UNIVERSITÀ DEGLI STUDI DI BERGAMO

UNIVERSITÀ DEGLI STUDI DI BERGAMO

Scuola di Ingegneria

Corso di Laurea Magistrale in Ingegneria Informatica

Malicious context and workaround analysis of decentralized VPN: the case of Mysterium Network

Relatore:
Chiar.mo Prof. Stefano Paraboschi

Tesi di Laurea Magistrale
Jacopo FEDERICI
Matricola n. 1025458

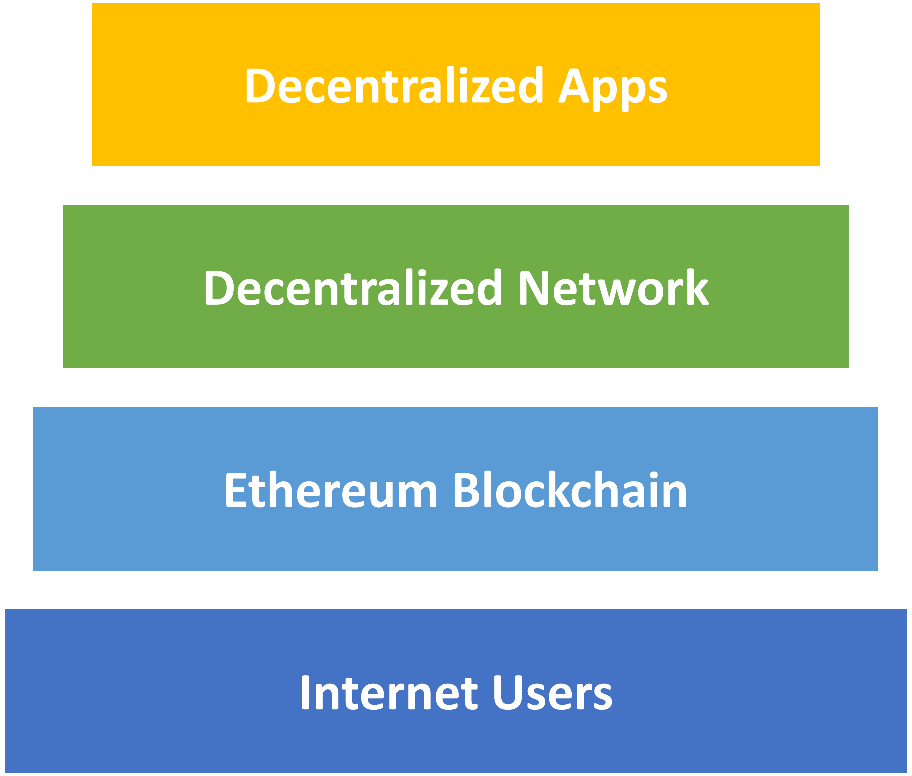
ANNO ACCADEMICO 2018/2019

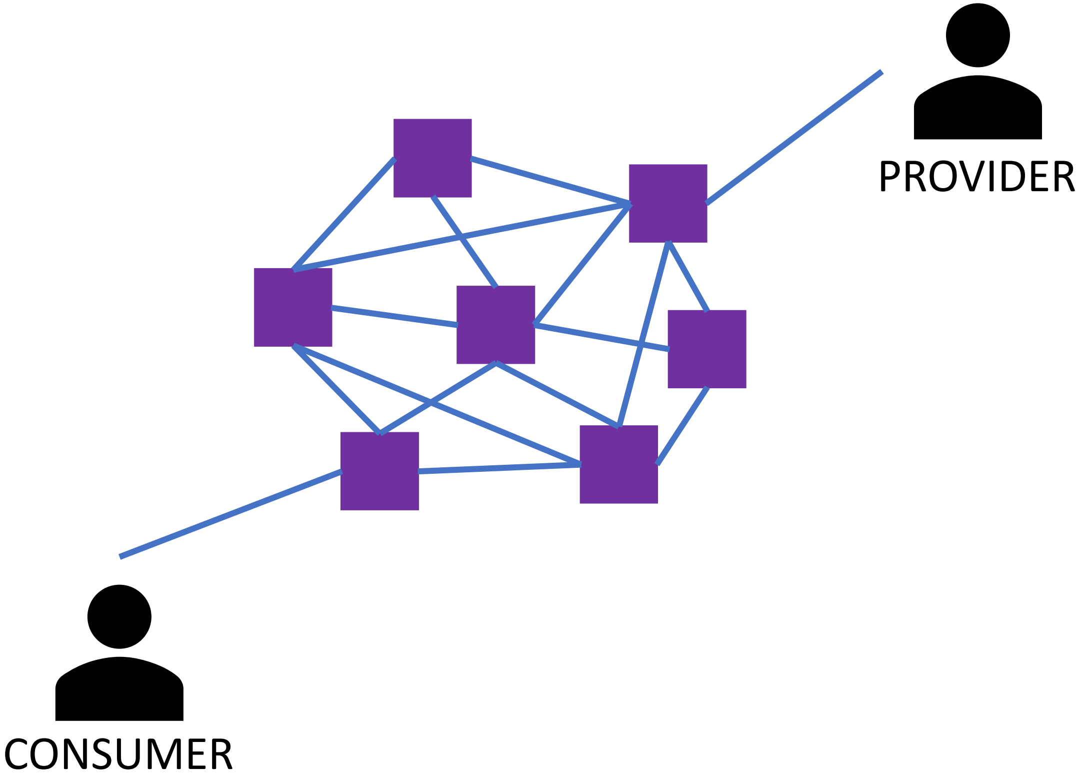
Thesis goals

1. Analyze malicious contexts & provide working PoCs
2. Design solutions & provide working PoCs

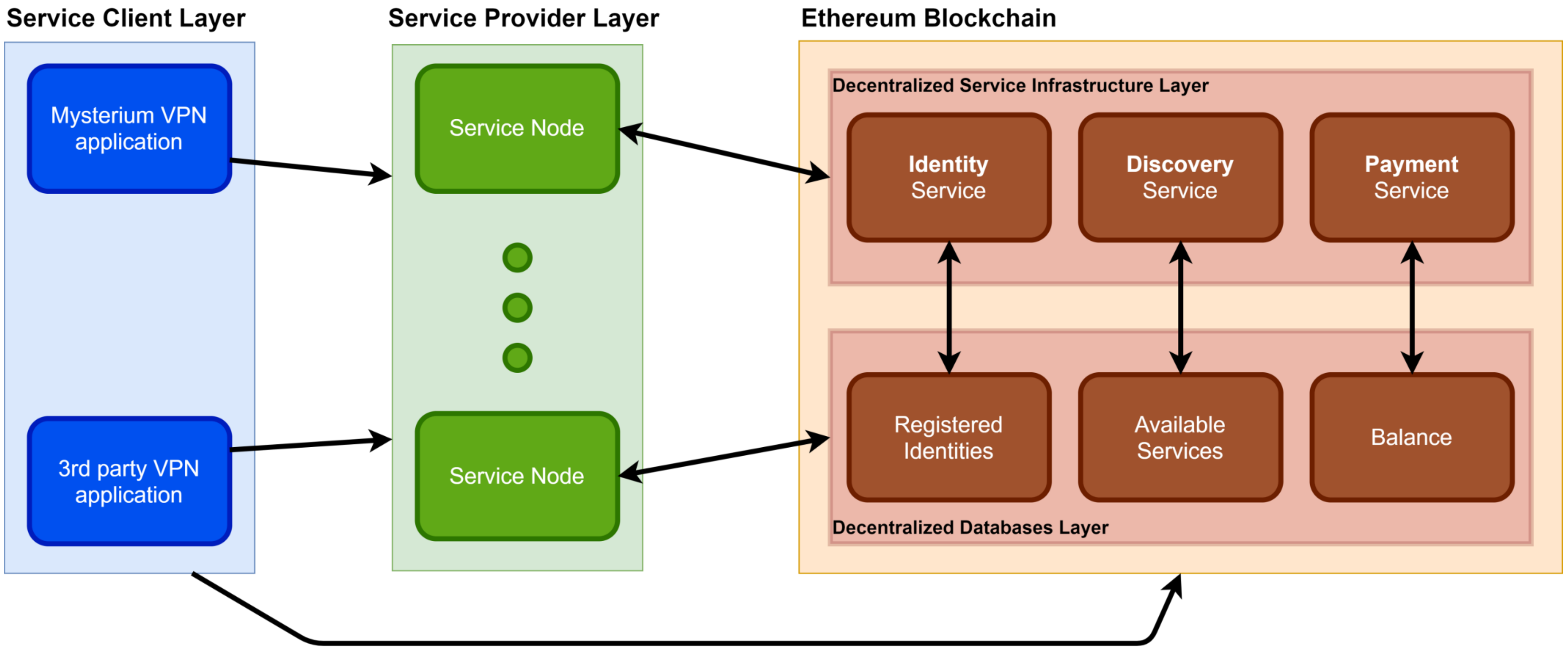
All the steps are based on the most advanced and complete decentralized vpn project: **Mysterium Network**

Decentralized VPN

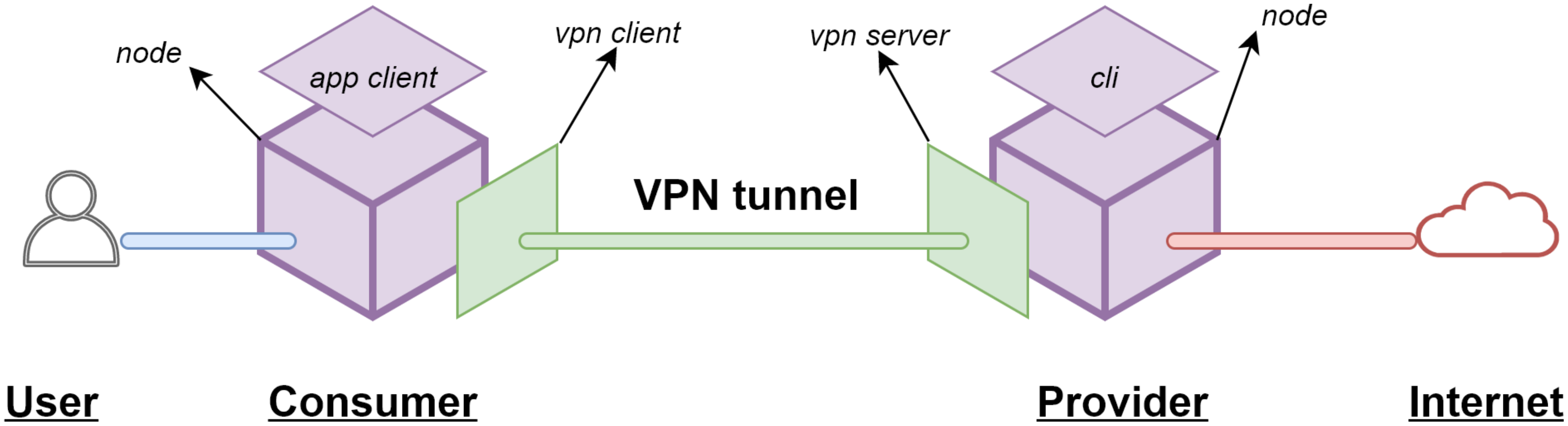




Mysterium Network: architecture



Mysterium Network: VPN connection



Mysterium Network: Vulnerabilities

User's questions

- Am I sure the content is original?
- Am I sure the content is private?
- Am I paying as much as I am using?

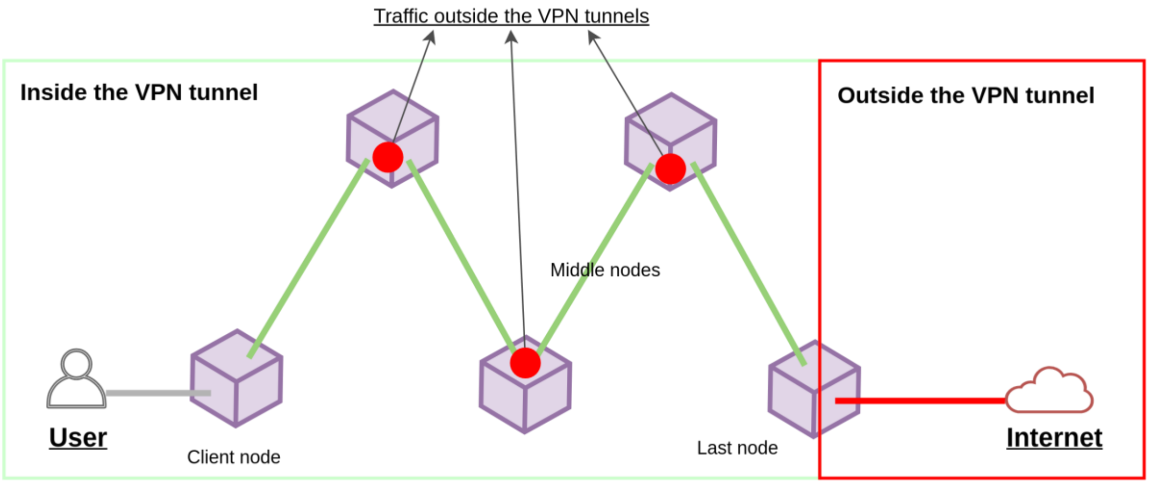
Mallory's questions:

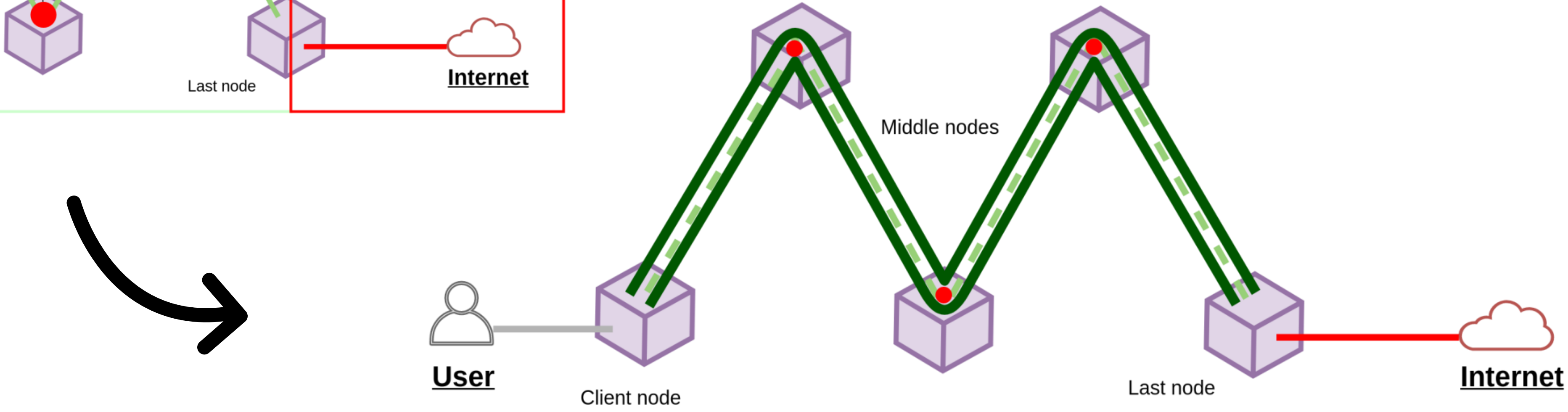
- How expensive is (time/money/reputation) being a bad guy?
- Can I create fake accounts leaving unpaid used connections as consumer
- Can I alter the traffic to get more money as provider

Mysterium Network Vulnerabilities: classification based on

1. the position in the network: starting, middle or end point
2. the step of the flow: the service proposals, the promise issuing, the transaction closing, and other steps
3. the operations on the passing data: sniffing, filtering or crafting the data
4. side channels attack and other particular scenarios

Mysterium Network Vulnerabilities: the position in the network



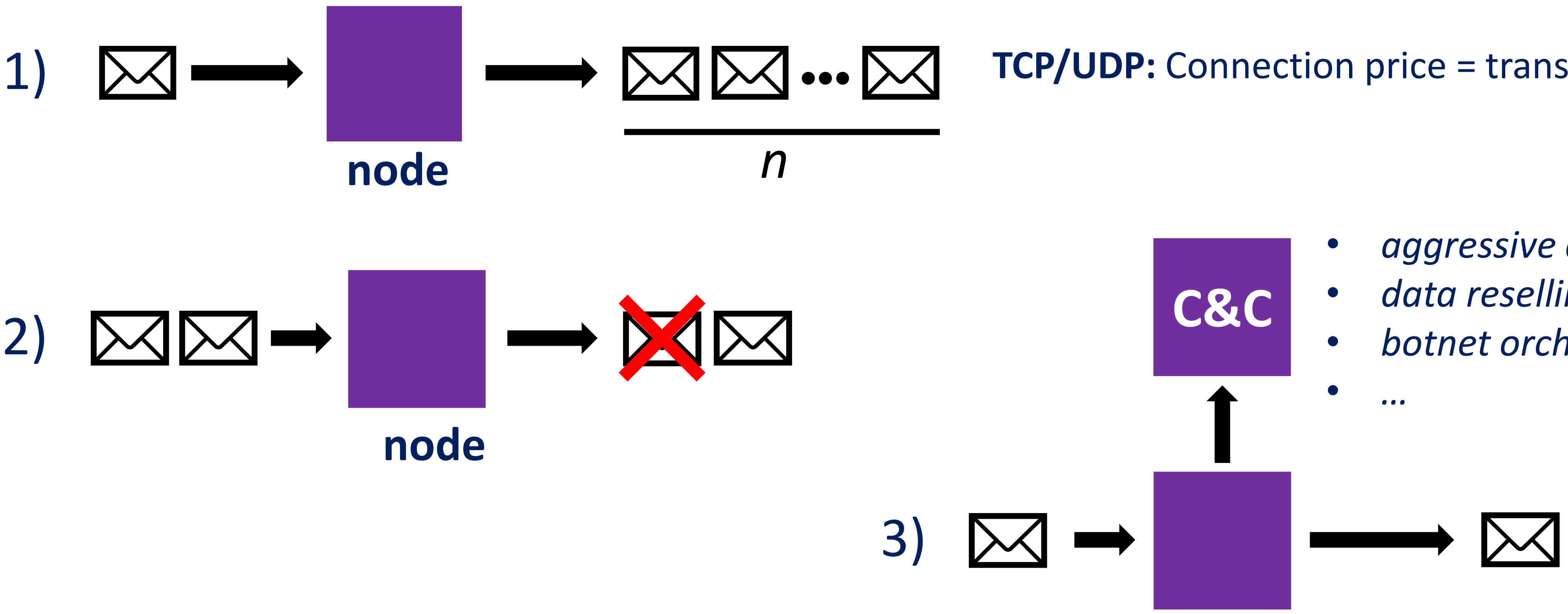


Mysterium Network Vulnerabilities:

- the step of the flow
- the operations on the passing data

Operations	Encrypted data	Not encrypted data
sniffing	No	Yes
filtering	Yes on protocol	Yes
crafting	Yes blind altering	Yes

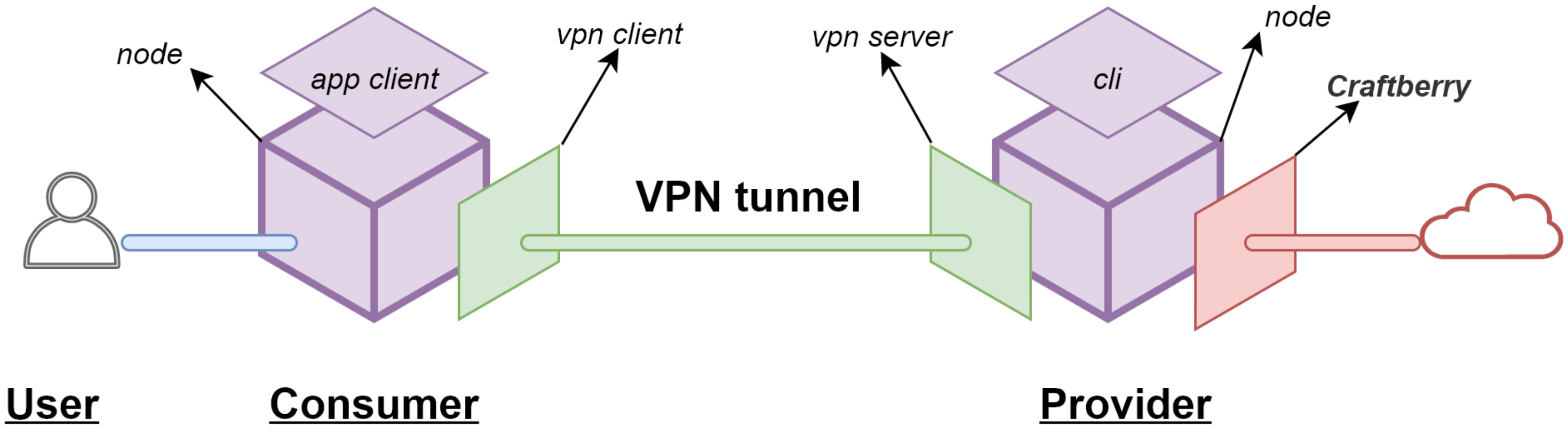
Mysterium Network Vulnerabilities: side channels attack and other particular scenarios



TCP/UDP: Connection price = transferred Bytes * *n*

- *aggressive ads*
- *data reselling*
- *botnet orchestator*
- …

CraftBerry: a proof of concept tool to demonstrate how a node can sniff, filter and craft the outgoing and incoming traffic from an exit node of the Mysterium Network



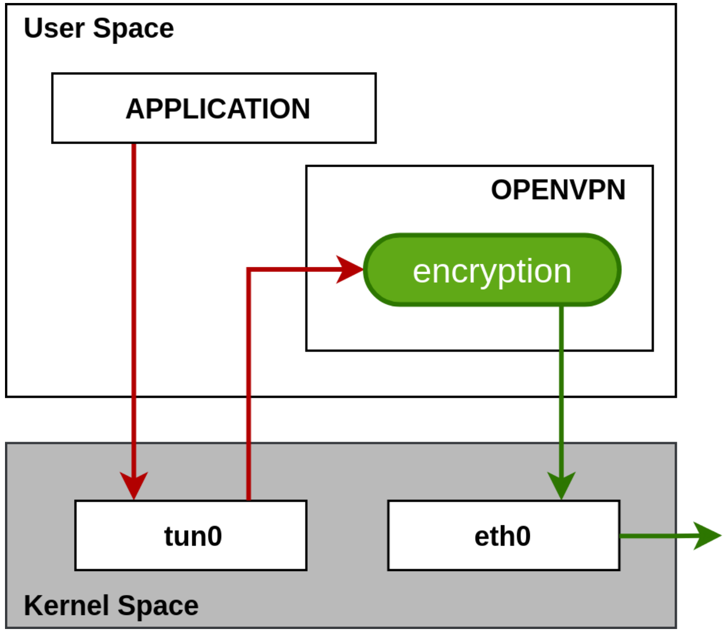
PcapPlusPlus

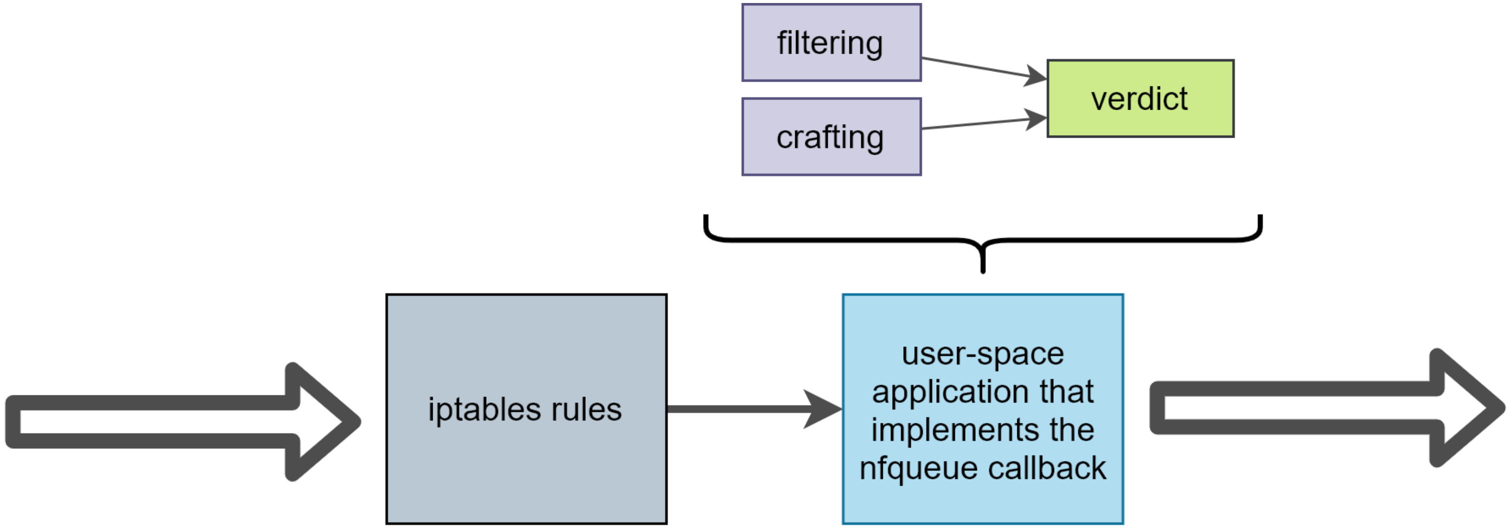
netfilter
firewalling, NAT, and packet mangling for linux

CraftBerry: how it works

Attack:
L3: IP, icmp
L4: TCP/UDP
L5: and above: HTTP, DNS, NTP

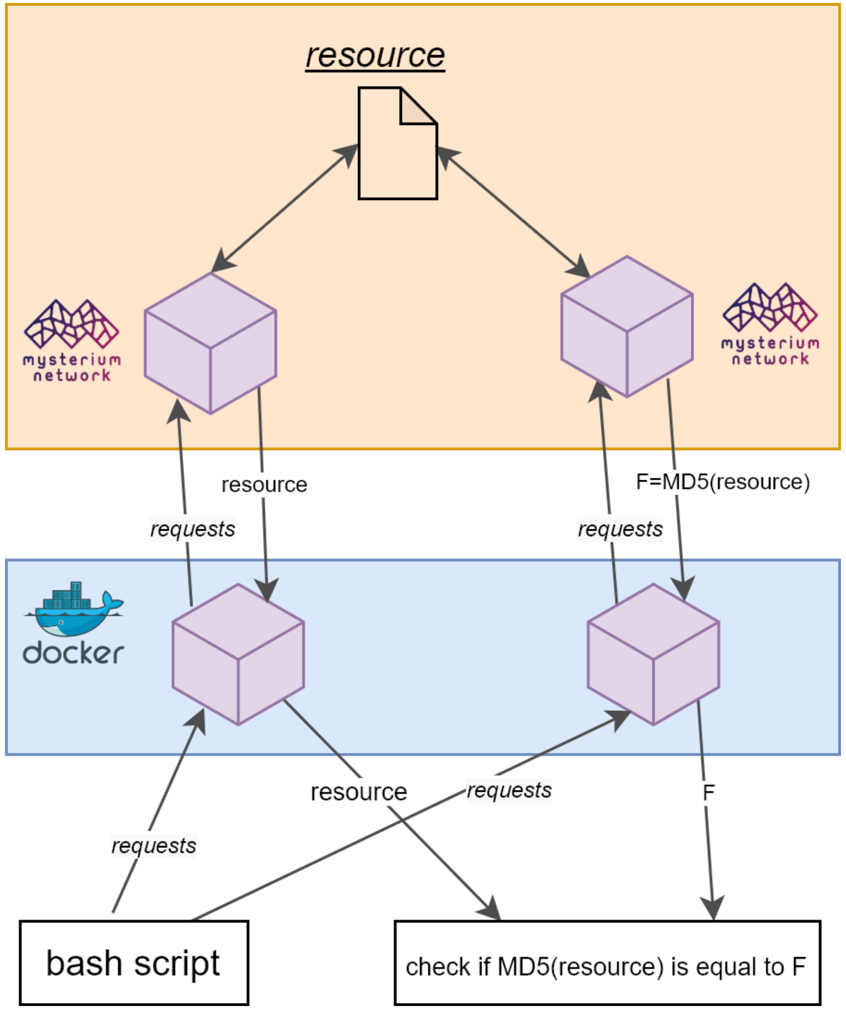
Defense:
L4: ChaCha20





Design solutions

- Decoy data
- Duplicated data
  - Data hashes



Thank you