Limited Proxying for Content Filtering based on X.509 Proxy Certificate Profile

Islam Faisal* and Sherif El-Kassas
The American University in Cairo, Egypt

* Travel supported by AUC Undergraduate Research Grant UG#1810898

Content Filtering: What and Why?

Inspecting web traffic for several reasons including:

- Parental Access Control
- Antivirus, Antimalware services
- Enterprises to filter contents for employees
- Surveillance and censorship
- Ad Blockers

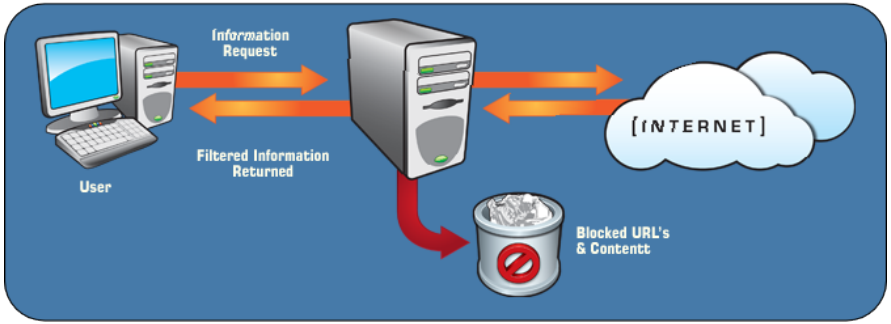


Image Credit power1inc.com

Man-In-The-Middle Model for Web Proxy

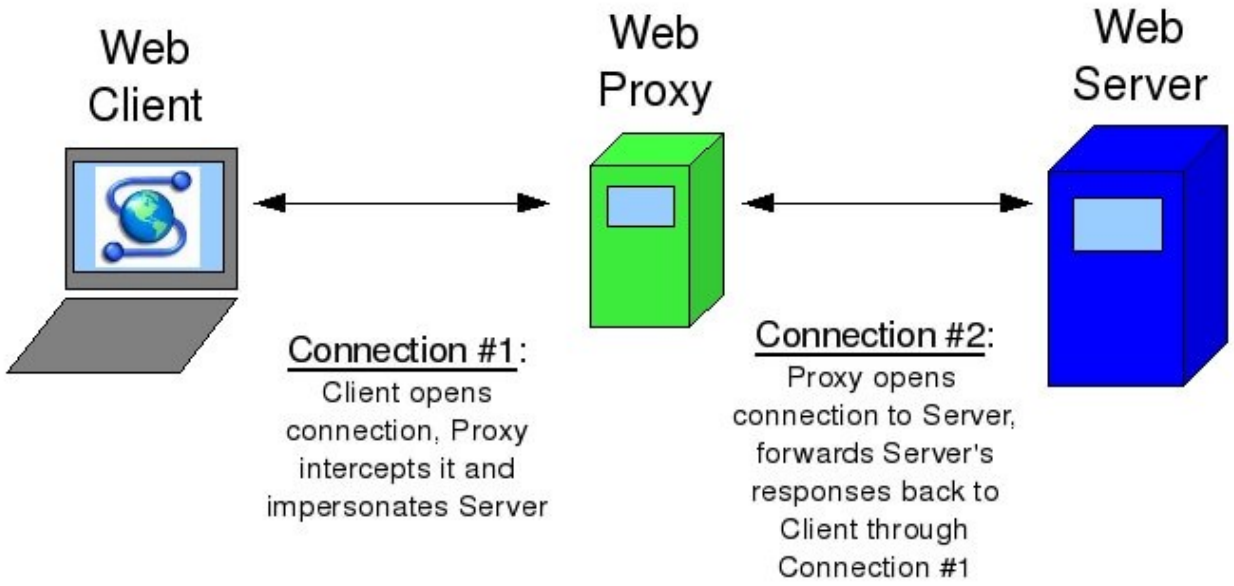


Image Credits: Ivan Kristianto

Transport Layer Security (TLS)

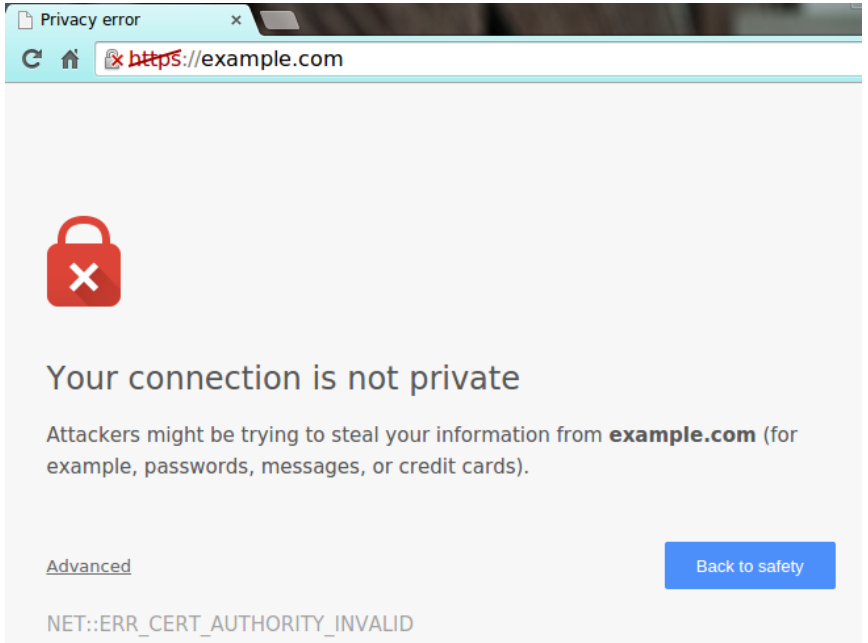
- Creates an authenticated encrypted communication channel between two endpoints
- In a client-server connection, a client can verify the identity of the server by:
  - Validating the introduced digital certificate
- It is up to the client (via the browser) to accept or reject the certificate
- TLS assumes all functionality must reside at the endpoints
  - Middlebox network security solutions are not “legal” under this assumption
  - Middleboxes resort to hacking or going around the protocol

Image Credit: swhosting.com

Invalid and Forged Certificates

Certificate misuse occurs for many reasons including:

- Legitimate proxies of which the user is aware:
  - Certificates are self-signed
  - The proxy is added to the list of certificate authorities by the user or IT personnel
- Server Misconfiguration
- Expired Certificates
- Forged Certificates by attackers



Why is intercepting TLS not a good idea? (Durumeric et al.)

Doesn’t distinguish an attacker from a legitimate proxy

Doesn’t inform the client and server that the connection is intercepted

Content can be modified

It is a **veil all** or **reveal all** strategy

Can degrade TLS security by using older versions or weaker cipher suites

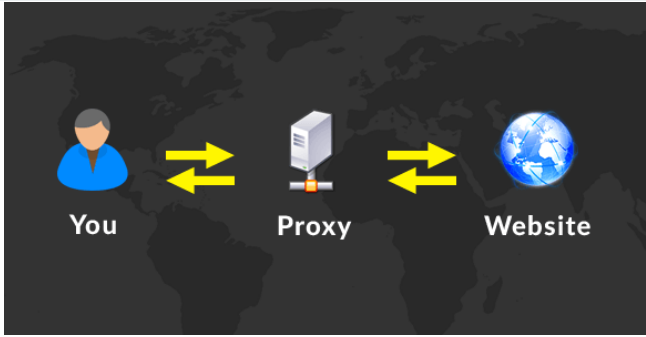
Alternatives to TLS Interception

- HTTP 2.0 Explicit Trusted Proxy (Loreto et al.)
  - Requires middleboxes to explicitly notify the client of interception
- TLS Proxy Server Extension (McGrew et al.):
  - Requiring the proxy to indicate the interception, and to additionally relay proxy–server session information back to the client
- Multi-context TLS (mcTLS) (Naylor et al.):
  - an extended version of TLS that requires endpoints to explicitly specify permitted middleboxes in order to securely authenticate each hop and cryptographically control exactly what data middleboxes can access.
  - Proven insecure by formal analysis (Bhargavan et al.)
- BlindBox (Sherry et al.): Deep Packet Inspection over encrypted traffic
- **Our Method: Using Proxy Certificate Profiles**

Security Requirements

- ➔ **Authorized Proxying**: Proxy connections are only accepted from proxies with valid certificates
- ➔ **Limited Proxying**: The client and server have control over what pages or parts of traffic can be shared with the proxy.
- ➔ **Limited-Depth Proxying:** The depth of the chain of delegation is controlled by the entity delegating the proxy.
- ➔ **Proxy Detection:** The client and server can **distinguish** proxy connections from direct connections.
- ➔ **Path Validation:** The relying party can trace the path of the delegation and verify that the delegation is legitimate.

Our Framework



- All entities are properly identified by X.509 Certificates
- The Client issues a proxy certificate to the proxy
- The proxy establishes a connection to both the client and the server with valid certificates
- The client (via the browser) and server bears the responsibility of choosing what content to share over a proxy

Image Credit: hideoxy.com

X.509 Proxy Certificate Profile (RFC 3820)

- X.509 is a standard that defines the format of public key certificates
- Proxy Certificate Profile is an extension to X.509 introduced in RFC 3820
  - Defines mechanisms for the format, issuance, and validation of proxy certificates
- In X.509 each entity is identified by:
  - End Entity Certificate (EEC): Identifies who the entity is
  - Authorization Certificate(AC): Defines what the entity can do
- A proxy certificate is a means of delegating restricted privileges to an entity:
  - Issued by a holder of an End Entity Certificate or another Proxy Certificate
  - Delegating some of the privileges they legitimately own either by an authorization or a proxy certificate
- A proxy certificate is validated by the relying party by tracing the path up to a root trusted issuer
- The profile defines fields for defining what is delegated and the depth of delegation

Terminology (RFC 3280, RFC 5280, RFC 5755)

- **Certificate Authority (CA):** Authority that is authorized to certify entities.
- **Attribute Certificate (AC):** Contains the attributes associated with an end entity.
- **Certificate Revocation List (CRL):** Certificates that were revoked before their expiry dates.
- **Attribute Authority (AA):** An authority that can issue attribute certificates.

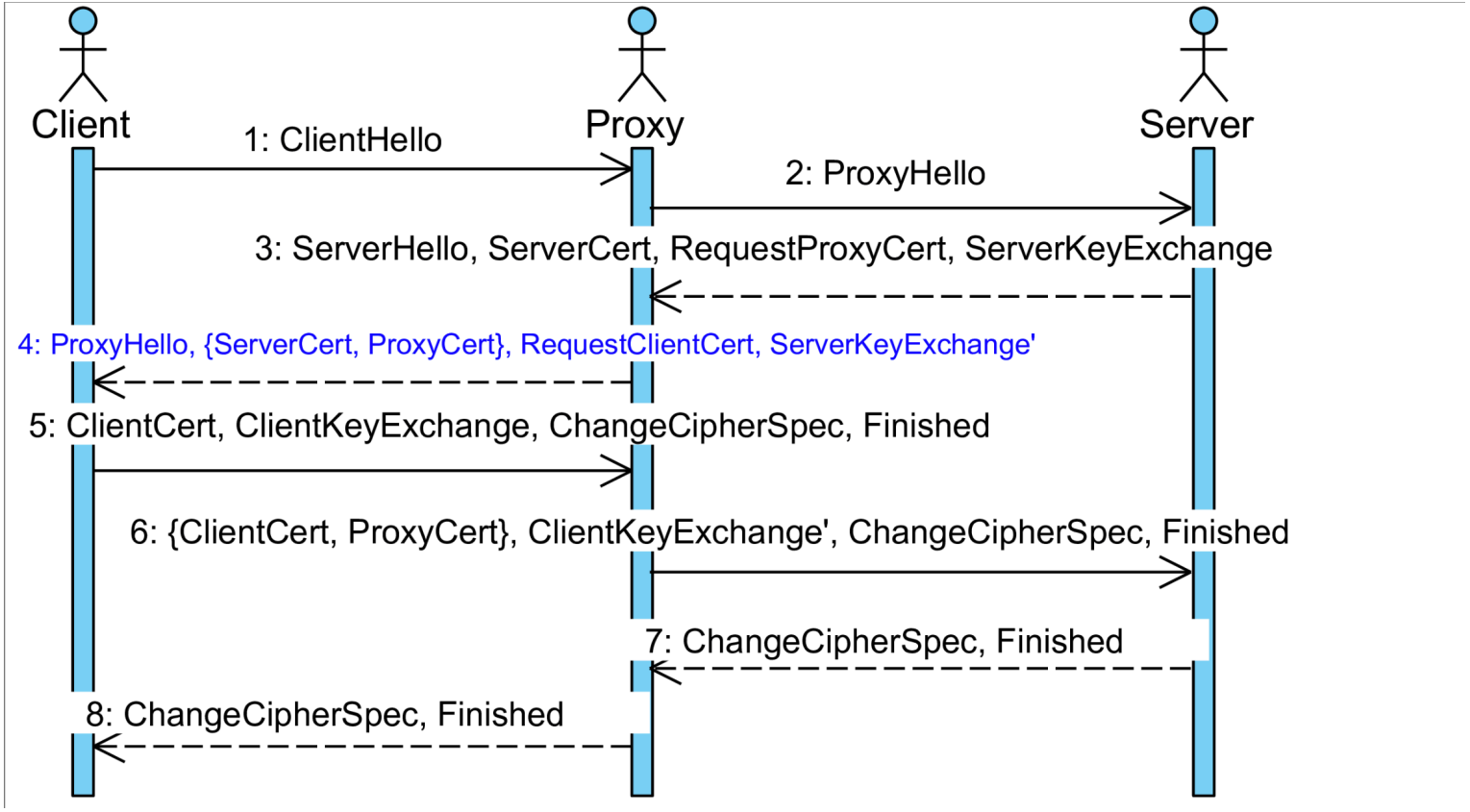
Proxy Certificate Profile

- **Proxy Certificate (PC):** A Certificate with special fields issued by an end entity delegating some of its privileges to another entity.
- **Proxy Issuer (PI):** An entity with an End Entity Certificate or Proxy Certificate that issues a Proxy Certificate.

Proxy Certificates Fields for Content Filtering

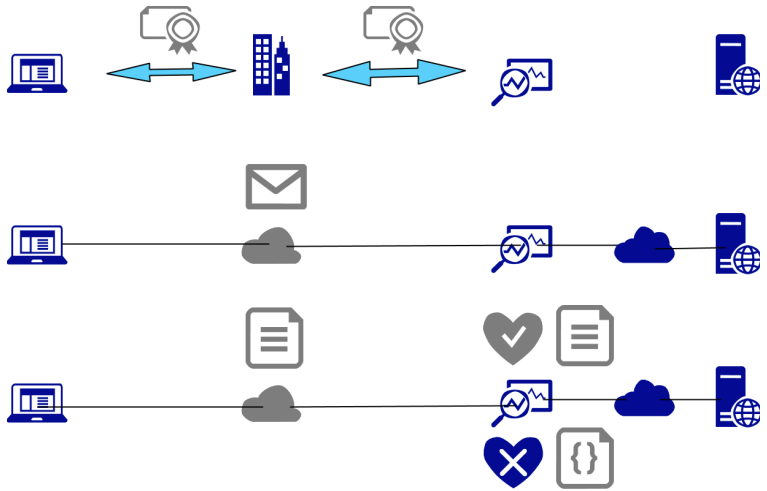
- Delegation Depth
- Allowed and disallowed domains the proxy can intercept
- Cipher suites allowed to be used by the proxy
- *Trust Level (t):* An integer that the client and server can mutually interpret
    - Each content is assigned a sensitivity level, and shared via proxy only if $s < t$

Proposed Proxy Handshake



Application: Enterprise Security

- Client (employee) issues a proxy certificate of depth 1 to Acme company
- Acme issues a proxy certificate of depth 0 to the proxy
- The employee can control what can be proxied by the enterprise.



Conclusion and Future Work

Proposed a method for limited proxying for content filtering

Provides clients with revokable fine-grained access control

Future Work

Analyzing how this work is applicable in the newly ratified TLS 1.3 and prove the security properties with formal methods.

Implement the framework in a software library and testing within browsers

References

- Farrell, S. and Housley, R. (2002). An Internet Attribute Certificate Profile for Authorization. RFC 3281, RFCEditor.
- Foster, I. and Kesselman, C. (1998a). Computational grids:The future of high performance distributed computing.
- Foster, I. and Kesselman, C. (1998b). The globus project: a status report. In Heterogeneous Computing Workshop,1998. (HCW 98) Proceedings. 1998 Seventh, pages 4–18.
- Foster, I., Kesselman, C., Tsudik, G., and Tuecke, S. (1998).A security architecture for computational grids. In Proceedings of the 5th ACM Conference on Computer and Communications Security, CCS '98, pages 83–92,New York, NY, USA. ACM.
- Housley, R., Ford, W., Polk, T., and Solo, D. (2002). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280,RFC Editor.
- Murdoch, S. J. and Anderson, R. (2008). Tools and technology of internet filtering.Access denied: The practice and policy of global internet filtering, 1(1):58.
- Novotny, J., Tuecke, S., and Welch, V. (2001). An online credential repository for the grid: Myproxy. In Proceedings 10th IEEE International Symposium on High Performance Distributed Computing, pages 104–111.
- Tuecke, S., Welch, V., Pearlman, D. E. L., , and Thompson,M. (2004). Internet X.509 Public Key Infrastructure(PKI) Proxy Certificate Profile. RFC 3820, RFC Editor
- Huang, L. S., Rice, A., Ellingsen, E., & Jackson, C. (2014, May). Analyzing forged SSL certificates in the wild. In Security and privacy (sp), 2014 ieee symposium on (pp. 83-97). IEEE.