Identities Exposed

Privacy Risks with Using Client Certificates for Authentication

David Johansson | Senior Consultant | Cigital Ltd.
Objectives

Objectives for this Tech Talk:
• Know the risks to user privacy when client certificate authentication is used
• Understand browser settings that affect user privacy
• Be aware of how attackers can spoof web sites to expose the identity of connecting clients
• Understand why you need to limit PII in certificates when you deploy client certificate authentication
Client Certificate Usage

- Server-to-Server Authentication
- Authentication of Devices
- Strong Authentication of Individuals
  - Provides stronger authentication than passwords
  - Can be 2-factor authentication (e.g., smartcard and PIN)
  - Acts as a “digital passport”

X.509 v3 certificates can be seen as a digital version of a passport.
Digital Certificates (X.509 v3)

Name
Issuer
Validity

Also contains:
- Serial number
- Information binding it to the subject
- Forgery protection, etc.
Identity Information

Information stored in client certificates may include:

• Name
• Organization
• Email
• User ID (e.g. UPN in AD)
• Date of Birth, SSN or equivalent
• Telephone Number
• Etc.

If exposed to attackers, this information can be used to track users, collect valid user names, social engineering, etc.
Privacy Risks with Client Certificates

• Privacy Risks Covered Today
  • Browser issues
  • SSL/TLS protocol issues

• Other Privacy Risks
  • Vulnerabilities in browser plugins
  • Lost or stolen smart card
  • Etc.
Mutual Authentication in SSL/TLS

- Client and server wants to establish a secure connection
- Server may ask for client certificate during SSL/TLS handshake
- Privacy requirements for clients:
  - I want to know when I authenticate
  - I want to know who I communicate with
  - I want to know that only the intended recipient can see my identity
Issue #1: Browser Configuration

- Browser may send client certificate without user interaction
  - Users are automatically logged in
  - Usually not enabled by default
- Any site you visit may request a client certificate
- User’s identity may be exposed without their knowledge

Browser may be configured to automatically send client certificate.
Ensure that users are aware of *when* they expose their identity:

- In general, don’t enable automatic submission of client certificates in browsers
- If needed, only allow automatic selection for the “Local intranet” zone in Internet Explorer (limits exposure to internal systems)
- Raise user awareness of privacy risks – only submit client certificate when talking with a trusted server

But are we safe if we only send our client certificate to trusted servers?
Issue #2: Browser Failure (IE & Chrome)

The user is warned of the certificate error, but the identity of the client is already exposed.
Ensure that users are aware of who they expose their identity to:

- Certificate pinning? (Doesn’t help here!)
- Avoid Internet Explorer and Chrome when using client certificates – prefer Firefox or Safari
- Or get Microsoft and Google to fix this...

But are we safe if the browser always validates the server certificate before sending the client certificate?
No explicit validation of private key possession:

- SSL/TLS only validates server’s possession of the private key for Server Key Exchange messages
- For most ciphers, only implicit validation is done (i.e., encryption fails)
- Malicious servers can exploit this by choosing an appropriate cipher suite, i.e., one that doesn’t require additional key material, such as TLS_RSA_WITH_AES_256_CBC_SHA
The SSL/TLS connection then fails, but the identity of the client is already exposed.
Issue #3: Remediation

Ensure that users are aware of *who* they expose their identity to (again):

- Only support ciphers that require explicit validation of private key (requires changes in both servers and browsers)
- Or wait for TLS 1.3 (current draft always require explicit proof of private key possession)

But are we safe if the browser always validates the server certificate AND private key possession before sending the client certificate?
Issue #4: Certificate Sent in Plaintext

Server

Client

Client Hello

Server Hello

Server Certificate

Server Key Exchange*

Certificate Request

Server Hello Done

Client Certificate

Client Key Exchange

Certificate Verify

ChangeCipherSpec

Ciphertext

Plaintext

Finished

Eavesdropping on network communication

*Server Key Exchange is only sent when more than the server certificate is needed for the key exchange, e.g. ephemeral Diffie-Hellman.
Ensure that users’ identity information is **protected** when they authenticate:

- Establish “normal” TLS connection first without client certificate, then renegotiate connection to send client certificate
- Implement warnings in browsers before sending client certificate in clear text
- Or wait for TLS 1.3 (certificates are encrypted within the handshake in current draft)
Conclusion

Key takeaways:

• Don’t forget to consider user privacy when designing authentication solutions

• SSL/TLS provides no protection for information stored in client certificates

• TLS 1.3 will provide better privacy protection

• Limit use of PII in client certificates
  • Use anonymous identifiers
  • Lookup required information server-side

Limit use of PII in client certificates, use an id to lookup additional data when needed.
• I will also be available at Cigital’s stand (A170) for the rest of this day

David Johansson
djohansson@cigital.com