Security Assurance in Short Range Communication with Wireless Channel Obfuscation

PIs: Hongbo Liu[1], Yingying Chen[2]

[1] Indiana University Purdue University Indianapolis, http://mypage.iu.edu/~hl45/

[2] Rutgers University, http://www.winlab.rutgers.edu/~yychen/

Motivation

➢ The prevalence of wide viewing angle screen and high standard cameras making information leakage over screen-to-camera channel become in-negligible
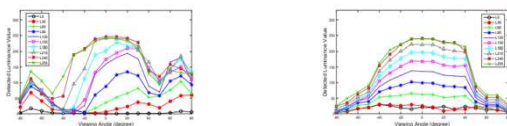

➢ Few studies have discussed how to secure data transmission over screen-to-camera channel

Secret Key Distribution over Screen-to-camera Channel

Map the secret key to a unique optical pattern on screen, which can only be correctly decoded by the legitimate user situated at an expected viewing angle
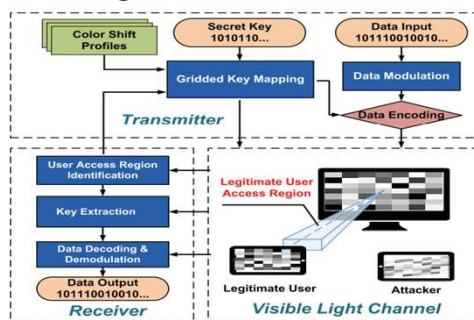

Challenges

➢ **Reliable Key Mapping:** Ensure the uniqueness of the secret key for the legitimate user over screen-to-camera channel.

➢ **Efficient Key Extraction:** Fast and accurately identify the encoded luminance pattern against various screen contents.

➢ **Secure Key Distribution:** Secret key distribution under the presence of eavesdropping attackers.

Scientific Impacts

➢ Secure numerous emerging IoT and AI applications and services heavily relying on short range communication

➢ Overcome the vulnerabilities of VLC communication by manipulating visible light signals on screen to conceal the data embedded in screen content

➢ Push forward the security study for various cyber-physical systems

Solution

➢ **Color Shift:** The change of the viewing angle towards the screen resulting in different captured optical patterns at the camera
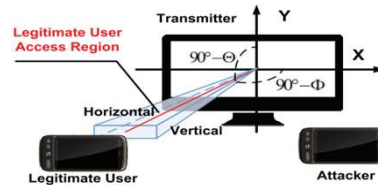

➢ **System Design**

➢ **Key Matching Method:** Map the secret key to such a luminance pattern on screen that could only be correctly detected within the legitimate user access region

➢ **Nearest Next Hop Method:** Construct an expected path, where each grid on the path has the minimum luminance difference from its previous grid

Broad Impacts

➢ Advance the knowledge in exploiting physical layer characteristics for the deployment of emerging security applications

➢ Offer interdisciplinary education and research environments on wireless security for the students

➢ Benefit numerous security sensitive cyber physics applications and services

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 | Alexandria, Virginia

NSF Award ID#: 1815908