In this section, I will introduce the security of IoT in automobile field. First, we need to know what IoT in automobile can do. IoT in automobile is also called connected car, which means our car is connected to the Internet so we can authenticate our identity without car key or turn on the air-conditioner remotely via any electronic devices. Since the connected car brought great convenience for us, it has been more and more popular in recent years in global market share. However, we should not ignore the potential security threats in this system.

There are two main sources of attack, one comes from car theft, who starts the car without owner’s permission, another one is cyber hacker who modifies owner’s information. To prevent the car theft, we can either reduce the error rate of our verification model, or send an email to owner if an unidentified user has been rejected so we can track them. To prevent the cyber hacker, we can disconnect our car if it is not necessary, or use a more complex communication protocol, which I will illustrate it in depth in the next few slides.

The protocol is called PSP, which can be divided into three stages. Stage 1 is very similar to Diffie-Hellman key exchange protocol, and this stage is to get the master key for permanent communication. Stage 2 is called session key generation. Instead of traditional session key exchange, that the session key is kept for the whole session, the session key in PSP will be valid for only one communication and discarded in the next communication. Also, each session key is generated based on the hash value of the previous session key, which increases the complexity of cryptanalysis. The third stage is to verify the generated session key. Both owner and car will verify other’s session key by comparing the received hash code and expected hash code that is computed by themselves. After verification, a secure communication will start.

The last part is the discussion of pros and cons of PSP. Since the master key is distributed when owner bought the car, no one knows the master key, and the key space of master key is much larger than session key, so the security is guaranteed. Also, if one session key happens to fail, all temporary session data will be reset to reduce the cost of leaking information. The disadvantage of PSP is lack of efficiency because of chained session key generation and verification. In addition, if the master key is stolen by the opponent, all session keys will be insecure, which is a large issue for this system.

Finally, the application of IoT is not just medical, home and automobile, like the name suggests, it will apply to everything. However, the backbone of this novel technology is to guarantee its security so that people are willing to use it and we hope that it will happen in the near future. That’s all for our presentation, thanks for your listening.