Opendium
e-Safety

I raised this issue following UKIGF2019, and had some useful discussions with Eva Ignatuschtschenko and Tom Rodden from the Department for Digital, Culture, Media & Sport. I would like to propose this issue for wider discussion at UKIGF2020.

Much of the discussion during UKIGF2019 revolved around the introduction of DNS-over-HTTPS, but this is just part of a wider issue. The thrust of our concern is threefold:

- The design of end user devices is under the control of a handful of businesses, who are in a position to unilaterally impose new policies upon the users. The phone/tablet market is dominated by Google (Android) and Apple (iOS), whilst the laptop/desktop market is dominated by Microsoft (Windows), Apple (OS X) and increasingly Google (ChromeOS).

  The problems described in this document are also endemic to platforms in which a single vendor has control over both the client and server. For example, where the Facebook phone app, rather than a standard web browser, is used to access Facebook.

- There isn't adequate multi-stakeholder discussion prior to imposing new privacy focused technologies or policies, and there is an unwillingness to reach a compromise. After the introduction of new technologies or policies, these large businesses are unwilling to enter into a discussion with stakeholders who are being negatively impacted by the change.

- Decisions over privacy are being taken out of the hands of the users and businesses who are buying and using these devices, and are instead being imposed upon stakeholders by the platform vendors.

As I'm sure you're aware, schools in the UK have a statutory obligation to undertake appropriate filtering and monitoring of their students' internet use for safeguarding purposes. We supply UK schools with systems to help them with this task. We're a small, but established vendor, and I think the comments below will largely mirror those of other online safety vendors of all sizes.

As with filtering offered by ISPs, schools rely on coarse filtering of HTTPS traffic by blocking access based on the web site's host name. Our systems do this by examining the SNI contained within HTTPS/TLS handshakes, but some other vendors do this through DNS. Schools usually go beyond this level of filtering by also decrypting ("man in the middling") HTTPS traffic to do fine-grained filtering and monitoring.

In order for the school's filter to decrypt HTTPS traffic, the user must install a certificate on the client device, which authorises the decryption. This should be done with the user's full knowledge and the different operating systems have various ways of protecting against certificates being installed surreptitiously. For, example, Android pops up a reminder that such a certificate is installed each time the device is booted.

As well as schools' statutory obligations, schools and businesses alike also have a desire to be able to scan traffic at the edge of the local network to detect and prevent malware infections and the ex-filtration of confidential data.

Here are a few examples of the problems that we have observed:

- Most of the social networks' apps employ certificate pinning, which prevents HTTPS decryption. This is obviously a concern for schools, who are implementing Bring Your Own Device networks for students. They have to make a choice whether to allow completely unfiltered and unmonitored access to these services or block them entirely.

  Twitter, in particular, allows users as young as 13 to use the service, but hosts a considerable amount of pornographic content which is unsuitable for users of that age. There is no mechanism within Twitter to allow schools to restrict access to inappropriate content whilst still allowing access to child-friendly content..
- In 2016, Google announced that user-installed certificates would no longer be trusted by Android apps, largely defeating HTTPS decryption entirely. In fact, modern versions of Android do not work if connections to https://www.google.com are being decrypted, which prevents schools from filtering or monitoring Google web searches. This affects both personal devices and MDM managed school-owned devices, and takes privacy decisions out of the hands of end users, schools and parents.
- In 2019, Apple changed their policies regarding certain iOS APIs and banned a number of parental control apps from their app store as a result. This decision was later reversed, but demonstrates how decisions are being taken out of the user's hands.
- Numerous schools and online safety suppliers across the world have filed bug reports against Android explaining the problems that the policies are causing. All of these reports have simply been closed or ignored by Google without discussion.
- We have reached out to a number of the platform vendors, and through our contacts at the IWF, we have reached out to Google. We have been roundly ignored in all cases.

- HTTPS/2 is now being widely deployed and includes a "connection reuse" mechanism. Although intended to improve the speed and responsiveness of websites, it does also impact filtering and monitoring.
- As discussed at UKIGF2019, DNS-over-HTTPS is being introduced and encrypted SNI is a proposal being incorporated into TLS 1.3. These are both of concern to online safety suppliers, and, depending on the exact details, are expected to become a significant problem when combined together.

Whilst improved privacy for adults is certainly welcome, the fact that some users are children is being completely missed. The refusal to discuss the issue prevents the platform vendors from understanding the problems and reaching a solution.

In the UK, we recognise that children are not capable of being completely responsible for their own welfare, which is why their parents and schools are held legally responsible for their safety. Whilst their guardians shouldn't have an absolute right to invade a child's privacy, it is impossible to protect a child who is given complete privacy. There is a balance point somewhere in the middle, and that fundamentally should be determined by parents, schools and children themselves; not by big corporations or even governments.

None of these technologies are inherently bad, but they are being deployed without proper consultation and in a way that takes the choice away from the end user. We very much feel that vendors need to put choice back in the hands of the users, and engage with concerned stakeholders instead of simply ignoring them. The attitude that more privacy is always better is simply not true, especially when it comes to people who are, in the eyes of the law, not capable of being fully responsible for their own safety.

Steve Hill

Technical Director, Opendium