My Dissertation Learning Journal

Sriram Kirthivas (kirthivs@tcd.ie)

Started: October 14, 2025

Contents

1 October 2025 - Protocol Fundamentals

1.1 Week 1: October 14-21, 2025

Focus Area: TLS Protocol Fundamentals

What I learned:

- **TLS (Transport Layer Security):** A cryptographic protocol designed to provide security over computer networks such as the Internet
- TLS primarily provides privacy through use of cryptography such as certificates
- TLS runs in the presentation layer and is composed of TLS Record Protocol and TLS Handshake Protocol
- The handshake protocol establishes the cryptographic parameters for the session
- TLS 1.3 is the current version with improved security and performance over earlier versions

Key Concepts:

- Symmetric vs. asymmetric encryption in TLS
- Certificate chain validation
- Perfect Forward Secrecy (PFS)

Questions/To Review:

- How do certificate authorities (CAs) validate domain ownership?
- What are the differences between TLS 1.2 and TLS 1.3?
- How does TLS relate to SSH and SMTP in terms of security guarantees?

1.2 Week 2: October 22-28, 2025

Focus Area: SSH Protocol and SMTP Basics

What I learned:

- **SSH (Secure Shell):** A cryptographic network protocol for secure remote login and command execution
- SSH uses public-key cryptography for authentication
- SSH host keys are used to verify server identity (relevant for key re-use detection)
- **SMTP (Simple Mail Transfer Protocol):** The protocol used for email transmission between mail servers

- SMTP runs on port 25 by default (the port we'll be scanning)
- STARTTLS command upgrades plaintext SMTP connections to encrypted TLS

Key Concepts:

- SSH key fingerprinting methods (MD5, SHA256)
- SMTP command sequence: HELO/EHLO, MAIL FROM, RCPT TO, DATA
- Opportunistic TLS vs. mandatory TLS in email

Relevance to Dissertation:

- Port 25 scanning will identify SMTP servers in Irish IPv4 space
- TLS certificates from STARTTLS connections will be analyzed for key re-use
- Understanding SMTP is essential for responsible scanning practices

Questions/To Review:

- What percentage of mail servers support STARTTLS?
- How are SMTP server certificates typically managed in practice?
- What are common misconfigurations that lead to key re-use?

1.3 Week 3: October 29 - November 4, 2025

Focus Area: TLS/SMTP Integration and Certificate Basics

What I learned:

- How SMTP servers negotiate TLS through STARTTLS command
- X.509 certificate structure and fields (subject, issuer, validity, public key)
- Self-signed certificates vs. CA-signed certificates in mail servers
- Many mail servers use self-signed certificates, making key re-use analysis important
- Certificate Subject Alternative Names (SANs) for multiple domains

Key Concepts:

- Certificate fingerprinting using SHA-256 hash
- Public key extraction from certificates
- Distinction between certificate re-use and key re-use

Practical Exercises:

- Used `openssl s_client` to connect to mail servers and inspect certificates
- Practiced extracting public keys from certificates using OpenSSL commands
- Examined certificate chains from major email providers

Questions/To Review:

- What is the average lifespan of mail server certificates in the wild?
- How common are wildcard certificates in email infrastructure?
- Review the "Clusters of Re-used Keys" paper methodology

---

2 November 2025 - Scanning Approaches and Research

2.1 Week 4: November 5-11, 2025

Focus Area: Internet-Wide Scanning Concepts

What I learned:

- **Internet-wide scanning:** Systematic probing of IPv4 address space to identify hosts and services
- Difference between horizontal scans (one port, many hosts) and vertical scans (many ports, one host)
- Our dissertation will use horizontal scanning on port 25 (SMTP)
- **Local scanning approach:** Focusing on Irish IPv4 space rather than global Internet
- Ethical considerations: rate limiting, respecting robots.txt, responsible disclosure
- Legal framework: Irish and EU regulations on network scanning

Key Concepts:

- IPv4 address space: approximately 4.3 billion addresses
- Irish IPv4 allocation: much smaller subset, needs identification via RIR data
- RIPE NCC as the Regional Internet Registry for Europe
- Autonomous System Numbers (ASNs) for identifying Irish networks

Research Papers Started:

- "Clusters of Re-used Keys" paper - initial reading

- ZMap paper - "Fast Internet-Wide Scanning and Its Security Applications"
- Notes on responsible scanning practices from security research community

Next Steps:

- Deep dive into "Clusters of Re-used Keys" paper methodology
- Identify Irish IPv4 address ranges from RIPE database
- Research cryptographic key management best practices
- Begin outlining scanning methodology for dissertation

Questions/To Review:

- How many IPv4 addresses are allocated to Ireland?
- What scan rate is considered ethical and non-disruptive?
- What are the legal requirements for notification before scanning?
- How do we handle complaints or takedown requests during scanning?
