Advanced Topics on Privacy Enhancing Technologies
CS-523
Censorship Resistance Exercises

1 My Directory

Alice decided to build a new anonymity network similar to Tor, but with no distinction on where can a node operate, i.e. all nodes can be guard, middle, or exit nodes at the same time. Alice has not figured out how to inform users about these node's addresses handles them. By analyzing and comparing the trade-off of the following approaches, help Alice to decide how to publish nodes information. You need to consider privacy and censorship resistance (availability).

1. Alice signs the list of all nodes and ships it with the application. We assume that all users verify the checksum of the application.
2. Alice runs a mail-server and automatically responds to each mail with a list of 10 random nodes.
3. Alice runs the mail-server as before but instead of using fresh randomness for each email, she uses the sender's address as a seed.
4. Alice asks Bob and Charlie to run identical mail-servers with their respective secret key. Every user has to mail all three and check their response's signature. Only if all three emails contain the same set of servers, the user will trust them.

2 Domain Fronting

Consider the following setup in a censored country:
`software-download.microsoft.com` is allowed
`https://blocked.azureedge.net` is censored
ISPs in the country will block HTTPS packets that declare `blocked.azureedge.net` in their server name indication (SNI) field. Both services, however, are

hosted on the same infrastucture (Microsoft Azure). In order to evade the censorship and access `blocked.azureedge.net`, an internet user in the country can try to obtain the IP address of `software-download.microsoft.com` through a DNS query, and then send the following HTTPS packet to this IP:

```
TLS
SNI: software-download.microsoft.com
...

  HTTP
  GET / HTTP/1.1
  Host:  blocked.azureedge.net
  ...
```

Per the externally visible SNI the packet appears as if it is directed to `software-download.microsoft.com`, but the hope is that Microsoft Azure redirects the packet to `blocked.azureedge.net` within the same connection. This censorship circumvention technique is called domain fronting.

1. What server-side conditions enable domain fronting? How can Microsoft Azure prevent people from using domain fronting through their websites?

2. How can a censor prevent domain fronting? At what cost?

3 Decoy Routing

Alice wants to access a censored site `blocked.com`, in the presence of a state-level adversary, Eve, that is monitoring her traffic. She makes use of a decoy routing system, which routes her connections to the uncensored site `notblocked.com` to `blocked.com`. Bob is another user who wants to access `notblocked.com`. He doesn't use the decoy routing system.

Consider Eve as a passive adversary – such an adversary only monitors client traffic and does not attempt to inject or modify traffic.

1. How can Eve use traffic analysis to determine if Alice was using a decoy router?

2. Would it be possible for Alice to reduce the impact of timing analysis performed by Eve?

3. Consider Eve as an active adversary now. Eve has recorded Alice's and Bob's TCP packets sent to `notblocked.com`. She decides to replay this connection over a route that does not contain decoy routers. Does she see a difference in the response for Alice's and Bob's connections? Why?

4. Consider Eve as an active adversary that can switch the first hop of the paths that Alice and Bob's messages take. Alice and Bob have established connections to `unblocked.com`, when Eve decides to implement a path switch. The new path does not contain decoy routers. How are their connections impacted? Would Eve be able to determine whether Alice is using decoy routing?