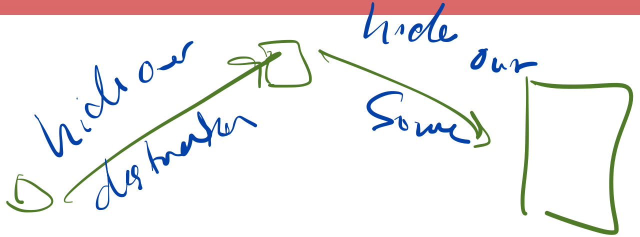
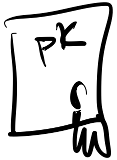
CS558 Network Security

Lecture 17: Tor pt3: Directories and Hidden Services

BOSTON UNIVERSITY

Review: Building a Tor Circuit



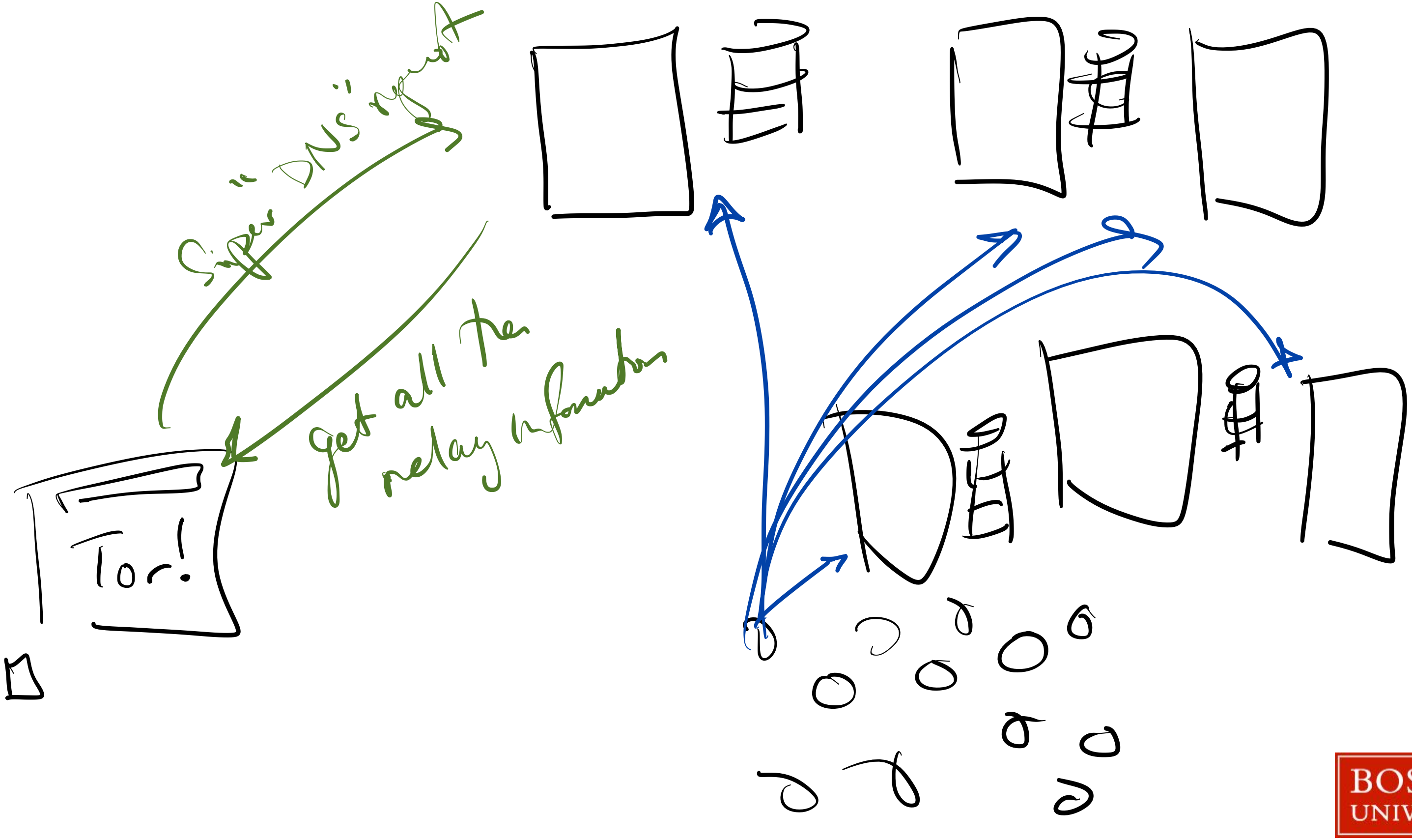


$$\underbrace{\begin{array}{c}\xrightarrow{\text{Enc}_{pk_g}(g^a)} \\ \xleftarrow{g^b,\, H(g^{ab})}\end{array}}_{K_1}$$

$$\text{Enc}_{K_1}(\text{Enc}_{K_2}(\text{Enc}_{K_3}(\text{Begin})))$$

$$\underbrace{\begin{array}{cc}\xrightarrow{\text{Enc}(\text{Enc}_{pk_m}(g^{a'}))} & \xrightarrow{\text{Enc}_{pk_m}(g^{a'})} \\ \xleftarrow{\text{Enc}(g^{b'},\, H(g^{a'b'}))} & \xleftarrow{g^{b'},\, H(g^{a'b'})}\end{array}}_{K_2}$$

Directory Services



Tor hidden Service

Basic Tor: Client anonymity from the Server

Hidden Services: Client anonymous to Server

Server anonymous to Client

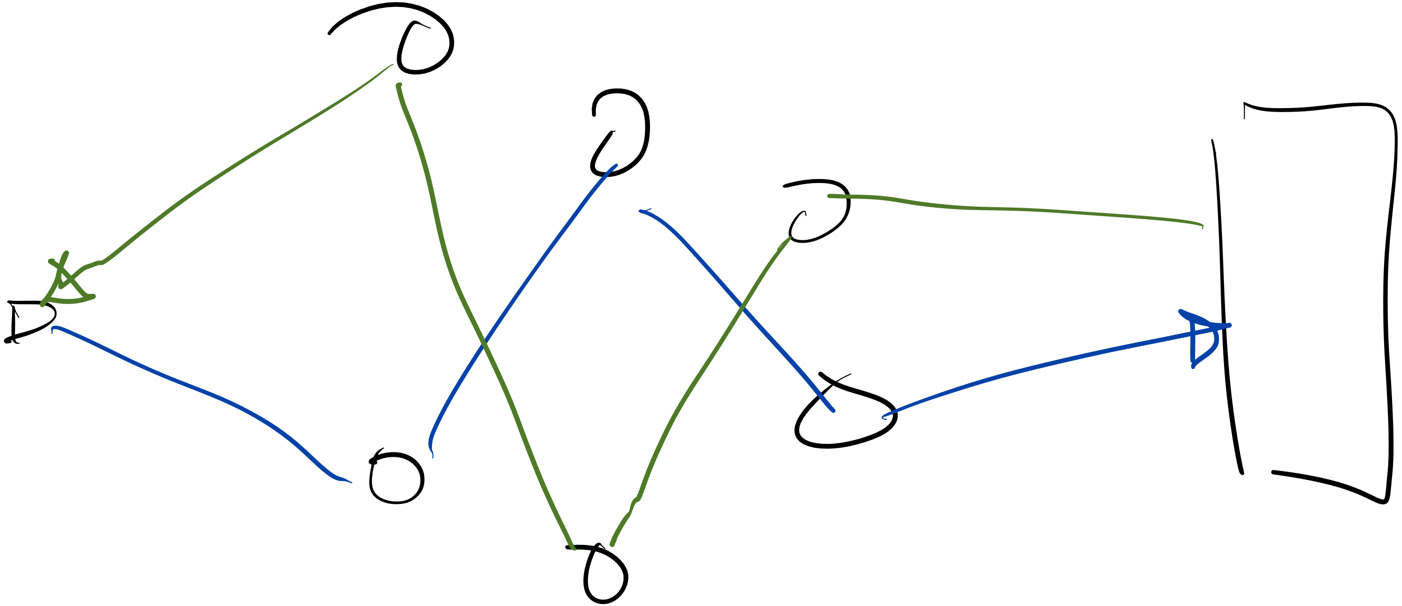
Tor -- Hidden Services

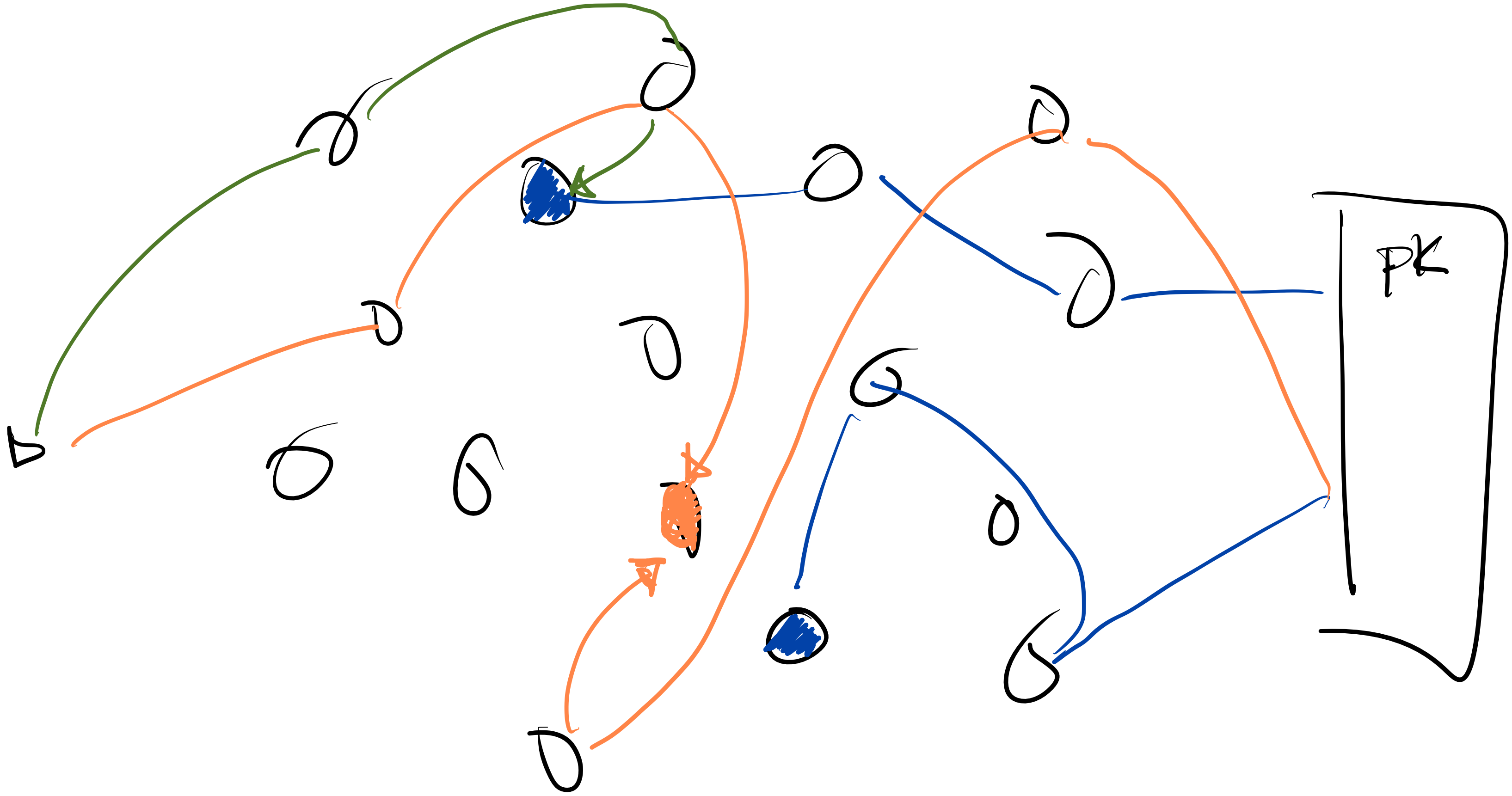
- DDos Protection

- Anonymity of the Server

- No ICANN integration

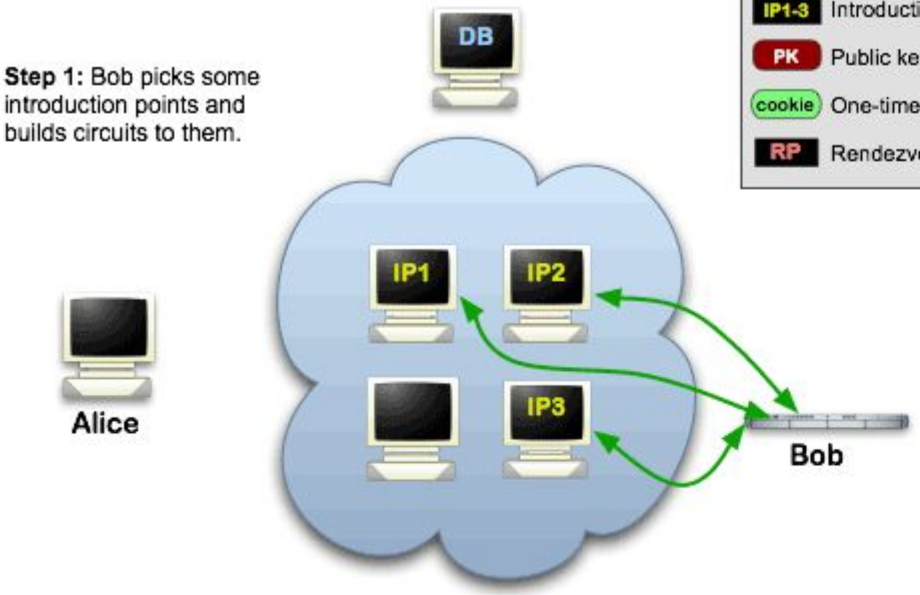
Tor -- Hidden Services




PK

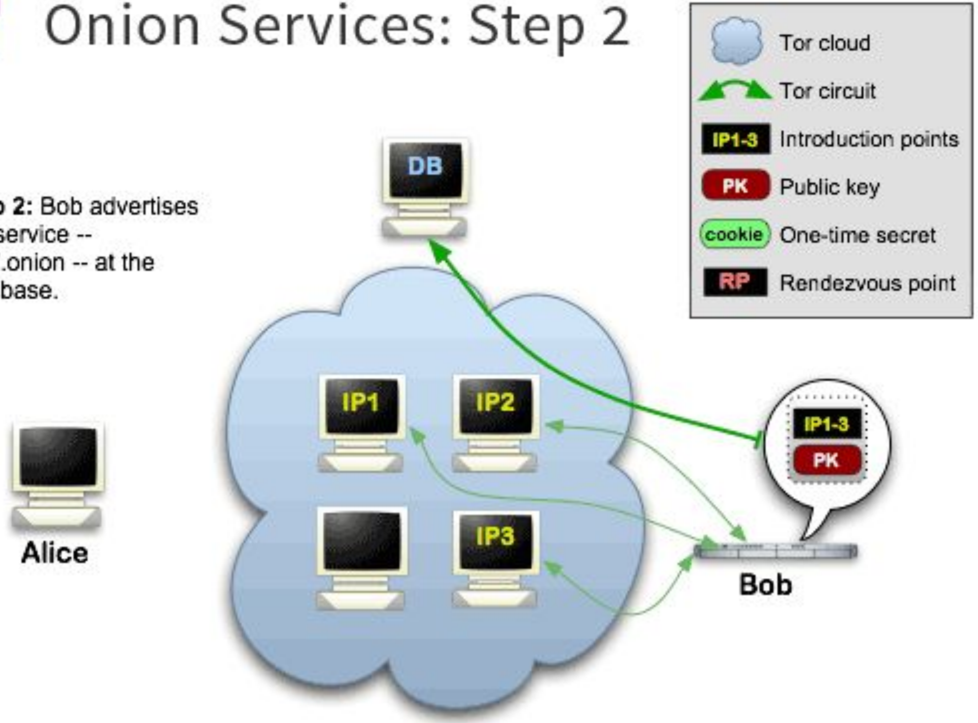
Tor Onion Services: Step 1

☁	Tor cloud
↔	Tor circuit
IP1-3	Introduction points
PK	Public key
cookie	One-time secret
RP	Rendezvous point



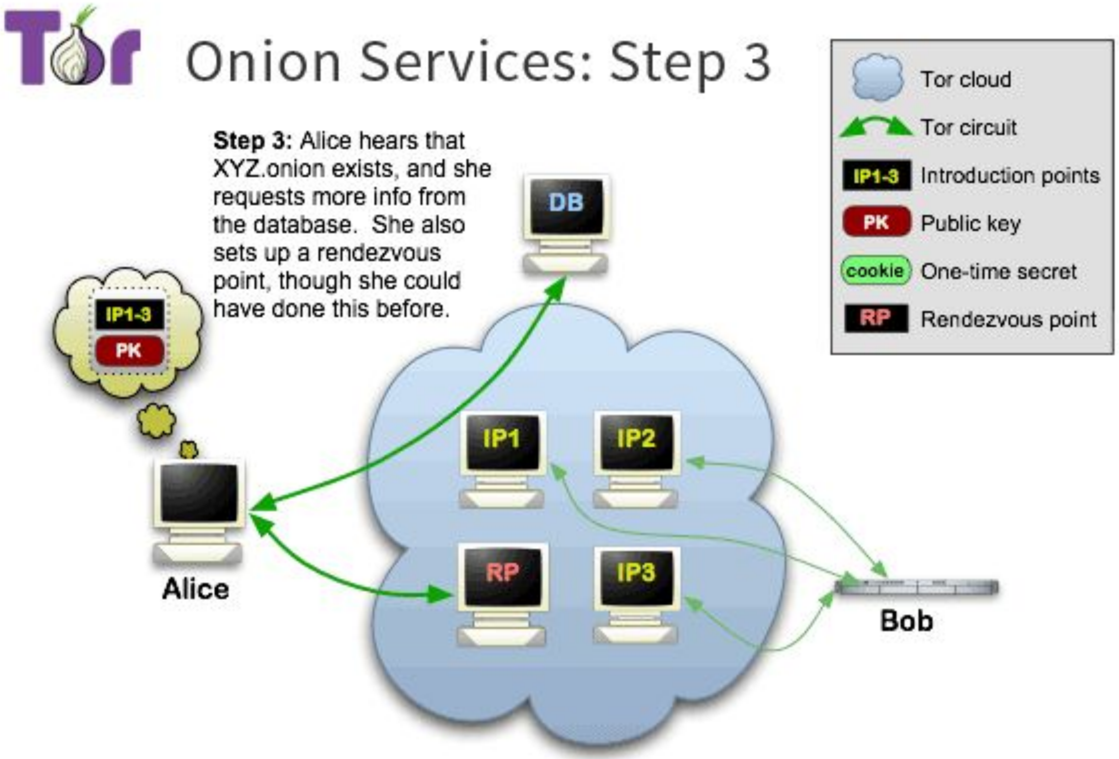
Step 1: Bob picks some introduction points and builds circuits to them.

Tor Onion Services: Step 2

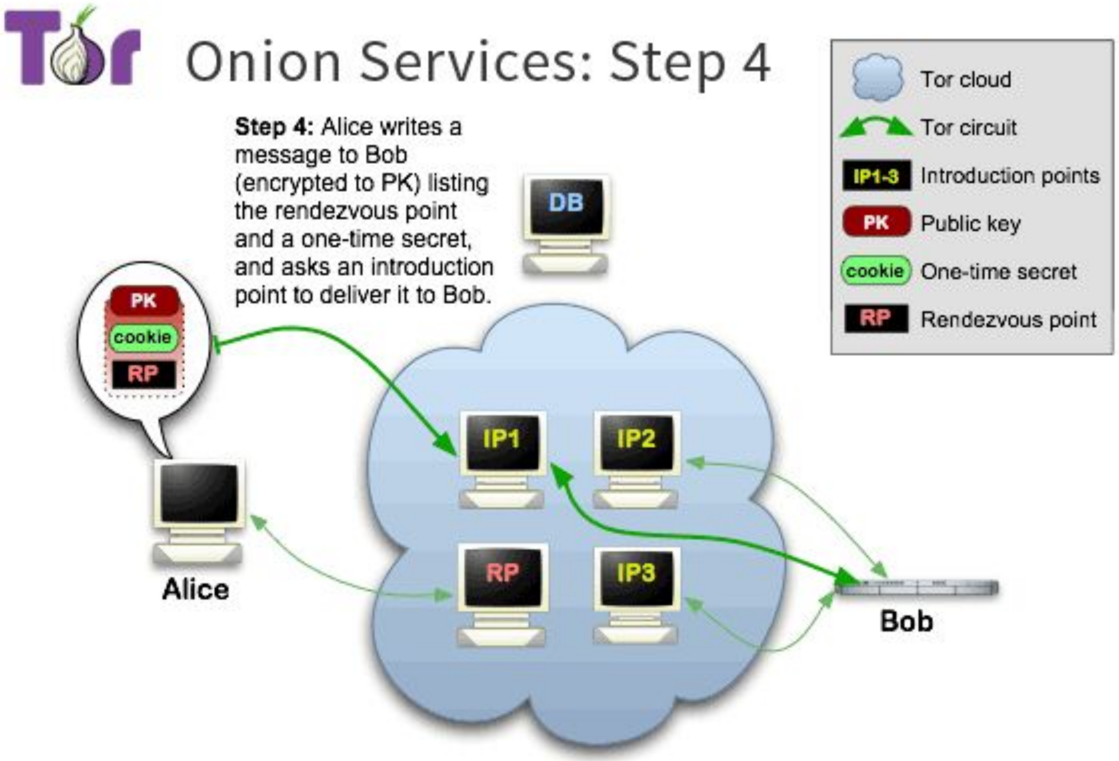


Step 2: Bob advertises his service -- XYZ.onion -- at the database.

Onion Services: Step 3



Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

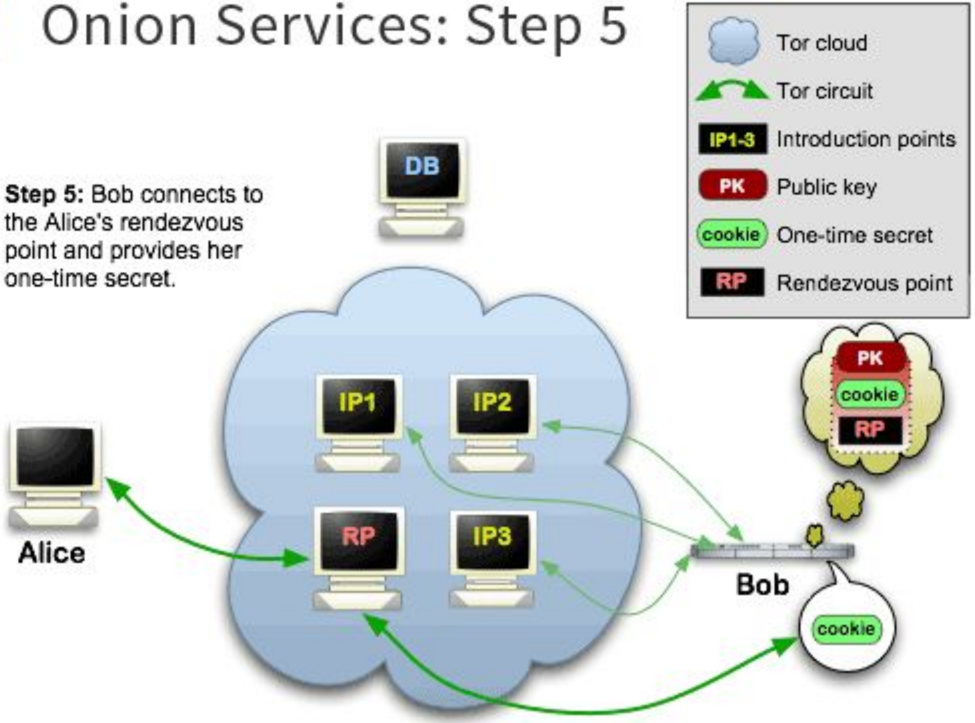


Onion Services: Step 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

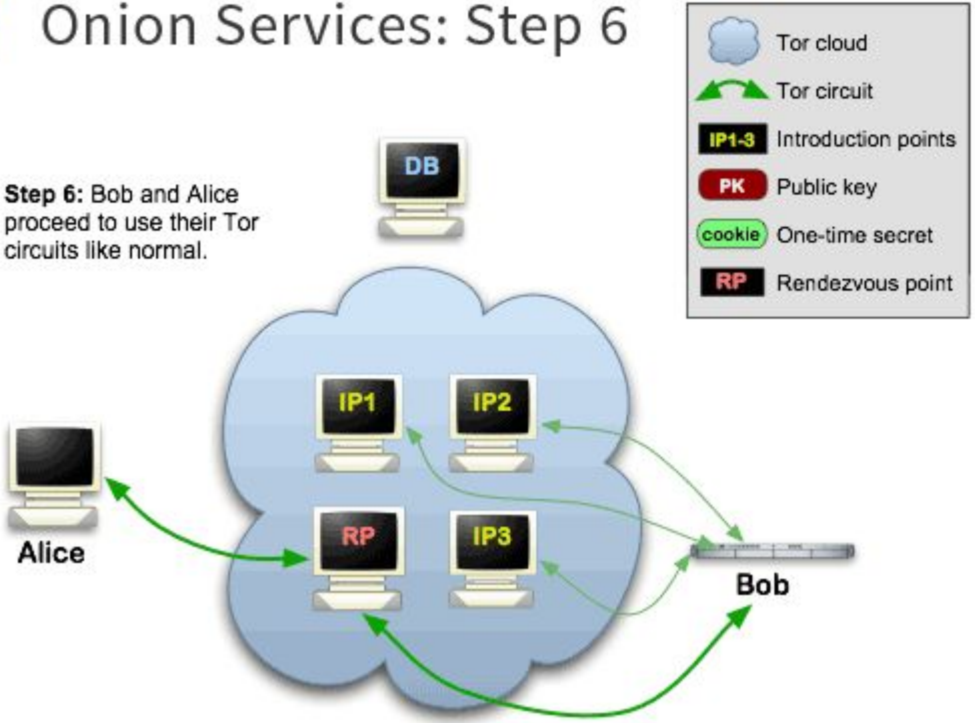
☁	Tor cloud
↔	Tor circuit
IP1-3	Introduction points
PK	Public key
cookie	One-time secret
RP	Rendezvous point

Onion Services: Step 5

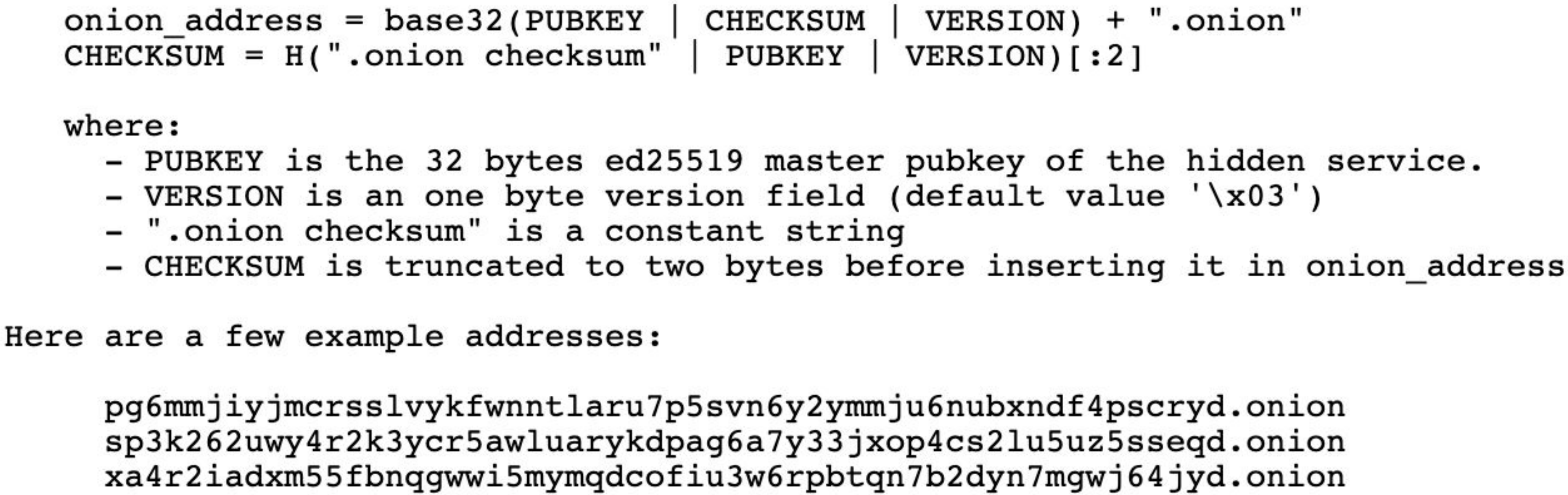


Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.

Onion Services: Step 6



Step 6: Bob and Alice proceed to use their Tor circuits like normal.

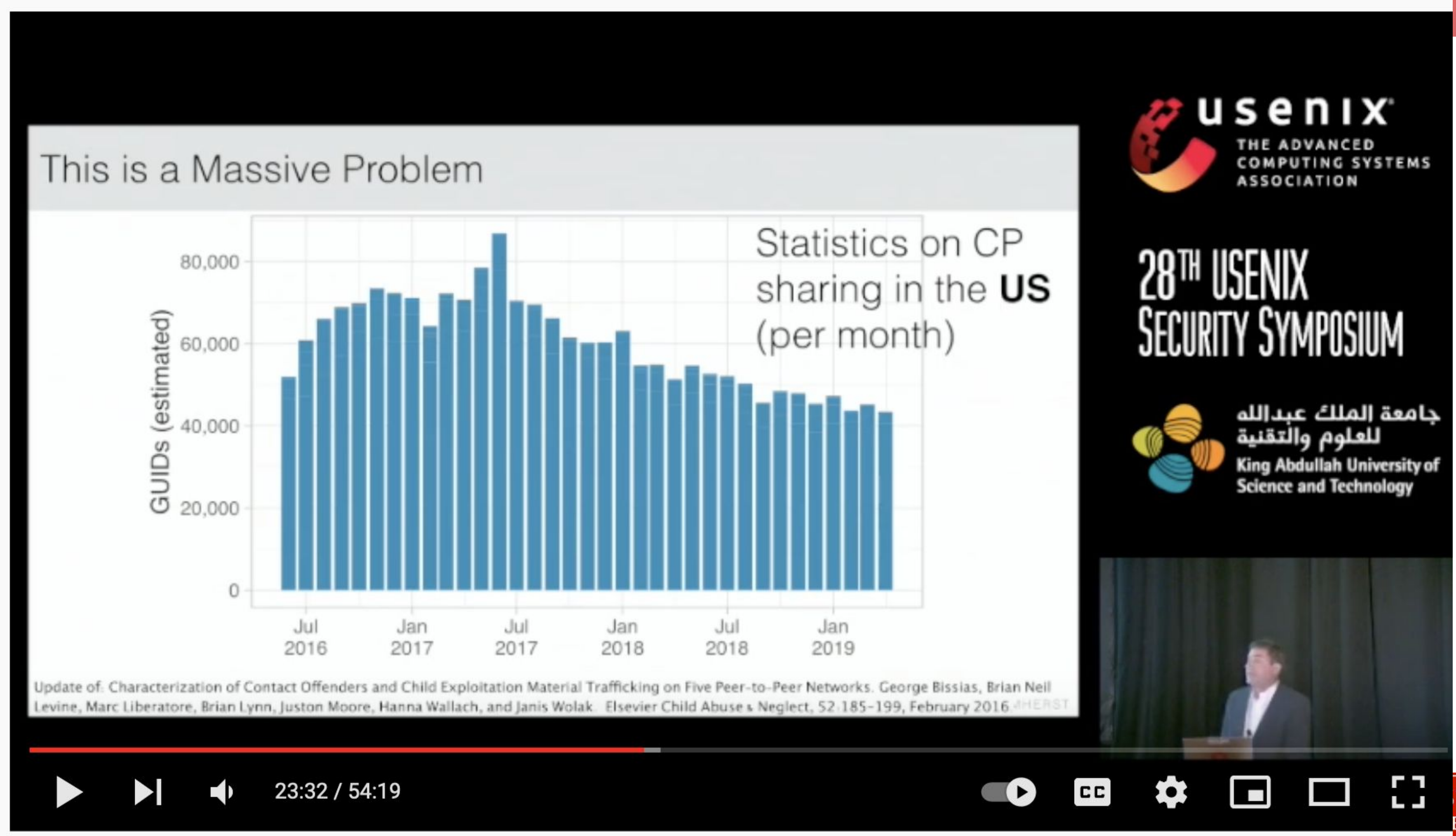


```
   onion_address = base32(PUBKEY | CHECKSUM | VERSION) + ".onion"
   CHECKSUM = H(".onion checksum" | PUBKEY | VERSION)[:2]

   where:
     - PUBKEY is the 32 bytes ed25519 master pubkey of the hidden service.
     - VERSION is an one byte version field (default value '\x03')
     - ".onion checksum" is a constant string
     - CHECKSUM is truncated to two bytes before inserting it in onion_address

Here are a few example addresses:

     pg6mmjiyjmcrsslvykfwnntlaru7p5svn6y2ymmju6nubxndf4pscryd.onion
     sp3k262uwy4r2k3ycr5awluarykdpag6a7y33jxop4cs2lu5uz5sseqd.onion
     xa4r2iadxm55fbnqgwwi5mymqdcofiu3w6rpbtqn7b2dyn7mgwj64jyd.onion
```



This is a Massive Problem

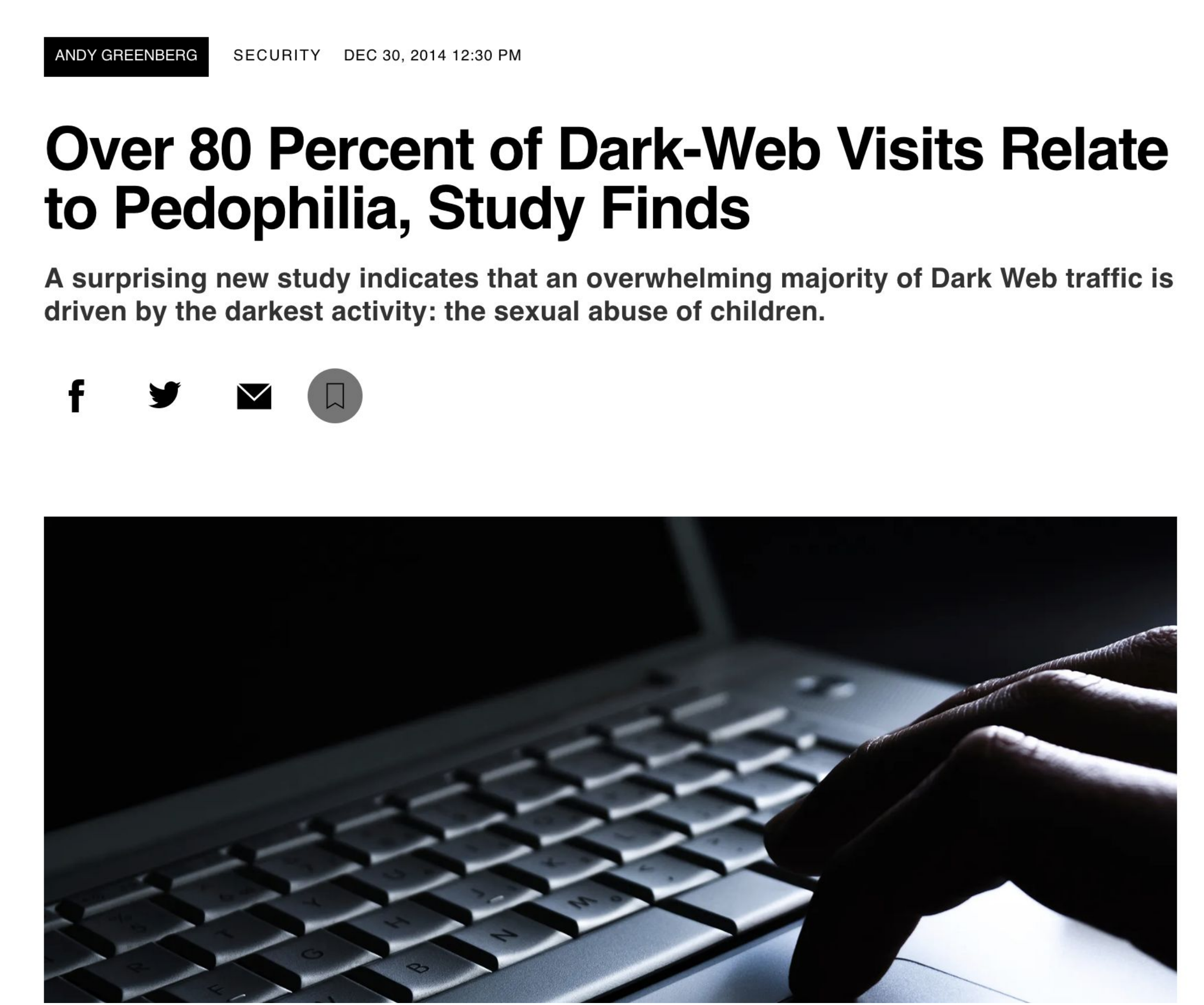
Statistics on CP sharing in the **US** (per month)

Update of: Characterization of Contact Offenders and Child Exploitation Material Trafficking on Five Peer-to-Peer Networks. George Bissias, Brian Neil Levine, Marc Liberatore, Brian Lynn, Juston Moore, Hanna Wallach, and Janis Wolak. Elsevier Child Abuse & Neglect, 52:185-199, February 2016

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

28TH USENIX SECURITY SYMPOSIUM

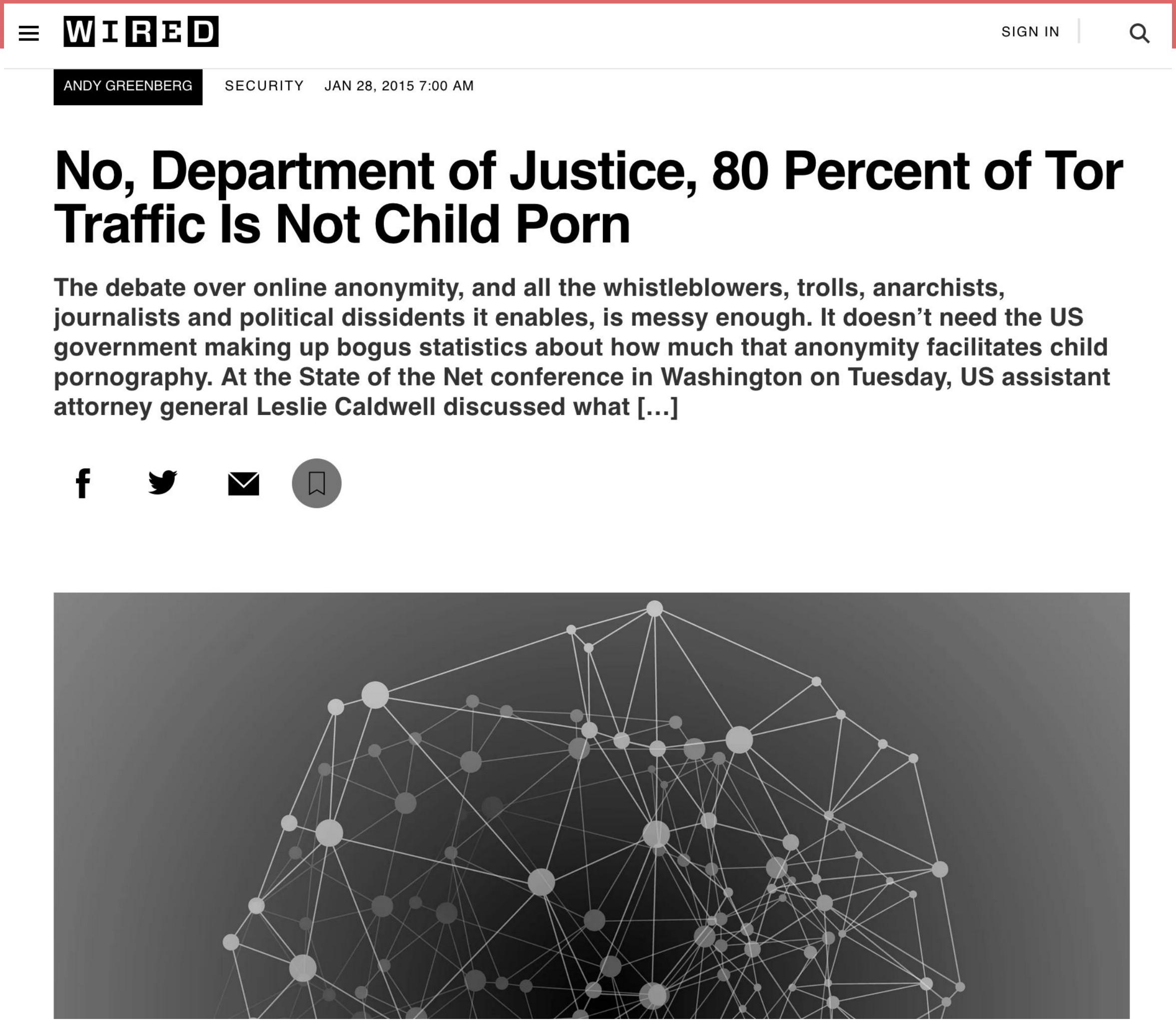
جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology



ANDY GREENBERG SECURITY DEC 30, 2014 12:30 PM

Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds

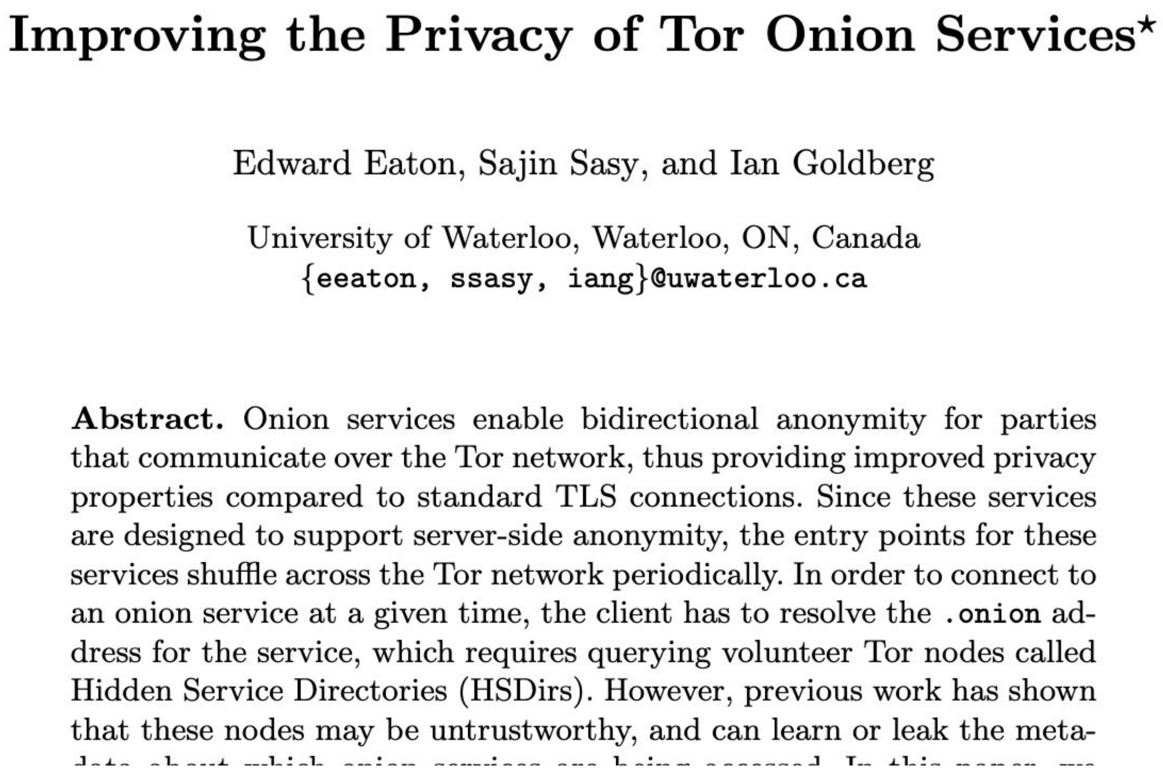
A surprising new study indicates that an overwhelming majority of Dark Web traffic is driven by the darkest activity: the sexual abuse of children.



ANDY GREENBERG SECURITY JAN 28, 2015 7:00 AM

No, Department of Justice, 80 Percent of Tor Traffic Is Not Child Porn

The debate over online anonymity, and all the whistleblowers, trolls, anarchists, journalists and political dissidents it enables, is messy enough. It doesn't need the US government making up bogus statistics about how much that anonymity facilitates child pornography. At the State of the Net conference in Washington on Tuesday, US assistant attorney general Leslie Caldwell discussed what […]



Improving the Privacy of Tor Onion Services*

Edward Eaton, Sajin Sasy, and Ian Goldberg

University of Waterloo, Waterloo, ON, Canada
{eeaton, ssasy, iang}@uwaterloo.ca

Abstract. Onion services enable bidirectional anonymity for parties that communicate over the Tor network, thus providing improved privacy properties compared to standard TLS connections. Since these services are designed to support server-side anonymity, the entry points for these services shuffle across the Tor network periodically. In order to connect to an onion service at a given time, the client has to resolve the `.onion` address for the service, which requires querying volunteer Tor nodes called Hidden Service Directories (HSDirs). However, previous work has shown that these nodes may be untrustworthy, and can learn or leak the metadata about which onion services are being accessed. In this paper, we