On the Applicability of Traffic-splitting Strategies as a Protection Shield against End-to-end Traffic Correlation Attacks in Tor

Asya Mitseva, Bozhan Cai, Andriy Panchenko

asya.mitseva@b-tu.de, bozhan.cai@b-tu.de, andriy.panchenko@b-tu.de
Chair of IT Security

17 September 2026

Brandenburg
University of Technology
Cottbus - Senftenberg

Motivation

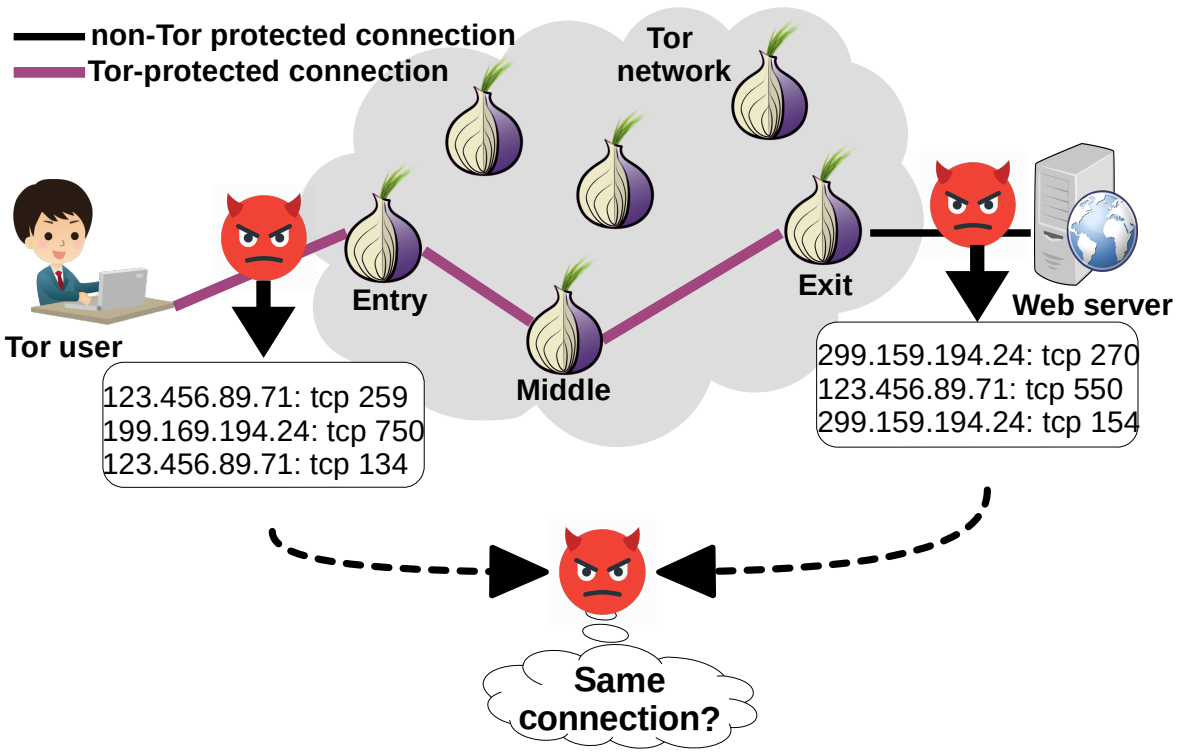
- **Users leave personal digital traces with each online action**
  - Often *abused for marketing purposes*, *user tracking*, *censorship*

Motivation

- **Users leave personal digital traces with each online action**
  - Often *abused for marketing purposes*, *user tracking*, *censorship*
- **Tor – most popular low-latency anonymization network**
  - Hides the relationship between users and websites visited by them

Motivation

- **Users leave personal digital traces with each online action**
  - Often *abused for marketing purposes*, *user tracking*, *censorship*
- **Tor – most popular low-latency anonymization network**
  - Hides the relationship between users and websites visited by them
- ***Problem:* Tor does not hide packet number, direction, timing**
  - Vulnerable to *end-to-end (E2E) traffic correlation* attacks



The Scope of This Work

- **E2E traffic correlation was considered impractical in real world**
  - Significant differences between the ingress and egress Tor traffic
  - Requires more computational resources to compare all traffic pairs
  - Explicitly excluded from the Tor's threat model

The Scope of This Work

- **E2E traffic correlation was considered impractical in real world**
  - Significant differences between the ingress and egress Tor traffic
  - Requires more computational resources to compare all traffic pairs
  - Explicitly excluded from the Tor's threat model

- ***Problem:*** **Significant evolution of E2E traffic correlation attacks**
  - Conducting E2E traffic correlation on Internet eXchange Points
  - Questioning the impracticality of E2E traffic correlation in real world

The Scope of This Work

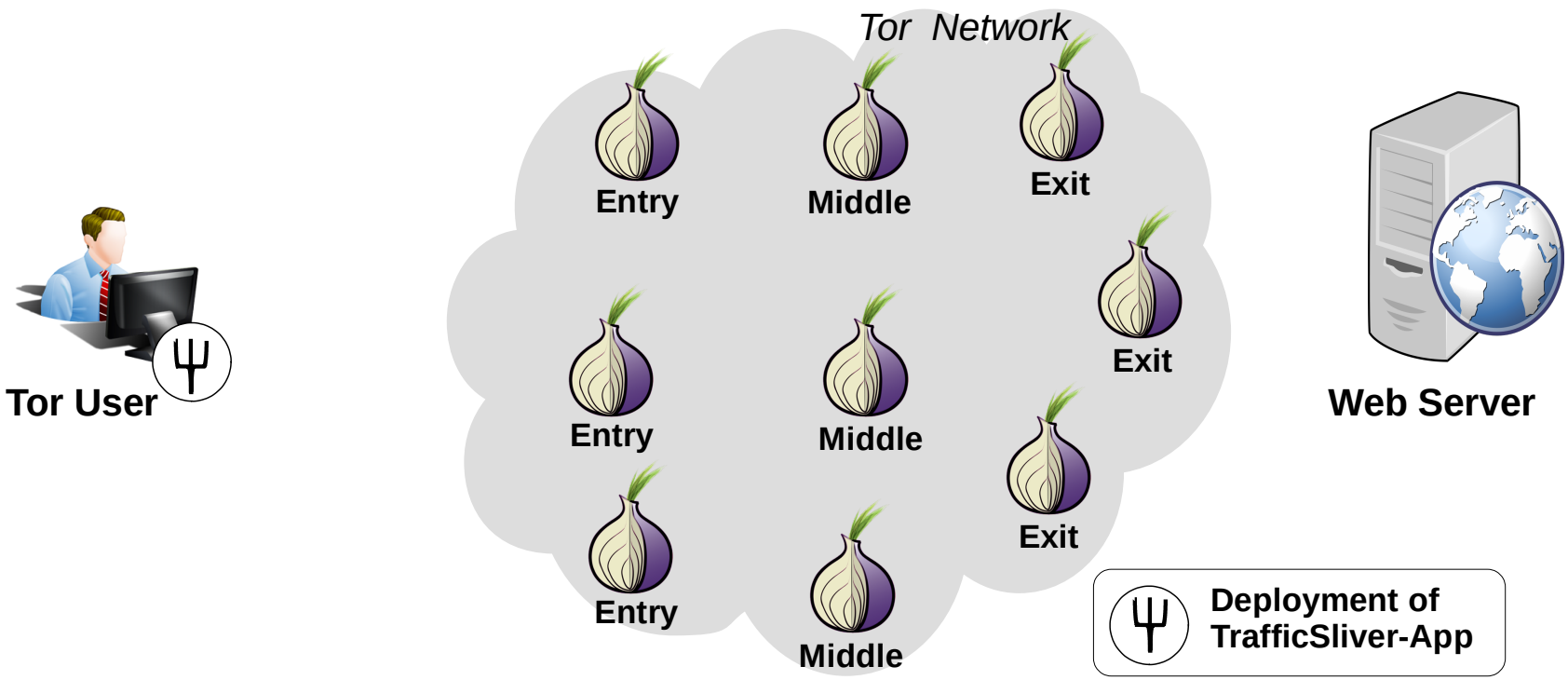
- **E2E traffic correlation was considered impractical in real world**
  - Significant differences between the ingress and egress Tor traffic
  - Requires more computational resources to compare all traffic pairs
  - Explicitly excluded from the Tor's threat model

- ***Problem:*** **Significant evolution of E2E traffic correlation attacks**
  - Conducting E2E traffic correlation on Internet eXchange Points
  - Questioning the impracticality of E2E traffic correlation in real world

- **Our contributions**
  - Bridge the gap between E2E traffic correlation and website fingerprinting (WFP) communities
  - Identify defense protecting against both traffic analysis attacks
  - Assess the effectiveness of two state-of-the-art, traffic-splitting-based WFP defenses against E2E traffic correlation

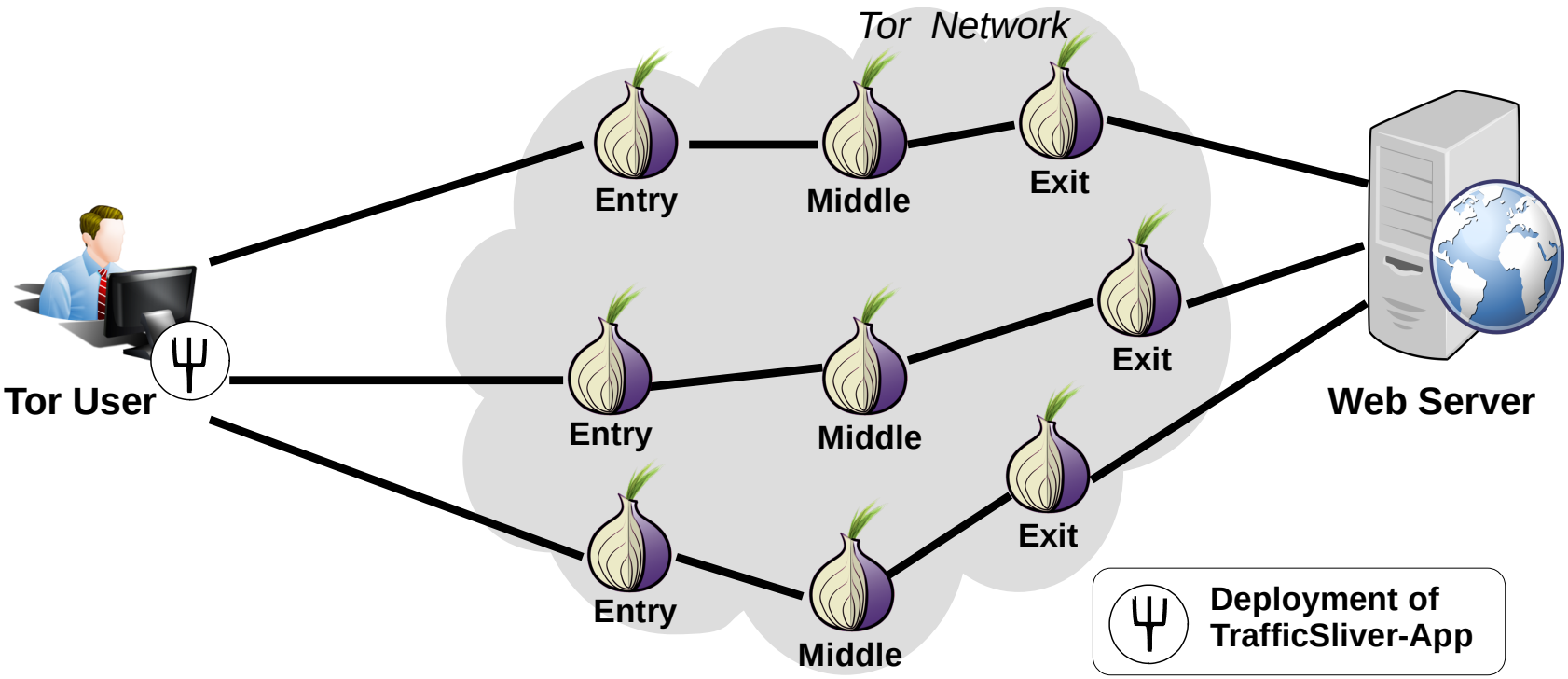
Splitting-based Traffic Analysis Defenses (1/2)

- **TrafficSliver-App: Traffic splitting at the application layer**
  - Published at *ACM CCS '20*
  - Independent of the Tor network, minimal overhead
  - Send *single*, *full* HTTP requests via different entry nodes



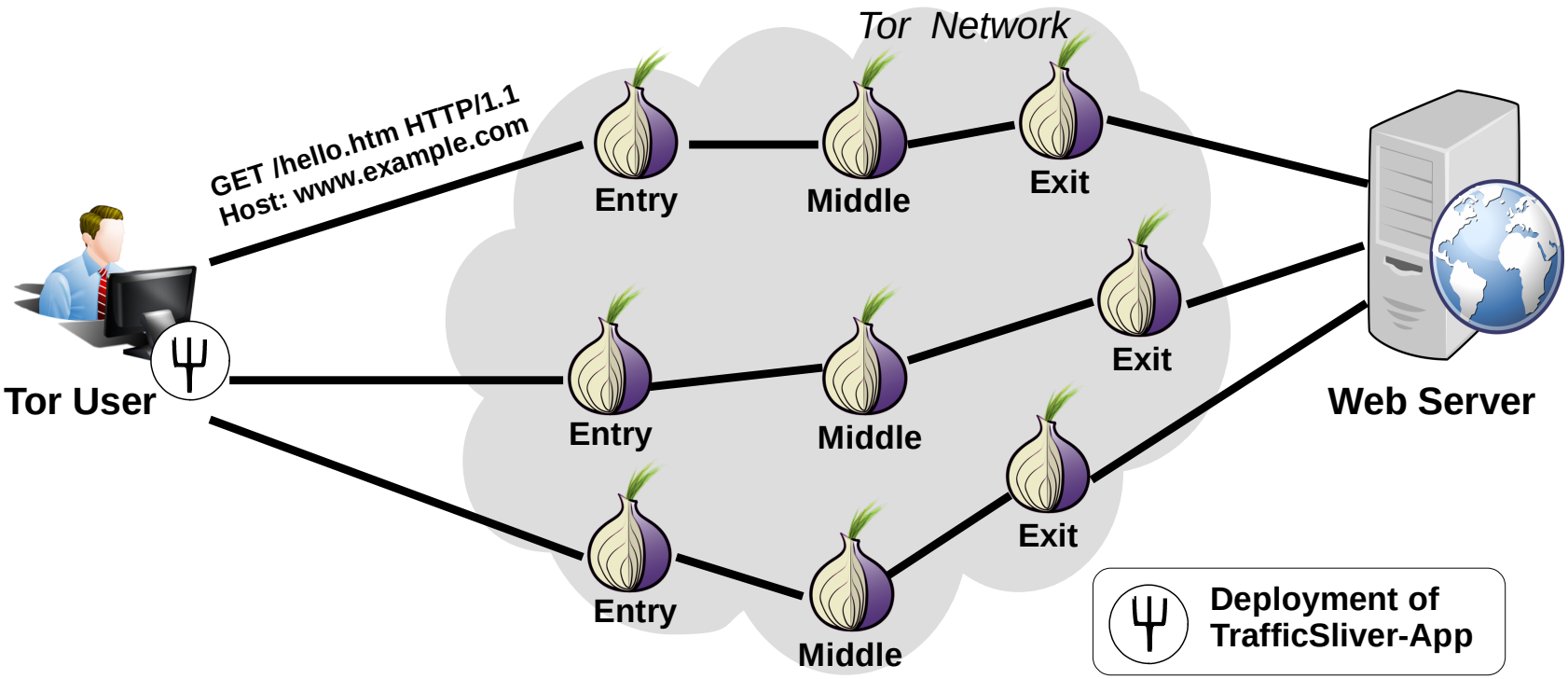
Splitting-based Traffic Analysis Defenses (1/2)

- **TrafficSliver-App: Traffic splitting at the application layer**
  - Published at *ACM CCS '20*
  - Independent of the Tor network, minimal overhead
  - Send *single*, *full* HTTP requests via different entry nodes



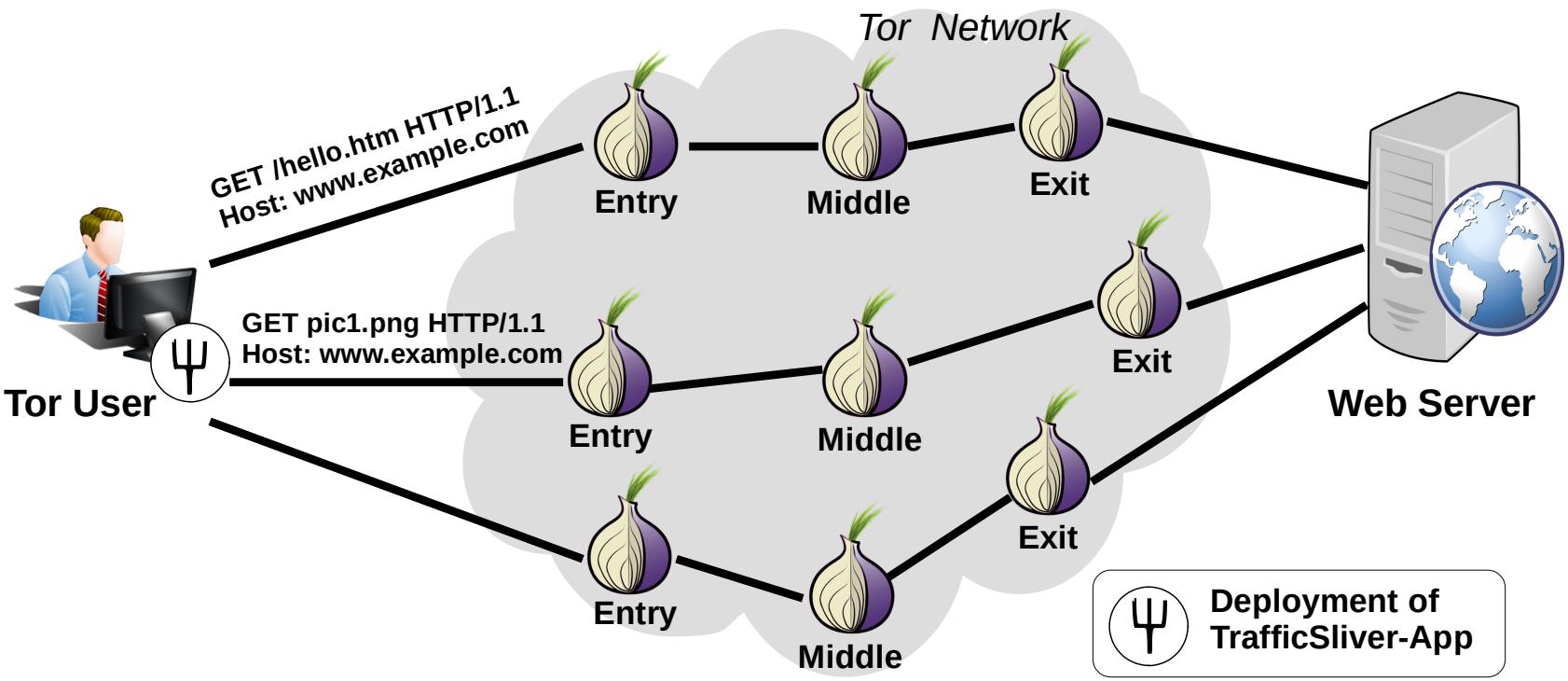
Splitting-based Traffic Analysis Defenses (1/2)

- **TrafficSliver-App: Traffic splitting at the application layer**
  - Published at *ACM CCS '20*
  - Independent of the Tor network, minimal overhead
  - Send *single*, *full* HTTP requests via different entry nodes



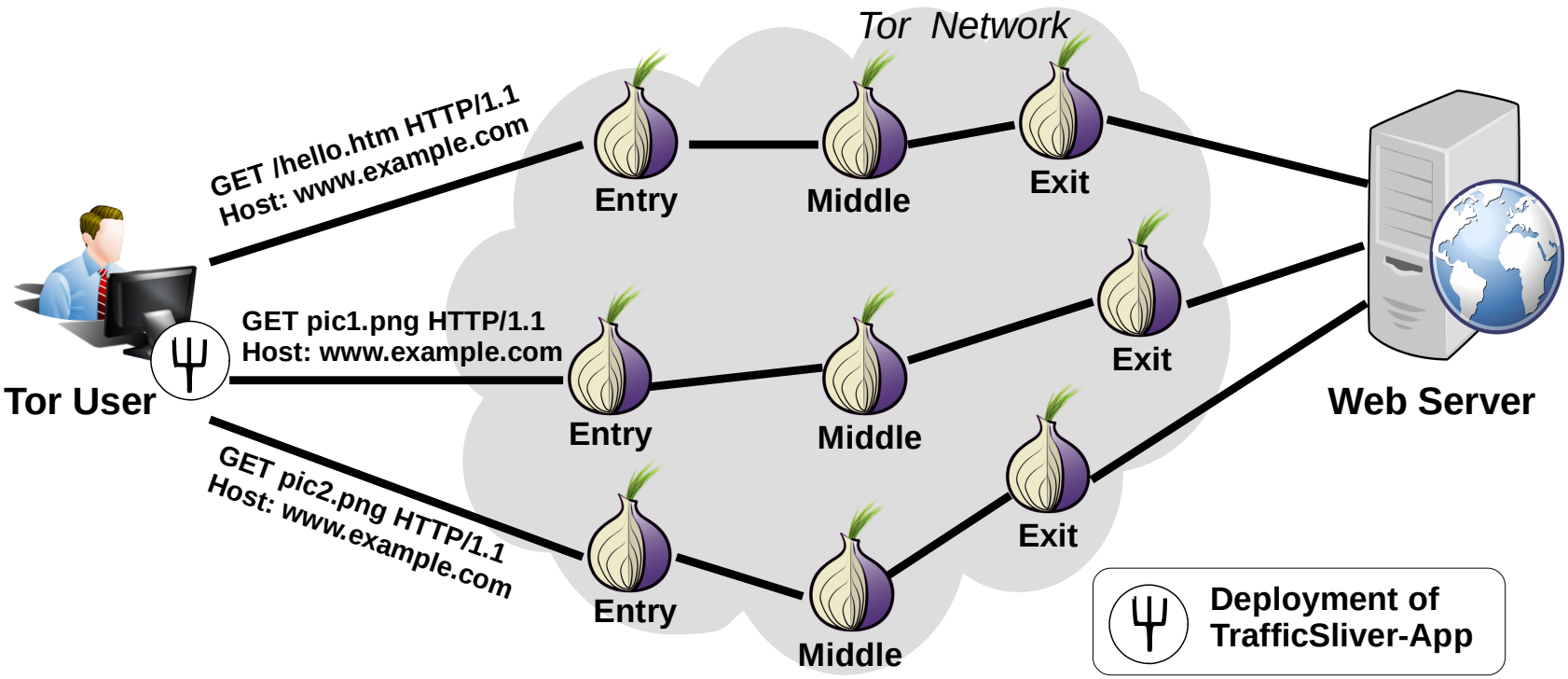
Splitting-based Traffic Analysis Defenses (1/2)

- **TrafficSliver-App: Traffic splitting at the application layer**
  - Published at *ACM CCS '20*
  - Independent of the Tor network, minimal overhead
  - Send *single*, *full* HTTP requests via different entry nodes



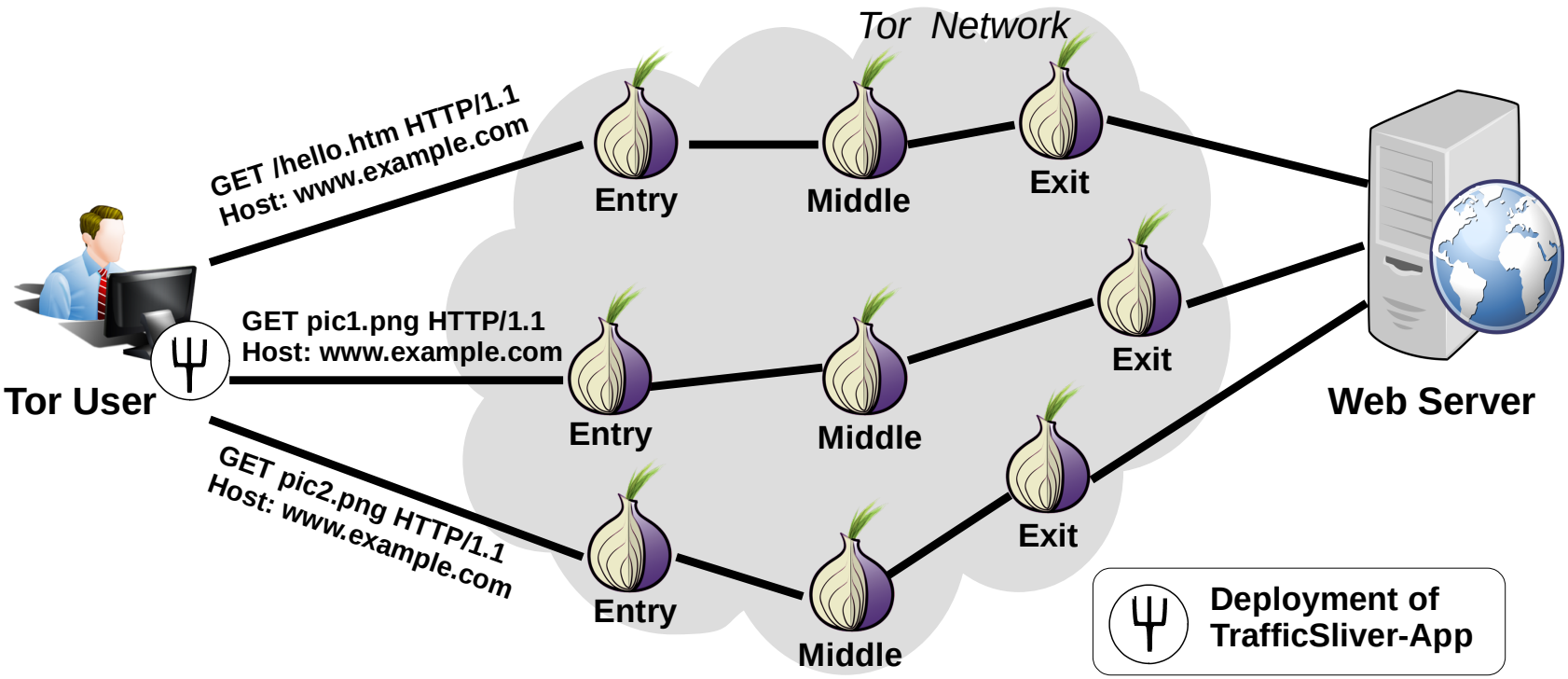
Splitting-based Traffic Analysis Defenses (1/2)

- **TrafficSliver-App: Traffic splitting at the application layer**
  - Published at *ACM CCS '20*
  - Independent of the Tor network, minimal overhead
  - Send *single*, *full* HTTP requests via different entry nodes



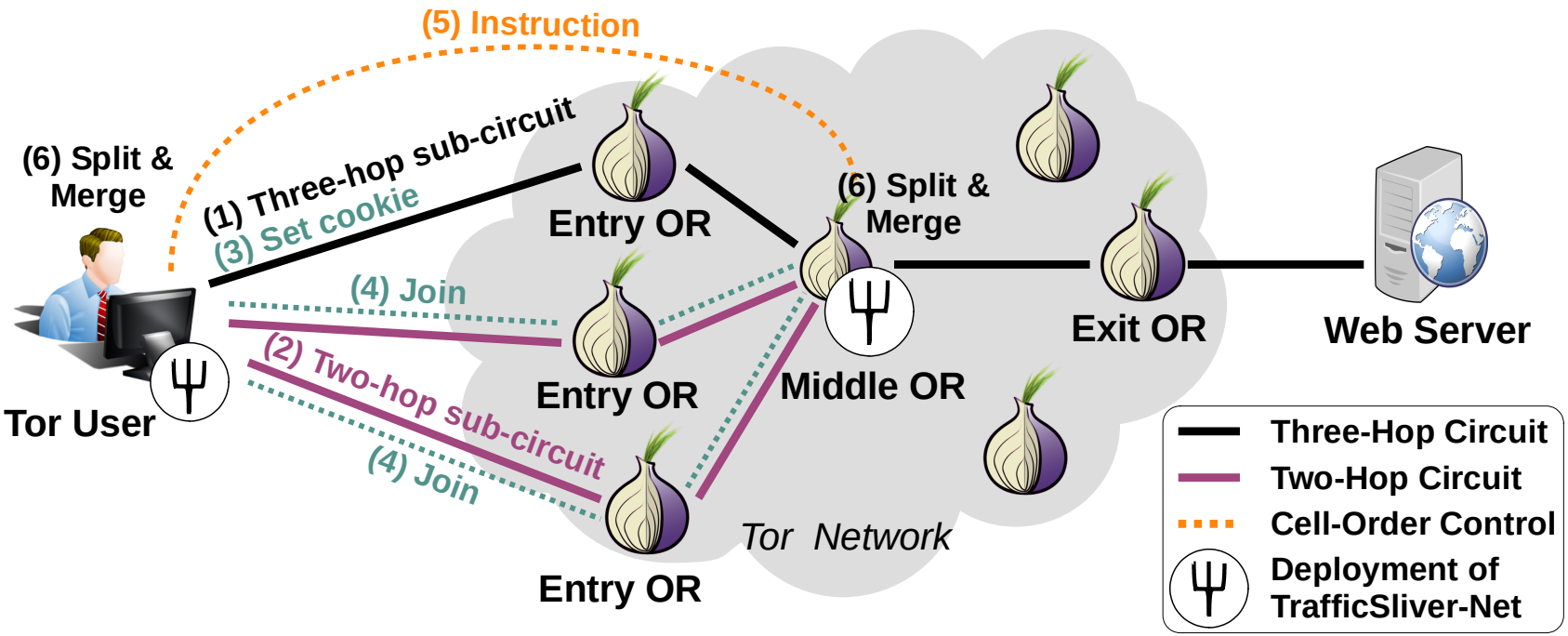
Splitting-based Traffic Analysis Defenses (1/2)

- **TrafficSliver-App: Traffic splitting at the application layer**
  - Published at *ACM CCS '20*
  - Independent of the Tor network, minimal overhead
  - Send *single*, *full* HTTP requests via different entry nodes
- ***Our extension*** **of the operational scope of TrafficSliver-App**
  - Different exit nodes for each sub-path of the multi-path connection
  - Single exit node for all sub-paths of the multi-path connection



Splitting-based Traffic Analysis Defenses (2/2)

- **TrafficSliver-Net: Traffic splitting at the network layer**
  - Published at *ACM CCS '20*
  - Modify Tor to distribute separate packets through different entry nodes
  - Splitting scheme: *Batched weighted random with five entry nodes*
    - Using a probabilistic distribution
    - Variable-sized batches of packets over multiple entry nodes



Experimental Setup

- **Datasets**
  - 500 websites from the Tranco Top list of the most popular websites

Experimental Setup

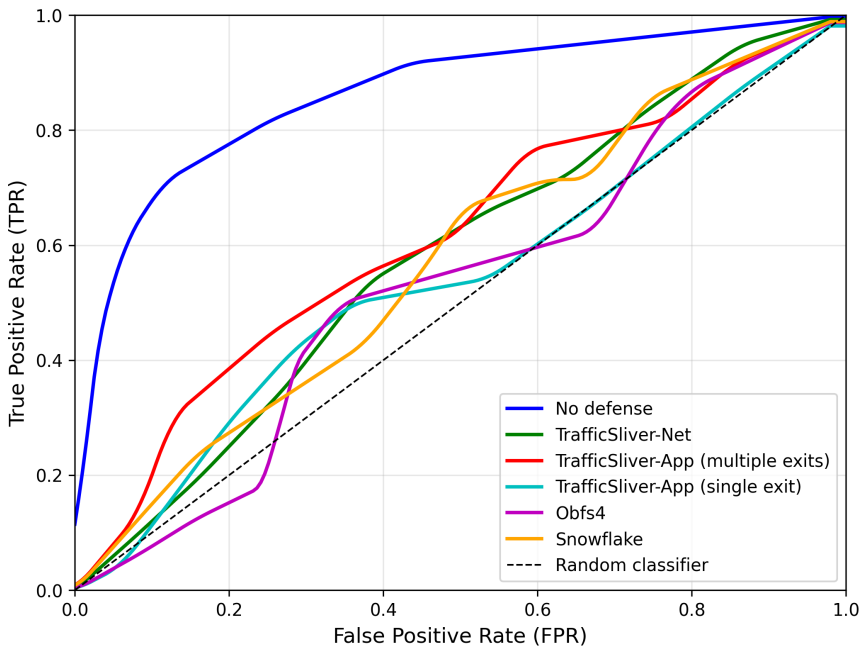
- **Datasets**
  - 500 websites from the Tranco Top list of the most popular websites
- **Network traffic collection**
  - Reverse proxy server located within the university campus network
  - Collects the traffic between Tor exit nodes and the final destinations
  - Rejects non-Tor user requests to reduce operational load
  - TCP packet sizes, direction, and timing extracted from collected traffic

Experimental Setup

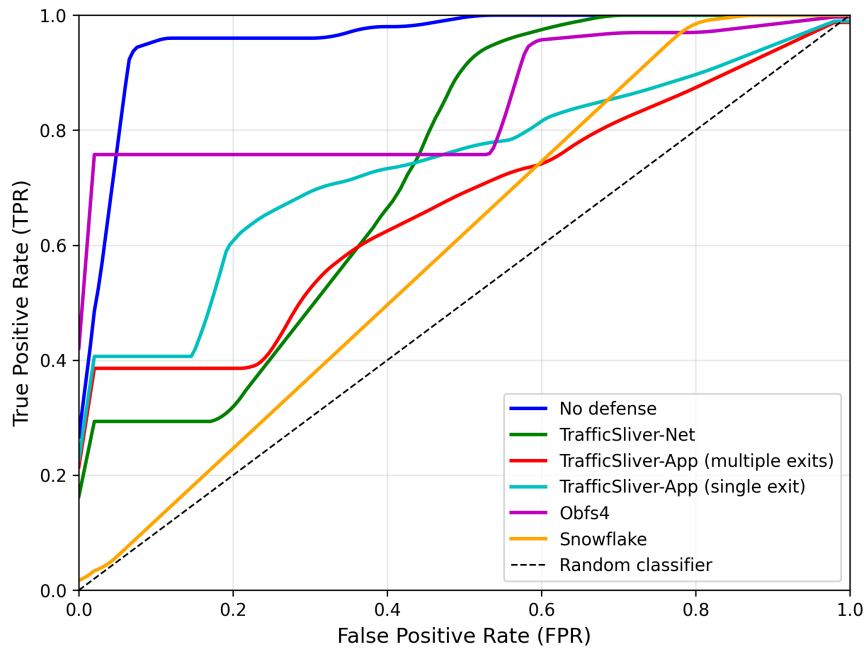
- **Datasets**
  - 500 websites from the Tranco Top list of the most popular websites
- **Network traffic collection**
  - Reverse proxy server located within the university campus network
  - Collects the traffic between Tor exit nodes and the final destinations
  - Rejects non-Tor user requests to reduce operational load
  - TCP packet sizes, direction, and timing extracted from collected traffic
- **Classifiers and evaluation setup**
  - Two state-of-the-art E2E traffic correlation classifiers
    - DeepCorr (*ACM CCS '18*) and DeepCoFFEA (*IEEE S&P '22*)
  - Evaluated metrics
    - True positive rate (TPR): fraction of detected, correctly correlated pairs
    - False positive rate (FPR): fraction of pairs that were falsely identified as correlated

Evaluation (1/2)

- **TrafficSliver defenses against E2E traffic correlation**
  - Significant drop in classifiers' detection rate for both defenses
  - Higher detection rate for TrafficSliver-App with multiple exit nodes
    - Possibly due to isolation of unique web objects over single sub-paths
  - Effective attacks in vanilla settings do not necessarily imply superiority in case of defenses



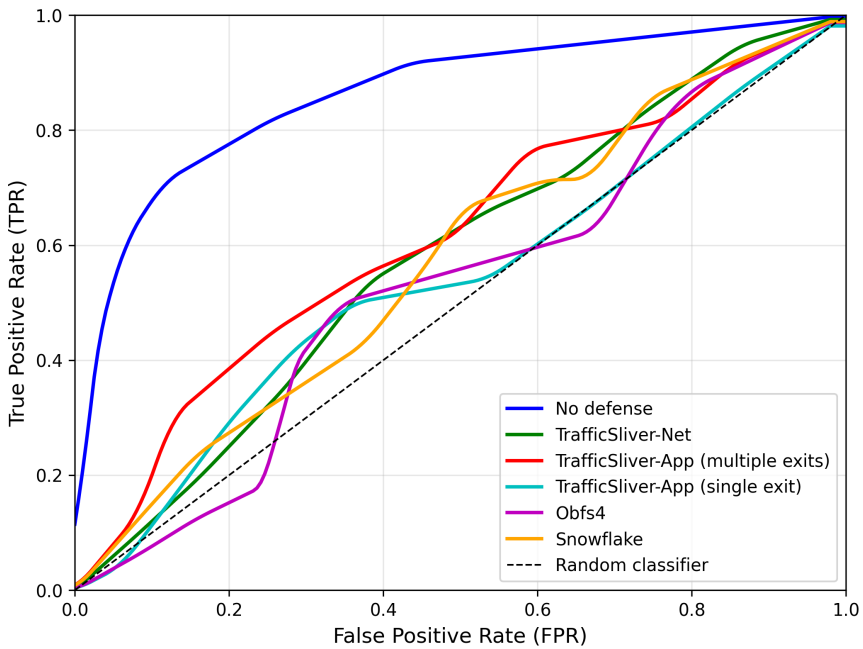
(a) DeepCorr



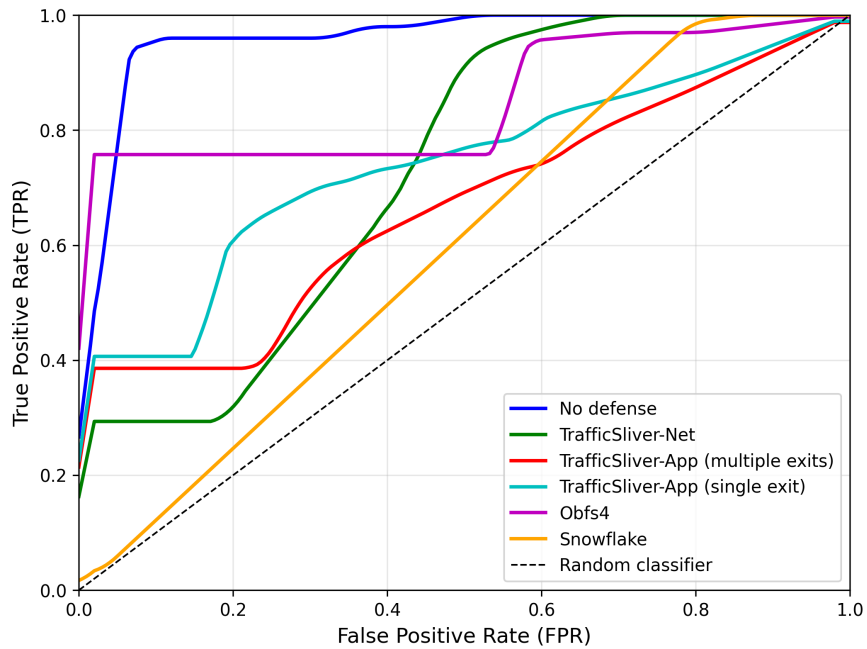
(b) DeepCoFFEA

Evaluation (2/2)

- **Comparison with Tor pluggable transports**
  - Obfs4's protection level is lower than TrafficSliver's for DeepCoFFEA
  - Snowflake provides higher level of protection than TrafficSliver defenses
  - *However,* pluggable transports are *not suitable* for all Tor users
    - Depend on the cooperation of Content Delivery Networks
    - Require Tor bridges, and have higher latency and bandwidth overhead



(a) DeepCorr



(b) DeepCoFFEA

Conclusion

- **E2E traffic correlation is privacy threat for Tor users**
  - More dangerous for Tor users than initially expected

Conclusion

- **E2E traffic correlation is privacy threat for Tor users**
  - More dangerous for Tor users than initially expected
- **Our goal: Analyze the protection level of existing WFP defenses against E2E traffic correlation**
  - Focus on two state-of-the-art traffic-splitting-based defenses

Conclusion

- **E2E traffic correlation is privacy threat for Tor users**
  - More dangerous for Tor users than initially expected
- **Our goal: Analyze the protection level of existing WFP defenses against E2E traffic correlation**
  - Focus on two state-of-the-art traffic-splitting-based defenses
- **Our takeaway**
  - Significant reduction of detection rates of modern E2E traffic correlation classifiers

Conclusion

- **E2E traffic correlation is privacy threat for Tor users**
  - More dangerous for Tor users than initially expected
- **Our goal: Analyze the protection level of existing WFP defenses against E2E traffic correlation**
  - Focus on two state-of-the-art traffic-splitting-based defenses
- **Our takeaway**
  - Significant reduction of detection rates of modern E2E traffic correlation classifiers

Thank you for your attention!