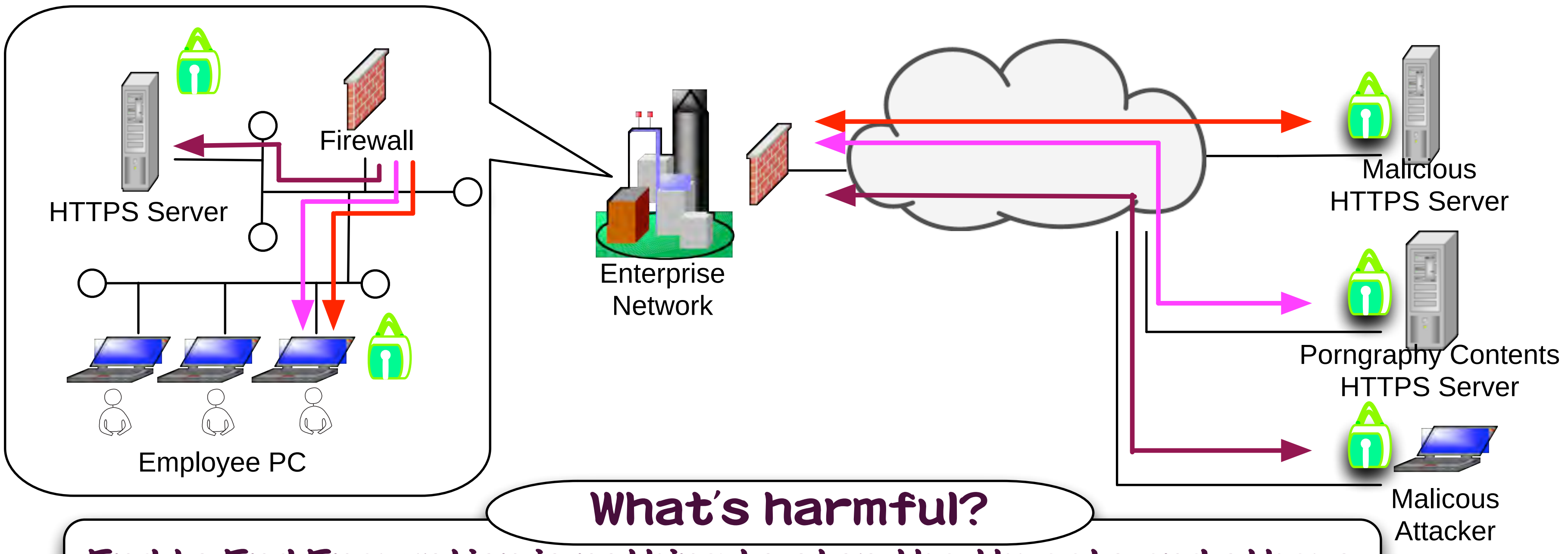
End-to-End Encryption Considered Harmful

Ryosuke Miura Yuuki Takano Tomoya Inoue



What's harmful?

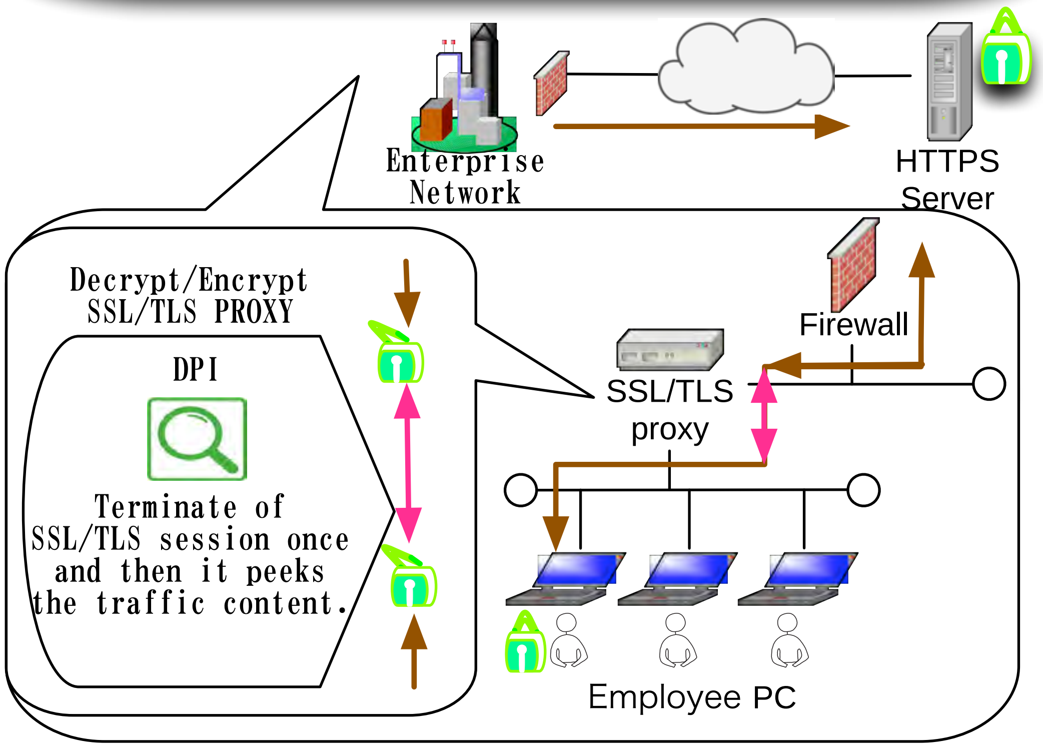
End-to-End Encryption is nothing to stop the threats and others on the middlebox managed by network operators directly.

↔ Drive by Download attack from a Malicious Server

↔ Contents Check based on Network Policy

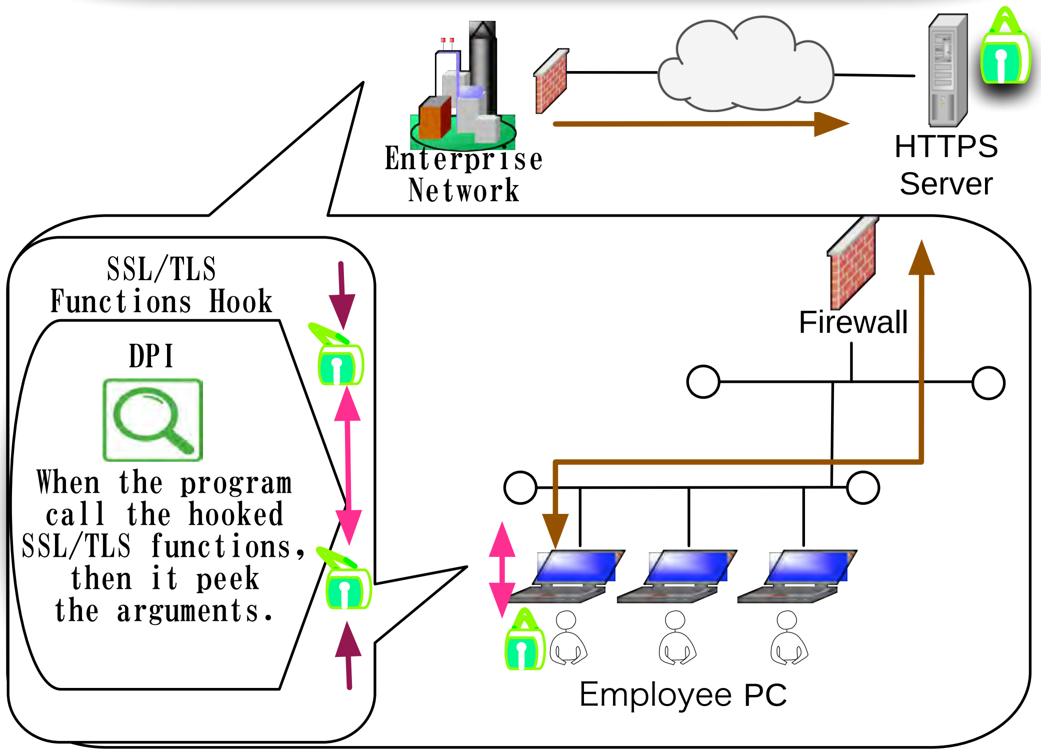
↔ Intrusion Detection with Encryption

Current the Proxy method


Enterprise Network
HTTPS Server
Decrypt/Encrypt SSL/TLS PROXY
DPI
Terminate of SSL/TLS session once and then it peeks the traffic content.
Firewall
SSL/TLS proxy
Employee PC

Decrypt/Encrypt with SSL/TLS proxy

Propose the Hook Method


Enterprise Network
HTTPS Server
SSL/TLS Functions Hook
DPI
When the program call the hooked SSL/TLS functions, then it peek the arguments.
Firewall
Employee PC

SSL/TLS API Hook

Problems

1. The Employee PC can not identify the certificates by HTTPS Server.
2. Two distinct SSL session caused amount of calclation.

1. SSL/TLS Hook can directly identify the certificates by HTTPS Server in transparency SSL/TLS Functions Hook.
2. No more CPU power with an identical SSL session only.

Essentially Encryption should be divided by each of management segment.