Secure Services for the Extensible Internet

Project #13 — William Lin, Cathy Lu, and Zach Van Hyfte

Background

Extensible Internet

- Private networks are increasingly deploying novel in-network services (custom caching, load balancing, etc.) while the public internet falls behind.
- The Extensible Internet is an effort to bring in-network services to the public internet through a consistent, open architecture that can be deployed across public and private networks alike.
  - Adds a new service layer (Layer 3.5) to the OSI model.
  - Services are provided by **service nodes**, commodity servers on the network edge with a set of public services chosen through IETF-like governance process.
    - Anyone can add a new service node to the network (somewhat like with Tor nodes).

Securing Service Nodes

- *Threat model:* Internal actors with physical accesses (e.g. rogue server operators, malicious network provider).
- *Solution:* Run service nodes inside secure **AMD SEV enclaves**.
  - Remote attestation is performed when a client first establishes its long-lived connection to local service node.

Our Project: EI Services

- We implemented **two services** that run on top of EI service nodes, both of which leverage the unique position and security properties of service nodes to enhance internet security and privacy.
  - Both demonstrate how EI makes it **easier to deploy secure services and adopt stronger security practices**.

Problem

Remote Attestation

- Enclave platforms like Intel SGX provide a way for the users of a third-party web service running in an enclave to verify that the service's code or execution environment has not been tampered with.
- Some issues preventing common adoption of this practice:
  - **Scalability:** Every single client device need to securely obtain updated enclave code hashes whenever the code changes
  - **Latency:** For SGX, every time a client connects to an enclaved service, it needs to communicate with the Intel Attestation Verification Service to validate the attestation "quote" received from the enclave.

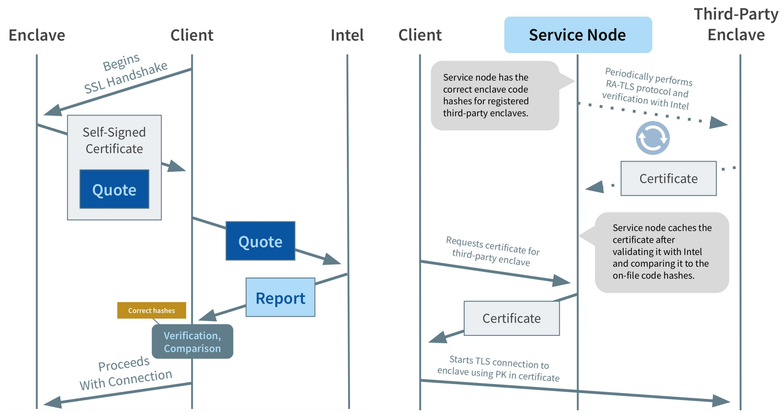
Oblivious DNS

- DNS recursive resolvers (Google, OpenDNS, ISPs) can see which domains and subdomains individual clients are visiting.
- In the Oblivious DNS protocol (Schmitt *et al.* 2019), DNS queries are encrypted with the public key of the resolver, and an additional party is added between name servers and the resolver, ensuring that no one party can link domain name queries to individual clients.
  - However, this increases both the **latency** of DNS queries and the **amount of DNS infrastructure** required.

Solution

Practical Remote Attestation

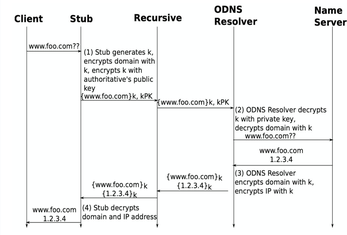
Standard RA-TLS Remote Attestation ***EI-Assisted Remote Attestation***



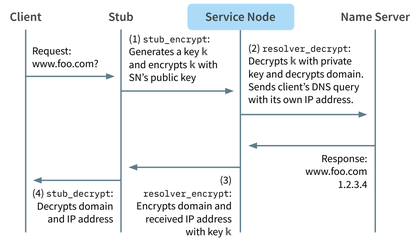
- The **attestation service** on each service node:
  - Has access to a list of up-to-date enclave code hashes for different third-party services, maintained by the EI governance body.
    - Services now distribute their correct hashes to just one party.
  - Periodically performs RA-TLS remote attestation for each of the enclaves on its list and caches the verified certificates.
    - Only the enclave knows the private key associated with the certificate's public key.
- Each **client**, when connecting to an enclaved third-party service for the first time:
  - Fetches the verified certificate from the attestation service
  - Uses the verified certificate to connect to the third-party service, making sure that it matches the certificate provided in the TLS handshake.
    - No longer needs to contact Intel to validate an attestation report.

Optimized Oblivious DNS

- Because service nodes run trusted open-source code in secure enclaves, they can serve as secure, private DNS recursive resolvers.
  - Eliminates a network hop for both the DNS query and the response.



Original ODNS Protocol. Figure from Schmitt *et. al.* 2019, *Oblivious DNS: Practical Privacy for DNS Queries*

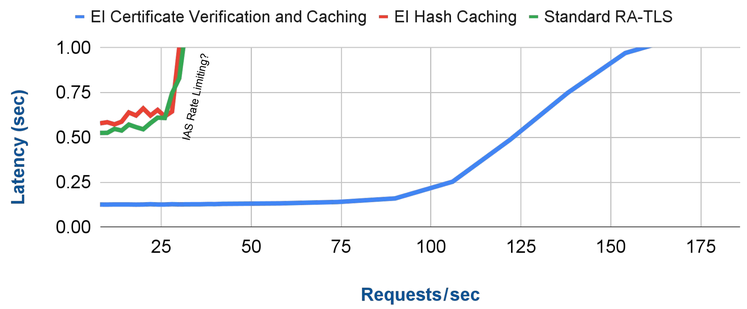


Optimized ODNS Protocol. The recursive resolver can be eliminated because the service node is verified to be running specific source code.

Results

Practical Remote Attestation

- Latencies for connecting to a third-party service start out much smaller than with client-side RA-TLS, and do not scale up as quickly.



Optimized Oblivious DNS

- The cryptographic overhead of ODNS limits its throughput compared to non-secure standard DNS, but our optimizations bring ODNS' latencies much closer to those of standard DNS.
  - We are currently exploring optimizations to lower the cryptographic overhead of our ODNS implementation.