Formal and **Automated** Exploitability Analysis of TLS Specification Violations

이재훈, 배경민

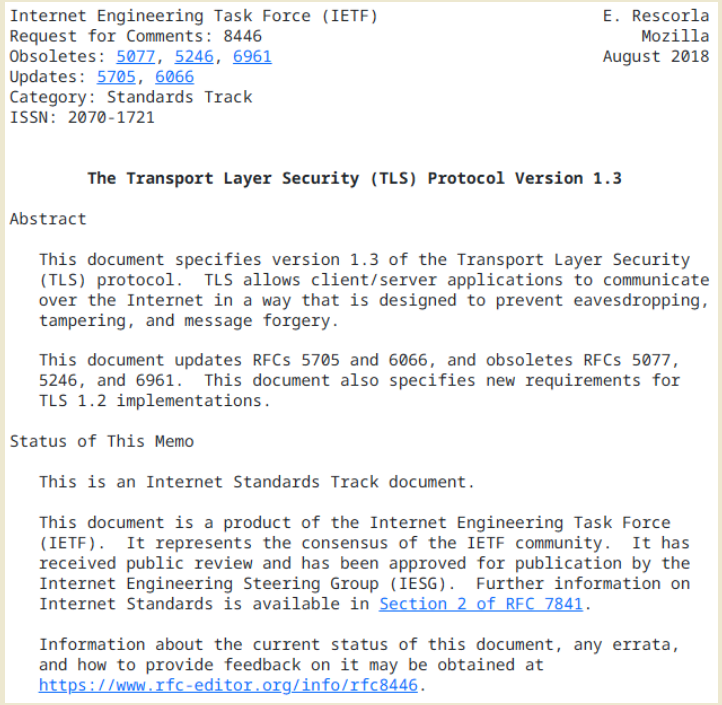
포항공과대학교

STAAR 10th Workshop, Ulsan, Korea

POSTECH

TLS Protocol

- TLS(Transport Layer Security) 프로토콜: 두 당사자 간 메시지 전송 시 데이터 보호/무결성을 보장하기 위한 보안 프로토콜



Internet Engineering Task Force (IETF) — E. Rescorla
Request for Comments: 8446 — Mozilla
Obsoletes: 5077, 5246, 6961 — August 2018
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track document.

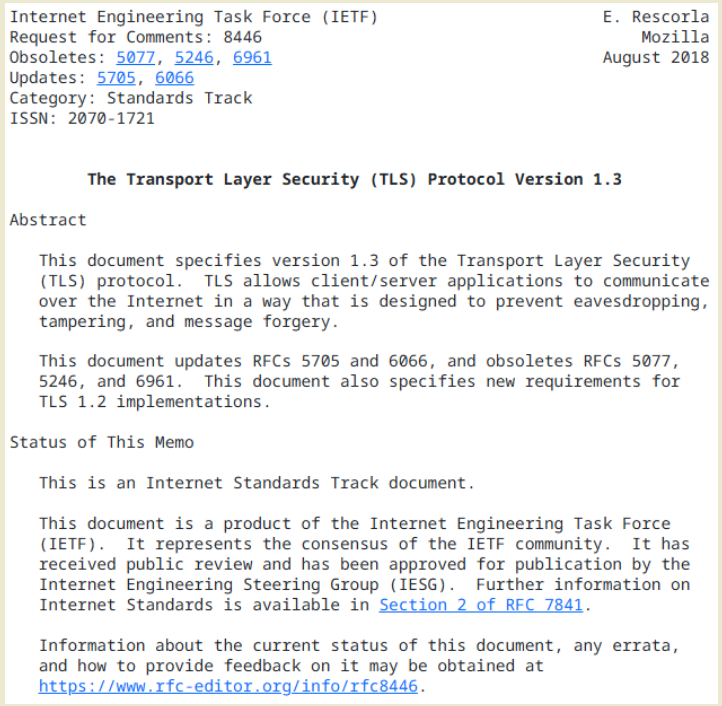
This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8446.

RFC 5246(TLS 1.2), 8446(TLS 1.3)

TLS Protocol

- TLS 프로토콜 RFC에 대해 Formal Verification을 통해서, 스펙 수준에서 여러 보안 속성들을 엄밀하게 검증



Internet Engineering Task Force (IETF) — E. Rescorla
Request for Comments: 8446 — Mozilla
Obsoletes: 5077, 5246, 6961 — August 2018
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

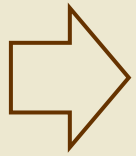
This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

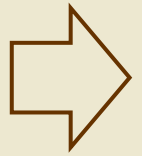
Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8446.





RFC 5246(TLS 1.2), 8446(TLS 1.3)

Formal Models

Correct / Failed

TLS Protocol

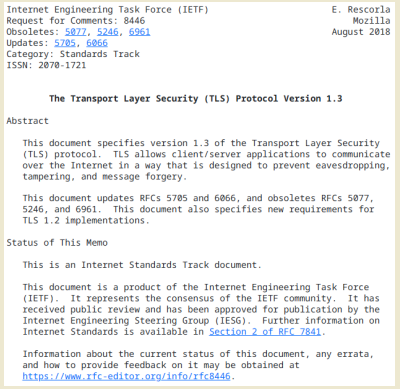
- TLS 프로토콜 구현 코드에 대해 Fuzzing, Combinatorial Testing, Differential Testing 등을 통해 오류 발견

TLS Implementation

Test Code

Correct / Failed

Formal 모델을 통한 테스트 및 취약점 탐지



Internet Engineering Task Force (IETF) — E. Rescorla
Request for Comments: 8446 — Mozilla
Obsoletes: 5077, 5246, 6961 — August 2018
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track document.

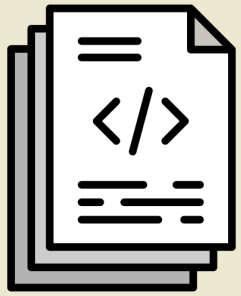
This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8446.

RFC Spec

MoudE3

Formal Model



Test Code

OpenSSL
Cryptography and SSL/TLS Toolkit

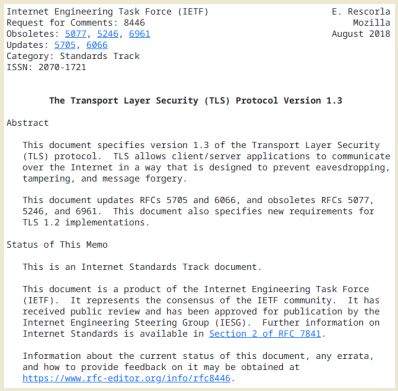
gnuTLS

wolfSSL

Mbed TLS

TLS Libraries

Formal 모델을 통한 테스트 및 취약점 탐지



Internet Engineering Task Force (IETF) — E. Rescorla
Request for Comments: 8446 — Mozilla
Obsoletes: 5077, 5246, 6961 — August 2018
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

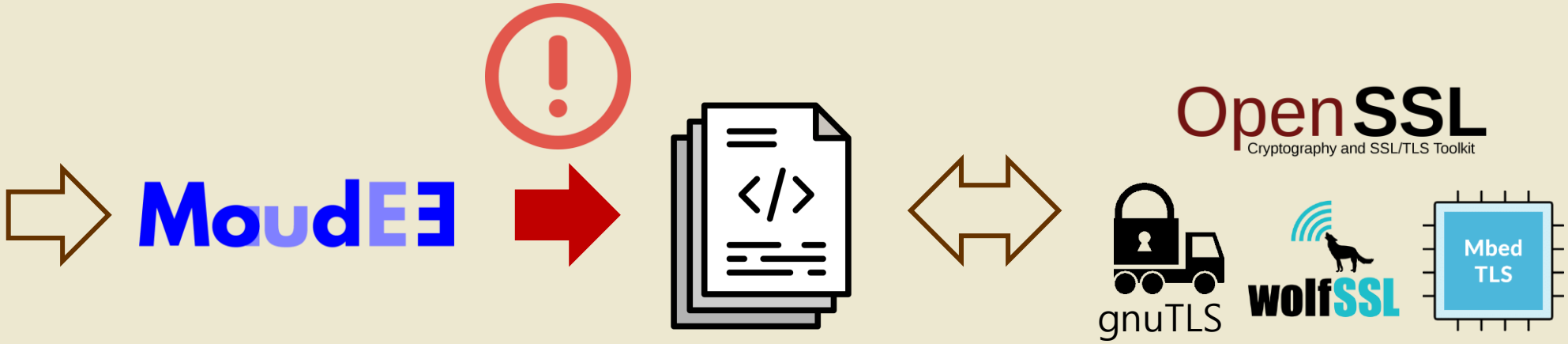
This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8446.



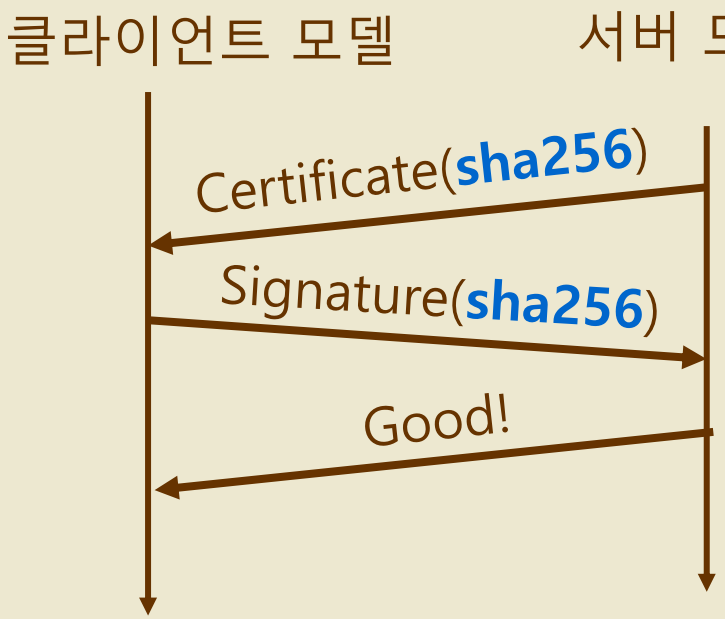
RFC Spec — Formal Model — Test Code — TLS Libraries

1. **효율적으로** RFC Spec을 위반하는지 테스트하는 시나리오 자동 생성
2. 버그를 넘어 **보안 취약점까지 탐지**하기 위한 테스트 시나리오 자동 생성

Formal Model 기반 테스트

RFC Requirement: 서버가 요구한 Hash 알고리즘으로 클라이언트는 서명해서 보내야 함.

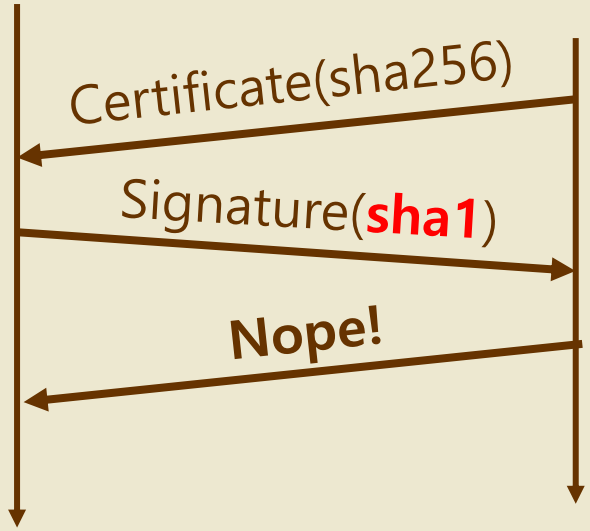
Formal Model 기반 테스트




```
rl [buildSignature]:
  < Client | sig : SA > => < Client | ... > Signature(SA)
```

Formal Model 기반 테스트

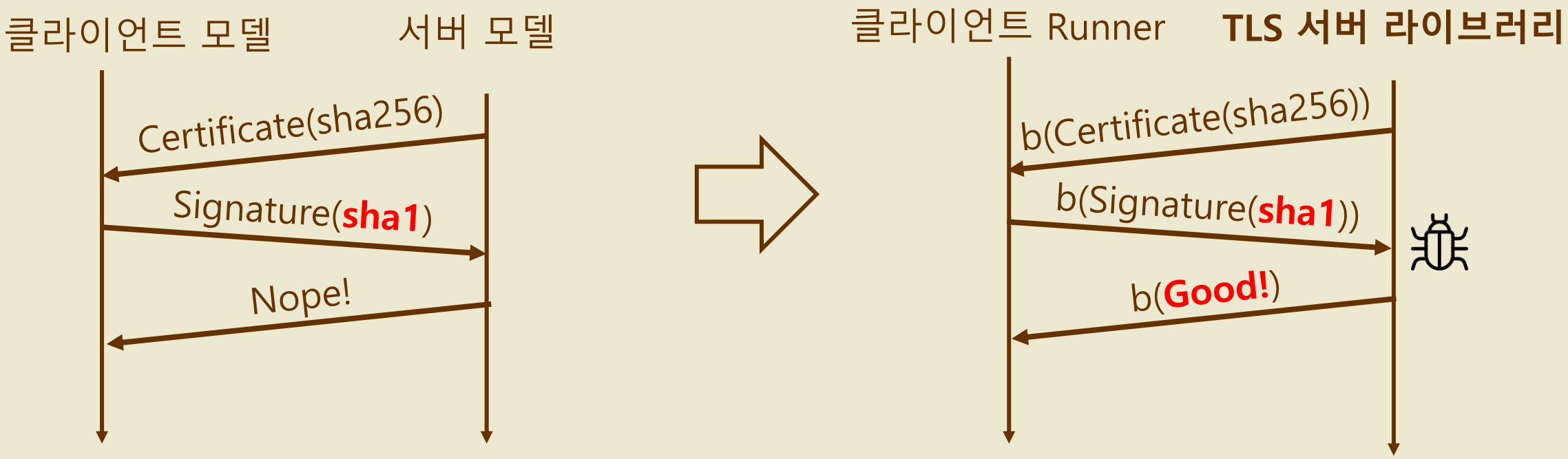
클라이언트 모델 서버 모델



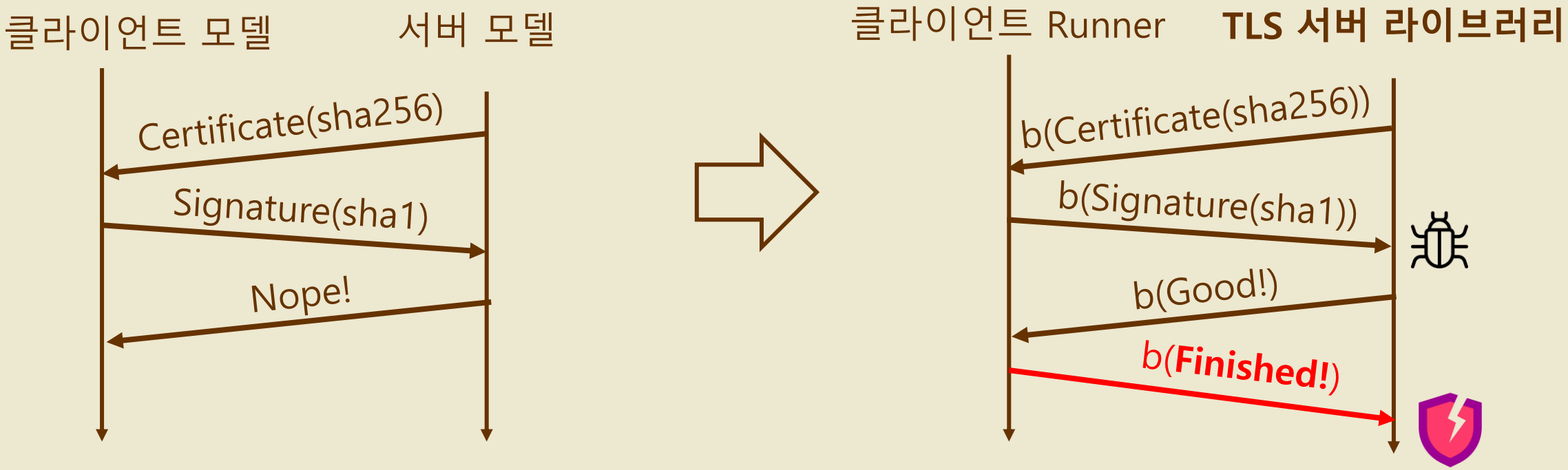

```
rl [buildSignature]:
  < Client | sig : SA > => < Client | ... > Signature(SA)

rl [buildModifiedSignature1]:
  < Client | sig : SA > => < Client | ... > Signature(sha1)

rl [buildModifiedSignature2]:
  < Client | sig : SA > => < Client | ... > Signature(md5)

. . .
```

현재 상태와 **Inconsistent한 메시지를 생성**하는 Rules을 자동 생성 후,
Maude Strategy를 이용하여 해당 Rules만 실행

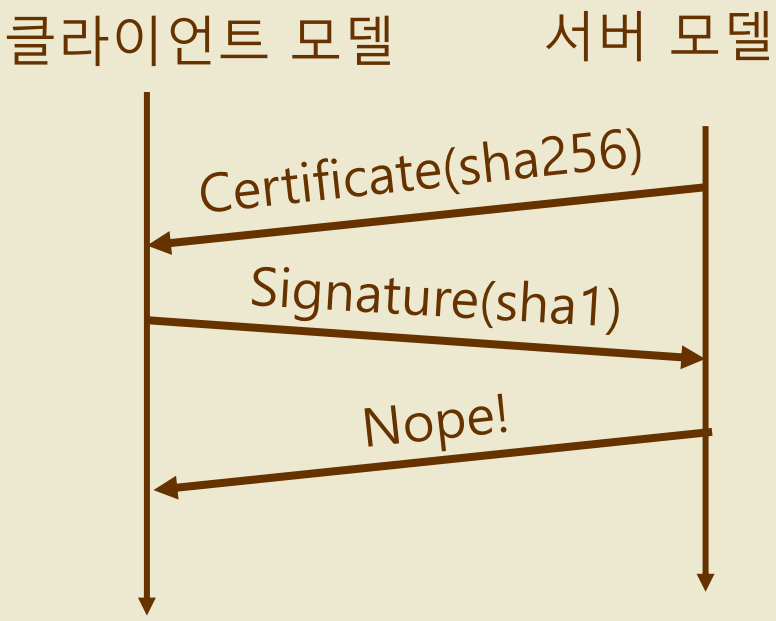
Formal Model 기반 테스트



Formal Model 기반 테스트



RFC 위반 버그에서 보안 취약점까지




```
crl [processSignature]:
  < Server | sig : SA1 > Signature(SA2) => < Server | ... > Good!
 if SA1 == SA2 .

crl [processSignature]:
  < Server | sig : SA1 > Signature(SA2) => < Server | ... > Nope!
 if SA1 =/= SA2 .
```

RFC 위반 버그에서 보안 취약점까지

클라이언트 모델 **서버 모델**


```
crl [processSignature]:
  < Server | sig : SA1 > Signature(SA2) => < Server | ... > Good!
 if SA1 == SA2 .

crl [processSignature]:
  < Server | sig : SA1 > Signature(SA2) => < Server | ... > Nope!
 if SA1 =/= SA2 .

crl [processModifiedSignature]:
  < Server | sig : SA1 > Signature(SA2) => < Server | ... > Good!
 if true .
```

잘못된 메시지가 왔을 때, **해당 메시지**로 상태를 강제 업데이트하는
Rules 자동 생성 및 해당 Rules 실행

실험 결과

- 신규 RFC 위반 **버그**: 20개
  - WolfSSL: 12개
  - gnuTLS: 4개
  - mbedTLS: 6개

- 신규 **CVE** 발급: 7개
  - WolfSSL: 5개
    - CVE-2025-11936, CVE-2025-11936, CVE-2025-11934, CVE-2025-11933, CVE-2025-12889
  - gnuTLS: 1개 (embargo)
  - mbedTLS: 1개 (embargo)