Lightweight Security Platform for IoT: Smart hotel use case
Mehdi Nacer Kerkar, Maissa Dammak, Sidi-Mohammed Senouci, Dr. Mohamed Ayoub Messous
DRIVE Lab, Univ. Bourgogne Franche Comté, F58000, Nevers France
Email: mehdi.kerkar@tuta.io, {maissa.dammak, sidi-mohammed.senouci, Mohamed-ayoub.messous}@u-bourgogne.fr

Smart hotel use case

- Easy reservation and access to rooms using your personal smartphone
- The system is lightweight and ensures a secure communication among system entities.

Challenges

- How efficiently ensure the trade-off between:
  - The security of the system
  - The efficiency of the system

  - Resist against known attack
  - Provide different security features
  - Resist man-in-the-Middle attack
  - Impersonation attack
  - Ensure the perfect forward secrecy when adopting the Token

Architecture

- Lightweight platform
- Data Base (logs, reservation, etc.)
- Trusted server

Room Reservation

- Generate Token of reservation
- Distribute Token to clients
- Distribute token to smart lock

Room Access

- Ask server for Token
- Authenticate clients
- Give access to legitimate clients

Attack Scenario

- Fake client cannot access to the door smart lock
- Adversary intercept communication cannot access to the door smart lock

Defense Strategy

- The attacker cannot generate the Token because it is randomly generated.
- The attacker can eavesdrop the reservation Token but it is encrypted, so, it cannot gain access.
- The attacker can have the access pass. However, it is hashed and the hash function is irreversible.
- The attacker could not have access with the user’s smartphone if he does not have the PIN code
- We can replace PIN by QRcode

Conclusion

- The system is lightweight and ensures a secure communication among system entities.

- Paper supports lightweight and secure platform for IoT
- Practical and robust security features
- Data Base (logs, reservation, etc.)

- Trusted server

- Lightweight platform
- Minimum Computation
- Minimum communication
- Lightweight authentication
- Provide different security features
- Resist man-in-the-Middle attack
- Impersonation attack
- Ensure the perfect forward secrecy when adopting the Token

- The attacker cannot generate the Token because it is randomly generated.
- The attacker can eavesdrop the reservation Token but it is encrypted, so, it cannot gain access.
- The attacker can have the access pass. However, it is hashed and the hash function is irreversible.
- The attacker could not have access with the user’s smartphone if he does not have the PIN code
- We can replace PIN by QRcode

- The system is lightweight and ensures a secure communication among system entities.