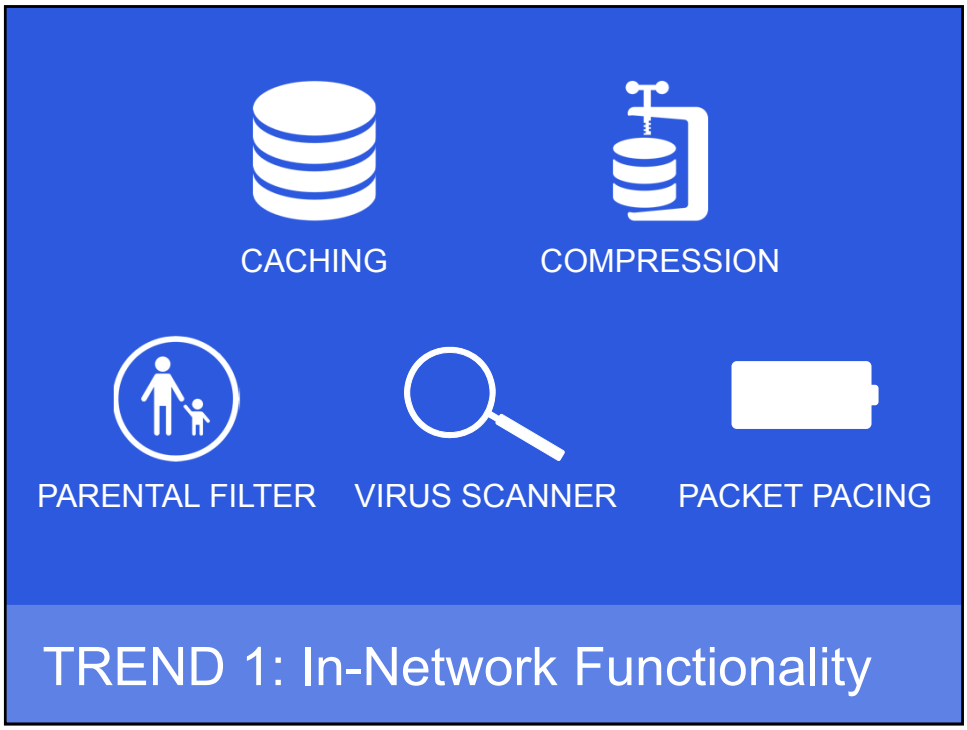
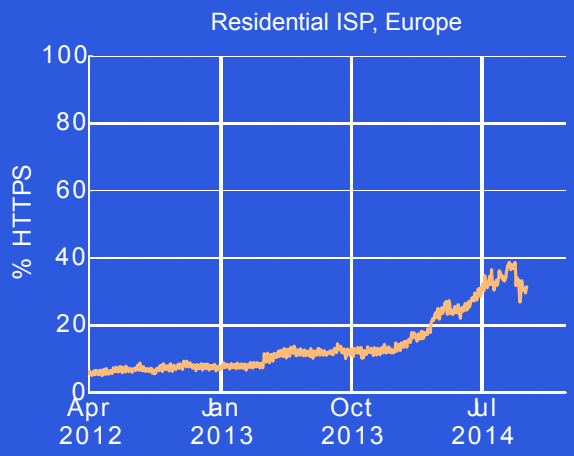
Making TLS and Middleboxes Play Together … Nicely

David Naylor
Peter Steenkiste

And many others …





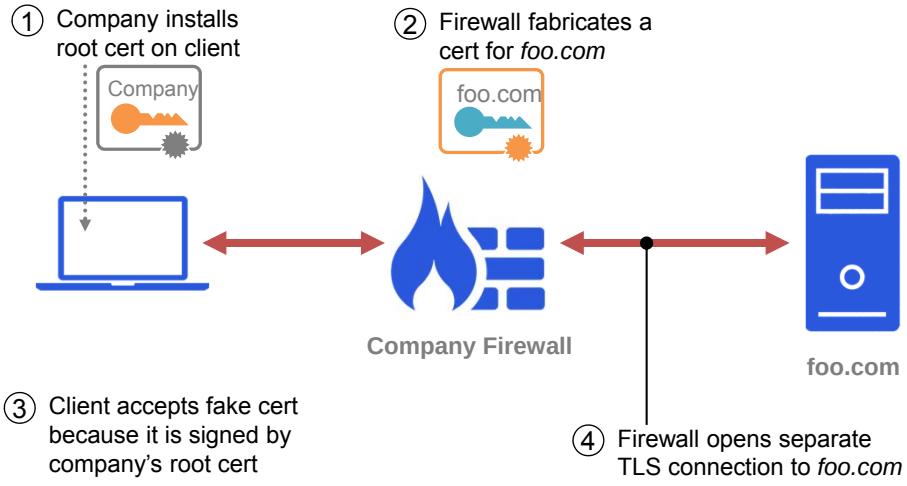
TREND 2: Privacy → Encryption

Encryption

+

In-Network Functionality

They do NOT play together nicely!



mcTLS Design Requirements

EXTEND TLS PROPERTIES TO MIDDLEBOXES:

R1 Entity Authentication

R2 Secrecy

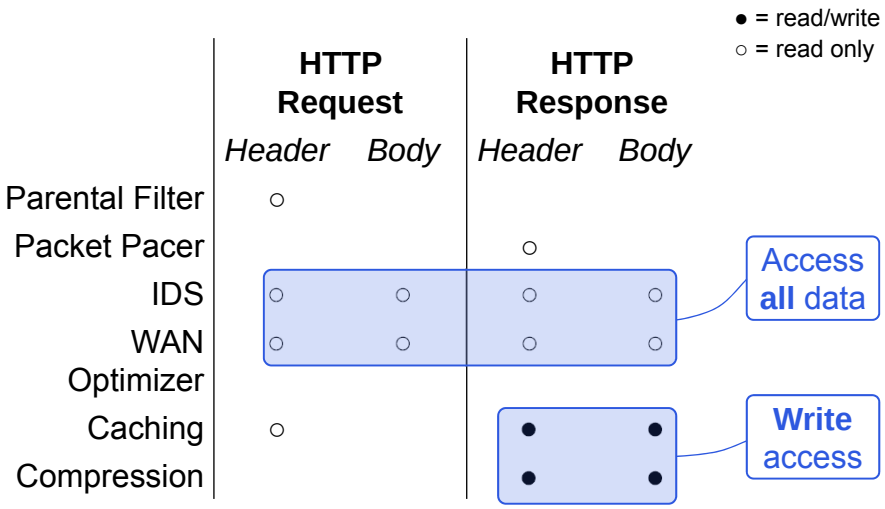
R3 Data Integrity

PLUS TWO NEW ONES:

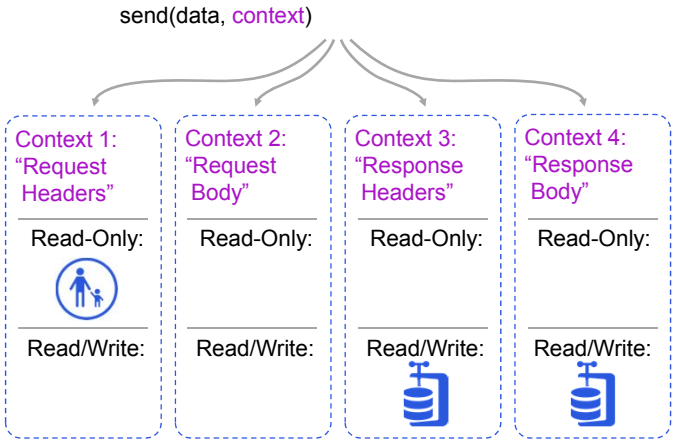
R4 Visibility & Control

R5 Least Privilege

Most middleboxes do not need *read/write* access to *all* data

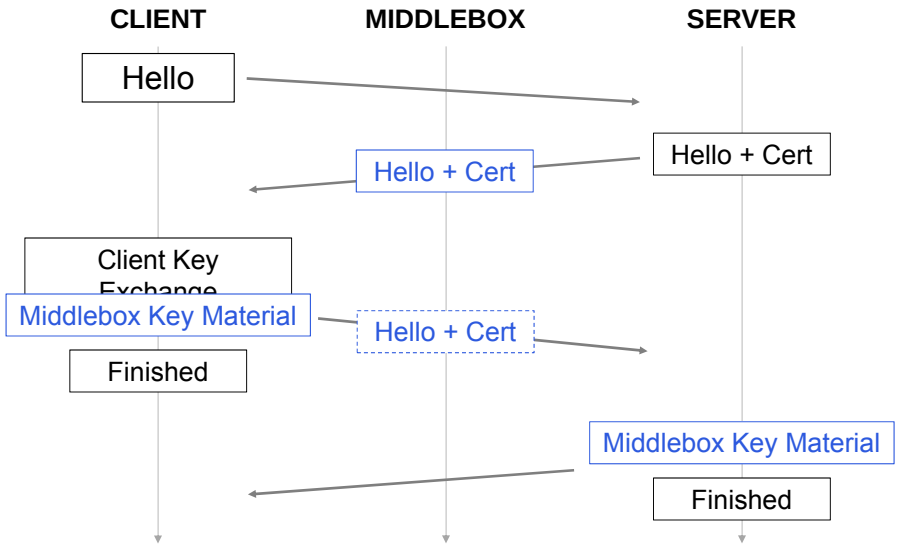


mcTLS extends record protocol with encryption contexts for setting read/write permissions



8

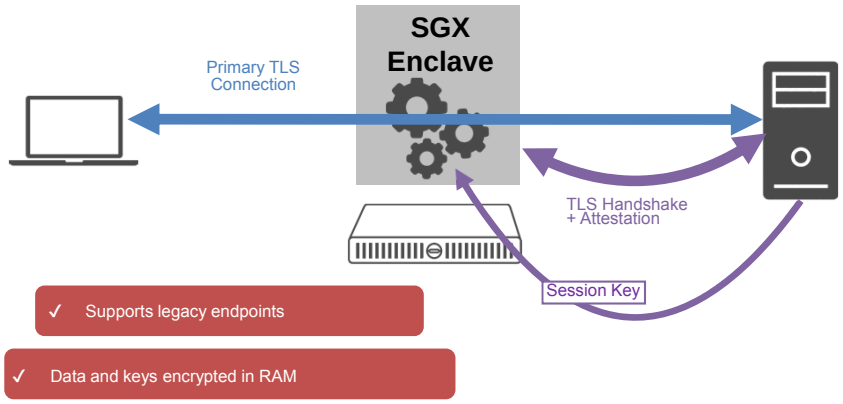
mcTLS Handshake



How about Other Design Points

- mcTLS: fine-grain middlebox access ctl
  - Both endpoint must agree on middlebox
  - ►Does not accommodate legacy endpoints!
- mbTLS: TLS plus two other requirements
  - Accommodate legacy endpoints
  - ►Endpoints can add middleboxes independently
  - Outsourcing of middleboxes to the “cloud”
  - ►Must verify execution of network function

mbTLS protects session data and keys using SGX



How to best play together?

- Access control: all/nothing vs. fine grain
- Who can see and authenticates
- Infrastructure assumptions
- Data change secrecy
- Legacy endpoints
- In-band discovery
- Path integrity

References + Collaborators

- The Cost of the "S" in HTTPS, D. Naylor, A. Finamore, I. Leontiadis, Y. Grunenberger, M. Mellia, M. Munafo, K. Papagiannaki, P. Steenkiste, ACM CoNEXT 2014, Sydney, December 2014
- multi-context TLS (mcTLS): Enabling Secure In-Network Functionality in TLS, D. Naylor, K. Schomp, M. Varvello, I. Liontiadis, J. Blackburn, D. Lopez, K. Papagiannaki, P. Rodriguez, P. Steenkiste, ACM Sigcomm 2015, London, August 2015
- And Then There Were More: Secure Communication for More Than Two Parties, D. Naylor, R. Li, C. Gkantsidis, T. Karagiannis, and P. Steenkiste, ACM CoNEXT 2017, Seoul, Dec 2017