A castle built on sand : ‘stochastic traffic padding’ – a paper review.

Camille Akmut

Abstract

A paper from PETS 2019 is reviewed. A general case.

Apthorpe et al. “Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping”

Even with encryption IoT devices reveal a lot about a person. These authors focus on information exposed by meta-data e.g. traffic rates.

“We demonstrate that a passive network observer (e.g., an Internet service provider) can infer private in-home activities by analyzing Internet traffic from commercially available smart home devices even when the devices use end-to-end transport-layer encryption.” they announce in their abstract.

See in particular their informative figure 1 (‘Traffic rate to and from a Sense sleep monitor over a 12-hour period. User activities are clearly visible as traffic spikes.’) for data, reproduced below.

They then review various existing solutions, e.g. VPN,

Another technique for preventing activity inference is to tunnel all smart home traffic through a virtual private network. A

VPN wraps all traffic from an endpoint in an additional transport layer, aggregating it into a single flow with the source and destination IP addresses of the VPN endpoints. This aggregation could make it difficult to determine which variations in the overall traffic rate observed from outside the VPN correspond to user interactions with individual devices.¹

and weaknesses they perceive in them, before turning to their own.

They introduce ‘stochastic traffic padding’ (STP), “*a traffic shaping algorithm which uses intermittent periods of traffic padding to limit the information revealed about user activities*” that they propose.

We disagree with what appears to be their general outlook on IoT : their title implies they want to make “the Smart Home” more private.

But, as they themselves point out these devices largely are outside of user control and live a life of their own :

Many smart home devices have always-on sensors that (1) capture users offline activities in their living spaces and (2) transmit information about these activities outside of the home, typically to cloud services run by device manufacturers.²

Or is it perhaps that they expect these manufacturers to suddenly find their good Samaritan souls back?

Was their specific method (padding has been employed in cryptography for a long time) really the missing key these companies did not possess? And, that none of their competent computer scientists and engineers would have been able to come up with? This seems doubtful.

The truth is IoT has brought us little, if anything at all. It has all the typical characteristics of a ‘false revolution’.

It created needs where there were none and increased our (emotional, psychological, and otherwise) dependency on largely and mostly useless technology, in fact gadgetery.

—

Rarely do we find answers to the large questions in computer science literature, and that is perhaps its greatest fault.

Perhaps that is also not its role, some will argue.

In any case, this science is too immature for anyone to say one way or the other. But, certainly :

No amount of equations will make up for a weak philosophical foundation, basis; or the absence of such discussions.

A castle built on sand.

<https://arxiv.org/abs/1812.00955>
Conference : PETS 2019.

¹Subsection 5.2.

²Introduction.