Enhancing Payment Security and Resilience Against DDoS Attacks

A Threat Protection ACS Case Study

WHITE PAPER

Contents

Introduction

It's no surprise that with the rise of cyberattacks, the payment ecosystem has become a prime target as bad actors seek to exploit security gaps. Even with industry-standard protocols such as EMV-3D Secure (3DS) authentication protocol, designed to strengthen the security of online translations by verifying the identity of cardholders, bad actors are constantly finding new ways to cause harm. Distributed Denial of Service (DDoS) attacks and Bank Identification Number (BIN) attacks are two examples of these emerging threats. These attacks disrupt business continuity and often result in substantial financial and reputational damage.

This is where Threat Protection by Mastercard comes in. Our cloud-based solution swiftly mitigates DDoS attacks, safeguards web servers and other Internet-facing assets and prevents BIN attacks before they even happen.

In this paper, we explore how Threat Protection strengthens the resilience of Access Control Servers (ACS), ensuring safe and secure processing of 3DS transactions. We'll also dive a real-world example, showcasing how a leading ACS provider in the Southeastern European region successfully mitigated large-scale DDoS attacks and prevented BIN attacks with Threat Protection.

1

SETTING THE STAGE

Understanding the growing threat of DDoS attacks

A DDoS attack occurs when cybercriminals intentionally overload an online service or network, such as a website, API, application, or other Internet-facing asset with excessive amounts of traffic. This disrupts normal operations, making systems slow or completely unavailable to legitimate Internet traffic. These attacks are conducted by various threat actors such as hacktivists, financially motivated actors, nation-state sponsored actors, data thieves, and more. Despite their varied motives, these threat actors share a common trait: their attacks are becoming increasingly diverse, frequent, and sophisticated each day. In fact, research shows that DDoS attacks increased 55% from 2023 to 2024.[1]

"The average cost per minute of downtime for a business is approximately $6,130."

The impact caused by DDoS attacks cannot be underestimated. DDoS attacks disrupt business continuity and operations, leading to lost revenue from downtime, reputational damage, and sometimes regulatory fines. It's estimated that the average cost per minute of downtime for a business is approximately $6,130 – that's over $100,000 just for 20 minutes of downtime. On average, the cost of an attack for an SME company is estimated at $50k and starting at $4.5M for larger enterprises depending on the size and industry of the organization.[2] Beyond the financial impact, DDoS attacks can severely damage an organization's reputation, undermining the customer trust that companies spent years building.

[1] G2, 2024

[2] Application Security in a Multi-Cloud World Report, 2023

The role of 3DS and ACS in payment security

Before diving deeper into BIN attacks, it's important to understand 3DS, the industry-standard authentication protocol developed by EMVCo to add an extra layer of security to card-not-present (CNP) transactions. The primary objective of 3DS is to verify the identity of cardholders during an online transaction before the approval to reduce the risk of fraud.

"During a CNP transaction, the issuer must determine whether the transaction is genuinely being made by the cardholder."

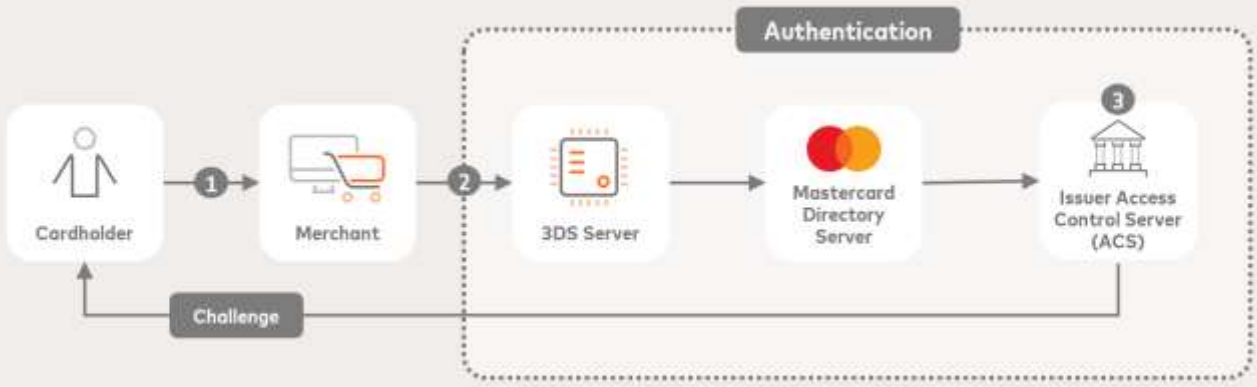
During a CNP transaction, the issuer must determine whether the transaction is genuinely being made by the cardholder. To achieve this, issuers use an ACS (Access Control Server) – either their own or third-party service. The ACS evaluates the transaction based on various data points, such as the device IP address, and ultimately decides if the cardholder has been verified or if additional authentication is needed such as a one-time password or biometric verification. The availability of the ACS is critical to this process as it helps prevent fraud by ensuring that only legitimate cardholders can complete the purchase.

If an ACS is nonresponsive during a Mastercard transaction, Mastercard's Directory Service steps in with Smart Authentication Stand-in and respond to the authentication request on-behalf of the issuer. In this scenario, the issuer remains liable for any fraud, thus highlighting the importance of ACS availability and reliability. Ensuring a fully operational ACS allows issuers to maintain full control over authentication decisions.

How 3DS Works

1. John finds a cool pair of sneakers online and enters his card details at checkout to make the purchase.
2. The online sneaker merchant sends John's payment request to his card issuer for authentication.
3. The issuer's ACS accesses John's transaction and either approves it or challenges John to verify his identity by sending John a one-time passcode to his phone.

Figure 1: 3DS Authentication Process



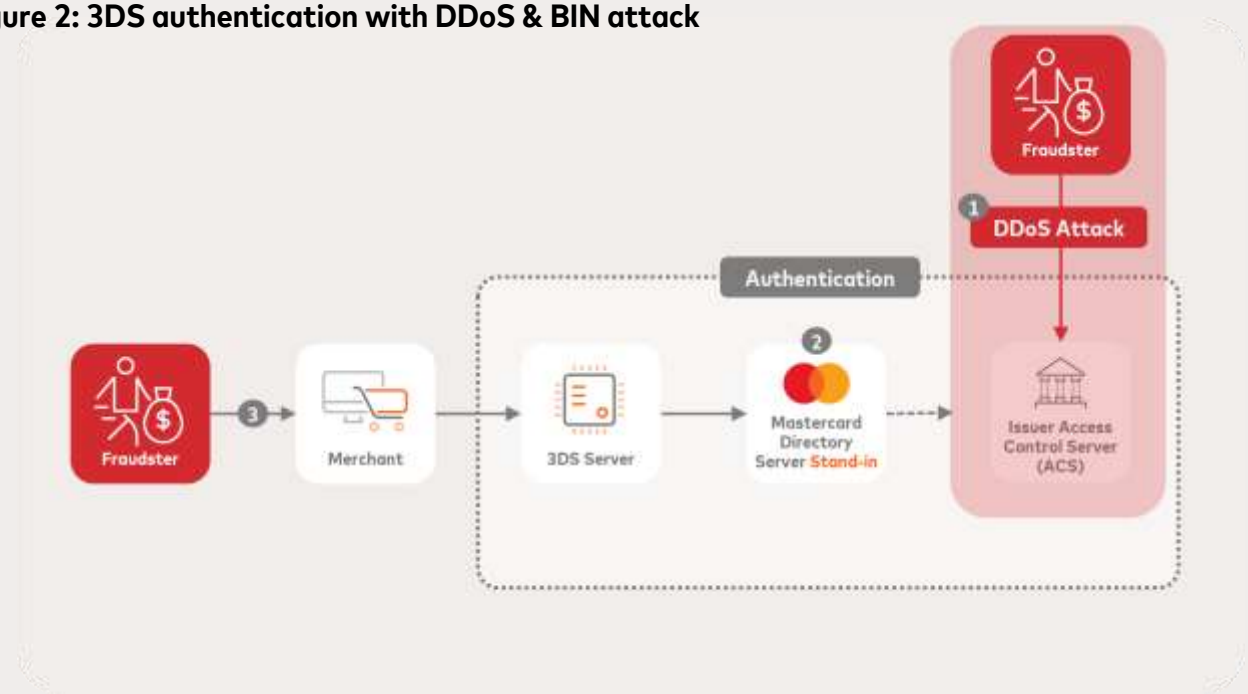
How DDoS attacks threaten the payments ecosystem

DDoS attacks are a significant risk to the payment ecosystem, particularly through BIN attacks targeting the issuer's ACS.

How BIN Attacks Work

1. A DDoS attack floods the issuer's ACS, causing it to crash and become inaccessible.
2. Mastercard's Directory Service and Smart Authentication Stand-in steps, authenticating transactions on behalf of the issuer.
3. Fraudsters take advantage of stand-in services to conduct card testing and get more fraudulent transactions approved.

Figure 2: 3DS authentication with DDoS & BIN attack



2

THREAT PROTECTION

Introducing Threat Protection

Threat Protection is a cloud-based service that can protect any organization's Internet-facing asset, wherever it is hosted, against a wide array of attacks, including DDoS, known bad actors (IPs), and firewall intrusions. Threat Protection is built on a globally distributed, resilient platform (Threat Protection Centers) that ensures high availability at all times. It leverages advanced machine learning and a global sensor network that provides unique IP Reputation and Intelligence to deliver proactive, accurate protection.

Designed for simplicity and operational efficiency, Threat Protection mitigates Layer 4 DDoS attacks and other malicious activities, such as port scanning and traffic from known bad actors, with minimal configuration or effort required from an organization's network, operations, or cybersecurity teams. Fully automated and always-on, it delivers exceptional accuracy with low false positives and negatives.

For organizations requiring application-layer protection, Threat Protection also offers optional Layer 7 defenses that can be configured and fine-tuned through an intuitive online portal. Detailed mitigation data is made available through visual dashboards and APIs.

Threat Protection's robust, full-stack protection enables organizations to receive clean, legitimate traffic while keeping bad actors at bay.

How It Works:

1. **Redirect –** Customers redirect their internet traffic to flow through our solution with a simple change of DNS address.
2. **Clean –** Our Global Threat Protection Centers clean traffic, removing bad traffic at network and application layers.
1. **Receive –** Customers receive good, trusted traffic, enabling businesses to continue operation.

Referring back to the digital payment ecosystem, a robust threat protection strategy is essential to ensure the stability of authentication systems. By actively filtering out bad traffic, our Layer 4 protection safeguards the integrity and availability of an ACS. This provides the issuer and ACS the opportunity to challenge a transaction instead of relying on a stand-in response, effectively blocking card testing attempts. As a result, the issuer retains full control over authentication decisions, reducing liability, fraud risks, and unauthorized transactions.

Enhanced Protection with IP Intelligence

Beyond Layer 4 mitigation, Threat Protection leverages rich IP intelligence to proactively block malicious actors based on previous behaviors and traffic patterns. Our Threat Protection module automatically integrates this intelligence to preemptively block high-risk traffic.

ACS service providers can also benefit from subscribing to our IP intelligence feed for an additional layer of security. With this module, ACS can identify malicious IP addresses in the authentication request, enabling them to make more informed authentication decisions and increase the accuracy of risk-based assessments. This, in turn, reduces the likelihood of fraud for which issuers are liable and decreases their exposure to financial loss.

The synergy between Threat Protection & IP Intelligence

In summary, Threat Protection and IP intelligence offers a comprehensive security framework, addressing both Layer 4 DDoS attacks and BIN attacks while increasing the reliability of the payment network for all ecosystem players. Together, our multi-layered security approach provides issuers and ACS service providers with:

- **Uninterrupted ACS availability** – Threat Protection ensures that an issuer's ACS remains operational to authenticate transactions directly instead of relying on stand-in services. This enables the issuer to retain full control of the authentication decision.
- **Enhanced ACS decisioning** – IP Intelligence gives ACS providers better risk guidance by identifying known malicious IP addresses, allowing the ACS to proactively reject the authentication request even before the challenge.

3

ACS CASE STUDY

Introducing the ACS service provider

Now that we've established the intersection between DDoS, attacks, BIN attacks, and 3DS authentication, it's time to see Threat Protection in action. This case study explores how a leading ACS service provider in Eastern and Southeastern Europe, leveraged Threat Protection to successfully defend against large-scale DDoS attacks and prevent BIN attacks.

This service provider is a key player in Romania, Hungary, Kosovo, Malta and Serbia, processing approximately 73MM authentications annually and representing 70% of the market share.

The growing threat to the provider's infrastructure

Given its strong market presence and critical role in securing digital transactions, any downtime or disruption to its services has severe consequences – not just for its own business, but for issuers, merchants, and cardholders across multiple markets. Prior to Threat Protection, the service provider frequently experienced large-scale DDoS attacks. These attacks severely impacted the authentication process, disrupting 2%-5% of monthly authentication transactions.

The effects of these attacks extended beyond direct downtime. Service disruptions led to long loading times, interrupted communications, and abandoned transactions which ultimately upset the service provider's customers, issuers, but also the cardholders who resorted to choosing alternative payment methods.

Figure 3: Service Provider Authentication Attempts

Deploying Threat Protection for bulletproof security

Recognizing the urgent need for a robust security framework, the provider searched for a solution capable of mitigating large-scale attacks while maintaining seamless availability of its ACS service. In June 2024, the service provider initiated a three-month trial of Threat Protection's Layer 4 DDoS mitigation and web application protection.

Threat Protection initially focused on safeguarding one server, an Eastern European bank covering their public web and card network interfaces.

Operating with a sense of urgency, our team successfully completed the technical deployment within one day. This swift setup enabled immediate protection against cyber threats without disrupting ongoing operations.

The impact of Threat Protection

With Threat Protection in place protecting the availability and reliability of the ACS, the service provider experienced a significant improvement in service stability and security resilience. Threat Protection effectively blocked DDoS attacks including a large volume attack of 500Gbps. The attack lasted over 60 seconds, using large volumes of PSH-ACK packets to overwhelm the network. Even if the attack continued with similar packet counts, sizes, and volume, Threat Protection would have been able to withstand it indefinitely. The patterns of this attack were detected using two major vectors: real-time traffic volume anomalies and TCP flag anomalies. Both of which helped prevent most of the attack.

Attack Traffic Statistics:

- ~1.925 billion packets in 3-minute window
- 500Gbps peak traffic volume
- 97.56% of malicious traffic mitigated

Figure 4: Service Provider DDoS Attack

The effectiveness of Threat Protection clearly reflected in the authentication metrics, demonstrating significant improvements in both authentication rate and Mastercard Stand-In. With Threat Protection in place, the bank (the service provider's customer) experienced a reduction in authentication requests handled by Mastercard's Stand-in service, compared to similar issuers that continued to experience higher reliance on Stand-in services. Stand-in represented 0.59% of the bank's authentication requests, versus similar issuers experienced 4.2%.

In addition, the bank's authentication success rate improved significantly, increasing by 2.85 percentage points from 87.1% in June (prior to the Threat Protection trial) to 89.95% in December. This substantial gain underscores the reliability of the ACS platform, ensuring fewer failed transactions.

2.85%

Percentage point increase in the bank's authentication success rate with Threat Protection.

Threat Protection not only outperformed Akamai and other DDoS providers based these metrics and customer feedback, but also delivered additional benefits, including:

- **Comprehensive reporting** – access to out-of-the-box reporting, real-time monitoring dashboards, and in-depth analysis performed by our team of experts.

- **Dedicated communication channels** – prompt, on-the-spot discussions when an attack is detected to ensure rapid coordination between stakeholders.
- **Rapid time-to-market** – seamless deployment within minimal disruption, ensuring protection begins on day one.

Conclusion

As cyber threats continue to evolve, securing the digital payment ecosystem is more critical than ever. This success story demonstrates how Threat Protection provides a robust, scalable defense against large-scale DDoS attacks, preventing BIN attacks and ensuring uninterrupted availability and security of ACS services.

By leveraging Threat Protection's Layer 4 mitigation, the service provider significantly reduced downtime, minimized reliance on stand-in authentication, and improved overall authentication success rates. These results highlight the importance of a multi-layered security strategy to safeguard the payments ecosystem and beyond.

To further enhance the security of its ACS and strengthen the resilience of its authentication network, the service provider can:

1. **Expand Threat Protection** across all its servers to ensure comprehensive DDoS mitigation and improved service availability.
2. **Integrate IP Intelligence** to gain real-time insights into IP behavior, enabling more accurate authentication decisions and stronger fraud prevention.

By taking these next steps, the service provider can reinforce its defenses against emerging threats, further reducing fraud risks and ensuring seamless, secure digital transactions for its customers.

Interested in learning more about Threat Protection?

Request a demo today and discover how to proactively defend your business with confidence.