Term Project Final Presentation - DNS Record Type Covert Channel Analysis

Yiğit Uçan

Middle East Technical University
Department of Computer Engineering

June 11, 2025

Table of Contents

Project Overview

Key Contribution

End-to-end analysis of a covert channel utilizing DNS record types

- **Phase 2**: DNS covert channel implementation and performance analysis
- **Phase 3**: Covert channel detection system development
- **Phase 4**: Mitigation strategy implementation and effectiveness evaluation

Phase 2: Covert Channel Methods

CNAME Method:

- Data embedded in domain names
- Structure: [data].[seq].[total].example.com
- **≈30 bytes per query**
- **≈12 kB/s capacity**
- Perfect accuracy (1.0)
- Easy to detect (obvious patterns)

Type-Based Method:

- Data encoded in DNS query types
- 2-bit chunks → DNS record types
- Mapping: 00→A, 01→AAAA, 10→CNAME, 11→MX
- **0.25 bytes per query**
- **<3 B/s capacity**
- Timing-sensitive reliability

Focus Selection

Type-based method chosen for later phases: more realistic threat model and detection challenges

Phase 2: Performance Comparison

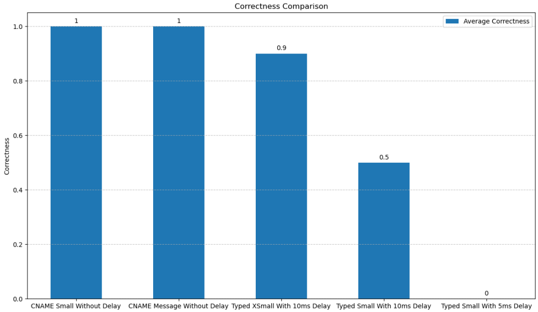


Figure: Correctness comparison: CNAME vs Type-based method

Trade-offs:

- **CNAME**: High capacity, reliable transfer, easily detectable
- **Type-based**: Lower capacity, unreliable transfer, subtle and stealthy

Phase 3: Detection Architecture

Core Components:

- **DNS Analysis**: Extract and analyze record types from intercepted packets
- **Rolling Window**: Analyze recent 100 packets for temporal context
- **Threat/Suspicion Scoring**: Deviation-based suspicion calculation

Statistical Frequency Analysis

Real-time DNS record type frequency monitoring with rolling window analysis

Phase3: Baseline Frequencies

The system establishes a baseline of expected DNS record type frequencies based on real-world network traffic patterns. The baseline categorizes DNS record types into different frequency classes:

- **Extremely High**: A records (40% expected frequency)
- **Very High**: AAAA records (20% expected frequency)
- **High**: NS, PTR, HTTPS, TXT, MX, CNAME, SOA records (8% each)
- **Moderate**: DS, DNSKEY, RRSIG, SRV, NSEC, NSEC3 records (5% each)
- **Low**: CAA, NAPTR, TLSA records (2% each)
- **Very Low**: SSHFP, DNAME records (0.5% each)
- **Extremely Low**: LOC, URI records (0.2% each)
- **Effectively Zero**: HINFO, RP records (0% expected)

Phase 3: Scoring Algorithm Details

Suspicion Score Calculation

Deviation-based scoring with squared penalty for anomalies

Scoring Formula:

- **Normal Range**: $score = 0$ (within 80%-120% of expected)
- **Under-representation**: $score = (expected \times 0.8 - observed)^2$
- **Over-representation**: $score = (observed - expected \times 1.2)^2$

Threat Level Classification:

- **Normal** ($<$50): No suspicious patterns
- **Low** (50-199): Minor deviations
- **Medium** (200-499): Moderate anomalies
- **High** (500-999): Significant activity
- **Critical** ($\geq$1000): Highly likely covert channel

Phase 3: Detection Performance

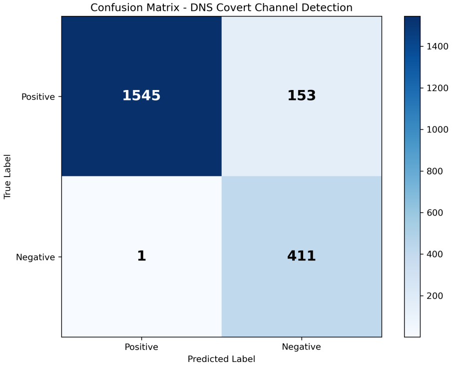


Figure: Detection confusion matrix

Good Performance:

- **92.7% Accuracy**
- **92.6% F2 Score**
- 1545 True Positives
- 411 True Negatives

Key Success Factors:

- Clear separation between normal and covert traffic
- Effective threshold ($\geq$1000)

Phase 4: Mitigation Implementation

Implementation Characteristics:

- **Threshold-Based Activation**: Triggers when suspicion score ≥ 1000
- **Probabilistic Application**: 10% mitigation probability for balance
- **Different Strategies:** Delay and drop mitigation strategies

Design Philosophy

Balance security effectiveness with operational impact on legitimate traffic

Phase 4: Mitigation Strategies

Delay Mitigation:

- 200ms delay on suspicious packets
- Disrupts timing-dependent channels
- Maintains packet integrity

Results:

- 67.1% capacity reduction
- 36.0% correctness remaining

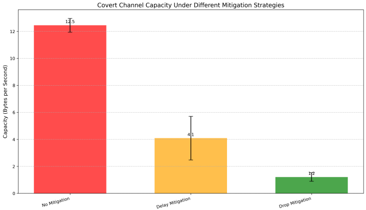
Drop Mitigation:

- Complete packet elimination
- Breaks message sequences
- Creates data gaps

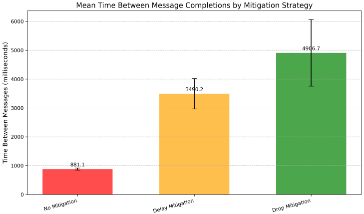
Results:

- **90.3% capacity reduction**
- 18.2% correctness remaining

Phase 4: Mitigation Effectiveness



(a) Capacity comparison



(b) Reassembly time

Figure: Comprehensive Phase 4 mitigation analysis results

Key Findings Summary

Phase 2: Implementation

- Domain name embedding: higher capacity but easily detectable
- Type-based channels: stealthier but timing-sensitive

Phase 3: Detection

- Statistical frequency analysis: **92.7% accuracy**
- Clear separation between normal and covert traffic

Phase 4: Mitigation

- Drop mitigation: **90.3% capacity reduction**
- Delay mitigation: **67.1% capacity reduction**
- Both strategies dramatically impact channel reliability

Future Work

Future Research Directions

- **Adaptive Covert Channels**: Investigation of channels that adapt to detection and mitigation. The current implementation is static and does not adapt to differences in the network.
- **Frequency Analysis Enhancements**: Current detection relies on static frequency baselines. Future work could explore dynamic baselines that adapt to changing network conditions.
- **Hybrid Mitigation**: Combination of multiple mitigation strategies for enhanced effectiveness. For example, drop strategy could be used with packets with higher suspicion scores, while delay strategy could be used with packets with lower suspicion scores.

THANK YOU

Term Project Final Presentation - DNS Record Type Covert Channel Analysis

Repository: github.com/ucanyiit/middlebox

Yiğitcan Uçan
ucan.yigitcan@metu.edu.tr