The Best TLS Training in the World
Day 1: SSL/TLS

Designed by the author of the much-acclaimed *Bulletproof SSL and TLS*, this practical course will teach you how to deploy secure servers and encrypted web applications during a day packed with theory and practical work. We'll focus on what you need in your daily work to deliver best security, availability and performance. And you will learn how to get an A+ on SSL Labs!

- Understand threats and attacks against encryption
- Identify real risks that apply to your systems
- Deploy servers with strong private keys and valid certificates
- Deploy TLS configurations with strong encryption and forward secrecy
- Understand higher-level attacks against web applications
- Use the latest defence technologies, such as HSTS, CSP, and HPKP

Course Outline – Day 1

1. Introduction
   a. The need for network encryption
   b. Understanding encrypted communication
   c. The role of public key infrastructure (PKI)
   d. SSL/TLS and Internet PKI threat model

2. Keys and certificates
   a. RSA and ECDSA: selecting key algorithm and size
   b. Certificate hostnames and lifetime
   c. Practical work:
      i. Private key generation
      ii. Certificate Signing Request (CSR) generation
      iii. Self-signed certificates
      iv. Obtaining valid certificates from Let's Encrypt
   d. Sidebar: Revocation

3. Protocols and cipher suites
   a. Protocol security
   b. Key exchange strength
   c. Forward security
   d. Cipher suite configuration
   e. Practical work
      i. Secure web server configuration
      ii. Server testing using SSL Labs
   f. Sidebar: Server Name indication (SNI)
   g. Sidebar: Performance considerations

4. HTTPS topics
   a. Man-in-the-middle attacks
   b. Mixed content
   c. Cookie security
   d. CRIME: Information leakage via compression
   e. HTTP Strict Transport Security
   f. Content Security Policy
   g. HTTP Public Key Pinning
   h. Practical work:
      i. Deploying HSTS to deploy robust encryption
      ii. Deploying CSP to deal with mixed content

5. Putting it all together: Getting A+ in SSL Labs
Day 2: Internet PKI

During Day 2, we'll start with the basics and the theory, then discuss how the PKI is implemented in the real world, and finish with a practical example of a realistic private certification authority. You will learn methods which you can easily replicate in your own work.

- Learn about key PKI standards and formats
- Understand where practice differs from theory
- Analyze certificate lifecycle in detail
- Evaluate PKI weaknesses and how they affect you
- Deploy robust protection using public key pinning
- Learn about what's coming in the future
- Practise what you've learned

By the end of the day you will have built a fully-functioning private CA—with multiple intermediate CAs and revocation—using a method that you can easily replicate.

Course Outline - Day 2

1. Introduction
2. Standards
    a. X.509 certificates
    b. Certificate chains
    c. Name constraints
    d. Trust path building
    e. Validation process
3. Internet PKI
    a. Certification Authorities
    b. Relying parties
    c. Certificate types (DV, EV, OV)
    d. Certificate lifecycle (validation, issuance, and revocation)
    e. CA/B Forum and its standards
    f. Weaknesses
    g. History of attacks
4. Revocation
    a. CRL
    b. OCSP
    c. OCSP stapling
    d. CRLsets and OneCRL
    e. Short-lived certificates
5. Defenses
    a. Certification Authority Authorization (CAA)
    b. Public key pinning
        i. Static pinning
        ii. HPKP
        iii. DNSSEC/DANE
6. Certificate Transparency
7. PKI ecosystem monitoring
    a. SSL Pulse
    b. Censys
    c. crt.sh
Project: Building and deploying a realistic private CA

Meet the Trainer

Scott Helme is a security researcher, consultant and international speaker. He can often be found talking about web security and performance online and helping organisations better deploy both. Founder of report-uri.io, a free CSP report collection service, and securityheaders.io, a free security analyser, Scott has a tendency to always be involved in building something new and exciting.