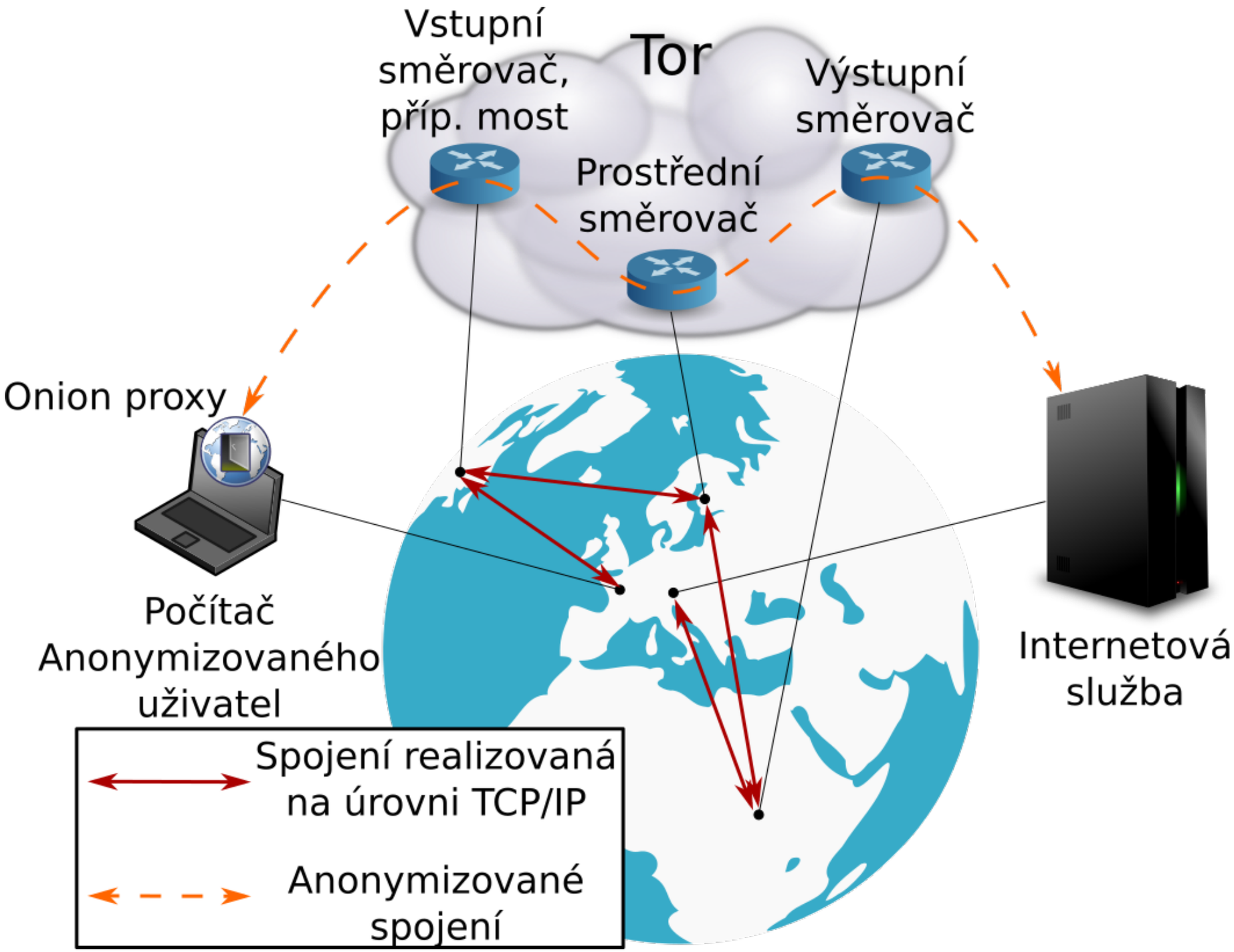
Identifikace v rámci Tor

Libor Polčák
2017-06-05

Jak funguje Tor?



Zjišťování uzlů Tor

EXONERATor

Enter an IP address and date to find out whether that address was used as a Tor relay:

IP address 147.229.13.223 **Date** 2013-04-03 Search

Summary

Result is positive

We found one or more Tor relays on IP address 147.229.13.223 on or within a day of 2013-04-03 that Tor clients were likely to know.

Technical details

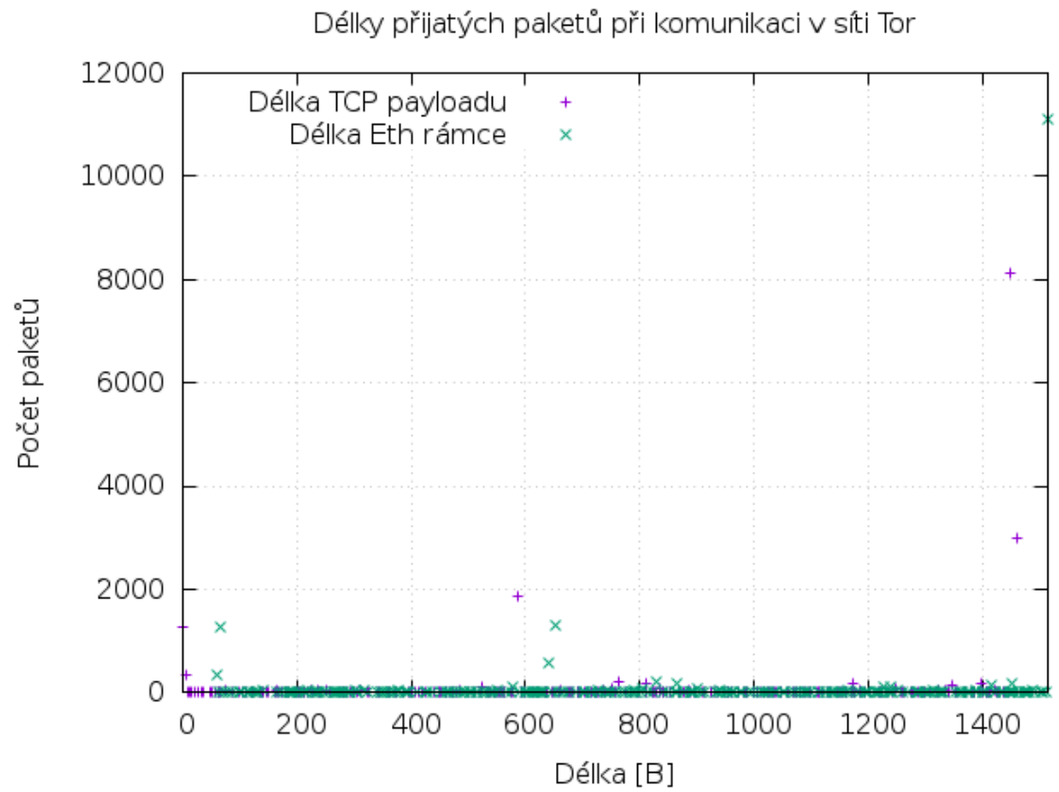
Looking up IP address 147.229.13.223 on or within one day of 2013-04-03. Tor clients could have selected this or these Tor relays to build circuits.

Timestamp (UTC)	IP address(es)	Identity fingerprint	Nickname	Exit relay
2013-04-02 21:00:00	147.229.13.223	33976F5A3FE0DFB0BB9D8436407C3D6C0D50353F	default	Yes
2013-04-02 22:00:00	147.229.13.223	33976F5A3FE0DFB0BB9D8436407C3D6C0D50353F	default	Yes
2013-04-02 22:00:00	147.229.13.223	33976F5A3FE0DFB0BB9D8436407C3D6C0D50353F	default	Yes

- Volně dostupné data o uzlech Tor
- Vyřešeno v komerčních nástrojích, i tak by se mohlo hodit jako součást integrované platformy
  - Např. omezení registrací na e-mailových službách
  - Detekce hotová ve Flowmon ADS

Vyhledávání uživatelů Toru

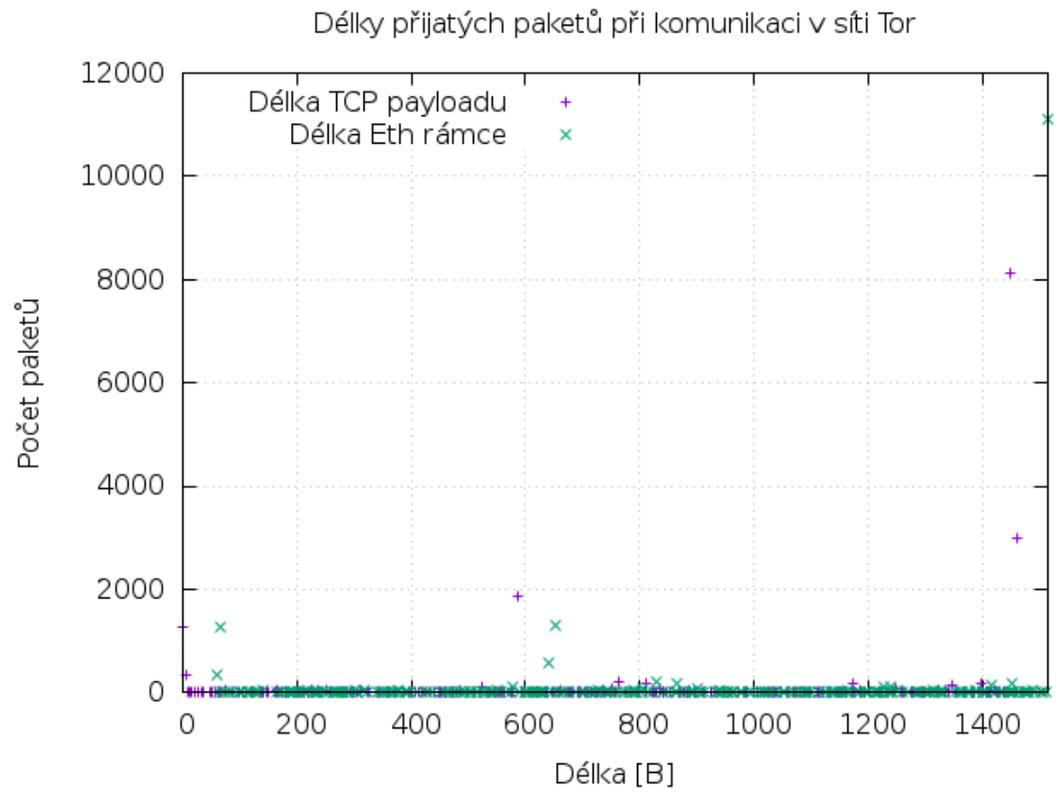
- Histogram velikosti délek paketů
- Uživatelé Toru mají specifickou charakteristiku
  - Payload TCP o velikosti 586B, 1172B



Délka TCP pld	Počet paketů
524	102
1348	143
1398	193
1172	195
812	195
762	215
6	358
0	1275
586	1862
1460	2992
1448	8121

Vyhledávání uživatelů Toru

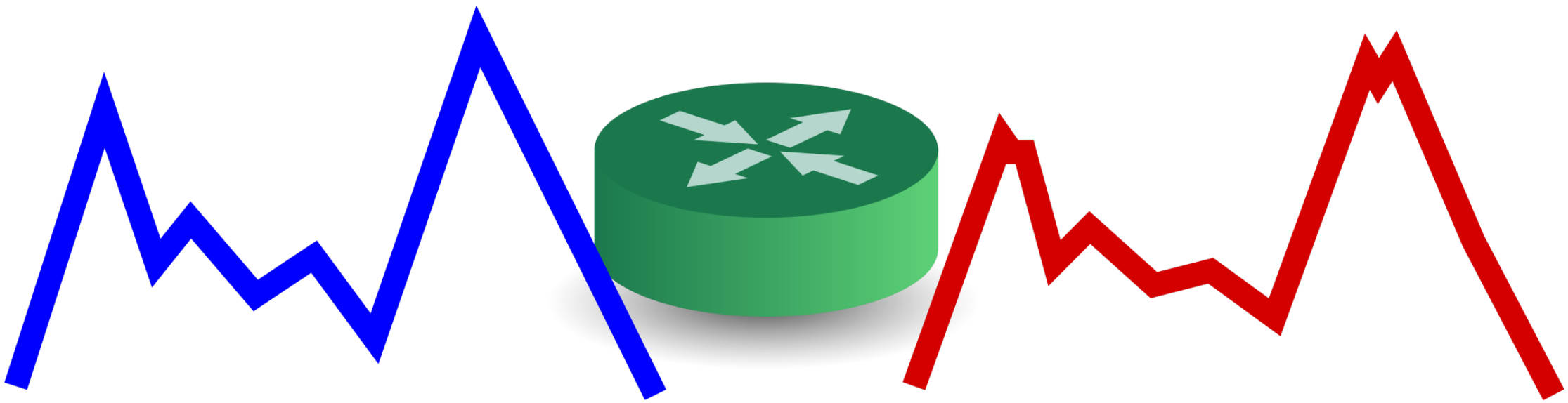
- Histogram velikosti délek paketů
- Uživatelé Toru mají specifickou charakteristiku
  - Payload TCP o velikosti 586B, 1172B
- Zdroj dat: např. obohacené NetFlow, volně dostupný seznam uzlů



Délka TCP pld	Počet paketů
524	102
1348	143
1398	193
1172	195
812	195
762	215
6	358
0	1275
586	1862
1460	2992
1448	8121

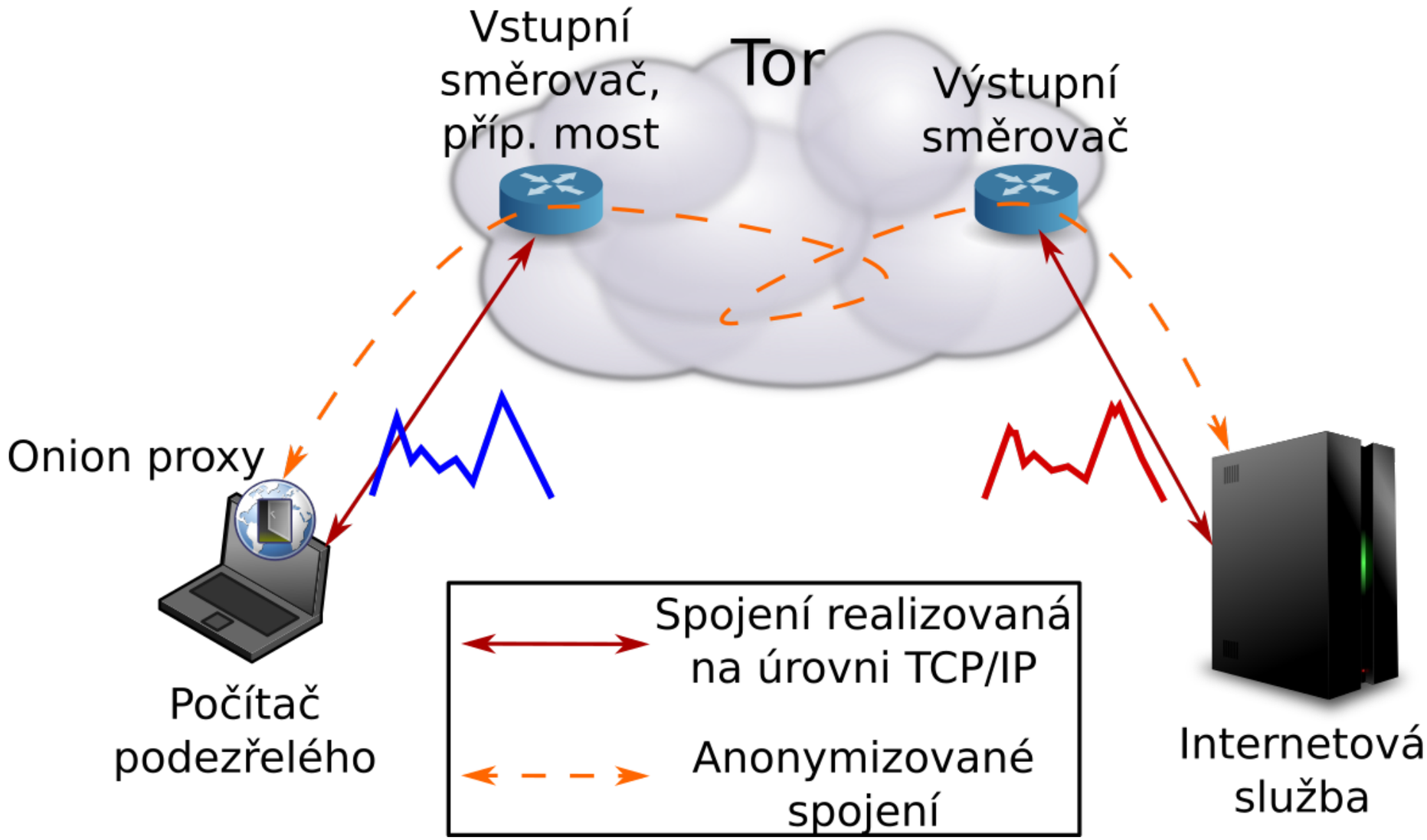
Korelační útoky

- Inter-Packet Delay Based Correlation for Tracing Encrypted Connections through Stepping Stones by Xinyuan Wang, Douglas S. Reeves, and S. Felix Wu. In the Proceedings of ESORICS 2002, October 2002, pages 244-263.
- On Flow Correlation Attacks and Countermeasures in Mix Networks by Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati, and Wei Zhao. In the Proceedings of Privacy Enhancing Technologies workshop (PET 2004), May 2004, pages 207-225.
- Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries by Aaron Johnson, Chris Wacek, Rob Jansen, Micah Sherr, and Paul Syverson. In the Proceedings of the 20th ACM conference on Computer and Communications Security (CCS 2013), November 2013.
- On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records by S. Chakravarty, M. V. Barbera, G. Portokalidis, M. Polychronakis, and A. D. Keromytis. In the Proceedings of the 15th Passive and Active Measurements Conference (PAM '14), March 2014.



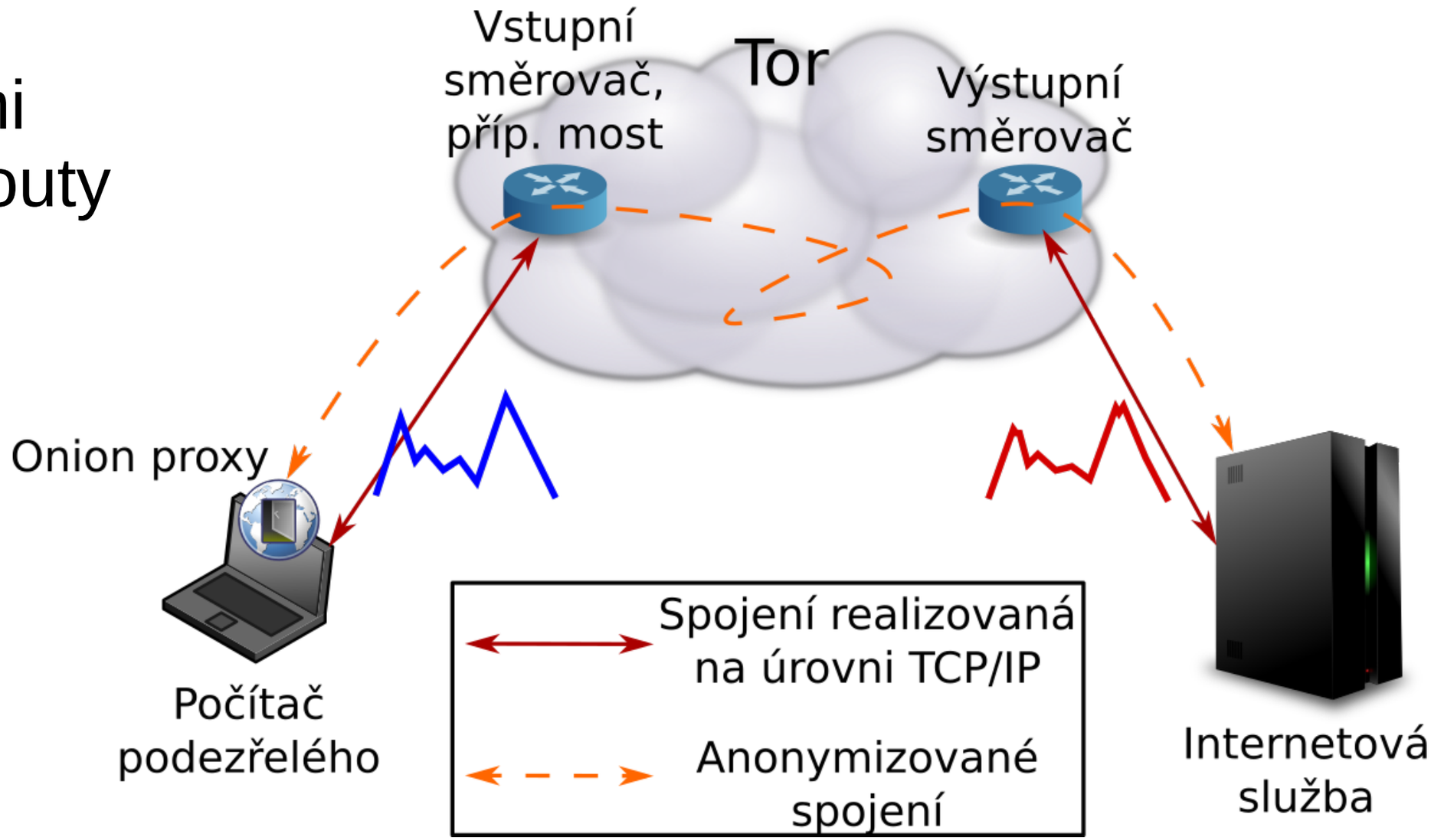
Navrhovaná aplikace korelace

- End-to-end, ne hop-by-hop jako uvažovala většina článků



Navrhovaná aplikace korelace

- End-to-end, ne hop-by-hop jako uvažovala většina článků
- Zdroj dat: netflow s velmi krátkými timeouty



Diskuze

- ExoneraTor – zkušenosti z používání?
- Užitečnost rozpoznání uživatelů Toru na základě délek přenášených paketů?
- Korelační útoky – má představený scénář smysl?

Questions?