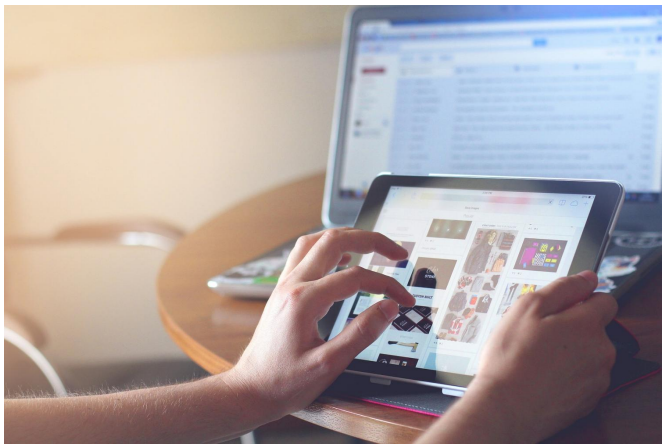
Approach enables experts to look beyond IP in cyber security investigations

5 September 2017, by Alan Williams



Credit: CC0 Public Domain

A technique which enables digital forensic investigators to assess an individual's internet use rather than simply focusing on traffic using Internet Protocol (IP) addresses has been developed by cyber security experts at the University of Plymouth.

Traditionally, network examiners have had to concentrate on IP analysis for any digital investigations as it has been the only characteristic available, when in reality the questions that an investigator wishes to ask are of the individual not the computer.

With the growth in tablets, smart phones and smart watches - where IP addresses are constantly changing - it is no longer a reliable and consistent means of understanding traffic from an individual user.

Now academics from the University's Centre for Security, Communications and Network Research (CSCAN) have developed a means to identify individual users' behaviour from network traffic using only the metadata of the traffic rather than the overall payload.

This means privacy of user information is maintained and the approach is viable even with end-to-end encrypted communications, which are commonplace across a wide range of Internet services.

In tests involving 46 users over a two-month period, the application achieved average recognition rates of 90 per cent, with some users experiencing recognition performance of 100 per cent.

Nathan Clarke, Professor in Cyber Security and Digital Forensics at the University, led the study alongside Research Fellow Dr Fudong Li and Professor Steve Furnell, Head of the University's School of Computing, Electronics and Mathematics.

Professor Clarke said: "The prevalence of the internet and cloud-based applications, alongside technological evolutions, has resulted in users relying upon greater network connectivity - and as a result generating more traffic - than ever before. And while Internet Protocols provide a certain level of information, finding a way to understand what users are doing rather than simply machines has long been the holy grail of network analysis. We believe this new approach has the potential to do that, providing a more detailed picture of an individual's internet use but also helping to enhance cyber security in the future."

The study, published in *Computers & Security*, was carried out as part of a four-year collaborative project funded by the Engineering and Physical Sciences Research Council (EPSRC).

In total over the two-month period, around 112GB of IP header information was accumulated (comprising 1.38billion individual interactions, or packets). This included information such as the date and time, sender and receiver's IP address, the packet length and the type of traffic.

But when the Plymouth application focusing on metadata was applied, it reduced the number of packets relating specifically to the 46 participants to under 5.5million.

The consequence of this, the study says, is an enormous reduction - more than 96 per cent - in the volume of traffic and investigator has to analyse, allowing them to focus upon a particular suspect or enabling them to disregard traffic and focus on what is left.

Professor Clarke added: "These results have presented us with a series of analyses that show the use of user interactions are a reliable means of creating a behavioural profile. We are already expanding on this work, and looking at ways to make it more applicable to digital forensic investigators while endeavouring to make the internet a safer place for everyone."

More information: N. Clarke et al, A novel privacy preserving user identification approach for network traffic, *Computers & Security* (2017). DOI: 10.1016/j.cose.2017.06.012