NTNU

MŰEGYETEM 1782

CrySyS

SafeLib: a comprehensive framework for secure outsourcing of network functions

Gergely Biczók (Enio Marku, Colin Boyd)

CrySyS Lab, BME

biczok@crysys.hu

Motivation: Ukraine

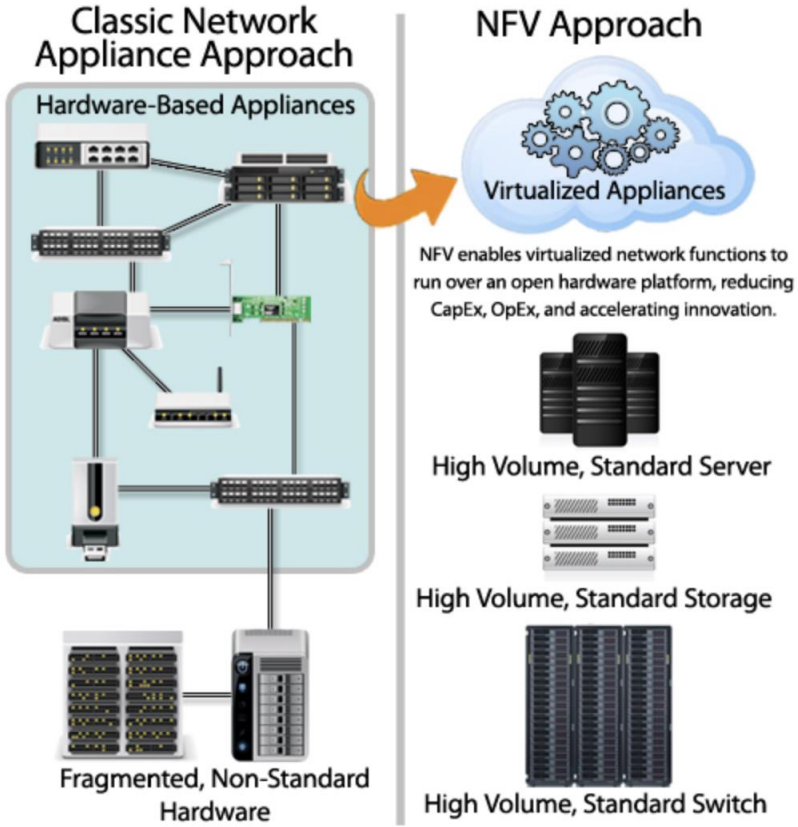
This report offers five conclusions that come from the war's first four months:

networks. But Ukraine's government has successfully sustained its civil and military operations by acting quickly to disburse its digital infrastructure into the public cloud, where it has been hosted in data centers across Europe.

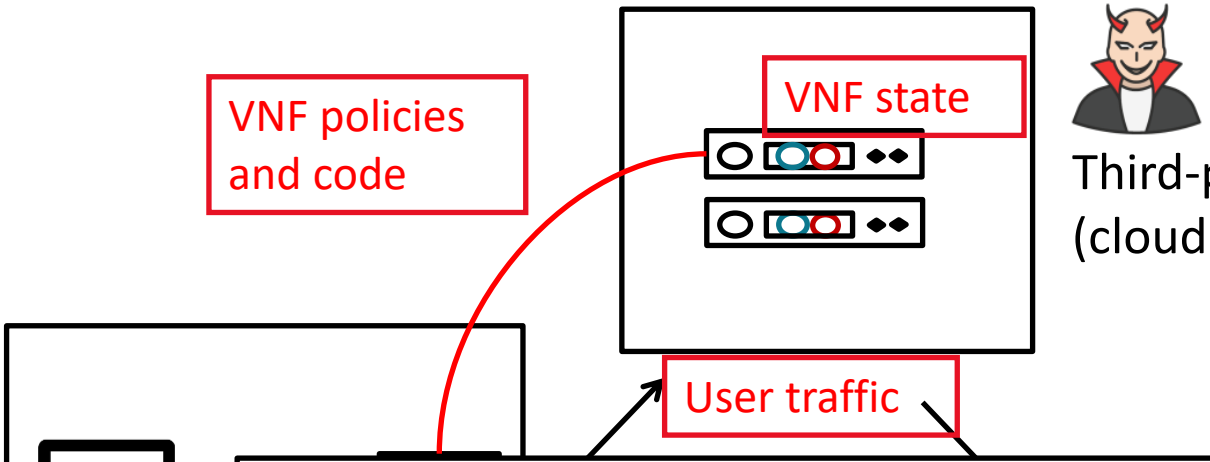
Motivation: NFV

Type of appliance	*Number*
Firewalls	166
NIDS	127
Media gateways	110
Load balancers	67
Proxies	66
VPN gateways	45
WAN Optimizers	44
Voice gateways	11
Total Middleboxes	***636***
Total routers	***~900***

Enterprise w/ 80K users and tens of sites



Problem statement: outsourcing security



Can we provide **security for outsourced VNFs**

- in terms of **enterprise traffic, VNF state, VNF code & input policies**
- with **performance comparable to** traditional dedicated **hardware NFs**?

Quick outline

- Existing solutions
- Trusted hardware enviroment (=SGX)
- SafeLib: idea
- Safelib: high-level design
- Safelib: detailed design for complex stateful NFs
- Some performance figures
- Security guarantees
- Technical papers and code

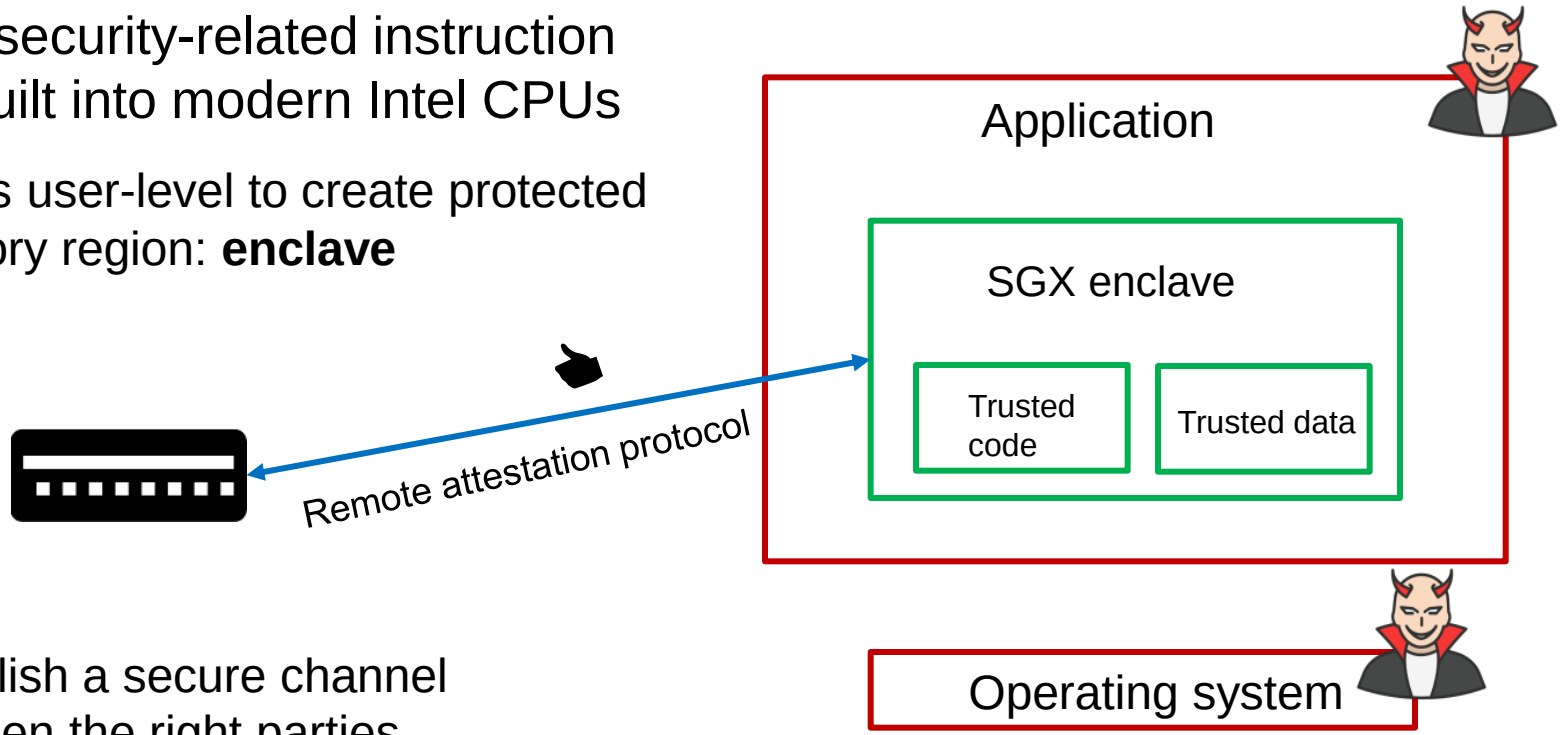
Existing solutions & limitations

		Protection					Supported Functionality		Supported
	System	Header	Payload	Code	Policies	State	Stateful VNF	Stateless VNF	Operation
Crypto	BlindBox [4]	✗	✓	✗	✓	✗	✗	✓	regular expression
	SplitBox [5]	✓	✓	✗	✓	✗	✗	✓	range matching
	Embark [3]	✓	✓	✗	✓	✗	✗	✓	range matching
Trusted Hardware	S-NFV [8]	✗	✗	✗	✗	✓	✓	✗	generic operation
	Trusted Click [6]	✗	✓	✗	✓	✗	✗	✓	generic operation
	ShieldBox [10]	✓	✓	✗	✓	✗	✗	✓	generic operation
	SGX-Box [9]	✗	✓	✗	✓	✓	✓	✗	generic operation
	SafeBricks [7]	✓	✓	✓	✓	⋆	⋆	✓	generic operation
	LightBox [11]	✓	✓	✗	✓	✓	✓	⋆	generic operation
	SafeLib [12]	✓	✓	✓	✓	✓	✓	✓	generic operation

- Standard encryption: NF cannot operate
- Fancy crypto approaches: limited operations w/ low performance
- Trusted Execution Environment based approaches?

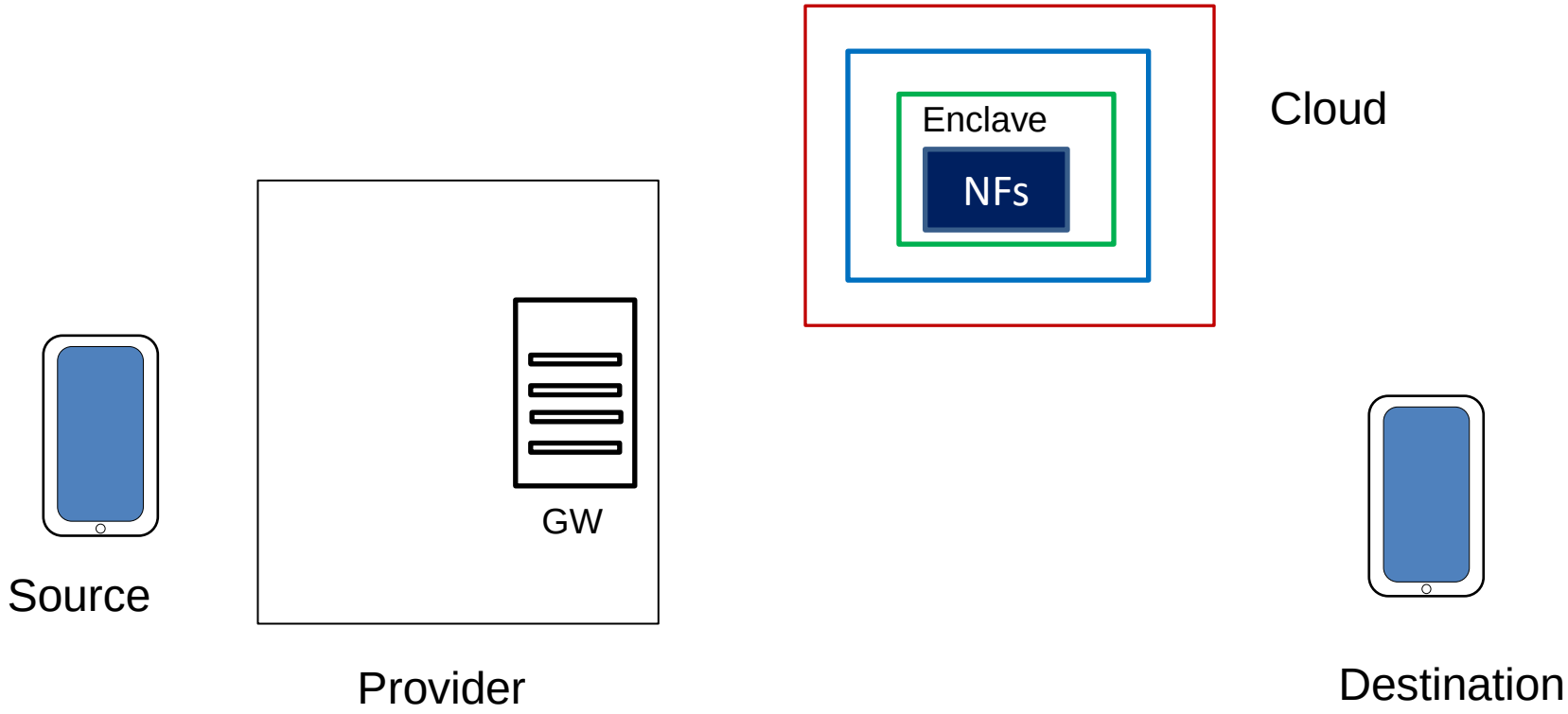
Trusted Execution Environment (Intel SGX)

- A set of security-related instruction codes built into modern Intel CPUs
  - Allows user-level to create protected memory region: **enclave**
  - Establish a secure channel between the right parties

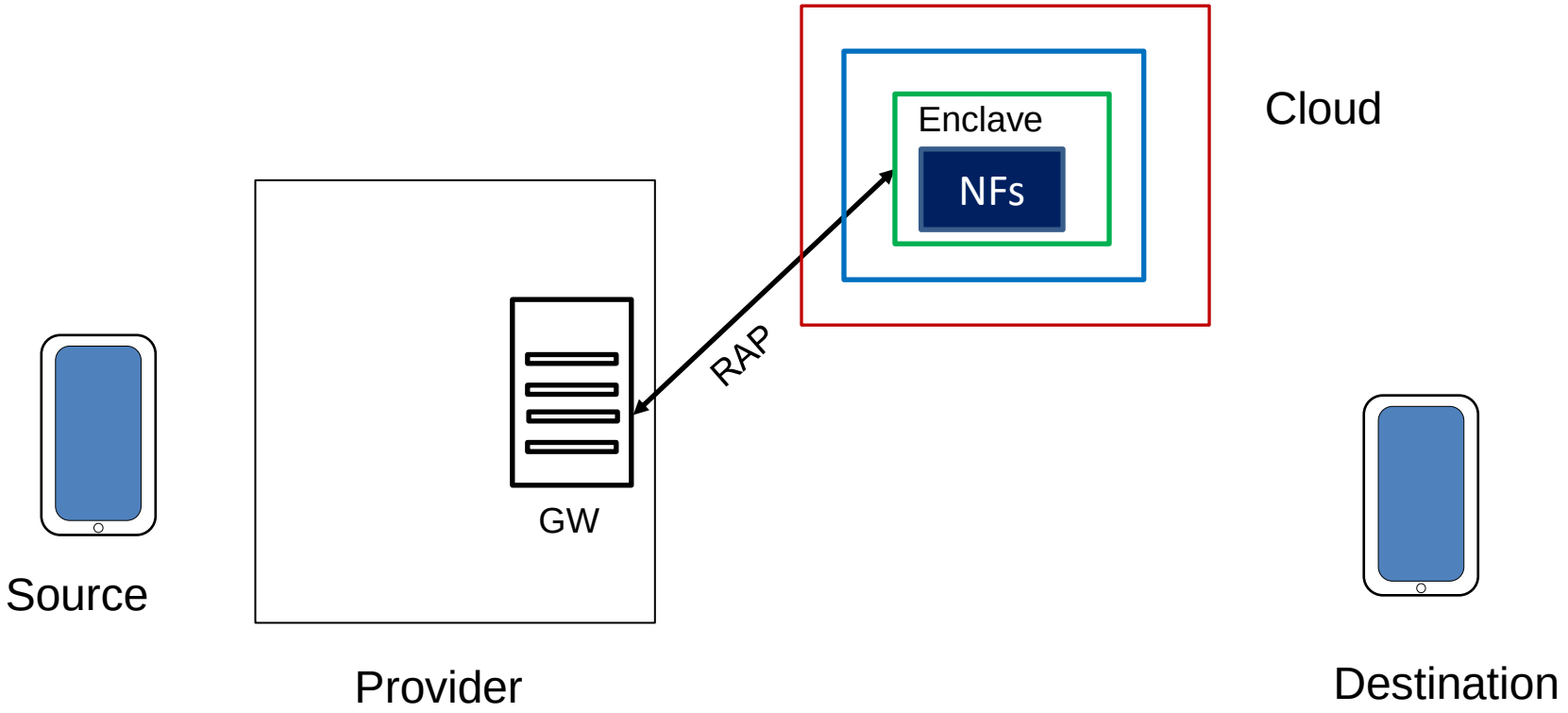


Untrusted part Trusted part

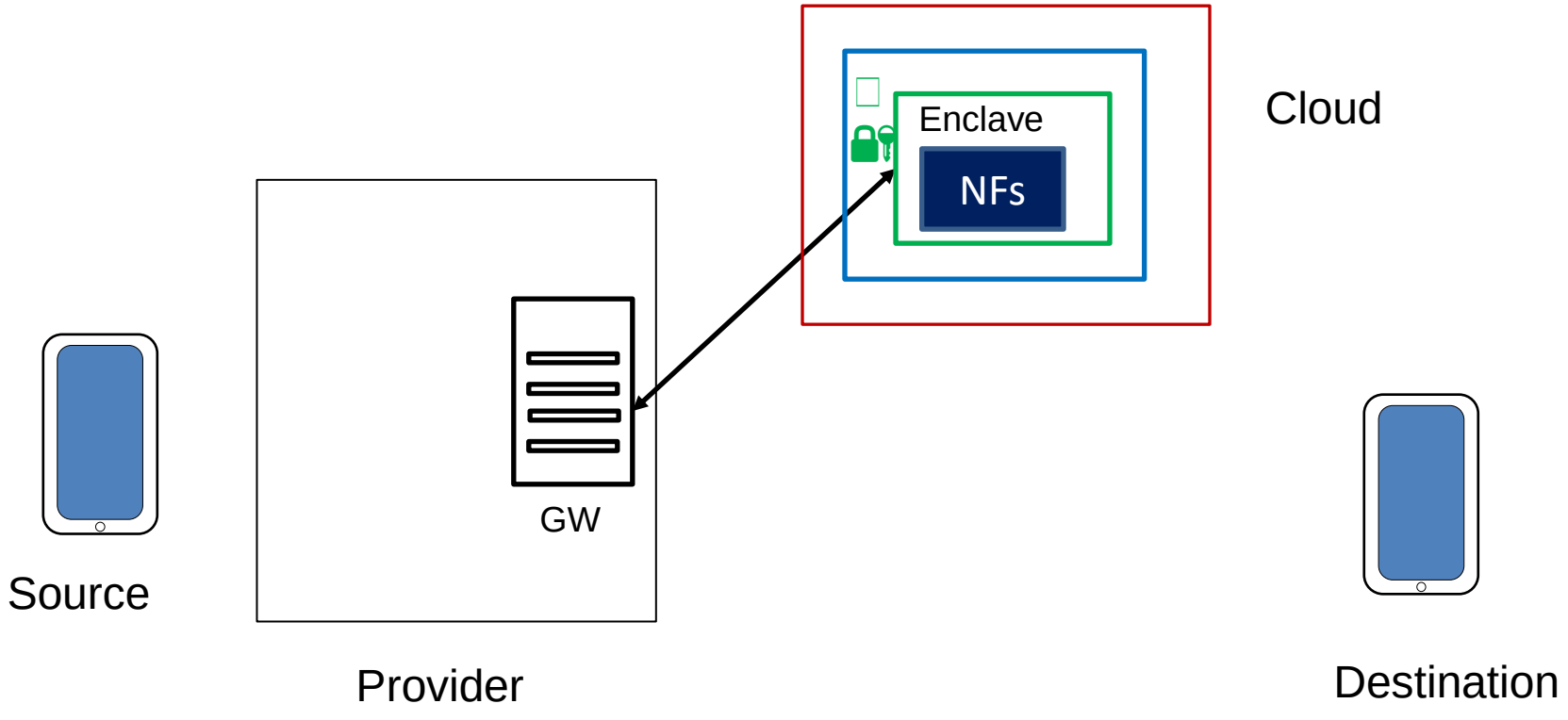
Example: protect user traffic from Cloud



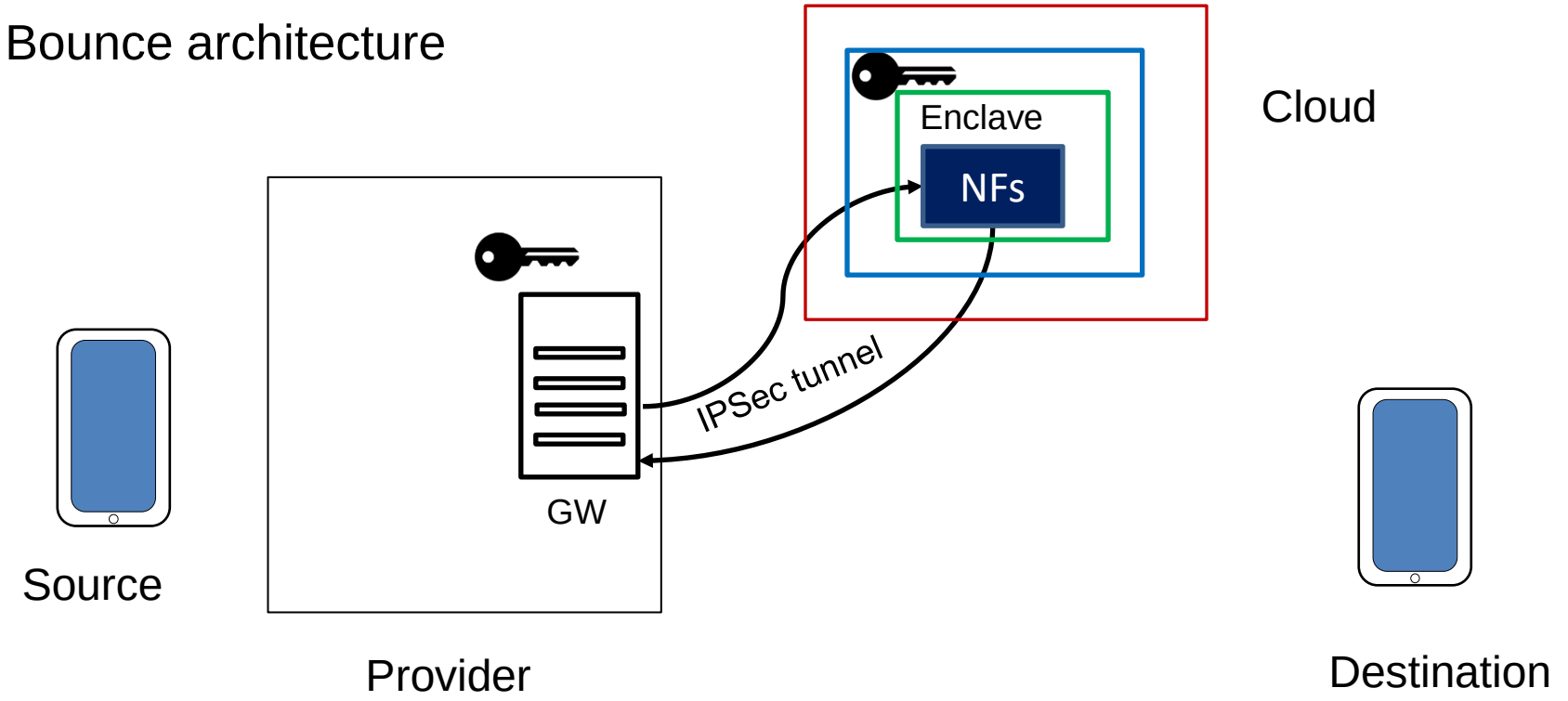
Example: protect user traffic from Cloud



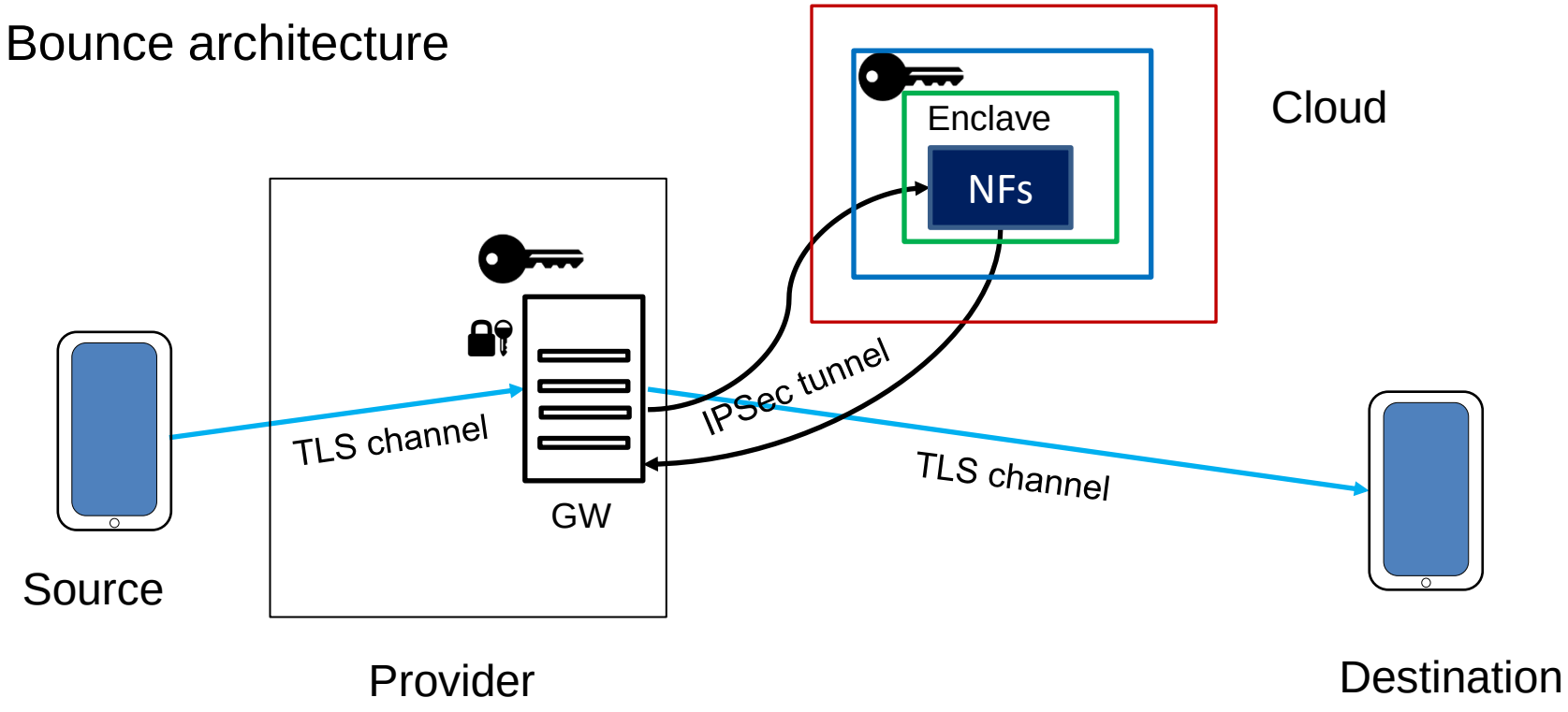
Example: protect user traffic from Cloud



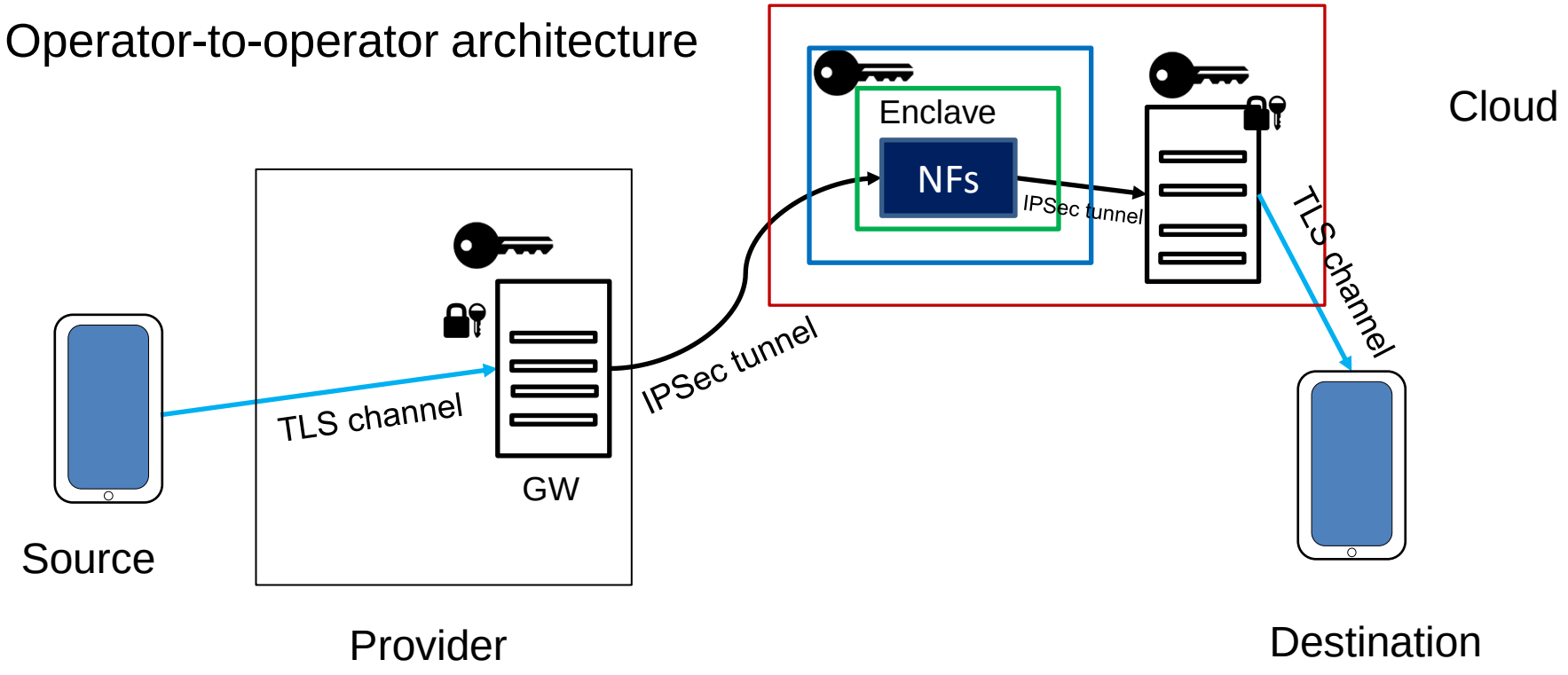
Example: protect user traffic from Cloud



Example: protect user traffic from Cloud

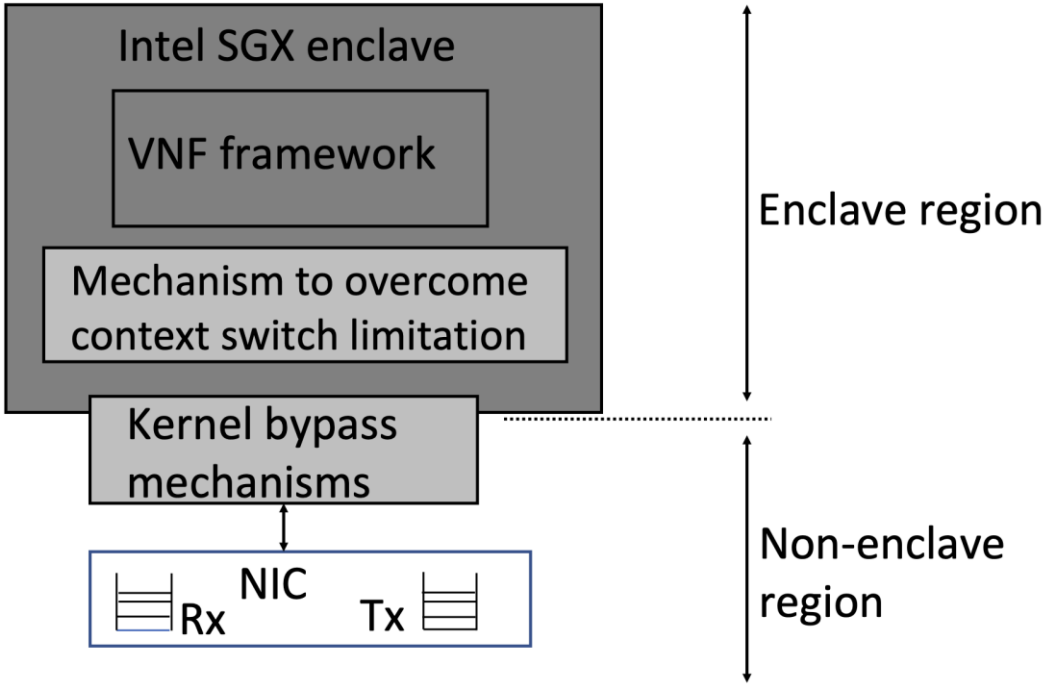


Example: protect user traffic from Cloud

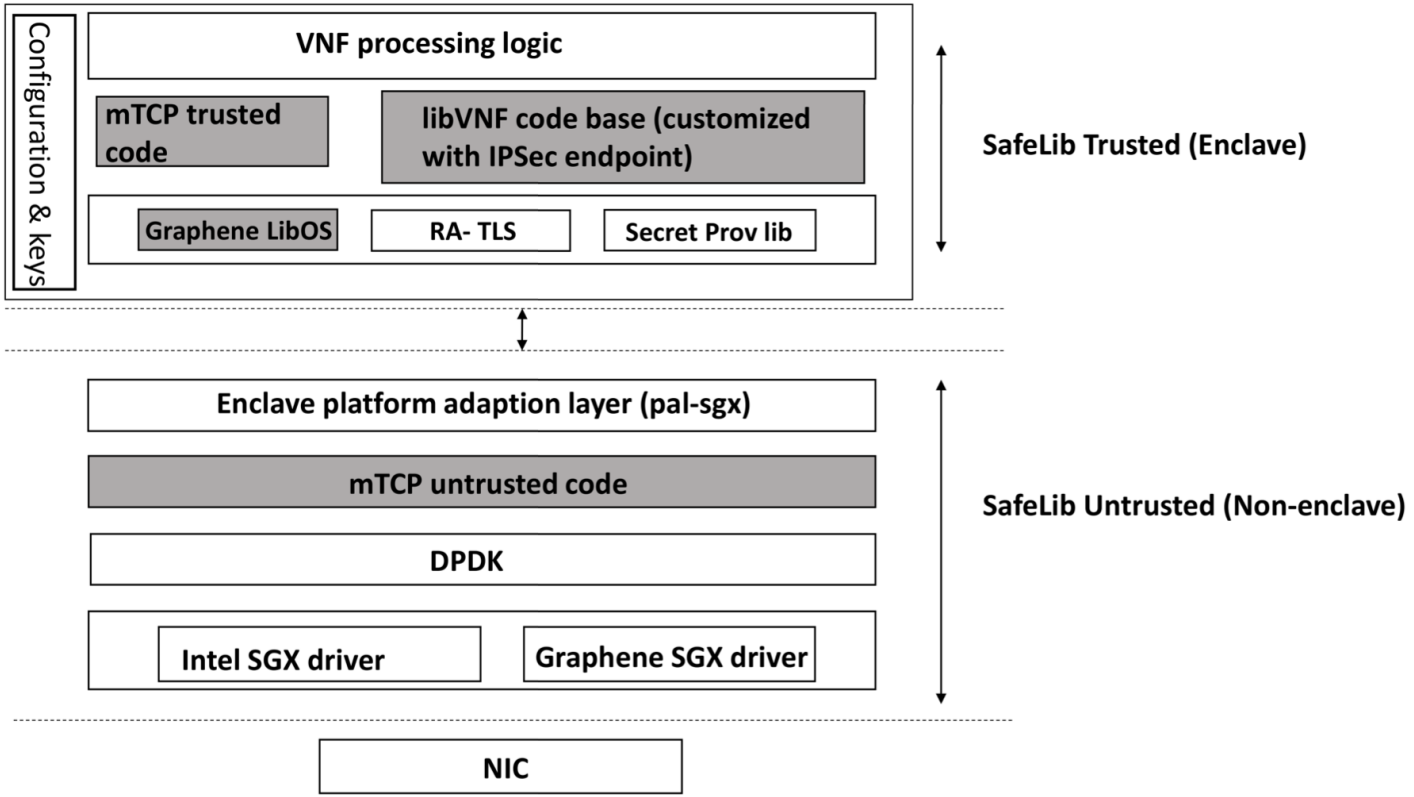


SafeLib: high-level architecture

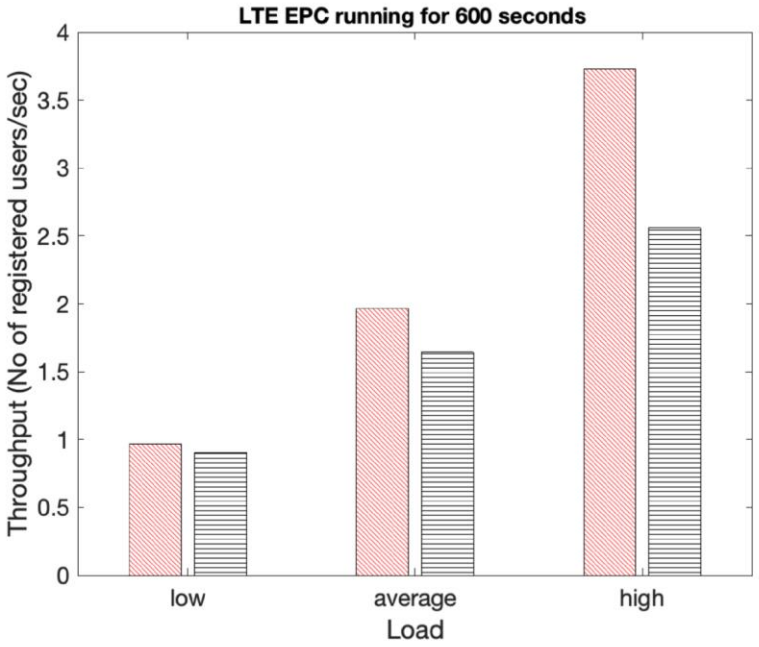
- SGX limitations!
  - Enclave memory size is limited
  - Transition between enclave and non-enclave region is costly -> performance!
- 3 libs for different NFs
  - Simple stateful
  - Complex stateful
  - Stateless

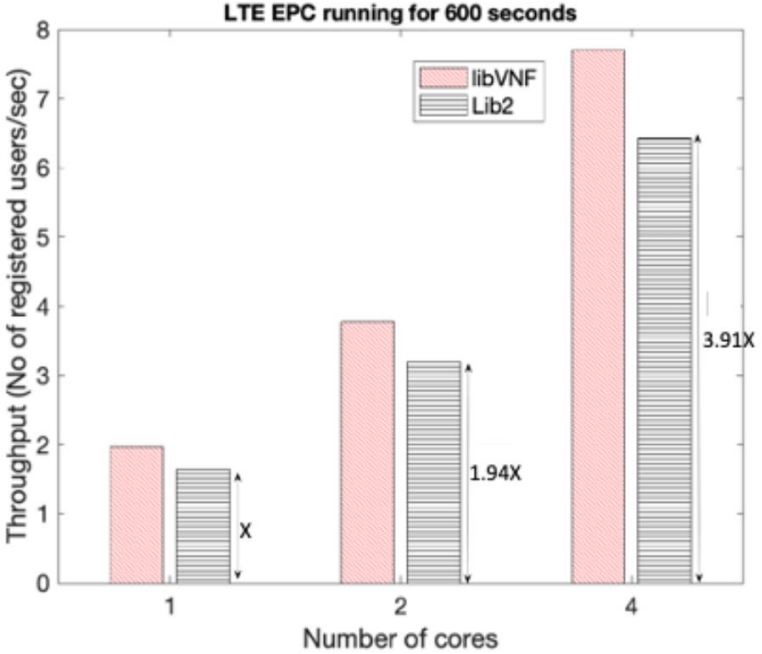


SafeLib: detailed architecture (lib2, complex stateful)



SafeLib: performance (LTE-EPC, MME outsourced)





Performance penalty is small(ish)

Performance scales linearly w/ #CPU cores

Key: choose appropriate libx for your VNF

SafeLib: summary

- Comprehensive* protection for outsorced NFs
- Support for simple/complex and stateful/stateless NFs
- Minimal performance penalty vs. vanilla libVNF
- Good scaling properties for multi-core
- Good usability for NF developers

Scope	Security Properties
VNF execution	Integrity
VNF state (flow stream)	Integrity and confidentiality
VNF policies	Integrity and confidentiality
VNF code	Integrity, confidentiality (at some level)
User traffic	Integrity and confidentiality

Papers…

SafeLib: a comprehensive framework for secure outsourcing of network functions
E. Marku, C. Boyd, G. Biczók
Under review in IEEE Transactions on Network and Service Management

SafeLib: a practical library for outsourcing stateful network functions securely
E. Marku, G. Biczók, C. Boyd
2021 IEEE 7th International Conference on Network Softwarization (NetSoft 2021), 2021

Securing Outsourced VNFs: Challenges, State of the Art, and Future Directions
E. Marku, G. Biczók, C. Boyd
IEEE Communications Magazine, vol. 58, no. 7, vol. 58, 2020, pp. 1-8.

Towards protected VNFs for multi-operator service delivery
E. Marku, G. Biczók, C. Boyd
1st International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft), IEEE, 2019, co-located with IEEE NetSoft 2019.

… and code!

“We believe in rough consensus and running code”

https://github.com/eniomarku/SafeLib-TNSM