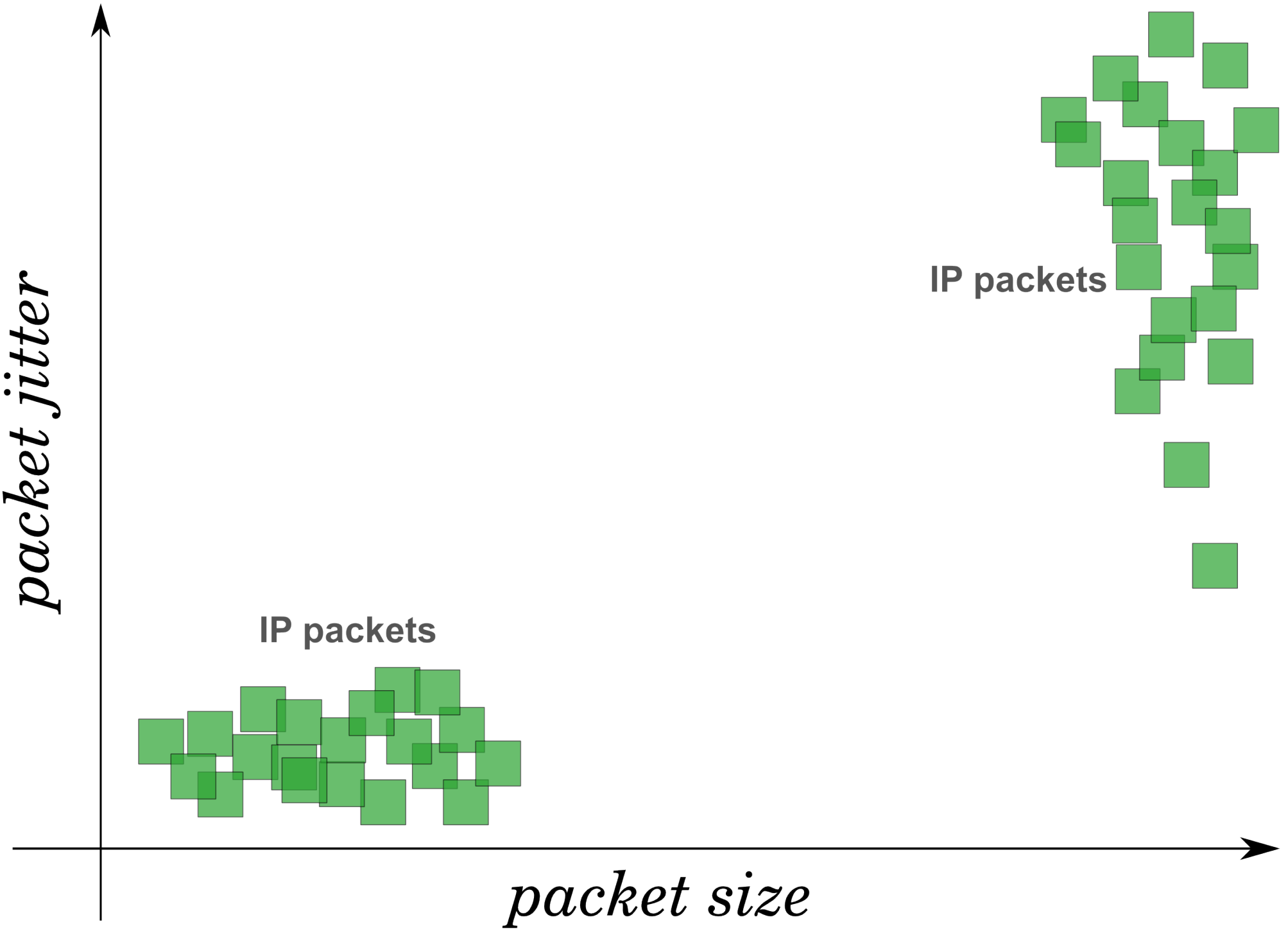
Statistical, real-time classification of IP traffic in Linux operating system

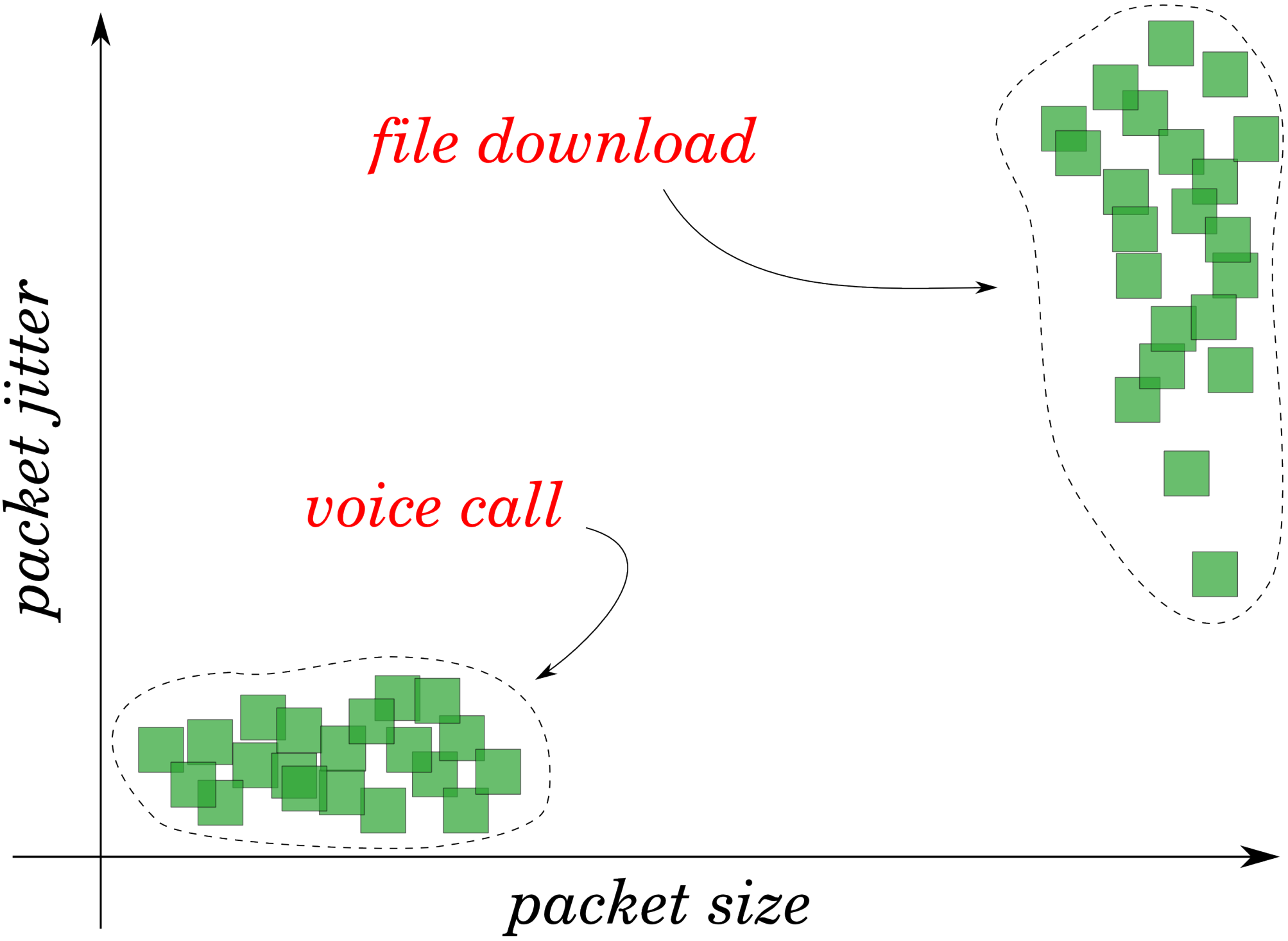
Paweł Foremski
Advisor: dr inż. Arkadiusz Biernacki

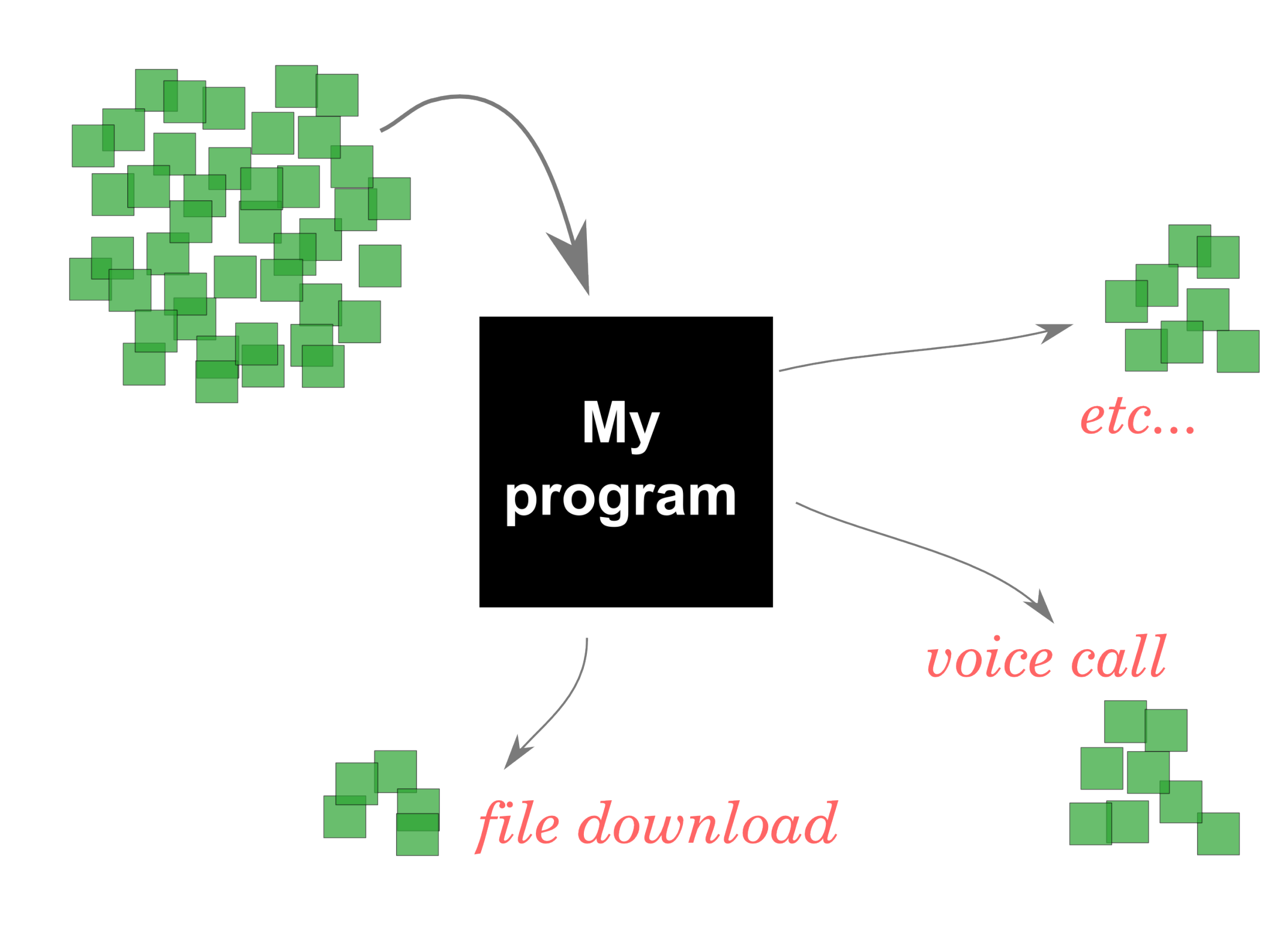
Agenda

- Short reminder
- Program architecture
- Technical summary and results
- Remaining work

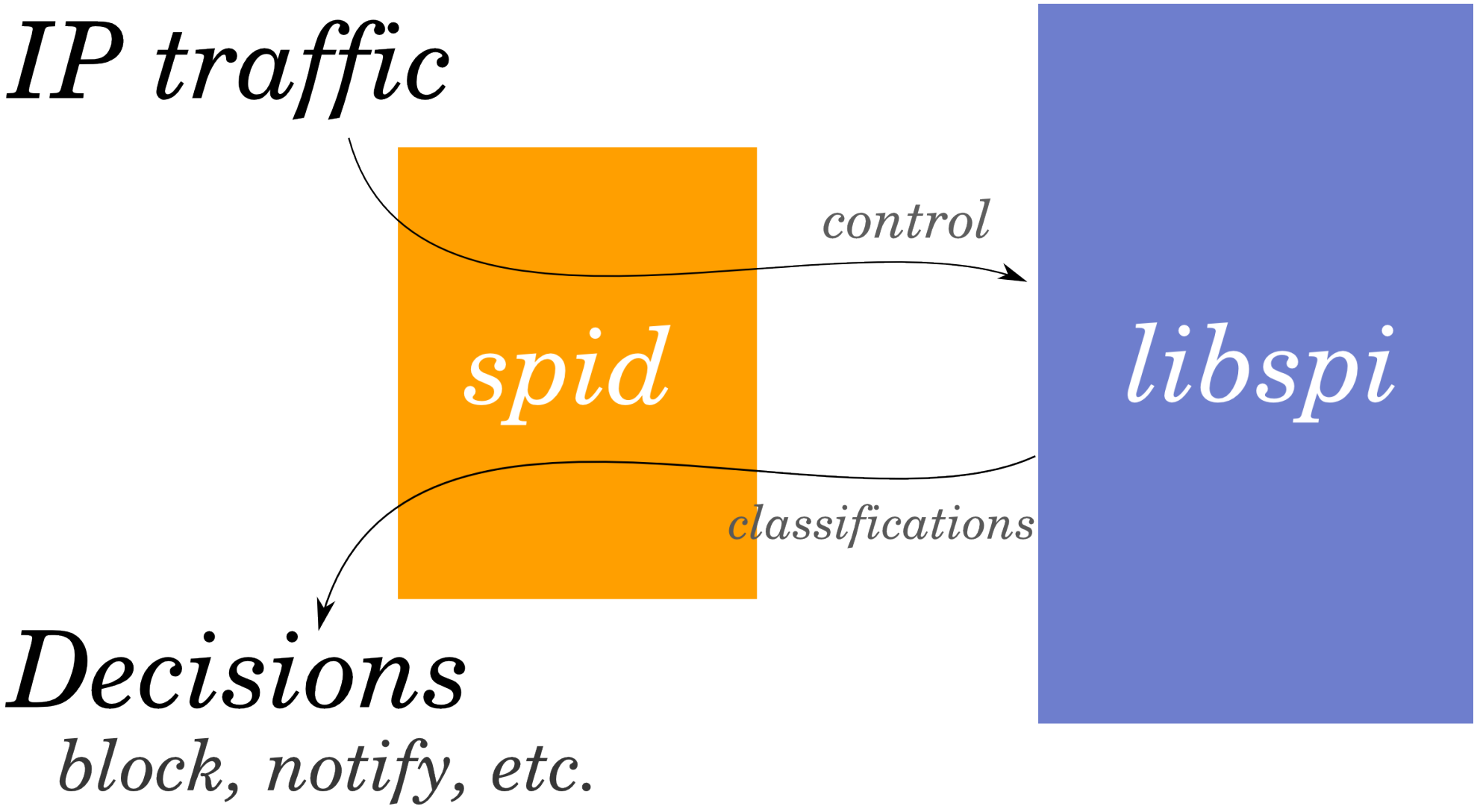
Reminder - IP traffic classification

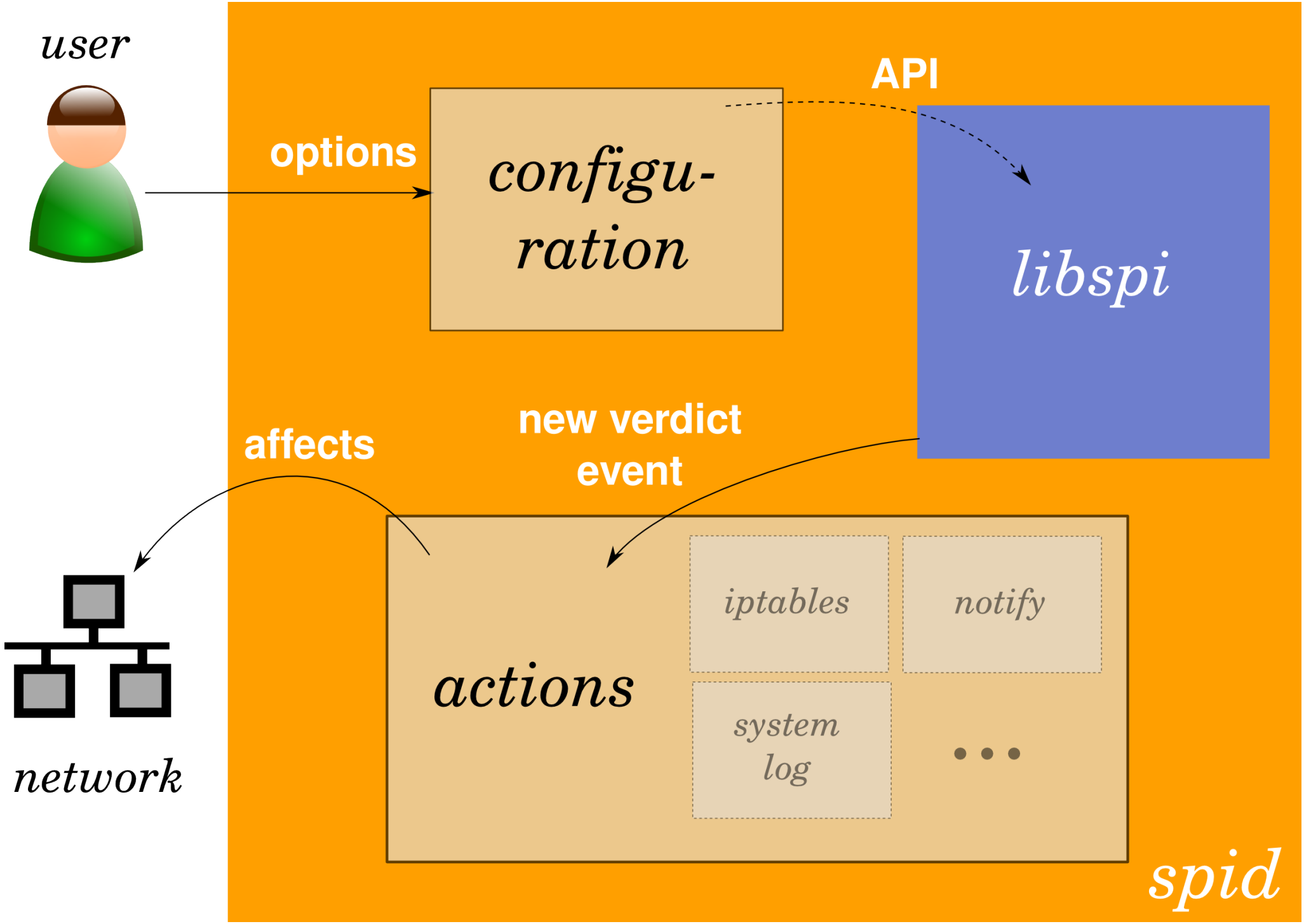

packet jitter
IP packets
IP packets
packet size

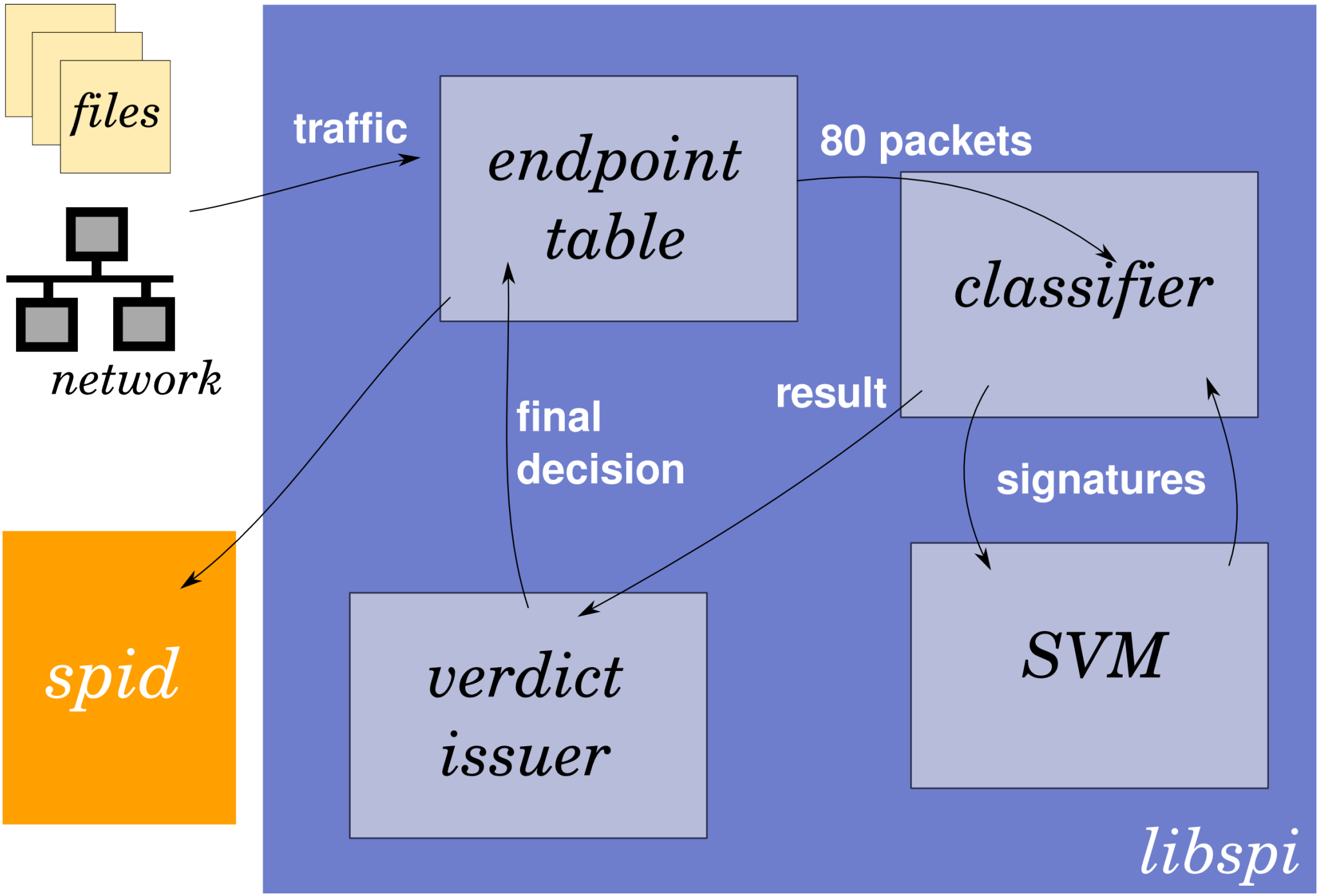

file download
voice call
packet jitter
packet size

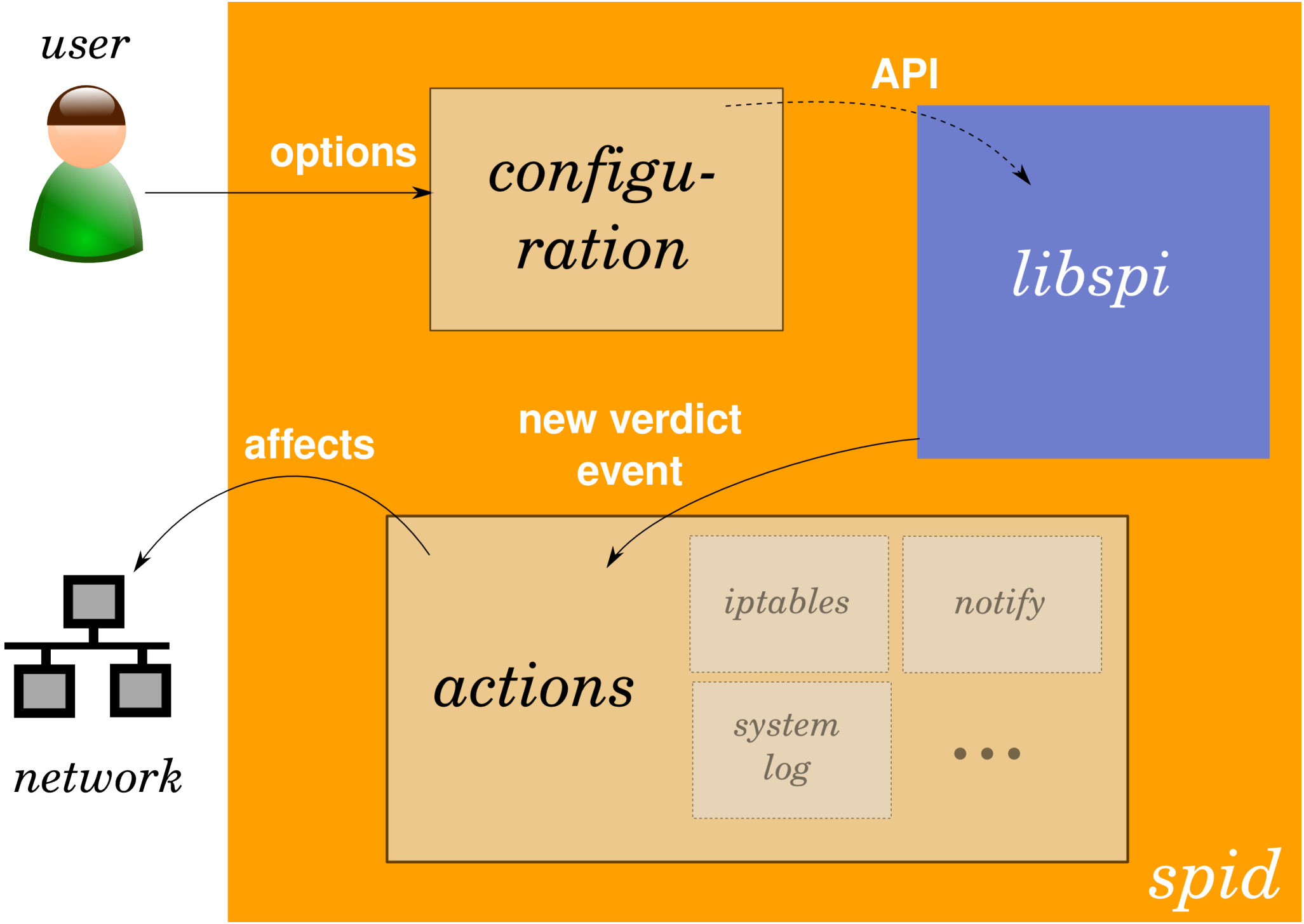

My program
etc...
voice call
file download

Program architecture


IP traffic
spid
control
libspi
classifications
Decisions
block, notify, etc.


user
API
options
configu-
ration
libspi
new verdict
event
affects
actions
iptables
notify
system
log
• • •
network
spid


files
network
spid
traffic
endpoint table
80 packets
classifier
result
final decision
signatures
verdict issuer
SVM
libspi

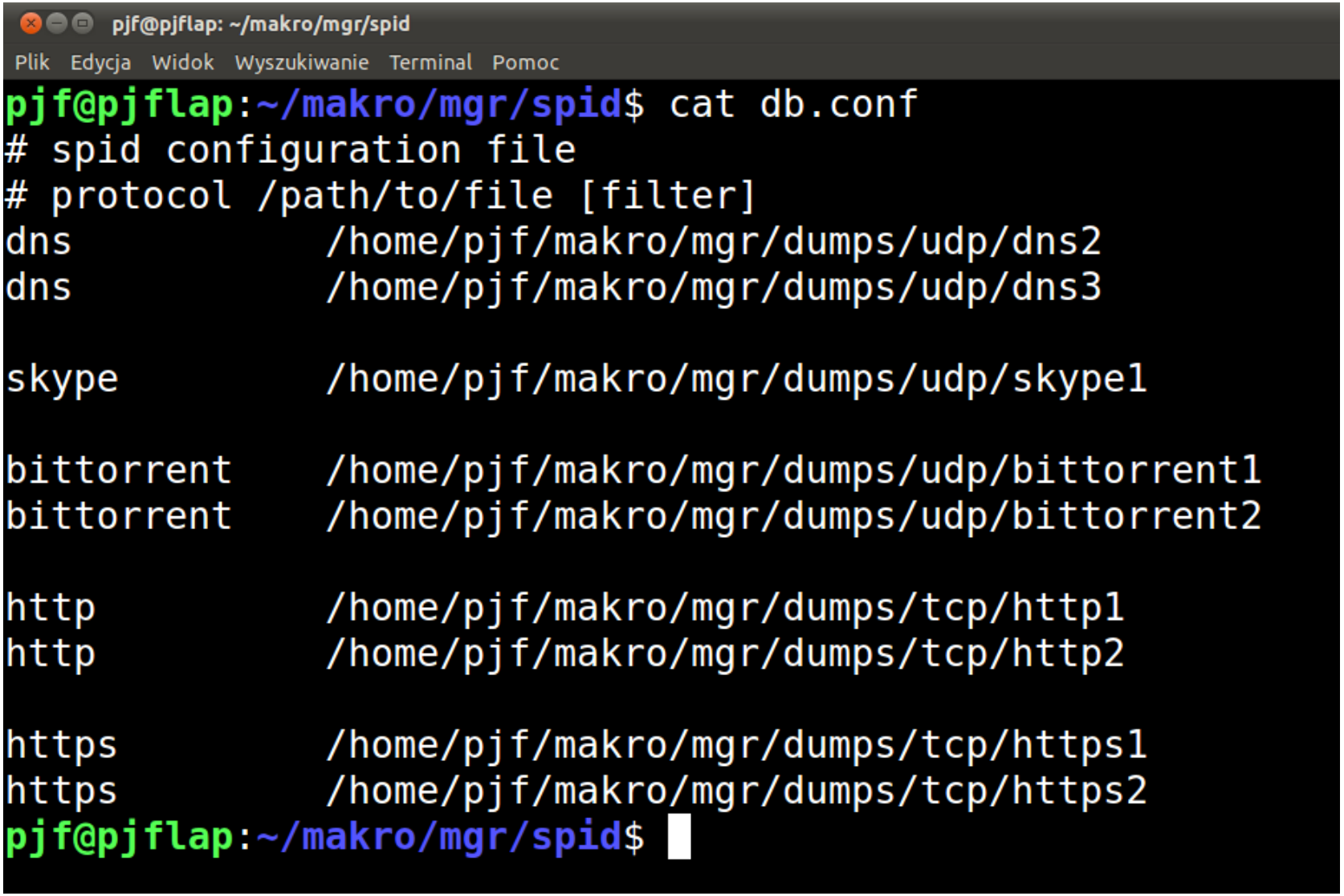

user
API
options
configu-
ration
libspi
new verdict
event
affects
actions
iptables
notify
system
log
• • •
network
spid

Technical summary and results

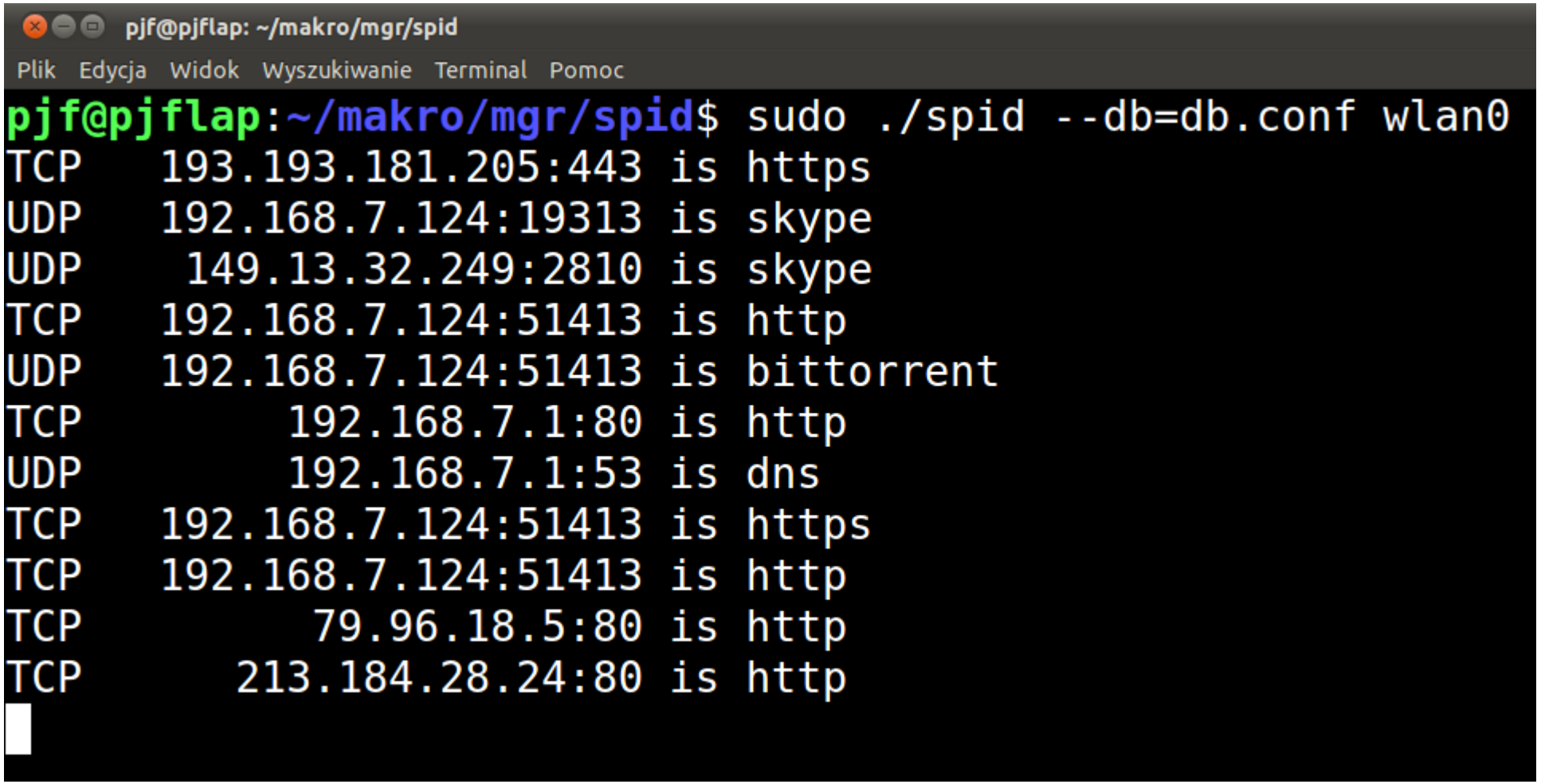
Technical summary

- C language, 2000 lines of code
- Single-threaded, event-driven
- Modular
  - libsvm, liblinear

Configuration file



Exemplary output



Results

- Learns ~100 000 packets / second
- Properly recognizes 5 protocols: HTTP, HTTPS, DNS, BitTorrent, Skype
- Event-driven control very fair

Remaining work

Remaining work

- SVM module
- Network actions
- System performance evaluation
- Linux netfilter integration
- The Thesis ;-)

Thank you.

Questions?