带外脆弱性

徐文渊　　冀晓宇　　闫　琛
浙江大学

中文名: 带外脆弱性

英文名: Out-of-Band Vulnerability

简　称: OOB Vulnerability

学　科: 网络空间安全

定　义: 带外脆弱性是指信息系统软硬件功能因“信号—信息”的理想映射与实际映射不一致而产生、可能造成严重危害的新型缺陷。

背景与动机

“脆弱性”(vulnerability)俗称漏洞,通常定义为一种在信息系统设计、实现、配置中因疏忽形成的、可导致系统安全策略遭受破坏的缺陷[1]。脆弱性是信息系统面临安全风险的主要原因,现有安全研究致力于发现、分析和解决各类信息系统的脆弱性,从而避免利用其进行攻击,造成安全危害。

传统脆弱性大部分涉及信息系统的功能缺陷。例如,软件设计中未对用户输入进行格式、类型与取值范围校验的缺陷可能导致结构化查询语言(structured query language, SQL)注入、跨站脚本(XSS)等攻击;硬件设计上调试接口保留或保护不当的缺陷可能造成未授权的访问和控制。因此,**信息安全领域通常根据安全缺陷所涉及的功能主体对脆弱性进行分类描述,如软件脆弱性、硬件脆弱性、算法脆弱性、协议脆弱性等**。不同类型的脆弱性又可根据其所涉及的细分功能进一步划分,例如通用缺陷枚举(common weakness enumeration, CWE)[2]将软件脆弱性分为认证错误、授权错误、密钥管理错误、数据处理错误、信息管理错误等 40 子类 399 种。这种基于功能划分的脆弱性语言体系很好地对应了系统设计开发的理想功能,体现了功能主体与安全缺陷一体的系统安全思路,为系统架构师、开发人员和安全人员提供了统一的视角,简化了脆弱性定位、分析和修复的协作流程。

随着传统行业的数字化发展,数字世界和物理世界逐渐融合,以传统计算机为主的信息系统正逐渐向智能终端、物联网设备、无人系统等“信息物理系统”演变,脆弱性的形式和内涵也随之变化,超出了传统脆弱性语言体系的覆盖维度。**特别是近年来的研究发现了一系列新型脆弱性,大量产生于信息系统在物理世界和数字世界间的“信号—信息”映射转换过程中,难以简单归咎于因疏忽形成的功能缺陷**。例如,Rowhammer 攻击[3]发现并利用了一种内存脆弱性,攻击者通过软件层高频访问内存硬件中相邻的行,可引起未访问过的目标行数据发生位翻转(bit flip),其原理就是在软件可控条件下触发利用动态随机存取存储器(dynamic random access memory, DRAM)硬件固有的行间电磁干扰特性。从理想功能的视角,该脆弱性涉及的 DRAM 硬件在内存数据读写层面并无缺陷,也满足在理想内存读写工况和物理环境下的数据可靠存储功能要求。再如,海豚音攻击[4]发现并利用了一种麦克风脆弱性,攻击者通过发射无声的调制超声波可以使麦克风记录到人耳听不到的语音指令,其原理是麦克风收到的高频超声波信号在被低通滤波器去除之前,经由放大器固有的非线性效应解调为正常可听频段的语音指令信号。从理想功能的视角,麦克风在语音采集层面并无缺陷,也设计了滤波器以去除超声波干扰。

类似的脆弱性案例还有很多,并且呈现逐年增多的趋势。这不禁引发我们思考,除了在信息系统的理

DOI: 10.11991/cccf.202603014
通信作者: 徐文渊, E-mail: wyxu@zju.edu.cn

想功能范围内研究脆弱性，是否存在理想功能视角外的脆弱性问题？“带外脆弱性”的概念构想也由此提出。

定义与内涵

带外脆弱性是指信息系统软硬件功能因“信号—信息”的理想映射与实际映射不一致而产生、可能造成严重危害的新型缺陷。在解释其内涵之前，首先有必要说明几个关键词的含义。

“信号—信息”映射 信息系统是物理和数字的复合体，其物理形态为系统的硬件等物理实体，数字形态为软件、数据、协议等虚拟主体，没有信息系统仅以物理或数字的单一形态存在。信号和信息分别是系统在物理形态和数字形态下的“血液”，二者相互依存，具有“映射转换”的关系——二进制数据在现实中对应晶体管的高低电平、磁盘的磁性极性、光纤的光场参数等物理载体状态。信息系统的功能实现离不开“信号—信息”映射，例如数据的加法操作在芯片中是由门电路组合成加法器电路，通过对信号的操作实现的。此外，传感器使信息系统具备了将物理信号转换为测量数据的感知能力，执行器使其具备了将指令信息转换为物理信号的控制能力，促成了信息物理系统的完全形态。

理想映射和实际映射 信息系统设计高度依赖对“信号—信息”理想映射的假设，如硬件电路能够可靠地反映和支撑数据运算，而这也是现代信息系统各类功能得以实现的前提。已有安全研究大多遵循此类理想映射假设，发现了大量表现为“信息处理缺陷”的软件脆弱性和“信号处理缺陷”的硬件脆弱性。然而，**由于硬件器部件的种种不可避免的固有特性，“信号—信息”的实际映射往往是不完美的，并且可能与理想映射有较大差异**。这种差异如果在不影响理想功能的情况下，形成了系统设计时未定义的“非理想功能”，则可能引入新的脆弱性。理想情况下，内存单元的电荷与数据应是一一映射，前文提及的 Rowhammer 攻击利用了相邻单元间异常的电荷映射，导致数据错误；海豚音攻击正是利用麦克风实际存在“超声波—语音数据”映射，而理想映射应是“声音—语音数据”。

带内/带外 “带外”（out-of-band）一词源自通信工程和网络技术领域，原指在常规或主数据通道之外进行的控制或传输行为，其中“带”（band）指频带（frequency band）。与之相反，在常规或主数据通道内的行为范畴称为“带内”（in-band）。该词后延伸出“带外数据、带外管理、带外认证”等场景，例如常见的多因子认证对于传统密码认证就属于带外认证。类似地，本文将由信息系统理想功能外的“信号—信息”异常映射导致的各类安全缺陷统称为“带外脆弱性”（out-of-band vulnerability），而在信息系统理想功能内的安全缺陷可认为是“带内脆弱性”（in-band vulnerability）。在这里，“带”指信息系统的理想功能，体现为“信号—信息”的理想映射，超出原本频带的狭义概念。

图 1 展示了麦克风的一组带外脆弱性案例。麦克风是一种测量可听声音的传感器，其理想映射为“声音—语音数据”。然而，多个研究发现，由于麦克风硬件具

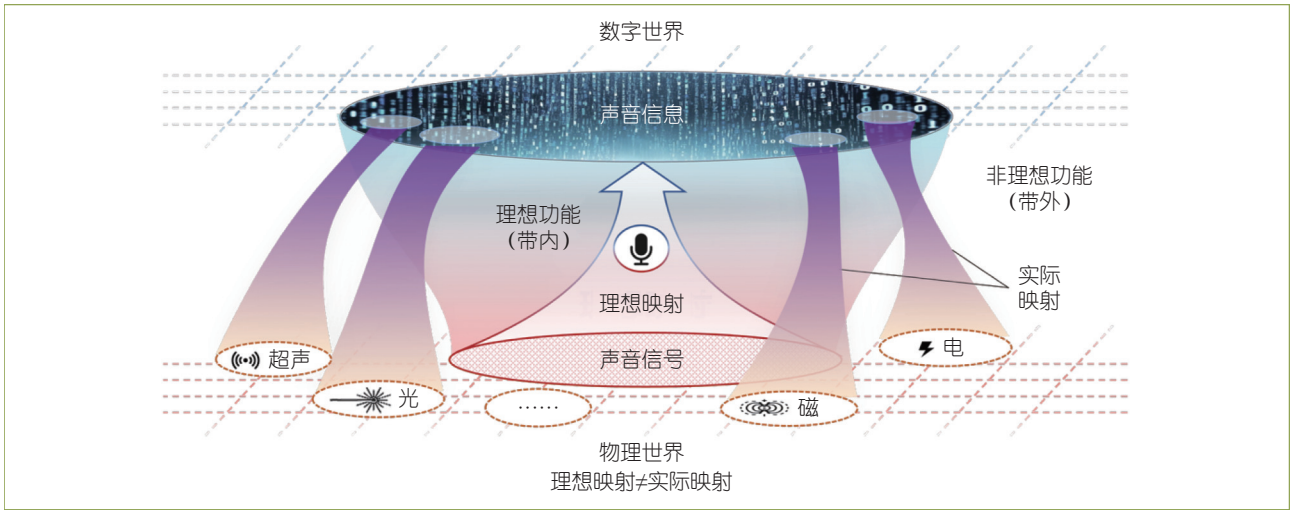


图 1 带外脆弱性示意

有光电光声转换、电磁耦合、非线性等固有效应，导致其除了海豚音攻击利用的“超声波—语音数据”映射，还存在“激光—语音数据”[5]、“电磁波—语音数据”[6]、“供电信号—语音数据”[7] 等理想功能外的异常映射，使攻击者可以通过激光、电磁波或供电干扰向麦克风中注入虚假语音指令，从而操控语音助手等智能语音系统。这些异常映射就是带外脆弱性。

“带外脆弱性”代表了近年来许多安全研究工作展现的一类共性思路，即打破对信息系统的理想假设，跳出常规系统认知来分析脆弱性。脆弱性是信息系统设计、实现、配置中因疏忽形成的缺陷，传统安全研究方法从“理想功能”的正向视角出发，按图索骥地分析设计、实现、配置等环节的理想功能缺陷，已经卓有成效地发现了大量“带内脆弱性”。然而，不同于有限的系统带内功能，带外功能以及其脆弱性是不可枚举的，其内涵随着技术创新和认知发展在不断扩展，“带外脆弱性”是未来安全研究需要持续探索的“边界”之一。

发展与研究概况

带外脆弱性是信息系统的重要风险，却是当前安全研究的短板，它的分析防护存在诸多独特挑战[8]。目前学术界已经积累了一些具有代表性的带外脆弱性案例和分立的研究方向，但是仍然缺乏统一的术语概念和理论体系来对此类问题进行系统性理解。

自 20 世纪 50 年代以来，研究人员开始发现一系列信息系统理想功能外的“信息”到“信号”异常映射，主要体现为计算机辐射物理信号导致的脆弱性。攻击者可以通过采集、分析计算机系统正常工作时伴生的声、光、电、磁、热等多物理场信号来推测目标系统的机密信息和隐私行为，后发展形成了物理侧信道攻击（physical side-channel attack）[9] 的研究方向。例如，美国国家安全局和国防部将关于电磁信息泄露的研究作为一个极为重要的保密项目，代号为“TEMPEST”，主要解决电子信息系统电磁泄漏带来的泄密隐患。此后，随着计算机技术的飞速发展和广泛应用，国内外相关研究逐渐从军工领域拓展到民用系统等其他领域上，从电磁泄漏拓展到其他物理场，通过泄漏信号恢复的内容从最早的计算机显示屏画面，拓展到推断系统所使用的加密密钥[10]、模型参数[11]、运行状态[12]、摄像头画面[13] 等领域。同时，研究人员发现主动利用计算机系统正常工作时的伴生声、光、电、磁、热等多物理场信号可以实现向外界的隐蔽通信，进而突破网络隔离泄漏机密信息，后发展形成了隐蔽信道（covert channel）的研究方向[14]。例如将信息编码至硬盘指示灯的闪烁上，实现向隔离网络外发送敏感数据[15]。

另一方面，由“信号”到“信息” 新型异常映射也逐渐被发现，主要表现为由物理信号注入造成信息系统异常，以传感器攻击[16] 为代表。研究人员近十年来围绕传感器发现了一系列带外脆弱性，攻击者可以通过发射物理信号干扰或操控传感器的测量结果，对信息系统的决策和控制造成严重威胁。如 2017 年提出的激光雷达攻击，通过虚假激光脉冲欺骗雷达的距离估计，使其测量到虚假的障碍物[17]；2022 年提出的“鬼手攻击”将调制电信号通过充电线注入到电容触屏传感器中，可实现触屏传感器的拒绝响应、触点注入和篡改[18]。此外，针对芯片的故障注入攻击（fault injection attack）[19] 也属于带外脆弱性的范畴，其通过向门电路、时钟、电源、IO 设备等组件注入恶意信号影响芯片的计算过程，如跳过指令、数据修改等。例如 2022 年的芯片电磁故障注入攻击通过干扰芯片控制流跳过了设备认证阶段，导致机密信息泄露[20]。

目前带外脆弱性的发现仍然以人工分析挖掘为主，高度依赖专家经验，自动化与大规模检测的能力还待完善。其主要挑战一是带外脆弱性涉及“信号—信息”异常映射，因此需要设计在物理世界和数字世界联动的测试方法；二是带外脆弱性不涉及特定的理想功能，难以形成确定性的测试目标和评估方法，测试维度也往往难以界定；三是带外脆弱性可能涉及系统软硬件等多模块联动，触发方式复杂。此外，带外脆弱性的防御方法研究起步较晚，现有以针对特定脆弱性的单点防御为主，系统性的带外脆弱性防御机制亟须研究。

展望

智能时代的信息系统安全研究范式需要从“带内”向“带内带外兼顾”转变。除了加快对带外脆弱性的概念形成共识，还有以下工作：

带外脆弱性理论体系 研究带外脆弱性的产生机理、效应特点、利用机制，构建带外脆弱性理论体系，为

带外脆弱性的检测、防护提供理论支撑。

带外脆弱性检测机制 参考带内脆弱性检测机制与方法，构建带内带外兼顾的检测体系，形成可扩展的自动检测框架，构建带外脆弱性知识库，实现脆弱性测试分析工具与检测仪器。

带内外协同防御架构 设计面向信息系统全生命周期的带内带外安全体系，明确安全需求、设计安全架构、确保安全生产、保障安全维护，实现带内带外脆弱性兼顾的主动防护安全架构。

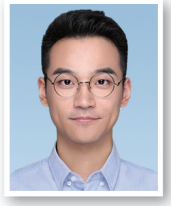
带外脆弱性安全标准 参考《信息安全技术网络安全等级保护基本要求：GB/T 22239—2019》[21]，推动带外脆弱性检测与量化评估标准建设，将带外脆弱性检测机制与带内外协同防御架构应用于现实信息系统，实现信息系统带外脆弱性从“被动响应”向“主动免疫”的范式升级。 ■

徐文渊

CCF 高级会员。浙江大学教授。主要研究方向为物联网安全、语音安全、智能电网安全。wyxu@zju.edu.cn

冀晓宇

CCF 专业会员。浙江大学教授。主要研究方向为物联网安全、具身智能安全、智能电网安全。xji@zju.edu.cn



闫 琛

CCF 专业会员。浙江大学副研究员。主要研究方向为硬件安全。
yanchen@zju.edu.cn

参考文献

[1] 全国科学技术名词审定委员会. 计算机科学技术名词（3 版）[M]. 北京: 科学出版社, 2018.

[2] MITRE. Common Weakness Enumeration [EB/OL]. (2025−06−18)[2026−02−09]. https://cwe.mitre.org/.

[3] Yoongu Kim, Ross Daly, Jeremie Kim, et al. Flipping Bits in Memory without Accessing Them: an Experimental Study of DRAM Disturbance Errors[C]//*2014 ACM/IEEE 41st International Symposium on Computer Architecture* . Piscataway: IEEE, 2014: 361−372.

[4] Guoming Zhang, Chen Yan, Xiaoyu Ji, et al. DolphinAttack: Inaudible Voice Commands[C]//*Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. New York: ACM, 2017: 103−117.

[5] Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, et al. Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems[C]//*Proceedings of the 29th USENIX Security Symposium*. Berkeley: USENIX, 2020: 2631−2648.

[6] Denis Foo Kune, John Backes, Shane S. Clark, et al. Ghost Talk: Mitigating EMI Signal Injection Attacks Against Analog Sensors[C]//*2013 IEEE Symposium on Security and Privacy*. Piscataway: IEEE, 2013: 145−159.

[7] Kai Wang, Shilin Xiao, Xiaoyu Ji, et al. Volttack: Control IoT Devices by Manipulating Power Supply Voltage[C]//*2023 IEEE Symposium on Security and Privacy*. Piscataway: IEEE, 2023: 1771−1788.

[8] 徐文渊, 郭世泽, 冀晓宇, 等. 从带内到带外——智能系统的脆弱性体系演变 [J]. 中国计算机学会通讯, 2022: 46−52.

[9] Stjepan Picek, Guilherme Perin, Luca Mariot, et al. SoK: Deep Learning-Based Physical Side-Channel Analysis[J]. *ACM Computing Surveys*, 2023, 55(11): 1−35.

[10] Giovanni Camurati, Sebastian Poeplau, Marius Muench, et al. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers[C]//*Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. New York: ACM, 2018: 163−177.

[11] Lejla Batina, Shivam Bhasin, Dirmanto Jap, et al. CSI NN: Reverse Engineering of Neural Network Architectures Through Electromagnetic Side Channel[C]// *Proceedings of the 28th USENIX Security Symposium*. Berkeley: USENIX, 2019: 515−532.

[12] Juchuan Zhang, Xiaoyu Ji, Yuehan Chi, et al. OutletSpy: Cross-Outlet Application Inference *via* Power Factor Correction Signal[C]//*Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2021: 181−191.

[13] Yan Long, Qinhong Jiang, Chen Yan, et al. EM Eye: Characterizing Electromagnetic Side-Channel Eavesdropping on Embedded Cameras[C]//*Proceedings 2024 Network and Distributed System Security Symposium*. Internet Society, 2024: 1−17.

[14] Butler W. Lampson. A Note on the Confinement Problem[J]. *Communications of the ACM*, 1973, 16(10): 613−615.

[15] Mordechai Guri, Boris Zadov, Yuval Elovici. LED-It-GO:

Leaking (a Lot of) Data from Air-Gapped Computers *via* the (Small) Hard Drive LED[M]//*Detection of Intrusions and Malware, and Vulnerability Assessment*. Cham: Springer International Publishing, 2017: 161−184.
[16] Chen Yan, Hocheol Shin, Connor Bolton, et al. SoK: a Minimalist Approach to Formalizing Analog Sensor Security[C]//*2020 IEEE Symposium on Security and Privacy*. Piscataway: IEEE, 2020: 233−248.
[17] Hocheol Shin, Dohyun Kim, Yujin Kwon, et al. Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications[C]//*Cryptographic Hardware and Embedded Systems – CHES 2017*. Cham: Springer, 2017: 445−467.
[18] Yan Jiang, Xiaoyu Ji, Kai Wang, et al. WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens[C]//*2022 IEEE Symposium on Security and Privacy*. Piscataway: IEEE, 2022: 984−1001.
[19] Aakash Gangolli, Qusay H. Mahmoud, Akramul Azim. A Systematic Review of Fault Injection Attacks on IoT Systems[J]. *Electronics*, 2022, 11(13): 2023.
[20] Shaked Delarea, Yossi Oren. Practical, Low-Cost Fault Injection Attacks on Personal Smart Devices[J]. *Applied Sciences*, 2022, 12(1): 417.
[21] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术网络安全等级保护基本要求: GB/T 22239—2019 [S]. 北京: 中国标准出版社, 2019.

Out-of-Band Vulnerability

Wenyuan Xu, Xiaoyu Ji, Chen Yan
Zhejiang University

Abstract: The rapid evolution of information systems continuously introduces new vulnerability types, especially those arising from the signal-information conversion processes at the interface between physical and digital realms. These vulnerabilities pose challenges for systematic analysis and detection. This article introduces the term "out-of-band vulnerabilities" to characterize such flaws, examining their conceptual foundations, causative mechanisms, current research landscape, and future directions. This article provides a valuable reference framework for addressing out-of-band vulnerabilities and enhancing the comprehensive vulnerability taxonomy.
Keywords: information system; vulnerability; out-of-band vulnerability; in-band vulnerability; vulnerability taxonomy; signal-information conversion

摘　要: 信息系统的发展不断引入新型脆弱性，特别是在物理世界和数字世界间的"信号—信息"映射转换过程中的安全缺陷难以被系统性地分析与挖掘，本文重点关注此类缺陷并定义为"带外脆弱性"，阐述其概念内涵、成因机制、研究发展与未来展望，为补齐带外脆弱性应对能力和健全脆弱性体系提供参考。
关键词: 信息系统；脆弱性；带外脆弱性；带内脆弱性；脆弱性分类；信号信息映射转换

中图分类号: TP393.08;TP309
中文引用格式: 徐文渊, 冀晓宇, 闫琛. 带外脆弱性 [J]. 计算, 2026, 2(3): 92−96.
英文引用格式: Wenyuan Xu, Xiaoyu Ji, Chen Yan. Out-of-Band Vulnerability[J]. *Computing Magazine of the CCF*, 2026, 2(3): 92−96.

（本文由 CCF 术语工委副主任**林俊宇**推荐）