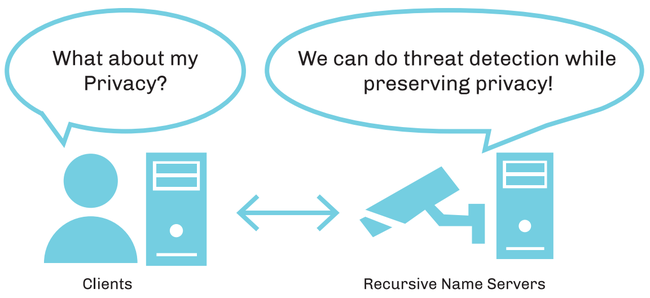
PRIVACY FRIENDLY

Threat Detection Using DNS

Gijs Rijnders / gijs.rijnders@surfnet.nl

MOTIVATION

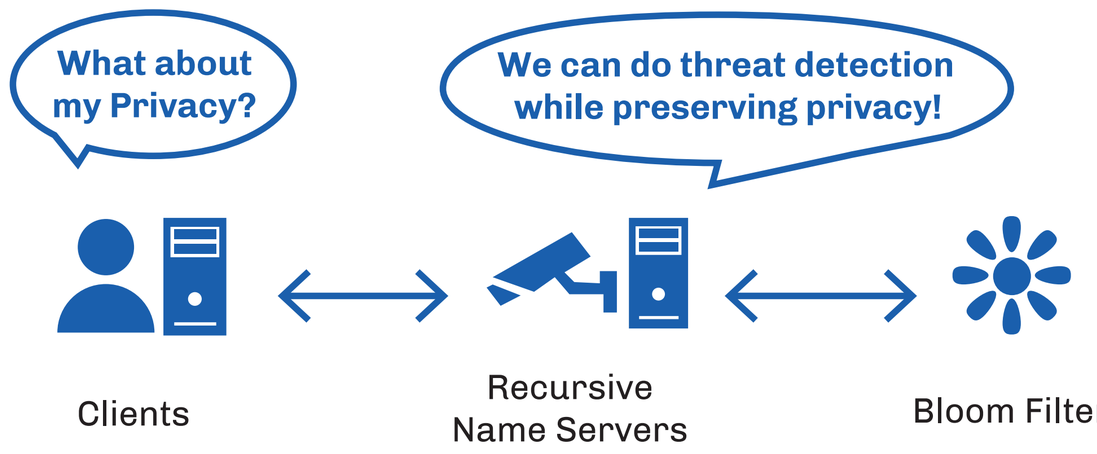
DNS is a useful tool in threat detection. However, monitoring DNS activity is very privacy infringing. We can perform threat detection using DNS while preserving the privacy of users.



General Data Protection Regulation

Solution: Bloom Filters

DNS queries are stored in a Bloom filter. We can ask the Bloom filter whether a DNS query is stored.



BENEFITS:

• Original information is not stored • No enumeration of stored information • Only exact information can be searched for • No correlation between users and queries • Historical lookups are possible • Space–efficient storage solution

EVALUATION OF SOLUTION

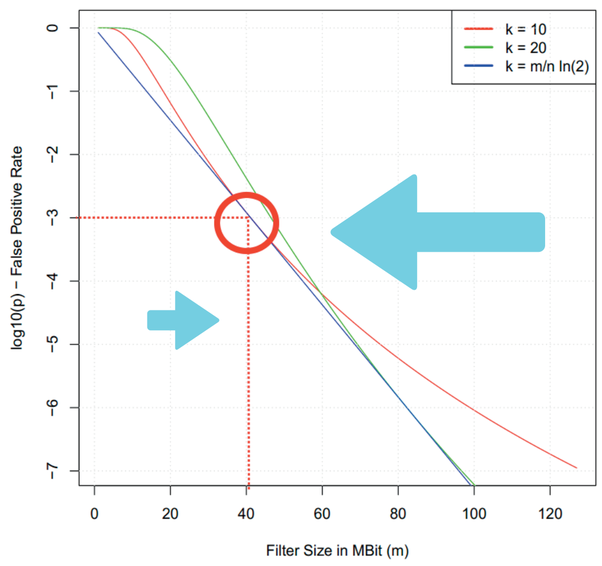
Bloom filters False Positives

Bloom filters introduce False Positives in detection. The FP–rate is low, and configurable using two parameters.

Image source: https://continuousimprover.com/2015/06/false-positives-and-semantic-versioning.html

False Positive Rate

Bloom Filter False Positive Rate: n = 3M

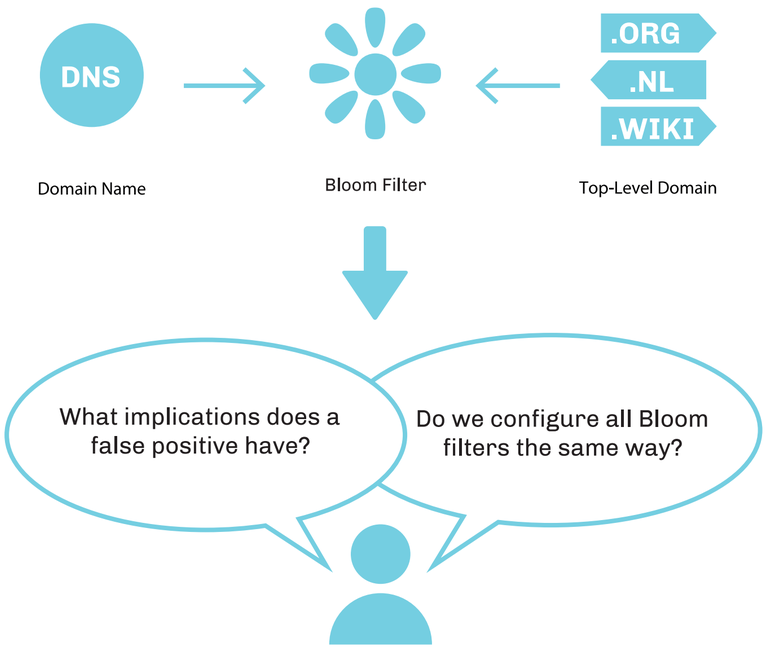


3M unique domain names per filter; False positive rate of 1/1000; Bloom filter size ~ 5 MB

Number of unique domain names is important for filter dimensions.

DNS storage in Bloom filters

What DNS Information to store in Bloom filters?



NETWORK THREAT DETECTION

We obtain Intel from our community, and want to use that for detection in our network. So far we did not have a way to do so, but with the Bloom filters, we can! That brings us a step closer to proper threat detection in our network.

BOOTERS

Students have launched DDoS attacks on their institution to have online exams cancelled. Such DDos attacks are often inside jobs. Students purchase them from so called Booter websites, offering DDoS–as–a–Service. The Bloom filters allow us to verify whether we are dealing with an inside job or not.

SPAM FILTERING

We offer our constituency mail filtering services, which use blacklists among other things. Using Bloom filters, we can find out whether blacklisted domain names are also queried by an institution.

Acknowledgements:

My Colleagues @SURFnet | My Supervisor @TU/e: Luca Allodi | Design help: @MOME: Bence Kiss