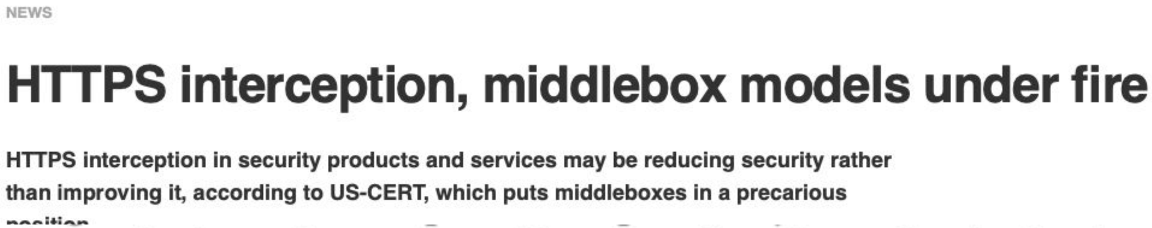
Middlebox Technologies with Intel SGX

A Literature Survey

Shiv Kushwah & Sumukh Shivakumar

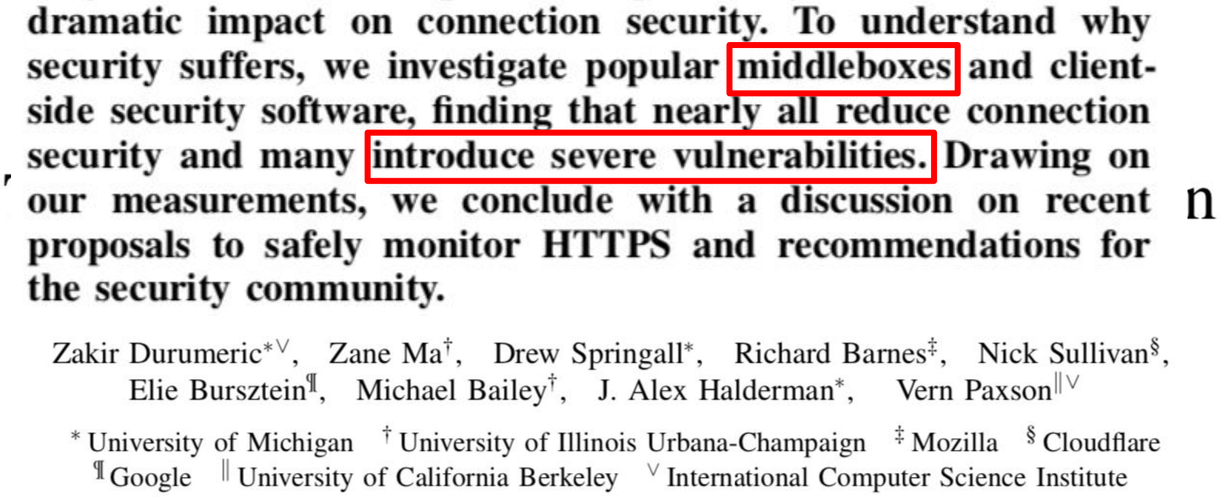
What’s all the fuss with middleboxes?



NEWS

HTTPS interception, middlebox models under fire

HTTPS interception in security products and services may be reducing security rather than improving it, according to US-CERT, which puts middleboxes in a precarious position



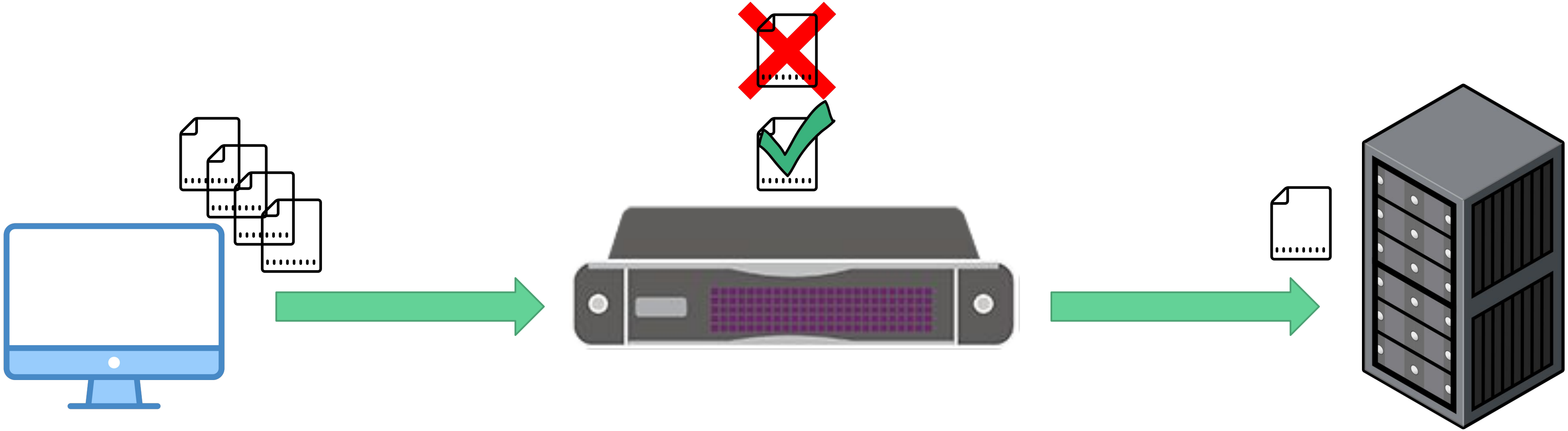
dramatic impact on connection security. To understand why security suffers, we investigate popular middleboxes and client-side security software, finding that nearly all reduce connection security and many introduce severe vulnerabilities. Drawing on our measurements, we conclude with a discussion on recent proposals to safely monitor HTTPS and recommendations for the security community.

Zakir Durumeric[*∨], Zane Ma[†], Drew Springall[*], Richard Barnes[‡], Nick Sullivan[§], Elie Bursztein[¶], Michael Bailey[†], J. Alex Halderman[*], Vern Paxson[‖∨]

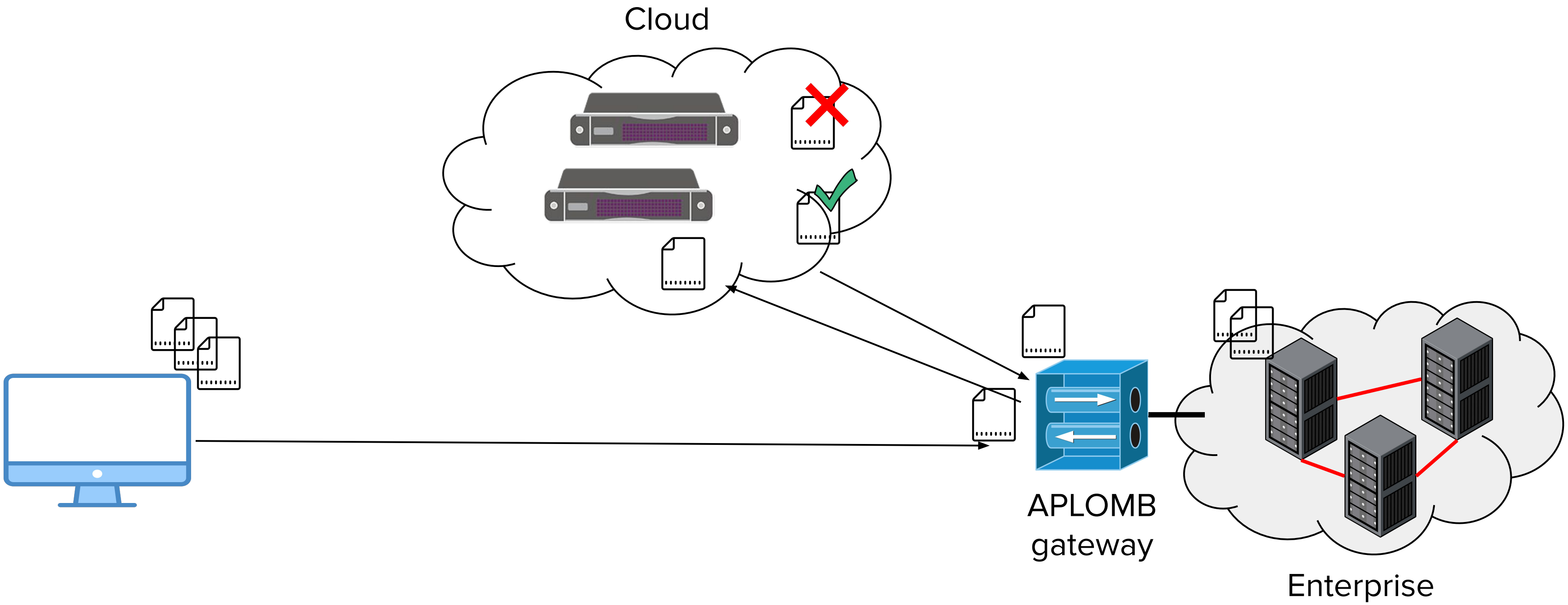
[*] University of Michigan [†] University of Illinois Urbana-Champaign [‡] Mozilla [§] Cloudflare [¶] Google [‖] University of California Berkeley [∨] International Computer Science Institute

Background

What are middleboxes?

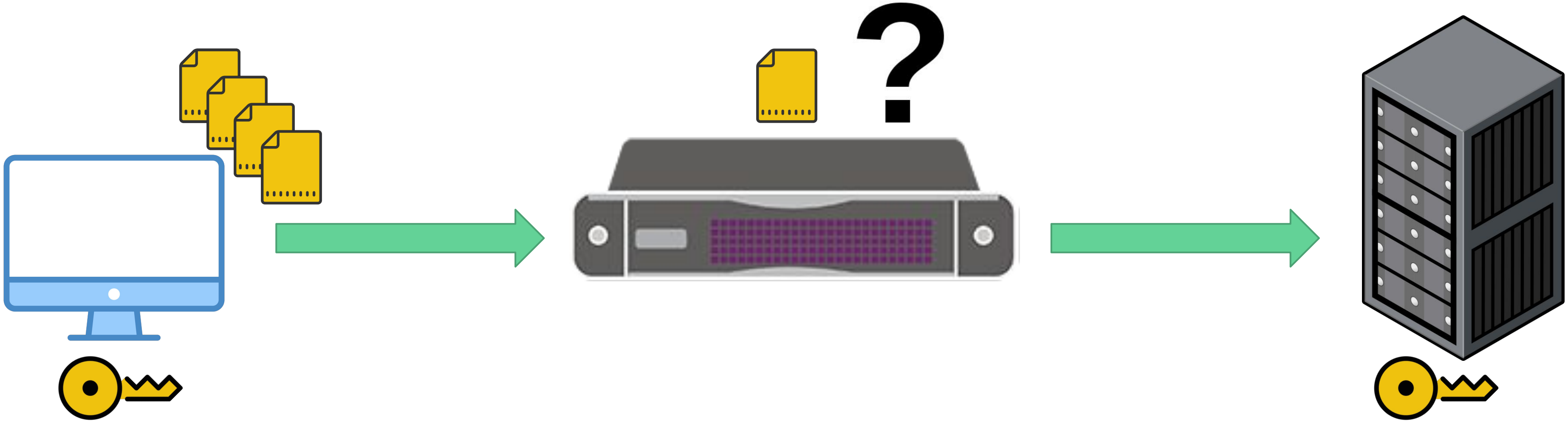


Middleboxes in the Cloud

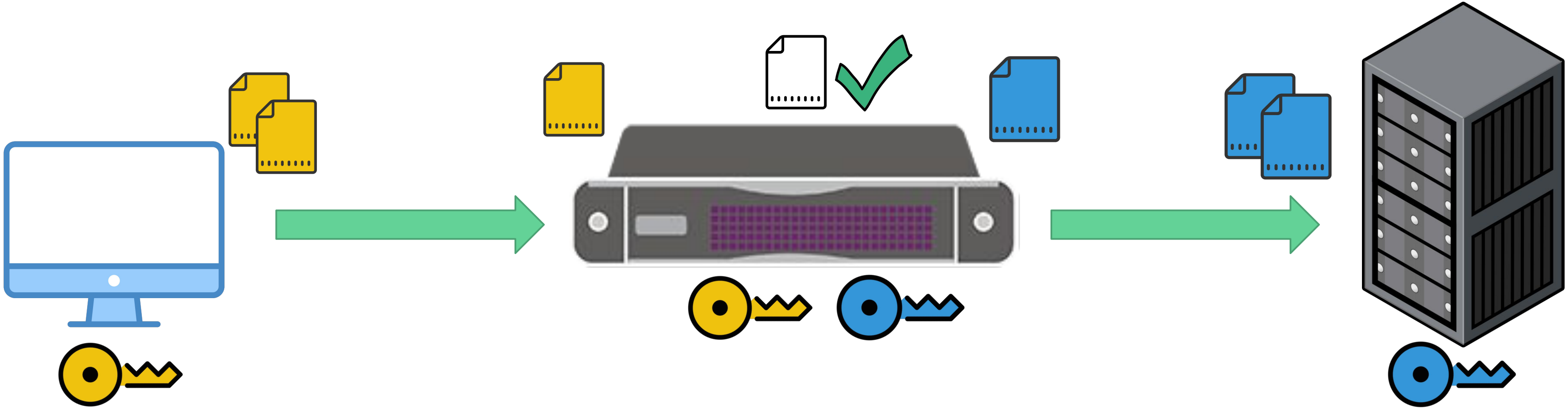


APLOMB: Making Middleboxes Someone Else's Problem - Network Processing as a Cloud Service

Problems with current Middlebox approaches

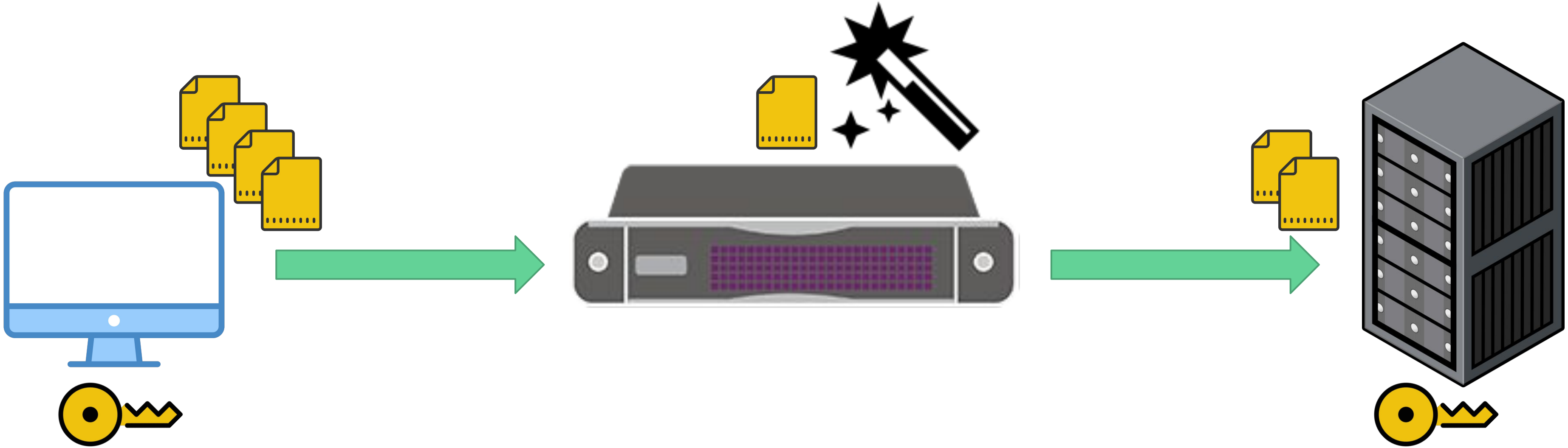


Alternatives



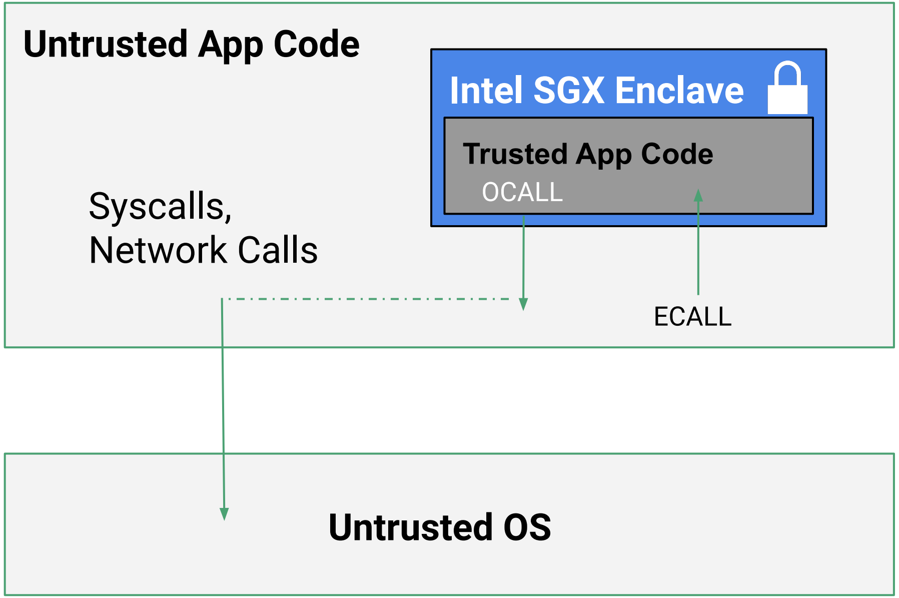
“Break and Inspect”

Alternatives



Homomorphic-Based

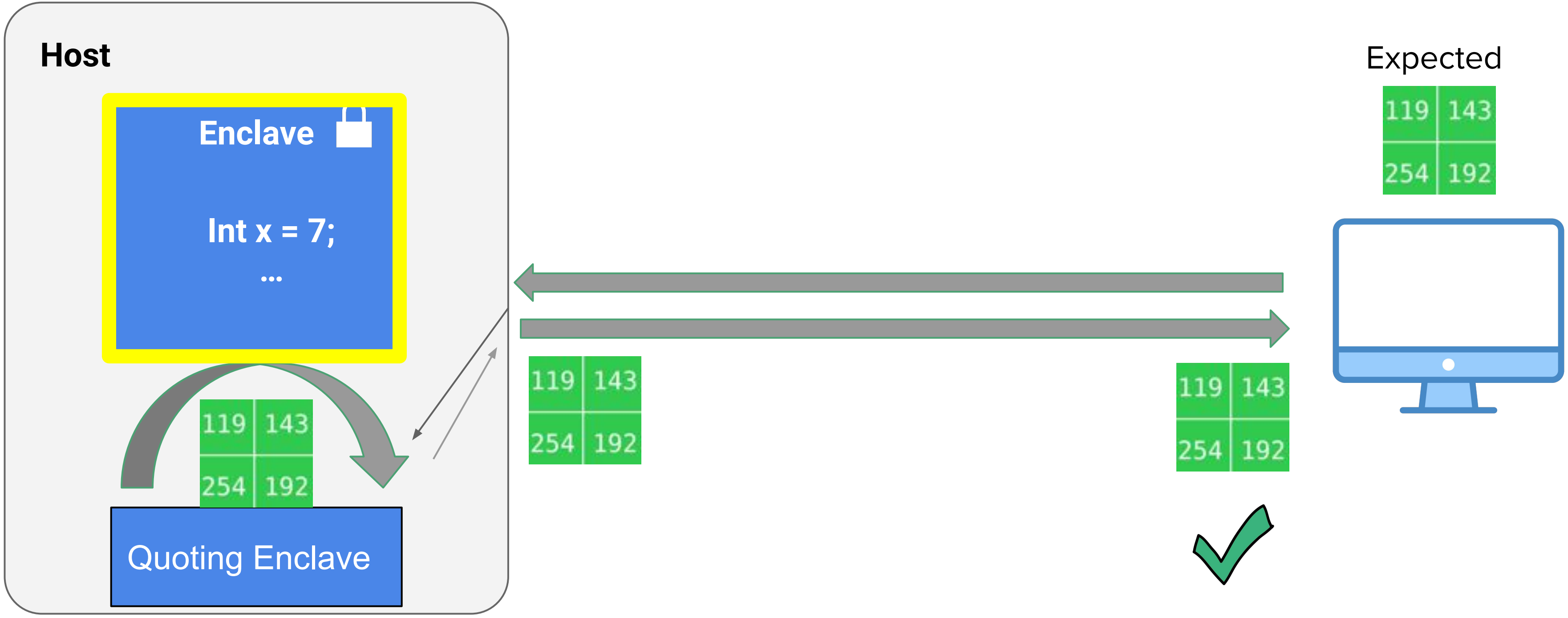
What are Enclaves?



Issues

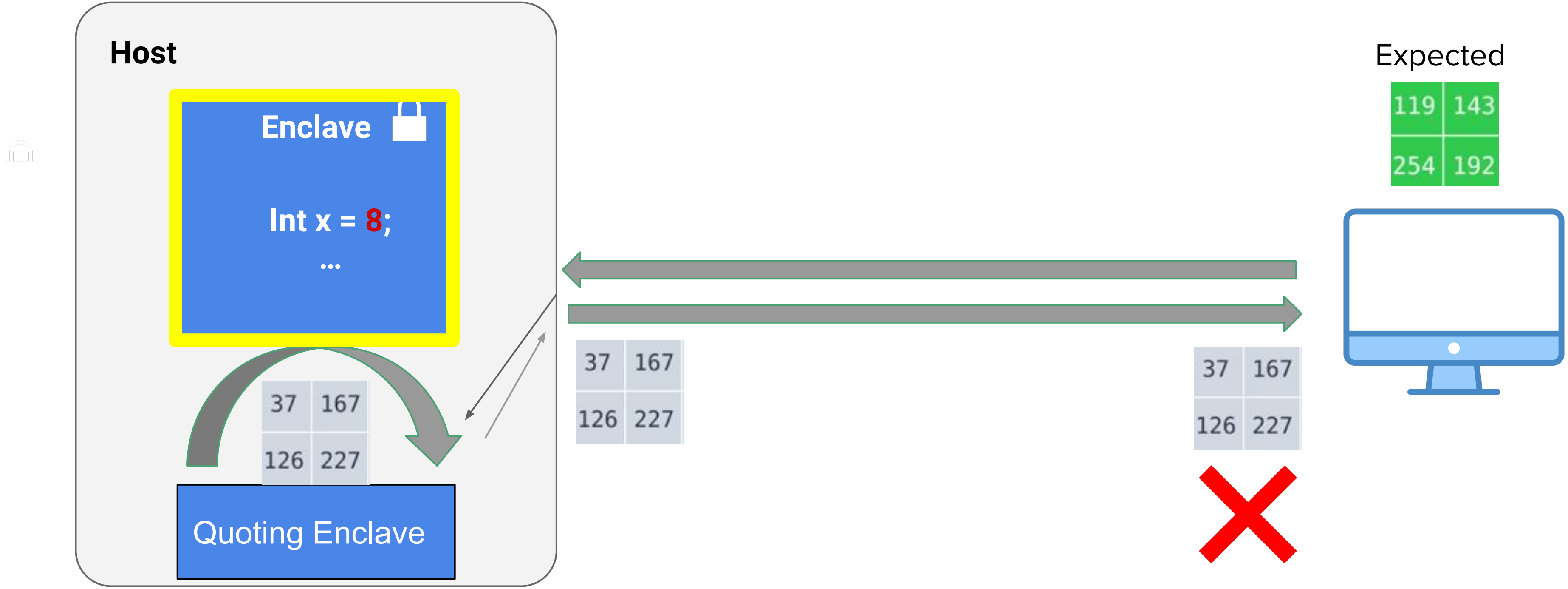
- Memory Constrained
- No Network Calls
- No Trusted Clock

What are Enclaves?



Remote Attestation

What are Enclaves?



37	167
126	227

37	167
126	227

37	167
126	227

119	143
254	192

Remote Attestation

How can SGX help Middleboxes?

- SGX provides **confidentiality** and **integrity**
- **Remotely** attest SGX-enabled middleboxes
    - **Enforce** correct and secure program behavior
    - **Bootstrap** secure channel of communication

SGX Solutions for Middleboxes

- **Decrypting** and **Inspecting** packets safely
- **Processing** and **Saving** information safely
- **Resource** efficiency

Evaluation Metrics

Metrics/Comparison Points

Security

- Network data **protection**
- **Processing** inside enclave?
- Network **metadata** protection?
- Protects NF Vendor code?

Features

- **Read** encrypted packets?
- Network function **chaining**?
- **Stateful** processing?

Usability

- Implementation?
- Performance
- Expressivity?
- Programmability?

Metrics/Comparison Points

Security

- Network data **protection**
- **Processing** inside enclave?
- Network **metadata** protection?
- Protects NF Vendor code?

Features

- **Read** encrypted packets?
- Network function **chaining**?
- **Stateful** processing?

Usability

- Implementation?
- Performance
- Expressivity?
- Programmability?

Metrics/Comparison Points

Security

- Network data **protection**
- **Processing** inside enclave?
- Network **metadata** protection?
- Protects NF Vendor code?

Features

- **Read** encrypted packets?
- Network function **chaining**?
- **Stateful** processing?

Usability

- Implementation?
- Performance
- Expressivity?
- Programmability?

Metrics/Comparison Points

Security

- Network data **protection**
- **Processing** inside enclave?
- Network **metadata** protection?
- Protects NF Vendor code?

Features

- **Read** encrypted packets?
- Network function **chaining**?
- **Stateful** processing?

Usability

- Implementation?
- Performance
- Expressivity?
- Programmability?

Overview of Space

Decrypt and Inspect

- PRI
- SGX-Box
- mbTLS

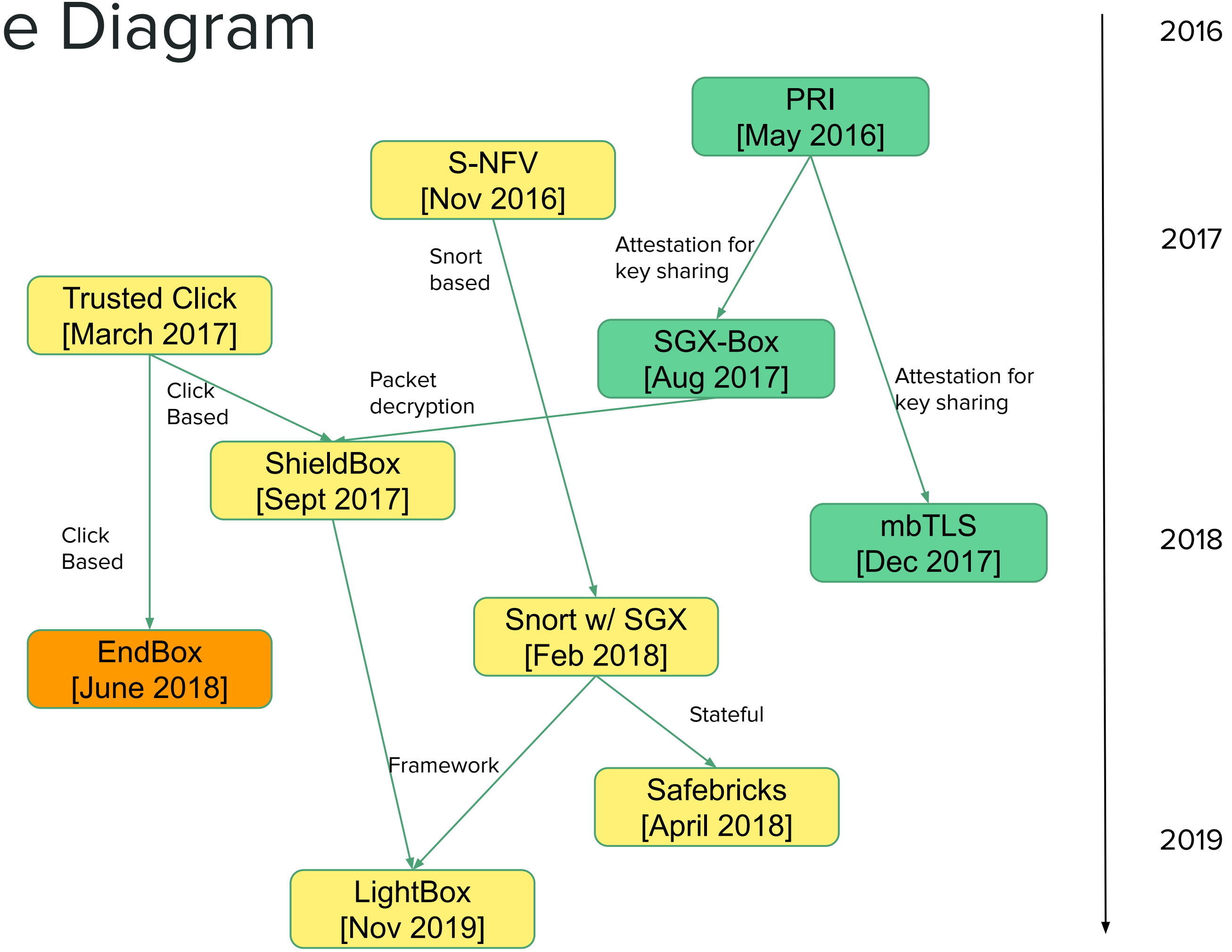
Secure Processing in Third Parties

- S-NFV
- Snort w/ SGX
- Safebricks
- LightBox
- ShieldBox
- Trusted Click

Resource Efficiencies

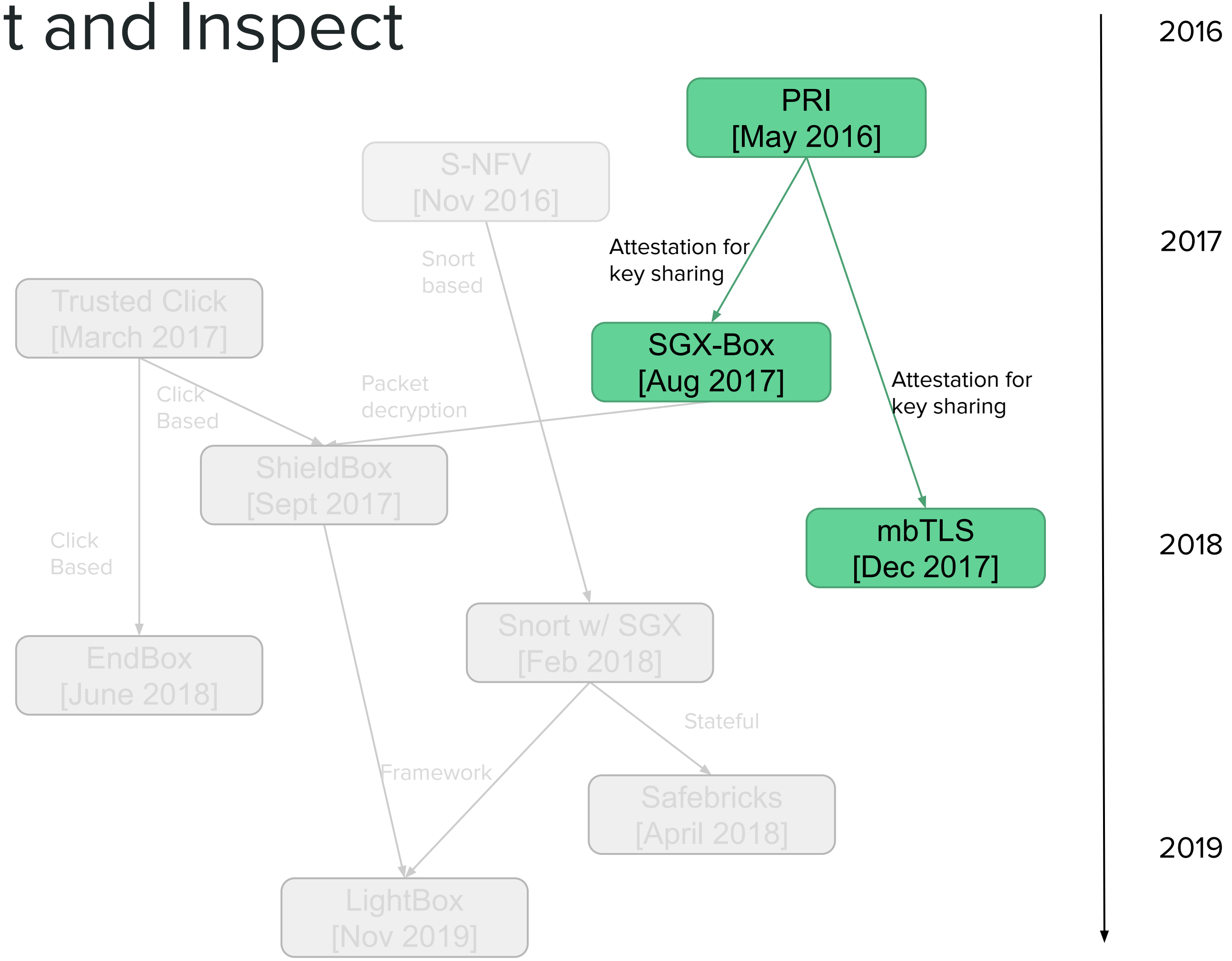
- EndBox

Lineage Diagram

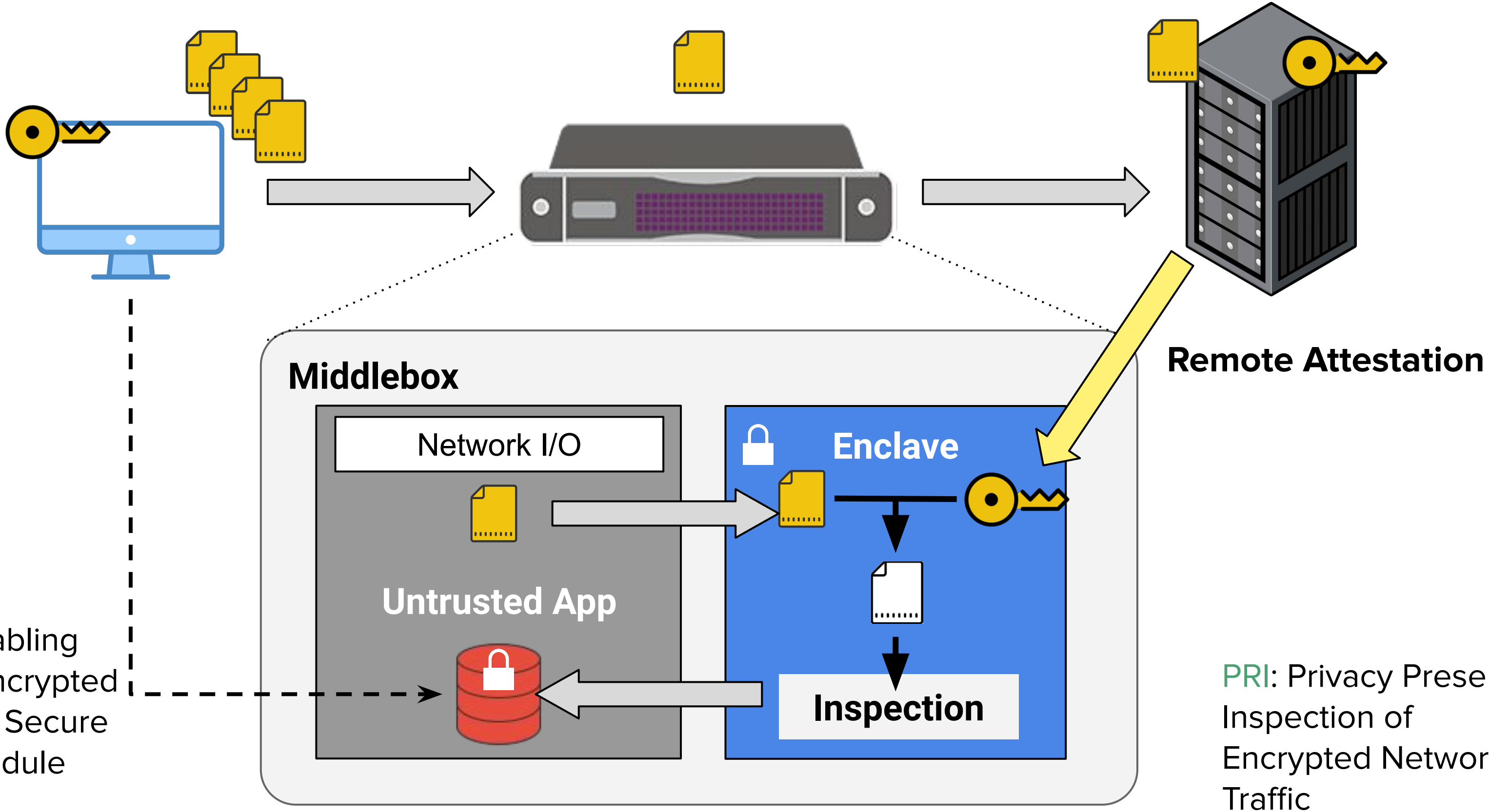


Category 1: Decrypt and Inspect

Decrypt and Inspect



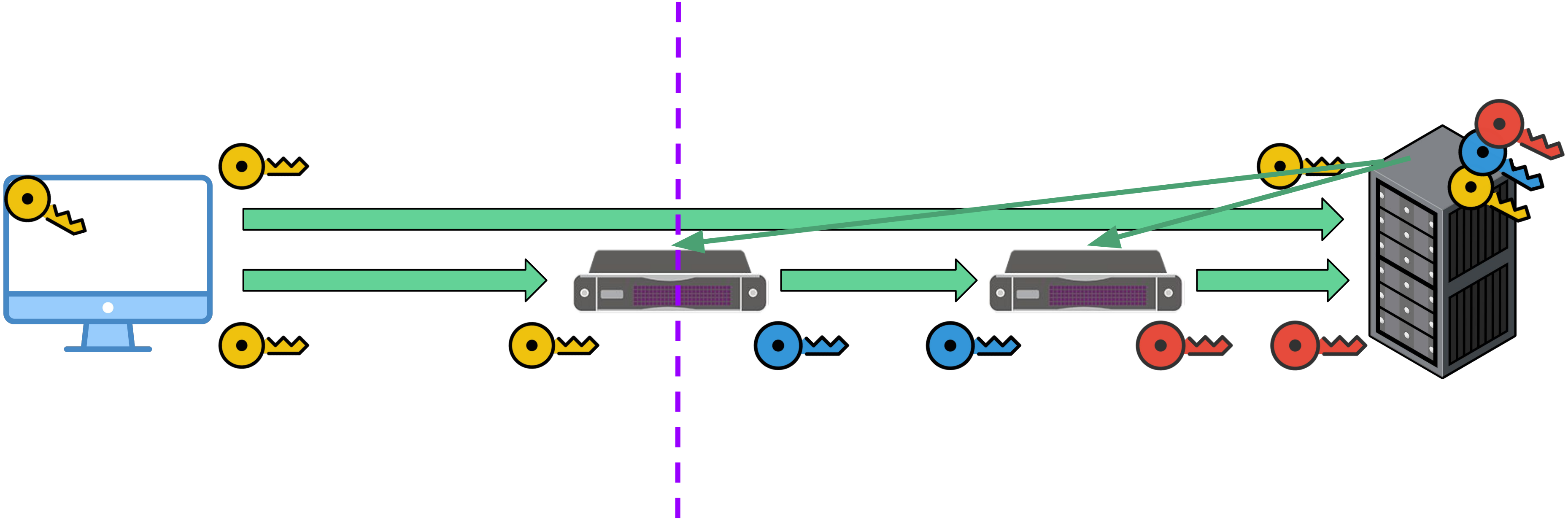
Decrypt and Inspect



SGX-BOX: Enabling Visibility on Encrypted Traffic using a Secure Middlebox Module

PRI: Privacy Preserving Inspection of Encrypted Network Traffic

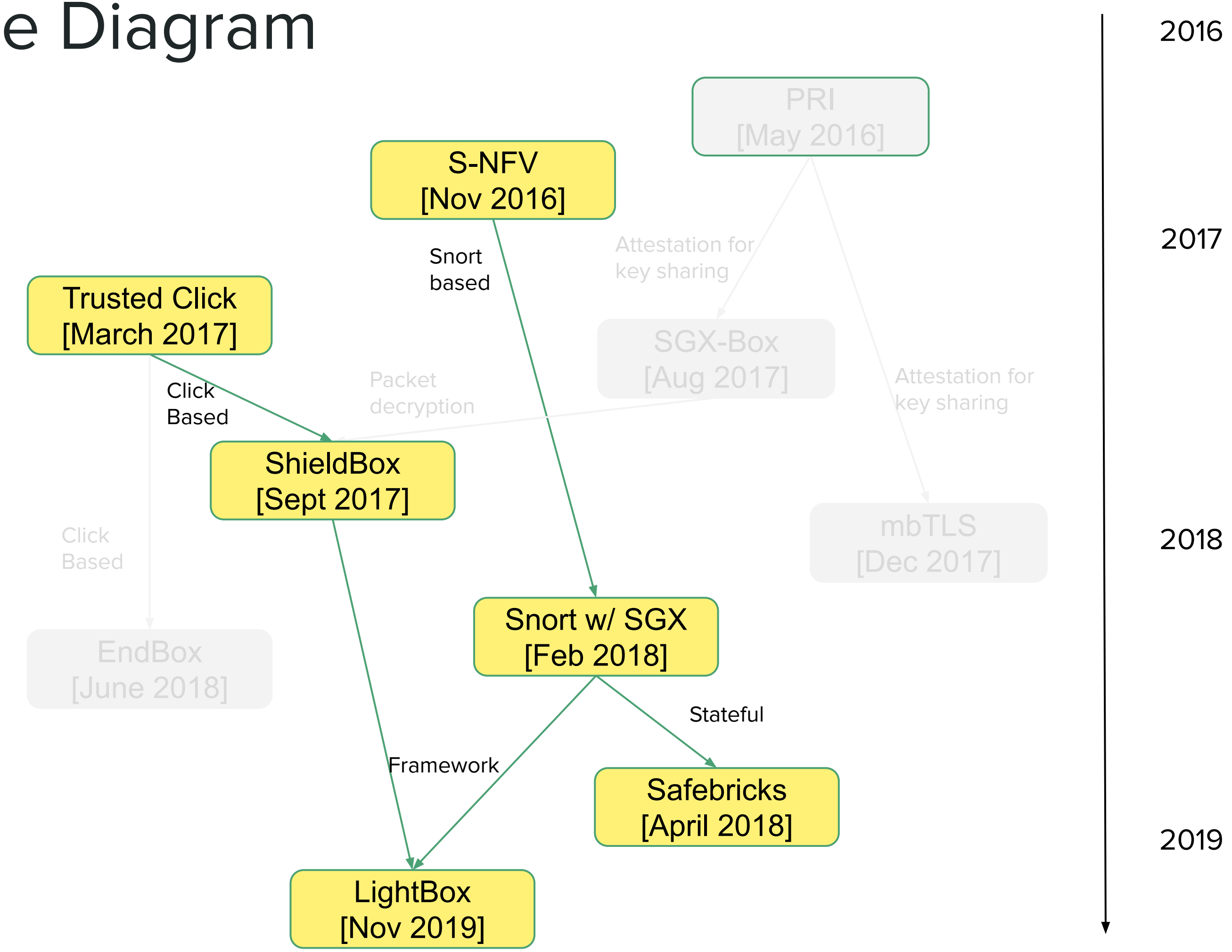
Multiple Middleboxes



mbTLS: And Then There Were More - Secure Communication for More Than Two Parties

Category 2: Secure Processing in the Cloud

Lineage Diagram

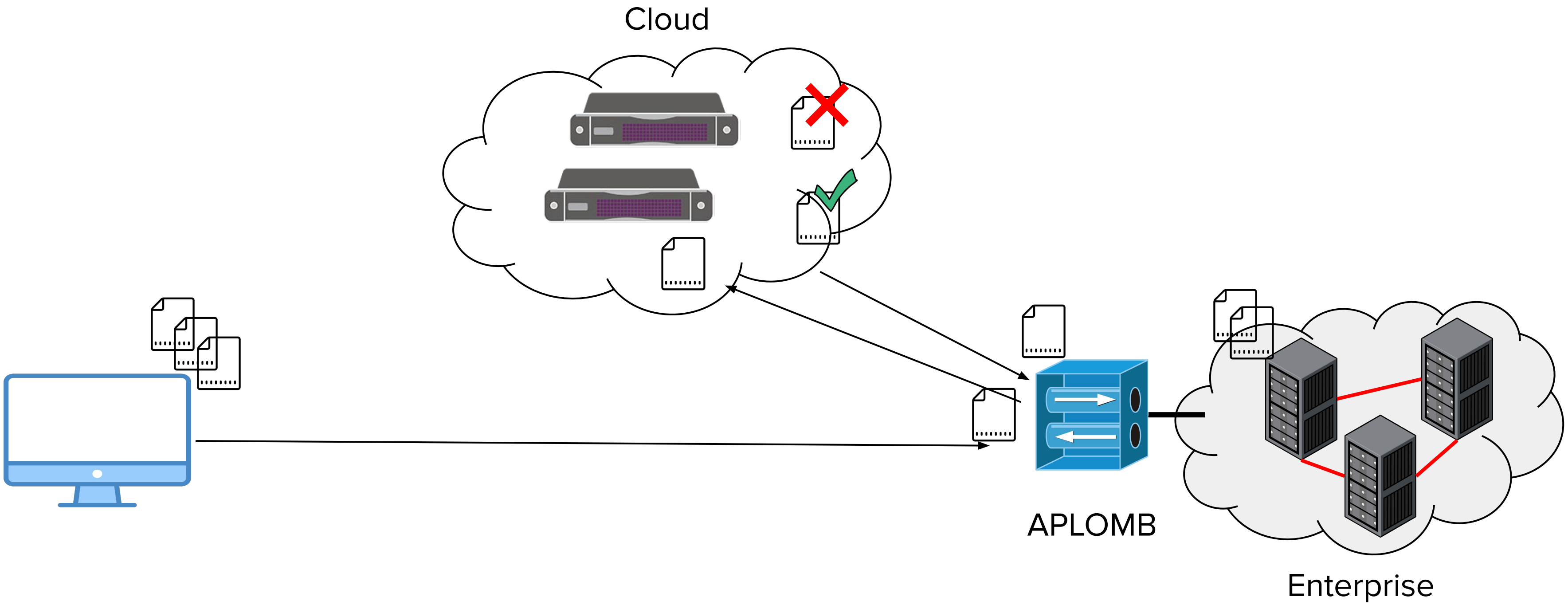


Main Ideas

- Approaches are concerned with problems of running NFs on cloud
    - Need to protect confidentiality of traffic
    - Securely and efficiently read packets
    - Securely enable NF chaining
    - Protect NF vendor code

- Build on existing NF technologies
    - Click
    - Snort
    - NF-enclave specific approaches

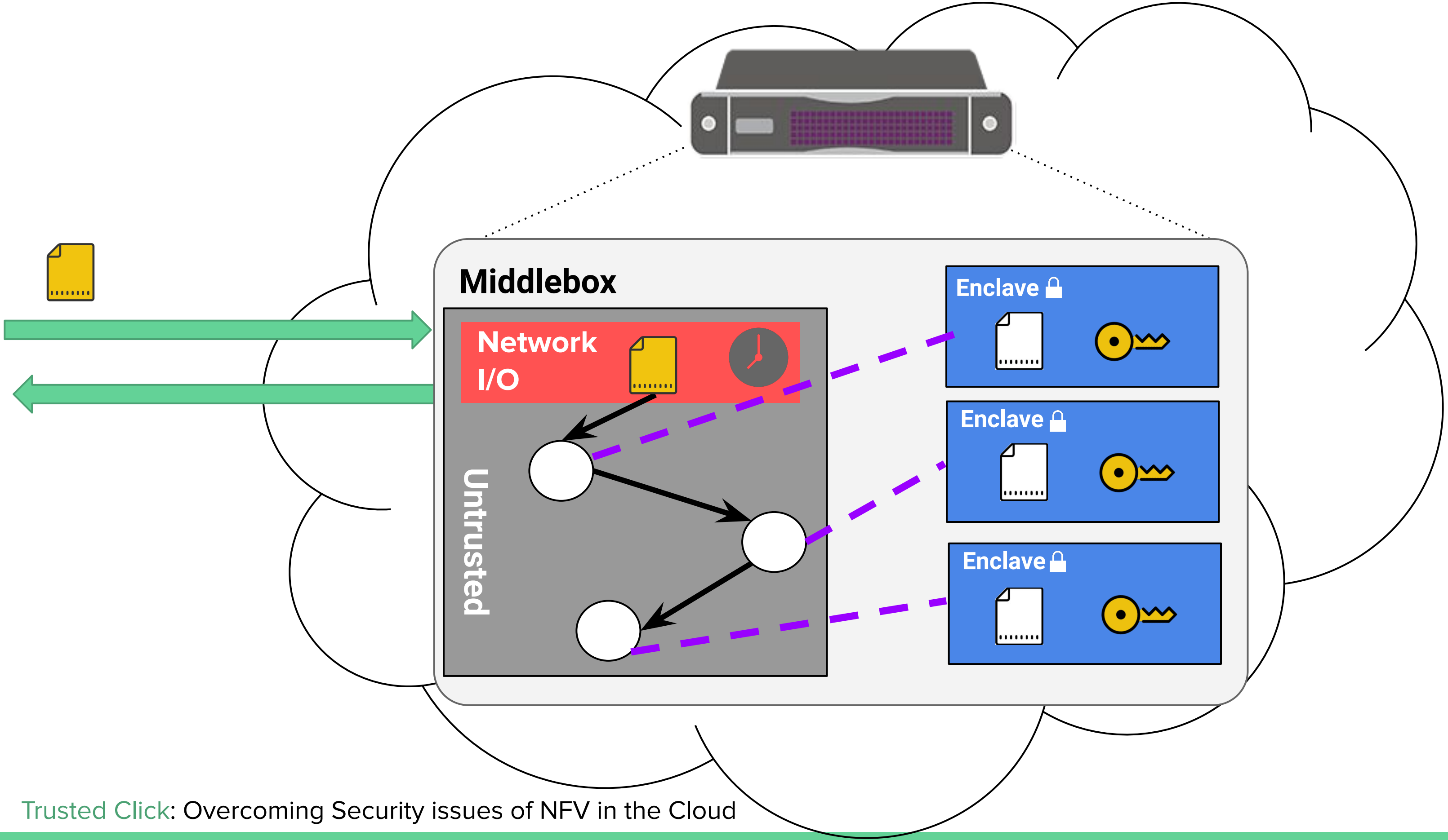
Middleboxes in the Cloud



What is Click?

- Software framework for packet processing
- Elements implement router functions
- Click configurations are modular and easy to extend

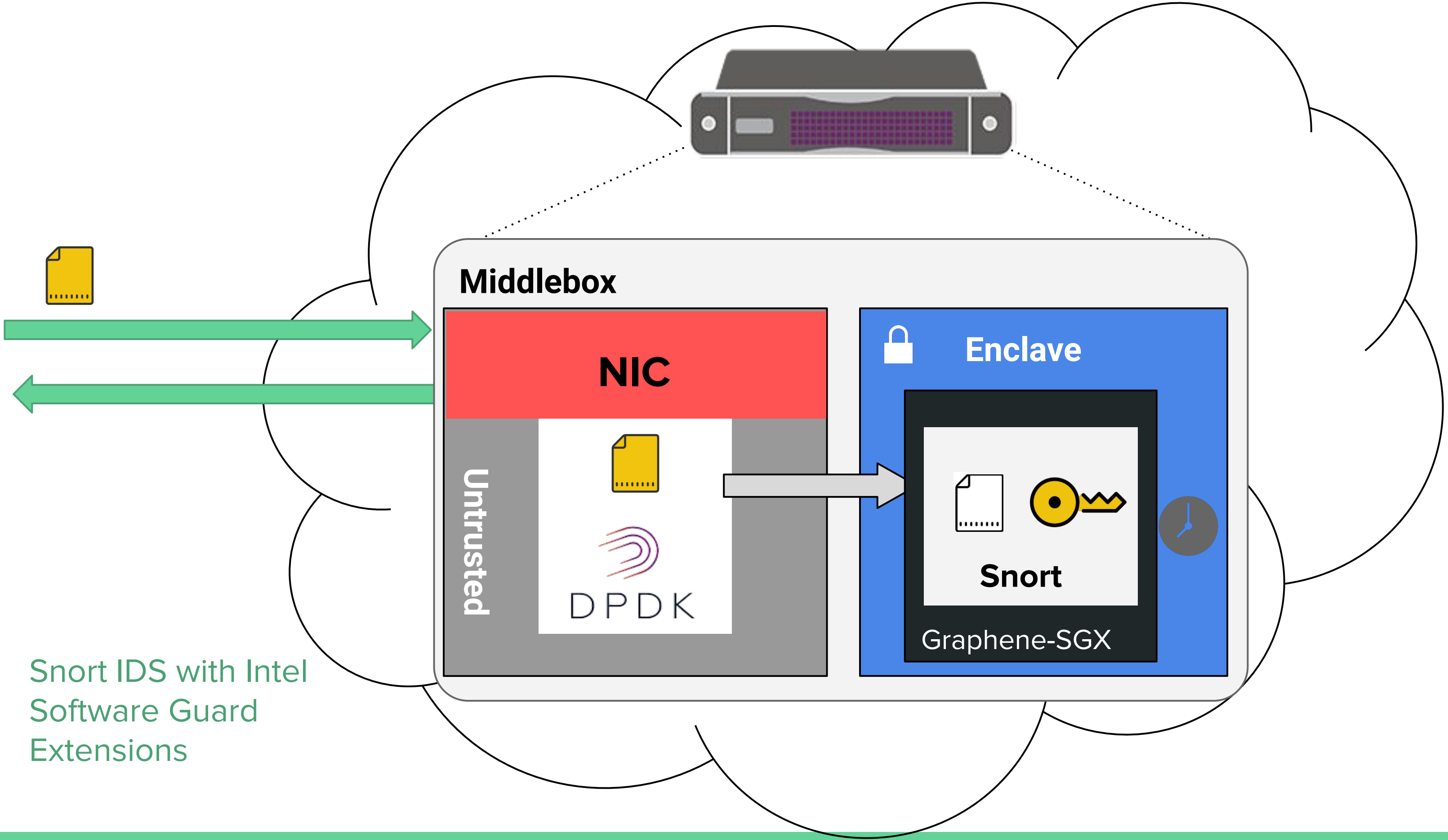
Click Based Approaches



What is Snort?

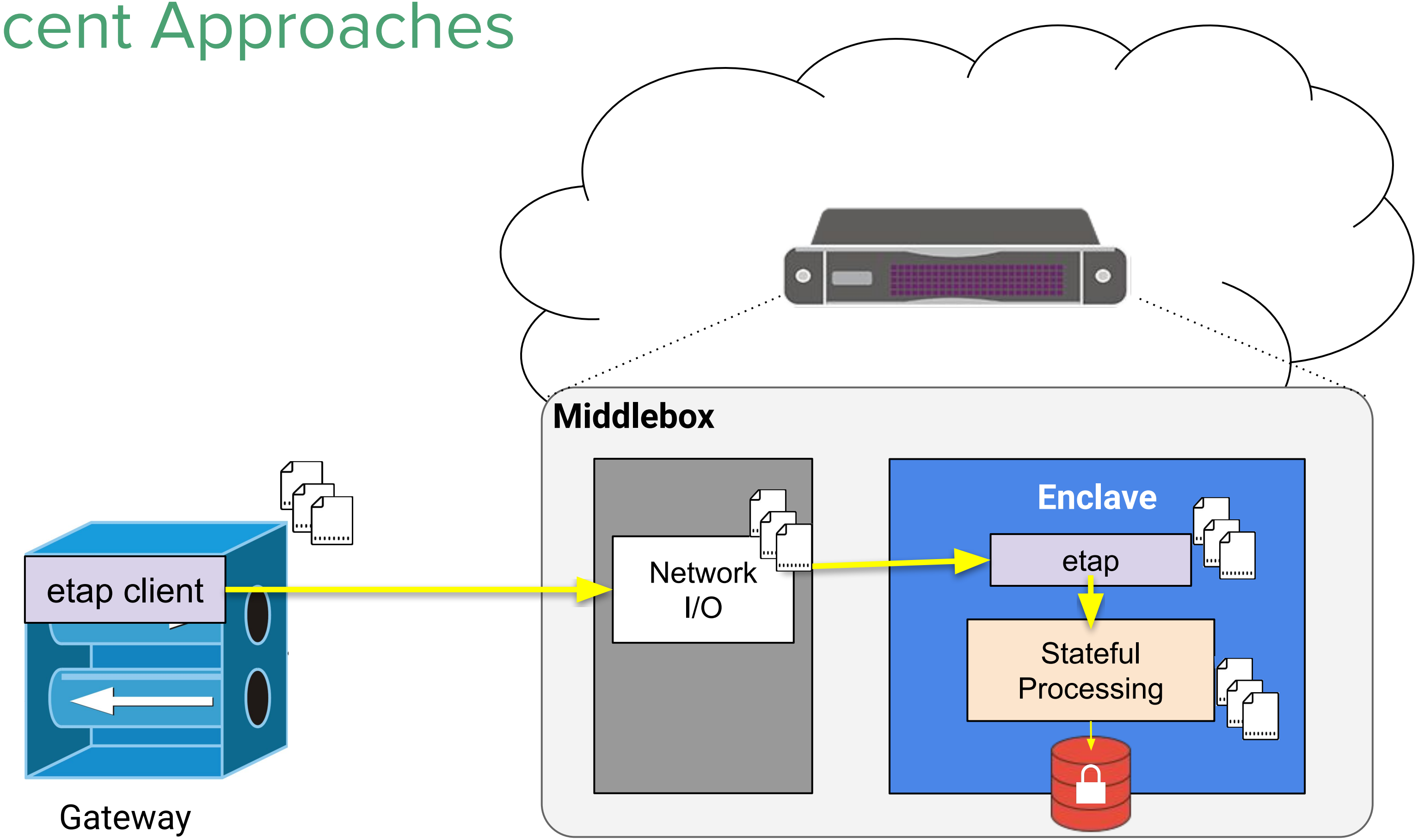
- Signature-based Intrusion Detection/Prevention system
- Real time traffic analysis and packet logging
- Stateful (based on flows)

Snort Based Approaches



Snort IDS with Intel Software Guard Extensions

Recent Approaches



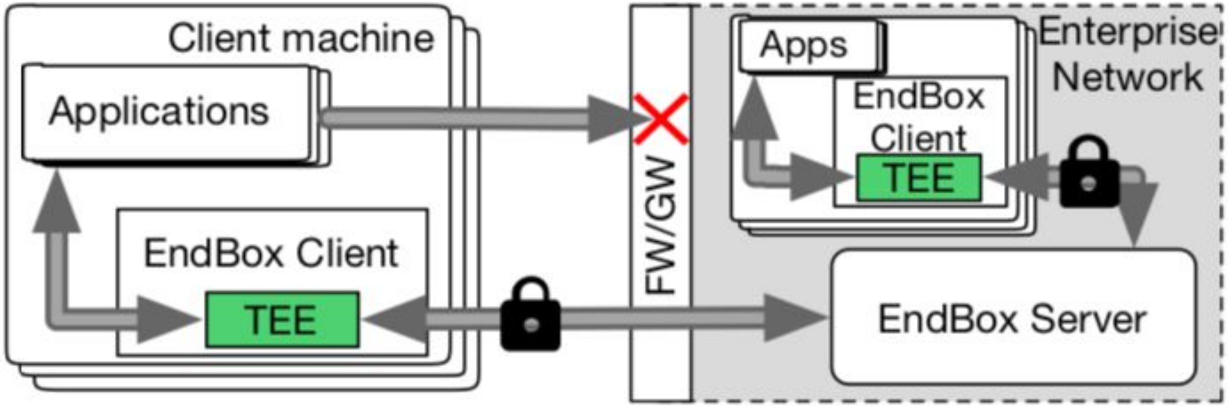
State management

LightBox: Full-stack Protected Stateful Middlebox at Lightning Speed

Category 3: Resource Efficiency

Resource Efficiency

- Run SGX middleboxes on client machines
  - Connections go through client SGX middleboxes because of VPN keys
    - Connections sent directly are refused
  - After, necessary processing, SGX middlebox forwards traffic accordingly



https://www.ibr.cs.tu-bs.de/users/goltzsch/slides/endbox-dsn18.pdf

EndBox: Scalable Middlebox Functions Using Client-Side Trusted Execution

Future Work

Future Directions

- Decentralized Approach
  - Stateful processing
  - Least Privilege to keep NFs “honest”
- Side Channels
  - Existing work focuses on metadata protection, not on timing related or other side channels