NYU Login Portal

Threat Model & Security Analysis

Sample Documentation

By: Michael Kazarian

Document Version: 1.0
Date: January 15, 2026

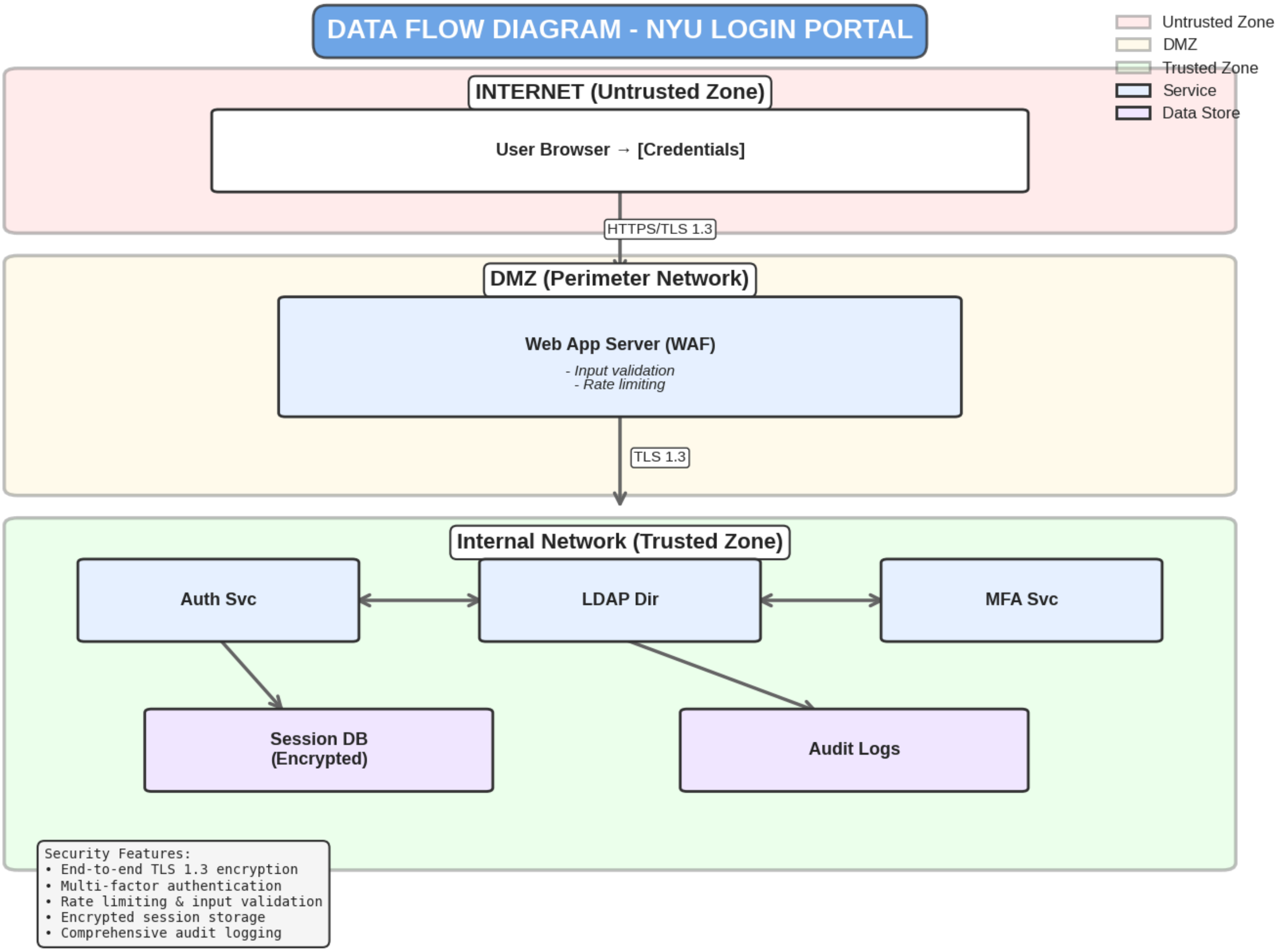
Executive Summary

This document provides a concise threat model for the NYU login portal, a critical authentication gateway serving over 60,000 students, faculty, and staff. The analysis identifies 9 distinct threat scenarios across four STRIDE categories, with particular focus on high-severity risks including credential theft, session hijacking, and authentication bypass attacks. This document is intended to support engineering, infrastructure, and security teams in proactively identifying systemic risk.

0. (Example) Document Governance

- **Author:** Michael Kazarian
- **Reviewed By**: Security Engineering Lead
- **Approved By:** VP Infrastructure
- **Review Cycle:** Quarterly
- **Last Risk Review:** Jan 2026
- **Next Review:** April 2026

1. Data Flow Diagram (DFD)



Security Features:
- End-to-end TLS 1.3 encryption
- Multi-factor authentication
- Rate limiting & input validation
- Encrypted session storage
- Comprehensive audit logging

1.1 Trust Boundaries

1. Internet to DMZ: External users accessing the login portal
2. DMZ to Internal Network: Web application to backend services
3. Internal Services: Authentication, directory, and session management

2. STRIDE Threat Analysis

[Note: “hypothetical risk” reflects industry-wide standards rather than NYU-specific data]

Category	Threat	Mitigation	Impact	Hypothetical Risk
Spoofing	Phishing attacks mimicking NYU login page	Browser security indicators, security awareness training, anti-phishing email filters	Credential theft	**Critical**
	Session token theft via XSS	HTTPOnly/Secure cookies, CSP headers, input sanitization	Session hijacking	**High**
	SAML assertion forgery	RSA-2048 signature verification, assertion expiry	Unauthorized access	**High**
Tampering	SQL injection in auth queries	Parameterized queries, ORM layer, WAF rules, input validation	Data breach	**Critical**
	LDAP injection attacks	LDAP query escaping, least privilege service accounts	Directory compromise	**High**
Denial of Service	Credential stuffing attacks	Account lockout after 5 attempts, CAPTCHA, IP-based rate limiting	Service unavailability	**High**
	DDoS attacks on login endpoint	CDN/WAF with DDoS protection, auto-scaling	System outage	**High**
Elevation of Privilege	Authentication bypass via parameter manipulation	Server-side validation, authorization checks, role verification	Unauthorized access	**Critical**
	Weak password policy	12-char minimum, complexity requirements, MFA	Account compromise	**Medium**

3. Risk Register

ID	Risk	Immediate Business Impact	Risk Level	Likelihood	Owner	Target Resolution Date
R-001	Phishing attacks	Reputational	Critical	High	Security Team	Feb 2026
R-002	SQL injection	Financial	Critical	Medium	Dev Team	Feb 2026
R-003	Auth bypass	Security	Critical	Medium	Dev Team	Feb 2026
R-004	DDoS attacks	Operational	High	High	Infrastructure	Feb 2026

4. Operational Security Guide

4.1 Daily Operations

Monitoring & Alerting

- Review SIEM dashboard for failed login spikes
- Monitor WAF block rate (baseline: <2% of traffic)
- Check certificate expiry (30-day warning)
- Verify MFA service uptime (99.9% SLA)

4.2 Incident Response

Level	Trigger	Response Time (Estimates)	Escalation
P1 - Critical	Service outage, data breach, auth bypass	~15 minutes	CISO + VP IT
P2 - High	Suspected breach, repeated lockouts	~1 hour	Security Manager
P3 - Medium	Performance degradation, unusual traffic	~4 hours	On-call Engineer

Immediate Actions

1. Capture system state (memory dump, network traffic)
2. Preserve audit logs (copy to immutable storage)
3. Initiate communication plan

4.3 Mitigation Validation

- SQL injection mitigations validated via automated penetration testing.
- Rate limiting effectiveness tested with simulated credential stuffing attempts.
- MFA enforcement verified through red-team authentication bypass testing.

4.4 Contact Information

Role	Contact	Availability
Security Operations Center	soc@nyu.edu	24/7/365
Incident Response Team	ir-team@nyu.edu	On-call rotation

5. CORE Issue Management Workflow

1. Risk identified via STRIDE or incident.
2. Risk logged in Jira (issue-tracking software) under CORE category
3. Assigned owner + severity level
4. Weekly review in Engineering Risk Sync
5. Closure verified via mitigation validation testing