OODA-HTTP   SecRoot.io
Internet-Draft   Intended status: Standards Track
2025-06-22   Expires: 2025-12-22

OODA-HTTP: Adaptive Security Framework for HTTP Communications
draft-secroot-ooda-http-00

Abstract

This document defines OODA-HTTP, an adaptive security framework applying the Observe-Orient-Decide-Act loop to HTTP and HTTPS communications. It enables dynamic threat detection and mitigation, including protection against emerging quantum attacks such as those utilizing Shor’s algorithm.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
3. Architectural Overview 4
4. OODA-HTTP Phases 5
  4.1 Observe 5
  4.2 Orient 5
  4.3 Decide 6
  4.4 Act 6
5. Message Formats and Protocol 7
  5.1 JSON Telemetry Payloads 7

5.2 Analysis and Decision Messages 7
6. Threat Models and Detection 8
6.1 Classical Threats 8
6.2 Quantum and Post-Quantum Threats 9
6.3 Extensibility 9
7. Integration with TLS/HTTPS 10
8. Security Considerations 11
9. IANA Considerations 12
10. References 13
Appendix A. Glossary 14
Appendix B. Author's Address 15

1. Introduction

HTTP and HTTPS communications face increasingly sophisticated threats, including quantum computing-based attacks such as those leveraging Shor’s algorithm. OODA-HTTP introduces a real-time adaptive security mechanism based on the OODA loop (Observe-Orient-Decide-Act) to enhance resilience.

2. Terminology

Terms such as OODA loop, threat score, post-quantum cryptography, and Shor’s algorithm are defined for clarity.

3. Architectural Overview

OODA-HTTP integrates telemetry collection, AI-assisted analysis, policy-driven decision making, and dynamic enforcement within HTTP/TLS infrastructure.

4. OODA-HTTP Phases

4.1 Observe

Collection of telemetry data from HTTP headers, TLS handshakes, and logs.

4.2 Orient

Intelligent threat analysis leveraging AI models to score and classify threats.

4.3 Decide

Policy-based decisions on mitigation strategies based on threat scores.

4.4 Act

Enforcement of decisions including key rotations, blocking, alerting.

5. Message Formats and Protocol

5.1 JSON Telemetry Payloads

OODA-HTTP uses structured JSON formats to carry telemetry data, including HTTP headers, TLS handshake parameters, connection metadata, and logs.

5.2 Analysis and Decision Messages

AI analysis results and policy decisions are exchanged as JSON messages specifying threat types, scores, and recommended actions.

6. Threat Models and Detection

6.1 Classical Threats

Includes SQL injection, DDoS, phishing, malware, session hijacking, and other common cyber attacks.

6.2 Quantum and Post-Quantum Threats

Covers emerging quantum attacks such as those leveraging Shor’s algorithm, with mechanisms for detection and mitigation.

6.3 Extensibility

The threat model framework supports addition of new threats and AI prompt templates.

7. Integration with TLS/HTTPS

OODA-HTTP is designed to interoperate with existing TLS termination points, proxies, and clients without protocol modifications.

8. Security Considerations

The protocol ensures confidentiality and integrity of telemetry and control messages and mandates secure channels and authentication.

9. IANA Considerations

Requests registration of new OODA-HTTP message types, threat identifiers, and action codes.

10. References

Lists normative and informative references relevant to the protocol.

Appendix A. Glossary

Defines terms and abbreviations used throughout the document.

Appendix B. Author's Address

Rachid Bouziane
Villa El Majd 171
Tamsna Temara
Rabat, Morocco

Email: contact@secroot.io