TEMPLE GARDENS 3 Temple Gardens

Is PGP still 'safe'?

Ahead of rumours that the software is about to be hacked, Tim Forte looks at the development of the encryption program Pretty Good Privacy software and how this can impact on the availability of data communication evidence.

When did Pretty Good Privacy software first appear? This decade? Last? No, 1991!

PGP is an encryption program that provides cryptographic privacy and authentication for data communication. It is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. PGP and similar software follow the OpenPGP, an open standard of PGP encryption software, for encrypting and decrypting data.

Email is a plaintext communication medium whose communication paths are partly protected by Transport Layer Security (TLS), and previously by Secure Sockets Layer (SSL, the predecessor protocol to TLS). For people in hostile environments (political activists, journalists and whistleblowers for example) who depend on the confidentiality of digital communication, this may not be enough. Powerful attackers such as nation state agencies are known to eavesdrop on email communications of a large number of people. To address this, OpenPGP offers end-to-end encryption specifically for sensitive communication in view of these powerful attackers. S/MIME is an alternative standard for email end-to-end encryption that is typically used to secure corporate email communication.

The use of PGP by "innocent" actors, such as journalists, demonstrates the trite point that there is nothing illegal *per se* in owning or using a PGP device, it is just that, in concert with other evidence, the use of PGP may add to the Crown's case against a defendant. Of course, as with an iPhone PIN etc, once the Police obtain a s.49 RIPA order from the Court, they can request an individual to provide a PIN or Password or that they unlock their device. Refusal so to do can make the individual liable to another criminal offence pursuant to s.53 RIPA, but that is the extent of the liability under RIPA.

The same concerns for confidentiality and security in a "hostile environment" apply to organised crime – they too are subject to "powerful attackers" such as state criminal investigation agencies, e.g. Police, National Crime Agency, Border Force, HMRC in the UK, and FBI, Interpol, Europol internationally. With the increasing ability of law enforcement over the last few decades to access "normal" communications – imaging and downloading seized "vanilla" handsets, RIPA authorised intercepts, Call Detail Records and subscriber checks from Service Providers – the organised criminal wanted a more secure way to keep in contact with his confederates.

Similarly, the rapid increase in terrorism offending in recent years has also led to an exponential increase in the number of available "encryption" mechanisms on the market – from the familiar, WhatsApp, to the more niche, Signal, Wire, Telegram and Wickr to name but a few.

For years now, practitioners in heavyweight criminal defence, dealing with Organised Crime Groups (that favoured mantra of numerous prosecutors up and down the land), have been faced with PGP issues – in the main, the use of PGP encrypted devices, the possession of which has come to be a species of *res ipsa loquitur* proof of guilt. Then came Encrochat – a premium service providing PGP encryption enabled devices with separate drives or volumes, between which the user can seamlessly switch, to enable both "work" and "personal" use on the same safe device.

The next major development came with the news in 2015 that the Netherlands government were devoting substantial funds to enhance data security, in a clear signal that they were intending to seek to break the digital padlock placed on criminal communication by PGP and Encrochat *et al*. It has been seen how State Agencies have pressured large tech companies to grant them access or a "backdoor" into their devices or software (viz Apple and iPhones). This was merely the next logical step in the tech arms race that has been running for decades – as fast as the criminals enhance their protections and security, the police (or whoever) enhance their hacking / codebreaking abilities, meaning the criminals need to up their game consequentially.

And thus it came about that the Dutch announced in mid-2016 that they were gaining some success in breaking into PGP devices and software. Indeed, in September 2016, a long running drugs trial, Operation Petral, was coming towards the end of the Crown's case, at Manchester Crown Court, when suddenly, new evidence was served. I was leading Counsel for one of the principle two defendants, and recall the Prosecution Silk turning to us with a big grin on his face, and saying "We have some more material for you… We've broken PGP!" That was the beginning of the end for the defendants in that trial.

Was it the beginning of the end for PGP though? Is PGP still secure?

The security of PGP is predicated upon the "public key" and "private key" generated by the recipient of any communication. If "A" wants to send an encrypted email to "B", "B's" device generates a "public key" and a "private key". The "public key" is sent to "A's" device, which then sends the email encrypted with the "public key" that can only be unlocked, i.e. decrypted, by the corresponding "private key" that "B" has retained.

Without the "keys" the system remains secure, that is the theory. The Dutch High Tech Crime Unit (NHTCU) have not vouchsafed how they cracked the PGPs that they did, but it is thought that the success stemmed from the access they had (provided by permission from a Canadian Judge) to the servers of the Service Providing Company – Ennetcom. Once they had access to those servers, any keys stored on those servers would, in all likelihood be saved there "in open" and therefore accessible. The PGP system is only as secure as the keys. Once the keys are in the hands of the police, then the unlocking becomes, relatively, trivial.

The analysis of the Ennetcom servers was not quite "brute force" but a specialised search engine, Hansken, was deployed, that would analyse all files, folders, deletions, packets, sectors etc that could be found, creating its own indexing system, and then, much as in aged-old cryptanalysis techniques, it lit upon certain key words, likely to be frequently reoccurring

– such as “drugs”, “murder”, “kill” – in this context, and sought out those repetitions. It was of some help for the cryptanalysis that the metadata of the devices saved to the servers was not encrypted and thus easier to analyse.

Another more general vulnerability of the PGP system was that which has come to be known as the “Efail” – where an encrypted email is sent with pictures or extrinsic HTML links, these are not properly encrypted or not fully so, and are therefore vulnerable to attack outside of the “public” “private” key security bubble. That is, however, a very specific vulnerability that can be avoided by not sending any HTML based material in the messages.

Indeed, those behind PGP claim that it is not, truly, a vulnerability of the opensource PGP software but rather of its implementation by some providers – Protonmail claim they are unaffected by the “Efail” vulnerability, and state that the issue lays in some providers “PGP libraries” and “plug-ins”.

PGP is not a particularly user-friendly system, it is cumbersome and inflexible, but despite the incursions into its security – via the Ennetcom server, via the unencrypted metadata or the Efail vulnerability – it is still the most secure email structure out there, and will doubtless continue to be used by those needing to do so. It may be that the more discerning user will be picky about which exact provider they use – e.g. avoiding those with susceptibilities like Ennetcom, preferring the more secure, such as Protonmail – but as ever this is a fast evolving and developing tech arms race.

In terms of recent developments, only this week (at time of writing), 22nd June 2020, there have been ever growing rumours circulating that Encrochat are closing up shop, after external actors (law enforcement agencies, be it Police, NCA, GCHQ or other, believed to be from the UK) have been starting to brute force hack into their customers’ devices… So, what will be the next level for the encrypters? Watch this space.

Tim Forte
3 Temple Gardens