
August 15–16
2015
I2P
GETI2P.NET
HackLab
1266 Queen Street West,
Toronto, Ontario
Canada
In Partnership
with:
Toronto Crypto for
helping orgainze this
event
Hacklab for providing
us with a great space

What's the buzz about HORNET?

HACK LAB .TO

to crypto

You've probably all seen the news…

- "Internet-scale anonymity"
- "Without sacrificing security, the network supports data transfer speeds of up to 93GBps"
- "can be scaled at little cost"
- "a better, faster Tor"

HACK LAB .TO

tor crypto

You've probably not read the abstract...

"We present HORNET, a system that enables high-speed end-to-end anonymous channels by leveraging next generation network architectures. HORNET is designed as a low-latency onion routing system that operates at the network layer thus enabling a wide rangeof applications. Our system uses only symmetric cryptography for data forwarding yet requires no per-flow state on intermediate nodes. This design enables HORNET nodes to process anonymous traffic at over 93 Gb/s. HORNET can also scale as required, adding minimal processing overhead per additional anonymous channel. We discuss design and implementation details, as well as a performance and security evaluation."

HACK LAB .TO

to crypto

HORNET: High-speed Onion Routing at the Network Layer

- Low-latency onion routing network
  - Leverages the existing Sphinx onion routing protocol
- Geared towards speed and scalability
  - Use next-gen network gear instead of building an overlay

HACK LAB .TO

to crypto

Desired properties

- Path information integrity and security
  - e.g. no tagging attacks
- No cross-link identification
- Session unlinkability
- Payload secrecy and end-to-end integrity
  - Adversary can only learn packet length and timing

HACK LAB .TO

to crypto

Claims

- Better speed than existing onion routing networks
  - Tor, I2P
- Better security than existing (proposed) network layer anonymity networks
  - LAP, Dovetail

HACK LAB .TO

to crypto

Speed

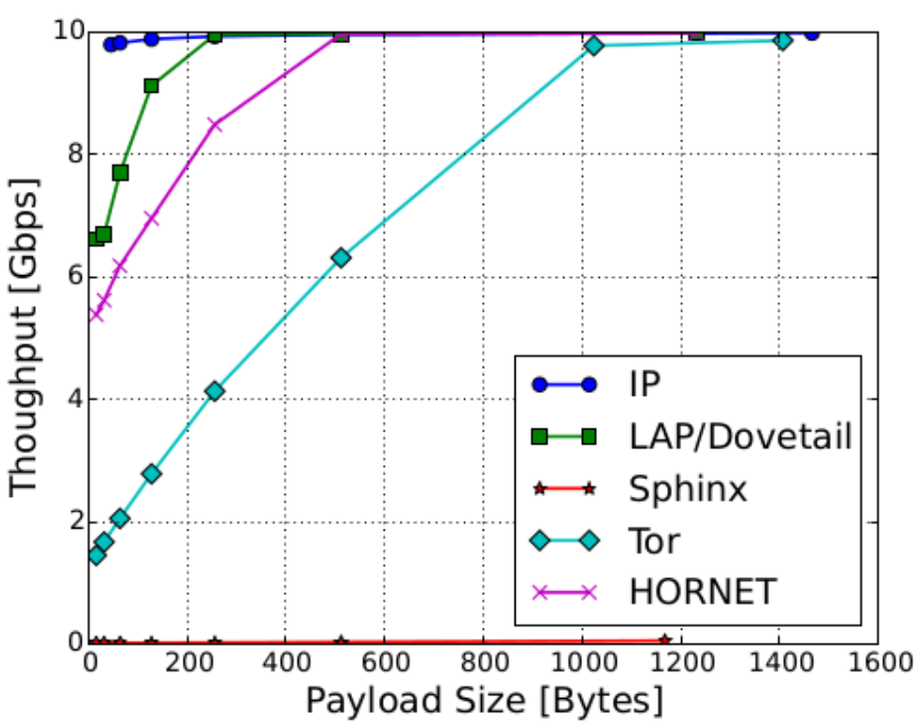
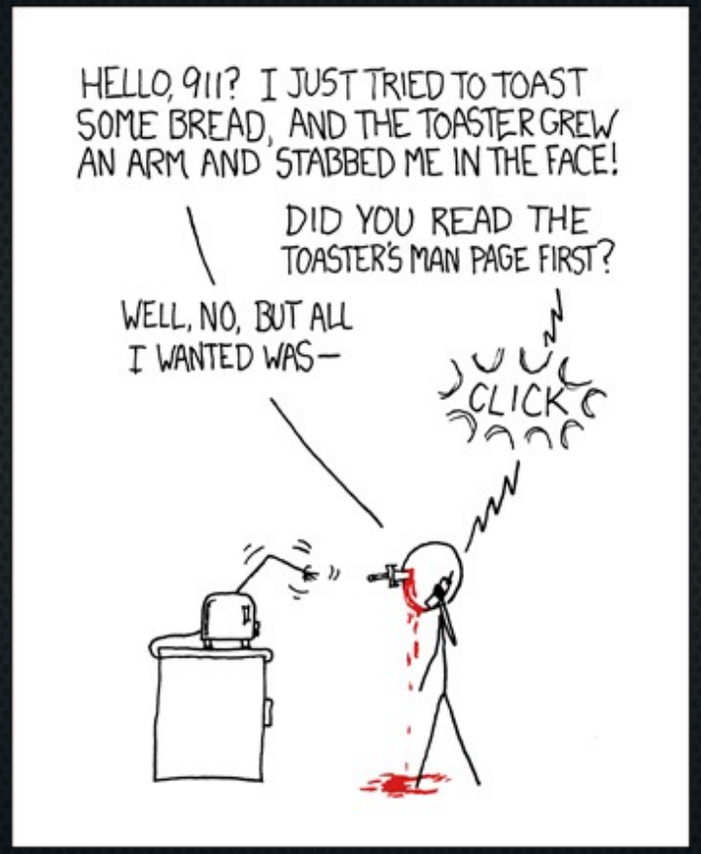


Figure 4: Data forwarding throughput on 10 Gb/s link

HACK LAB .TO

to crypto

Security



HACK LAB .TO

to crypto

Why is it fast?

HACK LAB .TO

to crypto

Stateless data transmission

HORNET Session Setup Packet

type	hops	EXP
Sphinx Header		
Sphinx Payload		
FS Payload		

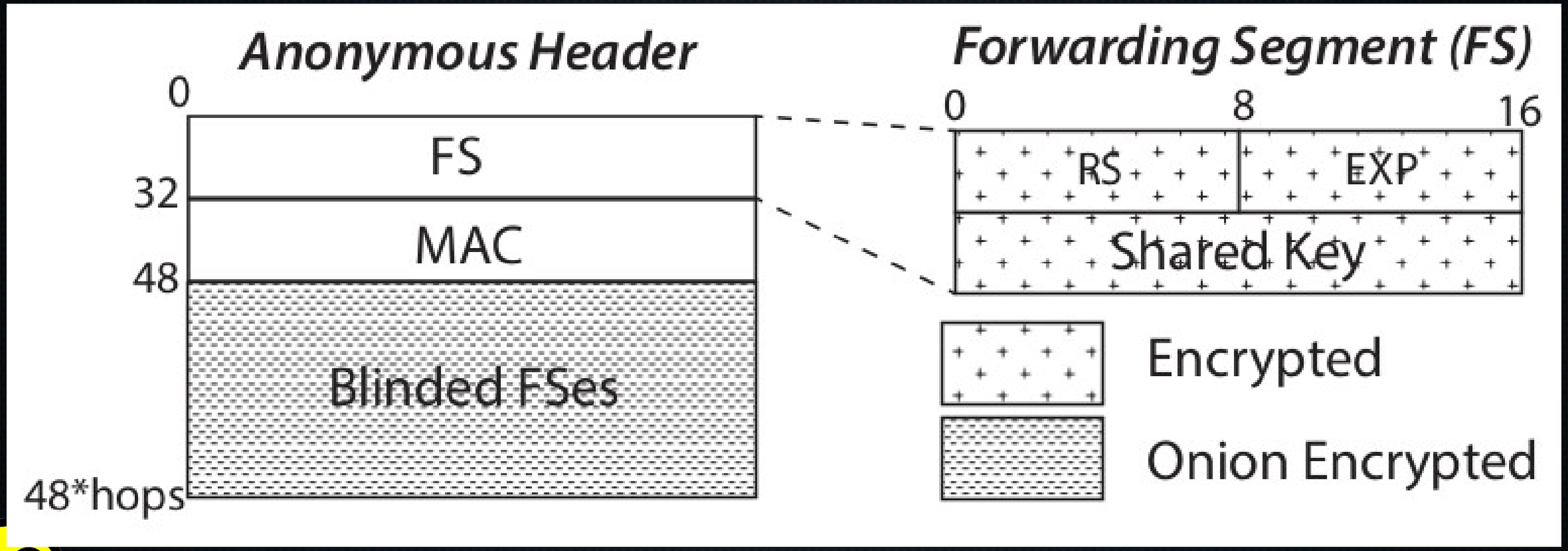
HORNET Data Packet

type	hops	nonce
AHDR		
Data Payload		

HACK LAB .TO

to crypto

Stateless data transmission



HACK LAB .TO

to crypto

Data packet header lengths

Scheme	Header Length	Sample Length (Bytes)
LAP	$12 + 2s.r$	236
Dovetail	$12 + s.r$	124
Sphinx	$32 + (2r + 2)s$	296
Tor	$3 + 11.r$	80
I2P	20	20
HORNET	$8 + 3r.s$	344

s = length of symmetric element
r = maximum AS path length

For sample length, *s* = 16 Bytes and *r* = 7

Gains

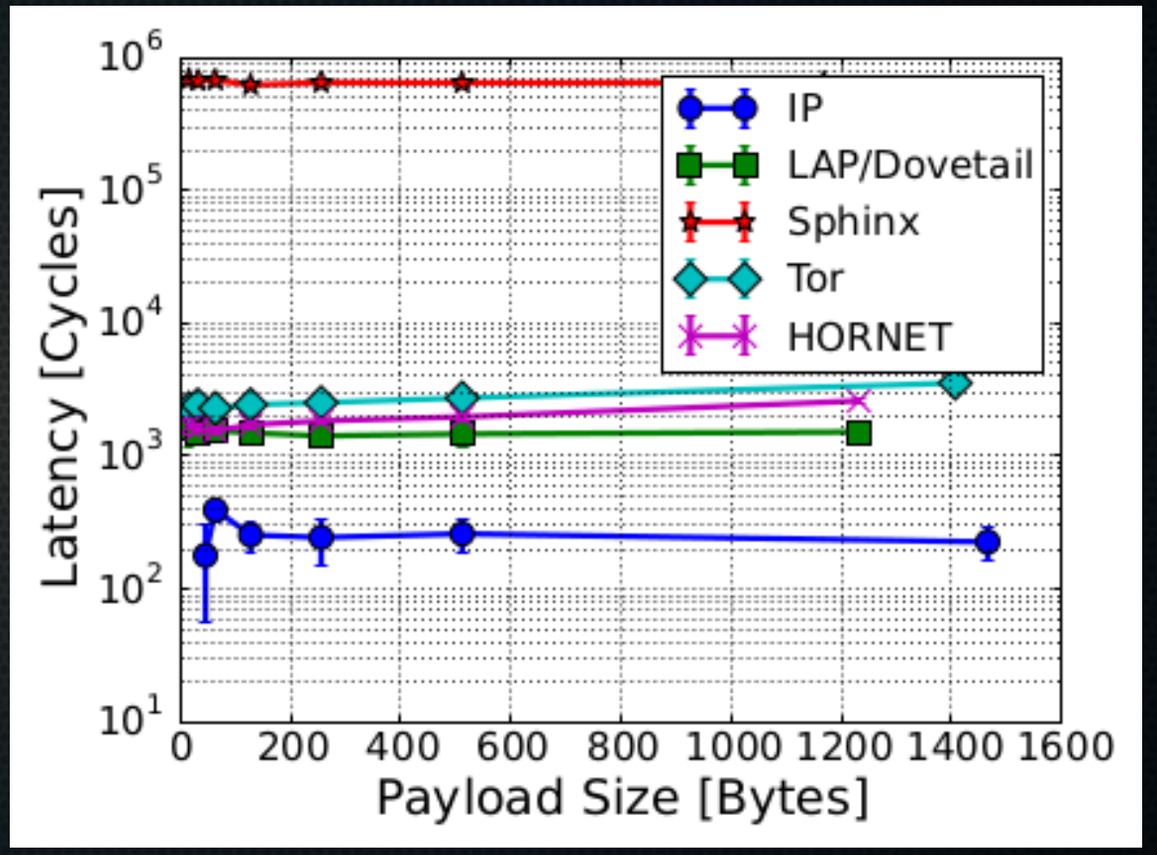
- No route lookup time
- No route storage
  - Tor stores at least 376 bytes per circuit
    - Requires almost 20GB of memory for a load level of 5 million new sessions per minute

HACK LAB .TO

to crypto

Mostly symmetric crypto

- Each HORNET node performs one DH key exchange during setup phase
- Only symmetric operations used during data phase
  - 5% slower than LAP and Dovetail for small packets (64 bytes)
  - 71% slower for large packets (1200 bytes)



HACK LAB .TO

to crypto

How?

- Decrypts setup packet
  - Sym key from medium/long-term DH priv key and sender's DH pub key
- Generate transient DH key
- Calculate a symmetric key from transient DH priv key and sender's DH pub key
- Encrypt routing info with local medium-term symmetric key
- Forward encrypted routing info + transient DH pub key
- Delete transient DH key

No replay protection

- Packet replay is ignored within the lifetime of a session
  - Leads to easy DoS
- They suggest that adversaries would be deterred by the risk of being detected by volunteers / organizations / ASs
  - but the detection process is going to add additional processing time and therefore compromise throughput

HACK LAB .TO

to crypto

So is this the end of Tor and I2P?

Why not?

- Designed for new routing hardware that doesn't exist
- Only covers session setup and data transmission
  - Assumes routing state only shows next hop
  - Assumes the presence of path discovery
  - Assumes the presence of node discovery
- Can be used with upper-layer anonymity protocols for stronger security guarantees

HACK LAB .TO

to crypto

It's actually very similar to I2P tunnels!

- Both use "non-interactive" telescopic tunnel building
- Both only use symmetric crypto for data transmission
  - Don't confuse I2P tunnels with I2P sessions
    - (But I2P sessions also use mostly-symmetric crypto via "session tags"…)
      - ((Yes, yes, this gets confusing...))

Key difference between HORNET and I2P

- I2P tunnel packet headers are smaller than HORNET
  - But I2P pads all to 1024 bytes
- I2P stores routing data
- I2P uses a bloom filter to detect packet replay
- I2P has a higher-level end-to-end crypto layer

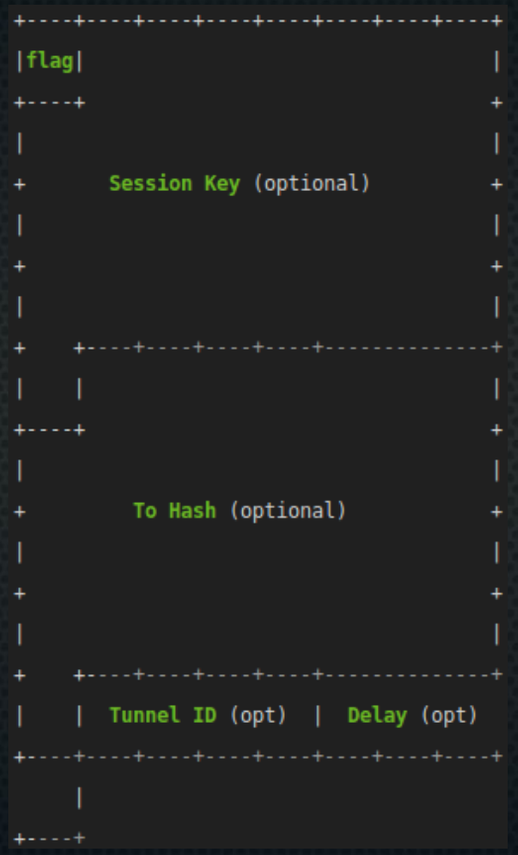
HACK LAB .TO

to crypto

Key points

- It doesn't actually exist
  - You can't throw away Tor and I2P just yet ;)
- It's only one piece of the puzzle
- Speed has trade-offs
- It's still a good idea!

Fun aside (if we get time): Implementing HORNET in I2P



HACK LAB .TO

to crypto

Discussion time :)

HACK LAB .TO

to crypto