Naming Content on the Network Layer: A Security Analysis of the Information-Centric Network Model

在网络层上命名内容：信息中心网络模型的安全性分析

1INTRODUCTION

1引言

The ubiquitous presence of the Internet points out its great success and emphasizes a future as promising as its past. A large portion of this success comes from the evolution of applications, services, and related technologies over the years, which have been shaping and evolving the way we use the Internet today. However, the Internet core architecture did not show the same evo-lution. Indeed, it has become extremely difficult to sustain the ever-increasing requirements for security, mobility, and availability through patches on protocols. This mismatch between the Inter-net architecture and its current requirments poses a huge motivation to look forward to a better architecture, more dynamic, modular, and adaptive, suitable to accommodate services we experi-ence today and foresee for the future [99].

互联网的无处不在表明了其巨大的成功，并有力展现出与过去一样充满希望的未来。这一成功的很大一部分来自多年来应用程序、服务和相关技术的发展，这些技术一直在塑造和发展我们今天使用互联网的方式。但是，互联网核心体系结构未显示出相同的发展。事实上，通过协议上的补丁程序来维持对安全性、移动性和可用性不断增长的需求已经变得极其困难。互联网体系结构与其当前要求之间的这种不匹配急需我们寻求一种更好的体系结构，使其更具动态性，模块化和适应性，以适应我们今天和未来所面临的服务[99]。

The Information-Centric Network (ICN) paradigm [25, 53] has gained considerable attention for a future Internet from both academia and industry, precisely by overcoming current Inter-net shortcomings, by shifting the main network entity from hosts to content, thereby requesting and routing named content directly at the network layer. Basically, the ICN model defines content requests using application-layer names directly on the networking layer, as opposed to the cur-rent IP model, in which the networking layer deals with machine addresses. The ICN approach is supposed to rethink the Internet foundations and to design a native ICN environment, embedding features like security, mobility support, and caching.

信息中心网络（ICN）范式[25，53]正是通过克服当前网络间的缺陷，通过将主要网络实体从主机转移到内容，从而直接在网络层请求和路由命名内容，这获得了学术界和工业领域对未来互联网的极大关注。基本上，ICN模型直接在网络层上使用应用层名称定义内容请求，这与当前IP模型不同，在IP模型中，网络层处理机器地址。ICN方法应该重新考虑互联网基础并设计本机ICN环境，并嵌入诸如安全性，移动性支持和缓存之类的功能。

From the security perspective, the architecture shift imposed by the ICN paradigm on the network-layer changes many aspects related to network security. Naming content instead of ma-chines changes the security paradigm from securing hosts and links to securing content, thus, naming content calls for authenticity and integrity protection mechanisms, to avoid well-known attacks such as spoofing. Moreover, naming content enables the detachment of a content from its location, allowing the deployment of in-network caches and resulting in content being retrieved from anywhere by anyone in the network. Although this brings obvious benefits, it also opens new challenges regarding privacy and access control on in-network cached content.

从安全性的角度来看，ICN范式在网络层上施加的体系架构转变改变了与网络安全性相关的许多方面。命名内容而不是机器将安全范式从保护主机和链接更改为保护内容，因此，命名内容需要真实性和完整性保护机制，以避免众所周知的攻击，例如电子欺骗。此外，命名内容可以使内容与其位置分离，从而可以部署网络内缓存，可以使得网络中任何人都可以从任何地方检索内容。尽管这带来了明显的好处，但它也带来了有关隐私和对网络内缓存内容的访问控制的新挑战。

Furthermore, as routing and forwarding are performed by content names, ICN also raises se-curity questions around monitoring and censorship. It becomes clear that ICN paves the way for potential security threats that are absent on current Internet; however, even known attacks from the Internet could undermine ICN architectures, as they may be emphasized when applied to ICN particularities. Thus, security in ICN should be provided differently from traditional networks. Consequently, security aspects in ICN need special attention, in order to ensure the architecture is robust to bear with current and future Internet requirements, and, more importantly, that the ICN paradigm is considered as a viable technology for content publishers.

此外，由于路由和转发是由内容名称执行的，因此，ICN还提出了有关监视和审查的安全性问题。很明显，ICN为当前互联网上未知的潜在安全威胁提供了缺口。然而，即使来自互联网的已知攻击也可能破坏ICN体系结构，因为它们在适于ICN特性时也可能会得到强化。因此，应以不同于传统网络的方式提供ICN的安全性保障。因此，ICN中在安全性方面需要特别注意，以确保该体系结构能够适应当前和将来的互联网需求，更重要的是，确保ICN范式被视为内容发布者的可行技术。

This article aims to provide a broad view and insights regarding security threats and their coun-termeasures introduced by naming content directly on the network layer. The main contribution of this text is the systematic organization, classification, and discussion of ICN security issues and their possible solutions. It does not propose new solutions for specific attacks; instead, it discusses possible solutions and provides references to research works that detail them. We expect this ar-ticle will open directions for a better understanding of current issues in ICN security and provide insights about new threats and potential directions for future works.

本文旨在通过直接在网络层上命名内容来提供有关安全威胁及其对策的广泛见解。本文的主要贡献是对ICN安全问题及其可能的解决方案进行了系统的组织、分类和讨论。本文没有针对特定攻击提出新的解决方案。相反，它讨论了可能的解决方案，并为详细介绍这些解决方案的研究工作提供了参考。我们期望这篇文章将为更好地理解当前的ICN安全问题开辟方向，并提供有关新威胁的见解以及未来工作的潜在方向。

This study considers aspects of security threats in the three main ICN architectures: (i) Named Data Networking, Content-Centric Networking (NDN/CCN1), (ii) Network of Information (Net-Inf), and (iii) Publish-Subscribe Internet Technology (PURSUIT). The text reflects the amount of research on security in each of these ICN architectures. Since some of them, like NDN/CCN, are far more explored than the others, the amount of work discussed for each architecture is not evenly distributed. In consequence, the solutions discussed in this text are mostly related to the NDN/CCN architecture.

本研究涉及了三种主要ICN架构中的安全威胁方面：（i）命名数据网络，内容中心网络（NDN / CCN1），（ii）信息网络（Net-Inf）和（iii）发布-订阅互联网技术（PURSUIT）。文本反映了每种ICN体系架构中对安全性的研究量。由于其中的一些架构（如NDN / CCN）要比其他的更为深入，因此针对每种体系结构讨论的工作量不是平均分配的。因此，本文中讨论的解决方案主要与NDN / CCN体系结构有关。

Some other surveys covering security aspects of ICNs were already published [1, 107]. Our text complements and updates them by analyzing, classifying, and organizing a broader number of papers about security in ICN and by giving an insight of current research and perspectives for

其他一些涉及ICN安全方面的调查早已发表[1107]。我们的文章通过分析，分类和组织有关ICN中安全性的大量论文，并对当前针对未来的研究和观点进行了分析，对本文进行了补充和更新。

1CCN was the original ICN architecture as proposed by Jacobson et al. [54]. NDN is a more recent architecture [127], largely inspired by CCN and initially based on the same code base (formerly called CCNx and recently renamed to NDNx). In this text, we use the acronym NDN/CCN to refer to both architectures, as their characteristics relevant to this survey are equivalent.

1CCN是Jacobson等人提出的原始ICN体系结构。[54]. NDN是一种更新的体系结构[127]，主要受CCN启发，最初基于相同的代码库（以前称为CCNx，最近更名为NDNx）。。在本文中，我们使用首字母缩写词NDN / CCN来指代这两种架构，因为它们与本次调查相关的特性是等效的。

future works. We also propose a brand new classification and organization for security attacks in ICN, enabling a new point of view on attacks and countermeasures in the ICN area. For a detailed review of the impact of some specific attacks in ICN architectures and the security requirements they impair, we refer the readers to AbdAllah et al. [1].

0000本文还提出了一种全新的ICN安全攻击分类和组织方法，为ICN领域的攻击和对策研究提供了新的视角。要详细了解某些特定攻击对ICN架构的影响及其对安全性的影响，我们向读者推荐AbdAllah等人的文章。[1].

The remainder of this article is structured as follows: Section 2 introduces the main entities of an ICN and explains their basic operations (2.1), as well as presents the vulnerabilities and types of attackers we could expect in an ICN architecture (2.2). Then, we discuss threats, attacks, and coun-termeasures on main ICN aspects, structured into three main groups: security in content naming (Section 3), security in routers (Section 4), and security in caching (Section 5). Section 6 discusses challenges and opportunities on ICN security for the effective adoption of ICN architectures, as well as lists future research directions. Section 7 provides final remarks.

本文的其余部分结构如下：第2节介绍了ICN的主要实体，并解释了它们的基本操作（2.1），以及ICN体系结构（2.2）中可能存在的漏洞和攻击者类型。然后，我们讨论有关ICN主要方面的威胁，攻击和对策，分为三大类：内容命名的安全性（第3节），路由器的安全性（第4节）和缓存的安全性（第5节）。第6节讨论了有效采用ICN架构的ICN安全方面的挑战和机遇，并列出了未来的研究方向。第7节为最后说明。

2INFORMATION-CENTRIC NETWORKS

2 以信息为中心的网络

Since the Internet inception, we have seen a continuous change in the way we use it. Among the services offered on the Internet, content distribution currently stands out as the most used service. In fact, applications that generate real-time content, such as Netflix and Spotify, represent the category with the highest global monthly traffic, exceeding 50% in North America and with expectations of growing in the next years [99]. However, the Internet shows flaws in efficiently distributing content to respond to the increasing traffic volume, as a legacy from an architecture designed for resource sharing through point-to-point communication. Indeed, solutions to cope with this new content demand were proposed and deployed, such as multicast protocols, peer-to-peer (P2P) networks, and content distribution networks (CDN). However, such solutions are overlays on top of the traditional IP network, inheriting the limitations of such protocol.

自Internet诞生以来，我们已经看到其使用方式的不断变化。在互联网上提供的服务中，内容分布式是目前最常用的服务。事实上，生成实时内容的应用程序，如Netflix和Spotify，代表着全球最高月度流量类别，在北美超过50%，并有望在未来几年内增长[99]。但是，作为一种旨在通过点对点通信进行资源共享的体系结构的遗留问题，互联网在有效分配内容以应对不断增长的流量方面显示出缺陷。事实上，已经提出并部署了一些解决方案来应对这种新的内容需求，如多播协议、对等网络（P2P）和内容分发网络（CDN）。但是，这样的解决方案是传统IP网络之上的叠加，继承了此类协议的局限性。

The inefficiency of the Internet also extends toward other areas [93]: multiple copies of the same data being transmitted, leading costs to Internet Service Providers (ISPs); no native support for traffic optimization in the IP architecture; network congestion and high dissemination latency; security focus on connections rather than the content; connection-oriented protocols preventing mobility; weak management of energy, as more hardware are needed to perform redundant tasks, and poor end-user delivery performance, especially when it comes to streaming flows. Thus, the perspective of evolving the Internet architecture to one better suited for content distribution con-stitutes the main driving force behind the ICN paradigm. However, not only the shortcomings of Internet Protocol (IP) addressing are driving this change, but also the desire to embed the ar-chitecture with features to provide adaptability, security, mobility, self-organization, and natural evolvability, tackling some current problems and anticipating others.

互联网的低效率还体现在其他方面[93]：同一数据的多个副本传输导致互联网服务提供商（ISP）加大开销；在IP体系结构中没有对流量优化的本地支持；网络拥塞和高传播延迟；安全性关注于连接而不是内容；面向连接的协议缺乏机动性；能源管理薄弱，因为需要更多的硬件来执行冗余任务，而且终端用户传输性能较差，尤其是在流媒体方面。因此，将互联网体系结构发展为更适合于内容分布的观点构成了ICN范例背后的主要驱动力。然而，不仅互联网协议（IP）解决方案的缺点正在推动这一变化，而且人们还希望将架构嵌入具有可提供适应性，安全性，移动性，自组织性和自然演进性的功能，从而解决当前的一些问题并预判未来的问题。

2.1 The Information-Centric Network Paradigm

2.1 以信息为中心的网络范式

Comparing ICN to the IP model, Jacobson et al. [54] highlight two prominent differences: what the network routes and how it routes. In terms of what is being routed, IP routers traditionally route IP packets through the network to a destination machine, while ICN routers are supposed to route requests for a named content toward the best available copy. Thus, IP names machines while ICN names content. To route a request from the user to the destination machine, IP routers are sustained by a routing infrastructure (i.e., autonomous systems), and requests must follow the routing hierarchy toward the destination machine. Besides, network nodes are assisted by Domain Name Service (DNS) servers to translate human-readable names to IP addresses. The ICN paradigm also routes requests toward a content publisher; however, as it provides means of caching content in routers, these can satisfy the user without requiring the request to proceed all the way back to the publisher. In ICN, we observe three main domains that differ from traditional IP networking:

比较ICN和IP模型，Jacobson等人[54]强调两个显著的区别：网络路由和其路由方式。就路由的内容而言，IP路由器通常将IP数据包通过网络路由到目标计算机，而ICN路由器应该将对命名内容的请求路由到最佳可用副本。因此，IP命名机器，而ICN命名内容。为了将请求从用户路由到目标计算机，IP路由器由路由基础结构（即自动化系统）维持，并且请求必须遵循路由层次结构向目标计算机的方向。此外，域名服务器（DNS）服务器协助网络节点将可读的名称转换为IP地址。ICN范式还将请求路由到内容发布者；但是，由于它提供了在路由器中缓存内容的方法，因此这些方法可以满足用户的要求，而无需请求一直继续返回发布者。在ICN中，我们观察到与传统IP网络不同的三个主要领域：

(i)naming, (ii) routing and forwarding, and (iii) caching. In the following, we highlight each of these domains.

（i）命名，（ii）路由和转发，以及（iii）缓存。在下文中，我们重点介绍了每个网域。

•Naming: Since ICN names content items rather than hosts, there is a real concern about scalability. There are many more content items than hosts on the Internet, and the naming scheme is supposed to unambiguously identify all such content. Basically, naming schemes in ICN are divided into two major approaches: flat naming [29] and hierarchical naming [103]. Both have pros and cons: while flat naming allows better naming persistence, as it is not related to any location or organization, it also limits the aggregation of names for routing performance purposes. Hierarchical naming, in contrast, optimizes routing infor-mation aggregation and performance by a name prefix hierarchy, but groups of content that share the same prefix may have to be dealt together by the same location. It is also useful for naming content items in a particular context, facilitating management actions. There is also the attribute-value naming scheme [12], in which a set of attributes representing the capabilities of a content is mapped into a content name. Attribute-value naming schemes have been explored mostly on mobile and Internet of Things environments [90].

•命名：由于ICN命名内容项而不是主机，因此其真正关注的是可伸缩性。互联网上的内容项比主机多得多，而且命名方案应该能够明确地识别所有此类内容。基本上，ICN中的命名方案分为两种主要方法：平面命名[29]和分层命名[103]。两者都有优点和缺点：虽然统一命名有利于更好的命名持久性，因为它与任何位置或组织都不相关，但它也出于路由性能的目的而限制了名称的聚合。相反，分层命名通过名称前缀层次结构优化了路由信息的聚合和性能，但是共享同一前缀的内容组可能必须由同一位置一同处理。它对于在特定上下文中命名内容项也很有用，从而有助于促进管理操作。还有一种属性值命名方案[12]，其将代表内容功能的一组属性映射到内容名称中。该方案已经在移动电话和物联网环境中得到了广泛的探索[90]。

•Routing and forwarding: Two main forwarding schemes have being considered in ICN archi-

•路由和转发：ICN架构中考虑了两种主要转发方式：

tectures: name based routing [54] and name-based routing with support of a Name Resolution Service (NRS) [4, 25]. Routers are populated with hierarchical prefixes and corresponding outgoing interface, and store the request state information to forward the content back to the requestor. Using this routing scheme, routers forward content based directly on the con-tent name. In the routing scheme with support of a name resolution service, route discovery acts similarly to the traditional DNS: NRSs map content names to a set of locations; requests are then resolved by the NRS and forwarded by a topology based routing protocol, using the locations retrieved from NRS.

基于名称的路由[54]和具有名称解析服务（NRS）[4，25]支持的基于名称的路由。路由器使用分层前缀和相应的传出接口填充，并存储请求状态信息以将内容转发回请求程序。路由器使用此路由方案直接根据内容名称转发内容。在支持名称解析服务的路由方案中，路由发现的作用与传统DNS类似：NRS将内容名称映射到一组位置；然后由NRS解析请求，并通过由从NRS检索到位置的基于拓扑的路由协议转发请求。

•Caching: three different caching solutions have been proposed to ICN architectures: on-path, off-path, and peer-caching. On-path caching opportunistically explores local content popularity in order to optimize content delivery. It caches content in routers based on the number of content requests passing through them. Off-path caching is performed by dedi-cated servers, very similar to CDNs today and is also sustained by content popularity. Peer-caching is tackled in mobile environments, where users’ devices can be used as content caches to provide a better content availability to nearby devices. Caching also manages the eviction of content items through cache eviction policies such as Least Recently Used (LRU) and Least Frequently Used (LFU) [125].

•缓存：已针对ICN体系结构提出了三种不同的缓存解决方案：路径上缓存、路径外缓存和对等缓存。路径高速缓存会适时探索本地内容流行度，以优化内容传输。它根据通过路由器的内容请求的数量在路由器中缓存内容。路径外缓存是由专用服务器执行的，这与当今的CDN非常相似，并且还受内容流行度的支持。对等缓存是在移动环境中解决的，在移动环境中，用户设备可用作内容缓存，以向附近的设备提供更好的内容可用性。缓存还通过诸如最近最久未使用算法（LRU）和最近最少使用算法（LFU）[125]之类的缓存策略来管理内容项的汰换。

To date, various ICN architectures have been proposed, such as NDN/CCN [54, 127], NetInf [25], PURSUIT [33], and Data-Oriented Network Architecture (DONA) [62]. Although these architec-tures share the same basic components (named content, routing by content name, and in-network caching), they have particularities regarding implementations. In this survey, we aim to system-atize the security literature about the ICN core function vulnerabilities; thus, we do not discuss particularities of such architectures. Throughout this article, we refer to ICN principles and re-quirements as the ICN paradigm. The set of ICN instances we call ICN architectures. We thought this clarification would be valid as this distinction is not always clear.

迄今为止，已经提出了各种ICN体系结构，例如NDN / CCN [54、127]，NetInf [25]，PURSUIT [33]和面向数据的网络体系结构（DONA）[62]。尽管这些架构共享相同的基本组件（命名内容，按内容名称进行路由和网络内缓存），但它们在实现方面具有特殊性。在此调查中，我们旨在将有关ICN核心功能漏洞的安全性分析文献系统化；因此，我们不讨论此类架构的特殊性。在本文中，我们将ICN原则和要求称为ICN范式。将ICN架构称为ICN实例。我们认为这种说明是确实必要的，因为这种区别并不总是很清楚。

Concerning ICN terminology, the RFC 7927 [64] defines three main terms: a Named Data Object (NDO), or simply a data object, is an addressable piece of information that can be requested from the network; a Publisher is an entity that publishes an NDO to the network (the publisher is not necessarily the NDO creator, it may just host data objects for the real producer); and a Requestor is an entity that issues a request for a named data object to the network. In this text, the terms content and data object are used interchangeably; the term publisher is used to represent both the

关于ICN术语，RFC 7927 [64]定义了三个主要术语：命名数据对象（NDO），或简称为数据对象，或是可以从网络请求的可寻址信息；发布者是将NDO发布到网络的实体（发布者不一定是NDO创建者，它可以仅托管实际生产者的数据对象）；请求程序是向网络发布对命名数据对象的请求的实体。在本文中，术语内容和数据对象可互换使用。“发布者”这一术语既代表

Fig. 1. Basic ICN content distribution model.

图1. 基本的ICN内容分布模型。

entity that produces a content (its creator or producer) and the entity that makes it available to the network; the terms requestor and user are considered equivalent; finally, the term source designates a generic entity providing a data object, may it be a publisher or a cache.

产生内容的实体（其创建者或生产者）以及使内容可用于网络的实体；“请求程序”和“用户”被视为等同术语；最后，术语“源”表示提供数据对象的通用实体，它可以是发布者或缓存。

Figure 1 depicts a simple example of how content flows in the ICN communication model, using the NDN/CCN architecture as a support for it. First, a publisher makes content available to users, in this example under the prefix /s1/, which became aware of such content by applications or search mechanisms. Users send requests for content items to the network (Figure 1(a)), without specifying a particular machine or address. The routers, based on their routing tables, route the request toward the content publisher, checking their caches for a cache hit. The reply contain-ing the payload follows the reverse path (Figure 1(b)). As the content is forwarded through the routers, they may store a copy in their caches, providing ways to reason bandwidth, link quality, or available connections, by satisfying further requests without routing them all the way back to the publisher, as depicted in Figure 1(c).

图1描绘了一个简单的示例，即使用NDN / CCN架构作为对ICN通信模型中内容的流动方式。首先，发布者向用户提供内容，在此前缀为/ s1 /的示例中，用户已通过应用程序或搜索机制意识到了这些内容。用户将对内容项的请求发送到网络（图1（a）），而无需指定特定的计算机或地址。路由器根据其路由表将请求路由到内容发布者，检查其缓存中是否有缓存命中。包含有效负载的回复遵循反向路径（图1（b））。当内容通过路由器转发时，它们可以将副本存储在其缓存中，从而通过满足进一步的请求而无需将它们一直路由回发布者来提供推理带宽，链接质量或可用连接的方法，如图所示。 1（c）。

2.2 Security Concerns in ICN

2.2 ICN中的安全问题

Despite the great benefits from adopting the ICN paradigm, the deep change it represents in the network layer invariably leads to new security challenges. For example, it is mandatory for all ICN architectures to provide a name-content integrity check mechanism, enabling users to check whether the retrieved content was tampered with. Furthermore, content authenticity should also be addressed, to provide means of assessing content origin. Content-based routing demands more management information to be handled in each router than IP-based routing, such as the Forward Information Base (FIB) and Pending Interest Table (PIT) structures in NDN/CCN. Since pending requests are stored by each router, they may be susceptible to Denial of Service (DOS) attacks by malicious users flooding them with requests [114] and should be protected. Caching mechanisms introduced by ICN may also be targeted by malicious users, and solutions to avoid well-known attacks as cache pollution and cache snooping need attention, as well as mechanisms to control access to cached content only to authorized users. Privacy is another concern for ICN architectures,

尽管采用ICN范式有很多好处，但其使网络层发生的深刻变化始终会带来新的安全挑战。例如，所有ICN架构都必须提供名称-内容完整性检查机制，使用户能够检查检索到的内容是否被篡改。此外，还应该解决内容的真实性问题，以提供评估内容来源的方法。与基于IP的路由相比，基于内容的路由需要在每个路由器中处理更多的管理信息，例如NDN / CCN中的转发信息库（FIB）和待定请求表（PIT）结构。由于每个路由器都存储挂起的请求，因此它们可能容易受到恶意用户的拒绝服务（DOS）攻击，并应受到保护。ICN引入的缓存机制也可能成为恶意用户的攻击目标，所以需要采取解决方案避免缓存污染和缓存窥探等众所周知的攻击，并建立机制管控仅对授权用户开放的缓存内容。隐私是ICN架构的另一个关注点，

Fig. 2. Classification and organization of security threats and the malicious entities they involve.

图2. 安全威胁及其涉及的恶意实体的分类和组织。

as content items are requested by name and may be cached on intermediary routers; malicious en-tities should have no access to privacy-sensitive information through content names. ICN does not use the notion of source address; thus, it is not simple to bind a content to a requester, preserv-ing her privacy. Nevertheless, the content name may reveal enough information to hinder users’ privacy in some specific scenarios.

因为内容项是按名称请求的，并且可以缓存在中间路由器上；恶意实体不应能通过内容名称访问到隐私信息。因为ICN不使用源地址的概念；所以，将内容绑定到请求程序以保留其隐私并不简单。但是，在某些特定情况下，内容名称可能会显示过多的信息导致侵犯用户的隐私。

Overall, we consider that attacks exploring ICN vulnerabilities may be triggered by any en-tity participating in the network: users, content publishers, routers, and cache custodians. We denominate as malicious any of these entities that aims to explore vulnerabilities in the ICN ar-chitecture to disrupt the network or to jeopardize users’ and content publishers’ privacy. These malicious entities can manifest either in passive or active ways, depending on their interaction with the network. While passive attacks are difficult to detect, as the malicious entity does not interact with the network, active attacks can be profiled, as the malicious entity interacts with other network entities to issue an attack. Also, we assume that malicious entities can act alone or by colluding with others malicious entities to extend the damage. We also consider malicious entities that may have limited resources to launch attacks, as well as malicious entities that have high computational power available for attacks, such as routers, publishers, and governments.

总体而言，我们认为，探索ICN漏洞的攻击可能是由参与该网络的任何实体（用户，内容发布者，路由器和缓存保管人）触发的。我们将这些旨在探索ICN体系结构中破坏网络或危害用户和内容发布者隐私的漏洞的实体称为恶意实体。这些恶意实体可以根据其与网络的交互以被动或主动方式显示。虽然由于恶意实体不与网络交互，被动攻击很难检测，但可以分析主动攻击，因为恶意实体与其他网络实体交互以发出攻击。此外，我们假设恶意实体可以单独采取行动，也可以与其他恶意实体勾结以扩大损害范围。我们还考虑了可能具有有限资源来发起攻击的恶意实体，以及具有高计算能力可用于攻击的恶意实体，例如路由器，发布者和政府。

To better understand how attacks influence the ICN behavior, we divided our analysis into the three main domains: security in content, in routers, and in caching. Figure 2 illustrates each of these domains and their respective classes of attacks, as well as the malicious entities that are most likely able to trigger them. For security in content, we expect attacks eased by the lack of security in content naming, leading to threats on content integrity, privacy, and unauthorized access. For routers security, we tackle attacks aiming to disrupt the network as a result of the ICN model, such as resource exhaustion, publisher unavailability, and route depletion. Finally, security in cache covers attacks to in-network caches as cache snooping, cache pollution, and cache poisoning. Each class of attack can be triggered by different vulnerabilities or security flaws in the ICN model, as detailed in next sections.

为了更好地了解攻击如何影响ICN行为，我们将分析内容分为三个主要部分：内容安全、路由器安全和缓存安全。图2说明了每个域及其各自的攻击类别，以及最有可能触发它们的恶意实体。在内容安全方面，我们分析由于内容命名缺乏安全性而缓解的攻击会导致对内容完整性，隐私和未授权访问的威胁。在路由器安全方面，我们分析旨在通过ICN模型破坏网络的攻击，例如资源耗竭，发布者不可用和路由耗竭。最后，缓存安全包括对网络内缓存的攻击，例如缓存侦听，缓存污染和缓存中毒。每种攻击类型都可以由ICN模型中的不同漏洞或安全缺陷触发，这将在下一部分中详细介绍。

In the next sections, we systematically present and organize the main attacks against ICN dis-cussed in the literature, and the countermeasures proposed to thwart them, when applicable. We

在接下来的部分中，我们系统地介绍和组织了文献中针对ICN的主要攻击的讨论，并在提出了在适用的情况下阻止这些攻击的对策。我们

specifically target intentional faults introduced by attackers, although ICN architectures are also prone to other faults, like physical and design faults. We also introduce tables containing the com-pilation of ICN attacks and their corresponding category, target, vulnerability, as well as references to papers tackling countermeasures to mitigate them. In such tables, we aim to specify exactly the name of the attacks used by authors in their papers, even though some of them may have identical functioning. We chose to stick with the naming convention used by the authors, to help the read-ers to identify these similarities. These tables are divided into three parts, each one presenting a category of attacks, being placed at the end of the corresponding section. Although distinct ICN architectures [5, 25, 33, 53] have particularities regarding implementations, they share the same basic ICN components (named content, routing by content name, and in-network caching). Thus, we are interested in security issues concerning the core functions of the ICN paradigm, and will not discuss particularities of such architectures.

特别针对攻击者引入的故意进行分析，尽管ICN体系结构也容易出现其他错误，如物理错误和设计错误。我们还介绍了以表格形式汇总的ICN攻击及其相应类别，目标，漏洞的信息，并提供了针对缓解这些问题的参考文献。在这些表格中，我们力求确切地指定作者在其论文中使用的攻击的名称，即使其中一些可能具有相同的功能。我们选择遵守作者使用的命名约定，以帮助读者识别这些相似之处。这些表格分为三个部分，每个部分标明一种攻击类别，分别位于相应部分的末尾。尽管不同的ICN体系结构[5、25、33、53]在实现方面具有特殊性，但它们共享相同的基本ICN组件（命名内容，按内容名称路由和网络内缓存）。因此，我们重点关注与ICN范式的核心功能有关的安全性问题，但将不讨论此类体系结构的特殊性。

3 SECURITY IN CONTENT

3 内容安全

The content naming scheme is at the core of any ICN architecture and thus is one of the most critical mechanisms to be secured. As important as the protection of the content name is the pro-tection of the content itself. Mainly due to content-location independence introduced by the ICN paradigm, the content is susceptible to threats regarding integrity and authenticity, privacy, and secrecy. Indeed, name and content security has been a main issue for ICN designers, and a great amount of vulnerabilities and solutions have already been studied. In this section, we categorize content naming security issues into three groups: content integrity and authenticity, content pri-vacy, and content secrecy. Content integrity and authenticity threats comprise attacks that aim to modify and tamper legitimate content payload, to cheat the network and the users, or to inject fake content in the network, as if it originated from a real publisher. Content privacy attacks aim to vi-olate users’ and content publishers’ sensitive information by tampering communication channels (privacy issues due to caching are discussed in Section 5) and may result in censorship and user monitoring. Finally, secrecy issues comprise attacks that aim to give access to cached content items to unauthorized entities. These attacks and their countermeasures are detailed in the following.

内容命名方案是任何ICN体系结构的核心，因此是需要保护的最关键的机制之一。与保护内容名称一样重要的是保护内容本身。主要由于ICN范式引入的内容位置独立性，内容容易受到与完整性和真实性、隐私和保密性相关的威胁。确实，名称和内容安全性已成为ICN设计人员面临的主要问题，并且设计人员对此已经研究了大量漏洞和解决方案。在本节中，我们将内容命名安全性问题分为三类：内容完整性及真实性，内容私密性和内容保密性。内容完整性和真实性威胁包括旨在修改和篡改合法内容载荷，欺骗网络和用户或将虚假内容注入网络中的攻击，就好像它们来自真正的发布者一样。内容隐私攻击旨在通过篡改通信渠道来侵犯用户和内容发布者的敏感信息（第5节中讨论了由于缓存引起的隐私问题），并可能触发审查机制和用户监控。最后，保密问题包括旨在将对缓存内容项的访问权授予未经授权实体的攻击。下面将详细介绍这些攻击及其对策。

3.1 Content Integrity and Authenticity

3.1 内容完整性和真实性

Because content may be distributed and cached by third-party entities, like routers and mobile devices, rather than just servers controlled by content publishers, it is subject to attacks targeting its integrity and authenticity [50, 97]. Malicious entities may tamper content items, by intercepting them and modifying their payload; they also can forge content and inject it in the network, as if it originated from a real publisher. Such attacks are simple and relatively easy to launch: first, the content name is visible to the network entities; thus, it is relatively easy for malicious entities to target popular content items. Second, because the content may be kept by any network entity, the content publisher has no control over it. However, it is easier for malicious routers to launch these attacks due to their privileged positions in the network. Figure 3 depicts this scenario; while user U2 requests for content /s1/A, router R2 produces and replies with a forged content. This attack is extremely damaging to users because it is expected that they accept content from locations other than the content publisher itself; thus, they are vulnerable to corrupted/suspicious content that does not correspond to the original request.

由于内容可能由路由器和移动设备之类的第三方实体分发和缓存，而不仅仅是由内容发布者控制的服务器，因此，内容会遭受针对其完整性和真实性的攻击[50，97]。恶意实体可能会通过拦截内容项并修改其有效载荷来篡改内容项；它们还可以伪造内容并将其注入网络，就像内容是来自真正的发布者一样。此类攻击简单且相对容易发起：首先，因为网络实体可以看到内容名称；所以恶意实体将流行内容项作为目标相对容易。其次，由于内容可以由任何网络实体保存，因此内容发布者无法对其进行控制。但是，由于恶意路由器在网络中的特权位置，因此更容易发动这些攻击。图3描述了这种情况。当用户U2请求内容/ s1 / A时，路由器R2生成并回复伪造的内容。这种攻击对用户造成极大破坏，因为用户很可能会接受非内容发布者本身以外的其他位置的内容。因此，他们很容易受到与原始请求不符的损坏/可疑内容的攻击。

Concerns about content integrity and authenticity are fundamental for any ICN design and indeed have been considered since the conception of naming schemes by adopting digital sig-natures to provide guarantees on content integrity and provenance [45]. It should be noted that content integrity and authenticity are two closely related issues. Most solutions to content integrity threats also apply to content authenticity issues. In most of ICN architectures, the content itself

对内容完整性和真实性的担忧对于任何ICN设计都是至关重要的，并且自从采用数字签名命名方案这一概念以保证内容完整性和来源，就已经考虑了这些问题[45]。应该注意的是，内容的完整性和真实性是两个密切相关的问题。大多数针对内容完整性威胁的解决方案也适用于内容真实性问题。在大多数ICN架构中，内容本身

Fig. 3. Integrity threat in ICN.

图3. ICN中的完整性威胁。

can ensure its integrity and authenticity, thus allowing its location independence. For instance, the NDN/CCN architecture ensures integrity by authenticating the linkage between the content and its name. This is performed by the content publisher, who digitally signs the mapping from the content name to the content [103].

可以保证其完整性和真实性，从而允许其位置独立性。例如，NDN/CCN体系结构通过验证内容及其名称之间的链接来确保完整性。这是由内容发布者执行的，内容发布者对从内容名称到内容的映射进行数字签名[103]。

Naming a data object after the cryptographic hash of its content allows checking the object’s integrity. Thus, upon the reception of a content, the user is able to check its integrity and prove-nance by confronting content hashes and certificates with the content publisher or with support of metadata. This schema is adopted in architectures that use flat naming schemes, like NetInf [24], but can also be applied to hierarchical naming ones, as in NDN/CCN [13, 41]. One should observe that this approach works as long as the cryptographic hash function is trustworthy; a broken hash function in an architecture that uses hash-based name binding would allow one to easily publish distinct contents with the same name. Alternatively, identity-based encryption is also proposed to assess the integrity and authenticity of content items [48, 50, 109, 129], where the content name serves as a public key for the content publisher to validate its authenticity. However, such schemes still need the use of auxiliary tools that allow the verification of content integrity.

在其内容的加密散列之后命名数据对象可以检查对象的完整性。因此，在接收到内容时，用户能够通过与内容发布者或元数据支持对抗内容哈希和证书来检查其完整性和出处。因此，在接收到内容时，用户能够通过与内容发布者或元数据支持对抗内容散列和证书来检查其完整性及出处。这种模式在使用平面命名方案的体系结构中采用，例如NetInf [24]，但也可以应用于分层命名方案中，如NDN / CCN [13，41]。应该注意的是，只要加密哈希函数是可信的，这种方法就可以实行。但在使用基于哈希的名称绑定的体系结构中，一个损坏的哈希函数就可以使人轻松地发布具有相同名称的不同内容。另一种方法是提出基于身份的加密来评估内容项的完整性和真实性[48、50、109、129]，其中内容名称用作内容发布者验证其真实性的公钥。但是，这样的方法仍需要使用允许验证内容完整性的辅助工具。

As essential as paying attention to content authenticity is addressing publisher authenticity, in which the user is able to identify and trust the content publisher. The user may decide to accept or reject a content based on trust information regarding the content publisher, thus involving trust management mechanisms [123]. As the users are able to assess integrity and authenticity from the content itself, they should also make sure the public key used to sign the content is trusted. Alternatives to traditional public-key infrastructures for content authentication are also proposed in ICN, mainly exploring distributed and decentralized mechanisms such as the use of distributed hash tables (DHT) [117, 118], social graphs [74], and traditional DNS-like mechanisms [75]. Another solution propose splitting public keys into several pieces that are redundantly scattered on the network; users can retrieve them from any entity to verify content integrity [55, 61] or even use edge routers to validate the authenticity of all content entering their networks [60]. Researchers also explored a scheme for authenticate old data by using a bookkeeping service that certificates data signatures anytime [124]. The main challenges in the design of trust management schemes are scalability and revocation of keys and certificates [82], since the keys and certificates can also be stored on uncontrolled caches.

与关注内容真实性一样重要的是解决发布者真实性问题，其中用户能够识别并信任内容发布者。用户可以基于有关内容发布者的信任信息来决定接受或拒绝内容，因此这就涉及到信任管理机制[123]。由于用户能够从内容本身评估完整性和真实性，因此他们还应确保用于签名内容的公钥是可信的。在ICN中还提出了用于内容认证的传统公钥基础结构的替代方法-主要探索分布和分散机制，例如使用分布式哈希表（DHT）[117，118]，社交图[74]和类似传统DNS的机制[75]。另一种解决方案是将公钥分成若干部分，这些部分充分地散布在网络上。用户可以从任何实体中检索它们以验证内容完整性[55、61]，甚至可以使用边缘路由器来验证进入其网络的所有内容的真实性[60]。研究人员还探索了一种通过使用簿记服务对旧数据进行身份验证的方案，该簿记服务可随时对数据签名进行认证[124]。设计信任管理方案的主要挑战是可伸缩性以及密钥和证书的撤消[82]，因为密钥和证书也可以存储在不受控制的缓存中。

3.2 Content Privacy

3.2 内容隐私

One of the main mechanisms of any ICN architecture is the name-based routing, which conse-quently makes content names visible to the network. This is a problem because names may con-tain semantic information about content items, thus hindering privacy practices. Malicious entities could explore this feature to monitor, filter, and block users’ requests based on content names

任何ICN体系结构的主要机制之一是基于名称的路由，它使内容名称对网络可见。这是一个问题，因为名称可能包含有关内容项的语义信息，从而妨碍了隐私惯例。恶意实体可以利用此功能来监视，过滤和阻止基于内容名称的用户请求。

Fig. 4. Privacy threat in ICN.

图4. ICN中的隐私威胁。

[20]. For example, a malicious entity may use a blacklist with content names to block/delete and then monitor channels (and caches) to match content with the blacklist. As routers are strategi-cally positioned in the network and have access to the network traffic, they are the best candidates to issue such attacks. Figure 4 illustrates U1 attempting against U2 privacy by monitoring the communication channel and learning what U2 is requesting. Alternatively, the malicious entity could simply inspect caches and channels for keywords [10]. Although it is difficult to pinpoint the specific user requesting the content, content monitoring and inspection could deny services or censure sensitive content items. This same tactic can be used for monitoring user requests, in which the malicious user eavesdrops the communication channel to figure out content names and to infer users preferences [2].

[20]. 例如，恶意实体可能使用具有内容名称的黑名单来阻止/删除，然后监视通道（和缓存）以使内容与黑名单匹配。由于路由器在策略上位于网络中并且可以访问网络流量，因此它们是发出此类攻击的最佳选择。图4说明了U1通过监视通信信道并了解U2正在请求的内容来尝试侵犯U2隐私。或者，恶意实体可以简单地检查高速缓存和通道以查找关键字[10]。虽然很难确定请求内容的特定用户，但是内容监视和检查可能会拒绝服务或谴责敏感内容项。同样的策略也可以用于监视用户请求，恶意用户用此策略窃听通信通道以找出内容名称并推断用户偏好[2]。

From the privacy perspective, the main countermeasure to ensure privacy in ICN is to hide or mask the content requests from network entities [106]. Bloom filters [14] have been extensively explored in ICN for this purpose, since this scheme allows a network entity (e.g., a router) to test whether a particular content name is in the routing table or in the cache, without revealing the content name [16, 79]. Before requesting a content, the user computes the Bloom filter for each sub-component in the hierarchical name. Then, routers perform the longest-prefix matching on the content identifier. As this approach transforms the content identifier in a random string of bits, it helps to prevent blacklist matching and user profiling. Alternatively, homomorphic encryption can also be used to hide requests, at the same time that allows routers and content publishers to check whether the requested content is in their content sets, ensuring that neither content publishers nor third-party elements, such as eavesdroppers, are able to deduce or discover the content the user is requesting [33].

从隐私的角度来看，确保ICN中的隐私的主要对策是隐藏或掩码来自网络实体的内容请求[106]。为此，布隆过滤器[14]在ICN中得到了广泛的研究，因为该方案允许网络实体（例如路由器）测试特定内容名称是在路由表中还是在缓存中，而不暴露内容名称[16，79]。在请求内容之前，用户为分级名称中的每个子组件计算布隆过滤器。然后，路由器对内容标识符执行最长前缀匹配。由于此方法将内容标识符转换为随机的位串，因此有助于防止黑名单匹配和用户侧写。或者，同态加密也可以用于隐藏请求，同时允许路由器和内容发布者检查所请求的内容是否在其内容集中，以确保内容发布者和第三方元素（例如窃听者）均不能够推断或发现用户正在请求的内容[33]。

Another approach used to provide privacy to users when requesting content in ICN is by mask-ing the content, using cover files, for example. The idea of such solutions is to create a computa-tional asymmetry for legitimate and malicious users when retrieving a content, avoiding blacklist attacks. Basically, the publisher mixes a legitimate content with a cover content. To retrieve the content, the user needs to gather some side information from the publisher using a secure chan-nel, namely the content hash and the algorithm used to generate the covered content. As content items are retrieved in covered blocks, it requires a huge computational effort from malicious users to uncover the content being requested without prior knowledge of the extra information, while le-gitimate users could easily extract the desired content using the information retrieved in the secure side channel [10]. Another idea for the user wanting privacy in content retrieval is to encapsulate the request with each router’s public key on a known circuit to the content, in an onion routing overlay. Upon reception, each node on the circuit extracts its encryption layer and forwards the request to the next node. This proceeds until the request reaches the publisher, which will receive it in plain text [26, 101, 108]. Also, a user may encode the content name on requests and have

用于在ICN中请求内容时为用户提供隐私的另一种方法是，例如，使用覆盖文件对内容进行掩码。这种解决方案的思想是在取回内容时为合法和恶意用户创建非对称计算，避免黑名单攻击。基本上，发布者将合法内容与覆盖内容混合在一起。为了取回内容，用户需要使用安全通道从发布者那里收集一些辅助信息，即内容哈希和用于生成覆盖内容的算法。由于内容项是在覆盖的块中检索的，因此恶意用户需要进行大量计算才能在事先不知道额外信息的情况下发现所请求的内容，而合法用户可以使用在安全侧通道中取回的信息轻松提取所需内容[10]。对于想要在内容检索中保护隐私的用户来说，另一个想法是将请求与每个路由器的公钥一起封装在内容的已知电路中，即封装在洋葱路由覆盖中。接收时，电路上的每个节点都提取其加密层，并将请求转发到下一个节点。这个过程一直持续到请求到达发布者，发布者将以纯文本格式接受它[26，101，108]。此外，用户对请求内容的名称进行编码，

Fig. 5. Unauthorized access threat in ICN.

图5. ICN中未经授权的访问威胁。

perfect secrecy, with the support of content publishers [106]. However, this solution generally impairs the benefits of in-network cache, negatively affecting network and caching performance.

并且在内容发布者的支持下，隐私得到完全保护[106]。但是，此解决方案通常会削弱网络内缓存的优势，从而对网络和缓存性能产生负面影响。

Privacy is also a concern for content publishers due to the possibility of censorship, mainly be-cause the content name may contain the publisher (producer) identification. Although censorship should not be handled by the network itself, the ICN behavior may ease it; thus, it is important to discuss such threats. A set of preventive measures to avoid monitoring and censorship of content publishers is proposed in Acs et al. [2], such as using group signatures, ring signatures, and confirmation signatures, which allow a user to verify whether the signature of the content is valid, but not specifically identifying which publisher has signed it, and thus guaranteeing the content publisher’s anonymity. Another idea is to use ephemeral identities under a reliable, per-manent identity. The permanent identity is trusted by users; from there, different identities may be provided on demand to other content publishers, without revealing which one is signing the content.

由于内容审查的可能性，隐私也是内容发布者所关注的问题，主要是因为内容名称可能包含发布者（生产者）标识。尽管审查不应由网络本身来处理，但ICN的行为可能会帮助审查。因此，讨论此类威胁非常重要。Acs等人提出了一套预防措施，以避免对内容发布者进行监视和审查。[2] ，例如使用组签名、环签名和确认签名，这些签名允许用户验证内容的签名是否有效，但不具体标识已由哪个发布者签名，从而保证内容发布者的匿名性。另一个想法是在可靠的永久身份下使用短暂身份。永久身份受用户信任；这样的话，可以根据需要向其他内容发布者提供不同的身份，而无需透露谁在对内容进行签名。

3.3 Content Secrecy

3.3 内容保密性

The enforcement of access control policies to protect content secrecy in ICN is a great concern, especially due to the in-network caching infrastructure proposed by the ICN paradigm [52, 73]. As the retrieved content is cached along the way by unreliable entities such as routers, mobile devices, or third-party servers as in a CDN-like infrastructure, content publishers face problems to manage and enforce access control to their content. This problem is even more concerning when consid-ering paid or copyrighted content, since cached copies of protected content may be accessed by users that do not have an account/subscription for it. Any user, despite her computational power, can retrieve unauthorized content from caches, since they do not validate access from users before replying. Figure 5 introduces a basic unauthorized access scenario, as U1 retrieves a protected con-tent from router R4 cache, which was previously requested by the legitimate user U2. Restricting the name of the content only to authorized users is not enough, since routing and forwarding in ICN are carried out directly by the name of the content, therefore names can be easily discov-ered. Thus, this type of application requires a more robust and appropriate solution for use in ICN. Although access control problems are intrinsic to the ICN paradigm due to in-network caches, ma-licious entities may also benefit from traditional attacks used to gain access to protected content, such as Sybil attacks [84].

为了保护ICN中的内容保密性，访问控制策略的实施是一个值得关注的问题，特别是由于ICN范式提出的网络内缓存基础设施[52，73]。由于像CDN一样的基础架构中的路由器，移动设备或第三方服务器等不可靠的实体一路缓存了取回的内容，因此内容发布者面临着管理和控制其内容访问的问题。当考虑付费或受版权保护的内容时，此问题甚至更加令人担忧，因为没有帐户/订阅的用户可能会访问受保护内容的缓存副本。任何用户，无论其计算能力如何，都可以从缓存中取回未经授权的内容，因为内容发布者在回复之前不会验证用户访问权限。图5引入了一种基本的未经授权的访问方案，即U1从路由器R4缓存中取回了受保护的内容，该内容为合法用户U2先前曾请求过。仅将内容的名称限制为授权用户是不够的，因为ICN中的路由和转发是通过内容的名称直接执行的，因此名称很容易被发现。因此，这种类型的应用程序需要更鲁棒和合适的解决方案才能在ICN中使用。尽管由于存在网络内缓存，访问控制问题是ICN范式固有的，但恶意实体也可能会受益于用于获取受保护内容访问权限的传统攻击，例如女巫攻击[84]。

The basic action to maintain content secrecy in ICN is through content encryption, ensuring that only users having a valid key can access it [17, 49, 53, 72, 116, 130]. However, depending on the encryption solution adopted, encrypted content may stumble upon caching versus access control trade-offs, mainly because content encrypted for a specific user using traditional symmetric encryption may not be cacheable to other users, who would not be able to decrypt it [76, 95]. To

在ICN中维护内容保密的基本操作是通过内容加密，确保只有拥有有效密钥的用户才能访问它[17、49、53、72、116、130]。然而，根据所采用的加密解决方案，加密内容可能会在缓存与访问控制的权衡中被意外泄漏，这主要是因为使用传统对称加密为特定用户加密的内容可能无法缓存到无法解密的用户[76，95]。

circumvent that, special cryptographic mechanisms have being proposed for access control in ICN. Attribute-Based Encryption (ABE), for example, encrypts content for a group of users sharing common attributes, thus users are able to decrypt the content only if their key satisfies access control policies embedded in the ciphertext or in the key itself [52, 69, 70, 92]. In ABE schemes, the cached content can be shared among users in the same group. In the Broadcast Encryption (BE) model, content publishers encrypt the content with a unique symmetric key and distribute that symmetric key encrypted under the broadcast group public key. Each user in the broadcast group can decrypt the symmetric key using her individual private key. In the BE model, cached content can also be shared among users in the same broadcast group [49, 84, 94, 126]. However, if such solutions use the same key to encrypt content for a large group, key leakage may be a problem, as any user with the key can retrieve content, even unauthorized ones [78].

因此，针对ICN的访问控制问题，人们提出了一种特殊的密码机制。例如，基于属性的加密（ABE）为共享公共属性的一组用户加密内容，因此只有当其密钥满足嵌入在密文或密钥本身中的访问控制策略时，用户才能解密内容[52、69、70、92]。在ABE方案中，可以在同一组用户之间共享缓存内容。在广播加密（BE）模型中，内容发布者使用唯一的对称密钥对内容进行加密，并分发在广播组公共密钥下加密的对称密钥。广播组中的每个用户都可以使用其各自的私钥来解密对称密钥。在BE模型中，还可以在同一广播组的用户之间共享缓存内容[49、84、94、126]。然而，如果这样的解决方案使用相同的密钥来加密大型组的内容，则密钥泄漏可能是一个问题，因为任何具有密钥的用户都可以取回内容，甚至是未经授权的用户[78]。

Another cryptographic scheme explored is Proxy Re-Encryption (PRE) [11]. In PRE-based so-lutions, content items are encrypted with a symmetric key. The symmetric key is encrypted with the content publisher’s public key and, to recover the symmetric key, users must retrieve a re-encryption key with the content publisher [119]. A common problem of such solutions is the symmetric key disclosure. Once users have the symmetric key, they can access the cached con-tent, even if they are not authorized. A variation of PRE solution is to encrypt each content with a distinct private key from an asymmetric key pair; thus, content items can be shared by all users through caches, while the content public key, if disclosed, is valid only in conjunction with the cor-responding user’s public key [77]. Different strategies, such as mixing symmetric and asymmetric encryption techniques [49, 76, 104, 126] and building access control frameworks that can be used in conjunction with any encryption-based solution [47, 63], have also been explored in the context of ICN. However, recent research discussed that encryption-based solutions are not sufficient for content secrecy, mainly because it is easy for attackers to infer a content by its popularity, even if they are encrypted [42].

这里探索的另一种加密方案是代理重新加密（PRE）[11]。在基于PRE的解决方案中，内容项使用对称密钥加密。对称密钥使用内容发布者的公共密钥加密，并且要恢复对称密钥，用户必须使用内容发布者取回重新加密的密钥[119]。 这种解决方案的一个常见问题是对称密钥泄漏。用户拥有对称密钥后，即使未授权，他们也可以访问缓存内容。PRE解决方案的一种变体是使用来自非对称密钥对的独特私钥来加密每个内容。因此，所有用户都可以通过缓存共享内容项，而内容公开密钥（如果公开）仅与相应用户的公开密钥结合使用才有效[77]。在ICN上下文中还探索了不同的策略，例如混合使用对称和非对称加密技术[49、76、104、126]和构建可与任何基于加密的解决方案结合使用的访问控制框架[47、63]。 但是，最近的研究讨论了基于加密的解决方案不足以实现内容保密，这主要是因为即使内容经过加密，攻击者也很容易通过其流行度来推断内容[42]。

Apart from encryption-based solutions, researchers also proposed alternative infrastructure-based solutions, such as using authorization servers for validating policies [31, 32, 36, 102]. One problem of such solutions is that they often assume that content custodians (e.g., caches) validate access policies before sending the content to users. These assumptions may be hard to ensure on the Internet environment, for some reasons. Access control decisions involve evaluating rules defined on users and contents. For a cache to validate an access request, it needs to evaluate access control rules defined by the content publisher for that content and that user. This means that each cache should be provisioned (and updated) with the access rules for all contents it may store and all users it may serve, which is not scalable. Otherwise, caches may outsource the access decisions to authorization servers that know all rules, thus adding extra latency to every content request. The use of access lists is also considered [15, 44]; however, it is more suitable for controlled environments such as sensor networks at small places rather than the Internet. Another idea is to use levels of access directly on routers, such that routers are able to cache only content items which the publisher authorizes to [71]. Such solution assumes that the router operating system is modified to comply with access rules attached to content items and enforced by the router itself on forwarding and caching process. This implies caches should be able to evaluate and apply the access rules defined by the content publishers, which demands more processing for each request. Furthermore, this also imposes a common access control schema in the entire network for all publishers and caches.

除了基于加密的解决方案之外，研究人员还提出了基于基础架构的替代解决方案，例如使用授权服务器来验证策略[31、32、36、102]。这种解决方案的一个问题是，它们通常假定内容保管者（例如，缓存）在将内容发送给用户之前验证访问策略。出于某些原因，这些假设可能很难在互联网环境中得到保证。访问控制决策涉及对用户和内容定义的规则进行评估。要使缓存验证访问请求，它需要评估内容发布者为该内容和该用户定义的访问控制规则。这意味着应该为每个缓存提供（并更新）针对其可能存储的所有内容以及它可能服务的所有用户的访问规则，这是不可扩展的。否则，缓存可能会将访问决策外包给知道所有规则的授权服务器，从而给每个内容请求增加了额外的延迟。访问列表也在考虑使用范围内[15、44]；但是，它更适用于受控环境，例如小地方的传感器网络，而不是互联网。另一个想法是直接在路由器上使用访问级别，以使路由器仅能缓存发布者授权的内容项[71]。这种解决方案假定修改路由器操作系统，以遵守附加到内容项的访问规则，并由路由器本身在转发和缓存过程中强制实施。这意味着缓存应能够评估和应用内容发布者定义的访问规则，这就需要对每个请求进行更多处理。此外，这还为所有发布者和缓存在整个网络中设置了一个通用的访问控制模式。

Another face of access control is the use of firewalls considering ICN characteristics to support network administration. This can be used, for example, to enforce local security policies. Firewall rules are implemented in terms of blocking content by name or by publisher. If a certain publisher becomes malicious, rules could be implemented to avoid content from such publisher to reach the

访问控制的另一面是使用考虑了ICN特性的防火墙来支持网络管理。 例如，这可用于实施本地安全策略。根据按名称或按发布者阻止内容的方式实施防火墙规则。如果某个发布者变得恶意，则可以实施规则来避免来自该发布者的内容到达网络。

network. Also, content could be checked against keywords for filtering purposes. Furthermore, as each content must be signed by its publisher, the firewall could be configured to ignore content with invalid signatures, for instance [44].

此外，可以根据关键字检查内容以进行筛选。此外，由于每个内容都必须由其发布者签名，因此可以将防火墙配置为忽略具有无效签名的内容，例如[44]。

Table 1 presents the compilation of works addressing attacks and countermeasures on content security for ICN.

表1汇编了针对ICN内容安全方面的攻击和对策的著作。

4SECURITY IN ROUTERS

4路由安全

Routers perform essential services for the core of the network layer, as routing and forwarding. Besides managing and updating all routing information, it takes care of finding content in the network, forwarding requests and content back to the requestor.routing information. As the ICN paradigm brings new features to the network layer, new threats in routers functions also arise, mostly due to forwarding based by names directly in the network layer. However, even known attacks as denial of service may hamper ICN forwarding. We categorize routers attacks in ICN in three groups: resource exhaustion, publisher unavailability, and route depletion. Resource exhaus-tion attacks comprise malicious entities that demand routers unnecessary computations. Publisher unavailability groups attacks targeting content publishers to limit or stop the content distribution. At last, route depletion attacks aim to disrupt routing paths, e.g., by advertising invalid routes. In this section, we detail each of these groups.

路由器为网络层的核心执行基本服务，例如路由和转发。除了管理和更新所有路由信息外，它还负责查找网络中的内容，将请求和内容转发回请求者的路由信息中。随着ICN模式给网络层带来了新的特性，路由器功能也面临新的威胁，这主要是由于直接在网络层根据名称进行转发。但是，即使是已知的拒绝服务攻击也可能会阻碍ICN转发。我们将ICN中的路由器攻击分为三类：资源耗尽，发布者不可用和路由消耗。资源耗尽攻击包括恶意实体，这些恶意实体要求路由器进行不必要的计算。发布者不可用针对目标内容发布者进行攻击，以限制或停止内容分发。最后，路由耗尽攻击的目的是破坏路由路径，例如通过发布无效路由。在本节中，我们将详细介绍每个组。

4.1 Resource Exhaustion

4.1 资源耗尽

To be able to forward the content back to the requestor, ICN architectures based on stateful routing, like NDN/CCN, demand routers to keep record of received and forwarded requests per interface, until the request is consumed, either by the content traversing the path back or by timeout expi-ration. This mechanism is pointed out as potentially vulnerable to Denial of Service (DoS) attacks aiming to disrupt forwarding service for legitimate users or to overload the network and disable it. The exploitation of this vulnerability has been extensively addressed in the literature, and can be effectively issued by any user in the network. For example, a malicious user or a set of collud-ing users could explore the stateful nature of routing in ICN by issuing an excessive number of requests, consequently depleting the available memory for pending requests entries and denying

为了能够将内容转发回请求者，基于状态路由的ICN体系结构（如NDN/CCN）要求路由器记录每个接口接收和转发的请求，直到请求被消耗为止，无论是通过遍历内容后返回还是通过超时到期。该机制可能容易受到拒绝服务（DoS）攻击，这些攻击旨在中断合法用户的转发服务，或使网络过载并禁用它。该漏洞的利用已在文献中得到了广泛解决，并且可以由网络中的任何用户有效地发布。例如，恶意用户或一组串通用户可以通过发出过多的请求来探索ICN中路由的状态性质，从而耗尽挂起请求进入的可用内存并拒绝

Fig. 6. Resource exhaustion threat in ICN.

图6. ICN中的资源耗尽威胁。

service for legitimate users. Whether the router employs a rate limit for pending requests entries is indifferent, as it is simple for malicious users to exceed this limit [112]. However, since requests entries for the same content are aggregated for performance, this attack is ineffective or minimized if the malicious user sends a burst of requests for the same content, even in a distributed way. To disable this natural defense, malicious users should issue an excessive amount of bogus requests in order to fill the pending request table with forged entries, thus causing legitimate requests to be dropped [3, 18, 21, 23, 28, 34, 59, 110, 112]. Such attacks would be much more aggressive and difficult to detect with distributed attackers working simultaneously [43], as depicted in Figure 6. In this example, U1 and U2 together are exhausting resources from router R4, which may not be available to accept any more requests due to the amount of requests in its pending request records.

为合法用户提供服务。路由器是否对挂起请求进入采用速率限制并不重要，因为恶意用户很容易超过此限制[112]。但是，自从相同内容的请求进入被聚集用于提高性能以来，如果恶意用户对相同内容发送一系列相同的请求（即使是以分布式方式），则此攻击无效或效果最小化。要禁用这种自然防御，恶意用户会发出过多的虚假请求，以便用伪造的进入填充挂起的请求表，从而导致合法请求被丢弃[3，18，21，23，28，34，59， 110，112]。如果分布式攻击者同时工作[43]，这种攻击将更具攻击性且难以检测，如图6所示。在这个例子中，U1和U2一起耗尽来自路由器R4的资源，由于其挂起的请求记录中的请求量，路由器R4可能无法接受任何更多的请求。

All these flooding attacks have a common consequence: They cause pending request entries to expire. To avoid this characteristic from being explored in countermeasures for flooding attacks, the user may collude with a malicious content publisher to avoid the detection of excessive requests being expired [65, 111, 114]. In this case, the malicious publisher replies forged requests right before the pending request entry timeout expires, causing the router to believe in a chan-nel congestion. As a consequence, re-transmissions are triggered, amplifying the damage. These attacks can also be explored by two subverted routers slowing down content forwarding, forcing pending request entries in other routers to expire before content delivery is complete, thus causing re-transmissions storms [111].

所有这些洪泛攻击都有一个共同的后果：他们导致挂起请求进入过期。恶意用户为了避免针对洪泛攻击的对策探索到此特性，该用户可以与恶意内容发布者串通，以避免过多的已过期请求被检测到[65、111、114]。在这种情况下，恶意发布者会在未决请求输入超时到期之前立即回复伪造的请求，从而使路由器相信通道拥塞。因此这会触发重新传输，加大损害程度。恶意用户还可以通过两个被破坏的路由器来减慢内容转发的速度，从而迫使其他路由器中待处理的请求条目在内容传递完成之前到期，从而引起重传风暴[111]。

The first attempts to mitigate flooding attacks in ICN suggest the use of hash functions on pending request tables to save storage or always accepting a new request, dropping the oldest ones [65]. However, these are simple ideas that may delay attack consequences but not avoid them. More sophisticated solutions are based on monitoring and identifying unusual amounts of requests in routers [89]. For example, routers may monitor unsatisfied requests rate [7–9, 30, 34, 43, 56, 58, 59], the amount of entries on the pending request table [21], or the amount of requests on each interface [3, 88]. Thus, in case routers identify abnormal amounts of requests for distinct content items in the same interface, they can limit the amount of accepted requests from such interface, possibly minimizing the consequences of flooding while allowing legitimate requests from this interface to have a fair chance of being satisfied. Some solutions allow these results to be shared among routers, thus helping other routers to avoid or to recover from flooding attacks [43, 116].

对此，减轻ICN泛洪攻击的首要选择是在挂起请求表上使用哈希函数以节省存储空间或始终接受新请求，从而丢弃最旧的请求[65]。然而，这些简单的想法只可能延迟攻击后果，但不能予以避免。更复杂的解决方案则是基于监测和识别路由器中异常数量的请求[89]。例如，路由器可以监视未满足的请求率[7-9、30、34、43、56、58、59]，挂起请求表中的进入数量[21]或每个接口上的请求数量[3] ，88]。因此，如果路由器在同一接口中识别出针对不同内容项的异常请求数量，则它们可以限制来自该接口的已接受请求数量，从而可以最大程度地减少洪泛带来的后果，同时允许来自该接口的合法请求有很大机会得到满足。一些解决方案允许这些结果在路由器之间共享，从而帮助其他路由器避免洪泛攻击或从洪泛攻击中恢复[43，116]。

Interest NACK (non-acknowledgement) packets can also be used to avoid routers to wait for malicious Interests timeout expiration. Using NACKs, routers can satisfy requests in routers, thus freeing PIT from malicious entries, if it is the case [122]. Also, routers may respond to suspicious requests to clean pending requests table on the way back to the malicious user, minimizing the impact of such attacks [23]. Another solution would be to adopt authenticated requests as a mean for routers to identify malicious users who issue an excessive amount of requests [15]. Also,

Interest NACK (non-acknowledgement) 数据包也可用于避免路由器等待恶意Interest超时过期。如果是这种情况，NACK使路由器可以满足路由器中的请求，从而可以将PIT从恶意进入中释放出来[122]。同样，路由器可能会响应可疑请求，以清除返回到恶意用户的挂起请求表，从而将此类攻击的影响降到最低[23]。另一种解决方案是将经过验证的请求作为一种手段使路由器识别发出过多请求的恶意用户[15]。

Fig. 7. Publisher unavailability threat in ICN.

图7. ICN中的发布者不可用威胁。

adopting an ICN architecture based on stateless forwarding would decouple malicious entries from PIT [40, 115].

而且，采用基于无状态转发的ICN架构将使恶意条目与PIT分离[40，115]。

4.2 Publisher Unavailability

4.2 发布者不可用

Just as sending excessive requests disrupts routing service for legitimate users, concentrating re-quests toward a unique publisher or a specific name space could also disable this entire name space or publisher, such as in the traditional IP network DoS attack. The most basic way of saturating the victim resources and making content unreachable for legitimate users is by sending a large amount of requests for the same content publisher, in which malicious users collude to flood the network with requests toward the same victim server [34, 65], as illustrated in Figure 7. This attack requires a substantial amount of requests toward the same publisher to be effective; how-ever, it does not require a significant amount of computational power from attackers, since the coordination of a group of users could be enough to deploy it.

就像发送过多的请求会破坏合法用户的路由服务一样，集中向唯一发布者或特定命名空间发送请求也可能会禁用整个命名空间或发布者，例如在传统IP网络DoS攻击中。使受害者资源饱和并使合法用户无法访问内容的最基本方式是向同一个内容发布者发送大量请求，其中恶意用户串通，向同一受害者服务器发送大量请求，从而使网络洪泛[34，65]，如图7所示。这种攻击需要针对同一发布者的大量请求生效才能实现；但是它不需要攻击者大量的计算能力，因为一组用户的协调就足以部署它。

However, targeting this kind of attack in an ICN infrastructure needs some special preparation by the malicious users. For example, they need to make sure that the content is not satisfied by any cache on the path, as well as that content requests are routed toward the victim and that each request creates new pending request table entries in routers. To subvert such adversities, malicious users could send bogus data requests with the same prefix, inducing the routing mechanism to forward the request toward the prefix publisher, while preventing content to be found in cache [3, 21, 34, 113]. Due to the nature of these attacks, monitoring solutions used to mitigate flooding attacks can also be applied for these cases. Specifically against publisher unavailability attacks, routers could adopt metrics such as monitoring the amount of requests for the same content pub-lishers, and reducing the requests forwarded to this prefix [65], avoiding that malicious requests overwhelm the content publisher.

但是，在ICN基础结构中针对这种攻击需要恶意用户进行一些特殊的准备。例如，他们需要确保路径上的任何缓存都不满足内容，并且必须将内容请求路由到受害者，且每个请求都在路由器中创建新的挂起请求表条目。为了解除这种不利条件，恶意用户可以发送具有相同前缀的虚假数据请求，诱导路由机制将请求转发给前缀发布者，同时防止在缓存中找到内容[3、21、34、113]。由于这些攻击的性质，用于缓解洪泛攻击的监视解决方案也可以应用于这些情况。特别是针对发布者不可用攻击，路由器可以采用诸如监视相同内容发布者的请求量、减少转发到此前缀的请求[65]等指标，避免恶意请求压倒内容发布者。

4.3 Route Depletion

4.3 路由耗尽

To correctly forward content requests toward publishers or available cached copies, each router needs to maintain its Forwarding Information Base (FIB) updated and free of malicious entries. Threats against FIB could potentially let legitimate domains unreachable or allow malicious users to redirect routes to malicious content or routers for monitoring purposes. This attack demands that attackers have access to route announcements; thus, it requires the subversion of routers or content publishers. Malicious content publishers could announce numerous malicious con-tent belonging to different domains, until the table is full and unable to register valid content from legitimate domains [43]. They could also announce content at a rate extrapolating the route update convergence time, causing problems with incorrect information about cached con-tent, misleading routes, and even opening security gaps for others attacks [111]. Alternatively, a

为了正确地向发布者或可用的缓存副本转发内容请求，每个路由器都需要维护其转发信息库（FIB）的更新，并且防止恶意条目。针对FIB的威胁可能会使合法域无法访问，或使恶意用户将路由重定向到恶意内容或路由器以进行监视。因为此攻击要求攻击者能够访问路由通告；所以攻击者需要破坏路由器或内容发布者。恶意内容发布者可能会发布属于不同域的众多恶意内容，直到该表已满并且无法注册来自合法域的有效内容[43]。他们还可能以推断出的路由更新收敛时间的速度发布内容，从而导致一些问题包括：有关缓存内容的信息不正确，误导路由，甚至为其他攻击打开安全漏洞[111]。

Fig. 8. Route depletion threat in ICN.

图8. ICN中的路由耗尽威胁

malicious router could announce valid content to the network and when asked for content retrieval, to delay the reply or even do not reply, causing a disruption in services for users [34, 73, 112]. This attack is worsened if several malicious routers collude to announce routes to popular content and then delay replies [111]. Figure 8 depicts a scenario where router R2 announces routes to /S1/ content items, however, instead of forwarding the requests to /S1/, it simple discards re-quests making pending requests in previous routers to expire.

或者，恶意路由器可能会向网络发布有效内容，并在请求内容取回时延迟回复甚至不回复，从而导致用户服务中断[34、73、112]。如果几个恶意路由器串通向流行内容发布路由，然后延迟回复，则这种攻击会更加严重[111]。图8描绘了一个场景，其中路由器R2发布了到达/ S1 /内容项的路线，但是，它并未将请求转发到/ S1 /，而是简单地丢弃了请求，使先前路由器中的挂起请求过期。

Routing information entries can also be threatened by passive monitoring, since a malicious router can announce routes to many content items, but does not keep all of them in its cache. The goal here is to intercept any request for such content and then forward it to the correct location. As the user is not directly affected by this attack, the attacker can monitor requested content in the network without been noticed [111]. This attack could be more dangerous when considering a collaborative network, such as mobile ad hoc networks, in which user devices are naturally placed as routers to forward packets.

路由信息条目也可能受到被动监视的威胁，因为恶意路由器可以发布到许多内容项的路由，但不会将所有内容项都保留在其缓存中。这里的目标是拦截对此类内容的任何请求，然后将其转发到正确的位置。由于用户不受此攻击的直接影响，因此攻击者可以监视网络中请求的内容，而不会被注意到[111]。在考虑协作网络（例如移动自组网）时，这种攻击可能会更加危险，在协作网络中，用户设备自然会放置为路由器来转发数据包。在考虑协作网络（如移动自组网）时，这种攻击可能更危险，在这种网络中，用户设备自然地被作为路由器来转发数据包。

Gasti et al. [34] argue that the NDN/CCN architecture is natively resilient against prefix hi-jacking attacks mainly because routing updates are signed, thus verifiable, preventing malicious users to register fake routes. However, this countermeasure does not apply in face of malicious routers having valid cryptographic keys, accepted and validated by other routers. Furthermore, a network facing such attack could benefit from monitoring for anomalous behavior, similar to solutions applied to request flooding attacks. Also, route hijacking could be subverted by multiple routes toward the victim content, though it would not be effective if attackers collude and attack the publisher in a distributed way [111]. Finally, Lauinger [65] gives some suggestions to prevent the misuse of special bits in request packets, as to limit the use of such bits, like allowing the use of scope field only on local requests, or requiring a digital signature for requests wishing to set the scope field, thus exposing the identification of the attacker.

加斯提等人[34]认为NDN / CCN架构本身具有抵御前缀劫持攻击的能力，这主要是因为路由更新已签名，因此可验证，从而防止了恶意用户注册虚假路由。然而，此对策不适用于具有有效加密密钥且被其他路由器接受和验证的恶意路由器。此外，面对这种攻击的网络可以借鉴监测异常行为的方案，这与应对请求洪泛攻击的解决方案类似。同样，路径劫持可能会被通向受害内容的多条路径破坏，但如果攻击者以分布式方式串通和攻击发布者则方法不会有效[111]。最后，Lauinger[65]提出了一些建议，以防止在请求包中误用特殊位，从而限制此类位的使用，例如只允许在本地请求上使用scope字段，或者对希望设置scope字段的请求要求数字签名，从而暴露攻击者的身份。

Table 2 provides a compilation on attacks and countermeasures in ICN routing aspects, together with the vulnerabilities they explore and the targeted entity.

表2汇总了ICN路由方面的攻击和对策，以及他们探索的漏洞和目标实体。

5SECURITY IN CACHING

5缓存安全

The caching mechanism is one of the most prominent features of ICN architectures. It aims to improve content distribution in the network, by placing content copies near users; this alleviates congestion and latency problems, specially for popular content, like video streaming. There is a well-known set of threats against cache systems in traditional networks. However, in ICN architec-tures these threats are amplified, as they scale globally to the Internet: malicious network entities (publishers and routers) can announce, update, and distribute malicious content that could be very difficult to detect.

缓存机制是ICN体系结构最突出的特征之一。它旨在通过将内容副本放置在用户附近来改善网络中的内容分发；这缓解了拥塞和延迟问题，特别是对于流行内容（例如视频流）而言。在传统的网络中，有一组众所周知的对缓存系统的威胁。然而，在ICN架构中，这些威胁被放大，因为它们在全球范围内扩展到互联网：恶意网络实体（发布者和路由器）可以发布、更新和分发可能很难检测到的恶意内容。

Route interception

路由拦截

Routing misuse

路由滥用

We organize attacks and countermeasures for caching attacks in ICN in three groups: cache snooping, cache pollution, and cache poisoning. Cache snooping attacks comprise malicious users aiming to profile user behavior on the Internet by analyzing content items stored in caches. Cache pollution groups attacks whose goals are to fill caches with unpopular or irrelevant content rather than popular content, making caches ineffective. Finally, cache poisoning differs from previous group by tackling attacks aiming to populate caches with illegal, fake, or forged content. This section lists the attacks that have been explored in literature regarding cache systems for ICN as well as solutions to mitigate them. Since great attention has been given to mitigate caching attacks in ICN, due to the extensive knowledge about caching in traditional networks, there are plentiful solutions.

我们将攻击和针对ICN中的缓存攻击的对策分为三类：缓存侦听，缓存污染和缓存中毒。缓存监听攻击指恶意用户旨在通过分析存储在缓存中的内容项来侧写互联网上的用户行为。缓存污染组攻击的目的是用不流行或无关的内容而不是流行的内容填充缓存，从而使缓存无效。最后，缓存中毒与前面一类有所不同，它针对旨在用非法，虚假或伪造内容填充缓存的攻击。本节列出了有关ICN缓存系统的文献中探讨的攻击以及缓解这些攻击的解决方案。由于对传统网络中缓存技术的广泛了解，在ICN中如何减少缓存攻击受到了广泛的关注，因此有很多解决方案。

5.1 Cache Snooping

5.1 缓存侦听

One of the most interesting cache policies used in ICN is storing content based on content popular-ity and relevance for nearby users. However, this policy makes the cache a relevant representative of information about users’ interest on the Internet, which can be explored to obtain sensitive information about a user or a group of users [83]. Although these attacks can be launched by users in general as it does not require much computational power, content publishers may better benefit from snooping caches to infer users’ behavior. Even though it is difficult to pinpoint the behavior of a specific user, content publishers may use snooping to infer preferences for users in a region and use it for advertisement, for example. Also, government agencies may use snooping for

ICN中使用的最有趣的缓存策略之一是根据内容的流行度和与附近用户的相关性来存储内容。但是，此策略使缓存成为有关互联网上用户兴趣信息的相关代表，可以利用它来获取有关用户或用户组的敏感信息[83]。尽管这些攻击通常不需要大量的计算能力即可由用户发起，但内容发布者可能会更好地受益于侦听缓存以推断用户的行为。例如，即使很难查明特定用户的行为，内容发布者也可以使用侦听功能来推断区域内用户的偏好并将其用于广告。此外，政府机构可能会利用侦听来

Fig. 9. Cache snooping threat in ICN.

图9. ICN中的缓存侦听威胁。

monitoring and blocking specific content. Malicious users closer to victims (e.g., in the same access router) pose an even greater risk for users’ privacy, as they share the same cache with fewer users, facilitating snoopers’ actions [91]. The snooper is able to list cached content, monitor content access, and even copy conversations [65], as shown in Figure 9, where user U1 snoops into router R4 for content items stored in cache, retrieving a copy of the content previously requested by user U2.

监视和阻止特定内容。距离受害者较近的恶意用户（例如，在同一访问路由器中）对用户的隐私构成更大的风险，因为他们与更少的用户共享同一缓存，从而有助于窥探行为[91]。侦听者能够列出缓存的内容，监视内容访问甚至复制对话[65]，如图9所示，其中用户U1侦听路由器R4中存储在缓存中的内容项，从而取回先前由用户U2请求的内容副本。

Strategies for cache snooping include cache probing by monitoring a content name and request-ing a specific content name until it is returned by the cache and by requesting random names to the cache, excluding those already obtained in subsequent requests. One particularly worrisome aspect, specific for the NDN/CCN architecture, is the exclude field [53], since it could be used to limit a query specifically to the first cache in the path2; if a content item is retrieved by the snooper from a specific cache, then a user under that cache has recently retrieved that content [65]. These threats are more worrisome when considering on-path caches, since they are traditionally based on routers and represent users’ behavior with more accuracy. Besides considering malicious en-tities that inspect caches to infer users’ behavior, privacy invasion attacks [73] also consider malicious content publishers that leak users’ sensitive information, although this is not a threat exclusive to ICN or under control of ICN architectures.

缓存侦听的策略包括通过监视内容名称并请求特定内容名称直到缓存将其返回为止，并通过向缓存请求随机名称（不包括在后续请求中已获得的随机名称）来进行缓存探测。对于NDN / CCN体系结构而言，一个特别令人担忧的方面是排除字段[53]，因为它可以将查询专门限制于path2中的第一个缓存。如果侦听者从特定的缓存中检索到内容项，则该缓存下的用户最近检索了该内容[65]。对于路径缓存，这些威胁更令人担忧，因为其传统上基于路由器所以可以更准确地表示用户行为。除了那些检查缓存以推断用户行为的恶意实体之外，泄漏用户敏感信息的恶意内容发布者也造成隐私入侵攻击[73]，尽管这种威胁不是ICN独有的，也不是在ICN体系结构控制之下的。

Another approach to infer whether a given content is in a cache and, consequently, if a nearby user accessed such content recently is through the time difference between replies from nearby caches and from the publisher [16, 86]. A malicious user can issue probes to the cache in order to measure its Round-Trip Time (RTT). Then, it issues a request for the content it aims to monitor and also measures its RTT. By analyzing both RTTs, the malicious user infers whether the content was retrieved from the cache or from anywhere else [65]. This strategy can also be used to infer if a publisher produced some specific content lately by probing the publisher to discover its RTT and then requesting the monitored content. If the RTT from the second request is lower than the first one, it is safe to deduce that such content was recently made available by the publisher for some user and was stored in the cache of some router. Although this attack is feasible and poses a threat against user privacy and anonymity, it is consensus that correlating a specific user with a content in cache is not trivial and may require additional information [2].

另一种推断给定内容是否在缓存中，以及由此推断最近是否有附近的用户访问了此类内容的方法是通过附近缓存和发布者的回复之间的时差[16，86]。恶意用户可以对缓存发出探测，以测量其往返时间（RTT）。然后，它发出对要监视的内容的请求，并测量其RTT。通过分析这两个RTT，恶意用户可以推断内容是从缓存还是从其他地方检索的[65]。此策略还可用于通过探测发布者以发现其RTT，然后请求监视的内容来推断发布者最近是否生成了某些特定内容。如果来自第二个请求的RTT低于第一个请求，则可以推断出该内容最近已由发布者提供给某些用户使用，并已存储在某个路由器的缓存中。尽管这种攻击是可行的，并对用户隐私和其匿名性构成威胁，但人们一致认为，将特定用户与缓存中的内容关联起来并不容易，可能需要额外的信息[2]。

Such attacks pose a greater privacy risk if governments or industries make efforts to spy users and disclose their content access privacy and anonymity by monitoring content requests. This is a fundamental concern for ICN architecture, since the network is aware of content items traveling over it. It can be even worse if routers are able to semantically interpret content names, since

如果政府或行业通过监视内容请求来监视用户并泄露其内容访问的隐私及匿名信息，则此类攻击将带来更大的隐私风险。这是ICN架构的基本问题，因为网络知道在其上传输的内容项。如果路由器能够在语义上解释内容命名，则情况会更加恶化，因为

2Due to this and other concerns, the exclude field is being removed from the current NDN protocol specification (0.3 at this time) [87].

2由于这个和其他问题，排除字段已从当前的NDN协议规范中删除（此时为0.3）[87]。

censorship and monitoring by malicious ISPs, governments, and industries would be much easier. In contrast to deep packet inspection tools in traditional networks, in which the snooper is required to be strategically located and powerful enough to inspect packets at line speed, the cache in ICN architectures allows snoopers to retrieve information on a longer time window [16]. However, correlating users and cached copies is not trivial and may require additional information.

政府和行业通过恶意ISPs进行审查和监视会更加容易。与传统网络中的深层数据包检查工具不同，在传统网络中，侦听器必须战略定位并且功能强大，可以以线速检查数据包，而在ICN体系结构中的缓存则可以使侦听器在更长的时间窗口上取回信息[16]。但是，关联用户和缓存副本并非易事，可能需要其他信息。

As the first countermeasures to tackle cache snooping attacks in ICN paradigm, a set of possi-ble preventive actions were proposed to alleviate the vulnerabilities in ICN for such attack, such as the restriction of content name parts in which the user could use the exclude field and the longest prefix matching, thus setting which part of the name content the user must have prior knowledge to request it [65, 66]. Also, disabling or limiting the use of the exclude field in request packets could prevent malicious users from restricting their search to local caches, where the threat is amplified. Besides prevention, detection actions like monitoring events such as un-usual requests from the same link in a very short time window at a very high hit rate is also an alternative [91].

作为解决ICN范式中缓存侦听攻击的第一个对策，人们针对此类攻击提出了一组可能的预防措施来减少ICN中的漏洞，如限制在其中用户可以使用排除字段和最长前缀匹配的内容命名部分，从而设置用户必须事先知道才能请求的命名内容部分[65，66]。同样，禁用或限制在请求数据包中使用排除字段可以防止恶意用户将其搜索限制在本地缓存中，因为在本地缓存中威胁会更大。除了预防之外，在很短的时间窗口内以很高的命中率监视来自同一链接的异常请求等检测操作也是一种替代方法[91]。

In face of timing-based cache snooping, the basic strategy is to delay replies from caches in order to equalize response times, thus avoiding malicious users to infer cached content by timing differences between content retrieved from publishers and caches [16, 65, 85, 86]. Another idea is to count how many times a user requests the same content; a request from the same user is replied directly from the cache and for different users the timing delay is applied, based on the number of hops from the publisher to the user. The use of collaborative caches can be used to undermine timing attacks, since routers cache content items based on internal state, like available storage, and their position in the forwarding path. Thus, it would be much harder for the malicious user to infer whether the retrieved content was in cache or not.

面对基于时间的缓存侦听，基本策略是延迟来自缓存的回复以便均衡响应时间，从而避免恶意用户通过测定从发布者和缓存检索的内容之间的时间差来推断缓存的内容[16、65、85， 86]。另一个想法是计算用户请求相同内容的次数。来自同一个用户的请求直接从缓存中得到回复，并且对于不同的用户，将根据从发布者到用户的跳数应用定时延迟。由于路由器基于内部状态（如可用存储）及其在转发路径中的位置来缓存内容项，因此可以使用协作式缓存来破坏定时攻击。因此，恶意用户很难推断取回的内容是否在缓存中。

In order to avoid malicious users from snooping content produced by point-to-point conversa-tions, the main idea is to turn content names unpredictable, e.g., by using ephemeral names, by tunneling requests, or by appending a random component to the content name [2]. This random component needs to be agreed between communicating parties. They choose and securely share a secret seed and use it to create and request content. Thus, content name is only known by the two communicating parties, preventing malicious users to probe the cache. Also, hiding content names from the network may help to avoid malicious users from inferring which content items are relevant for users; however, increased privacy comes in detriment of performance [83].

为了避免恶意用户侦听由点对点对话产生的内容，主要想法是使内容命名变得不可预测，例如，通过使用临时名称，通过通道请求或将随机组件添加到内容命名中[2]。通信双方须对这种随机组件达成一致。他们选择并安全地共享一个秘密种子，并使用它来创建和请求内容。因此，内容命名仅由两个通信方知道，从而防止恶意用户探测缓存。此外，向网络隐藏内容名称可能有助于避免恶意用户推断哪些内容项与用户相关；然而，隐私性的加强会损害性能[83]。

5.2 Cache Pollution

5.2 缓存污染

As populating caches in ICN architectures may depend on users’ access pattern, it also raises the possibility of malicious users to populate the cache with uninteresting content, thus disrupting the performance gain brought by caches. Moreover, all users could potentially serve as caches to the network, as in mobile networks in which all nodes are potentially engaged on routing and forwarding tasks, meaning they have unconditional control over their cached content and cache access. A cache pollution attack [43] is non-intrusive in the sense that malicious users’ interac-tions appear like normal interactions. For example, malicious users could request a large amount of unpopular content in order to disrupt content locality and degrade cache efficiency [22, 65, 120]. On-path caching is more vulnerable to such attack, since routers have limited memory for caching purposes; if irrelevant content items are cached, more requests for valid content will be forwarded to the content publisher. On the other hand, to pollute off-path caches, the attack has to be ampli-fied by colluding a large amount of users to maximize the amount of requests to unpopular content and fake popular interest. Figure 10 illustrates two users, U1 and U3, colluding to pollute caches be-tween them. In this scenario, U3 requests unpopular content from U1, leaving a cached copy of this uninteresting content on caches of R4 and R3, which may displace a legitimate popular content.

由于在ICN体系结构中填充缓存可能取决于用户的访问模式，因此还增加了恶意用户用不感兴趣的内容填充缓存的可能性，从而破坏了缓存带来的性能增益。此外，所有用户都可能充当网络的缓存，就像在移动网络中，其中所有节点都可能从事路由和转发任务一样，这意味着他们对其缓存内容和缓存访问具有无条件控制权。缓存污染攻击[43]是非侵入性的，即恶意用户的交互看起来像正常的交互。例如，恶意用户可能会请求大量非主流内容，以破坏内容的位置并降低缓存效率[22、65、120]。路径缓存更容易受到这种攻击，因为路由器的缓存内存有限。如果缓存了不相关的内容项，则内容发布者将收到更多对有效内容的请求。另一方面，恶意用户要污染路径外缓存，必须通过勾结大量用户来扩大攻击，以最大程度地增加对非主流内容和伪造的公众兴趣的请求量。图10说明了两个用户U1和U3串通污染他们之间的缓存。在这种情况下，U3向U1请求非主流的内容，而在R4和R3的缓存中保留此无用内容的缓存副本，这可能会取代合法的主流内容。

Fig. 10. Cache pollution threat in ICN.

图10. ICN中的缓存污染威胁。

Fig. 11. Cache poisoning threat in ICN.

图11.ICN中的缓存中毒威胁。

Monitoring content on caches is the most efficient solution for avoiding cache pollution [57, 121]. For example, the same monitoring mechanisms used for detecting and monitoring other at-tacks may be used to prevent cache pollution, since they already foresee cache monitoring metrics [22, 43, 120]. Specifically, the monitoring of incoming content requests to the same prefix in a short period is especially useful on monitoring cache pollution attacks [121].

监视缓存中的内容是避免缓存污染的最有效解决方案[57，121]。例如，用于检测和监视其他攻击的相同监视机制可用于防止缓存污染，因为它们已经预见了缓存监视度量[22、43、120]。具体来说，在短时间内对到相同前缀的传入内容请求进行监视对于监视缓存污染攻击十分有效[121]。

5.3 Cache Poisoning

5.3 缓存中毒

Cache poisoning attacks pose a serious threat to ICN architectures, since their main advantage is easy content production and distribution. A malicious user could populate its cache and satisfy legitimate requests with forged content, which will subsequently be cached along the forwarding path. Moreover, if the content name for a popular content could be anticipated, a malicious user could potentially produce fake content beforehand and collude with others to request this content, in order to spread it along the caches. Then routers with content in cache will deliver the fake content for legitimate requests when the original content becomes available and legitimate users start to request it [30, 34, 38, 73]. However, polluting caches is not trivial, may require additional preparation from attackers, such as subverting the routing system [68], and may require greater computational power, since they should spread fake content toward caches as much as possible. For example, Figure 11 exemplifies the case in which router R2 anticipates the name of a popular content; it produces and distributes the content for inadvertent users while populating caches with the forged content.

缓存中毒攻击严重威胁ICN架构，因为后者的主要优势是易于生产和分发内容。恶意用户可能会用伪造的内容填充缓存并使其满足合法请求，这些伪造内容随后将沿着转发路径进行缓存。而且，如果可以预期流行内容的内容命名，则恶意用户可能会事先生成假内容，并与其他恶意用户串通以请求此内容，以便将其沿缓存传播。然后，当原始内容可用且合法用户开始请求时，缓存中有内容的路由器将为合法请求传递假内容[30、34、38、73]。但是，污染缓存并非易事，可能需要攻击者做额外的准备，例如破坏路由系统[68]，并且可能需要更大的计算能力，因为它们应尽可能地向缓存传播假内容。例如，图11举例说明了路由器R2预期流行内容命名的情况。它为处在疏忽状态的用户生成和分发内容，同时用伪造的内容填充缓存。

Concerning fake content distribution, ICN relies on policies for cache content eviction or explicit exclusion of undesired content by users, which is usually not sufficient to avoid cache poisoning [38]. Having routers to verify all content items signatures before caching them is the natu-ral countermeasure, as it prevents the router to cache fake content. However, this may severely

关于虚假内容分发，ICN采取的策略是将缓存内容逐出或用户明确排除不想要的内容，这通常不足以避免缓存中毒[38]。对此，在缓存所有内容项签名之前让路由器验证签名是自然的对策，因为这可以防止路由器缓存假内容。但是，这可能严重

impact routing performance, as the router would need to check signatures for all incoming con-tent, and a trust mechanism should also be deployed (possibly application-specific). Alternatively, routers may verify signatures only when they are requested to serve content from their caches, preventing fake content to spread into other routers and the users [51]. Also, using information about content excluded from users requests would lead to the same problems: the router would need to authenticate the user to avoid that malicious users deliberately exclude valid content [39, 65]. Another approach to avoid cache poisoning consists in deploying blacklists with illegal con-tent names; routers can then deny their delivery and periodically re-validate cache entries with the content publishers [65]. However, more robust countermeasures seem necessary to effectively avoid fake content on caches.

影响路由性能，因为路由器需要检查所有传入内容的签名，还要在路由器上部署信任机制（可能特别针对申请）。或者，只有当请求路由器从其缓存中提供内容时，路由器才可以验证签名，以防止假内容扩散到其他路由器和用户[51]。此外，使用用户请求中排除的内容信息也会导致同样的问题：路由器需要对用户进行身份验证，以避免恶意用户故意排除有效内容[39，65]。另一种避免缓存中毒的方法是部署带有非法内容命名的黑名单；然后，路由器可以拒绝其传送，并定期与内容发布者重新验证缓存条目[65]。然而，为了有效地避免缓存上的假内容，似乎有必要采取更强有力的对策。

The basic approach of countermeasures to cache poisoning attacks is to check content prove-nance; for example, routers may accept to cache content items only if the incoming interface matches the outgoing interface in which the request was issued [51]. Assuming that users have means of knowing the content name beforehand, one solution is to include the hash of the static content as an alternative component in a content request [34]. Thereby, upon the reception of such content, the user could be sure the content is the right answer for her request. For dynamic content, the idea is to include the hash of the content publisher’s public key into the request; each intermediate router should check whether the returned content references the same public key. However, in this scenario, malicious users could collude with a malicious content publisher that signs every content with a distinct cryptographic key, forcing the router to ask for every key and consequently delaying content signature checking. Also, the malicious publisher could delay sending the key to the router and choose keys and signatures that require more computational resources to be verified. This scenario leads the router to deny services to legitimate users or even to stop verifying signatures, inducing a momentary security breach.

针对缓存中毒攻击的基本方法是检查内容来源。例如，仅当传入接口与发出请求的传出接口匹配时，路由器才能接受缓存内容项[51]。假设用户预先知道内容命名，一种解决方案是将静态内容哈希作为替代组件包含在内容请求中[34]。因此，在接收到这样的内容时，用户可以确定该内容是对于其请求的正确答案。 对于动态内容，其策略是将内容发布者的公钥的哈希包含在请求中；每个中间路由器应检查返回的内容是否引用了相同的公钥。但是，在这种情况下，恶意用户可能会与恶意内容发布者串通，后者使用不同的加密密钥对每个内容进行签名，从而迫使路由器询问每个密钥，从而延迟了内容签名检查。而且，恶意发布者可能会延迟将密钥发送到路由器，并选择需要更多计算资源进行验证的密钥和签名。这种情况导致路由器拒绝向合法用户提供服务，甚至停止验证签名，从而导致暂时的安全漏洞。

Routers could stop checking content signatures if the load become too high or, in case of facing a suspicious content publisher, to verify content signatures only when the router has enough free processing power [35, 37, 39]; however, it may lead to an unnecessary performance loss. Alterna-tively, they propose signature checks only if the content is stored long enough in cache [65]. Since in NDN/CCN data packets are signed, DiBenedetto and Papadopoulos [27] propose that end hosts report their routers about the bad data packets they detect. Each router then verifies the packet signature and, if needed, removes it from its cache, forwards the report upstream, and adjusts its forwarding strategies to avoid that content’s source.

如果负载过高，路由器可以停止检查内容签名，或者在面对可疑的内容发布者时，只有当路由器有足够的空闲处理能力时才验证内容签名[35、37、39]；但是，这可能会导致不必要的性能损失。或者，路由器仅当内容在缓存中存储足够长时间时才进行签名检查[65]。由于在NDN / CCN中对数据包进行了签名，因此DiBenedetto和Papadopoulos [27]建议终端主机向路由器报告其检测到的错误数据包。然后，每个路由器都会验证数据包签名，并在需要时将其从缓存中删除，并将报告转发到上游，调整其转发策略以屏蔽该内容的来源。

Table 3 lists the last part of security attacks and countermeasures for ICN, grouping attacks in ICN caching mechanisms and their corresponding category, target, vulnerability, as well as countermeasures to mitigate them.

表3列出了针对ICN的安全攻击和对策的最后一部分，包括ICN缓存机制中的分组攻击及其相应的类别，目标，漏洞，以及减轻它们的对策。

6CHALLENGES AND FUTURE PERSPECTIVES

6挑战与未来展望

Effectively securing computing systems in general is not a trivial task [100]. The Internet poses an extra challenge, as its pervasiveness and ubiquitous presence give users the sense of anonymity. As more applications are available on the Internet, more users expose information regarding many facets of their lives, such as credit card numbers, bank accounts, addresses, daily routines, aspects about private life, and so on. With the advent of the Internet of Things [81], it is expected that everything will eventually be connected to the Internet, from appliances to health devices. Thus, the security aspect becomes even more worrying, as sensitive content (e.g., concerning user’s health) requires guarantee that only authorized users can access and modify it.

通常，有效地保护计算系统并不是一件容易的事[100]。互联网带来了额外的挑战，因为其普遍性和无处不在给用户匿名的感觉。随着互联网上可用的应用程序日益繁多，越来越多的用户暴露了许多生活中的信息，如信用卡号码、银行账户、地址、日常生活、私人生活等。随着物联网的出现[81]，人们预计，从电器到医疗设备，所有的东西最终都将与互联网相连。因此，网络安全方面变得更加令人担忧，因为敏感内容（例如，与用户健康有关的信息）需要保证只有授权用户才能对其访问和修改。

As stated by AbdAllah et al. [1], ICN security solutions should ensure content integrity and authenticity, certify content provenance, and protect user privacy. Considering also availability and scalability issues, this scope statement is not easy to be fulfilled. While ICN itself is natively

如AbdAllah等人所述[1]，ICN安全解决方案应确保内容的完整性和真实性，认证内容来源并保护用户隐私。考虑到网络可用性和弹性问题，以上并不容易实现。而ICN本身

prone, to a certain extent, to some well-known attacks (such as DoS), other important security aspects should be addressed before it can be deployed in real world. In the following, we discuss some ideas we think are important to promote for the evolution of security foundations in ICN:

在某种程度上易于受到某些众知的攻击（例如DoS）的影响，所以在实践部署之前，还应解决其他重要的安全问题。下面，我们将讨论一些我们认为会促进ICN安全基础发展的重要观点：

Old threats in a new architecture: ICN security area would benefit from a deep inspection concerning the feasibility and impact of attacks already known in IP-based networks on ICN architectures, as web page hijacking, traffic interception, and spam, for example. It would be helpful to thoroughly explore these attacks to discover new vulnerabilities and also defenses against them, possibly provided by the ICN paradigm itself.

新架构中的旧威胁：对基于IP网络中的已知攻击对ICN架构的可能性和影响进行深入检查将利于ICN安全领域的发展，例如，网页劫持，流量拦截和垃圾邮件。深入研究这些攻击有助于发现新的漏洞，并对其进行防御，且ICN范式本身可能提供这些防御。

Security vulnerabilities in mobile environments: Mobile environments pose an extra challenge for security in ICN, since all devices are supposed to serve as content caches, thus raising the potential for cache snooping, monitoring, and censorship. Works address-ing mobile ICN security vulnerabilities and threats are still scarce. There should be more investigation about the impact of the ICN paradigm in a mobile environment, as ICN may be vulnerable to current mobile threats or even introduce new forms of vulnerabilities in mobile networks.

移动环境中的安全漏洞：移动环境对ICN中的安全性提出了额外的挑战，因为所有设备都会用作内容缓存，从而加大了缓存侦听、监视和审查的范围。但目前有关于解决移动ICN安全漏洞和威胁的投入仍然很少。人们对于ICN范式在移动环境中的影响应该进行更多的研究，因为ICN可能容易受到当前移动威胁的影响，甚至在移动网络中引入新形式的漏洞。

User privacy versus malicious activity detection: Previous cases concerning unautho-rized monitoring and spying on users’ Internet traffic have raised the level of worry about user privacy and anonymity. In order to be fully considered as an alternative to the current Internet, the ICN architecture must comply with users rights and international rules con-cerning user privacy. It is not easy to reason about implications of such mechanisms, and it is not clear how to simultaneously enable both privacy and malicious activity detection. Moreover, ensuring that governments collect users’ traffic patterns only for security rea-sons and not for censorship, or preventing misuse of such information to coerce or threat individuals, goes beyond what technology can offer: It requires users behaving properly and citizens vigilance over government activities.

用户隐私与恶意活动检测相矛盾：以前涉及未经授权的监测和监视用户网络流量的案例加剧了对用户隐私和匿名性的担忧。若要被完全视为当前互联网的替代方案，ICN体系结构必须维护用户权利和遵守有关用户隐私的国际规则。这种机制很难把握，并且不清楚如何同时保护隐私和启动恶意活动检测。此外，确保政府只为安全而非审查收集用户的流量模式，或防止滥用此类信息胁迫或威胁个人，这超出了技术所能提供的范围：因为这要求用户行为适当，公民对政府活动保持警惕。

Attack impact assessment: A deep understanding of the potential of attacks in ICN is a con-siderable challenge. We have listed several research works suggesting potential security

攻击影响评估：深入了解ICN中攻击的潜在性是一个巨大的挑战。我们列出了几项研究工作来表明ICN中潜在的安全问题。

problems in ICN; however, only few of them effectively show and analyze the impact of such attacks, in simulations or in a real ICN deployments. Such analysis and discussions are important to really understand which aspects need further study and then correctly orientate the research toward more secure ICN architectures.

但是，在模拟或实际的ICN部署中，只有极少数能有效地显示和分析此类攻击的影响。这样的分析和讨论是非常重要的，因为它们有利于真正了解哪些方面需要进一步研究，进而正确地将研究方向转向部署更安全的ICN体系结构。

Better evaluation of solutions: To date, many solutions proposed in the surveyed literature are not deeply evaluated. More realistic and detailed evaluations are crucial to better un-derstand the behavior of the proposed solutions, including effectiveness, overhead, side effects, and trade-offs [6]. Many testbeds have been developed for ICN architectures [46, 80, 98, 105], and they should be more extensively used to provide better knowledge about ICN security solutions. In particular, solutions that hamper content caching or limit re-quest rates may negatively affect the user experience and should be better investigated [107].

更好地评估解决方案：迄今为止，调查文献中提出的许多解决方案尚未得到深入评估。更现实，更详细的评估对于更好地理解所提出的包括有效性，间接费用，副作用和权衡取舍的解决方案至关重要[6]。人们已经为ICN体系结构开发了许多测试台[46、80、98、105]，所以应该更广泛地使用测试台来提供关于ICN安全解决方案的更好的知识。特别是，阻碍内容缓存或限制重新请求速率的解决方案可能会对用户体验产生负面影响，应进行更好的调查[107]。

Scalability issues: Many of the security solutions described here directly affect scalability, the raison d’être and central feature in ICN architectures. For instance, some solutions use centralized entities for access control enforcement [31, 32, 36, 102] or for key authenticity verification [96]. Scalability should be a foreground property in the assessment of security solutions for attacks in the ICN context.

弹性问题：这里描述的许多安全解决方案直接影响ICN架构中的弹性，存在理由和核心特性。例如，一些解决方案使用集中式实体来执行访问控制[31、32、36、102]或用于密钥真实性验证[96]。在评估针对ICN环境中的攻击的安全解决方案时，弹性应该是一个前台属性。

Fault tolerance: Some of the proposed solutions are based in third-party entities that may constitute a single point of failure [32]. Such entities, besides impacting the system scal-ability, may constitute interesting targets for DoS attacks, impairing the whole network. Some controlled redundancy is expected from solutions to leverage fault tolerance and scalability.

容错:一些解决方案的提出基于可能构成单点故障的第三方实体[32]。这些实体除了影响系统的弹性外，还可能成为DoS攻击的目标，从而损害整个网络。一些受控冗余可能利用解决方案中的容错性和可扩展性。

Trust management: The binding between a key and its owner should be ensured by a trust mechanism. ICN does not impose a specific trust management scheme, leaving to ap-plications to define their own mechanisms and sources of trust. Approaches used in the current Internet, like hierarchical Public Key Infrastructures (PKI) can also be adopted in ICN, but more scalable approaches, like SPKI/SDSI [19], fit better to the decentralized nature of ICN, as stated by Zhang et al. [128].

信任管理：密钥和密钥所有者之间的绑定应通过信任机制来确保。ICN并不强加特定的信任管理方案，而是由应用程序定义其自己的信任机制和信任源。ICN不强制实施特定的信任管理方案，而是由应用程序定义自己的机制和信任源。如Zhang等人所述，在当前的互联网中使用的方法，例如层级公钥基础设施（PKI），也可以在ICN中采用，但是更具扩展性的方法，例如SPKI / SDSI [19]，更适合ICN的去中心化性质。[128]。

Key revocation: Besides checking the bound between a key and its owner, clients also need to verify whether a given key is yet valid (i.e., it was not revoked). Since a key is a data content, it can be stored in and retrieved from network caches and thus may be outdated if its issuer revoked it. Some approaches were proposed to check the status of keys in ICN [82, 96, 123], but more generic solutions, possibly integrated with trust management schemes, would be welcome.

密钥撤销：除了检查密钥与其所有者之间的绑定外，客户还需要验证给定密钥是否仍然有效（即，尚未撤销）。由于密钥是数据内容，因此可以将其存储在网络缓存中并从中检索，因此如果其颁发者吊销了密钥，则密钥可能已过期。有人提出了一些方法来检查ICN中密钥的状态[82、96、123]，但采用可能与信任管理方案整合的更通用的解决方案则更受欢迎。

The ICN paradigm gives researchers the opportunity to embed security into the core of the Internet and to rethink what worked and what has been unsuccessful in the traditional Internet architecture. Nonetheless, securing the network will always be a continuous effort, as new threats appear, new attacks are explored, and new security measures are provided. Starting with robust and consolidated security foundations embedded into the architecture, researchers will be able to provide better and quicker countermeasures, turning the Internet into a safer place.

ICN范式使研究人员有机会将安全性嵌入到互联网的核心，并重新思考在传统的互联网架构中哪些是有效的，哪些是不成功的。然而，随着新的威胁出现，新的攻击被探索，新的安全措施被提供，保护网络的安全将始终是一项持续的工作。从嵌入到架构中的鲁棒和巩固的安全基础开始，研究人员将能够提供更好更快的对策，使互联网更加安全。

7 CONCLUDING REMARKS

7 结束语

The ICN paradigm is a promising future Internet architecture that comes to provide an Inter-net more suitable to content distribution. However, from the security perspective, ICN features great challenges. In this article, we organized, classified, discussed, and explored the literature about security vulnerabilities, attacks, and countermeasures in ICN, regarding three key ICN as-pects: content, routers, and caching. We observed that while severe vulnerabilities on content and

ICN范例是一种可实现的未来互联网架构，它将提供一个更适合内容分发的互联网络。但是，从安全角度来看，ICN面临着巨大挑战。在本文中，我们就ICN的三个主要方面：内容，路由器和缓存，对ICN中的安全漏洞，攻击和对策进行了组织，分类，讨论和探索。我们注意到，尽管内容和

content names, such as integrity and privacy, have been extensively addressed, threats against routers and caching still needs attention, especially when they allow fake or corrupted content to reach users. Thus, further research is needed on security solutions and metrics, to leverage ICN as a complete, robust architecture, able to meet current and future demands for performance, mobility, and security. We expect that this knowledge systematization can provide the reader to insights re-garding ICN attacks and vulnerabilities, helping into building future works on discovering points of vulnerabilities and new solutions and countermeasures to mitigate them.

内容命名中的严重漏洞，如完整性和隐私性，已经得到了广泛的解决，对路由器和缓存的威胁仍然需要注意，特别是当它们允许虚假或损坏的内容到达用户手中时。因此，我们需要对安全解决方案和指标进行进一步研究，以将ICN用作一个完整的，鲁棒的体系结构，使其能够满足当前和将来对性能，移动性和安全性的需求。我们希望这种知识系统化能够为读者提供对ICN攻击和漏洞的新见解，这将有助于在发现漏洞点和新的解决方案及对策方面展开未来的工作。