FORMAL VERIFICATION OF TLS IN THE SECURE SOCKET API

PRESENTED BY CHEYENNE SON AND MATTHEW CHRISTENSEN

THE SECURE SOCKET API

- Using TLS is hard
- Symbols in libssl: 504
- Lines of code: 317

```
int socket = socket(PF_INET, SOCK_STREAM, IPPROTO_TCP);
```

```
int socket = socket(PF_INET, SOCK_STREAM, IPPROTO_TLS);
```

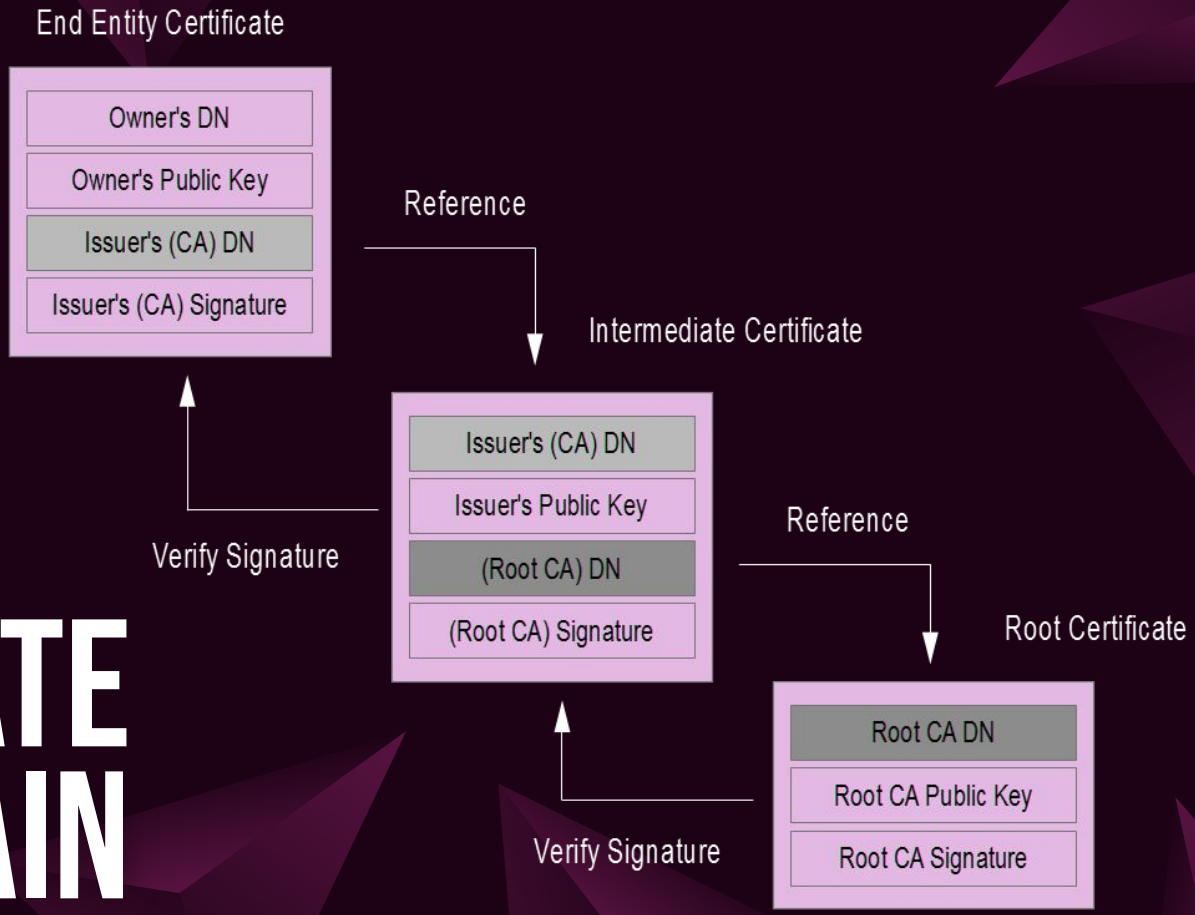
THE PROBLEM

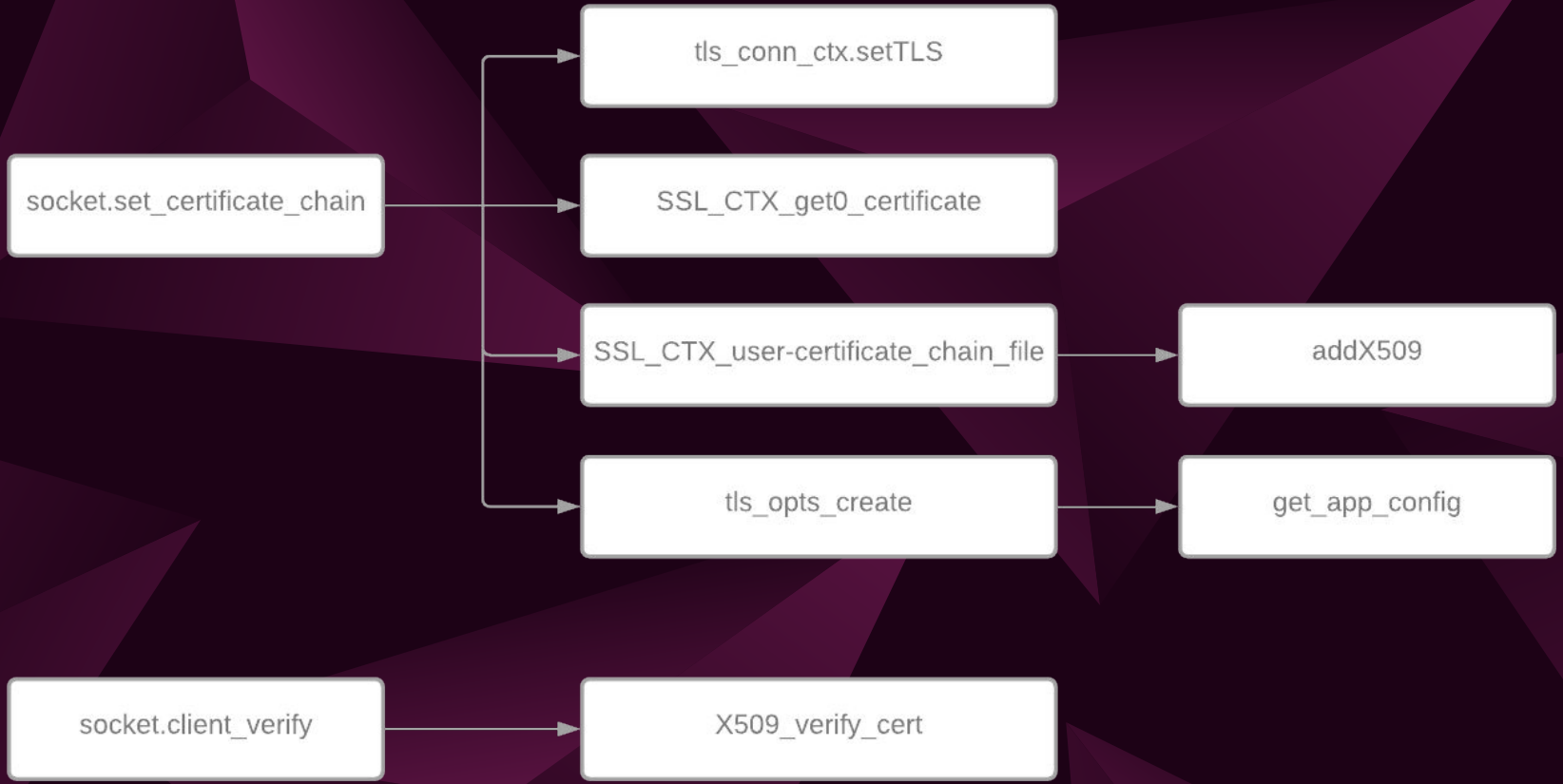
How do we know the Secure Socket API actually makes your socket secure?

FORMAL VERIFICATION PROCESS

Contracts	Dafny	Code verification
Determine what state changes are necessary to maintain security.	Implement contracts and state changes in dafny code.	Verify that the codebase implements the contracts.

CERTIFICATE CHAIN




tls_conn_ctx.setTLS
socket.set_certificate_chain
SSL_CTX_get0_certificate
SSL_CTX_user-certificate_chain_file
addX509
tls_opts_create
get_app_config
socket.client_verify
X509_verify_cert

```
// loads a certificate chain from B<file> into B<ctx>.
method SSL_CTX_use_certificate_chain_file
  (file : string, ctx : SSL_CTX?)
  returns (ret : int)
  requires file != ""
  requires ctx != null
  ensures ctx.num_certs != old(ctx.num_certs)
{
  var x509 := new X509.Init();
  ctx.addX509(x509);
  ret := 0;
}
```

```
71
72      method addX509(cert : X509?)
73        modifies `num_certs
74        modifies cert_store
75        requires cert != null
76        requires 0 <= num_certs < cert_store.Length - 1
77        ensures num_certs == old(num_certs) + 1
78        ensures num_certs < cert_store.Length
79        ensures forall i : int :: 0 <= i < old(num_certs)
80                ==> cert_store[i] == old(cert_store[i])
81        ensures cert_store[old(num_certs)] == cert
82      {
83        cert_store[num_certs] := cert;
84        num_certs := num_certs + 1;
85      }
86
```

Conclusion and what next?

- The Secure Socket API is an effective way of guaranteeing a secure TLS connection
- Formal verification of meaningful (non-trivial) code is hard
- We lack formal verification that our model represents the codebase
- Solution: Integrate proof into the codebase

THANKS!

Any questions?