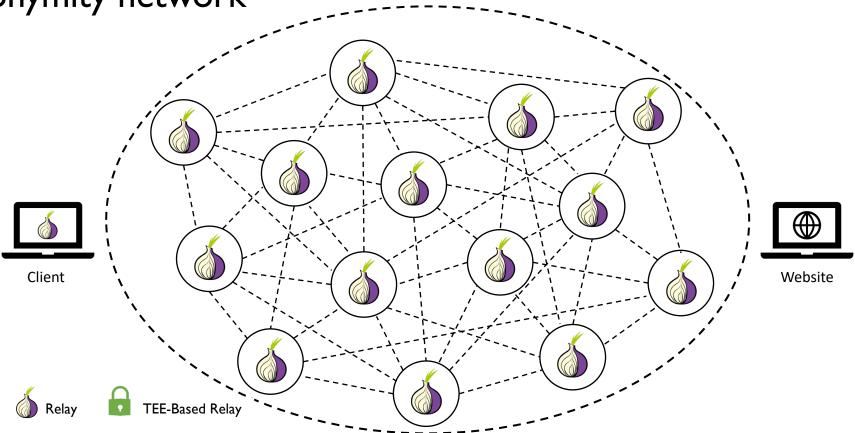
ParTEETor: A System for Partial Deployments of TEEs within Tor

Rachel King

Quinn Burke, Yohan Beugin, Blaine Hoak, Kunyang Li, Eric Pauley, Ryan Sheatsley, Patrick McDaniel

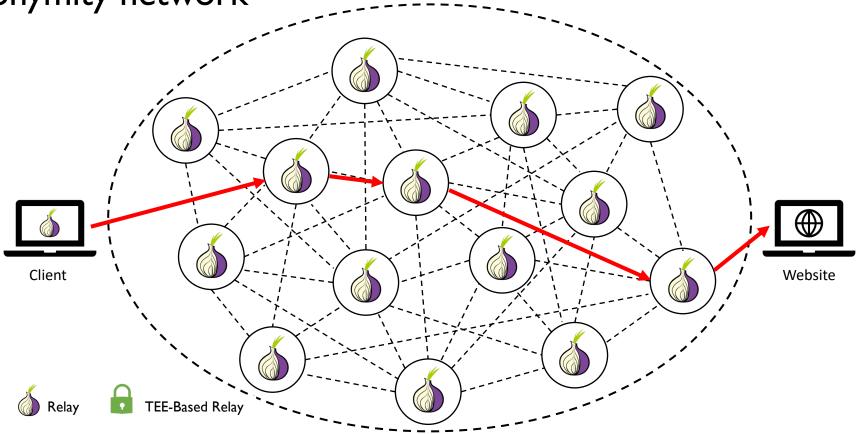


• Tor anonymity network





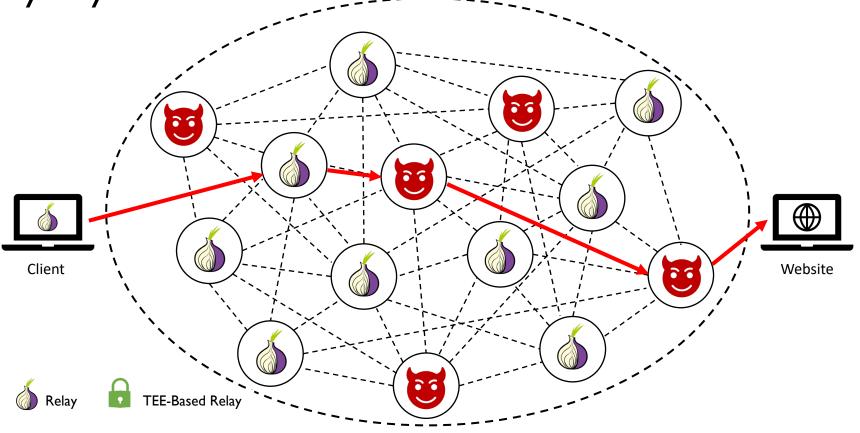
• Tor anonymity network





• Tor anonymity network

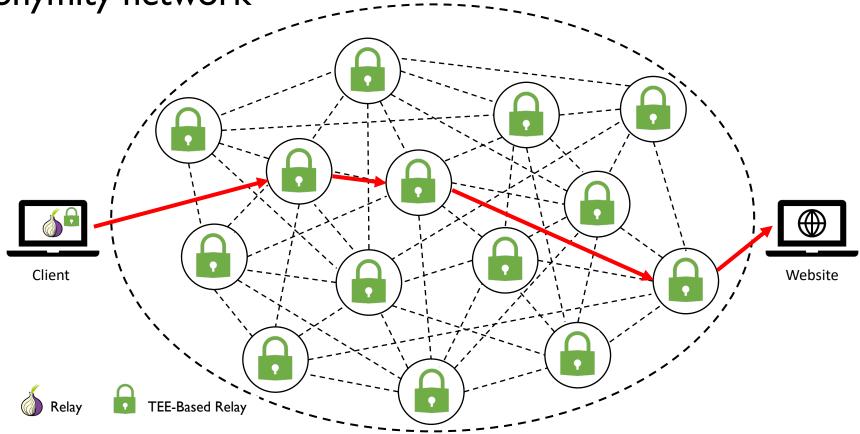
- Replay Attack [1]
- Onion Services Attack [2]
- Fingerprinting Attack [3]
- Bad Apple Attack [4]
- > Bandwidth Inflation [5]







Tor anonymity network

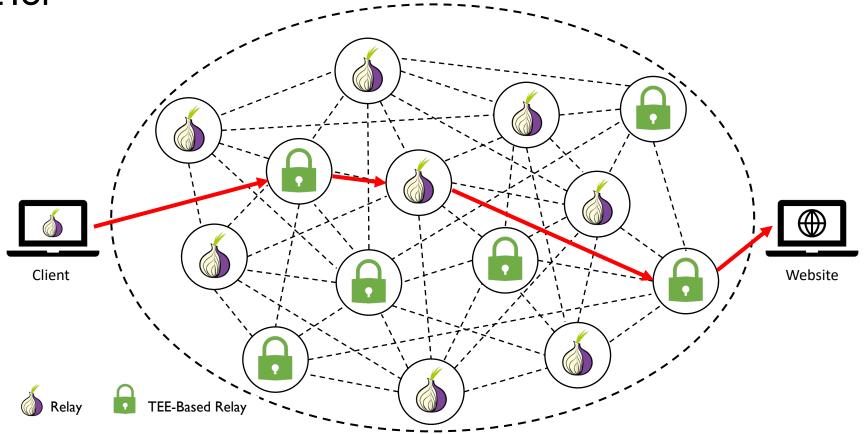




S. Kim, J. Han, J. Ha, T. Kim and D. Han, "SGX-Tor: A Secure and Practical Tor Anonymity Network With SGX Enclaves," in IEEE/ACM Transactions on Networking, Oct. 2018,

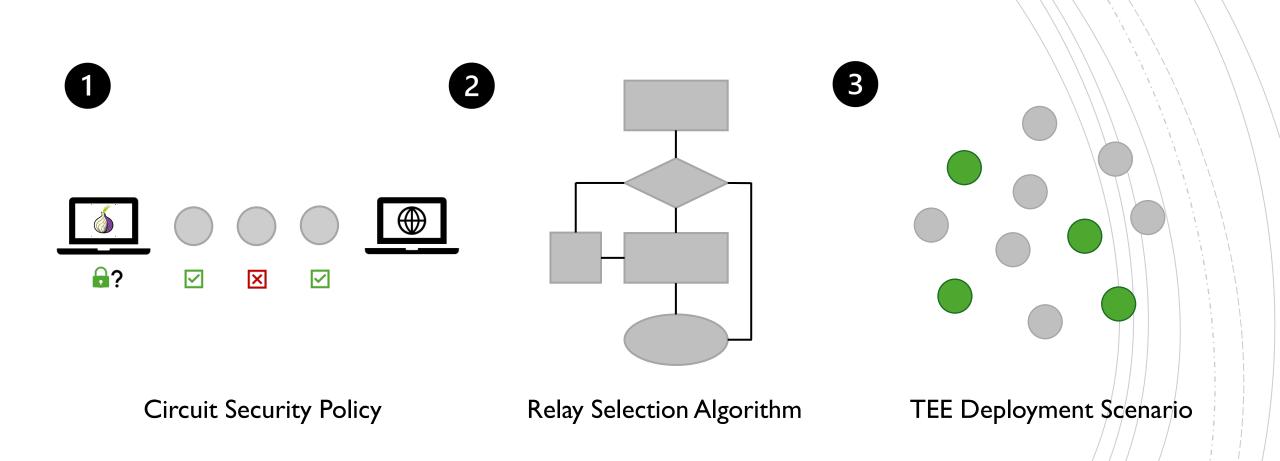
System Overview

• ParTEETor





ParTEETor





Circuit Security Policy

Attack	Adversarial Relays	TEE Requirement
Replay Attack [1]	Entry and Exit	Entry
Onion Services Attack [2]	Entry and Exit	Exit
Fingerprinting Attack [3]	Entry	Entry
Bad Apple Attack [4]	Exit	Exit
Bandwidth Inflation [5]	Entry, Middle, and Exit	Entry, Middle, and Exit

Required TEE placement to mitigate attacks

Security Policies			
None			
Entry			
Exit			
Entry, Exit			
Entry, Middle, Exit			

Security Policies



Extended Relay Selection Algorithm

```
Function RelaySelection (G = (V, E), R = (P, T)):
   circuit = [];
   for position, TEEreq \in R do
       relaylist = \{ \};
       for v \in V do
           if position \in v.positions then
               if v. TEE or not TEEreq then
                  add v to relaylist;
               end
           end
       end
       totalBW = \sum_{\forall r \in relaylist} r.bandwidth;
       select relay r with probability \frac{r.bandwidth}{totalBW};
       add relay to circuit;
   end
   return circuit
end
```

Security Policies

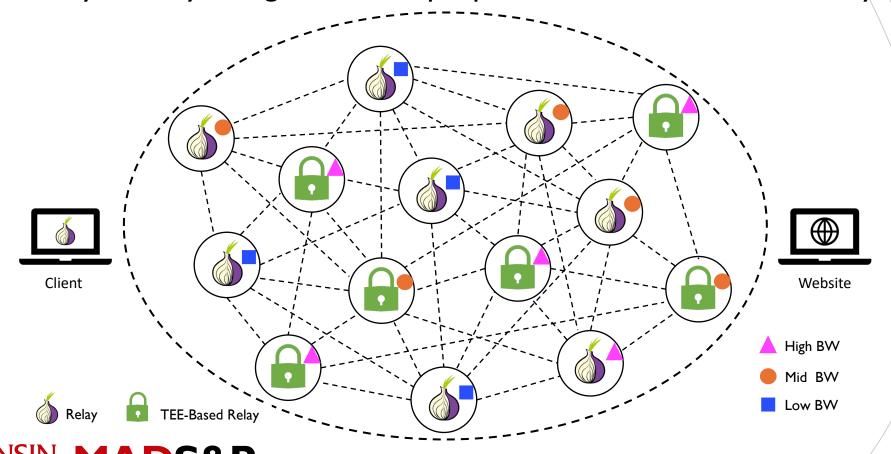
None
Entry
Exit
Entry, Exit
Entry, Middle, Exit



TEE Deployment Scenarios

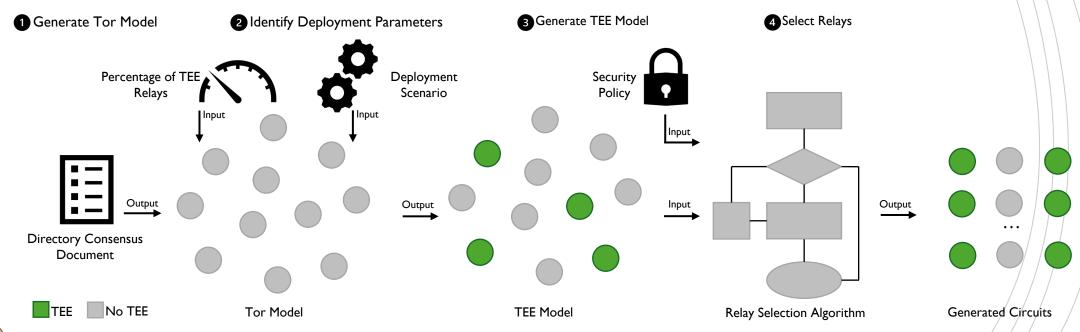
Bandwidth Weighted Deployment

• Probability of relay being TEE-based proportional to bandwidth of relay



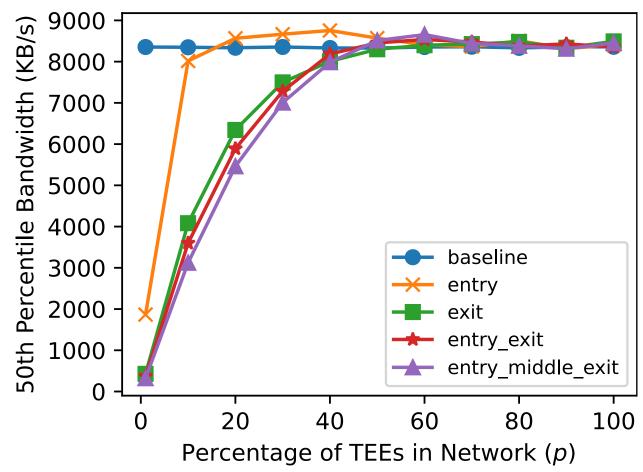
Evaluation

- (I) How much congestion is present in circuits when enforcing TEE requirements under partial deployments?
- (2) What is the reduction in availability of circuits when enforcing TEE requirements under partial deployments?





Performance





Privacy

TEEs	p=1%	p=5%	p=10%	p=25%
None	3.36×10^{10}			
Entry	3.36×10^{8}	1.68×10^{9}	3.36×10^{9}	8.42×10^{9}
Exit	3.36×10^{8}	1.68×10^9	3.36×10^9	8.42×10^{9}
Entry, Exit	3.36×10^{6}	8.42×10^{7}	3.36×10^{8}	2.10×10^{9}
Entry, Middle, Exit	3.36×10^4	4.21×10^{6}	3.36×10^{7}	5.26×10^{8}

Number of unique circuits possible based on the ratio of TEE-based relays in the network and the security policy.



Conclusions

Partial deployments of TEEs within Tor improve security.

Users can achieve the same performance seen in Tor today.

Users can meet privacy guarantees seen in historical versions of Tor.













Thank You!



https://rachelking.me



rachelking@cs.wisc.edu









References

- [1] R. Pries, W. Yu, X. Fu, and W. Zhao. 2008. A New Replay Attack Against Anonymous Communication Networks. In 2008 IEEE International Conference on Communications. IEEE, Beijing, China, 1578–1582.
- [2] Alex Biryukov, Ivan Pustogarov, and Ralf-Philipp Weinmann. 2013. Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. In 2013 IEEE Symposium on Security and Privacy. IEEE Computer Society, Oakland, California, 80–94.
- [3] Albert Kwon, Mashael AlSabah, David Lazar, Marc Dacier, and Srinivas Devadas. 2015. Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services. In 24th USENIX Security Symposium (USENIX Security 15). USENIX Association, Washington, D.C., 287–302.
- [4] Stevens Le Blond, Pere Manils, Abdelberi Chaabane, Mohamed Ali Kaafar, Claude Castelluccia, Arnaud Legout, and Walid Dabbous. 2011. One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users. In 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 11). USENIX Association, Boston, MA.
- [5] Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. 2007. Low-Resource Routing Attacks against Tor. In Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society (WPES '07). Association for Computing Machinery, Alexandria, Virginia, 1 I–20.

