Evaluation of a new technology from a BISS perspective

Introduction

This report is looking at the risks associated with making new cars completely keyless. The idea is that it could make cars almost impossible to steal. This can be achieved by using facial recognition and fingerprint readers. At the time of writing this report the Genesis GV60 SUV is the only known mainstream vehicle to use this technology. They have called the facial recognition system, Face Connect. The solution is set up using the Genesis Connected Services (GCS) app, with customers only needing to access the car once with the physical key before face recognition can be used for entry. The driver's fingerprint can also be used to start the car. The facial recognition is achieved by using a micro camera and the fingerprint technology by using a scanner within the vehicle (Brook-Jones 2022).

There is very limited information available with regards to the technology being used by Genesis. I will be analysing risks associated with the technology and any potential repercussions and benefits to both Genesis and the end user.

Overview of the Technology

For the first time in the world, the Genesis GV60 has a revolutionary Face Connect feature that allows you to unlock and start your car using your face. The GV60 is equipped with a face recognition sensor and a deep learning image processing controller that allows you to lock and unlock the car without a physical key. All information is securely stored via encrypted software inside the vehicle and is managed via HMI. The facial recognition camera is built into the driver's side pillar. The fingerprint scanner is located on the dashboard within the vehicle. The vehicle can store the information of upto 4 users (Genesis, 2023).

Security with regards to the Hardware Placement

Before looking at the technology in more detail, it is first worth looking at the placement of the camera and fingerprint scanner. As mentioned above, a camera fitted in the driver's side pillar of the vehicle is used to scan the face of the potential user. Placing the camera in the side pillar seems to have several flaws that in turn, can have an adverse effect on the vehicle's security. The scanner, as a security feature, will only work, if the camera is able to recognise the face of the user. The first issue this brings to our attention is adverse weather. The reality is the camera would not be able to recognise users if it was covered with snow, ice or frost. The same would apply if the camera was covered with dirt and debris. Another issue is that reviews indicate that the camera does not always work when the user is wearing sunglasses or if the sun is directly behind the user when they try to gain entry (Marriage, 2023). Also, the camera takes a few seconds to scan the user's face. How practical is the entry system if it can be affected by so many third-party issues? The reality is users would probably still need to carry the physical key.

Can the issues above be overcome without changing the hardware on the vehicle. It is secure by using a two-pronged approach and the reality is, for ultimate security, both would

need to stay. I believe the issues above can be overcome by switching the two pieces of hardware, having facial recognition within the vehicle and the fingerprint technology on the outside. The camera inside the vehicle would eliminate most of the issues identified above. It would not be prone to the elements and would not put the user at risk of being hit by another vehicle. The fingerprint scanner can be fitted to both front doors and the vehicle's boot.

Security from the view of Genesis

Genesis would need to keep up to date with technology for new devices hackers may use that would enable them to gain access to the vehicles. Should such a device become available, the vehicle's security would be compromised, and the cars could be stolen in large numbers. This would almost certainly result in a product recall. Genesis would also face potential lawsuits which in turn would cost money and future sales. The worst-case scenario would be that Genesis would no longer be a viable business.

The reviews on the technology seem to be just on the side of the Genesis. To drive sales Genesis would need to sort out the above-mentioned issues. Currently, the market indicates that the technology is a gadget, but only marginally above being branded a gimmick (Marriage, 2023). This brings into question the risk assessments Genesis would have carried out before marketing the product. The idea, although in theory very good, has flaws that would need to be overcome before it can be marketed as a fully operational security system. If I can see the issues, why were they not spotted by Genesis? The issue Genesis have, is that to market the product they need favourable reviews of the security system, currently they are lukewarm at best.

Security from the view of the customer

From the perspective of potential customers you must ask, is this the right vehicle to introduce to the company fleet? It cannot be argued that the system, fully operational, would be an asset and a step up in security from having to use a key. Internal vehicle thefts (thefts from within the company) would be almost impossible; you would be able to allow staff access to certain vehicles and you would always know who was driving. Companies using pool vehicles would always have information as to who has what vehicle. The master key can be kept locked away to prevent staff from overriding the security settings and allowing themselves access to the vehicle. It would certainly reduce external thefts (third party car thieves). Even if a window was smashed to gain access, they would not be able to start the vehicle. Lifting the vehicle onto a tow truck would be the only way it could be taken. As a security feature, this is as good as it can get on a vehicle. The reality is that savings would also likely be made through lower insurance premiums if the market decides the vehicle is, indeed, almost impossible to steal.

So from a customer’s perspective is everything positive? The answer appears to be no. A customer checking reviews would soon realise issues with the cameras do not appear to be going anywhere at any time soon. Reviews online are all similar, the technology is good, but does not come without drawbacks. With the current layout of the hardware, it is clear to see the security risks, namely, not always being able to always gain access to the vehicle. Struggling to enter your vehicle on a sunny day or in adverse weather conditions pose a real security risk. Afterall, what use is a vehicle if it cannot be used? Man hours would be lost which in turn would reduce productivity. You also need to look at the limited number of users,

four per vehicle. Some companies have cars used by dozens of different staff members. Ikea for example, use store cars that can be used by any member of the management team. Only allowing four per vehicle would be impractical. The master key would be in constant use overriding the security settings. Any poor publicity received by Genesis, in turn, has an effect on their customers. If the vehicle gets a poor reputation it would become a rapidly depreciating asset.

For these reasons, asking the question, is it a gadget or gimmick? From the perspective of a business user, the latter is more probable.

Facial Recognition Cameras and Fingerprint Scanners

The purpose of this report is to look at facial recognition cameras and fingerprint scanners as a means of security within the Genesis GV60 SUV. The body of the report above looks at the hardware as installed in a motor vehicle but what about the risks associated with the hardware and software?

Facial recognition cameras come under the scope of facial recognition technology (FRT). The FRT matches captured images with other facial images held. It is used by Genesis to verify individuals to grant them access to using a particular vehicle. But, as with any technology, there are potential disadvantages to using FRT, including privacy and security issues. Facial Recognition Tracking (FRT) can be used to identify people without their knowledge or permission, which raises privacy concerns, as biometrics are personal identifiers (Sheikh & Ahmed, 2022). FRT also raises privacy concerns because, unlike fingerprints, facial scans can be easily, remotely, and covertly recorded. FRT can also be used to trick a system using images or 3D masks made from a victim's image. FRT is also susceptible to presentation attacks or to physical or digital spoofing, such as masking or deep fakes. Inaccuracy is another common critique of FRT. A captured facial scan that misidentifies someone could have long-term consequences. False positive rates being highest among women and people of colour (Sheikh & Ahmed, 2022). We cannot tell if Genesis have carried out risk assessments with regards to the FRT they are using but it would be a fair assumption that they would have done so. The consequences of the FRT being compromised could have significant implications for both Genesis and the customer. Genesis would suffer from a lack of trust if their system was found to have vulnerabilities and may be open to lawsuits. Poor publicity and reviews could see technology used finished whilst still in its infancy stage. It could also have an adverse effect on the brand and not just the technology being used on the GV60 SUV. From the customers perspective, they may have vehicles that are unusable or at risk of a security breach when they are left unattended. There would be concerns as its continued use and any associated cost implications.

Fingerprint authentication has become a popular way to secure mobile devices but how would it fair when used in a vehicle? One of the major risks associated with fingerprint authentication is the vulnerability of a user's fingerprint being stolen and replicated by a hacker. Unlike a password, which can be easily modified in case of compromise, a fingerprint remains unchangeable. If a hacker manages to obtain a user's fingerprint, they could exploit it to circumvent the authentication system and gain unauthorized access to the device or confidential data (Dusane, 2023).Furthermore, Genesis may utilize cloud services for storing fingerprint data, allowing the cloud provider to access it. In the event of a hack or

malicious intent on the provider's part, there is a risk that a user's fingerprint data could be misused for unauthorized activities. In extreme cases there is the risk of personnel losing fingers too/getting kidnapped by car thieves. Again, the consequences for Genesis would be the same as the consequences for their FRT. For the customer, the consequences would be the same as FRT but with the addition of personal data also being stolen and potentially used. Far reaching consequences could be lawsuits from staff members.

Professional, social, ethical issues when using biometric technology

The use of biometric technologies has several ethical ramifications (Kumar et al, 2019). A few of the problems include using one's biometric information for any other purpose, disclosing one's identity, and acting against one's beliefs and values. Civil liberties organisations asserted that biometric technology diminish privacy-related human rights. Since technology can be tricked, it is constantly prone to malfunction and is not absolute proof.

The idea that biometric technology is infallible is one of the most common misconceptions about it; in reality, it isn't always 100% feasible. Because of this flaw, there's always a chance that someone may pose as someone else and obtain their ID by hacking into a database. Given that the biometric database contains each person's distinct attributes, there is a great deal of expectation regarding correctness. Replacing biometric readings with another biometric reading from the same individual is impractical, given the state of password changes in standard security systems. However, chopping off a finger could result in a criminal issue. Biometrics are irreversible for life if lost or stolen (Groopman, 2020). Because each person's biometrics are unique and, in fact, the most uniquely identifiable aspect about them, they are very hard to hack and need a lot of computational power, specialised tools, and unique data to recreate. However, there is a bad side to this: if these data pieces are compromised, the harm is doubled. A person's biometrics cannot be replaced, and stolen identity credentials can be exploited for a variety of crimes, including theft, falsification, and incrimination.

Proportionality is a key factor to keep in mind when biometric technologies are used. These systems have wide-ranging social implications. A suggested solution's proportionality and appropriateness to the problem it seeks to solve should be considered, in addition to the technical and engineering features of the system that make it effective. Because biometric systems are intimately linked to an individual, even highly efficient technical solutions may prove unsuitable because of real or imagined side effects. Therefore, proportionality—taking into account potential effects as well as how the system will be viewed by its user communities—must be taken into account when initially exploring the solution space.

A review on the legislation being used for biometric technology was carried out by Matthew Ryder QC (Vallance, 2022). He found the rules in England and Wales were fragmented, unclear and had not kept up with technology. There is no specific piece of legislation that covers all aspects and it is currently governed by at least 8 different Acts and Regulations.

There is a need for a new legislative framework specific to biometrics (Vallance, 2022). The Department for Digital, Culture, Media and Sport is still reviewing Mathew Ryder's review.

Reflection

When deciding to look at completely keyless cars, I understood that I would be looking at biometrics already in use, being used in a new environment. My investigation needed to look at what Genesis were doing with regards to the biometrics. As this technology is only being used on the Genesis GV60 SUV, I went into the project knowing there would be limitations on the information available. When investigating the technology being used by Genesis, I could find no data on the specific hardware and software being used. For this reason, I took a broader view of facial recognition cameras and fingerprint scanners and how they could be used as part of vehicle security.

Facial recognition cameras and fingerprint scanners used as a security feature in a vehicle, in theory seem a very good idea. The reality is that there are some obvious shortcomings in the technology being used by Genesis on their GV60 SUV. The risks associated with the FUT and fingerprint scanners would be the same as if being installed in any other setting. The risks can be managed using encrypted software, but they would remain. The security with regards to the hardware placement could be overcome by installing the camera on the car interior and the fingerprint scanner on the vehicle exterior. The current system has several positives and negatives. At the time of writing this report, I believe the technology used is not a realistic option as a means of vehicle security. It is not a million miles away from where it needs to be, and I foresee a tweaked version of this technology becoming mainstream in the future.

In writing this report I have been able to take a look at the use of biometrics and their implications with regards to use in a motor vehicle. Whilst there was little information with regards to the technology used on vehicles, there was a wealth of information on the technology in general.

The difficulty I faced was trying to implement all of the information in a limited report. I found I had continuously gone over the word limit and I faced issues trying to trim the content down whilst trying not to remove necessary information. This was made more difficult as my dyslexia causes reading and short term memory issues. I did not have any issues researching the subject online even though information was limited. Completing the citation when the report was finished was a mistake. It was significantly more difficult than if I had cited the facts as the report was being written. I am pleased with the report and feel I have a better understanding of writing academically.

Ahmed, A., & Sheikh, H. (2022 December 21). Facial Recognition Technology and Privacy Concerns. ISACA. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns

Brook-Jones, c. (2022, December 20). Keyless entry face recognition technology for 2023 Genesis GV60. automotiveinteriorsworld. https://www.automotiveinteriorsworld.com/news/connectivity/keyless-entry-face-recognition-technology-for-2023-genesis-gv60.html

Dusane, J. (2023, April 28). Risks of Using Fingerprint Authentication for Mobile Devices. Linked in. https://www.linkedin.com/pulse/risks-using-fingerprint-authentication-mobile-devices-jayant-dusane

Groopman, J. (2020, june 15). In biometrics, security concerns span technical, legal and ethical. Techtarget. In biometrics, security concerns span technical, legal and ethical | TechTarget

Marriage, O. (2023, May 26). Genesis GV60 facial recognition review: does this scary new tech actually work?. BBC Topgear. https://www.topgear.com/car-news/future-tech/genesis-gv60-facial-recognition-review-does-scary-new-tech-actually-work

Vallance, C. (2022, june 29). New biometrics laws urgently needed, review finds. Bbc. New biometrics laws urgently needed, review finds - BBC News

GENESIS INTRODUCES WORLD FIRST KEYLESS ENTRY FACE RECOGNITION TECHNOLOGY ON 2023 GV60. genesisnewseurope https://www.genesisnewseurope.com/english/news/genesis-introduces-world-first-keyless-entry-face-recognition-technology-on-2023-gv60/s/68b5a48c-38ba-4a92-b3a0-98525bb5747b

Kumar, N.,Obaidat, M., Tanwar, S., Tyagi S. (2019). Ethical, Legal, and Social Implications of Biometric Technologies. Traore, I., Obaidat, M., Woungang, I. (Eds.). Biometric-Based Physical and Cybersecurity Systems. (pp. 535–569). Springer. Ethical, Legal, and Social Implications of Biometric Technologies | SpringerLink

Millett, L., Pato, J. (Eds.). (2010). 4 Cultural, Social, and Legal Considerations. Biometric Recognition: Challenges and Opportunities. (pp. 85-115). The national academy of sciences. 4 Cultural, Social, and Legal Considerations | Biometric Recognition: Challenges and Opportunities | The National Academies Press