CASE STUDY

IAV Automotive Engineering Autonomous Car, CES 2018

Secure Driver Authentication for Vehicle Entry / Operation with ZoOm® 3D Biometric Login

automotive engineering iav

At a Glance

IAV Project Requirements

- Authorized driver authentication for vehicle entry and operation
- Universal mobile smart device support
- Intuitive, user-friendly interface
- IT-friendly implementation

Solution

Outperforming all other biometric solutions, FaceTec's 100% software, 3D biometric login, ZoOm, met or exceeded all IAV's connected car driver authentication process requirements. ZoOm will be further integrated into IAV's and their customers' upcoming projects.

Overview

The connected vehicles category in transportation is a fast-growing segment that requires a persistent link to the internet, a network of computing devices with access to an enormous store of personal and confidential information.

To prevent account breaches and potential damage or loss of life through unauthorized access to this sensitive data, the authorized driver vehicle access method must:

- Ensure the person requesting access is actually the authorized driver and - to prevent spoofing - they are alive and present *at the time of login*
- Be fast and very easy to use
- Work for all users of smart devices with standard hardware and operating systems
- Perform in a broad range of physical environments and circumstances
- Be simple for IT to integrate and manage

After thorough internal testing and a successful proof-of-concept (POC) trial in a real-world environment, the ZoOm® 3D Mobile Face Login solution met or exceeded demanding consumer-level requirements an authorized driver is expected to encounter in a wide variety of typical operational circumstances.

Business Problem

Broad, global vehicle use has created traffic gridlock, pollution and productivity losses. However, connected, smart vehicles will soon be driving themselves efficiently and safely, reducing negative consequences, and further offering transportation "experiences" that provide anything from purchases-on-the-fly to personalized environments.

To ensure the experience is safe and secure, authenticating an authorized driver - ensuring they are the correct user, and that they are actually present (and alive) at the time of the login request - is a fundamental requirement.
At CES 2017, IAV presented a hyper-connected car that demonstrated a rich, autonomous driving car experience. As 2017 was another record year for account breaches, it was necessary to establish a fully secure experience from the very first user-vehicle interaction. FaceTec and IAV worked together to integrate the ZoOm SDK into their mobile app to be used in a CES 2018 "future car" demonstration.

Choosing the Authenticator

IAV considered several access methods, including password, fingerprint, voice, eye scans, 2D face recognition and 3D face authentication.

Password: Easy to initially create, relatively simple to use and eminently portable, passwords were rejected because they are very easy to share or phish. According to an annual security report by Verizon, 82% of all breaches involve compromised passwords.

Fingerprint: Fingerprint is easy to use, and cannot be forgotten, easily shared or phished. However, a hardware fingerprint sensor is required in the user's device and they do not work well if the sensor or finger is dirty. Fingerprint sensors in mobile devices can be spoofed relatively easily using a photo or a "lift" taken. There are also usability issues for people with weak or worn-down fingerprints, such as senior citizens, artisans and people who engage in daily physical labor.

"

FaceTec's professional, innovative team and their outstanding commitment to our project helped us integrate ZoOm - the most secure face biometric we've ever tested - into our successful connected car project at CES 2018 in Las Vegas. We look forward to continuing to work together on several upcoming projects.

"

--Christoph Kielmann, Senior Vice President Vehicle Electronics, IAV Automotive Engineering

Voice: Vehicle access environments do not lend themselves well to voice. Ambient noise is nearly always present, and many circumstances would not be ideal for an audible code that can be recorded and reused for vehicle access.

Eye scans: Retina and iris scans can be very secure. However, they require special hardware, do not work well in bright light and require the sensor to be uncomfortably close to the eye. The specialized hardware requirement made eye scans a non-starter.

2D Facial Recognition: Two-dimensional facial recognition can be very effective at matching the face a camera sees with a stored image from a previous enrollment, but it cannot distinguish between a photo or video spoof and a real, live person, making presentation attacks far too easy to execute. Ambient lighting can also be an issue.

3D Face Authentication: Three-dimensional face/head authentication (not just facial recognition) processes a video feed into a biometric FaceMap. This modality contains more data than photos or 2D video, and can verify both identity and three-dimensionality with the same data. Some 3D face authentication methods are proprietary-hardware based and do not verify liveness traits, and some require several seconds to authenticate, asking users to move their heads or smile (not a true liveness indicator). Intense, direct lighting can also overwhelm smart device cameras regardless of how good the software is, preventing authentication.

The Solution Chosen

ZoOm 3D face authentication from FaceTec met the demanding security and consumer-level usability needs for daily vehicle interaction ensuring the experience was safe from compromising account breaches that could create opportunities for hackers to gain vehicle control:

- ZoOm demonstrated a very high degree of image matching accuracy
- ZoOm used standard 2D mobile device cameras to create encrypted 3D face maps, allowing immediate use on all modern Android and iOS smart devices
- ZoOm enrolled and authenticated authorized drivers consistently and reliably
- Enrollment took only 15-30 seconds and authentication took 1-2 seconds, well within an acceptable, consumer-friendly timeframe

Secure login was simple and quick, with only two major steps:

1. Enroll (15-30 seconds): A new driver enrolled with ZoOm integrated into the access app so they could be later authenticated when entering and operating the vehicle.
2. Authenticate (1-2 seconds): The driver walked to within 5-6 feet of the vehicle and logged in (authenticated). Once authenticated, the vehicle door immediately unlocked, allowing the authorized driver to enter and operate the vehicle.

Recommendations

Before deployment, security, usability, IT manageability and overall cost must all be evaluated in both structured in-lab tests and a real-world proof-of-concept trial.

1. *Security*: A vehicle controlled by an unauthorized person can be dangerous and costly, requiring a very high level of security for a vehicle entry/operation. For true authentication, it must do three things:

    1) match images captured by the device to the enrolled user facemap
    2) verify three-dimensionality
    3) verify human liveness

FaceTec's patented human authentication software increases security and convenience with the most secure and intuitive 3D face biometric on the market. Now universally available for all smart mobile devices and webcams, ZoOm leverages decades of Computer Vision, Artificial Intelligence-Machine Learning experience to ensure positive identification, image three-dimensionality and unparalleled human liveness.

ZoOm is trusted to reduce fraud by organizations of all sizes on four continents in banking, government, transportation and more.

For more information about FaceTec and how ZoOm can solve your toughest authentication problems, please visit www.ZoOmLogin.com.

For business inquiries, please contact Satya Yenigalla at Satya@FaceTec.com.

For press inquiries please contact John Wojewidka at JohnW@FaceTec.com.

For the application to avoid being spoofed by non-human reproductions of the user (photos, videos, image projections, masks, etc.), the three steps listed above must happen concurrently. Other biometric options met one or two of the three required authentication attributes. ZoOm executed all three seamlessly.

2. *Usability*: Driver authentication will occur in a wide variety of circumstances and environments and needs to be consistent, fast and reliable. Authentication processes that take more than a few seconds, require special hardware, or are not easily accessible in inclement weather will be rejected by typical users. The interface must work quickly, and be easy to understand and to access at all times. ZoOm's simple selfie interface proved easy to use, even for the least tech savvy.

3. *IT Management*: Without IT intervention, ZoOm can perform user authentication entirely on the device, or match to a facemap stored on a remote server. In either case, a pass-fail token and a liveness confidence score is provided to the app allowing or blocking account access. No additional processing is required, except when an organization requires other authentication steps, such as document verification.

4. *Total Cost*: Overall costs must include all direct and indirect expenses, as well as any projected savings from reductions in support overhead, breach mitigations and brand-damage repair.

Use licenses, subscriptions, in-house development or outright purchase costs are just the beginning of a true cost assessment. Technology support requirements must also be assessed, such as server setup and maintenance, additional in-house or user hardware, additional IT personnel, custom coding and interface customization, vendor support agreements, upgrades, bug fixes and internal customer support representatives.

As an offset, a reduction in breaches afforded by a secure, easy-to-use solution will lower internal IT costs and post-breach mitigation costs, preventing costly brand damage. Software-based solutions that operate on any existing smart device, and process and securely store data exclusively or primarily on the device, are the most cost-effective.

Summary

In the demanding use case of *James*, every aspect of using ZoOm as a secure, mobile biometric entry method met or exceed expectations and requirements.

- *Integration*: A simple 2-3-hour app integration and the option to extensively customize look-and-feel, and the ability to quickly deploy for POC trials and production
- *Management*: Immediately available SDK and all supporting integration and customization documentation, no server configurations or costs, hands-off operation focused only on authentication
- *User Experience*: Simple selfie-style UI, fast enrollment and authentication, works in nearly all environments and circumstances, no special user-related hardware or additional costs required, minimal environmental adaptation required
- *Effectiveness*: Very high level of authorized driver authentication certainty
- *Costs*: No additional servers or hardware, no additional IT support, reduced breach-related costs expected, very low cost/user subscription