Visual Cryptography and Obfuscation Using Augmented Reality

Patrik Lantz[1][2], Bjorn Johansson[1], Martin Hell[2], and Ben Smeets[1][2]

[1] Ericsson Research, Sweden
{patrik.lantz, bjorn.a.johansson, ben.smeets}@ericsson.com
[2] Department of Electrical and Information Technology
Lund University, Sweden
{patrik.lantz, martin.hell, ben.smeets}@eit.lth.se

As new technologies emerge such as wearables, it opens up for new challenges, especially related to security and privacy. One such recent technology is smart glasses. The use of glasses introduces security and privacy concerns for the general public but also for the user itself. In this talk we present ongoing work which focus on privacy of the user during authentication. We propose and analyze two methods, visual cryptography and obfuscation for protecting the user against HUD and camera logging adversaries as well as shoulder-surfing.

Recent research in privacy-preserving human-computer interaction allows users to authenticate and decipher data using smart glasses equipped with a camera. Decrypted data or one-time authorization codes (OTAC) are displayed as an image overlay in a heads-up display (HUD). The user can then interact with a terminal screen while preventing shoulder-surfing as an adversary cannot observe the HUD. However, this does not mitigate attacks where the adversary has access to the information presented in the HUD.

In our proposed methods, using visual obfuscation and a modified visual cryptography scheme, we split information shown in the HUD into two or three partitions. These partitions are displayed on a terminal screen and in the HUD. Decrypting and deobfuscating information is then a matter of aligning the image overlay in the HUD with the information displayed on the screen. For the attack model we assume that an adversary has access to a) one of two or b) two of three partitions. The adversary could be shoulder-surfing or is capable of observing the HUD. In case b) we assume that the adversary is capable of combining these partitions easily. In case of an adversary which has control over the camera, then we rely on b) only if the terminal screen features a 3D autostereoscopic display. However, case a) still holds if camera recording can be disabled or prevented.