**[Press Release]**

**SSenStone receives OTAC technology verification from world-class universities**

* The University of Surrey conducts academic verification for OTAC algorithm and application solutions
* Korea University verifies OTAC-based business security by combining drone and OTAC technology
* SSenStone expects technological synergy with application fields such as payments, drones, and connected cars

The innovative authentication technology of a Korean startup has completed academic verification at world-class universities in cybersecurity. The one-time authentication code (OTAC), the world's first one-way dynamic authentication technology of SSenStone has successfully completed technical algorithm verification from University of Surrey and ~~the~~ Korea University. As OTAC technology has been recognized by leading universities in cybersecurity, SSenStone is expected to accelerate its business in global market.

OTAC is a next-generation authentication technology that generates a one-way dynamic code that can identify and authenticate users and devices. Unlike existing methods such as ID & password, OTP, and token, it creates a one-time code that does not duplicate with any other users at any given time, even in an off-the-network environment, which builds a strong security environment. SSenStone's OTAC has been recognized for its technological prowess and marketability at international awards in cybersecurity, along with over 190 global patents and intellectual property rights. SSenStone is gradually expanding its business targets from the financial service industry to IoT industry such as drones, connected car, and smart factory by successfully collaborating with industry leaders in vertical markets.

Dr. loana Boureanu, a senior lecturer in Secure Systems at the University of Surrey and the deputy director of Surrey Centre for Cyber Security, analysed SSenStone’s generic description of its OTAC system as well as two specific instantiations for two concrete use cases: the “ephemeral” payment card use case and the drone use case. The report by the University of Surrey demonstrates that the generic construction of the OTAC algorithm satisfies the stated requirements within the bounds of the specified system parameters. It confirms the fact; the generic OTAC algorithm provides identification of a given user; the system can operate well in a client “off-line” fashion; and the uniqueness of the OTAC values for each user is guaranteed by its construction. Furthermore, it also demonstrates that the specific use case instantiations of the OTAC system for the “ephemeral” payment card use case and the drone use case, respectively, also meet these requirements within their specified system parameters.

The study conducted by the School of Cybersecurity at Korea University reveals that the uniqueness of the OTAC code, the predictability of the code, and the security of drones with OTAC are all consistent in theory and practice. According to the study, the OTAC seed is refreshed every 10 seconds, so that an attacker cannot gather enough ciphertext to affect the operation of the drone. It results in defensing effectively against replay attacks. In particular, when OTAC is applied to the overall drone network communications, it has been found that the security of internal and external communication of the drone can be greatly improved.

Chang Hun Yoo, CEO of SSenSstone and swIDch, said, “It is a very meaningful achievement to us that our OTAC algorithm has been officially verified along with its industrial applicability, from the well-known academic institutions with authority and reputation in cybersecurity in the world.” As the scientific basis for OTAC technology ~~is~~ has become clearer, we will continue to prove the value of OTAC so that it can become the most reliable and secure device/user authentication technology in more diverse industries in the future.”

# # #

**[Image 1] SSenStone Logo**

텍스트, 클립아트이(가) 표시된 사진

자동 생성된 설명

**[Image 2] swIDch Logo**

텍스트, 클립아트이(가) 표시된 사진

자동 생성된 설명

**About SSenStone**

****

SSenStone Inc. ([www.ssenstone.com](http://www.ssenstone.com)) is the parent company of swIDch, proving its technological prowess and growth potential by taking first place with the best score in the "Baby Unicorn 200 project" of the Ministry of SMEs and Startups, Republic of Korea. Consisting of cybersecurity experts with over 10 years of experience, SSenStone continues to research and develop technologies that provide safer and more convenient identification and authentication between humans and devices or devices and devices in a rapidly changing ICT environment.

**About swIDch**

Logo

Description automatically generated

swIDch Ltd. ([www.swidch.com](http://www.swidch.com)) is a cybersecurity start-up based in London with an R&D center in South Korea. The company helps businesses to identify and authenticate its users through our patented algorithm, one-time authentication code (OTAC) that generates in a networkless environment, to tackle problems of identity theft and CNP frauds. It is a security feature for uninterrupted use of devices by combining user identification and authentication steps into one only with the dynamic authentication code. Since its foundation in 2018, the company has been chosen for leading accelerator programmes in Europe and Asia – LORCA, Global Entrepreneur Programme, and Accenture FinTech Innovation Lab. Furthermore, swIDch gained global recognition for its innovative authentication technology, selected the winner of the “Authentication Solution of the Year” in CyberSecurity Breakthrough Awards, the winner of the hottest Cybertech Company from Europas 2020, and the annual list of the world's most innovative Cybertech Company 'Cybertech100' three years in a row since 2019.