

RUHR
UNIVERSITÄT
BOCHUM

RUB

جامعة نيويورك أبوظبي

NYU | ABU DHABI

Radboud
Universiteit
Nijmegen



WE BUILT THIS CIRCUIT: EXPLORING THREAT VECTORS IN CIRCUIT ESTABLISHMENT IN TOR

6th IEEE European Symposium on Security and Privacy (Euro S&P '21), September 9, 2021

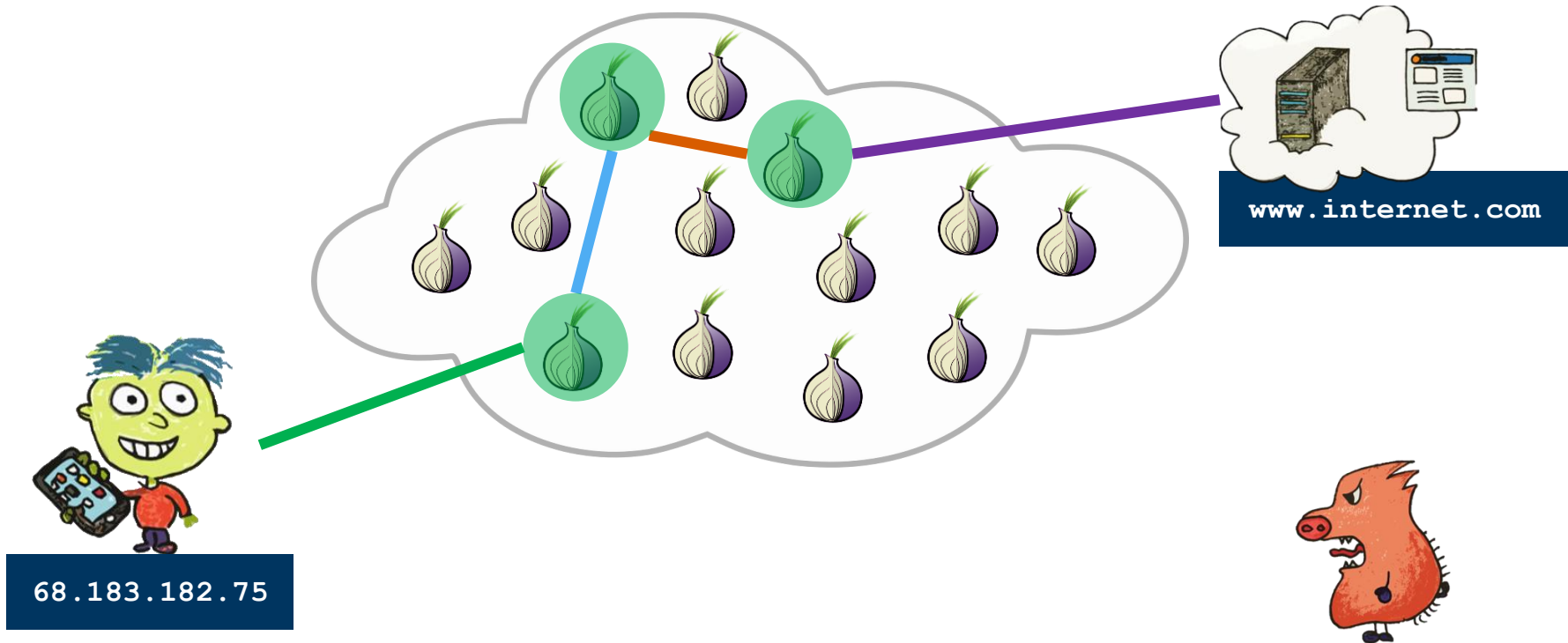
Theodor Schnitzler
Ruhr-Universität Bochum
theodor.schnitzler@rub.de

Christina Pöpper
New York University Abu Dhabi

Markus Dürmuth
Ruhr-Universität Bochum

Katharina Kohls
Radboud University

ANONYMITY IN TOR



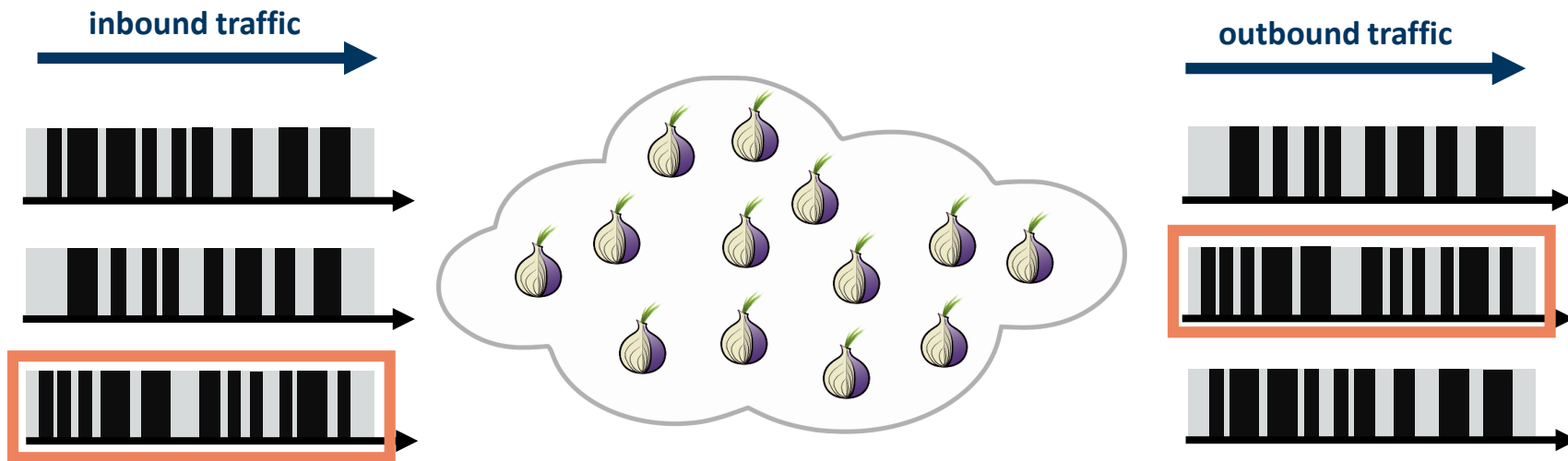
EXPLORING THREAT VECTORS IN CIRCUIT ESTABLISHMENT IN TOR

IEEE Euro S&P 2021 – Online Event

Theodor Schnitzler, Christina Pöpper, Markus Dürmuth, Katharina Kohls



TRAFFIC ANALYSIS



[1] Nasr et al.: DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning (ACM CCS 2018)

EXPLORING THREAT VECTORS IN CIRCUIT ESTABLISHMENT IN TOR

IEEE Euro S&P 2021 – Online Event

Theodor Schnitzler, Christina Pöpper, Markus Dürmuth, Katharina Kohls



REQUIREMENTS FOR TRAFFIC ANALYSIS

Monitoring Effort

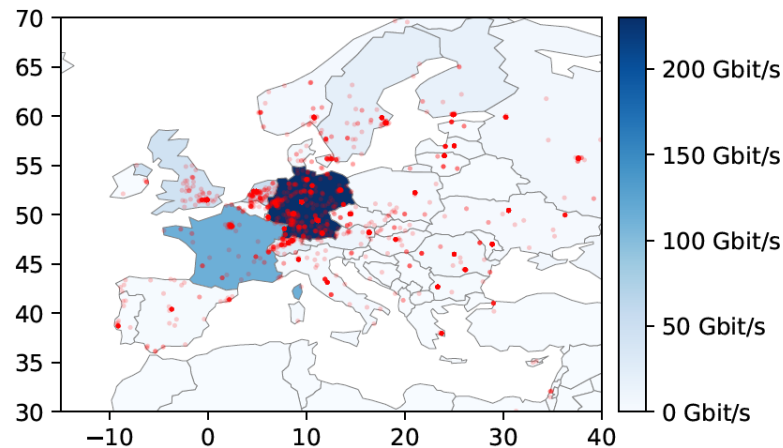
*Capture and evaluate
large amounts of Tor traffic*

Access to Traffic

*capture traffic of 7,000 relays
in different geographical locations*

600 Gbit/s
advertised bandwidth

300 Gbit/s
consumed bandwidth



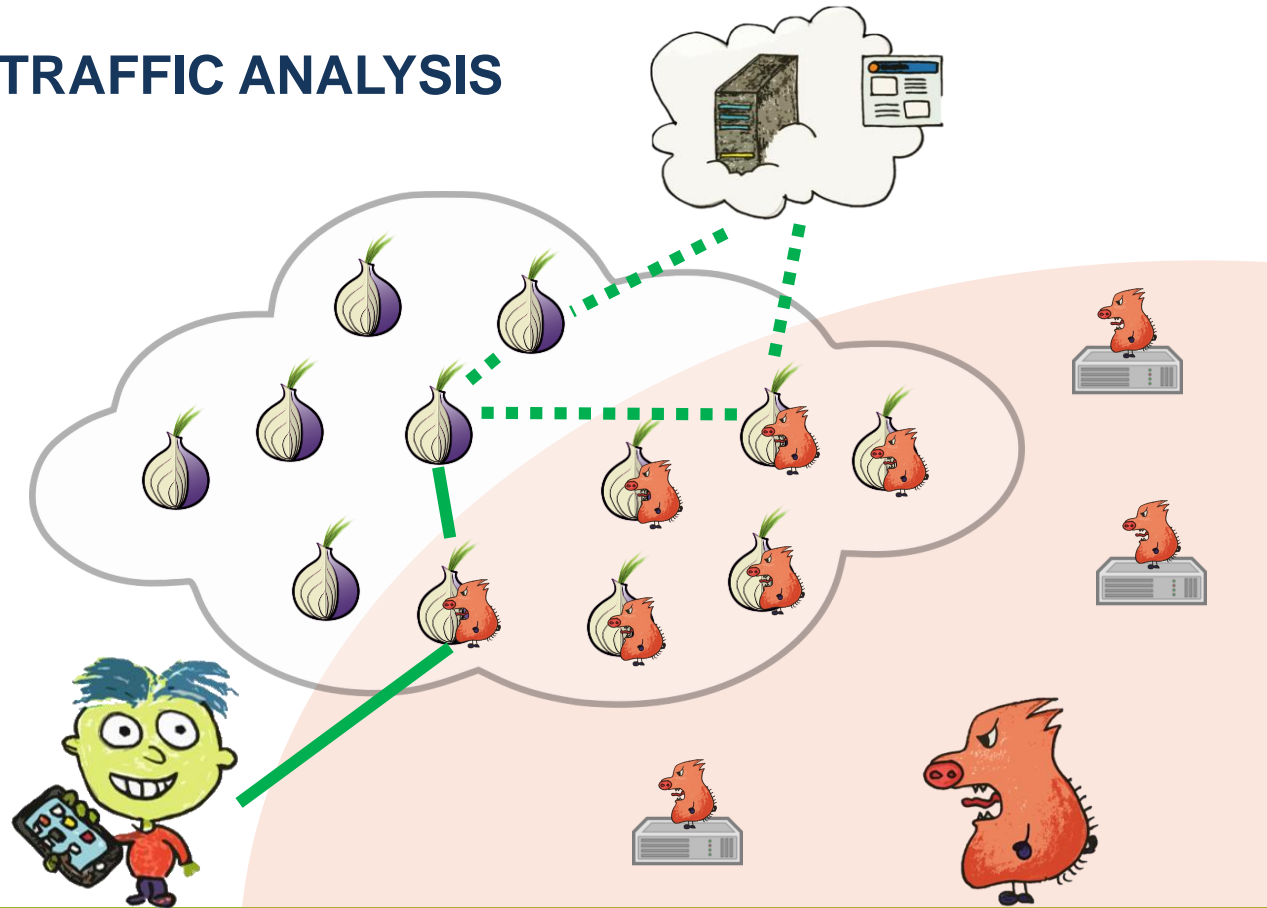
REQUIREMENTS FOR TRAFFIC ANALYSIS

Assumptions

- Adversary has access to exit traffic of a set of relays
- Adversary has access to client's entry traffic
- Targeted scenario

Research Questions







Can an adversary determine if they have access to Tor exit traffic?



EXIT PREDICTION

Goal: Exit Candidate Ranking

Determine success of traffic analysis from positions of relays that can be accessed

1.		ConnecTor	$p = 0.0185$
2.		PredaTor	$p = 0.0141$
3.		MoniTor	$p = 0.0110$
4.		BenefacTor	$p = 0.0102$
5.		EigenTor	$p = 0.0094$
6.		Liberator	$p = 0.0092$

Relay Selection

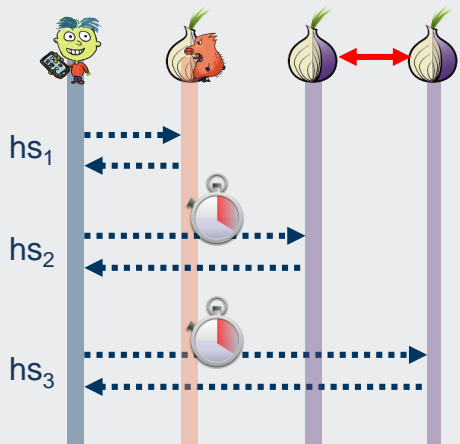
- More bandwidth → Higher probability
- Few restrictions to avoid collusions

Limited Utility

- Same result for each prediction
- No specific information for particular circuits

EXIT PREDICTION FOR INDIVIDUAL CIRCUITS

nTor Handshake Timings



$$\Delta_t(m, x) = t(hs_3) - t(hs_2)$$

Experiment

- 257k handshake timings
- Transmission models for groups of relays (per country)
- Find most likely model for new observations
- Probability for each exit candidate \rightarrow ranking

RESEARCH ETHICS

MEASUREMENTS CONDUCTED AT OUR CLIENTS, TO NOT RECORD TRAFFIC OF OTHER USERS

Evaluation

- Adversary with access to all relays in a country
- Median exit rank [%] in prediction

Ranking	DE				
COMBI	4	12	7	9	8
TIME	10	25	13	15	17
BW	11	21	16	23	22
RAND	49	50	50	51	50

IN THE PAPER

Further Evaluation

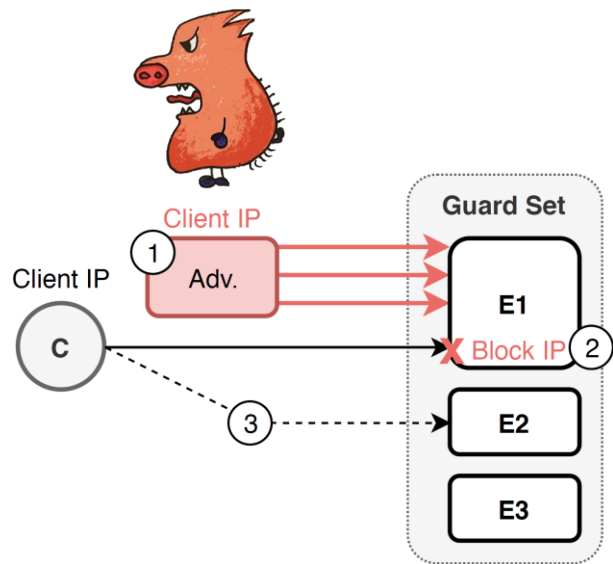
- Success rates \leftrightarrow monitoring effort

Actively Interfering with Circuit Establishment

- Force client to switch to another guard
- Trigger DoS Mitigation
- Benefits: Stealthy Attack

Mitigation Options Affect Performance

- Delays for Timing Obfuscation
- Randomized Relay Selection





WE BUILT THIS CIRCUIT: EXPLORING THREAT VECTORS IN CIRCUIT ESTABLISHMENT IN TOR

6th IEEE European Symposium on Security and Privacy
Euro S&P '21, September 9, 2021



Theodor Schnitzler
Ruhr-Universität Bochum
theodor.schnitzler@rub.de
@the0retisch



Illustrations: Katharina Kohls

Key Takeaways

- Access to traffic is a critical requirement for traffic analysis
- Information leak in Tor circuit establishment can improve the position of the adversary
- Attacks using *defensive* features are hard to mitigate