WPA2 and why it matters to you

The stakeholders who pioneered Wi-Fi, the quick and reliable method of transmitting and receiving data wirelessly, formed an alliance which went on to own and control the ‘Wi-Fi Certified’ registered trade mark, the use of which it only allows for equipment that meets very specific criteria. From 2006 onwards, this meant that to have products designated as Wi-Fi Certified, they had to make use of a specific security certification protocol called Wi-Fi Protected Access II (‘WPA2’). Use of WPA2 has become so commonplace that it would actually be difficult to find Wi-Fi transmissions occurring without it.

Discovery of the WPA2 security flaw

In October 2016, security researchers from the University of Leuven uncovered a flaw in WPA2 that established a significant vulnerability in the protocol. The researchers referred to the vulnerability as a Key Reinstallation Attack (‘KRACK’) and the discovery was widely reported in the media, often in a somewhat exaggerated manner, such as with the headline: ‘Almost every Wi-Fi connection in the world has been hacked!’ Nevertheless, the KRACK vulnerability raises some interesting technical and legal questions which businesses and organisations need to consider and deal with. This is especially so for those impacted by data protection and other data legislation imposing data security obligations, particularly those impacted by the impending EU General Data Protection Regulation (‘GDPR’), which will apply in full from 25 May 2018.

Vulnerability

The encryption used in WPA2 is not broken and not all communications are automatically laid bare. It has, though, been identified that there is a vulnerability in relation to how encryption keys are exchanged as part of setting up the secure communications. That weakness can be exploited by an attacker to trick victim machines into reinstalling keys that are already in use, by manipulating and replaying handshake messages. Where successful, this novel attack technique can then be used to intercept and read information that was previously assumed to be safely encrypted by WPA2, which could include sensitive information such as credit card numbers and passwords, confidential or proprietary information, or other personal data. In terms of access to and potential misuse of those details, this has serious potential consequences for individuals, businesses and organisations affected. In terms of the body legally responsible for the security of the affected data, there can be serious compliance consequences. These include regulatory enforcement action and sanctions, including fines (all made public); individual compensation claims by affected individuals, possibly on a class action basis; breach of contract claims from commercial partners; and damage to reputation which may impact share price, goodwill and future ability to win business.

Limitations

Despite the media reports, the ability to exploit the KRACK vulnerability is limited by several factors.

Physical proximity limiter
An attack can only occur if an attacker or eavesdropper is within sufficient range of the victim network. The stereotypical hacker is not going to be able to use this attack against you, unless they are very close to the victim’s machine, making the physical proximity limiter significant.

Secondary cryptographic security limiter
The vulnerability appears to be limited to communications where the relevant WPA2 protocol has not been suitably enhanced by an additional overlaying security layer. The internet has evolved
to be very secure and most internet traffic is protected by more than one layer of security. In those cases, although communications might still be intercepted and the WPA2 security stripped away, the transmissions may remain safely encrypted using a cryptographic protocol at the Transport or Application Layer, such as HTTPS, or through the use of a Virtual Private Network (‘VPN’).

Effective patching limiter
The researchers uncovered the vulnerability and reported it to vendors before the details were publicly released, in order that patches could be prepared to remedy the issue. Vendors have been providing patches in software updates which should help reduce the risk of attack.

Legal position
Before breathing a sigh of relief about the limiters and assuming there is no ongoing issue, we suggest you read on and, if not already in hand, make some checks.

Security principle
In the EU, current data protection laws, such as implemented by the UK’s Data Protection Act 1998 (‘DPA’), have a data security principle, imposing an obligation on data controllers to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data. Although the security principle continues under the GDPR, rebadged ‘integrity and confidentiality’, its impact spreads and the importance of compliance with it increases.

The GDPR
The GDPR explicitly references taking account of the ‘state of the art’ and the likelihood of risk and its impact, as well as the need to ensure ‘resilience’ of processing systems and services. It also specifically requires an appropriate ‘process for regularly testing, assessing and evaluating the effectiveness’ of security measures. In addition, not only does this more explicit security obligation affect data controllers, but it will from May 2018 also directly bite on data processors subject to the GDPR. As a result, both customers using software and hardware and the suppliers of those products must comply with this obligation.

Compliance becomes more important as the other big changes in the GDPR are mandatory breach reporting of security breaches affecting personal data to the relevant data protection authority, with limited exceptions, combined with the potential for the regulator to issue a fine of up to 2% of annual global turnover, potentially at group level for a security breach.

Effect of a failure to patch
The WannaCry ransomware attack targeted vulnerabilities that Microsoft had actually already sought to resolve by way of patches introduced two months previously. The attack was therefore arguably avoidable and as a result, potentially, so too was much of the estimated $6 billion cost of the attack.

While that was troubling enough, the NotPetya ransomware attack then exploited the exact same vulnerability a month later. Businesses should have been aware of the original WannaCry issue by then and would have a challenge explaining why they had not appropriately dealt with that vulnerability after three months. That NotPetya worked at all is demonstrative of a major issue in reacting to news of security vulnerabilities and patches.

Regulatory enforcement action and lessons learned
What does a data protection authority think of security breaches in such circumstances and how will it react? Although there are no regulatory decisions yet on data security under the GDPR, guidance and experience under the current legal security principle should at least be persuasive under the GDPR and help us prepare for it. Regulator decisions to date on security obligations and breaches are therefore likely to indicate the minimum that will be expected under the GDPR.

Already there have been reported cases and fines triggered for breaches in the context of published software vulnerabilities and patches. In one case, a business failed to implement appropriate security over a database that held the personal data (including financial information) of over 100,000 customers. This was duly accessed by a hacker, who gained access through exploiting a known vulnerability that had not been patched. This was found to be a breach leading to a penalty of over £250,000. A similar case arose in relation to another vulnerability, when an organisation took just over three months to install a patch released to fix the issue. In that time, a hacker was able to exploit the vulnerability and access data. The data protection authority imposed a six figure penalty for these failings.

We can learn several things from these decisions and from our experience of assisting clients to manage similar cyber attacks.

...
The GDPR explicitly references taking account of the ‘state of the art’ and the likelihood of risk and its impact, as well as the need to ensure ‘resilience’ of processing systems and services.

• The regulator clearly expects businesses and organisations to be aware of security flaws about which they are alerted and to act on them.
• Organisations and businesses can take a considerable amount of time to implement patches, often two to three months and sometimes longer. There can be sound reasons why a patch cannot immediately be adopted across a large and complex IT estate whilst the implications of it are considered and worked through, but in the event of an attack in the meantime, it may be difficult to convince a regulator that appropriate prompt action had been taken.
• If data security and maintenance is outsourced internally or externally, checks are still required to ensure the provider has implemented the patches and in a timely manner.
• Even if no data is stolen or lost, the mere access to the personal data by an unauthorised person involves a breach of security.
• We have dealt with a number of breaches where between a flaw being identified and a patch implemented, there has been a data exfiltration as above. In each case, the business checked and initially thought that even if there had been a compromise of security, there had been no loss of data. In each case, on later, deeper checking, it was found that serious data exfiltration had occurred and the breach then had to be reported and affected individuals informed.

What measures can be taken to reduce risk?
The patches made available to counter the WPA2 issue should normally have been implemented by now. Many users will now find that installing the most up-to-date versions of applications, browsers and wireless router software will remove the vulnerability from the network altogether. It will be hard to convince regulators that failing to deal with a well-known security vulnerability, especially where an appropriate fix is likely to have been released and is available normally at minimal cost, meets the appropriate security standard required.

Businesses and organisations should check to make sure this action has been completed and if not, take appropriate steps urgently. In addition, but especially where a patch cannot be applied or adopted, can hardware be replaced, or can use be made of additional layers of security and encryption, such as through a VPN? Continuing use of areas remaining exposed should be minimised.

The process and timing of noting and responding to such security updates should be considered. How long is it taking to become aware of such updates once made known? How long is it taking to adopt patches released once available? Are they applied to key areas urgently? How can security and awareness of attacks and data exfiltration be improved pending patch application? If there are delays or problems, why is this and what can be done to reduce them?

Suppliers designing software and hardware should use the greater awareness to avoid repeating the vulnerability or similar issues. In addition to suppliers becoming directly liable for security under the GDPR, there is a new legal obligation under the GDPR to ensure that use of personal data is subject to ‘privacy by design and default,’ to build in data minimisation and security from the outset for all systems and processes. Buyers will in future be far more concerned to receive assurances about data security and data controllers must ensure products and systems meet this standard.

Post-reform landscape
Risks caused by the KRACK vulnerability, first revealed in October 2016 but not widely known until almost a year later, should be largely resolved by the time the GDPR applies in full in 2018. Nevertheless, many data controllers will have simply neglected to implement the patches necessary to secure the personal data held and that might still see regulatory enforcement around this vulnerability. In the event of a KRACK-based incident post May 2018 under the GDPR regime, it will be interesting to see how regulators respond and their decision will give a valuable indication of the real extent of obligations in this area.

1. https://www.wi-fi.org/who-we-are/history
5. Article 5(1)(f) of the GDPR
8. Known as Eneral1Blue and reputed to have been a vulnerability previously used by the NSA and released ‘into the wild’ as a result of the Edward Snowden data dumps.