GIST researchers apply for 'U.S. patent' on technology to increase IoT security reliability

-Physical copy prevention function and channel information combination, security key generation and authentication method that are strong against retransmission attacks developed

- Professor Euiseok Hwang's research team presented the results at the IEEE Big Data Conference following the Minister of Science and ICT Award

▲ GIST Professor Euiseok Hwang

A research team at GIST (Gwangju Institute of Science and Technology, President Kiseon Kim) has developed a new authentication technique that can defend against replay attacks* targeting the Internet of Things (IoT), which is becoming more common.

* replay attack: One of the strategies an attacker can use when trying to disrupt a wireless communication authentication scheme. It is a technique that eavesdrops on authentication signals sent and received by legitimate users and retransmits them as they are, and it is generally known as an attack that is difficult to defend against.

This is expected that to promote the vitalization of the IoT industry by preventing serious social problems that may occur when the security of IoT-applied systems is breached and by improving the reliability of IoT-related security.

GIST School of Electrical Engineering And Computer Science Professor Euiseok Hwang and School of Electrical Engineering And Computer Science students Seungnam Han, Haewon Lee, and School of Mechanical Engineering student Seungwook Yoon won the Minister of Science and ICT Award at the <2022 University ICT Research Center Research Director Workshop> held by the Ministry of Science and ICT last November for this research achievement. The related technology has been applied for a patent in the United States. (Patent Name: PUF-based Internet of Things Device Using Channel State Information and Its Authentication Method)

▲ Professor Euiseok Hwang (right) receiving the Minister of Science and ICT Award in the Student Creative Autonomous Project category at the <University ICT Research Center Research Director Workshop 2022>

In addition, related research results will be presented at the 「IEEE International Conference on Big Data 2022」, an international academic conference related to 'big data' to be held in Osaka, Japan from December 17 to 20.

The research team devised an authentication method that combines PUF measured by an IoT device with channel state information (CSI) collected from a wireless communication channel.

All devices have different response characteristics due to errors that occur in the process, and this is called 'Physically Unclonable Function (PUF)'. If a security key is generated using only this characteristic and user authentication is performed, it is known to be vulnerable to a retransmission attack based on signal eavesdropping.

Just as each person has a different fingerprint, channel state information (CSI) is measured by reflecting the spatial characteristics of the physical environment, so the value is different depending on the environment being measured. Therefore, even if the attacker intercepts and retransmits the legitimate authentication signal, it is impossible to physically exist in the same location as the legitimate user, so the attacker's authentication attempt is neutralized.

As a result of the research team evaluating the identity authentication performance against replay attacks using a 32-bits long security key, the existing authentication method using PUF allowed an attacker to attempt authentication with a probability of about 0.5% out of 500,000 attacks. The authentication method was able to block all authentication attempts by the attacker.

Professor Euiseok Hwang said, "IoT is widely installed from home appliances to socially important facilities, and cyber attacks on IoT devices can lead to serious social problems. The security key generation method combining CSI and PUF can be a solution that can protect IoT devices from eavesdropping by attackers."

Student Seungnam Han said, "I was able to overcome the difficulties that arose during the research process because of the constant exchange of opinions among the team members and the guidance of the professor. I want to carry out various researches using PUF and CSI in the future."

▲ Students participating in the 2022 ICT Innovation Talent Fostering Project (from left) School of Electrical Engineering And Computer Science Seungnam Han, Haewon Lee, and School of Mechanical Engineering student Seungwook Yoon

This research was carried out with the support of the Ministry of Science and ICT's Information, Communication, and Broadcasting Innovation Talent Fostering Project (Task name: zero-knowledge sensing, cryptographic authentication, blockchain-based cloud service convergence technology development, research director: GIST Professor Heung-No Lee).