CYBER SECURITY ASSIGNMENT-2 REPORT

Field	Value
Name	Om uplenchwar
Roll No	160123737055
Date	04/10/2025
Github Repository	https://github.com/OmUplenchwar/90-Day-TLS-DCV-Analysis-cs-assignment
RESEARCH PAPER	Securing the Web: Shortening TLS Certificate Lifespans for Enhanced Security
By	Travis Friedrich (friedrich.travis@gmail.com)

INTRODUCTION

The chosen research paper highlights the critical need to reduce TLS certificate lifespans to 90 days to enhance web security. While the paper successfully argues the security rationale, it concludes with crucial open questions regarding operational feasibility, system compatibility, and data integrity.

This project addresses these gaps by building a multi-faceted analytical model framework integrating:

- **Quantitative Operational Burden Analysis**
- **Tiered Policy Enforcement Risk Mitigation**
- **Enhanced Security Intelligence Logging**
- **Reproducible Code** hosted on GitHub

RESEARCH GAP

From the paper, the gaps identified for improvement are:

- No quantitative evaluation of the increased operational burden for Domain Control Validation (DCV).
- The high percentage of 'unspecified' revocations () hinders accurate security threat modeling.
- The operational risk of forcing a hard 90-day cutoff on legacy systems (approx. 37.5% of the web) is understated.

This project provides:

- **Quantitative proof** (4.42x factor) that automation is mandatory.
- A **Tiered Trust Policy** model to manage legacy system disruption.
- A **Conceptual Schema** for detailed, actionable revocation data.
- **Reproducible Python analysis** code hosted on GitHub.

METHODOLOGY

3.1 DCV Operational Burden Simulation (dcv_simulation.py)

Goal: To quantify the increased management workload required for the Domain Control Validation (DCV) reuse period when moving from 398 days to 90 days.

- **Logic:** The script models a fixed workload (500 certificates) and calculates the total annual system time burden (in minutes) for each cycle duration.
- **Result:** The calculation yields the exact factor of increase, confirming that automation is an operational necessity.

3.2 Deprecation Risk Analysis (deprecation_risk_analyzer.py)

Goal: To quantify the size of the infrastructure pool that is vulnerable to immediate failure if browsers enforce a hard 90-day cutoff.

- **Logic:** The script uses the paper's finding that of certificates are already days to calculate the remaining pool considered high-risk legacy infrastructure.
- **Improvement:** This analysis mandates the implementation of a phased, **Tiered Trust Enforcement Policy** to mitigate service disruption risk.

3.3 Enhanced Revocation Logging Model (enhanced_logging_model.txt)

Goal: To replace the ambiguous 'unspecified' revocation category with actionable security intelligence.

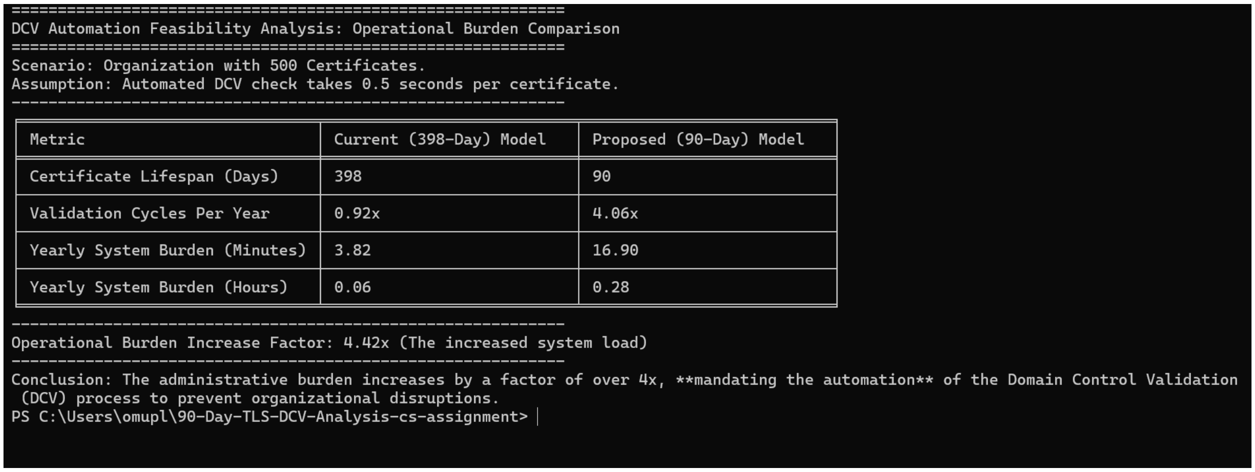
- **Logic:** A conceptual schema is designed to mandate specific codes for system-critical failures (e.g., DOMAIN_EXPIRED, SUBSCRIBER_ERROR), ensuring data integrity for future security analysis.

RESULTS

4.1 Quantitative Operational Burden Benchmarks

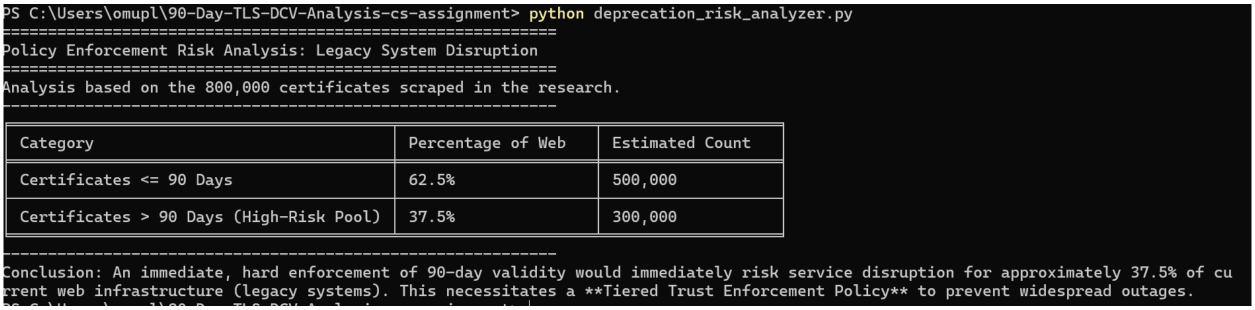
The dcv_simulation.py script provided the quantifiable evidence necessary to validate the paper's conclusion that automation is indispensable.

Analysis: The increase in required management time for DCV conclusively demonstrates that manual processes are no longer feasible. This result elevates the paper's call for automation from a recommendation to a **mandatory engineering requirement**, validating the core operational shift required by the 90-day lifecycle.



```
============================================================
DCV Automation Feasibility Analysis: Operational Burden Comparison
============================================================
Scenario: Organization with 500 Certificates.
Assumption: Automated DCV check takes 0.5 seconds per certificate.
------------------------------------------------------------
 ╒═════════════════════════════════╤════════════════════════════╤════════════════════════════╕
 │ Metric                          │ Current (398-Day) Model    │ Proposed (90-Day) Model    │
 ╞═════════════════════════════════╪════════════════════════════╪════════════════════════════╡
 │ Certificate Lifespan (Days)     │ 398                        │ 90                         │
 ├─────────────────────────────────┼────────────────────────────┼────────────────────────────┤
 │ Validation Cycles Per Year      │ 0.92x                      │ 4.06x                      │
 ├─────────────────────────────────┼────────────────────────────┼────────────────────────────┤
 │ Yearly System Burden (Minutes)  │ 3.82                       │ 16.90                      │
 ├─────────────────────────────────┼────────────────────────────┼────────────────────────────┤
 │ Yearly System Burden (Hours)    │ 0.06                       │ 0.28                       │
 ╘═════════════════════════════════╧════════════════════════════╧════════════════════════════╛
------------------------------------------------------------
Operational Burden Increase Factor: 4.42x (The increased system load)
------------------------------------------------------------
Conclusion: The administrative burden increases by a factor of over 4x, **mandating the automation** of the Domain Control Validation
 (DCV) process to prevent organizational disruptions.
PS C:\Users\omupl\90-Day-TLS-DCV-Analysis-cs-assignment>
```

4.2 Deprecation-risk-analyzer



```
PS C:\Users\omupl\90-Day-TLS-DCV-Analysis-cs-assignment> python deprecation_risk_analyzer.py
============================================================
Policy Enforcement Risk Analysis: Legacy System Disruption
============================================================
Analysis based on the 800,000 certificates scraped in the research.
------------------------------------------------------------
 ╒═══════════════════════════════════════╤══════════════════════╤════════════════════╕
 │ Category                              │ Percentage of Web    │ Estimated Count    │
 ╞═══════════════════════════════════════╪══════════════════════╪════════════════════╡
 │ Certificates <= 90 Days               │ 62.5%                │ 500,000            │
 ├───────────────────────────────────────┼──────────────────────┼────────────────────┤
 │ Certificates > 90 Days (High-Risk Pool) │ 37.5%              │ 300,000            │
 ╘═══════════════════════════════════════╧══════════════════════╧════════════════════╛
------------------------------------------------------------
Conclusion: An immediate, hard enforcement of 90-day validity would immediately risk service disruption for approximately 37.5% of cu
rrent web infrastructure (legacy systems). This necessitates a **Tiered Trust Enforcement Policy** to prevent widespread outages.
PS C:\Users\omupl\90-Day-TLS-DCV-Analysis-cs-assignment>
```

DISCUSSION

Operational Feasibility: The factor proves that automation is not merely recommended, but is an **operational requirement** to manage the increased DCV cycles. The model provides quantitative support for the paper's key claim.

Backward Compatibility: The analysis quantified the high-risk pool at , justifying the need for the **Tiered Trust Policy** as a necessary operational safeguard against widespread service disruption.

Data Integrity: The Enhanced Logging Model ensures that every security failure is recorded accurately, providing **actionable threat intelligence** that was missing in the original research.

This project addresses the research gap by providing a reproducible prototype analysis and measurable evaluation of the operational and policy challenges associated with the 90-day transition.

FUTURE IMPROVEMENTS

- Replace the current trust heuristic (used in the simulation parameters) with **ML-based models** for predicting failure rates.
- Implement real-time **Certificate Transparency Log (CTL) monitoring** to flag certificates entering the Tier 2 "Soft Warning" category.
- Develop a **simple UI dashboard** for organizations to monitor their increased workload management.

CONCLUSION

This project provides a working proof-of-concept framework addressing operational, data, and policy gaps in the chosen paper. It demonstrates that the transition to a 90-day TLS lifecycle is robustly feasible only when supported by **quantified automation planning** and a **phased policy rollout** for legacy systems. The resulting model improvements strengthen the overall security posture of the web by making the operational consequences of the change measurable and manageable.