访问功能有序进行，RDMA 引入了保护域（protection domain, PD）概念。每个 PD 可以包括若干个 MR 和 QP，QP 仅可访问本 PD 中的 MR。PD 和 MR 工作关系如图 6 所示。RDMA 强制要求每个 QP 都必须是某个 PD 的成员，而且不能同时属于多个 PD。

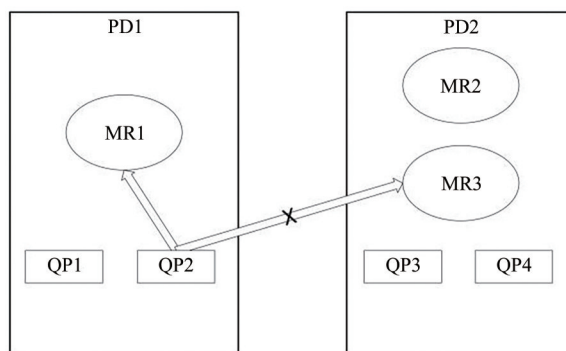


图 6 PD 和 MR 工作关系
Figure 6 Relationship of PD and MR

1.3 RDMA 安全脆弱性分析

单侧操作虽然能够极大提升传输性能，但带来了许多 TCP/IP 协议栈中不存在或被忽略的安全风险。虽然 RDMA 已经提供了一些基本的安全机制，但仍然无法保证实际传输中的数据的安全。这些弱点可整理为如下 11 点。

1.3.1 无法利用传统攻击检测工具

RDMA 是一个单侧操作，由网卡硬件完成，建链完成后对侧的 CPU 都是无法感知的，这意味着任何依赖于 CPU 工作、建立在应用层上的网络安全工具（如网站应用级入侵防御系统（web application firewall, WAF）、基于流量的入侵检测系统（intrusion detection system, IDS））都无法对 RDMA 的内存操作达到实时敏感。

1.3.2 无法进行攻击溯源和问责

在 RDMA 操作中，当安全问题发生在被单侧操作的机器上时，无法根据流量分析工具或日志系统来确定攻击来源或定位不当操作。考虑到

国内外 RDMA 正被部署在大型的分布式数据系统中^[30-31],而在分布式系统中形成共识,精确定位错误来源是极为重要的^[32]。假设集群中某台主机被不当地进行了 RDMA 操作,它虽然可以在操作完成后通过内存检查,发出违规警报,但由于主机对于此次违规的 RDMA 操作没有感知,无法提供此次非法操作的具体内容和实施者的任何信息,也就无法帮助集群的管理人员定位并且排除威胁。

1.3.3 无加密传输

RDMA 协议是一个纯传输协议,其本身不提供加密功能,在不采用特定 RDMA 实现协议时, RDMA 传输是明文传输的,这意味着 RDMA 报文中一些很关键的字段(如内存虚拟地址、rKey、PSN 等字段)都是暴露的。

1.3.4 无认证和完整性保护字段

现有 RDMA 协议都不存在完整性校验功能。虽然报文头部有校验和字段,但是并没有完整性保护功能,它的作用是在传输过程中数据受到干扰发生比特值改变时,能够帮助接收方定位并修复错误。校验和的生成公式和种子数据都是官方指定且公开的,当 RDMA 报文头部字段被人为修改且填充了正确的校验和时,接收方无法通过现有协议机制得知报文内容已被篡改。

1.3.5 内存访问密钥可预测

rKey 和 lKey 是 RDMA 操作中实现内存访问控制的安全核心,但是一些研究表明, rKey 和 lKey 的安全性存在漏洞且可预测其具体值。如果 rKey 可以预测或被盗,敌手就可以获取对端机器的内存权限,这意味着敌手可以在主机不知情的情况下任意操作内存。实际上, rKey 的数学实质是一个 32 bit 的比特串,当敌手拥有足够的算力或额外的信息时,预测一个正确的 rKey 实际上是可能的。

Tsai 等^[33]对 3 款使用最多的 Mellanox 公司生产的 RDMA 网卡进行连续的 MR 注册,收集并比较生成的 lKey/rKey 序列。他们的实验采用的 ConnectX-3、ConnectX-4 和 ConnectX-5 这 3 款 RNIC 的 lKey/rKey 几乎均为线性自增模式,尤其是前 500 个 MR 对应的 lKey/rKey 值均为顺序增长,考虑一般的 RDMA 系统(如 FaRM 等^[34-35])均采用

少量的 MR 处理大量的业务,这个漏洞可能会导致 rKey 的泄露。

Rothenberger 等^[4]的实验说明了同样问题,他们指出,在使用 bnxt_re 驱动程序的 RNIC 生成 rKey 时,时间顺序上相邻的 2 个 rKey 之间的增加值总是 0x100;对于使用 mlx4 驱动程序的 RNIC 设备, rKey 的数学规律还取决于注销操作。因此,假设攻击者能够获得这一系列递增 rKey 密钥的一部分,并且可以以合法身份注册若干的 MR,那么攻击者就能以更高的概率预测出其他用户的 rKey,从而构造合法的报文,达到内存访问的目的。

除增长方式存在规律外, rKey 的初始化也是静态的。初始的 rKey 一般是机器从静态的密钥集合中随机生成的,然而 Rothenberger 等^[4]发现,使用 mlx4 或 bnxt_re 驱动程序的 RNIC 都在复用相同的密钥集合,即使物理机器被重新启动。

1.3.6 QP 号可被预测

Rothenberger 等^[4]的硬件实验除了证实 rKey 存在安全风险外,还发现 RNIC 的主要生产厂商 Mellanox 和 Broadcom 都采用了线性分配 QP 号的硬件驱动程序。QPN 也是 RDMA 报文中传输头部的重要字段,当攻击者能够连续注册多个 QP 号或能够观察其他主机的注册 QP 行为时,能轻易地预测目标用户的 QP 号。

1.3.7 PSN 号可被预测

RDMA 传输头部中的另一字段 PSN 也存在安全问题。PSN 号用于在已经建链完成的 QP 通信中标识报文顺序,当报文序列号能被敌手预测时,可能会导致系统受到类似 TCP 流量劫持^[6]的攻击等。对一些上层的 RDMA 应用(如 NVMe-oF 等高层应用)而言,建链过程一般会被 RDMA 链接管理器封装以提高用户友好度。RDMA 链接管理器能够自动分配 RDMA 较底层的组件,如 MR、QP、起始 PSN 号等,但是 Rothenberger 等^[4]通过实验发现,一些常见的开源 RDMA 应用都采用了手动设置静态 PSN 起始号的策略,如 Octopus^[36]、Dare^[37]等。

1.3.8 滥用性能提升配置或安全配置未启动

一些 RDMA 设备厂商为了性能优化或提升便捷性,引入了一些新的配置,这些配置实际上威胁到了 RDMA 的内存安全。

如在默认配置下,用户在注册 MR 时,需要向 RNIC 发起申请, RNIC 会进行实际分配的物理地址到内存虚拟地址的转化,用户使用此虚拟地址注册和访问 MR。Tsai 等^[38]指出,高版本的 Mellanox RNIC 引入的一项新功能允许用户进程直接使用物理内存地址注册 MR,可能会导致一些基于 SRAM 的攻击发生。虽然这项功能能够减少地址转换带来的性能损失,但暴露物理地址在安全防护的角度会带来(如 hammer 攻击^[39-40]这样的)硬件攻击。

此外,当选择配置隐式按需寻呼(implicit on-demand paging, ODP)时,进程无须主动注册内存地址,使用的内存直接由 RNIC 动态分配,在一些高性能场景下 ODP 被频繁使用。但 Rothenberger 等^[4]指出,当启动 ODP 时,由于需要按照需求分配, RNIC 的访问控制权限将提升至整个物理内存,原来的 RDMA 安全机制也将失效,若攻击者能够在启用 ODP 的主机上拥有权限,那么他将能够访问整个内存空间。

此外,调查发现^[4],无论是底层的研究人员的一般工作习惯,还是上层的 RDMA 链接管理器,都倾向于默认使用单 PD 策略,这样确实减少了 RNIC 用于管理和维护 PD 所消耗的资源,但每个 QP 都能访问到全部内存区域, RDMA 进程之间的隔离性也被破坏。

1.3.9 内存地址可预测

进行 RDMA 操作时,需要的远程内存地址 Addr 通常都是指远端内存虚拟地址,一般来说是敌手无法成功预测的。但是 Rothenberger 等^[4]指出, RDMA 操作中 RNIC 操作内存时会将对对象直接分配在连续的内存空间中,攻击者能够根据某个地址和长度去预测其他对象的具体位置。在一般的操作系统中,类似于地址空间布局随机化^[41]技术会随机化排列进程的地址空间位置,但基于 RDMA 的应用程序基本为独立进程运行。除了能够预测具体对象的地址外,敌手还可以预先申请合法内存,然后填充大量垃圾数据,使得其他正常用户的内存溢出,生成攻击者所需的软件控制流^[42]。

1.3.10 无抗拒绝服务攻击能力

由于接收端无法感知报文的到达,在 RDMA

操作中识别流量来源、控制发送方链接数量和速率都是十分困难的^[43]。敌手可以在不被发现的情况下发送任意数量的单方面请求,虽然 RDMA 本身速率很快,一般网络环境下的大流量对于 RDMA 应用而言并不会引起拒绝服务攻击,但是,考虑主机硬件资源是有限的,尤其是 RNIC 上的 SRAM 内存需要存储 RDMA 链接上下文等重要信息,很容易被攻击者的写入请求清洗。

攻击者可利用 RDMA 的链接安全机制,篡改其他用户报文中的内存字段,使受害者的链接被服务器设置为错误状态从而中断链接;敌手也可以大量发送正常的建链申请,不断消耗 QPN 等 RDMA 链接资源以达到服务器的承载上限,使正常用户的请求无法被处理,以达到破坏系统可用性的目的。

1.3.11 RDMA 网卡存在侧信道

Tsai 等^[33]在分析 RDMA 硬件时发现 RNIC 在处理访问内存地址请求时,网卡中缓存命中与否会显著影响 RDMA 请求的处理返回时间,利用这种时间差异可建立 RNIC 上的侧信道^[44],为敌手定位目标消息所在的内存提供额外信息。在默认配置下,为了完成虚拟地址到物理地址的映射并且提高转换效率, RNIC 会在内置的 SRAM 中缓存部分内存转换页表,当 RDMA 请求的内存地址并不在 RNIC 的页表记录中时, RNIC 需要访问主存以更新缓存页表。经过实验测算,页表缓存命中与未命中时的延时差在 1 ms 左右。除了页表之外, RNIC 也会缓存一些 MR 参数(如 rKey、lKey 等),这些 MR 在缓存未命中时,也会存在可供建立侧信道的明显延时。以 ConnectX-5 为例,在上述 3 起事件中,直接命中页表时,响应速度最快,约在 2 μ s 以下;未命中页表需要访问内存时,响应速度约在 2~4 μ s;未命中 MR 时,速度最慢,约在 4~6 μ s。考虑全体 RDMA 应用会共享 RNIC 上的 SRAM,这些侧信道的存在可以使敌手定位目标数据的存储位置或预测任务的执行情况,从而协助攻击者获取额外的系统信息或者发起基于存储系统的攻击^[45]。

除了 RDMA 协议本身通信机制或硬件实现上的弱点,在一般网络环境下,针对其他 TCP/IP 协议栈的网络攻击也会对 RDMA 协议造成影响,

如泛洪攻击和流量分析等^[46]。

2 相关研究工作

在2005年IETF RDDP工作组发布的RFC 4297中,首先认识到了RDMA的安全问题^[43]。2003年初,文献[47]指出,可以利用IPSec协议来保证传输数据的保密性。在随后的两年里, Lee等^[48]首次提出IB架构中rkey和数据载荷以明文传输的问题。文献[48]指出,可以利用带数据分组拆分功能的交换机、符合RDMA特点的密码体制以及维持一个封装数据分组中从源地址发往目的地址时保持不变循环冗余检验(invariant CRC, ICRC)来保证RDMA协议的可用性、保密性和完整性。这样做的问题是支持数据分组拆分的交换机和ICRC字段对传统的交换机网络并不友好,而且密码体制中QP级密钥管理的前提是假设所有节点都有全网节点的可信公钥,然而这样的密钥管理机制在复杂的远程传输环境中很难实现。另外,将24位的PSN作为nonce来抵御重放攻击,在目前硬件条件下可行性不高。因为目前最先进的网络接口控制器(network interface controller, NIC)可以在数秒内完成24位PSN的枚举。

2007年,IGTF RFC5042回顾了信息欺诈、篡改、信息披露、拒绝服务攻击(denial of service, DoS)等攻击方式^[49],并建议使用IPSec完成RDMA传输协议的认证和加密。RFC5042提供了基于RDMA的安全协议蓝图,但只提及了对RDMA潜在危害的安全问题,并没有具体的实现方式。2007年, Lee等^[50]针对RDMA的IB协议实现提出了增强其安全性的综合框架。其提出的安全服务包括密钥管理方案、消息加密与认证方案、状态过滤和源认证4个方面。密钥管理方案是以对称密钥机制为基础的QP级密钥管理,并规定了初始密钥分发的规则;消息加密与认证方案规定了报文格式中MAC在每个数据包中的位置,并展示将认证加密算法GCM集成到IBA中;状态过滤和源认证提供了抗DOS攻击的手段。

Noronha等^[51]讨论了实现网络文件系统(network file system, NFS)/RDMA协议的设计原则,实施并评估了不采用IB架构实现NFS/RDMA的设计,并通过修改NFS的文件读写方式解决了以

往NFS/RDMA系统中服务器缓存区被暴露而易于受到攻击的问题,能显著提高存取系统中RDMA服务器的安全性。

2017年, Rashti等^[18]提出了将安全防护环节卸载到网卡硬件的方式来确保安全,利用用户可编程的FPGA硬件实现能在10 Gbit/s以太网下工作的SmartNIC,并且支持OpenSSL等安全软件库,以提供网络数据流的加密和身份验证。由于SSL需要大量主机资源,SSL协议卸载到SmartNIC后,可以大大降低RDMA安全方案的资源消耗。

2019年, Tsai等^[33]对目前的RDMA原型硬件系统加以分析,设计并实现了一套攻击框架,用于建立一个侧信道,并且分析受害者对目标数据的访问情况。文献[33]利用攻击框架对现有RDMA原型系统Crail实施攻击,发现Crail并不能抵御侧信道攻击,并指出适用于RDMA的缓解机制。此外, Tsai等^[38]讨论了单边通信的机遇和挑战,特别指出了像RDMA这种单边通信时需要注意单边操作无感知带来的安全风险和易受DoS攻击的威胁。文献[38]指出,用于支持RDMA类的单侧通信的硬件存在一些缺陷,包括硬件生成的rKey和lKey可被预测、智能网卡存在侧信道、本地内存地址泄露3个硬件漏洞。在防护措施方面,对于单边操作无感知威胁,服务器端可以对读写的客户端使用加密密钥认证来源,但这会使单边操作增加一定性能开销。对于DoS威胁,可以考虑使用SmartNIC和可编程交换机来实现防御;对于RDMA的硬件漏洞带来的威胁,在抗密钥预测方面, RNIC可以使用加密生成的密钥作为lKey和rKey;在防御侧信道攻击方面,可以为不同的应用隔离SRAM,或引入噪声干扰时序差异;在解决物理地址泄露和抗hammer攻击方面,可以在软件级别、浏览器级别以及DRAM和内存控制器的硬件中消除物理内存地址暴露的风险,这为硬件安全防护提供了多种思路。

2020年, Taranov等^[52]提出了安全RDMA(security RDMA, sRDMA)协议概念和利用SmartNIC来实现安全的RC链接的具体方式。为了克服SmartNIC内部存储空间少的缺陷,sRDMA中使用保护域级密钥和动态计算来自动推导链接中的密钥,而不是针对每个QP单独设置并且存储密

钥。文献[52]在实现了 sRDMA 的同时,对各种对称加密算法和哈希算法应用到 sRDMA 时,进行了 RDMA 性能损失上的测算,为后续研究提供了算法和协议构建选择。

2021 年, Rothenberger 等^[4]首先分析了 RDMA 各种安全风险,以此为基础,广泛调查了现有使用了 RDMA 的各种原型系统中的潜在安全威胁,并提出了多种应对方案。他们指出,支持 RDMA write 和 IB Send 混合操作的键值对存储系统 HERD^[36],其使用单个内存缓冲来注册所有 RPC 的客户端请求,客户端使用 RDMA write 写入服务端内存,但是服务器并不会对客户端的链接资源设置数量限制,因此 HERD 并不能抵御 DoS 攻击;支持 RDMA 的分布式持久化文件系统 Octopus^[37],其使用单一内存缓存注册响应请求,并不对服务器链接资源和数量做限制,也不能抵抗 DoS 攻击,而且 Octopus 使用硬编码来初始化 PSN,导致敌手容易线性地预测 PSN;使用 RDMA 高性能特性来加速共识,形成的协议 Dare^[53]与 Octopus 类似,PSN 的初始化是静态的,并且所有数据注册到一块单一区域,但是利用了共识协议限制客户端数量,能够在一定程度上缓解 DoS 攻击;高性能分布式数据存储系统 Crail^[54]设置每次注册一个固定大小的内存区域,这使得预测虚拟地址和 rKey 变得较为容易,而且 Crail 也不对请求内存缓存做限制,因此其不能抵御 DoS 攻击。他们提出在软件层面进行 QPN 和 SPN 的随机化等手段,以防止敌手预测。在硬件层面,参考了一些 IB 的安全方案,通过为硬件添加计数器,引入内存窗口和概念等方式提升硬件安全等级。在协议层面,提出了基于 IPSec 的网络层加密方案和基于 TLS 的应用层加密方案 2 种不同的加密方案,并且加密方案可以参考 IB 的相关流程。在网络流量层面,在客户端设置相应的最大链接数限制器,并在服务器端的前置链路上新增一些流量限制配置,如具有过滤功能的交换机和路由器。

2022 年, Diamond 等^[55]提出在 IB 上进行端点加密保护以确保 RDMA 安全,他们用常见的高性能智能网卡接口 NVIDIA Mellanox Bluefield-2 100 Gbit/s 进行实验,将处理报文和解密 RDMA

流量的步骤卸载到网卡硬件上,实现了协议的加速。实验结果表明,使用硬件加速后(即在实现 RoCEv2 协议时,使用了如 IPSec 方案这样成熟的加密方案),其 RDMA 流量的最大吞吐量也能接近 86 Gbit/s,性能损失在可以接受的范围内。同年, Tranov 等^[56]对使用 RDMA 工作的成熟协议、基于 Fabrics 的非易失性存储器扩展(non-volatile memory express over fabrics, NVMeoF)^[57]进行了安全分析,发现目前 NVMeoF 协议的安全机制并没有解决 RDMA 带来的安全漏洞。他们指出,一般用户也可以绕过操作系统及其内核的安全机制,对任意一个本地的 RDMA 链接进行数据包注入攻击,即使启用了 RoCE 上的 IPSec,也能达到获取使用 NVMeof 设备任意内存区域访问权限的目的。

在以上研究中,考虑了对于 RDMA 协议的各种可能出现的攻击以及相应的防护方案。综合来看,针对 RDMA 协议的安全研究虽然广泛,但是考虑 RDMA 协议目前正在从专用设备和专用网络的 IB 协议,拓展到不依赖于特殊网络设备和 RoCEv2 协议,仍然需要研究一套能有效应对各种应用场景的 RDMA 安全防护方案。

3 对 RDMA 的攻击方案

综合第 2 节分析的多种 RDMA 安全威胁,整理针对 IB 和 RoCEv2 协议的有效攻击方案,概括如下 4 点。

3.1 明文嗅探攻击

由于 RDMA 的几种协议模式默认都没有采用加密,所有的报文字段均可以通过报文内容直接获得,因此敌手通过网络嗅探器可以轻易截获用户信息,可能间接造成 lKey 和 rKey 密钥等重要信息的泄露。

3.2 拒绝服务攻击

在 RDMA 合法建链完毕后,利用 RDMA 应用进行交互的 2 台主机可以视作客户端与服务端,因此传统网络模型下的拒绝服务攻击对于 RDMA 而言,也是必须面临的问题。对 RDMA 的拒绝服务攻击大致包括消耗网卡资源降低服务质量、消耗链接资源阻止新链接建立、恶意降低其他用户服务速率或断联 3 类。

3.2.1 消耗网卡资源以降低服务质量

智能网卡 RNIC 除了承担接发控制、解析处理报文的功能外, 还需要存储链接信号、临时缓存、缓存上下文等信息, 这些信息存储在 RNIC 中的高速低延迟的 SRAM 中; 但 SRAM 空间大小有限, 攻击者在多个客户端上可以快速消耗服务器 RNIC 上的资源, 如恶意注册内存空间导致合法用户的请求无法及时处理。当收到敌手发来的大量 RDMA 请求时, 由于 RNIC 自身可存储的空间有限, RNIC 会将原有的一部分正常链接的记录转存到主机内存中并在 SRAM 上覆写, 由第 1.3.11 节的侧信道实验可知, 当 RNIC 缓存未命中时 RNIC 的处理延时存在很明显的增加, 造成正常用户连接速率的下降。而且, 由于数据传输过程对于服务端的 CPU 而言是不可见的, 服务端无法察觉到自身资源已被耗尽, 因此利用一般的网络工具去追踪攻击来源是不可行的。

Rothenberger 等^[4]利用实验测试了攻击者发送的总报文字节数量对于受害者链接速率的影响。他们为每台实验机配置了 Mellanox ConnectX-3 的 RDMA 网卡, 若干台攻击机器与一台正常的客户机同时连接到提供 RDMA 服务的服务器上, 以 4 KB 为单个报文字节大小的最小增加单位, 不断发送 RDMA 请求以消耗 RNIC 的报文处理能力, 变量维度为攻击者发送的单个报文字节大小与攻击者数量, 攻击有效程度体现在受害者机上增加的链接延时和减少的可用带宽。

实验结果表明, 链接延时作为指标时, 增加单个报文的大小对于受害者的链接延时影响不大, 但是攻击者发起的链接数量对链接延时有明显的影响, 每个不断发送报文的攻击者大约会使受害者的链接延迟增加 4.20 μs 。吞吐量作为指标时, 在 read 场景下, 当攻击者数量小于 3 并且发送的报文大小超过 128 byte 时吞吐量才会有急剧的下降, 报文越大降幅越明显, 最大约为 80%~90%, 而攻击者数量大于 3 时, 吞吐量始终维持在一个很低的水平, 约为 500~1 000 rqs; 在 write 场景下, 攻击者数量会阶梯式地影响吞吐量, 当发送的报文大小超过 128 byte 时对吞吐量才会有明显影响, 他们建议至少配置 5 台攻击者机器, 才能得到很明显的实验结果。

3.2.2 消耗链接资源阻止新链接建立

在客户机 RDMA 建链过程中, 对端接收到建链请求后, 需要分配相应的 QP 和 MR 等链接组件用于处理本次 RDMA 链接, 但是开放 RDMA 服务的机器能够同时维持的链接数量是有限的, 受到 QP 号等资源上限的限制。QP 序列号是一串 24 位长的比特串, 这意味着一台机器最多可以维持 2^{24} 个 RDMA 链接, 如果攻击者能够无限制地发送新的建链请求, 那么服务器请求达到饱和后将无法处理新的建链请求。

Rothenberger 等^[4]在实验中发现, 目前 RNIC 厂商都会在硬件驱动中限制发起的最大链接数量, 如 Broadcom 公司支持的上限是 32 707 个活跃链接, Mellanox 公司支持的上限是 261 359 个链接, 这个数字远远小于 2^{24} , 因此若想耗尽 QPN 这类软件链接资源, 需要有相当多的攻击者参与且服务器也需要进行重新配置, 实现起来较为困难。他们发现, 一些使用 RDMA 链接管理器上层的应用程序会分配 Linux 系统下的文件描述符, 用于接收 RDMA 事件, 而文件描述符存在数量上限, 限制为 4 096 个, 因此对使用了 RDMA 链接管理器上层的 RDMA 应用采用建链资源消耗类的拒绝服务攻击时, 效果会更明显。

3.2.3 恶意降低其他用户服务速率或断联

由于网卡的缓存空间相较于一般主机显得十分珍贵, 为了防止缓冲区溢出, RoCEv2 使用基于优先级的流量控制 (priority-based flow control, PFC) 进行拥塞控制^[25]。当网卡中的缓冲区占用超过指定阈值时, PFC 机制会控制交换机向上一个结点发送 PFC 暂停帧, 此暂停帧提示上游应暂停发送某一队列和等待时间, 拥塞解除时会重新发送暂停帧来恢复数据传输。利用这种机制, 敌手可以通过大量泛洪或恶意破坏 NIC 缓冲区方式发出大量暂停帧。PFC 暂停帧风暴影响的是全体网络的速率, 因为受攻击的网卡会向上游交换机持续发送 PFC 暂停帧, 进而影响更上层的网络设备, 从而造成对整个网络的拒绝服务攻击, 这种攻击方式叫作 PFC 暂停帧风暴。

在 IB 协议体系下, 可实现针对特定用户链接的恶意断联攻击。在使用 RC 链接的前提下, 收到 QPN 和 PSN 等序列号不正确的请求时, 会

具有一定的容忍度，不会立刻断开链接，而在访问地址、rKey、操作编号、载荷长度等重要字段发生错误时，会立刻断开链接。当攻击者能推测出受害者的 QPN 时，攻击者可以伪装成受害者向服务器发送字段错误的报文，即简单地修改部分字段与有效载荷长度后，让服务器误认为链接发生了不可逆的错误，从而丢弃链接，并将此 QP 状态标记为错误，造成受害者链接被恶意断开。

Rothenberger 等^[4]在实验中利用 RoCEv2 协议数据包生成和注入工具，对某一特定的 QP 枚举 2^{24} 个 PSN 号，经测试，大约每 10.6 s 就能生成一个能使得原链接被主动丢弃的伪报文，而考虑第 1.3 节的 RDMA 存在 QPN 和 PSN 易于被猜测出的安全弱点，若能结合这些额外的信息，攻击者就能够以更高的把握在极短的时间内实现对特定 QP 的断联攻击。因此，无论是攻击者只针对特定的客户端链接，还是无目的地单纯破坏服务器上的链接都是有可能的。

3.3 伪造报文注入攻击

参考 RDMA 安全脆弱性分析第 1.3.4 节，RDMA 由于无认证机制，敌手可以随意篡改报文内容后重新计算校验和，将伪造的报文注入链路后就能被目标 QP 接收。

实施一次成功的伪造报文注入攻击需要结合第 1.3 节提出的 RDMA 的多种安全威胁，预测出正确的 rKey、QPN 和 PSN 之后，攻击者才具备成功伪造 RDMA 报文头部的能力。以 RoCEv2 协议的注入为例，伪造注入报文需要将关键的字段填充入 RoCEv2 的报文头，将其封装成传输层为 UDP 的一般报文，并且将其注入网络中即可。

假设敌手构造了受校验字段正确的报文并且报文成功注入，当攻击者的单个伪造报文先于受害者的正常报文到达服务器时，服务器会将受害者用户的报文视作正确但重复的报文直接接收，且不发出回复，仍然保持链接状态，受害者处于等待对方 ACK 回复的状态；当伪造报文被处理接收后，服务器端的 PSN 计数器会增加，受害者的后续报文会因为 PSN 错误而被丢弃，变为请求超时，等待 QP 重新链接的状态。这段时间由攻击者代替受害者与 RDMA 服务器进行通信，造成了实际上的身份顶替，并且需要使注入时间

与受害者超时重连的时间相同。Rothenberger 等^[4]指出，如果攻击者准确地注入 $2^{24}-n$ 个报文 (n 为攻击者注入的报文数量)，则此操作可以将 PSN 号重置为正确的序号，服务器和受害者都完全无法察觉到存在报文注入，但是要求受害者在注入 $2^{24}-n$ 个报文期间不发送新的请求。实验中，周期约为 13 s，这实际上是一个完全可以接受的窗口期。

为了成功伪造报文，需要攻击者预测出正确的字段。首先考虑 rKey 的预测问题，rKey 在本质上是一段 32 bit 的数字序列，其中前面的 24 bit 为 index 字段，用于寻址，帮助快速索引地址转换表，后面 8 bit 为校验字段。rKey 结构如图 7 所示。

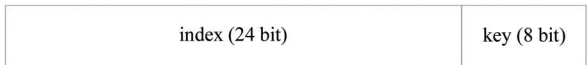


图 7 rKey 结构
Figure 7 rKey structure

rKey 具有高度的规律性可供敌手预测，研究表明 rKey 的数学实体与 RDMA 系统采用的 RNIC 型号是强相关的^[38]，假设敌手能作为正常用户取得一系列 rKey 中的一部分，那么对于敌手而言通过数学运算取得其他 RDMA 操作的 rKey 是相对容易的。

其次是预测 QPN 和 PSN。QPN 和 PSN 的实体均为长度为 24 bit 的数字序列。24 bit 并不是一个足够安全的长度，Tsai 等^[38]指出，对于一个确定的单对单 QP 链接而言，生成有效 PSN 平均只需要 223 个数据包。在数学规律上，与 rKey 相同，QPN 和 PSN 的增长机制同样存在可预测性，由第 1.3.6 节和第 1.3.7 节的分析可知，几乎所有的硬件驱动中的 QPN 增长机制均为简单的线性增长，敌手只需要观测部分 QPN，就能推断出前后任务使用的 QPN。而且很多应用下 PSN 被设定为静态初始化或伪随机生成，当敌手自己能够以合法身份去大量发起建链申请时，他能通过申请 QP 号，缩小受害者可用的 QP 范围。

由于 QP 号在建链后基本不变，PSN 的预测是更重要的。考虑 PSN 和 QPN 均只有 2^{24} 个，直接发送 PSN 在 1 至 2^{24} 的枚举报文也有很大概率成功构造注入有效的数据包，暴力破解 PSN 的策略

与枚举 TCP 链接的序列号类似^[58]。当受害者保持链接时,成功遍历并且发送这些数据包的时间并不是不可接受的。

Rothenberger 等^[4]分别对 IB 和 RoCEv2 协议进行了报文注入实验,并且开发了数据包生成工具 ReDMark,用于模拟 RNIC 的报文生成功能。实验结果表明,当使用 RoCEv2 协议对一个完全随机 PSN 号进行全枚举时,ReDMark 对于 Mellanox 类 RNIC 耗时约 10.6 s,对于 Broadcom 类 RNIC 耗时为 23 s。由于 ReDMark 用 CPU 模拟 RNIC 的功能,并没有绕过操作系统发送报文,生成正确 PSN 耗时实际上会更少一些。

此外,一些 RDMA 应用服务端(如 NVMe-oF)^[56]仅要求在报文中包含目的 PSN 和 QPN 即可,并不要求检验报文的源 PSN 和 QPN,此时攻击者甚至无须猜测 PSN 和 QPN,只需要将受害者的报文进行简单的修改和预测,随后从自身的任一 QP 发出即可。攻击者尝试进行预测从而构造出的有效数据头部如图 8 所示。

3.4 内存任意读写攻击

伪造报文攻击的最终目的是推测正确的内存地址,在 RoCEv2 协议下,攻击者可以将已预测出的 rKey 和报头中虚拟内存地址进行组合,得到 RDMA 传输层头部,并且获得受害者的通信信息。

除了对受害者本人的信息窃取之外,攻击者

还可能威胁使用同一个 RDMA 应用的其他用户。虽然直接抓包获取的是内存虚拟地址,但是在弱点分析的 RDMA 应用(见第 1.3.8 节和第 1.3.9 节)会直接使用物理地址进行注册或让 RDMA 链接管理器自行分配,这可能导致敌手直接抓包,得到一个准确的物理内存地址。由于一个 RDMA 应用进程通常将资源置于一个 PD 中,创建为每个用户服务的 MR 时也会集中连续分配相邻内存,当这些 RNIC 中的缓冲区邻近时,敌手能够根据自己缓冲区的地址去预测属于其他用户的内存区域的地址,随后遍历不同长度发送至服务端,直至成功读取目标内存块的内容。而且,由于 rKey 本身的特性,结合硬件驱动的类型根据本区域的 rKey 获得其他相邻内存区域的访问权限并不困难^[38],即使不能准确地预测出这些字段值,攻击者也可以通过 rKey 和内存位置的组合进行暴力遍历。当应用开启在 ODP 功能(见第 1.3.8 节的由 RDMA 链接管理器自动分配缓冲区)时,攻击者甚至无须预测其他内存块的 rKey,只需要得到启动 ODP 注册的第 1 个 rKey 就可以直接访问全体内存空间。

通过 RDMA 实现的内存任意读写造成的威胁很大,Rothenberger 等^[4]认为,攻击者可以利用 RDMA 的 CPU 无感知的特点静默地读写数据,这意味着受害者无法得知自己的内存数据被访问

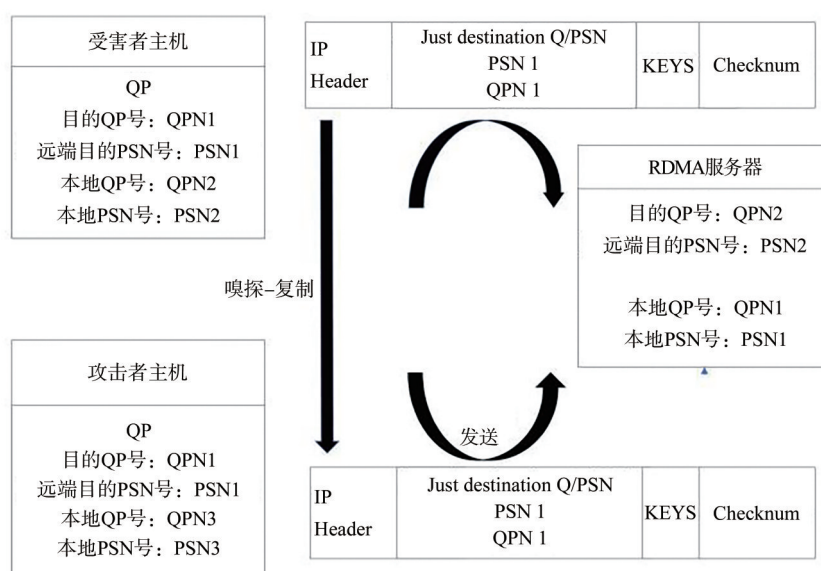


图8 攻击者尝试进行预测从而构造出的有效数据头部

Figure 8 Effective data headers constructed by attackers attempting to make predictions

或修改过。如果攻击者能够预先在使用了 RDMA 应用的目标主机上安装后门, 如一些能够调用 RDMA 应用的木马程序或预加载库, 假设这些后门能够自动开启 RDMA 服务, 那么攻击者就能静默地与受害者主机建立 RDMA 链接并且读取数据。在实验中, Rothenberger 等^[4]实现了一个恶意二进制文件, 能自动在 RNIC 上注册一片尽可能大的内存空间, 并且能够将生成的 rKey 和内存地址发送给攻击者, 恶意程序随后释放这片内存区域, 但是并不向 RNIC 发送注销信息, 因此这片空间仍然是攻击者可以通过 RDMA 操作访问的。由于受害者机器刚知道这块内存已经被释放, 操作系统会回收这片空间将其用于存储其他信息, 此时攻击者就可以通过 RDMA 读操作静默地读取这些信息。

4 相关防护对策说明

目前, 研究界针对第 3 节的攻击方式提出了多种防护手段, 引入的防护措施包括一套加密认证体系协议、随机化 (包括 rKey、PSN、QPN 与连续分配的内存地址) 和杂凑函数与硬件计数器。

多种攻击。RDMA 安全缺陷与其对应的防护措施如图 9 所示。

4.1 加密认证体系

多种攻击方式的发起依据来源于报文中的字段可被敌手预测, 并且可以在不被发现的前提下直接修改, 增加加密和认证模块后能够极大提升敌手实施攻击的难度。然而, RDMA 协议对于其配套的加密体系有特殊的要求, 首先 RDMA 协议需要尽量避免被拖慢原传输速率, 需要对加解密和哈希算法进行硬件实现并且加速, 以更大的空间开销换取时间复杂度的降低。其次在具体加解密模式的选择上, 不可采用报文之间有解密依赖关系的分组加密算法 (如 CBC 模式下的 AES 算法), 若被加密的报文乱序抵达, 由于无法立刻解密并且不能利用对端机器的 CPU, 只能缓存在 RNIC 的有限而且珍贵的空间上, 有可能会造成所有 RDMA 应用程序的性能下降。

对 IB 协议而言, 由于其有独特的报文设计, 实现 IB 协议的加密和认证需要修改或增加其原有结构, 盲目增加安全方案会产生冲突。在实践中, 由于哈希算法的时间开销相对较小, 也可以仅考虑完整性认证保护手段。目前, 已经有比较

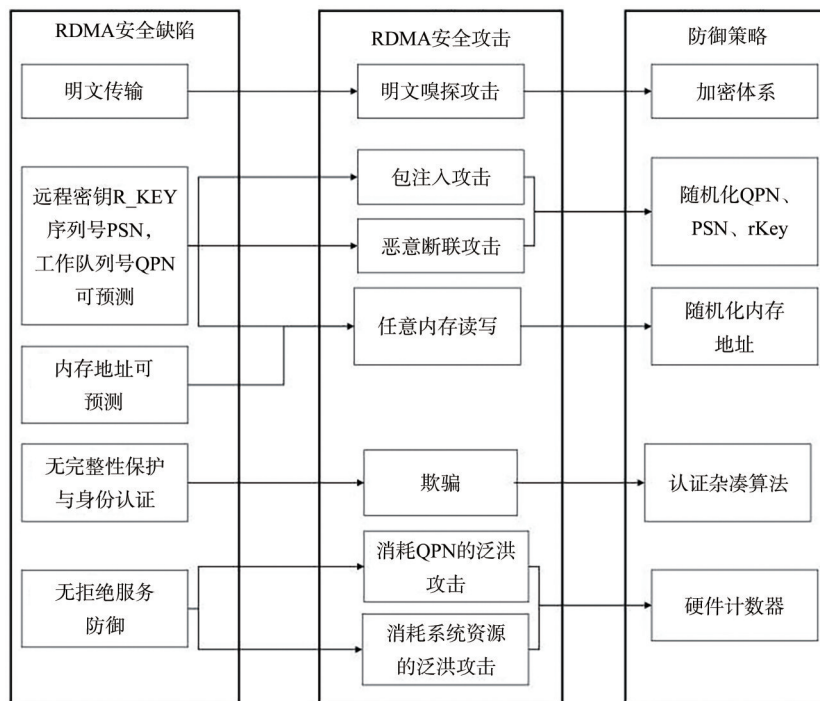


图9 RDMA 安全缺陷与对应的防护措施
Figure 9 RDMA security defects and corresponding protective measures

成熟的 IB 加密认证方案, 如 Lee 等^[12]提出的用 MAC 替换 CRC 字段实现认证功能和 sRDMA^[52]协议。本文主要介绍 sRDMA 协议。

对于 RoCEv2 协议, 由于其可以被视作普通的 UDP 报文, 因此可以复用部分安全方案。目前业界主要有在网络层引入 IPSec 协议^[59]和在应用层采用 TLS1.3 快速版 QUIC 模式^[60]2 种发展思路, 这 2 种方案各有缺陷。基于应用层加密的方法需要 CPU 参与处理, 等待 RDMA 传输完毕后再由 CPU 解密, 这实际上违反了 RDMA 中 CPU 全程不参与的原则。而且, 因为应用层加解密方案无法在网络层即时处理, 系统需要为加密消息提供更大临时缓冲区, 造成了额外的时间和空间消耗。而 IPSec 工作在网络层, 不能识别 RDMA 报头, 因此无法完成源认证。虽然其可以在不影响 RDMA 原有流程的前提下加入, 并不会造成太大的速率损耗, 但是其重要的认证功能无法很好地运行。

4.1.1 引入 sRDMA 加密体系

Taranov 等^[52]提出的 sRDMA 协议提供了 IB 协议的加密体系所需要设置的相关加解密算法、密钥协商方案、哈希算法和密钥存储方案, 这些加密体系需要在 RDMA 握手过程和 RNIC 上实现。sRDMA 协议基于 RC 场景, 引入该体制能够实现数据的机密性和完整性。在详细说明 sRDMA 加密体制之前, 先假设需要进行安全防护的场景描述如下。

(1) 在一个相对隔离的网络环境下, 受害者利用 IB 协议中的 RC 链接, 向同一网络环境下启用了 RDMA 功能的服务器主机发出读写请求。

(2) 敌手同样处于此网络环境中, 可以是另外一个数据库服务器的连接者, 也可以是中间的某个路由器节点或某个远程云服务提供者, 拥有合法进入此网络环境的能力。但是敌手事先并不知道受害者的其他信息。

(3) 敌手能够自由地利用网络嗅探工具抓包, 拥有读取、篡改并且重新注入数据包的能力, 能够分析数据包头部信息。发送数据包的数量和内容不受限制, 能够将数据包发送到正确的目标。

假设需要进行防护实验的场景有以下 3 个

前提。

(1) 与 RNIC 相关的硬件不会受到攻击, 其运算的内容不会被窃取或出错。

(2) 所使用的哈希算法和随机数产生算法是可靠的。

(3) 此网络环境中没有开启任何传统网络安全工具 (如防火墙、IDS 等, 这是合理的, 因为在 RDMA 环境中采用这些手段是无效的, 强行使用会降低 RDMA 的性能优势)。

为便于描述 sRDMA 协议, 引入 sRDMA 协议术语, 如表 2 所示。

表 2 sRDMA 协议术语
Table 2 sRDMA basic concept interpretation

符号	描述
PRF()	随机数生成器
MAC	消息认证码
SM3	国产哈希算法
A, B	终端节点 A, B, 由端口和 QPN 唯一确定
K_{PD}	PD 关联的密钥, 保存 RNIC 保存, 不对外使用
$K_{A,B}$	终端节点 A, B 间使用的对称密钥, 由 K_{PD} 派生
K_{MR}	与 MR 关联的对称密钥, 由 K_{PD} 派生
nonce_{AB}	节点 A, B 通信中产生的一个随机数
	字符串拼接操作

整个加密体系由以下 3 种密钥实现, 对应几种级别的安全措施, 用户可以按照需求选择是否使用这些密钥并与对端协商一致。

(1) K_{PD} (保护域级密钥): PD 是 RDMA 中基本的安全单元, 以每个 PD 记录一个可信的核心密钥 K_{PD} 。 K_{PD} 不直接参与加密, 不对外暴露, PD 创建时由系统创建并且与本 PD 相关联, 存储在 RNIC 中。为了节省 RNIC 中的存储空间, 除了核心密钥 K_{PD} 外, 所有的密钥都在使用前即时计算。

(2) $K_{A,B}$ (会话时使用的对称密钥): $K_{A,B}$ 是 QP 通信时使用的会话密钥, 由 K_{PD} 派生。每次建立链接都派生一个新的会话密钥 $K_{A,B}$ 。 $K_{A,B}$ 不保存在 RNIC 中 (在会话中将暂时缓存)。 $K_{A,B}$ 具体的计算方法是不固定的, 本文给出一种示例, 如式 (1) 所示, 即利用双端的 QP 号与目前网卡的设备编号 NICID 进行派生。

$$K_{A,B} = \text{PRF}_{K_{PD}}(\text{QPN}_A || \text{QPN}_B || \text{NICID}) \quad (1)$$

(3) K_{MR} (内存区域级密钥): 当用户需要对 MR 进行保护时, 利用 rKey 为信任基可以计算出安全性更高的密钥 K_{MR} , 用于增加远端访问时本地内存的安全性。为了节省 RNIC 中 SRAM 资源, K_{MR} 也通过派生计算, 参与派生的元素通常应该与内存区域相关, 这里将 rKey、即将要访问内存的起始地址与中止地址作为派生参数。

$$K_{MR} = \text{PRF}_{K_{PD}}(\text{StarAddr} \parallel \text{EndAddr} \parallel \text{rKey}) \quad (2)$$

为进一步增加安全性, 可以考虑对 K_{MR} 进行再派生。MR 下可以细分成子域或内存窗口, 利用这些细分得到的内存块的地址或编号可以进行更多密钥的派生。

上述 3 种密钥将作为 sRDMA 体系中的安全核心: 安全管理传输头 (security management transport header, SMTH) 的组成部分, 以实现数据源认证和完整性保护。SMTH 头部结构如图 10 所示。SMTH 使用各种密钥、随机数 nonce 和全局路由头 (global routing header, GRH)、基础传输头 (basic transport header, BTH) 为每个数据包计算一个 MAC 值, GRH 指路由头, 包含 IP 地址和 UDP 端口, BTH 包含了目标 QPN。这些数据包头唯一标识了发方和收方的 RNIC 中的特定 QP。

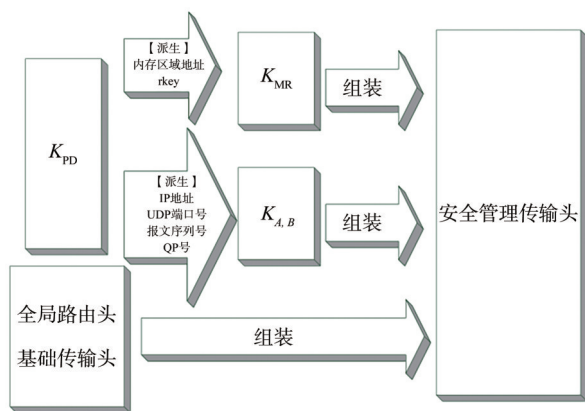


图 10 SMTH 头部结构
Figure 10 SMTH head structure

$$\text{MAC}_{\text{SMTH}} = \text{Hash}(\text{nonce}_{A \rightarrow B} \parallel \text{GRH} \parallel \text{BTH} \parallel K_{A,B} \parallel K_{MR}) \quad (3)$$

为抵御重放攻击, 需要在 SMTH 中加入 nonce, 为了减少传输 nonce 的开销, 可以考虑复用 PSN 的某些比特位, 该方法类似于 TLS1.3 利用数据包序列号作为 nonce。但是由于 PSN 比特

位只有 24 位, 因此 24 位 nonce 并不能很好地抵抗重放攻击。为提高安全性需要再引入 40 位比特构成长度为 64 位的 nonce, 这种更安全的 nonce 扩展是 sRDMA 协议的可选项, 如果不选择采用 SMTH 保护则可以直接复用 PSN 作为 nonce。要穷举 64 位 nonce, 目前是不可行的, 因此从应用安全角度来说, 扩展 64 位的 nonce 能够防止重放攻击, 保证认证用户。

$$\text{nonce}_{A \rightarrow B} = \text{PSN}_{A \rightarrow B} \parallel \text{ExtendBits} \quad (4)$$

sRDMA 体系中对称加密标准一般采用 AES 算法, 采用的对称密钥是 $K_{A,B}$, 在进行握手之前服务器与客户端之前先进行额外的一次建链用于协商。在组织密文并且进行分块发送时有 2 种设计方式: 一是将加密耦合在 RDMA 协议中, 这样的缺点是由于对每个分片都单独地加解密, 传输延迟很高, 而且在某些分组加密的工作模式下每个分组之间的解密可能并不是独立的, 因而接收端可能需要等待其他相关分组抵达后才能开始解密; 二是将加密工作置于传输层之上进行, 在将报文发送出去之前数据已经加密完成。这样的优点是无需修改 RDMA 协议的设计, 发送方只负责发送加密完成的数据块, 因此每轮加密处理的数据块长度可以更长。发送时, 这些密文数据块按照固定大小切分为不同的 segment, 填充至 payload 中, 并且指定每段密文的 segment 号, 接收方即使接收到多个乱序的 segment, 也可以自动按照标号进行整理重组。此方案相较于第 1 种耦合方案更加优秀, 推荐采用方案 2。

在 sRDMA 协议加密体系中, 除了建链数据包外, 每个报文头都需要加入 SMTH 字段。假定通信场景是搭载了 RNIC 的客户机器向 server 机器发送一个远程读取或写入请求, 整体的通信流程如下。

(1) 预备阶段: 服务器 server 收到来自客户端客户的 RDMA 操作请求, 在正式开始通信之前, 双方进行资源筹备, 分配 PD、MR 和 QP, 运算出所需的密钥后建立链接, 本次链接不是 RDMA 操作, 因此利用其他的可证明安全的密钥交换协议 (如 TLS) 交换通信所需的信息, 包括对端的路由头、QP、PSN、rKey 和 $K_{A,B}$ 等。

(2) 建立链接: 客户和 server 双方开始正式

RDMA 建链, 首先, 双方都需要在本地内存与 SmartNIC 之间进行 DMA 操作, 将所有必需的对称密钥等复制到 SmartNIC 中; 然后, RNIC 中通信组件设定完毕的 QP 根据目标信息向 server 发送建链请求, 经过协商后双端开始 RDMA 通信。

(3) 发送请求: 客户的主机通过 DMA 操作向 RNIC 发送一个读写请求包, 客户的 RNIC 通过规定的接口收集这个数据包, 根据 sRDMA 协议进行数据包处理, 利用 SM4 等对称加密算法进行加密, 增加 SMTH 报头后, 将其发送到网络链路上。

(4) 验证报文: sRDMA 报文流程如图 11 所示, 接收方 RNIC 接收报文, 并且确认头部是否合法, 合法的报文将进入 RDMA 报文处理流程, 并且向发送方的 RNIC 发送 ACK。

客户端可以与服务端协商是否需要采用安全性更高的加密方式, 这些解密方式会决定接收方对报文的检验流程, 当接收方收到报文并且检验了路由头、QP 等基础字段的安全性之后, 会依据客户端选择的加密等级进入不同的检验流程: 最后接收方会对解密结果执行另一次杂凑运算, 比对报文中解析得到的 MAC, 以验证解密结果是否正确。

当发送方选择不采用任何加密等级时, 此数据报将和其他普通数据报一样直接放行, 这也意味着采用原始的明文传输, 并且在验证时不产生上下文缓存内容, 这时等效于原生的 RDMA 操

作 (即 UC 链接)。

以上 MAC 操作实现了数据源完整性。当敌手试图发起中间人攻击, 即注入一个伪装成受害者发出的报文时, 假设按照第 3.3 节的攻击方式, 拥有受害者的正确 BGH 并且预测出了 QPN、PSN 和 rKey 等信息, 但是由于他无法拥有第 1 次链接中的 $K_{A,B}$ 密钥 (第 1 次链接是基于非 RDMA 协议的安全密钥协商协议), 也无法得知 server 方 RNIC 上 K_{PD} 的任何信息, 因此, 当此次会话开启了 payload 级别的检测时, 注入的报文缺少 K_{PD} 或 $K_{A,B}$ 相关的信息, 导致 MAC 不一致, 因此会被接收方丢弃。当敌手试图发起重放攻击时, 即抓包后不做 RDMA 相关字段的修改重新将其发送, 由于存在 nonce 和 PSN, 这个重放的包同样会由于 MAC 不正确被丢弃。

以上对称加密流程实现了数据机密性, 整个加密过程的安全性由 K_{PD} 保证, 在 K_{PD} 不会被泄露或被盗取的情况下, 派生出的密钥 $K_{A,B}$ 也是安全的, 对称密钥分发的安全通过 QUIC 协议协商, 而 QUIC 的安全性已经得到了认可, 因此可以认为用户被分发的密钥 $K_{A,B}$ 也是安全的。

4.1.2 引入 IPSec 加密

IPSec 是用于提供对 IP 层数据包的安全性和认证的一组协议和算法, 能够保护网络通信的机密性、完整性和身份验证, IPSec 可用于建立虚拟专用网络 (virtual private network, VPN) 链接、远程访问和安全的站点到站点通信。虽然 IPSec

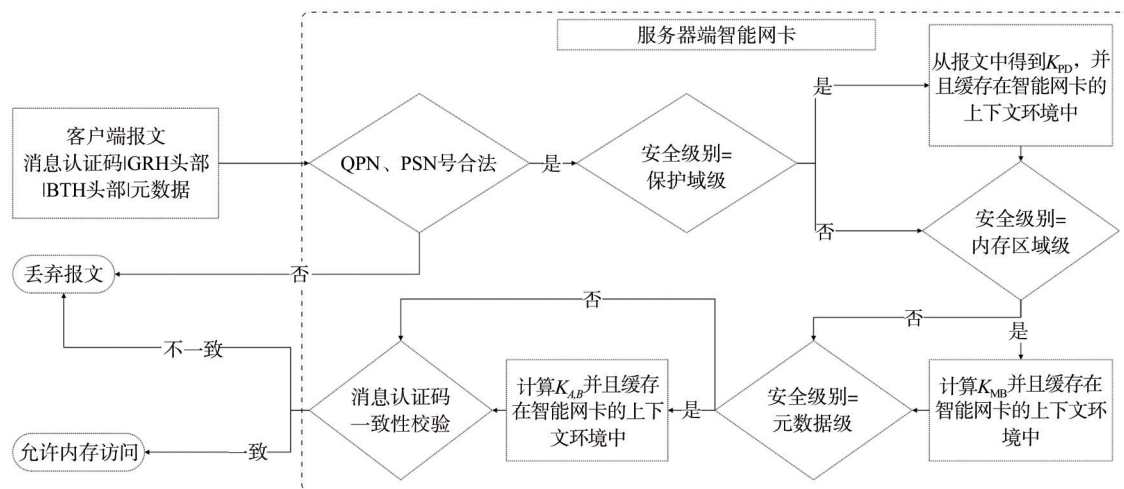


图 11 sRDMA 报文流程
Figure 11 sRDMA message verification process

不直接支持 RDMA 流量,但是由于 RoCEv2 报文兼容了 TCP/IP 的底层结构,IPSec 能忽视 RDMA 流量的差异,直接在网络层提供加密和认证服务,不会对 RDMA 原有工作流程和传输效率产生显著影响。

IPSec 的主要功能包括加密、认证和完整性保护,通过在站点之间传输 IP 数据包的过程增加安全组件、应用加密算法来实现这些功能^[47],主要用到的是 IPSec 的封装安全载(encapsulating security payload, ESP)。ESP 提供数据包的加密性、完整性和可选的身份验证,会对整个 IP 数据包进行封装,包括源地址和目标地址,而且会添加加密和完整性校验码,并可选地进行身份验证。在数据传输过程中,源地址和目标地址被加密,从而保证了数据的机密性和匿名性,适用于对数据保密性要求较高的场景。对于 RoCEv2 协议,IPSec 可以通过 IP 地址和 UDP 端口对流量进行认证,引入 IPSec 后的 RDMA 报文结构如图 12 所示。

虽然 IPSec 的保护是基于 IP 的,而具体需要保护的对象 QP 却工作在传输层,RoCEv2 实际上等效于增加了 BTH 的 UDP 报文,硬件网卡在发送或接收数据包之前就可以解析出目的 QP 或源 QP,可以利用 QP 的对应关系引入 IPSec 协议。Menachem 等^[61]提出,可以复用 Linux 中已经具备了 IPSec 的相关组件——Linux 变换框架(transform framework, XFRM)^[62]和因特网密钥交换

(Internet key exchange, IKE) 协议^[63],给出了在 RoCEv2 配置 IPSec 的 2 种实现方式,分别是将 IKE 协议卸载到网卡上和为每个 QP 单独设定 IPSec 套接字。

在性能上,将 IPSec 操作卸载到硬件上可以显著降低 IPSec 的计算开销^[64]。2020 年, Mellanox 公司推出的 ConnectX-6 Dx 通道适配器是同类产品第 1 个为以太网和 RoCEv2 提供完全 IPSec 加速的片上系统。

4.2 随机化

由于众多针对 RDMA 特点攻击的前提是攻击者能够正确预测出 RDMA 报文中的重要字段,包括 rKey、QPN、PSN 和内存地址,因此只需要保证这些字段的安全性就能避免很多种类的攻击。相较于引入加密体系而言,随机化是一种更加轻量级的安全防护方案,有速率和实现难度上的优势。引入随机化方案后,攻击者虽然仍然能够实施相应的攻击,但是其预测成功的概率大幅下降,付出的时间和算力成本也将增多。虽然随机化方案对其他字段部分没有进行防护,但其仍能够作为加密体系的替代方案。

QPN 的随机化可以通过引入序列号池和伪随机函数来实现, Rothenberger 等^[4]指出,虽然一些 RNIC 产生 QPN 的方式是线性的,但是可以通过预先生成一些 QPN 放入 QPN 池中,引入伪随机函数来随机选择一个 QPN 进行 RDMA 链接,考虑枚举空间的大小为 2^{24} ,这能够大幅增加敌

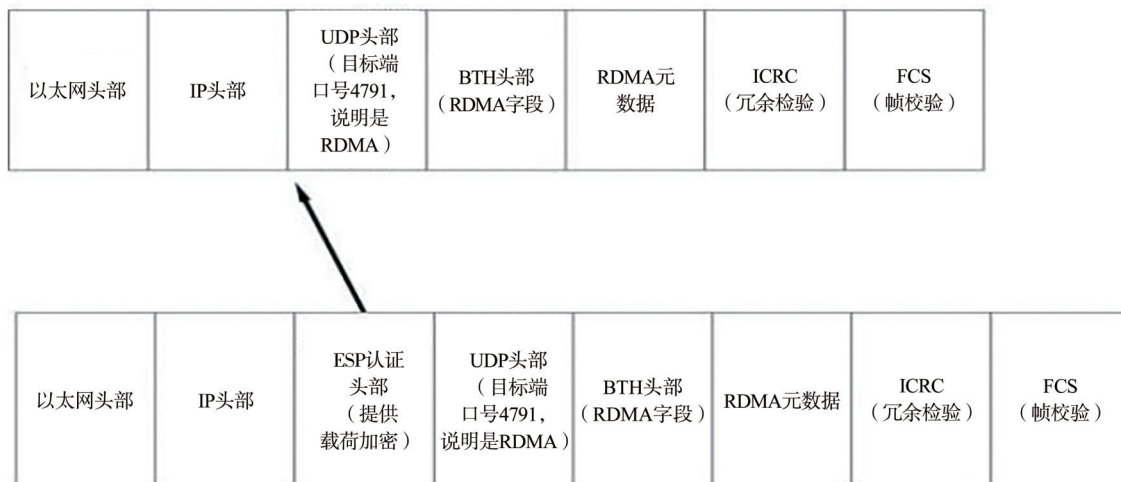


图 12 引入 IPSec 后的 RDMA 报文结构
Figure 12 RDMA message structure after introducing IPSec

手线性猜测 QPN 的难度。

在提高 PSN 安全性方面, 在第 1.3.7 节的 RNIC 采用静态 PSN 号作为链接起始序列号, 所以每个 QP 链接都应该使用随机启动的 PSN 进行初始化。然而, Rothenberger 等^[4]指出, 由于 PSN 保持线性增长的特点, 随机化初始 PSN 对于防御 PSN 枚举攻击帮助甚微, 抵御 PSN 猜测的重点在于同时提高 QPN 和 PSN 的随机化程度。在两者共同初始随机化情况下, 敌手的枚举空间将扩大许多, 在有限时间内很难通过枚举进行数据包注入攻击。根据 Rothenberger 等^[4]进行了一次面向全部 QP 的攻击实验, 不加区分地对所有可能的 QP 链接发起基于暴力枚举的断联攻击, 如果 QPN 是随机生成的, 受害者机器上同时打开的链接数是 n , 那么攻击者平均需要探测大约 $2^{24}-n$ 个 QPN 才能找到正确的结果, 付出的时间成本会变得巨大。例如, 如果受害者打开了 1 024 个打开的 QP, 如果攻击者已知 QPN, 那么攻击工具大约 10 s 就能预测正确的 PSN 号, 以断开链接, 但是引入 QPN 随机化后, 攻击工具平均每 48 h 只能断开一个链接, 攻击性能会很明显地下降。

内存地址的安全性同样可以通过引入变量池与随机算法来保障。对于虚拟地址的保护, 可以对报文中的虚拟地址 (virtual address, VA) 字段进行一次转换, 即对实际物理地址进行双重虚拟化或修改原有的内存分配机制, 不再为连续的 QP 申请分配邻近的地址。

远端内存钥匙的保护可仿照 QPN 的随机化方案, 引入重新混淆机制和密钥池, 避免敌手按照数学规律预测。考虑 rKey 与内存地址存在关联, Rothenberger 等^[4]指出, 应用程序可以预先生成不同的 rKey 注册区域并且共同加入一个内存区域池中, 当需要注册新区域时, 应用程序会得到一个随机的内存地址描述符, 并且从内存池中选择一个随机内存, 将此内存地址描述符映射到随机内存上, 就能同时减少 rKey 和内存地址同时泄露的问题。

4.3 杂凑算法

杂凑算法又称哈希算法, 能够将任意长度的数据串转化为同样长度但不同的消息摘要, 用于

检测报文的完整性是否被破坏。

杂凑算法能够保护 IB 和 RoCE 头部安全, 防护中间人攻击。当攻击者截获报文进行报文头篡改并且重新发送时, 接收端收到报文后会以同样的过程计算一次 MAC, 并且与报文携带的原系统 MAC 进行比较, 如果存在差异, 证明报文已被篡改或者发送错误, 接收方会丢弃此报文, 攻击失效。

由于每次 RDMA 报文的收发过程都需要应用杂凑算法, 因此需要进行相关的算法步骤优化或硬件加速以提升速率。在未来的防护方案研究开发中, 预计将基于 SM3 算法进行硬件加速, 通过增加和复用寄存器降低硬件运算的轮数。

4.4 硬件计数器

硬件计数器用于防御和追踪拒绝服务攻击^[4], 在硬件层面上进行攻击的溯源和保护。具体来说, 可以在 RNIC 上搭载一个硬件计数器, 用于记录一段时间内各自不正常的 RDMA 链接数量, 包括无效请求和导致访问的错误请求, 大量此类不正常的流量可能来自敌手的自动请求脚本; 硬件计数器还能设置负载阈值, 实时检测目前的链接数量和总流量, 当链接即将超过负载能力时就限制最大链接数量。目前 Mellanox 公司出产的基于 mlx5 驱动的新一代 RNIC 内置了多种不同功能的硬件计数器^[6], 如访问错误链接计数器 resp_mote_access_errors 可用于监视导致访问错误的无效请求。

除了被用于防护外, 计数器也可以作为防止攻击发生的硬件约束, Rothenberger 等^[4]指出, 支持 RDMA 的设备应该限制本机并发的链接数量, 以防止攻击者同时建立大量的链接进行消耗系统资源的攻击, 限制的依据可以是 RoCEv2 协议中的 IP 地址或 IB 协议中的端点号, 此时攻击者若想成功实施攻击需要控制大量的主机。

4.5 防护方案对比

上面提出的 4 种防护方案都在一定程度上解决了 RDMA 的一些安全痛点, 但其适用场景和实际防护效果都有所差异, 需要根据情况灵活引入。目前来看尚不存在一种安全性与性能优势均表现突出的通用方案, RDMA 各防护技术对比如表 3 所示。

表3 RDMA各防护技术对比
Table 3 RDMA comparison table of protection technologies

防护技术	安全能力	性能影响	引入成本	适用场景
sRDMA	加密完整性保护抗拒绝服务身份认证	大	较大,需要RNIC	需要充分防护,能够接受性能代价的高安全需求场景
IPSec	加密完整性保护	大	一般	无须身份认证的场景,作为一种普遍防护手段引入
随机化	核心字段保护	小	小	需要关注欺骗、拒绝服务的场景,安全要求低,但对性能要求较高
杂凑函数	完整性保护	大	小	需要身份认证的场景,并且接受性能损失
硬件计数器	抗拒绝服务	小	一般,需要RNIC	需要关注拒绝服务攻击的场景

5 结束语

5.1 成果

RDMA作为依赖特殊硬件且能有效提升网络交换速率的下一代技术,已经在大型远程数据存取领域被大量投入,如NVMe over Fabric等,在数据计算、人工智能模型训练等领域的使用也是可预见的。但由于其使用范围的局限,RDMA的安全性长期没有得到重视。由于涉及内存操作并且缺少对端监视机制,一旦RDMA被暴露在有安全风险的环境内,RDMA的攻击会造成很严重的后果。为解决以上问题,本文主要贡献如下。

(1) 论述了安全RDMA体系的设计理念。本文从基础的数据安全特性入手,明确了一个通信模型的基础安全需求,明确RDMA安全系统需要保证的安全方向。

(2) 全面调研了RDMA协议需要面临的安全威胁。本文通过分析常见通信协议的安全漏洞,并且结合RDMA自身的软硬件特点,分析了以RoCE协议为例的RDMA协议的安全脆弱性。

(3) 总结了RDMA协议可能遇到的安全攻击。以RoCE协议为例,结合RDMA的安全威胁,提出了针对RoCE协议的各种安全攻击。

(4) 分析了近年来国内外在RDMA安全领域的相关理论研究和实验,整理了应对各种RDMA安全攻击的已被证实可靠的防护手段。

(5) 设计了在满足安全需求的基础上能够应对各种RDMA安全攻击的防护体系,并论证了其有效性和可行性。

未来,随着DPU等专业数据处理芯片的普及,RDMA技术的前景也十分广阔。本文梳理了RDMA安全的基础知识、面临的实际问题和可靠

的解决方向,为其他RDMA安全性的研究和技术开发提供了前进方向和指引思路,提出了可拓展性强、实现难度低的解决方案。

5.2 局限性及未来展望

本节旨在说明目前国内外RDMA安全防护方案的缺陷和RDMA攻击手段的发展方向。在安全方案领域,尚且存在以下不足。

(1) RDMA安全体系并不完备。目前提出的RDMA安全防护方案(如sRDMA和IPSec)都有其缺陷。sRDMA协议的密钥协商方案无法保证通信双方的前向安全性,遭受攻击后之前的通信记录将被泄露;IPSec无法对更高层的RDMA流量做定向的识别和保护。

(2) 安全方案代价过高。在空间上,引入sRDMA协议后每个数据包需要额外携带最多64 bit的头部;引入IPsec,则更多。这些额外的负载均由RNIC承担。考虑RNIC上还需要预留空间以实现加密算法和传输数据,这实际上限制了RNIC可同时支持并发链接的数量和流量大小。

(3) 缺少具体实验数据支撑。本文所述的加密方案大多基于软件模拟实现,在实验中得到的结论能否用于实际的工业生产尚未明确。在实际工程应用中,主要还是搭载FPGA的硬件网卡。将加密等方案运用到硬件平台上,需要重新评估加密方案的性能损失以及受限的可用硬件轮数。虽然目前利用FPGA实现RDMA存取的案例已经有很多(如NVme-oF),但方案能否适配修改完善后的RDMA协议仍然存疑,需要进行广泛实验和评估后续方案的可行性。

在攻击手段上,对于RDMA的攻击方案逐渐偏重于与底层硬件特性相结合。由于RDMA本身是与硬件强关联的技术,从底层总结出的安

全缺陷实际上更难防御。如攻击者通过观测底层网卡的密钥产生规律,可以进行报文注入攻击,通过收集网卡 Cache 命中与否的返回时间差异可建立侧信道。这些攻击方式都是从网卡的底层结构出发,很难防御。此外, RDMA 攻击方案广泛应用于上层的 RDMA 应用(如 NVMeof、HERD 等),由于设计缺陷,即使引入了上述安全方案,也无法保证它们的安全性。

在防护手段的发展上,大量实验表明, RDMA 的安全性和高效率是可兼容的。RDMA 安全防护技术正朝着软硬结合、体系化、轻量级化的方向发展。

(1) 软件实现转向可编程网络设备。随着可编程硬件技术的发展,经过硬件加速后为 RDMA 搭载已经成熟的协议防护方案不再会造成不可容忍的性能丢失,因此目前以及未来大部分的 RDMA 安全研究都会逐渐采用网卡卸载技术;而且, RNIC 厂商也正进行与网卡加速适配的独特设计改进。可以预见的是,将来使用基于 RNIC 的身份验证和加密可以为需要高性能保证(如 RDMA 机制)的系统提供高效且安全的通信。

(2) 安全防护体系化。在 RDMA 的漏洞被充分挖掘后,研究界已经从针对单个漏洞进行研究,逐步转为提出或引入一套安全防护体系以解决 RDMA 的安全,其中 sRDMA 提供了强大的认证和保密功能, IPsec 提供了较底层的加密和完整性保护, Mellanox 等协议开发供应商也为 IB 协议引入了一套安全方案。在 RDMA 应用逐渐推广的背景下,相信未来会出现更多通用的 RDMA 安全体系方案设计。

(3) RDMA 安全协议轻量化。一些 RDMA 安全学者都指出了目前安全方案略显冗余的缺陷,过多地牺牲性能对于 RDMA 而言,并不是一个好选择。已有学者提出引入一个完整的安全体系并不适用于所有场景,亟须对这些 RDMA 方案进行内部解耦并且增加轻量级替代,增加 RDMA 安全方案的灵活性势在必行。

5.3 未来工作计划

本文旨在整理目前国内外 RDMA 安全防护领域的研究进展,在此基础上,下一步研究工作和未来工作方向如下。

(1) 为 sRDMA 增加更多安全可选项。随着 RDMA 技术被应用在“东数西算”等国家重点项目中,在事关国民数据安全的重要领域出现了国产化的需求。目前,对国产加密算法 SM4 系列进行硬件加速的研究已有起步^[66],然而 sRDMA 协议可支持的加密算法与哈希算法还很少,考虑不同安全选项适用的场合不尽相同,未来计划将为 sRDMA 协议加入包括 SM 系列在内的更多套件,以提升其可拓展性。

(2) 实现安全方案的轻量化开发。sRDMA 和 IPsec 协议在实现上均高度耦合,加之目前工作中以 Openssl 库为载体进行开发,导致整体的框架有较多冗余。实际上,部分功能完全可被更轻量级的随机化、计数器等方案取代,计划在未来的工作中将 sRDMA 的核心加密功能剥离,提供易于部署的轻量级 RDMA 安全传输框架。

(3) 进行更多的实验数据验证。目前,部分的攻击方案以及防护手段停留在理论分析或实验阶段,缺少验证防护能力必需的数据支持。未来计划进行攻击方案的更多实验及防护效果评估,包括采用不同加密算法的效率损失、攻击成功的期望次数和时间等。

参考文献:

- [1] AGUILERA M K, AMIT N, CALCIU I, et al. A abstraction for remote memory[C]//Proceedings of the USENIX Conference, Usenix Annual Technical Conference. Boston: USENIX Association, 2018: 775-787.
- [2] 夏亮. 基于 RoCE 协议的网络传输技术研究[D]. 北京: 北京邮电大学, 2023.
XIA L. Research and implementation of network transmission technology based on RoCE protocol[D]. Beijing: Beijing University of Posts and Telecommunications, 2023.
- [3] SIMPSON A K, SZEKERES A, NELSON J, et al. Securing RDMA for high-performance datacenter storage systems[J]. HotCloud, 2020: 1-8.
- [4] ROTHENBERGER B, TARANOV K, PERRIG A, et al. ReD-Mark: bypassing RDMA security mechanisms[J]. USENIX Security Symposium, 2021: 4277-4292.
- [5] TSAI S Y. Building fast, scalable, low-cost, and safe RDMA systems in datacenters[D]. West Lafayette: Purdue University, 2019.
- [6] 刘建伟, 王育民. 网络安全: 技术与实践[M]. 第3版. 北京: 清华大学出版社, 2017.
- [7] LIU J W, WANG Y M. Network security: technology and practice[M]. 3rd Edition. Beijing: Tsinghua University Press, 2017.
- [7] GLÄVAN D. Sniffing attacks on computer networks[J]. Scien-

- tific Bulletin of Naval Academy, 2020, XXIII(1): 202-207.
- [8] JOSHI M, HADI T H. A review of network traffic analysis and prediction techniques[EB]. arXiv preprint, arXiv: 1507.05722. 2015.
 - [9] HENINGER N, DURUMERIC Z, WUSTROW E, et al. Mining your Ps and Qs: detection of widespread weak keys in network devices[C]//Proceedings of the 21st USENIX conference on Security symposium. New York: ACM Press, 2012: 35.
 - [10] 赵景, 王澍. 基于 Internet 的 TCP 会话劫持欺骗攻击与防御策略[J]. 现代电子技术, 2020, 43(16): 122-125.
ZHAO J, WANG S K. TCP session hijacking spoofing attack and defense strategy based on Internet[J]. Modern Electronics Technique, 2020, 43(16): 122-125.
 - [11] DIETRICH S, LONG N, DITTRICH D. Analyzing distributed denial of service tools: the shaft case[C]//Proceedings of the 14th USENIX conference on System administration. New York: ACM press, 2000: 329-340.
 - [12] LEE M, KIM E J, LEE C W. A source identification scheme against DDoS attacks in cluster interconnects[C]//Proceedings of the Proceedings of the 2004 International Conference on Parallel Processing Workshops. New York: ACM press, 2004: 354-361.
 - [13] MESSADI I, NEUMANN S, ALMSTEDT L, et al. A fast and secure key-value service using hardware enclaves[C]//Proceedings of the 20th International Middleware Conference Demos and Posters. New York: ACM Press, 2019: 1-2.
 - [14] MIHIR B, PHILLIP R. Optimal asymmetric encryption[C]//Proceedings of the Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques. Perugia: Springer Berlin Heidelberg, 1994: 92-111.
 - [15] MARK L, SEAN S. Improving DES Coprocessor Throughput for Short Operations[C]//Proceedings of the 10th USENIX Security Symposium (USENIX Security 01). Berkeley: USENIX Association, 2001: 67-84.
 - [16] WANG X Z, WANG S, LI D. sRDMA: a general and low-overhead scheduler for RDMA[C]//Proceedings of the 7th Asia-Pacific Workshop on Networking. Hong Kong: Association for Computing Machinery Press, 2023: 21-27.
 - [17] MANSOUR W, JANVIER N, FAJARDO P. FPGA implementation of RDMA-based data acquisition system over 100-Gb Ethernet[J]. IEEE Transactions on Nuclear Science, 2019, 66(7): 1138-1143.
 - [18] RASHTI M J, SABIN G, KETTIMUTHU R. Long-haul secure data transfer using hardware-assisted GridFTP[J]. Future Generation Computer Systems, 2016, 56: 265-276.
 - [19] KIM D, LEE S, PARK K. A case for SmartNIC-accelerated private communication[C]//Proceedings of the 4th Asia-Pacific Workshop on Networking. New York: ACM press, 2020.
 - [20] 廖湘科, 肖依. 新型高性能计算系统与技术[J]. 中国科学: 信息科学, 2016, 46(9): 1175-1210.
LIAO X K, XIAO N. Emerging high-performance computing systems and technology[J]. Scientia Sinica (Informationis), 2016, 46(9): 1175-1210.
 - [21] 梁戈. 基于 RDMA 的分布式数据库内存存储系统[D]. 成都: 电子科技大学, 2020.
 - LIANG G. RDMA-based distributed database memory storage system[D]. Chengdu: University of Electronic Science and Technology of China, 2020.
 - [22] KALIA A, KAMINSKY M, ANDERSEN D G. Design guidelines for high performance RDMA systems[C]//Proceeding of 2016 USENIX Annual Technical Conference (USENIX ATC 16). Denver: USENIX Association, 2016: 437-450.
 - [23] GUO C X, WU H T, DENG Z, et al. RDMA over commodity Ethernet at scale[C]//Proceedings of the 2016 ACM SIGCOMM Conference. New York: ACM press. 2016: 202-215.
 - [24] MACARYHUR P, Russell R D. A performance study to guide RDMA programming decisions[C]//Proceedings of the 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems. Liverpool: IEEE Press, 2012: 778-785.
 - [25] YAN D Y, LIU Y P, ZHANG S, et al. A survey of RoCEv2 congestion control[C]//International Conference on Information Science, Communication and Computing. Singapore: Springer, 2024: 42-56.
 - [26] GRANT R E, RASHTI M J, AFSABI A, et al. RDMA capable iWARP over datagrams[C]//Proceedings of the 2011 IEEE International Parallel & Distributed Processing Symposium. Piscataway: IEEE Press, 2011: 628-639.
 - [27] MA S, MA T, CHEN K, et al. A survey of storage systems in the RDMA Era[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, 33(12): 4395-4409.
 - [28] STEVENS W R, FENNER B. UNIX 网络编程[M]. 北京: 机械工业出版社, 2004.
STEVENS W R, FENNER B. UNIX network programming[M]. Beijing: China Machine Press, 2004.
 - [29] MAMBRETTI A, SANDULESCU A, SORNIOTTI A, et al. Bypassing memory safety mechanisms through speculative control flow hijacks[C]//Proceedings of the 2021 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2021: 633-649.
 - [30] MIAO R, ZHU L J, MA S, et al. From luna to solar: the evolutions of the compute-to-storage networks in Alibaba cloud[C]//Proceedings of the ACM SIGCOMM 2022 Conference. New York: ACM press, 2022: 753-766.
 - [31] LU X Y, SHANKAR D, SHI H Y, et al. Spark-uDAPL: cost-saving big data analytics on microsoft azure cloud with RDMA networks[C]//Proceedings of the 2018 IEEE International Conference on Big Data. Piscataway: IEEE Press, 2018: 321-326.
 - [32] POPA R A, LORCH J R, MOLNAR D, et al. Enabling security in cloud storage SLAs with CloudProof[C]//Proceedings of the 2011 USENIX Conference on USENIX Annual Technical Conference. New York: ACM press, 2011: 31.
 - [33] TSAI S Y, PAYER M, ZHANG Y. Pythia: remote oracles for the masses[C]//Proceedings of the 28th USENIX Security Symposium (USENIX Security 19). Santa Clara: USENIX Association, 2019: 693-710.

- [34] DRAGOJEVIĆ A, NARAYANAN D, HODSON O, et al. FaRM: fast remote memory[C]//Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation. New York: ACM press, 2014: 401-414.
- [35] TSAI S Y, ZHANG Y Y. LITE kernel RDMA support for datacenter applications[C]//Proceedings of the 26th Symposium on Operating Systems Principles. New York: ACM Press, 2017: 306-324.
- [36] KALIA A, KAMINSKY M, ANDERSEN D G. Using RDMA efficiently for key-value services[J]. ACM SIGCOMM Computer Communication Review, 2015, 44(4): 295-306.
- [37] LU Y Y, SHU J, CHEN Y M, et al. Octopus: an RDMA-enabled distributed persistent memory file system[J]. ACM Trans Storage, 2017, 17(19): 1-19.
- [38] TSAI S Y, ZHANG Y. A double-edged sword: security threats and opportunities in one-sided network communication[C]//Proceedings of the 11th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 19). Renton: USENIX Association, 2019.
- [39] TSAI S Y, ZHANG Y Y. A double-edged sword: security threats and opportunities in one-sided network communication[EB]. arXiv preprint, arXiv: 1903.09355.2019.
- [40] GRUSS D, MAURICE C, MANGARD S. Rowhammer.js: a remote software-induced fault attack in JavaScript[C]//Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Cham: Springer, 2016: 300-321.
- [41] VANO-GARCIA F, MARCO-GISBERT H. KASLR-MT: kernel address space layout randomization for multi-tenant cloud systems[J]. Journal of Parallel and Distributed Computing, 2020, 137: 77-90.
- [42] IYER V, KANITKAR A, DASGUPTA P, et al. Preventing overflow attacks by memory randomization[C]//Proceedings of the 2010 IEEE 21st International Symposium on Software Reliability Engineering. Piscataway: IEEE Press, 2010: 339-347.
- [43] ROMANOW A, TALPEY T, BAILEY S. Remote direct memory access (RDMA) over IP problem statement: RFC4297[S]. 2005: 2-14.
- [44] JOY PERSIAL G, PRABHU M, SHANMUGALAKSHMI R. Side channel attack-survey[J]. International Journal of Advanced Scientific Research Review, 2011, 1(4): 54-57.
- [45] KHAN M, SWAROOP G. Analysis of row hammer attack on sttram[C]//Proceedings of the IEEE 36th International Conference on Computer Design (ICCD). Orlando: IEEE Press, 2018: 75-82.
- [46] 李永康. 基于 RDMA 的虚拟化安全网关系统设计与实现[D]. 深圳: 中国科学院大学, 2022.
- LI Y K. Design and implementation of an RDMA-based virtualized security gateway system[D]. Shenzhen: Chinese Academy of Sciences, 2022.
- [47] NAGANAND D, DAN H. IPsec: the new security standard for the Internet, intranets, and virtual private networks[M]. Englewood Cliffs: Prentice Hall Professional, 2003.
- [48] LEE M, KIM E. J., YOUSIF M. Security enhancement in InfiniBand architecture[C]//Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium. Denver: IEEE Press, 2005:10.
- [49] PINKERTON J, DELEGANES E. Direct data placement protocol (DDP)/remote direct memory access protocol (RDMA) security: RFC5042[S]. 2007: 4-49.
- [50] LEE M, KIM E. J. A comprehensive framework for enhancing security in InfiniBand architecture[J]. IEEE Transactions on Parallel and Distributed Systems, 2007, 18(10): 1393-1406.
- [51] NORONHA R, CHAI L, TALPEY T, et al. Designing NFS with RDMA for security, performance and scalability[C]//Proceedings of the 2007 International Conference on Parallel Processing (ICPP 2007). Piscataway: IEEE Press, 2007: 49.
- [52] TARANOV K, ROTHENBERGER B, PERRIG A, et al. sRDMA: efficient NIC-based authentication and encryption for remote direct memory access[C]//Proceedings of the 2020 USENIX Conference on Usenix Annual Technical Conference. New York: ACM press, 2020: 691-704.
- [53] POKE M, HOEFLE T. DARE: high-performance state machine replication on RDMA networks[C]//Proceedings of the 24th International Symposium on High-Performance Parallel and Distributed Computing. New York: ACM Press, 2015: 107-118.
- [54] STUEDI P, TRIVEDI A, PFEFFERLE J, STOICA R, et al. Crail: a high-performance I/O architecture for distributed data processing[J]. IEEE Data Eng Bull, 2017, 40: 38-49.
- [55] DIAMOND N B. Securing infiniband networks with end-point encryption[D]. Dayton: Air Force Institute of Technology, 2022.
- [56] TARANOV K, ROTHENBERGER B, DE SENSI D, et al. NeVerMore: exploiting RDMA mistakes in NVMe-oF storage applications[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM press, 2022.
- [57] 朱佳平, 李琼, 宋振龙, 等. NVMeoF 网络存储协议及硬件卸载技术研究[C]//第22届计算机工程与工艺年会暨第8届微处理器技术论坛论文集. 长沙: 中南大学出版社, 2018: 24-33.
- ZHU J P, LI Q, SONG Z L, et al. Research on NVMeoF network storage protocol and hardware offloading techniques[C]//Proceedings of the 22nd Annual Conference on Computer Engineering and Technology and the 8th Microprocessor Technology Forum. Changsha: Central South University Press, 2018: 24-33.
- [58] QIAN Z Y, MAO Z M, XIE Y. Collaborative TCP sequence number inference attack: how to crack sequence number under a second[C]//Proceedings of the 2012 ACM conference on Computer and communications security. Raleigh: ACM Press, 2012: 593-604.
- [59] ALSHAMSI A, SAITO T. A technical comparison of IPsec and SSL[C]//Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers). Piscataway: IEEE Press, 2005: 395-398.
- [60] CHEN S, JERO S, JAGIELSKI M, et al. Secure communication channel establishment: TLS 1.3 (over TCP fast open) versus QUIC[J]. Journal of Cryptology. 2021, 34(3): 26.
- [61] MENACHEM A, LISS L, PISMENNY B. Offloading communication security operations to a network interface controller

[P]. US10958627, 2021.

- [62] 阚闯, 栾新, 戚玮玮. 基于 Linux 的 XFRM 框架下 IPSec VPN 的研究[J]. 计算机工程, 2008, 34(20): 109-111.

KAN C, LUAN X, QI W W. Research on IPSec VPN under XFRM framework based on Linux[J]. Computer Engineering, 2008, 34(20): 109-111.

- [63] HARKINS D, DAVE C. The internet key exchange (IKE): RFC2409[S]. 1998: 2-41.

- [64] AGRAWAL H, DUTTA Y, MALIK S. Performance analysis of offloading IPsec processing to hardware based accelerators[C]// Proceedings of the 2012 International Symposium on Electronic System Design (ISED). Piscataway: IEEE Press, 2012: 291-294.

- [65] KONG X, CHEN J, BAI W, et al. Understanding RDMA microarchitecture resources for performance isolation[C]// Proceedings of the 20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23). Boston: USENIX Association, 2023: 31-48.

- [66] 黄沛昱, 宋佳波, 贾洋凡. 基于 FPGA 的高速国密 SM4 光纤通信系统方案[J]. 网络与信息安全学报, 2023, 9(6): 46-55.

HUANG P Y, SONG J B, JIA Y F. High speed national secret SM4 optical fiber communication system scheme based on FPGA[J]. Chinese Journal of Network and Information Security, 2023, 9(6): 46-55.

[作者简介]



刘雨蒙 (1998-), 男, 湖北武汉人, 华中科技大学硕士生, 主要研究方向为工业互联网安全。



唐正梁 (1998-), 男, 贵州遵义人, 华中科技大学硕士生, 主要研究方向为工业互联网安全。



路松峰 (1968-), 男, 河南巩义人, 华中科技大学教授、博士生导师, 主要研究方向为密码学、区块链及其应用、工业互联网及其安全。



朱建新 (1966-), 男, 浙江临海人, 华中科技大学副教授、硕士生导师, 主要研究方向为工业互联网安全。



刘运渠 (1972-), 男, 贵州遵义人, 江苏为是科技有限公司首席架构师, 主要研究方向为先进网络计算、网络数据安全、非对称光网络、广播与一致性和网络智能计算。