Packets to Privacy

Understanding Evolving Network Security

Max Hampshire

DevRel, Nym

Section 1

How Packets Move Through a Network

How packets move through a network

- Data is sent in packets
  - Chunks of data sent between networked devices
- Packets contain
  - Header:
    - protocol info
    - content info
    - origin IP
    - destination IP
  - Payload:
    - the actual data
  - (Sometimes) Tailers

Metadata (data about data) exposure:

- Origin & Destination ID
- IP address (location)
- Time (start, end, duration)
- Volume (amount of data sent in each direction)
- Packet exchange sequences
- Interpacket delays (sequence, dist.)
- Packet size (sequence, dist.)
- Amount of packets

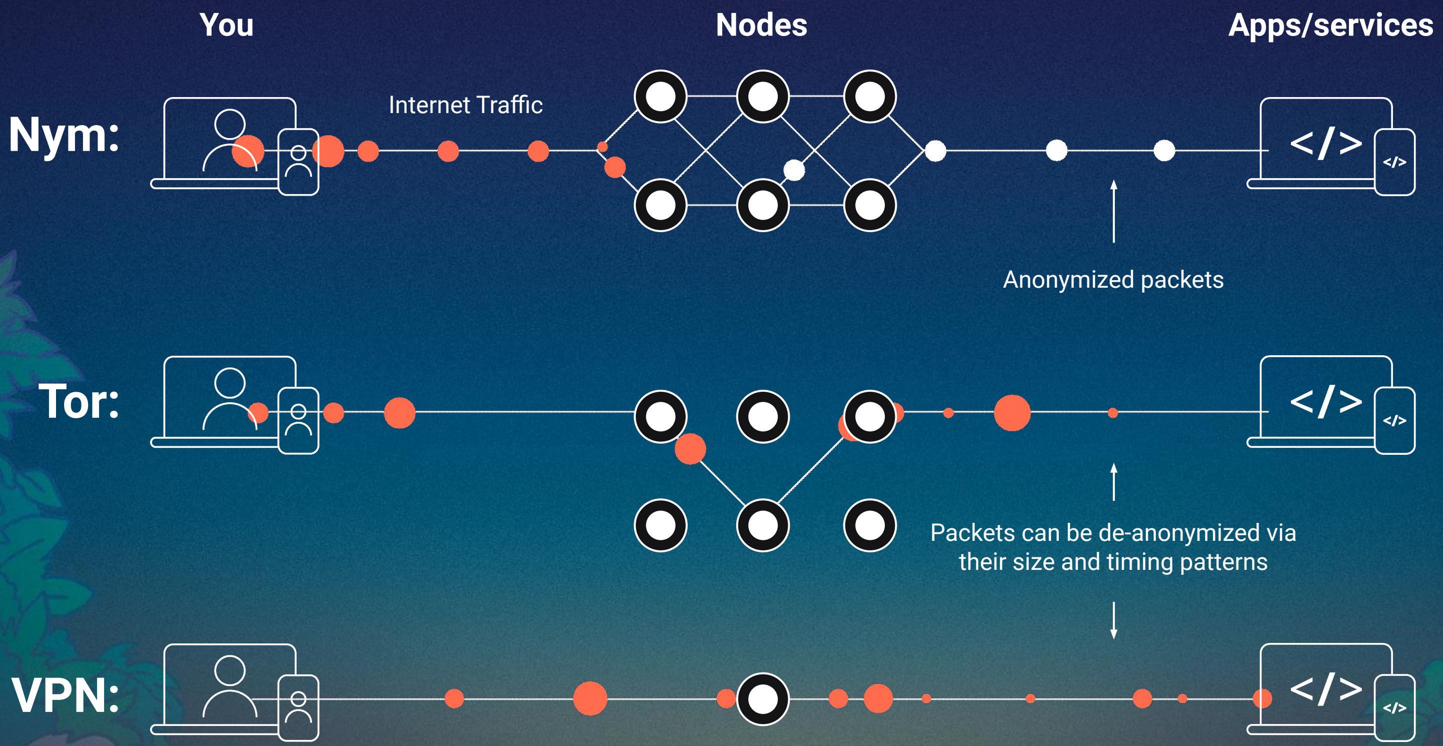
- Higher order patterns
  - Request-response (within a flow)
  - Traffic “signature”
  - Repeated communication patterns
  - Deviations from standard patterns
  - Clusters of entities
- Persistent identifiers
  - Account, nick, ID
  - Device ID
  - Email address
  - Cookies, fingerprints, locations

The internet was not created with network privacy in mind

- Network traffic is captured & analysed by governments and corporations en masse.
- Patterns are found via ML
  - Who is talking to who, and when
  - Where parties are located
  - What kind of traffic is being sent/received
- Inferences can be made from any patterns
  - Why is x talking to y?
  - What is the nature of their relationship?

Section 2

Mixnets Against Surveillance


You
Nodes
Apps/services
Nym:
Internet Traffic
</>
</>
Anonymized packets
Tor:
</>
</>
Packets can be de-anonymized via
their size and timing patterns
VPN:
</>
</>

Section 3

Zk-nyms: Anonymous Credentials for Payments

Non-anon Payments Are A Problem

The big problem: payment!

- Private crypto:
  - small anonymity set
  - Even Monero, Zcash, Railgun, etc susceptible to network deanonymisation
- Most people want to pay with fiat
- VPN providers can be subpoenaed

zk-nyms

Private unlinkable payments!

- Private transactions
  - Usage is cryptographically unlinkable via re-randomization.
- Selective disclosure
  - Prove identity or key possessions while preserving privacy with ZKPs of private attributes (i.e. KYC, payments in any token, unlinkable pseudonyms).
- Decentralised
  - No centralised third party is required to issue credentials, uses threshold signatures by a majority of validators.
- Coconut + Offline Ecash schemes

Section 4

NymVPN

NymVPN

An app built on top of the Nym Network for network traffic protection

- Private payments
  - Even if you pay with fiat, your usage is unlinkable to your payment methods
- Anonymous mode (5 hop mixnet)
  - Use the Mixnet for all device traffic
- Speedy mode (2 hop)
  - Wireguard tunnel-in-a-tunnel for network protection and speed

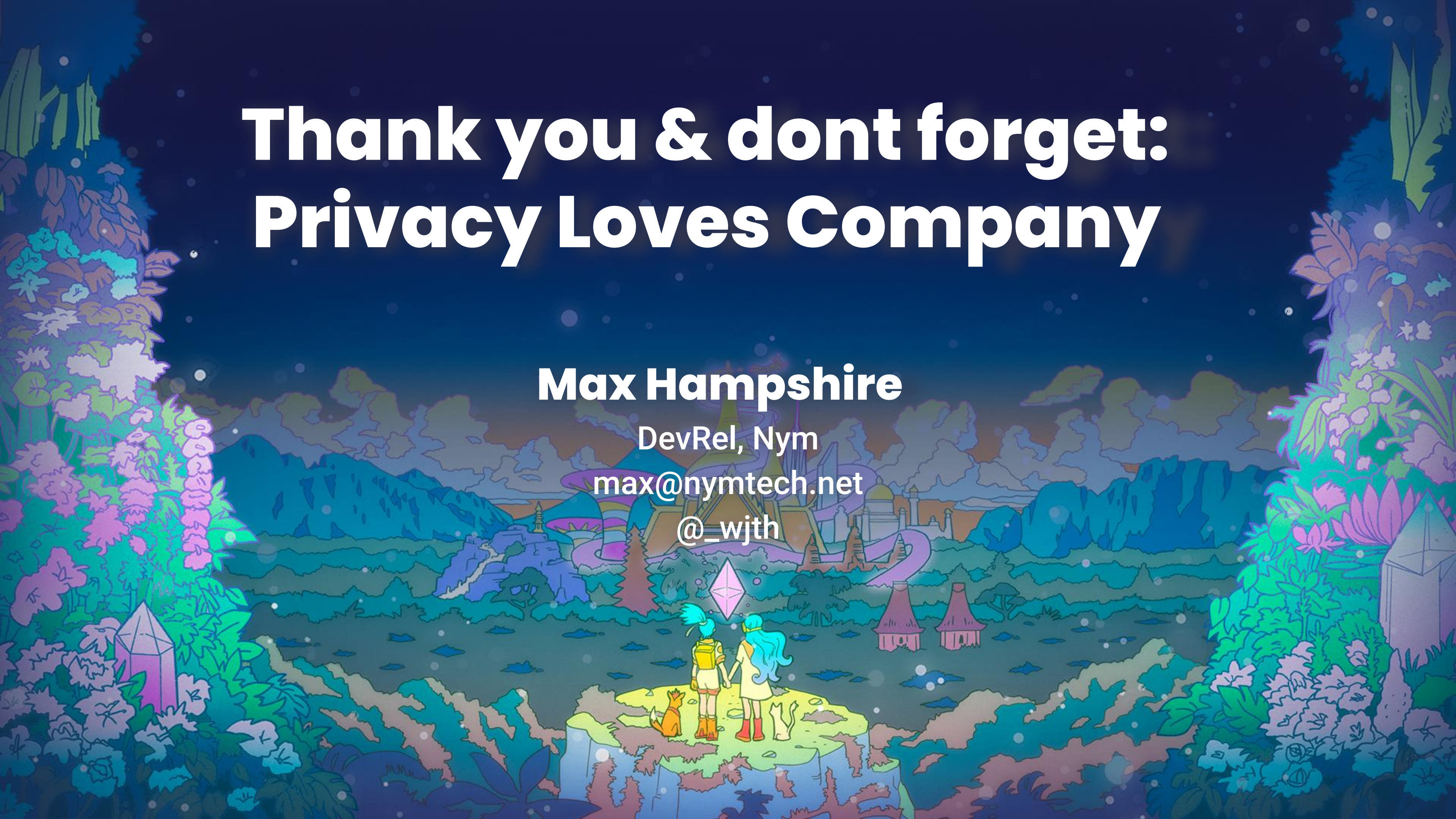
NymVPN Open Beta:

nymvpn.com/download

Builder Docs:

nymtech.net/docs/developers

Thank you & dont forget: Privacy Loves Company



Max Hampshire

DevRel, Nym

max@nymtech.net

@_wjth