A Survey of Contemporary Research in Firewall and Intrusion Detection System Security (2024-2025)

Executive Summary and Overview of Surveyed Research

This report presents a comprehensive survey of cutting-edge academic research focused on the security of Firewalls, Intrusion Detection Systems (IDS), and functionally equivalent network security infrastructure. The analysis is strictly confined to peer-reviewed papers published in the proceedings of the four premier cybersecurity conferences—IEEE Symposium on Security and Privacy (S&P), ACM Conference on Computer and Communications Security (CCS), USENIX Security Symposium, and the Network and Distributed System Security Symposium (NDSS)—during the 2024 and 2025 publication years.

The survey reveals a significant and discernible shift in the research community's focus. Rather than targeting the vulnerabilities of traditional, monolithic firewall appliances, the most impactful research investigates the security of the underlying and adjacent infrastructure upon which all modern network security relies. The findings are clustered around three primary themes:

1. **Systemic Flaws in Core Internet Services:** A substantial body of work demonstrates that foundational services like the Domain Name System (DNS) and Network Address Translation (NAT) are rife with implementation and protocol-level vulnerabilities. These flaws can be exploited to bypass security policies, conduct Denial-of-Service (DoS) attacks, and undermine the very trust on which network defenses are built.
2. **The Ascendance of Logical and Algorithmic Attacks:** The most potent novel attacks presented are not based on classic memory corruption but on the sophisticated manipulation of protocol logic, state machines, and algorithmic complexity. These attacks target the rules and standards themselves, making them particularly widespread and difficult to mitigate with traditional defenses.
3. **The Specialization of Security Tooling:** In both offensive and defensive

domains, there is a clear trend towards highly specialized, domain-aware tools. Advanced fuzzing frameworks are now tailored to specific protocols like DNS and 5G, while next-generation defensive systems leverage programmable hardware and control planes to create more adaptive and scalable security architectures.

Notably, during the surveyed period, no papers published in the proceedings of the IEEE Symposium on Security and Privacy (S&P) met the strict inclusion criteria of having a firewall or IDS as the primary subject of a systematic analysis, novel attack, or new security tool. Therefore, the findings of this report are drawn from the proceedings of ACM CCS, USENIX Security, and NDSS.

The following table provides a high-level summary and index of the research analyzed within this report, categorizing each paper by its primary technological target and its core contribution.

Table 1: Summary of Surveyed Research on Firewall and IDS Security (2024-2025)

Paper Title	Conference & Year	Primary Target/Technology	Core Contribution Category
Wallbleed: A Memory Disclosure Vulnerability in the Great Firewall of China	NDSS '25	National Firewall (GFW)	
Understanding the Implementation and Security Implications of Protective DNS Services	NDSS '24	Protective DNS (PDNS)	
ReDAN: An Empirical Study on Remote DoS Attacks Against NAT Networks	NDSS '25	Network Address Translation (NAT)	
The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC	ACM CCS '24	DNSSEC Protocol	[Novel Attack]

CAMP: Compositional Amplification Attacks against DNS	USENIX Security '24	DNS Protocol	[Novel Attack]
Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation	USENIX Security '24	SSH Protocol	[Novel Attack]
Inbox Invasion: Exploiting MIME Ambiguities to Evade Email Attachment Detectors	ACM CCS '24	Email Security Gateway	[Novel Attack]
You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks	USENIX Security '24	Security Information and Event Management (SIEM)	
Manipulating OpenFlow Link Discovery Packet Forwarding for Topology Poisoning	ACM CCS '24	Software-Defined Networking (SDN) Controller	[Novel Attack]
ResolverFuzz: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing	USENIX Security '24	DNS Resolver	
ReqsMiner: Automated Discovery of CDN Forwarding Request Inconsistencies... with Grammar-Based Fuzzing	NDSS '24	Content Delivery Network (CDN)	
RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G	ACM CCS '24	5G Cellular Core	

RAN-Core Interfaces			
No Peer, no Cry: Network Application Fuzzing via Fault Injection	ACM CCS '24	Network Protocol Implementation	
HYPERPILL: Fuzzing for Hypervisor-bugs by Leveraging the Hardware Virtualization Interface	USENIX Security '24	Hypervisor / Virtualization	
SmartCookie: Blocking Large-Scale SYN Floods with a Split-Proxy Defense on Programmable Data Planes	USENIX Security '24	DoS Defense / Programmable Switch	
5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service	NDSS '24	5G Open RAN (O-RAN)	
Detecting Tunneled Flooding Traffic via Deep Semantic Analysis of Packet Length Patterns	ACM CCS '24	IDS / DDoS Detection	
ERW-Radar: An adaptive detection system against evasive ransomware	NDSS '25	Host-based IDS / Ransomware Detection	

Part I: Systematic Analysis of Deployed Network Security Infrastructure

This section focuses on research that conducts deep, empirical studies of real-world, large-scale systems that function as, or are integral to, firewalls and intrusion

detection systems. These papers are crucial as they ground academic theory in the realities of deployed infrastructure, often revealing systemic weaknesses that arise from the complexity of implementation, non-standard operational practices, and the inherent fragility of the underlying protocols. The analysis demonstrates a recurring theme: the security of these large-scale systems is frequently undermined not by exotic new attacks, but by classic vulnerability classes and flawed design assumptions.

1.1 Probing National-Scale Censors and Protective Services

The security posture of distributed, policy-enforcing systems that act as national or provider-level firewalls is a critical area of study. Two papers from NDSS provide unprecedented visibility into such systems, revealing that even sophisticated, state-level infrastructure and well-intentioned security services suffer from fundamental flaws.

- **Paper Title:** Wallbleed: A Memory Disclosure Vulnerability in the Great Firewall of China [1]
- **Authors:** Shencha Fan, Jackson Sippe, Sakamoto San, Jade Sheffey, David Fifield, Amir Houmansadr, Elson Wedwards, Eric Wustrow [1]
- **Conference & Year:** NDSS '25 [1]
- **Abstract/Summary:** This paper presents *Wallbleed*, a buffer over-read vulnerability that existed in the DNS injection subsystem of the Great Firewall of China (GFW). This flaw caused certain censorship middleboxes to leak up to 125 bytes of their memory when processing a specially crafted DNS query. The authors conducted a longitudinal, Internet-wide measurement study for over two years to understand the vulnerability's causes and implications. The work involved reverse-engineering the GFW's DNS parsing logic, analyzing the content of the leaked memory, assessing the impact on users, and monitoring the censor's patching behavior over time. The leaked data provided rare insights into the GFW's internal architecture, including its memory management, load-balancing mechanisms, and process-level behavior. The study revealed that an incorrect patch was deployed in November 2023 before the vulnerability was fully remediated in March 2024.[1]
- **Key Contribution & Relevance:**. This work is a premier example of a systematic security analysis of one of the world's most opaque and large-scale network filtering systems. It demonstrates that even highly sophisticated, state-sponsored

infrastructure is susceptible to classic memory safety vulnerabilities. The analysis of the leaked data provides invaluable "ground truth" about the internal operations of a national-level firewall, showing how such flaws can be repurposed for intelligence gathering against the system itself. The vulnerability reveals that poorly implemented censorship systems not only infringe on freedom of expression but also pose severe privacy and confidentiality risks to all Internet users whose traffic is inspected.[1]

- **Link:** https://www.ndss-symposium.org/ndss-paper/wallbleed-a-memory-disclosure-vulnerability-in-the-great-firewall-of-china/
- **Paper Title:** Understanding the Implementation and Security Implications of Protective DNS Services [3]
- **Authors:** Mingxuan Liu, Yiming Zhang, Xiang Li, Chaoyi Lu, Baojun Liu, Haixin Duan, Xiaofeng Zheng [3]
- **Conference & Year:** NDSS '24 [3]
- **Abstract/Summary:** This paper presents the first large-scale measurement study of Protective DNS (PDNS) services, which function as distributed, policy-based firewalls by blocking access to malicious domains. The authors developed a methodology to identify PDNS servers at scale by triggering their DNS rewriting behavior with a curated list of malicious domains. They successfully identified 17,601 open PDNS servers. While finding that PDNS is widely deployed and adds negligible latency, the study uncovered significant security flaws in their implementations. These flaws include methods to evade blocking policies, the ability for attackers to launch Denial-of-Service attacks against legitimate users by spoofing their IP addresses in queries for blocked domains, and the use of dangling pointers in rewritten DNS responses (e.g., resolving to de-registered cloud IPs), which enables domain takeover attacks.[3]
- **Key Contribution & Relevance:**. This paper systematically analyzes a widely deployed but poorly understood security infrastructure. PDNS services are, in effect, a massive, distributed firewall for the Internet. This research reveals that the non-standardized and often ad-hoc implementation of these services has introduced new, systemic vulnerabilities into the DNS ecosystem. It highlights a critical trade-off where a well-intentioned security mechanism, when poorly implemented, can create novel attack vectors, undermining its own purpose.[3]
- **Link:** https://www.ndss-symposium.org/wp-content/uploads/2024-782-paper.pdf

The findings from these two papers, though focused on systems with different objectives—one on censorship (GFW) and the other on protection (PDNS)—converge on a critical point. The security of large-scale, distributed firewall systems is often

compromised by foundational implementation errors rather than by exotic, novel attack techniques. The Wallbleed vulnerability is a classic buffer over-read, a type of memory safety error that has been understood for decades.[1] Similarly, the vulnerabilities in PDNS services, such as susceptibility to IP-spoofed DoS and the use of dangling pointers in responses, stem from a failure to adhere to robust, secure-by-design principles in a distributed environment.[3]

This pattern suggests that the sheer complexity and operational pressures of deploying and maintaining such vast infrastructure can lead to the neglect of fundamental security practices. The imperative to "make it work" across a heterogeneous network may supersede the imperative to "make it secure," resulting in an accumulation of security debt. This has a profound implication: any future security architecture that relies on large-scale, distributed policy enforcement using complex, legacy protocols like DNS is likely to inherit or introduce similar vulnerabilities. The research focus for such systems must therefore extend beyond the correctness of the security policy itself to encompass the robustness and security of the underlying implementation and its operational practices.

1.2 Uncovering Flaws in Core Network Functions

The security of any firewall or IDS is predicated on the secure and correct functioning of the underlying network protocols and devices it is meant to protect. Research in this area exposes how flaws in these core components, particularly Network Address Translation (NAT), can completely undermine higher-level security controls.

- **Paper Title:** ReDAN: An Empirical Study on Remote DoS Attacks Against NAT Networks [4]
- **Authors:** Xuewei Feng, Yuxiang Yang, Qi Li, Xingxiang Zhan, Kun Sun, Ziqiang Wang, Ao Wang, Ganqiu Du, Ke Xu [4]
- **Conference & Year:** NDSS '25 [4]
- **Abstract/Summary:** This paper presents ReDAN (Remote DoS Attacks targeting NAT), a comprehensive empirical study demonstrating that NAT devices are vulnerable to remote, off-path DoS attacks. The attack is a two-stage process. First, an attacker exploits a side channel in the Path MTU Discovery (PMTUD) mechanism to remotely identify whether a given public IP address belongs to a NAT device or a single host. This side channel exists because of inconsistencies between RFC specifications and real-world NAT implementations. Second, once a

NAT device is identified, the attacker sends specially crafted packets that exploit widespread implementation flaws in how NATs manage their connection state tables. These packets deceive the NAT into prematurely removing legitimate TCP connection mappings, effectively terminating ongoing connections for internal clients without their knowledge. The study tested 8 router firmwares and 30 commercial NAT devices, finding the majority vulnerable. A real-world assessment of 180 NAT networks (including public Wi-Fi, 4G/5G cellular, and cloud networks) found over 92% to be susceptible to the attack.[4]

- **Key Contribution & Relevance:** / [Novel Attack]. This work is a critical contribution that combines a systematic analysis of real-world NAT implementations with the development of a novel, practical attack vector. NAT is the most ubiquitous form of a stateful firewall deployed today. This research demonstrates that the foundational security assumption of NAT—that it provides stateful connection tracking and isolation—is broken in the vast majority of deployed devices. An external, off-path attacker can disrupt the connectivity that firewalls and IDS systems are designed to protect, rendering their deep packet inspection or policy enforcement moot. The security of the end-host is irrelevant if the network infrastructure providing its connectivity can be remotely manipulated.[4]
- **Link:** https://www.ndss-symposium.org/wp-content/uploads/2025-972-paper.pdf

The ReDAN research underscores a dangerous and recurring theme in network security: the divergence between protocol standards (RFCs) and the diverse, often flawed, implementations in the wild creates systemic vulnerabilities. The attack's success is not due to a flaw in the TCP/IP protocols themselves, but in how NAT devices, produced by a multitude of vendors, fail to implement them with security rigor.[4] This parallels the findings in the PDNS study, where non-standard implementations created new risks.[3]

This points to a misplaced trust in the fundamental "plumbing" of the internet. Network operators and security professionals implicitly assume that NAT devices and DNS resolvers function correctly and transparently. This research shatters that assumption, revealing them as a fragile and directly attackable surface. A firewall or IDS operating behind a vulnerable NAT is built on a foundation of sand; its ability to inspect traffic is contingent on that traffic not being prematurely terminated by an external adversary manipulating the NAT's state table. This has significant implications, suggesting a pressing need for a new paradigm in testing and certifying network infrastructure equipment. Mere interoperability and performance testing are insufficient. Devices must undergo rigorous adversarial security testing that

specifically probes for deviations from secure protocol handling and state management. This could catalyze a new sub-field of security focused on "protocol conformance and security auditing" for the hardware and firmware that form the internet's backbone.

Part II: Novel Attack Methodologies and Evasion Techniques

This section collates research that introduces new offensive techniques, providing a critical window into the evolving threat landscape. These papers are vital for informing the development of next-generation defenses. The analysis reveals a distinct trend away from simple implementation bugs towards more sophisticated attacks that target the logic of protocols, the semantic gaps between systems, and the centralized control planes of modern networks.

2.1 Algorithmic Complexity and Protocol-Level Attacks

This area of research focuses on sophisticated attacks that exploit logical flaws within protocol designs and their implementations. Rather than corrupting memory, these attacks weaponize the protocol's own rules to induce resource exhaustion or degrade security guarantees, often with devastating effect.

- **Paper Title:** The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC [6]
- **Authors:** Elias Heftrig, Haya Schulmann, Niklas Vogel, Michael Waidner [7]
- **Conference & Year:** ACM CCS '24 [6]
- **Abstract/Summary:** This paper introduces KeyTrap, a new and powerful Denial-of-Service attack targeting DNSSEC-validating resolvers. The vulnerability stems from a fundamental flaw in the DNSSEC standard itself, which dictates that resolvers must attempt to validate all available cryptographic keys against all available signatures for a given record. An attacker can construct a malicious DNS zone with a large number of keys and signatures that share the same key-tag. When a victim resolver attempts to validate this zone, it is forced into a validation workload that grows quadratically. The research demonstrates that a single, specially crafted DNS packet can exhaust the CPU resources of major resolver

implementations (including BIND9, Unbound, Google Public DNS, and Cloudflare) for a period ranging from minutes to over 16 hours, effectively achieving a complete DoS with minimal attacker effort.[7]

- **Key Contribution & Relevance:** [Novel Attack]. KeyTrap represents a devastating algorithmic complexity attack that targets a flaw in an IETF standard, rendering virtually all compliant implementations vulnerable. It is a canonical example of how security protocols can be attacked not by breaking their cryptographic primitives, but by exploiting their specified operational logic to induce resource exhaustion. This has profound implications for any system that relies on DNSSEC for integrity, as an attacker can now deny access to any DNSSEC-protected domain.[7]
- **Link:** https://dblp.org/rec/conf/ccs/HeftrigSVW24.html (Search Query: "The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC")
- **Paper Title:** CAMP: Compositional Amplification Attacks against DNS [8]
- **Authors:** Huayi Duan, Marco Bearzi, Jodok Vieli, David Basin, Adrian Perrig, Si Liu, Bernhard Tellenbach [8]
- **Conference & Year:** USENIX Security '24 [8]
- **Abstract/Summary:** This work performs a systematic investigation of the DNS protocol as a vector for DoS amplification attacks. The authors move beyond analyzing individual DNS features and instead establish a taxonomy of amplification "primitives" and a framework to analyze how these primitives can be composed. This approach led to the discovery of a large family of CAMP (Compositional Amplification) vulnerabilities. By chaining legitimate DNS features together in a novel way, these attacks produce a multiplicative amplification effect, achieving message amplification factors of hundreds or even thousands—far exceeding previously understood limits. The study found these vulnerabilities to be ubiquitous across popular DNS implementations and open resolvers.[9]
- **Key Contribution & Relevance:** [Novel Attack]. This paper introduces a new methodology for discovering amplification attacks. Rather than finding single-shot vectors, the CAMP framework provides a way to reason about and discover compositional attacks that arise from the complex interaction of protocol features. This fundamentally alters the threat model for DNS-based DoS, demonstrating that the protocol's complexity can be weaponized to create unexpectedly powerful attacks. This work is directly relevant to any firewall or IDS that attempts to mitigate DoS attacks, as it reveals a new class of threats that may bypass existing rate-limiting or filtering rules.[9]
- **Link:** https://www.usenix.org/conference/usenixsecurity24/presentation/duan

- **Paper Title:** Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation [10]
- **Authors:** Fabian Bäumer, Marcus Brinkmann, Jörg Schwenk [10]
- **Conference & Year:** USENIX Security '24 [11]
- **Abstract/Summary:** The Terrapin attack is a novel prefix truncation attack against the SSH protocol. It breaks the integrity of the secure channel by allowing a Man-in-the-Middle (MitM) attacker to delete an arbitrary number of packets from the beginning of an encrypted SSH session without detection by either the client or the server. The attack is achieved by carefully manipulating sequence numbers during the initial handshake. A practical application is to drop the EXT_INFO message, which is used to negotiate protocol extensions. This can be used to downgrade the connection's security, for instance by disabling countermeasures against keystroke timing attacks in OpenSSH or forcing the use of weaker public key algorithms for authentication. The vulnerability affects implementations that support ChaCha20-Poly1305 or CBC with Encrypt-then-MAC.[10]
- **Key Contribution & Relevance:** [Novel Attack]. This is a fundamental attack on the integrity of the SSH protocol, a cornerstone of secure network and systems administration. Since firewalls, routers, and other security appliances are almost universally managed via SSH, a vulnerability that allows an attacker to silently downgrade the security of the management channel is of critical importance. It demonstrates that even mature, widely trusted protocols can harbor subtle logical flaws in their state machine and handshake design.[10]
- **Link:** https://www.usenix.org/conference/usenixsecurity24/presentation/b%C3%A4umer

The research presented in this section signals a clear and important evolution in network protocol attacks. The focus is shifting from exploiting memory corruption bugs in a specific implementation to identifying and weaponizing logical flaws within the protocol's own state machine and specified behavior. The KeyTrap attack does not corrupt memory; it uses the mandated DNSSEC validation logic against itself to create a computational bottleneck.[7] Similarly, the

CAMP attacks do not rely on a buffer overflow but instead combine legitimate DNS features in an unforeseen way to generate an enormous amplification factor.[9] Finally, the

Terrapin attack does not break the underlying cryptography but rather abuses the sequence numbering and handshake logic to compromise the integrity of the

established channel.[10]

This common thread—targeting protocol logic—indicates a maturation of offensive security research. These attacks are more insidious and harder to detect with traditional tools like memory sanitizers, which are blind to logical errors. This trend has significant implications for the way we design and validate network protocols. It suggests that current practices, which focus heavily on cryptographic strength and memory-safe implementation, are insufficient. There is a clear and growing need to systematically analyze protocols for logical vulnerabilities, including algorithmic complexity traps and state-machine weaknesses. This necessitates a paradigm shift towards the broader adoption of formal methods and automated modeling in the design and verification of network standards. Simply publishing an RFC and waiting for implementers to find flaws is proving to be a dangerously reactive approach. Future work must aim for provable guarantees not only of cryptographic security but also of resource consumption bounds and state-machine integrity, even when under adversarial influence.

2.2 Evasion of Application-Layer Inspection and Detection

This section covers research focused on techniques designed to bypass higher-level security systems, such as application-layer firewalls and signature-based IDS, which inspect application content and behavior. These attacks typically exploit the "semantic gap" between how a security device interprets data and how the end application ultimately processes it.

- **Paper Title:** Inbox Invasion: Exploiting MIME Ambiguities to Evade Email Attachment Detectors [12]
- **Authors:** Jiahe Zhang, Jianjun Chen, Qi Wang, Hangyu Zhang, Chuhan Wang, Jianwei Zhuge, Haixin Duan [12]
- **Conference & Year:** ACM CCS '24 [12]
- **Abstract/Summary:** This paper presents the first systematic evaluation of how parsing ambiguities in the MIME email standard can be exploited to evade email attachment detectors, which act as application-layer firewalls for mail servers. The authors developed MIMEminer, a novel testing tool that automatically discovers parsing discrepancies between email security gateways (e.g., Gmail, iCloud) and end-user email clients (e.g., Outlook, Thunderbird). By mutating email structures and observing differences in how they are parsed, MIMEminer

identified 24 evasion vulnerabilities, 19 of which were new discoveries. These vulnerabilities affected all 16 tested email services and 7 email clients, allowing an attacker to craft an email that is deemed safe by the security scanner but is rendered as a malicious attachment by the user's client.[13]

- **Key Contribution & Relevance:** [Novel Attack] /. This work introduces a powerful new attack methodology and an automated tool (MIMEminer) for discovering it. It perfectly illustrates the classic "impedance mismatch" or "parser differential" problem, a recurring source of vulnerabilities in systems where a security middlebox and an end application must interpret the same complex data format. This is highly relevant for any firewall or gateway that performs deep packet inspection on application-layer protocols.[13]
- **Link:** https://doi.org/10.1145/3658644.3670386
- **Paper Title:** You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks [14]
- **Authors:** Rafael Uetz, Marco Herzog, Louis Hackländer, Simon Schwarz, Martin Henze [14]
- **Conference & Year:** USENIX Security '24 [14]
- **Abstract/Summary:** This research systematically analyzes the fragility of Security Information and Event Management (SIEM) detection rules. The authors demonstrate that adversaries can easily evade a significant portion—almost half—of a widespread set of public SIEM rules by making minor, semantically-irrelevant modifications to their actions (e.g., quoting a command). To counter this, they propose a novel defense concept called "adaptive misuse detection" and implement it in a proof-of-concept system named AMIDES. Instead of relying on rigid signatures, AMIDES uses machine learning to compare an incoming event to both the SIEM rules it is *supposed* to match and a learned baseline of known-benign events, allowing it to flag successful evasions. In an evaluation using real enterprise network data, AMIDES successfully detected a majority of over 500 handcrafted evasions with no false alerts.[14]
- **Key Contribution & Relevance:** /. This work provides a crucial systematic analysis of the brittleness of signature-based IDS and introduces a novel defensive tool (AMIDES) to address it. It directly tackles the core problem of rule-based detection: attackers can easily learn the rules and craft their actions to fly just under the radar. The concept of adaptive misuse detection offers a promising path forward for making IDS more resilient to trivial evasions.[14]
- **Link:** https://www.usenix.org/conference/usenixsecurity24/presentation/uetz

The attacks detailed in this section highlight a fundamental weakness in application-layer firewalls and IDS: their reliance on a specific interpretation of

complex data formats and rigid detection logic. The Inbox Invasion paper shows that by exploiting ambiguities in the MIME standard, an attacker can craft an email that is interpreted as benign by a security gateway's parser but as malicious by an email client's parser.[13] Similarly, the SIEM evasion research shows that an attacker can make a minor change to a command—one that has no effect on its execution by the operating system's shell—that is nonetheless sufficient to prevent it from matching a specific, syntactically-rigid detection rule.[14]

Both attacks succeed by exploiting a "semantic gap." In the MIME attack, it is the gap between the gateway's parser and the client's parser. In the SIEM evasion, it is the gap between the rule's rigid syntax and the shell's more flexible, semantically equivalent syntax. This demonstrates the inherent limitations of any security system that relies on exact pattern matching or assumes a single, canonical interpretation of a complex data format. The clear implication is that defenses must evolve to become more "semantically aware." They need to understand the ultimate *effect* of the data or command, not just its superficial structure. This trend will inevitably drive the security industry further towards behavior-based and anomaly-based detection systems, as exemplified by the AMIDES framework.[14] In the long term, it may even necessitate that security tools incorporate full-fidelity parsers or sandboxed emulators for the applications they protect in order to fully close this semantic gap, though this presents formidable performance and scalability challenges.

2.3 Manipulation of Software-Defined Network Infrastructure

This section focuses on attacks targeting the control and management planes of modern, programmable networks. As networks become more software-defined, the centralized controller becomes a high-value target, and attacks are evolving to manipulate its perception and logic.

- **Paper Title:** Manipulating OpenFlow Link Discovery Packet Forwarding for Topology Poisoning [16]
- **Authors:** Mingming Chen, Thomas La Porta, Teryl Taylor, Frederico Araujo, Trent Jaeger [16]
- **Conference & Year:** ACM CCS '24 [17]
- **Abstract/Summary:** This paper introduces Marionette, a novel and stealthy topology poisoning attack against Software-Defined Networking (SDN) controllers. Previous attacks focused on spoofing or replaying link discovery

packets at the data plane. In contrast, Marionette operates from the control plane, assuming an attacker has compromised a network application with privileges to install flow rules. The attack uses a reinforcement learning algorithm to compute an optimal "fake" topology target. It then achieves this by injecting carefully crafted flow entries into the network switches, which manipulate the forwarding of legitimate Link Layer Discovery Protocol (LLDP) packets. This manipulation tricks the SDN controller into building an internal network map that does not match the physical reality. A poisoned topology view can lead to the complete bypass of security policies and traffic monitoring, as the controller makes routing decisions based on false information. The evaluation showed that Marionette successfully attacks five major open-source controllers and nine discovery protocols, and is able to overcome state-of-the-art defenses.[16]

- **Key Contribution & Relevance:** [Novel Attack]. This is a sophisticated attack on the foundational security of SDN. The integrity of the controller's topology view is a prerequisite for any security policy it enforces. By poisoning this view, Marionette undermines the entire security model of the SDN. If the controller's map of the network is wrong, any firewall rules or IDS policies it deploys are built on a foundation of lies and can be trivially bypassed. This work exposes a new class of attacks that initiate from the control plane, which are significantly stealthier and more powerful than data-plane attacks.[16]
- **Link:** https://doi.org/10.1145/3658644.3690345

The Marionette attack demonstrates that the centralization of control in SDN, while offering unprecedented flexibility, also creates a uniquely high-value target. The attack surface of these networks is evolving. While securing the data plane remains important, the most potent attacks are now targeting the control plane, specifically the controller's logic and its perception of the network state. This is another manifestation of the "semantic gap" vulnerability pattern. In this case, the gap is between the *actual* physical network topology and the *perceived* topology that exists within the controller's data structures. The Marionette attack directly poisons this perception.[16]

This has critical implications for the security of programmable networks. It is not sufficient to simply secure the controller from compromise; one must also secure the integrity of the information-gathering processes, like topology discovery, upon which the controller relies. Trust in control-plane data cannot be implicit. This points toward a clear future research direction: the development of "control-plane intrusion detection systems" for SDN. Such a system would need to actively validate the controller's worldview, perhaps by cross-correlating its topology map with data-plane

measurements, looking for anomalous flow rule installations that defy physical constraints, or even using physically-grounded information like packet travel times to detect the presence of forged links. This opens a new and vital research area focused on securing the "brain" of the modern network.

Part III: Innovations in Offensive and Defensive Tooling

This part is dedicated to papers that introduce and validate new frameworks and tools for security analysis. These contributions represent the practical embodiment of the theoretical attacks and defenses discussed in other sections, providing tangible artifacts that push the boundaries of both offensive and defensive capabilities. The surveyed work reveals a clear trend towards highly specialized fuzzers and disaggregated, programmable defense systems.

3.1 Advanced Fuzzing Frameworks for Network Services

This section surveys the next generation of fuzzing tools. The research demonstrates a move away from generic, mutation-based approaches towards highly domain-specific, grammar-aware, and state-aware frameworks that are tailored to find deep bugs in complex network targets.

- **Paper Title:** ResolverFuzz: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing [18]
- **Authors:** Qifan Zhang, Xuesong Bai, Xiang Li, Haixin Duan, Qi Li, Zhou Li [18]
- **Conference & Year:** USENIX Security '24 [18]
- **Abstract/Summary:** ResolverFuzz is a new fuzzing system designed specifically to find vulnerabilities in DNS resolvers. It addresses several key challenges in this domain, including the prevalence of non-crash bugs (like cache poisoning), the lack of rigorous specifications to serve as bug oracles, and the difficulty of stateful fuzzing. The system focuses on short query-response sequences, which the authors' analysis of past CVEs showed to be most effective. It combines a probabilistic context-free grammar (PCFG) for generating syntactically valid inputs with byte-level mutation for deeper exploration. To detect non-crash logical flaws, it leverages differential testing across multiple resolver

implementations and clustering techniques. The evaluation of ResolverFuzz against six mainstream DNS software products uncovered 23 new vulnerabilities, leading to the assignment of 15 CVEs.[18]

- **Key Contribution & Relevance:**. This is a highly effective and specialized tool that demonstrates the power of domain-specific, state-aware fuzzing for critical internet infrastructure. Its success in finding numerous high-impact bugs in mature, widely-deployed DNS resolvers highlights the inadequacy of general-purpose fuzzers for such complex targets.[18]
- **Link:** https://www.usenix.org/conference/usenixsecurity24/presentation/zhang-qifan
- **Paper Title:** ReqsMiner: Automated Discovery of CDN Forwarding Request Inconsistencies and DoS Attacks with Grammar-Based Fuzzing [20]
- **Authors:** Linkai Zheng, Xiang Li, Chuhan Wang, Run Guo, Haixin Duan, Jianjun Chen, Chao Zhang, Kaiwen Shen [20]
- **Conference & Year:** NDSS '24 [20]
- **Abstract/Summary:** ReqsMiner is an innovative fuzzing framework designed to automatically discover inconsistencies in how Content Delivery Networks (CDNs) parse and forward HTTP requests. Such inconsistencies can lead to serious vulnerabilities like request smuggling and Denial-of-Service. The tool employs a grammar-based fuzzer that understands the structure of HTTP. To overcome the challenge of minimal feedback from black-box CDNs, it incorporates techniques from reinforcement learning (specifically, the UCT algorithm) to guide the generation of valid and interesting test cases. The framework was developed to provide a systematic and efficient method for auditing the complex request-handling logic of CDNs.[20]
- **Key Contribution & Relevance:**. This tool targets the complex logic of CDNs, which function as massive, distributed reverse proxies and Web Application Firewalls (WAFs) for a large portion of the internet. By automating the discovery of request parsing inconsistencies, ReqsMiner provides a scalable way to find vulnerabilities that could bypass WAF protections or disrupt service for countless websites.[20]
- **Link:** https://github.com/Konano/ReqsMiner
- **Paper Title:** RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces [22]
- **Authors:** Nathaniel Bennett, Weidong Zhu, Benjamin Simon, Ryon Kennedy, Patrick Traynor, Kevin Butler, William Enck [23]
- **Conference & Year:** ACM CCS '24 [22]
- **Abstract/Summary:** This paper presents RANsacked, a domain-informed fuzzing framework targeting the critical security boundary between the Radio Access

Network (RAN) and the Core Network in LTE and 5G cellular systems. Recognizing the complexity and stateful nature of the protocols used on this interface (e.g., NGAP), the work focuses on building a fuzzer that incorporates deep knowledge of the cellular protocol specifications to generate meaningful and effective test cases. The goal is to uncover vulnerabilities in the core network functions that process messages from the RAN.[22]

- **Key Contribution & Relevance:**. This research pushes automated vulnerability discovery into the highly specialized and historically opaque domain of cellular network infrastructure. A fuzzer for the RAN-Core interface is a critical tool for auditing the security of the infrastructure that underpins all modern mobile communications and a vast number of IoT devices. It provides a means to proactively find flaws before they are deployed at scale.[22]
- **Link:** https://wspr.csc.ncsu.edu/news.html (Search Query: "RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces")
- **Paper Title:** No Peer, no Cry: Network Application Fuzzing via Fault Injection [25]
- **Authors:** Nils Bars, Moritz Schloegel, Nico Schiller, Lukas Bernhard, Thorsten Holz [26]
- **Conference & Year:** ACM CCS '24 [25]
- **Abstract/Summary:** This paper introduces a novel approach to fuzzing network applications that circumvents the need to set up and run a corresponding peer application. The key idea is to use fault injection at the system call level to simulate network events and errors. For example, instead of sending a malformed packet from a client to a server, the fuzzer can directly intercept the server's recv() call and inject the fuzzed data, or it can simulate network failures by making system calls return error codes. This allows the fuzzer to efficiently and deterministically explore the target application's error-handling code paths, which are notoriously difficult to reach with traditional network fuzzing techniques.[27]
- **Key Contribution & Relevance:**. This work presents a clever new methodology and tool that solves a major practical challenge in network application fuzzing: testing the robustness of error-handling logic. Failures in these code paths are a common source of Denial-of-Service vulnerabilities and other stability issues in production systems. This approach makes it significantly easier to audit this critical but often-overlooked part of the attack surface.[25]
- **Link:** https://doi.org/10.1145/3658644.3670355
- **Paper Title:** HYPERPILL: Fuzzing for Hypervisor-bugs by Leveraging the Hardware Virtualization Interface [28]
- **Authors:** Alexander Bulekov, Qiang Liu, Manuel Egele, Mathias Payer [28]
- **Conference & Year:** USENIX Security '24 [28]
- **Abstract/Summary:** HYPERPILL is a generic, black-box hypervisor fuzzing

framework. Its core innovation is that it works without access to the hypervisor's source code by leveraging the standardized hardware-virtualization interface (e.g., Intel VT-x or AMD-V) that all modern hypervisors use. The approach involves taking a single full-system snapshot of a running hypervisor and transplanting it into an emulated environment. HYPERPILL then uses the hardware interface to inject fuzzed inputs directly, allowing it to test all major attack surfaces, including Programmed I/O (PIO), Memory-Mapped I/O (MMIO), hypercalls, and Direct Memory Access (DMA). This method found 26 new bugs in mature hypervisors like QEMU, Microsoft Hyper-V, and the Apple macOS Virtualization Framework.[28]

- **Key Contribution & Relevance:**. This tool represents a significant breakthrough for the black-box security auditing of hypervisors. Virtualized firewalls, routers, and other Network Function Virtualization (NFV) security appliances are commonly deployed on these platforms. A vulnerability in the underlying hypervisor can lead to a complete collapse of the security guarantees provided by these virtual appliances. HYPERPILL provides a powerful, generic method for finding such critical vulnerabilities.[28]
- **Link:** https://www.usenix.org/conference/usenixsecurity24/presentation/bulekov

The tools presented in this section collectively illustrate a significant maturation in the field of fuzzing. Generic, mutation-based fuzzers are being supplanted by highly specialized frameworks that are essential for testing the complex, stateful network targets that form the internet's backbone. ResolverFuzz and ReqsMiner both demonstrate the power of using grammars (PCFG, ABNF) to generate inputs that are syntactically valid but semantically interesting, a far more efficient strategy than random bit-flipping for protocols like DNS and HTTP.[18]

RANsacked further emphasizes this by adopting a "domain-informed" approach, acknowledging that effectively fuzzing cellular protocols requires deep, built-in knowledge of their structure and state machines.[22]

Furthermore, tools like No Peer, no Cry and HYPERPILL innovate on the *environment* in which the target is fuzzed.[25] The former simulates network errors through fault injection, while the latter uses hardware emulation to directly manipulate the hypervisor's interface with the CPU. This represents a move beyond simply providing malformed data to an input channel; these tools intelligently manipulate the target's entire execution context to explore hard-to-reach states.

The success of these specialized tools, which have collectively uncovered dozens of new CVEs in mature, widely-used products, proves that large classes of vulnerabilities remain undiscovered in our critical infrastructure. It strongly suggests that for any

sufficiently complex protocol or system, a dedicated, domain-specific fuzzer is likely to yield significant security findings. This trend may eventually lead to a "fuzzer-as-a-service" market for critical protocols, where specialized firms offer continuous, deep fuzzing for specific technologies like DNS, BGP, or 5G Core. It also highlights a need for protocol specifications themselves to be designed with "fuzzability" in mind, featuring clearly defined state machines and data formats that can be readily translated into grammars for automated testing.

3.2 Next-Generation Detection and Mitigation Systems

This section provides an overview of novel defensive systems designed to counter modern threats. The research here reflects a clear architectural shift away from traditional, monolithic, signature-based appliances towards more programmable, adaptive, and data-driven solutions that distribute security logic across the network fabric.

- **Paper Title:** SmartCookie: Blocking Large-Scale SYN Floods with a Split-Proxy Defense on Programmable Data Planes [30]
- **Authors:** Sophia Yoo, Xiaoqi Chen, Jennifer Rexford [30]
- **Conference & Year:** USENIX Security '24 [30]
- **Abstract/Summary:** SmartCookie is a novel system for mitigating large-scale SYN flooding attacks by leveraging the capabilities of modern programmable network switches. It implements a "split-proxy" defense architecture where the data plane (the switch) and the control plane (a host server) collaborate. The system offloads the computationally intensive task of validating cryptographically secure SYN cookies directly onto the high-speed switch hardware. This allows the switch to absorb and filter 100% of the SYN flood attack traffic at line rate, preventing CPU exhaustion on the protected servers. Legitimate connection attempts that pass the cookie check are then forwarded to the host, which uses modern kernel technologies like eBPF for efficient connection establishment. The evaluation shows that SmartCookie can block attacks of up to 136.9 million packets per second and provides 2x-6.5x lower end-to-end latency for benign clients compared to existing switch-based defenses.[30]
- **Key Contribution & Relevance:**. SmartCookie presents a new architectural blueprint for high-performance DoS defense. By intelligently splitting the logic of a classic firewall function (SYN flood protection) between programmable hardware and host software, it achieves a level of scalability and security that is

not possible with purely software-based or insecure hardware-based solutions. It is a prime example of how programmable data planes are transforming network security.[30]

- **Link:** https://www.usenix.org/conference/usenixsecurity24/presentation/yoo
- **Paper Title:** 5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service [32]
- **Authors:** Haohuang Wen, Phillip Porras, Vinod Yegneswaran, Ashish Gehani, Zhiqiang Lin [32]
- **Conference & Year:** NDSS '24 [32]
- **Abstract/Summary:** 5G-Spector is the first comprehensive framework designed to detect a wide spectrum of Layer-3 protocol exploits within the new Open RAN (O-RAN) 5G architecture. The O-RAN standard disaggregates the base station and introduces programmable components, which 5G-Spector leverages for security. The system features two key components: MOBIFLOW, a novel security audit stream that exports fine-grained cellular network telemetry from the data plane, and MOBIEXPERT, a programmable control-plane application (an "xApp") that runs in the O-RAN Near-Real-Time RAN Intelligent Controller (RIC). MOBIEXPERT analyzes the MOBIFLOW data to detect attacks in real time. The prototype can detect 7 types of known cellular attacks and demonstrated scalability to unknown attacks with high accuracy and low performance overhead.[32]
- **Key Contribution & Relevance:**. This is a forward-looking and highly significant tool that provides a blueprint for building a programmable, software-defined IDS for 5G networks. It capitalizes on the new "open" architecture of 5G to enable security services that were impossible in previous generations of closed, proprietary cellular networks. It represents a paradigm shift for securing critical mobile infrastructure.[32]
- **Link:** https://www.ndss-symposium.org/ndss-paper/5g-spector-an-o-ran-compliant-layer-3-cellular-attack-detection-service/
- **Paper Title:** Detecting Tunneled Flooding Traffic via Deep Semantic Analysis of Packet Length Patterns [35]
- **Authors:** Chuanpu Fu, Qi Li, Meng Shen, Ke Xu [35]
- **Conference & Year:** ACM CCS '24 [35]
- **Abstract/Summary:** This paper presents Exosphere, a system designed to detect tunneled Distributed Denial-of-Service (DDoS) flooding attacks. Such attacks are inherently difficult to detect for traditional IDS because tunneling protocols encrypt or encapsulate the packet headers and payloads, hiding the features that detectors typically rely on. Exosphere overcomes this by operating

solely on an unencrypted metadata feature: packet length. It uses a deep learning model to perform a "deep semantic analysis" of packet length patterns over time. The core idea is that flooding attacks, even when tunneled, exhibit strong statistical correlations in their packet length distributions that differ from benign traffic. The system was prototyped on FPGAs to ensure high-performance processing and achieved high accuracy in detecting various attacks, including stealthy ones, significantly outperforming existing models.[35]

- **Key Contribution & Relevance:**. Exosphere provides a novel and powerful IDS technique for a very challenging problem: detecting malicious traffic in an almost fully encrypted internet. By focusing on metadata like packet length, it offers a way to identify attacks without needing to perform costly and often impossible decryption. This approach is highly relevant for modern network security where end-to-end encryption is the norm.[35]
- **Link:** https://doi.org/10.1145/3658644.3670353
- **Paper Title:** ERW-Radar: An adaptive detection system against evasive ransomware [37]
- **Authors:** Lingbo Zhao, Yuhui Zhang, et al. [38]
- **Conference & Year:** NDSS '25 [37]
- **Abstract/Summary:** ERW-Radar is a host-based detection system specifically designed to counter modern, evasive ransomware that uses techniques like intermittent encryption to fly under the radar of traditional detectors. It employs a hybrid detection strategy. First, it uses a contextual correlation mechanism to identify malicious I/O behavior patterns over time. Second, it performs fine-grained content analysis, using statistical tests (like the Chi-squared test) to identify files that have been encrypted. The system incorporates adaptive mechanisms to achieve a better trade-off between detection accuracy and performance overhead, for example by adjusting the size of its detection window and timing its content analysis to coincide with idle I/O cycles. The evaluation showed a high detection accuracy (96.18%) against evasive ransomware with low CPU and memory overhead.[37]
- **Key Contribution & Relevance:**. While this is a host-based IDS, its techniques for detecting evasive, low-and-slow attacks are directly applicable to network-based security systems, such as those protecting network file servers. It advances the state-of-the-art in behavioral threat detection by combining I/O pattern analysis with content-based checks in an adaptive framework. It demonstrates a robust approach to countering adversaries who are actively trying to mimic benign behavior.[37]
- **Link:** https://www.ndss-symposium.org/ndss-paper/erw-radar-an-adaptive-detection-s

ystem-against-evasive-ransomware-by-contextual-behavior-detection-and-fine-grained-content-analysis/

The defensive systems presented here collectively signal a fundamental architectural evolution in network security. The era of the monolithic, closed-box security appliance is giving way to a new paradigm of disaggregated, programmable, and data-driven defenses. SmartCookie exemplifies this by moving a classic firewall function—SYN flood defense—out of a dedicated appliance and distributing it between the host kernel and the programmable network switch itself.[30] Similarly,

5G-Spector transforms cellular IDS from a function embedded in proprietary base station hardware into a software application (an xApp) running on an open, intelligent control plane.[32]

This "softwarization" and disaggregation of security functions is further complemented by a shift towards more intelligent detection logic. Both Exosphere and ERW-Radar move beyond simple signature matching and instead rely on sophisticated, data-driven analysis of metadata—packet lengths and I/O patterns, respectively—to identify complex and evasive threats that are invisible to traditional methods.[35]

This architectural shift creates both immense opportunities and new categories of risk. The opportunity, as demonstrated by these papers, is for defenses that are more flexible, scalable, intelligent, and adaptable than their monolithic predecessors. The risk, as highlighted by the Marionette attack on SDN controllers [16], is that the control plane itself becomes a new, highly concentrated, and extremely valuable attack surface. The future of network security will be defined by these open, programmable systems. This will demand a new skill set from security professionals, who will need to be as proficient with technologies like P4, eBPF, and machine learning models as they are with firewall rule sets today. It will also foster a new ecosystem of security applications, like O-RAN

xApps, designed to run on these open platforms.

Part IV: Synthesis and Future Research Directions

This survey of the most recent research from the premier cybersecurity conferences

provides a clear snapshot of the current state and future trajectory of firewall and IDS security analysis. By synthesizing the findings from the individual papers, several overarching trends, common vulnerability patterns, and critical areas for future research emerge.

4.1 Observable Trends and Thematic Clusters

Three dominant themes are evident in the 2024-2025 literature:

1. **The Primacy of DNS Security:** A remarkable concentration of high-impact research focuses on the Domain Name System. Papers like KeyTrap [7], CAMP [9], ResolverFuzz [18], and the systematic study of Protective DNS [3] collectively paint a portrait of DNS not as a simple utility, but as a complex, distributed application with a vast and fragile attack surface. This trend marks a shift in perspective, recognizing that the security of DNS infrastructure is a prerequisite for nearly all other network security controls. A firewall rule blocking a domain name is useless if the underlying resolver can be crashed (KeyTrap) or if the DNS response can be manipulated to bypass the block.
2. **The Ascendance of Logical and Algorithmic Attacks:** There is a clear and sophisticated evolution in attack methodologies away from conventional memory corruption exploits. The most significant novel attacks presented target the inherent logic and complexity of protocols. KeyTrap weaponizes the specified validation algorithm of DNSSEC to cause resource exhaustion.[7] Terrapin manipulates the SSH state machine to achieve a security downgrade.[10] CAMP abuses the compositional nature of DNS features to create unforeseen amplification effects.[9] And Marionette poisons the perception of the SDN control plane to undermine its logic.[16] These attacks are stealthier, often stem from flaws in the standards themselves, and are invisible to traditional memory-safety defenses.
3. **The Specialization of Fuzzing:** The field of automated vulnerability discovery is undergoing significant specialization. The most effective tools presented are no longer generic, one-size-fits-all fuzzers. Instead, they are highly domain-aware frameworks tailored to specific, hardened targets. ResolverFuzz for DNS [18], ReqsMiner for CDNs [20], RANsacked for 5G core networks [22], and HYPERPILL for hypervisors [28] all demonstrate that combining deep protocol or

system knowledge with advanced search heuristics is now essential for finding meaningful vulnerabilities. This marks a maturation of the field, moving from brute-force mutation to intelligent, targeted testing.

4.2 Common Targets and Vulnerability Patterns

The research consistently focuses on the infrastructure that firewalls and IDS depend on, rather than on the appliances themselves.

- **Common Targets:** The most frequently analyzed systems include:
  - **DNS Infrastructure:** Specifically resolvers like BIND, Unbound, and PowerDNS.
  - **Core Network Components:** NAT gateways, SSH servers, and SDN controllers.
  - **Large-Scale Distributed Systems:** Content Delivery Networks, Cellular Networks, Protective DNS services, and National Firewalls like the GFW.
- **Common Vulnerability Patterns:** Across these diverse targets, several vulnerability patterns recur:
  - **Implementation Divergence from Standards:** A primary source of weakness, as seen in ReDAN's analysis of NATs [4] and Terrapin's findings on SSH [10], is the gap between how protocols are specified in RFCs and how they are actually implemented. This divergence arises from ambiguity in the standards, performance-optimization shortcuts, or simple developer error, but consistently leads to exploitable flaws.
  - **Semantic Gaps and Parser Differentials:** This pattern, where a security middlebox and a backend application interpret the same data differently, is a recurring theme. It is the root cause of the vulnerabilities found by Inbox Invasion in email gateways [13] and is the principle behind the SIEM evasion techniques [14] and the CDN inconsistencies found by ReqsMiner.[20]
  - **State-Machine and State-Management Flaws:** Attacks like ReDAN and Terrapin succeed not by corrupting data, but by manipulating the state machines of network protocols. They send legitimate-looking but out-of-context packets to trick devices into entering an insecure state or incorrectly tearing down a valid connection state.[4]

4.3 Emerging Research Trajectories and Open Questions

The surveyed work illuminates several critical areas for future research.

- **Securing Programmable Infrastructure:** The rise of programmable data planes (P4, eBPF) and control planes (SDN, O-RAN) is a double-edged sword. While papers like SmartCookie [30] and
  5G-Spector [32] demonstrate their immense potential for building flexible and scalable defenses, the
  Marionette attack [16] shows that the control plane itself is a new and powerful attack surface. This creates a major avenue for future work: the security *of* these programmable systems. Open questions include: How can we formally verify the security properties of a P4 program or an eBPF filter? How do we build an effective IDS for the SDN control plane to detect malicious applications or anomalous flow rules?
- **The Security of AI/ML-driven IDS:** This survey identified several next-generation defensive systems that rely on machine learning, such as Exosphere [35],
  AMIDES [14], and
  ERW-Radar.[37] However, the broader offensive security community has extensively demonstrated that ML models are themselves vulnerable to adversarial examples, data poisoning, and model extraction attacks. A critical and still nascent research direction is to systematically analyze the security of these new, ML-based IDS and firewall systems. Are their models robust against adversarial evasion? Can their training data be poisoned to create blind spots? Can their detection logic be stolen via model extraction?
- **Formal Verification for Critical Protocols:** The discovery of devastating, protocol-level flaws in mature and critical standards like DNSSEC (KeyTrap) [7] and SSH (
  Terrapin) [10] is a clear indictment of the current process for developing internet standards. The reactive cycle of "write an RFC, deploy, and wait for breaks" is no longer tenable for critical infrastructure. A crucial research trajectory is the proactive application of formal methods and automated reasoning to the *design phase* of new protocols. The goal should be to prove the absence of logical, state-machine, and algorithmic complexity vulnerabilities before a standard is ever finalized and deployed at scale.

- **Systematic Analysis of Commercial Appliances:** A conspicuous gap in the surveyed academic literature is the deep, systematic security analysis of proprietary, commercial firewall and Next-Generation Firewall (NGFW) appliances from major vendors. While work like HYPERPILL gets close by fuzzing the underlying hypervisors [28], there is a lack of research that, for example, reverse-engineers and analyzes the security of the custom deep packet inspection engines, proprietary TLS interception stacks, or application identification logic of leading commercial products. This remains a challenging endeavor due to legal and technical hurdles, but it is a vital area for future work to ensure that the security guarantees marketed by vendors hold up to rigorous, independent academic scrutiny.

Works cited

1. Wallbleed: A Memory Disclosure Vulnerability in the Great Firewall ..., accessed June 23, 2025, https://www.ndss-symposium.org/ndss-paper/wallbleed-a-memory-disclosure-vulnerability-in-the-great-firewall-of-china/
2. Wallbleed: A Memory Disclosure Vulnerability in the Great Firewall of China (NDSS 2025) · Issue #456 · net4people/bbs - GitHub, accessed June 23, 2025, https://github.com/net4people/bbs/issues/456
3. Understanding the Implementation and Security Implications of ..., accessed June 23, 2025, https://www.ndss-symposium.org/wp-content/uploads/2024-782-paper.pdf
4. ReDAN: An Empirical Study on Remote DoS Attacks against NAT ..., accessed June 23, 2025, https://www.ndss-symposium.org/wp-content/uploads/2025-972-paper.pdf
5. [2410.21984] ReDAN: An Empirical Study on Remote DoS Attacks against NAT Networks, accessed June 23, 2025, https://arxiv.org/abs/2410.21984
6. Michael Waidner - DBLP, accessed June 23, 2025, https://dblp.org/pid/90/308
7. KeyTrap - ATHENE, accessed June 23, 2025, https://www.athene-center.de/keytrap
8. CAMP: Compositional Amplification Attacks against DNS - USENIX, accessed June 23, 2025, https://www.usenix.org/conference/usenixsecurity24/presentation/duan
9. CAMP: Compositional Amplification Attacks against DNS - USENIX, accessed June 23, 2025, https://www.usenix.org/system/files/usenixsecurity24-duan.pdf
10. Terrapin Attack, accessed June 23, 2025, https://terrapin-attack.com/
11. Find and explore academic papers | Connected ... - Connected Papers, accessed June 23, 2025, https://www.connectedpapers.com/main/7a6b31fe51cc87e47f6a4a79a8741dc131a429a2
12. Hai-Xin Duan - DBLP, accessed June 23, 2025, https://dblp.org/pid/36/5143

13. 202410_email_ccs_evade_detection | PDF | Computing | Internet, accessed June 23, 2025, https://de.scribd.com/document/818014232/202410-email-ccs-evade-detection
14. You Cannot Escape Me: Detecting Evasions of SIEM Rules in ..., accessed June 23, 2025, https://www.usenix.org/conference/usenixsecurity24/presentation/uetz
15. You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks - USENIX, accessed June 23, 2025, https://www.usenix.org/system/files/usenixsecurity24-appendix-uetz.pdf
16. Manipulating OpenFlow Link Discovery Packet Forwarding for ..., accessed June 23, 2025, https://www.researchgate.net/publication/386591812_Manipulating_OpenFlow_Link_Discovery_Packet_Forwarding_for_Topology_Poisoning
17. Cryptography and Security Aug 2024 - arXiv, accessed June 23, 2025, https://www.arxiv.org/list/cs.CR/2024-08?skip=235&show=500
18. ResolverFuzz: Automated Discovery of DNS Resolver ... - Qifan Zhang, accessed June 23, 2025, https://qifanz.com/publication/usenix24a/
19. ResolverFuzz - Fuzzing Survey, accessed June 23, 2025, https://fuzzing-survey.org/?k=ResolverFuzz
20. Konano/ReqsMiner: [NDSS 2024] ReqsMiner is an ... - GitHub, accessed June 23, 2025, https://github.com/Konano/ReqsMiner
21. Thinkst Citation, accessed June 23, 2025, https://citation.thinkst.com/speaker/76648
22. News | WSPR, accessed June 23, 2025, https://wspr.csc.ncsu.edu/news.html
23. ACM CCS 2024 - ACM SIGSAC, accessed June 23, 2025, https://www.sigsac.org/ccs/CCS2024/program/accepted-papers.html
24. WSPR Lab, accessed June 23, 2025, https://wspr.csc.ncsu.edu/
25. CCS 2024 - dblp, accessed June 23, 2025, https://dblp.org/db/conf/ccs/ccs2024
26. CCS 2024 - dblp, accessed June 23, 2025, https://dblp.org/db/conf/ccs/ccs2024.html
27. Moritz Schloegel, accessed June 23, 2025, https://mschloegel.me/
28. Hyperpill: Fuzzing for Hypervisor-bugs by Leveraging the Hardware Virtualization Interface - USENIX, accessed June 23, 2025, https://www.usenix.org/system/files/usenixsecurity24-bulekov.pdf
29. tag: hypervisor-bugs - Semiconductor Engineering, accessed June 23, 2025, https://semiengineering.com/tag/hypervisor-bugs/
30. SmartCookie: Blocking Large-Scale SYN Floods with a Split-Proxy ..., accessed June 23, 2025, https://www.usenix.org/conference/usenixsecurity24/presentation/yoo
31. SmartCookie: Blocking Large-Scale SYN Floods with a Split-Proxy Defense on Programmable Data Planes - USENIX, accessed June 23, 2025, https://www.usenix.org/system/files/usenixsecurity24_slides-yoo.pdf
32. 5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection ..., accessed June 23, 2025, https://www.ndss-symposium.org/ndss-paper/5g-spector-an-o-ran-compliant-layer-3-cellular-attack-detection-service/

33. [Award] 5G-Spector won the NDSS'24 Distinguished Artifact Award, accessed June 23, 2025, https://www.5gsec.com/post/award-5g-spector-won-the-ndss-24-distinguished-artifact-award
34. 5GSEC/5G-Spector: An O-RAN compliant runtime intrusion detection system (xApp) for layer-3 (L3) celluar attack detection - GitHub, accessed June 23, 2025, https://github.com/5GSEC/5G-Spector
35. Detecting Tunneled Flooding Traffic via Deep Semantic ... - thucsnet, accessed June 23, 2025, http://www.thucsnet.com/wp-content/papers/chuanpu_CCS2024.pdf
36. Chuanpu Fu - dblp, accessed June 23, 2025, https://dblp.org/pid/274/0756
37. ERW-Radar: An Adaptive Detection System against Evasive Ransomware by Contextual Behavior Detection and Fine-grained Content Analysis, accessed June 23, 2025, https://www.ndss-symposium.org/wp-content/uploads/2025-349-paper.pdf
38. NDSS Symposium 2025 Accepted Papers, accessed June 23, 2025, https://www.ndss-symposium.org/ndss2025/accepted-papers/
39. Publications | WELCOME - Rui Hou, accessed June 23, 2025, http://hourui-arch.net/publication/