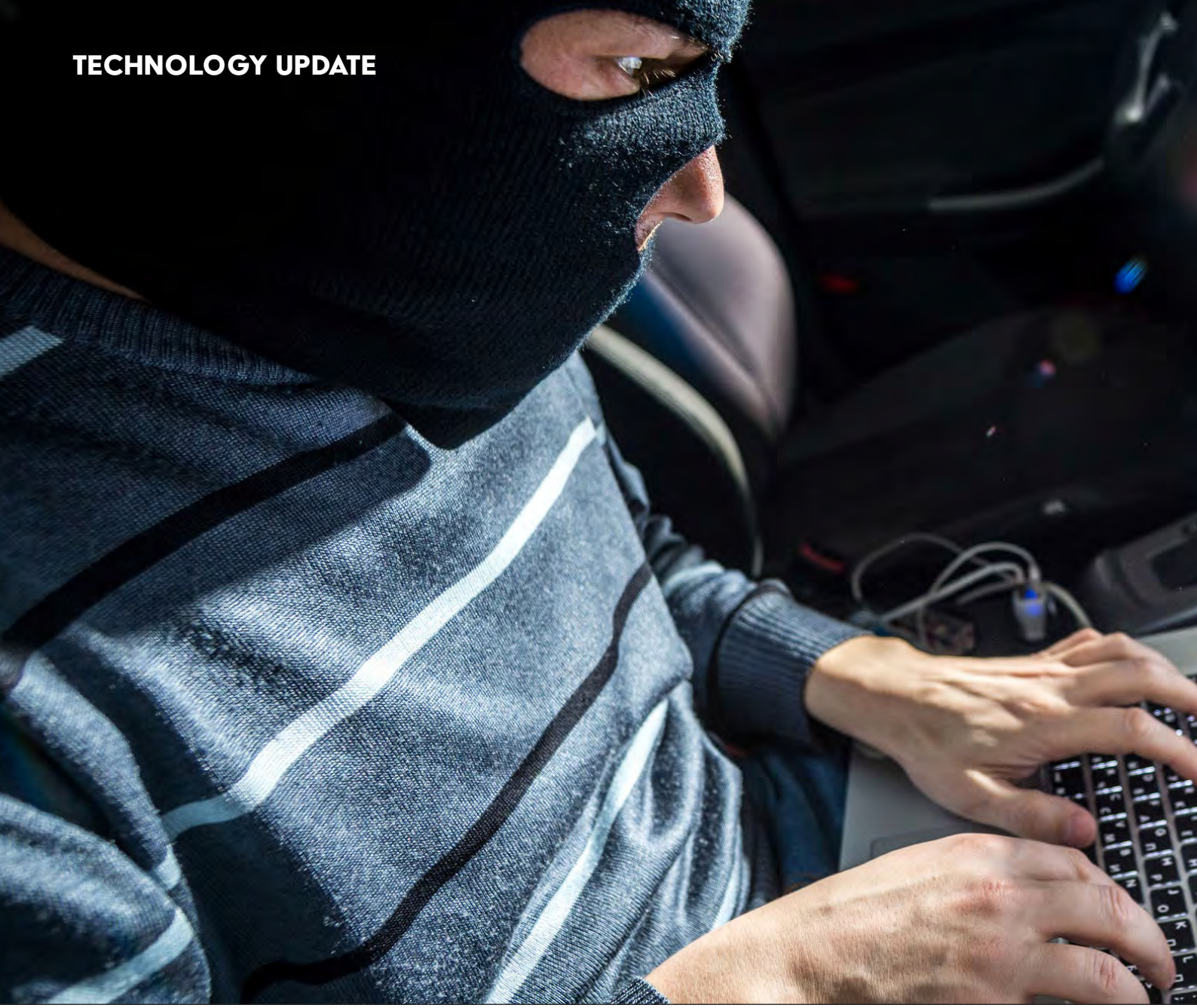


Technological thievery

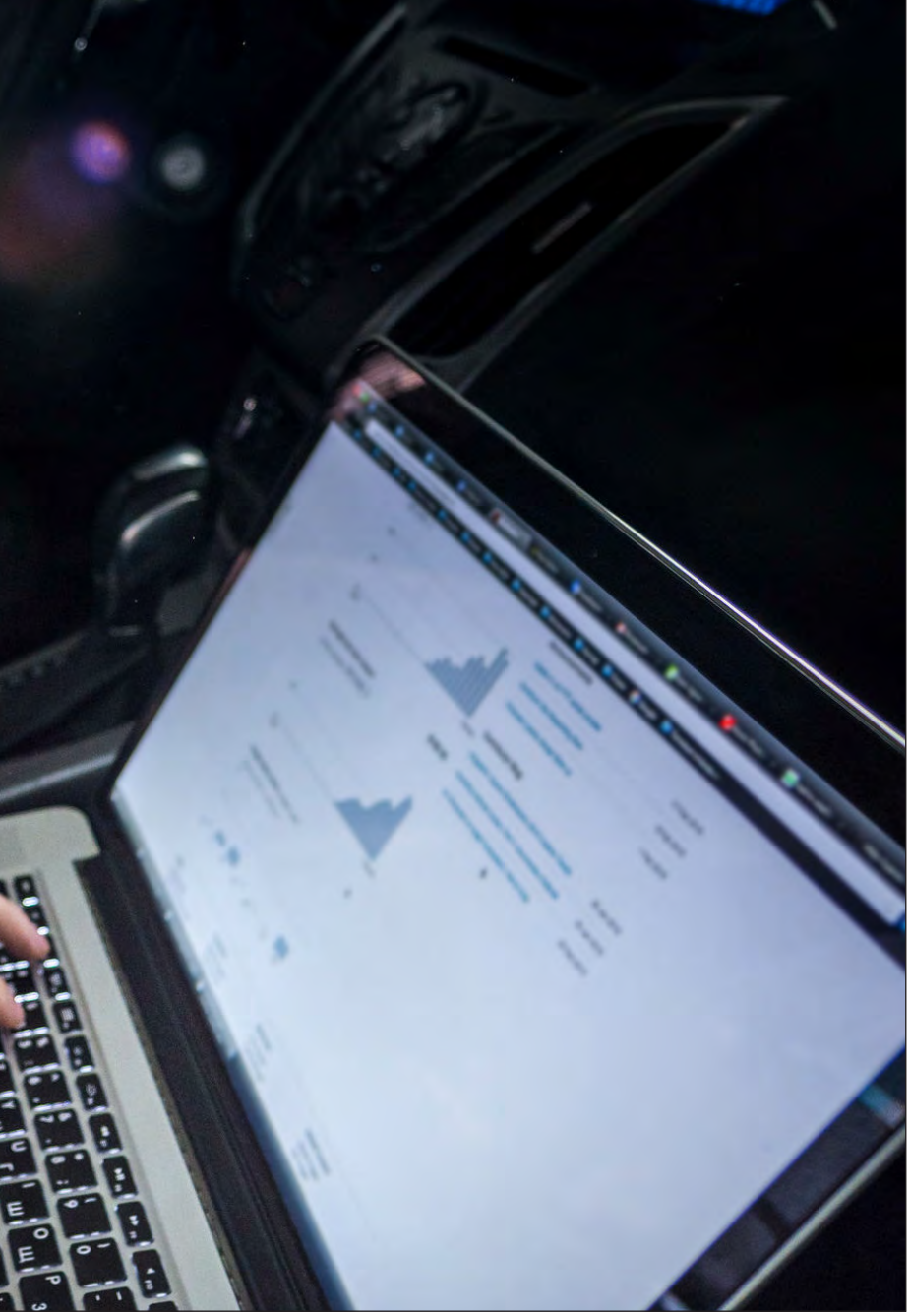
The car's been stolen. From the driveway. Without the keys. This is a story told with perhaps surprising levels of frequency these days, as the impressive convenience added to vehicles in recent years is opening up the potential for security vulnerabilities. Neil Barrett reports

ACCORDING TO Home Office figures, car thefts are up around 48 per cent over the last five years, with a similar percentage of stolen vehicles not being recovered. This is remarkable by any measure.

So what has changed? Quite simply, this: the hooded car thief going in the hard way, with all the old-school tools for the job in hand, is being replaced by that same thief using technically complex gadgets, essentially to trick a keyless entry car into thinking that the key is close by.

THE RELAY ATTACK

For the uninitiated, here are the basics. Savvy car thieves can obtain an amplifier and transmitter from their preferred black market supplier. Once



they've done this, they seek out suitable vehicles, parked near the owner's property. The thief's assistant looks for a signal using the amplifier by walking around the outside of the property trying to detect a signal from the key. If a signal is found, it is sent to the transmitter, which is now acting as the vehicle's key. With the key, it's possible to deactivate the alarm, get in and drive away.

These 'relay attacks' are carried out quickly and quietly, which helps explain their contribution to the theft statistics.

Such is their significance that Thatcham Research has launched new security ratings for vehicles, which specifically assess what is being done to address keyless entry/start vulnerabilities.

Richard Billyeald, chief technical officer at Thatcham Research, is uncompromising on how big a deal this is: "We've seen too many examples of cars being stolen in seconds from driveways," he told us. "Now, any vehicle assessed against the new Thatcham Research Security Rating that has a vulnerable keyless entry/start system, will automatically not achieve the best rating.

"The shame is that most of the cars rated 'poor' would have achieved at least a 'good' rating had their keyless entry/start systems not been susceptible to the relay attack."

Whatever your vehicle's rating, one strong recommendation to help prevent relay attacks is a Faraday-cage style shielding pouch for the keys, with the advice being to make sure that anything you buy is tested to make sure that it really does block the signal.

Manufacturers are putting in place a number of measures to tackle this problem. Thatcham have been really pleased to see some clever solutions such as key fobs which go to sleep when not being used and not in motion, such as in the key tray at home.

"the hooded car thief going in the hard way is now using technically complex gadgets..."

INTERNET OF THEFT?

There's another potential problem in the world of technical vulnerabilities - aftermarket comfort and security 'improvements' made to vehicles, using networked apps.

The Internet of Things (IoT) has seen various appliances in the home go online including, perhaps, devices you wouldn't have expected to need an internet connection. Each one of these appliances becomes a potential gateway into your home network and everything else connected to it, with an opportunity for hackers to steal information, view video feeds or even cause significant physical damage. All it could take is just one device not having been developed with the absolutely highest security standards in mind, not having been configured and secured properly by the end-user and not having been kept up to date. Even then, there's still the possibility of 'unpatched' vulnerabilities being found.

It's suggested that perhaps some - just some - of these devices have been developed with the balance of concerns between profit and security not quite right.

Unsurprisingly, as the convenience factor is ramped up, the same challenges are playing out in the vehicle security sphere, right now.

In March of this year, three specialist car alarms were found to contain security vulnerabilities which could have resulted in vehicles being hijacked or stolen given the right knowledge and circumstances, according to security consultants Pen Test Partners who were working for a BBC programme.

One system, described by its manufacturer as 'unhackable', had the potential for any user to reset any other user's password. The consultants could track any vehicle - live - with great accuracy, activate the alarm remotely, open the locks of the vehicle, start the engine... well, I'm sure you >>

>> see where this is going.

Dr Budi Arief from the School of Computing at the University of Kent (*pictured*) is an expert on cybersecurity with one of his focus areas being the IoT. Dr Arief sums up the situation very well: "As technology progresses and devices are becoming more interconnected through the concept [of IoT], there is a growing risk that any additional feature may introduce security vulnerabilities to the overall system."

Dr Arief is unsurprised about the situation: "These third-party systems have likely gone through a less rigorous process of security evaluation compared to those systems developed directly by the official car manufacturer. Nevertheless, there is no guarantee that the latter would be 100% secure, as it is pretty much impossible to prove the absence of flaws.

There's also a strong sense of irony in the situation: "Whoever bought these vulnerable car alarm systems did so out of a desire to improve the security of their vehicle. But inadvertently, they introduced security vulnerabilities that would allow attackers to take control of their vehicle. In a sense, it would have been better if these car owners did not bother to add a third-party system that may or may not have been approved by the car manufacturer."

> *"... it would have been better if these car owners did not bother to add a third-party system that may or may not have been approved by the manufacturer."*

It's worth noting that there has been the occasional reported security issue with manufacturer-fitted remote access apps, although these household names have the resources - and it's very much in their interests - to fix problems or otherwise answer concerns quickly and effectively.

What of the future? Whether it's in the home, the factory, the office or the car, the IoT isn't just a security mess waiting to happen. Unfortunately there have been some serious consequences already.

A final thought from Dr Arief: "Sadly the IoT market is akin to a gold rush for new features rather than security, and this is a challenge that needs to be addressed urgently."

In this writer's view, very urgently indeed.

As connected vehicle technologies continue to develop, so will hacking methods and security measures. It's more and more important to stay informed about cybersecurity and how it affects your vehicle. So as a buyer, when you're kicking the tyres and asking about economy, don't forget to include a question about security — it may be the difference between driving the latest model and the sad loss of a prized possession.