# A Trustworthy Middlebox-aware Networking Architecture

Hyunwoo Lee[1], Zachary Smith[2], Selin Chun[1], and Ted "Taekyoung" Kwon[1]
Seoul National University[1] and University of Luxembourg[2]

Network Convergence & Security Lab

## Motivation

**To be practical, TLS with middleboxes must address not only secure participation of middleboxes but also trustworthiness of middleboxes**

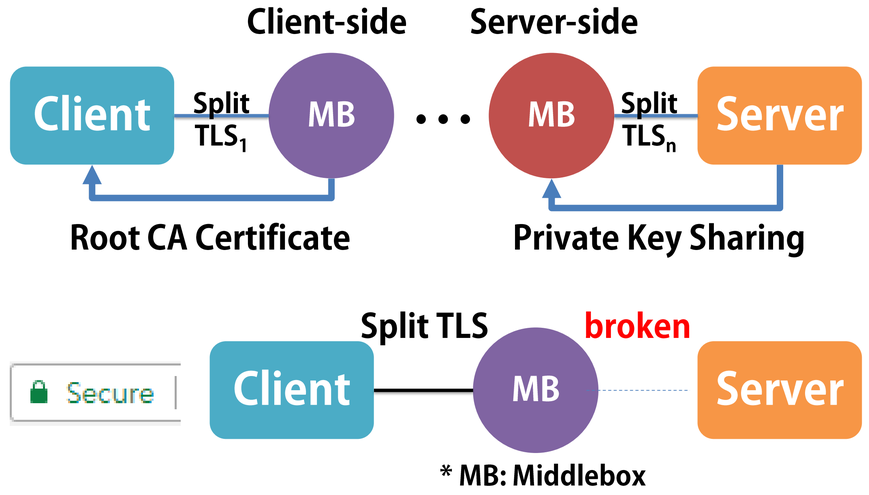
### 1 Middleboxes are valuable but become useless with TLS


Middleboxes can offer

- Defense from attacks at the network edge
- Performance improvement

However, value-added service for security and performance cannot be carried out with TLS

### 2 Current TLS Interception (Split TLS) breaks security and infringes privacy




* MB: Middlebox

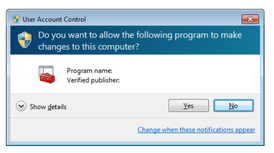
Even though data secrecy, data authentication, and entity authentication are broken, a user agent still say "secure"

### 3 We do not know how to trust TLS middleboxes

Much research assumes trustworthiness of middleboxes through their certificates

Only certificate validation for trust is insufficient since a user does not explicitly intend to communicate with middleboxes

User access control can be used, but it will decrease usability




## Trustworthiness Building Blocks

**We define trustworthiness of middleboxes as public auditability which becomes feasible with explicit authentication and modification check**

### 1 Difference from a man-in-the-middle attacker

We add auditability on read/write operation to be different from passive/active adversary

For read operation,
Explicit authentication by Middlebox Certificate in Middlebox Transparency

For write operation,
Modification check with Modification Record

### 2 Middlebox Certificate in Middlebox Transparency

Middlebox Certificate includes

- Name of a middlebox provider
- Read/Write permissions on key usage
- Role of a middlebox
- Access URL to information page of a middlebox

All CAs or middlebox providers must register middlebox certificate into middlebox transparency, the same public log server with certificate transparency

Only middlebox having middlebox certificate can participate into TLS session as a reader and every entity can audit readers in middlebox transparency

### 3 Modification Record

This is a data structure recording the history of modification by middleboxes, starting from a source

Writer records its ID, the hash of original message, and HMAC of modification whenever it modifies

$m'$ | $H(secret_s, H(m))$ | $ID_{mb}$ | $H(m)$ | $H(secret_{mb}, H(m)||H(m'))$

Example: Server sends m and MB modifies it into m′

Experiment shows verification only takes less than 350 us on the desktop, even with 100 writers

## Middlebox-aware TLS

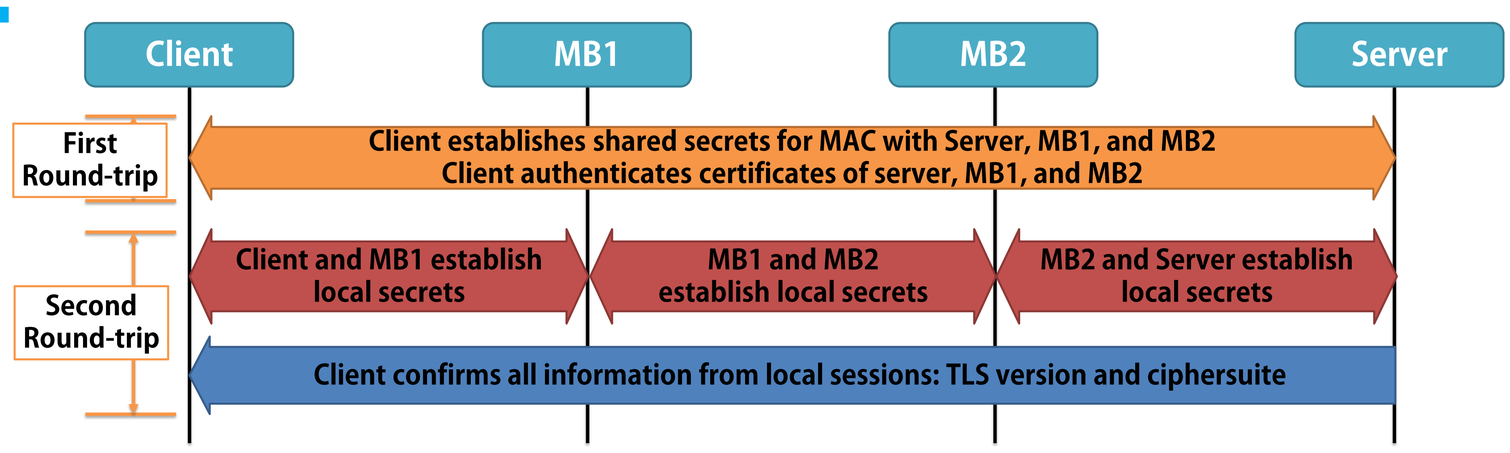
**Middlebox-aware TLS guarantees new TLS security requirements with trustworthiness-managed middleboxes**

### 1 New Security Requirements

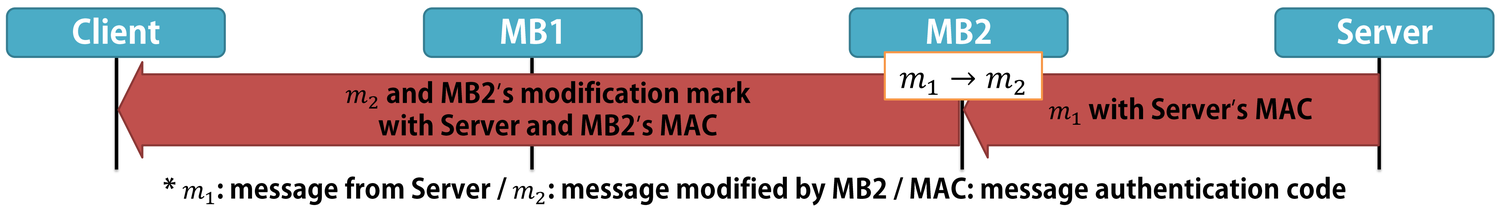
- Data secrecy → **Path secrecy**
  Endpoints (Client) confirm(s) every local session is encrypted with higher TLS version/ciphersuite
- Data authentication
  → **Data source authentication**
  Endpoints (Client) confirm(s) the source of data, that is, who sends the data
  → **Modification accountability**
  Endpoints (Client) confirm(s) valid modification, that is, who modifies the data
- Entity authentication
  → **Server/Middlebox authentication**
  Endpoints (Client) authenticate(s) all the entities in the session by their certificates

### 2 End-to-end TLS layer over Split TLS layer

* MB: Middlebox




Endpoints (Client) confirm(s) all the certificates and negotiates shared secret for MAC on end-to-end layer during handshake




* $m_1$: message from Server / $m_2$: message modified by MB2 / MAC: message authentication code

Endpoints (Client) check(s) modification record on end-to-end layer

## Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government(MSIT)
(No.2016-0-00160, Versatile Network System Architecture for Multi-dimensional Diversity)
Many Thanks to **David T. Naylor** (Nefeli Network), **Doowon Kim** (University of Maryland), **Juhyeng Han** (KAIST), and **Yongbae Bang** (Seoul National University) for their comments and advices