SAND2019-8167D

The Center for Cyber Defenders

Expanding computer security knowledge

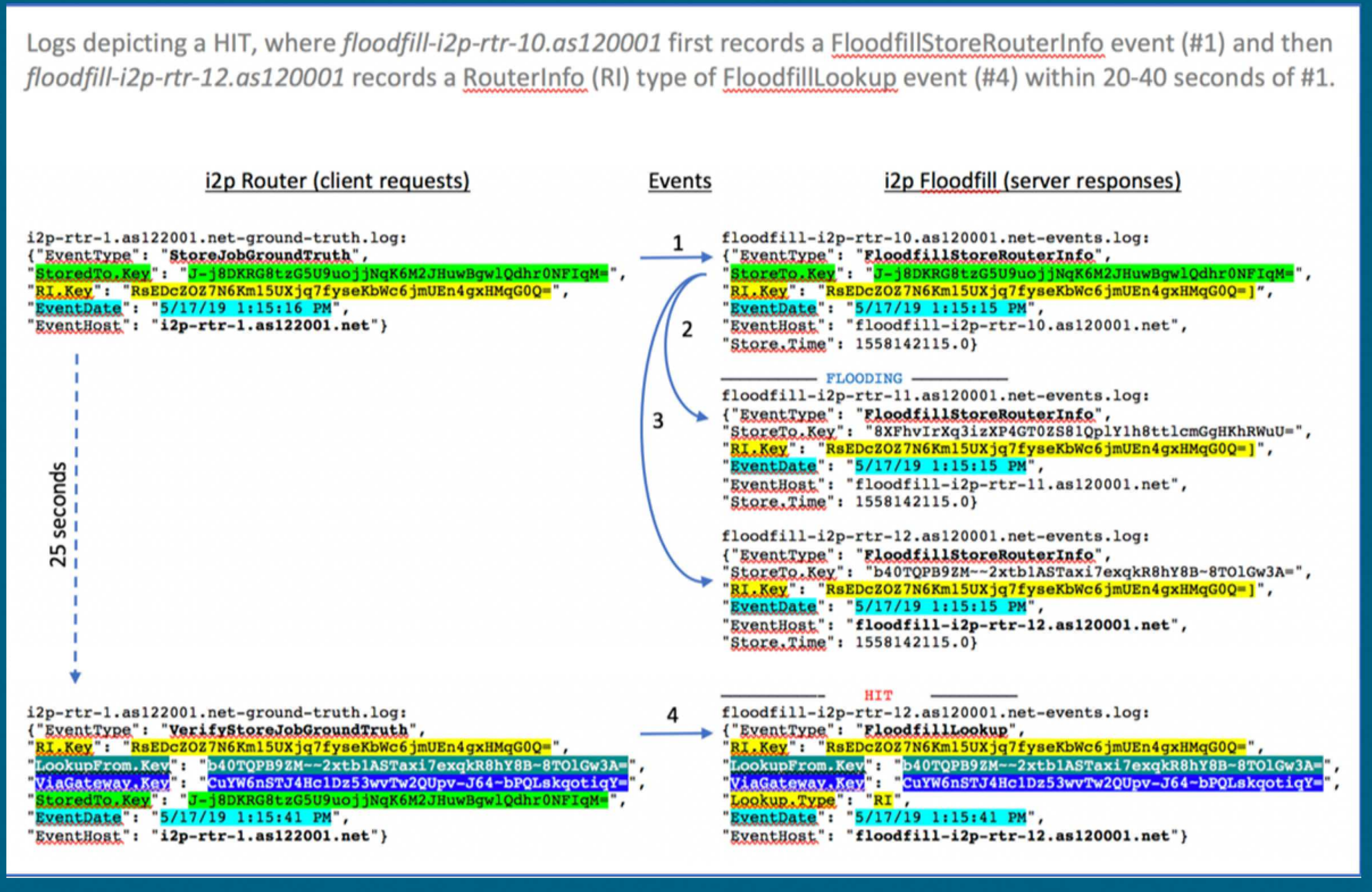
Network Uncertainty Within Cybersecurity

Corithian Williams, North Carolina A&T

Team: Thomas Tarman; 5582, Michael Stickland; 5582, Laura Swiler; 1463

Problem Statement:

Attacks within a network may be affected by factors outside of the control of the victim or adversary. The paper *Practical Attacks Against The I2P Network* (Egger et al., 2013) describes an attack capable of identifying the end node of a targeted victim's tunnels 52% of the time, which could then be monitored to reveal what sites they are visiting within the I2P network.



Logs depicting a HIT, where *floodfill-i2p-rtr-10.as120001* first records a FloodfillStoreRouterInfo event (#1) and then *floodfill-i2p-rtr-12.as120001* records a RouterInfo (RI) type of FloodfillLookup event (#4) within 20-40 seconds of #1.

i2p Router (client requests)

```
i2p-rtr-1.as122001.net-ground-truth.log:
{"EventType": "StoreJobGroundTruth",
"StoredTo.Key": "J-j8DKRG8tzG5U9uojjNqK6M2JHuwBgwlQdhr0NFIqM=",
"RI.Key": "RsEDcZOZ7N6Km15UXjq7fyseKbWc6jmUEn4gxHMqG0Q=",
"EventDate": "5/17/19 1:15:16 PM",
"EventHost": "i2p-rtr-1.as122001.net"}
```

25 seconds

```
i2p-rtr-1.as122001.net-ground-truth.log:
{"EventType": "VerifyStoreJobGroundTruth",
"RI.Key": "RsEDcZOZ7N6Km15UXjq7fyseKbWc6jmUEn4gxHMqG0Q=",
"LookupFrom.Key": "b40TQPB9ZM~~2xtblASTaxi7exqkR8hY8B~8TOlGw3A=",
"ViaGateway.Key": "CuYW6nSTJ4HclDz53wvTw2QUpv-J64-bPQLskqotiqY=",
"StoredTo.Key": "J-j8DKRG8tzG5U9uojjNqK6M2JHuwBgwlQdhr0NFIqM=",
"EventDate": "5/17/19 1:15:41 PM",
"EventHost": "i2p-rtr-1.as122001.net"}
```

Events

1, 2, 3, 4

i2p Floodfill (server responses)

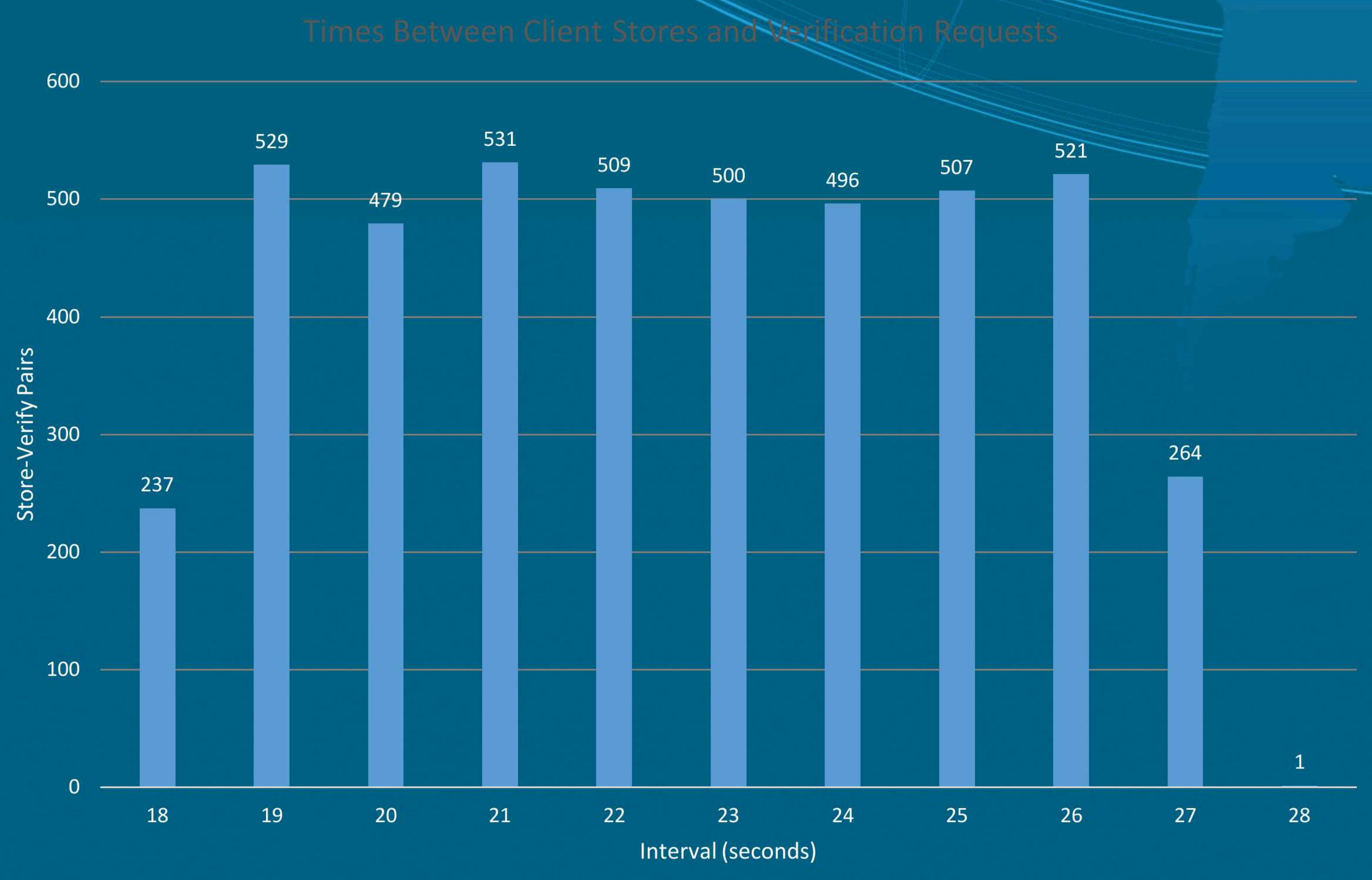
```
floodfill-i2p-rtr-10.as120001.net-events.log:
{"EventType": "FloodfillStoreRouterInfo",
"StoreTo.Key": "J-j8DKRG8tzG5U9uojjNqK6M2JHuwBgwlQdhr0NFIqM=",
"RI.Key": "RsEDcZOZ7N6Km15UXjq7fyseKbWc6jmUEn4gxHMqG0Q=]",
"EventDate": "5/17/19 1:15:15 PM",
"EventHost": "floodfill-i2p-rtr-10.as120001.net",
"Store.Time": 1558142115.0}

———— FLOODING ————
floodfill-i2p-rtr-11.as120001.net-events.log:
{"EventType": "FloodfillStoreRouterInfo",
"StoreTo.Key": "8XFhvIrXq3izXP4GT0ZS81QplY1h8ttlcmGgHKhRWuU=",
"RI.Key": "RsEDcZOZ7N6Km15UXjq7fyseKbWc6jmUEn4gxHMqG0Q=]",
"EventDate": "5/17/19 1:15:15 PM",
"EventHost": "floodfill-i2p-rtr-11.as120001.net",
"Store.Time": 1558142115.0}

floodfill-i2p-rtr-12.as120001.net-events.log:
{"EventType": "FloodfillStoreRouterInfo",
"StoreTo.Key": "b40TQPB9ZM~~2xtblASTaxi7exqkR8hY8B~8TOlGw3A=",
"RI.Key": "RsEDcZOZ7N6Km15UXjq7fyseKbWc6jmUEn4gxHMqG0Q=]",
"EventDate": "5/17/19 1:15:15 PM",
"EventHost": "floodfill-i2p-rtr-12.as120001.net",
"Store.Time": 1558142115.0}

———— HIT ————
floodfill-i2p-rtr-12.as120001.net-events.log:
{"EventType": "FloodfillLookup",
"RI.Key": "RsEDcZOZ7N6Km15UXjq7fyseKbWc6jmUEn4gxHMqG0Q=",
"LookupFrom.Key": "b40TQPB9ZM~~2xtblASTaxi7exqkR8hY8B~8TOlGw3A=",
"ViaGateway.Key": "CuYW6nSTJ4HclDz53wvTw2QUpv-J64-bPQLskqotiqY=",
"Lookup.Type": "RI",
"EventDate": "5/17/19 1:15:41 PM",
"EventHost": "floodfill-i2p-rtr-12.as120001.net"}
```

The original I2P network had around 30k nodes at the time of the study. We want to measure the accuracy across simulated I2P networks of different sizes to examine whether this 52% accuracy could vary with the size of the network.

Objectives and Approach:

- Examine logs of attacks against simulated I2P network
- Correlate client requests based on logs, authenticate against ground truth logs
- Note times of client's Store requests and corresponding Lookup requests.

Results



Using a small simulated network, the Lookup requests occurred from 18–28 seconds after their corresponding Store requests. We have created a script that is able to access the floodfill logs and find possible hits in which a client had their router info stored, and then possibly attempt to verify their storage.

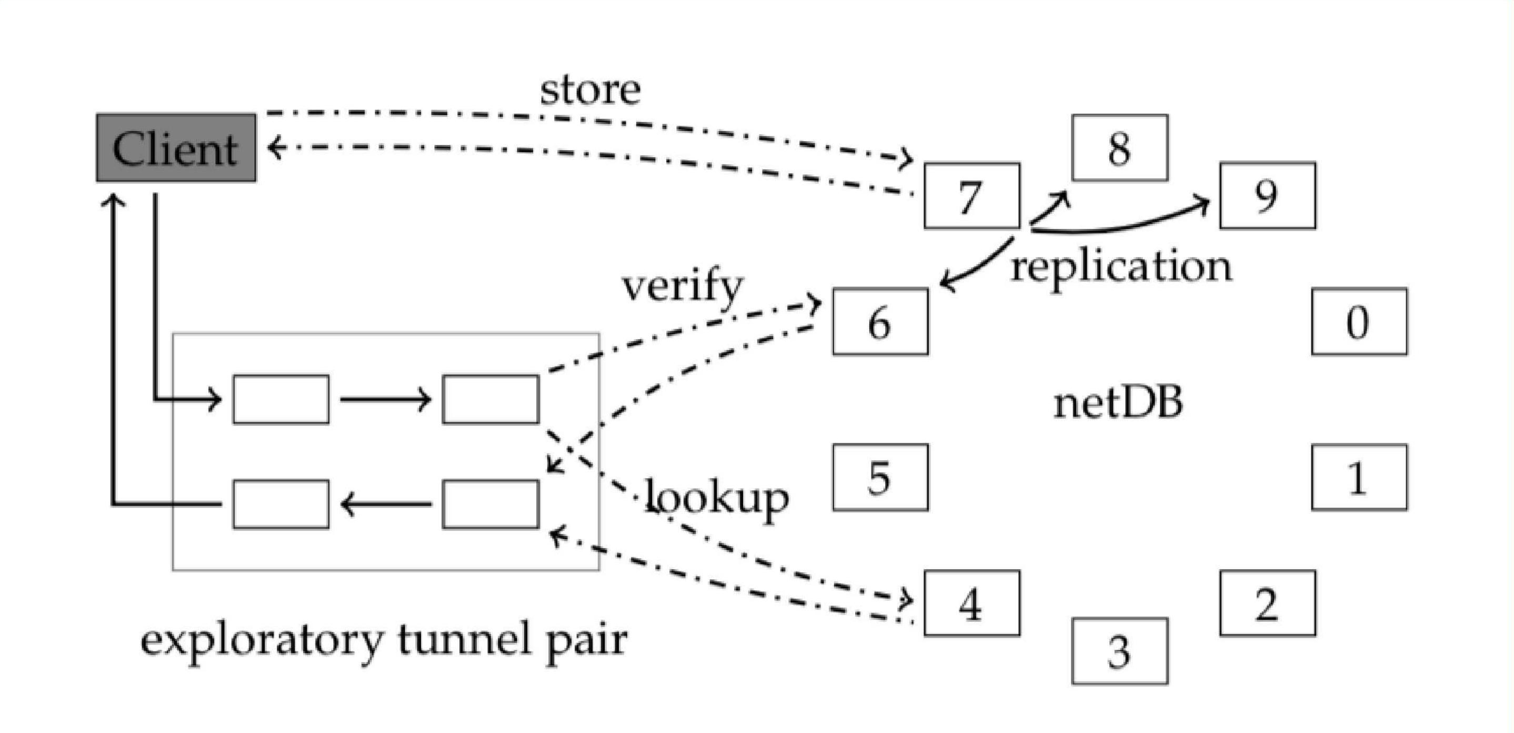


Fig. 1. Deanonymizing attack

Egger, C., et al. *Practical Attacks against the I2P Network*. 2013. Berlin, Heidelberg: Springer Berlin Heidelberg.

Impact and Benefits:

By varying factors within the network, we can examine how Uncertainty Quantification can aid us in refining the results of studies on large-scale, distributed cyber systems.

- Egger, Christoph & Schlumberger, Johannes & Kruegel, Christopher & Vigna, Giovanni. (2013). Practical Attacks against the I2P Network. 8145. 432-451. 10.1007/978-3-642-41284-4_22.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.