Institute of Operating Systems
and Computer Networks

Technische
Universität
Braunschweig

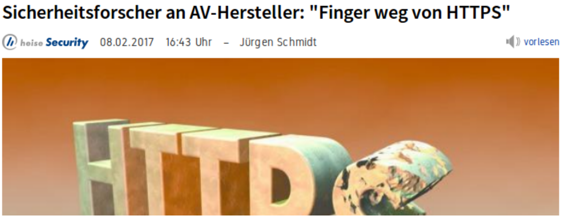
EndBox: Scalable Middlebox Functions Using Client-Side Trusted Execution

David Goltzsche, Signe Rüsch, Manuel Nieke, Rüdiger Kapitza

02.03.2018

Motivation

- Network attacks on companies and organizations
- 2016: $1/3$ of hacked organizations reported customer, opportunity and revenue loss $> 20\,\%$ (Cisco 2017 Cybersecurity Report)
- Filtering and inspecting of encrypted traffic often problematic
- Terminating TLS connections introduces new security risks, e.g. insecure ciphers[1]



Sicherheitsforscher an AV-Hersteller: "Finger weg von HTTPS"

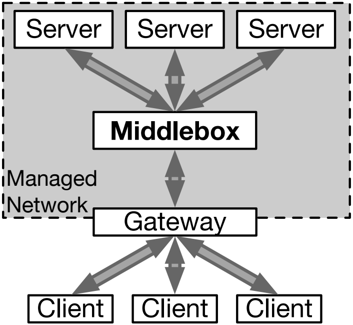
heise Security 08.02.2017 16:43 Uhr – Jürgen Schmidt

[1] https://www.heise.de/newsticker/meldung/US-CERT-warnt-vor-HTTPS-Inspektion-3660610.html

Motivation

Intrusion Prevention Systems

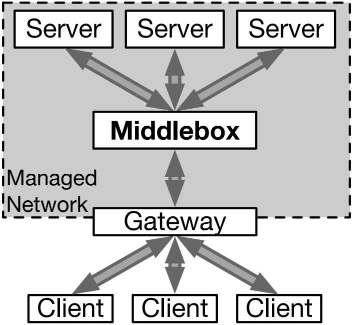
- Detect network attacks by monitoring traffic
- Employed on central middleboxes, used to improve network performance and security
- High costs for operators



Motivation

Problems of Current Middleboxes

- Centralized hardware . . .
  - is expensive: ≈ $50.000 in 5 years in small networks (Sherry et al., 2012)
  - is vulnerable
  - has limited scalability

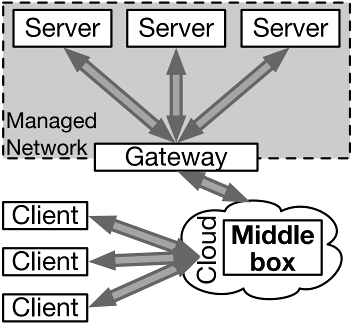


Motivation

Problems of Current Middleboxes

- Centralized hardware . . .
  - is expensive: ≈ $50.000 in 5 years in small networks (Sherry et al., 2012)
  - is vulnerable
  - has limited scalability
- Offloading to cloud services . . .
  - introduces higher complexity and latency
  - requires trust in cloud provider
  - processing of encrypted traffic problematic

→ **Shifting middleboxes to clients!**

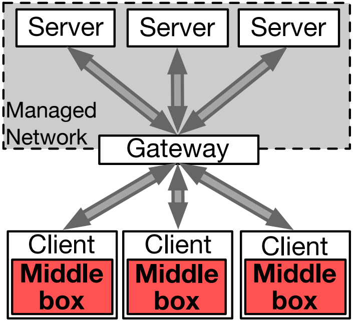


Motivation

Client-Side Functionality

- Advantages:
  - Better utilization of clients
  - Scales well with number of clients
- Problems:
  - Both users and client machines cannot be trusted
  - Users have to be forced to use middlebox function

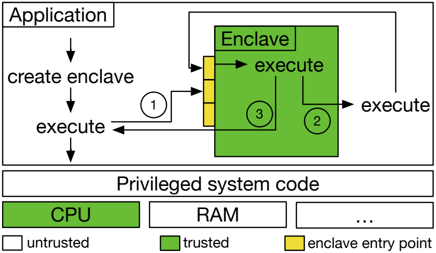
→ **Leverage trusted execution!**



Intel’s Software Guard Extensions (SGX)

Basics

- Extension to Intel’s x86 CPUs
- Introduced with Skylake series
- Isolated environment for trusted execution, called *enclave*
- Encrypted system memory and integrity checks
- No access from OS



Motivation

Requirements

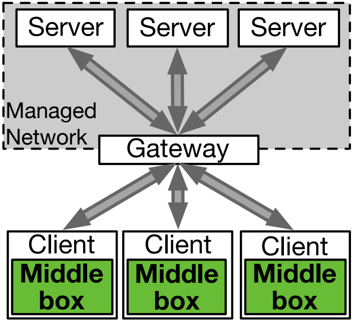
- Enforcement: no circumvention
- Integrity of middlebox function & privacy of user data
- Manageability: centrally update middlebox functions
- Generality: support for multiple middlebox functions
- Scalability & performance

Design

Objectives

→ Middlebox functions run inside enclave!

- Network owner can keep control over network, machines, and configurations
- Execution of middlebox functions on client can be enforced
- Encrypted traffic can be analyzed locally, no MitM

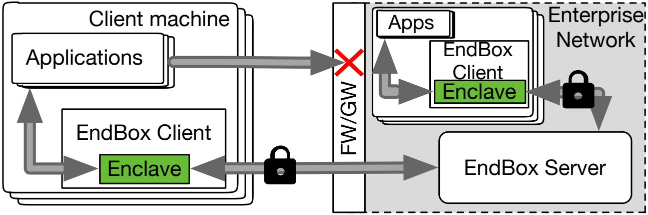


Design

Leveraging VPN Tunnels

Enforcement

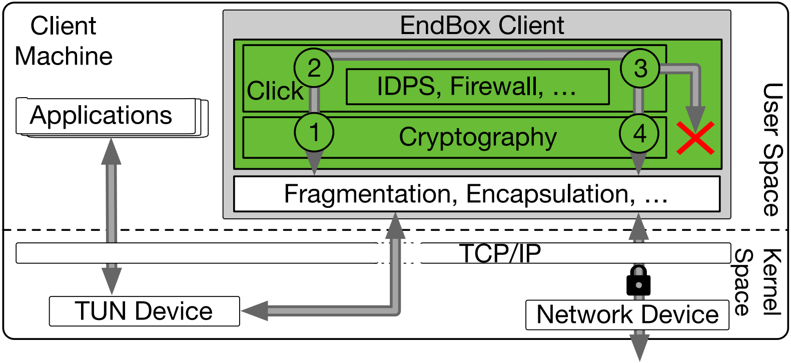
- Packets are routed through SGX enclaves using VPN tunnel
- Terminate VPN connection inside enclave
- Central hardware now less complex



Design

EndBox VPN Client Architecture

Integrity & Privacy

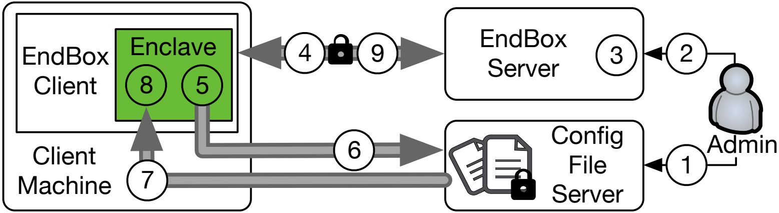


Design

Configuration Update Mechanism

Manageability

- Centrally update distributed middlebox functions
- Update should be provable
- VPN server enforces update by dropping packets



Implementation

VPN and Middlebox Functions

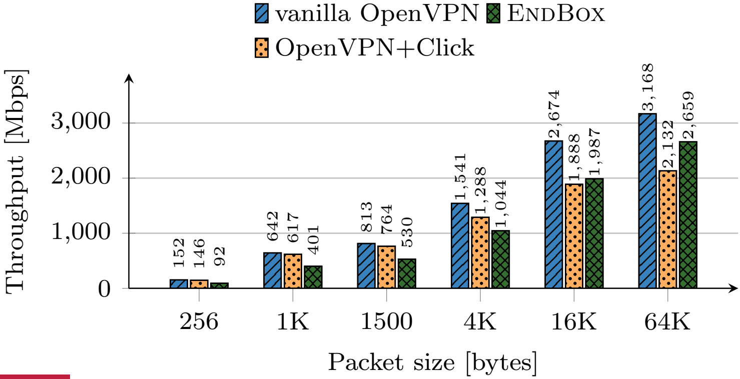
Generality

- OpenVPN v2.4.0
- Click Modular Router
- Multiple use cases:
  - Forwarding (**FOR**)
  - Firewall (**FW**)
  - Intrusion Prevention (**IDPS**)
  - Load balancer (**LB**)
  - DDoS protection (**DDoS**)

Evaluation

Performance Evaluation – Microbenchmark

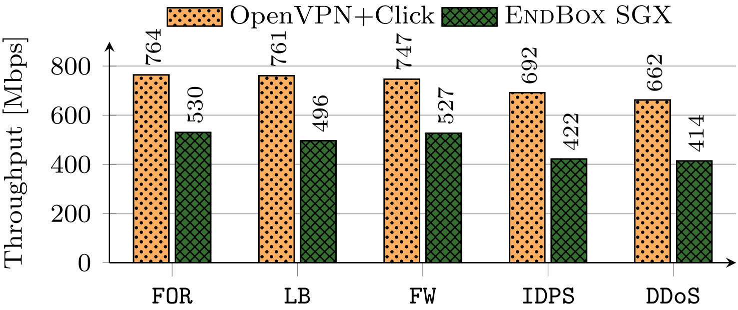
- EndBox: 16–39 % overhead compared to OpenVPN
- OpenVPN+Click: avg. 26 % overhead



Evaluation

Performance Evaluation – Use Cases

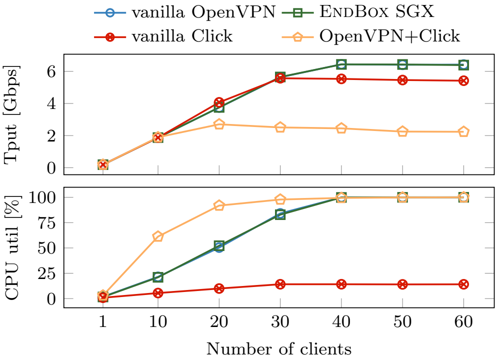
- 30-39 % overhead for EndBox



Evaluation

Scalability Evaluation

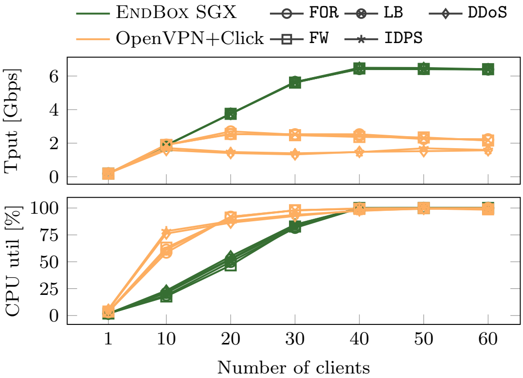
- Clients generate 200 Mbps of traffic
- Click runs with only one instance



Evaluation

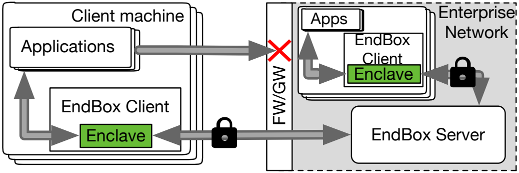
Scalability Evaluation – Use Cases

- 2.6-3.8x higher throughput using EndBox



Conclusion

- Shifting middlebox functions from central middleboxes to clients
  → Improve scalability and performance
- Supports generic middlebox functions with Click
- Enforce execution by using OpenVPN and SGX enclaves
- Throughput up to 3.8x higher than centralized deployment
- Accepted at DSN'18:
  - TU Braunschweig: David Goltzsche, Signe Rüsch, Manuel Nieke, Nico Weichbrodt, Rüdiger Kapitza
  - Université de Neuchâtel: Sébastien Vaucher, Valerio Schiavoni, Pascal Felber
  - Imperial College London: Pierre-Louis Aublin, Paolo Costa, Peter Pietzuch
  - TU Dresden: Christof Fetzer



Backup Slides

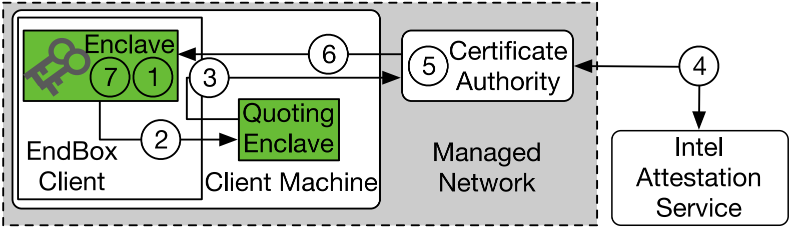
Related Work

- ETTM (Dixon et al., 2011):
  - Middlebox functions on end hosts secured by TPM
  - Fully decentralized, employs Paxos instead of trusted server
- Eden (Ballani et al., 2015):
  - Specialized hardware on end hosts
  - Higher performance, but no commodity hardware
- Middlebox functions in the cloud (Sherry et al., 2012; Lan et al., 2016)
  - Good scalability, but increased complexity and latency
  - Privacy and legal issues

Design

EndBox Key Management

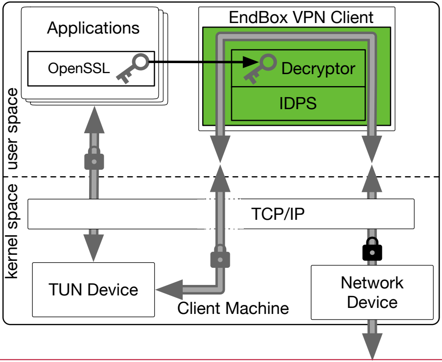
- Attacker should not create unauthorized VPN connection
- SGX remote attestation & sealing features and Certificate Authority



Design

Handling of encrypted traffic

- Extract TLS session key and store in enclave
- No decryption and traffic inspection on remote server



References I

- Hitesh Ballani u. a. „Enabling End-Host Network Functions“. In: *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*. SIGCOMM '15. 2015.
- Cisco. *Cisco 2017 Annual Cybersecurity Report: Chief Security Officers Reveal True Cost of Breaches and the Actions Organizations are Taking*. `https://newsroom.cisco.com/press-release-content?articleId=1818259`. 2017.
- Chang Lan u. a. „Embark: Securely Outsourcing Middleboxes to the Cloud“. In: *13th USENIX Symposium on Networked Systems Design and Implementation*. NSDI '16. 2016.

References II

- Jürgen Schmidt. *US-CERT warnt vor HTTPS-Inspektion*. https://www.heise.de/newsticker/meldung/US-CERT-warnt-vor-HTTPS-Inspektion-3660610.html. 2017.
- Justine Sherry u. a. „Making Middleboxes Someone Else's Problem“. In: *SIGCOMM*. 2012.