NEUROCRYPT: Coercion-Resistant Implicit Memory Authentication (Student Abstract)

Ritul Satish, Niranjan Rajesh, Argha Chakrabarty, Aditi Jain, Sristi Bafna, Arup Mondal, Debayan Gupta

Ashoka University, Rajiv Gandhi Education City, NCR 131029, India
{ritul.satish_ug22, niranjan.rajesh_ug23, argha.chakrabarty_ug22, aditi.jain_ug22, sristi.bafna_ug23, arup.mondal_phd19, debayan.gupta}@ashoka.edu.in

Abstract

Overcoming the threat of *coercion attacks* in a cryptographic system has been a top priority for system designers since the birth of cyber-security. One way to overcome such a threat is to leverage implicit memory to construct a defense against *rubber-hose attacks* where the users themselves do not possess conscious knowledge of the trained password. We propose NEUROCRYPT, a coercion-resistant authentication system that uses an improved version of the "Serial Interception Sequence Learning" task, employing additional *auditory* and *haptic modalities* backed by concepts borrowed from cognitive psychology. We carefully modify the visual stimuli as well as add auditory and haptic stimuli to improve the implicit learning process, resulting in faster training and longer retention. Moreover, our improvements guarantee that explicit recognition of the trained passwords remains suppressed.

Introduction and Technical Background

Assume you know the password to a system that keeps certain information secure. This system is a state-of-the-art cryptographic system that is very difficult to crack by an attacker. The attacker could choose to coerce you to reveal the password by resorting to torture or blackmail instead of attempting to break the encryption. This type of an attack is called a *rubber-hose attack* and is the least costly method in terms of time and effort to defeat the most complex cryptographic systems. We can prevent such rubber-hose attacks if the authentication credentials cannot be extracted from the user by force.

Now, imagine that you possess the ability of Leonardo DiCaprio from the movie Inception and are able to implant information into someone's mind without them having explicit knowledge of said information. Although this concept seems to be heavily based on science fiction, it is possible through cognitive psychology that we will be employing in our proposed authentication system albeit to a less nefarious extent. In our knowledge-based authentication system, we employ the concepts of implicit learning and memory to prevent rubber hose attacks.

Contributions. We present NEUROCRYPT, an authentication system built upon an existing system that leverages implicit learning and retention (Bojinov et al. 2012).

Our novelty to the existing system comes from the employment of various computer-human modalities such as vision, audition and tactition, and their contributions to improved implicit memory retention of sequences. Finally, we wish to show that experiments with these individual modalities and their combinations will help to identify the best multi-modal interaction that maximises the effectiveness for the NEUROCRYPT system.

Implicit memory and learning. In cognitive psychology, implicit learning is the learning of complex information in a subconscious manner. Implicit learning is considered to be one of the most important complex cognitive processes for many motor, perceptual and cognitive skill acquisition. Several tasks have been designed to showcase implicit learning in humans such as Serial Interception Sequence Learning (SISL) (Gobel, Sanchez, and Reber 2011). The evidence of learning in these tasks without the player's knowledge of the learning itself is proof of the functioning of the implicit memory system.

NEUROCRYPT Authentication System

Our proposed authentication system is inspired by the Serial Interception Sequence Learning (SISL) task. The task's objective is similar to the game – Guitar Hero. The subject is expected to intercept falling circular cues by pressing keys on the keyboard corresponding to the columns that they fall through. If the cues are intercepted when they reach the end line at the bottom of the screen, the game registers a hit. If the cue passes the end line without the subject pressing the correct key, or if the subject presses an incorrect key, a miss is registered. Their performance is measured using the hitrate parameter which is the ratio of hits to the sum of hits and misses. The speed of the cues falling is dictated by an algorithm that tries to maintain a hitrate of around 70%.

The sequence-learning aspect of the game entails the repetition of a predetermined 30-item sequence (the possible items being the six keys that correspond to the six columns) in the training phase. The passcode sequence is repeated multiple times during the course of the training session to facilitate implicit learning. The training sessions last for about 40 minutes and the subject is expected to have implicitly learnt the sequence with minimal or no explicit retention of the sequence.

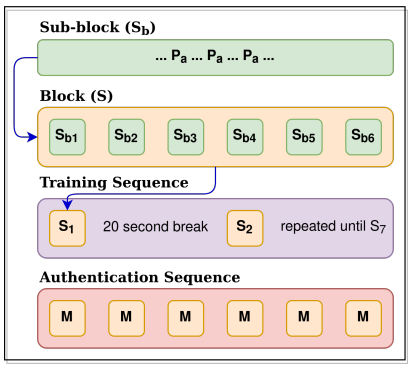

Figure 1: Schematic overview of NEUROCRYPT. "M" is random permutation of (P_1, P_2, P_a).

This minimization of the explicit retention and increase in potential secret key sequences are achieved by employing several additional measures like the lack of repetition of items in the passcode sequence, the random noise and an addition of 2 extra columns (and thus possible items) compared to the original SISL task. Additionally, our proposed passcode sequence (30 items) is significantly more difficult to explicitly learn than the passcode sequence proposed in the original SISL task (12 items). We use the following modality-specific features adopted from cognitive psychology to maximise subject's implicit learning and retention.

Visual modalities incorporated. There are solid visual separators between the columns for better visual perception. The color contrast of the cues and the background is maximized by making the cue black and the background white.

Auditory modalities incorporated. It has been proved that background white noise improves performance in inattentive participants for memory tasks and reduces performance in attentive participants (Gobel, Sanchez, and Reber 2011). A mild white noise is played in the background while the participant is playing the game. The volume of this white noise is decreased with the improved performance of the participant. A musical note (intended to improve retention) is played on a key press by the participant. 3 unique notes that minimize perceptual grouping are mapped to 2 keys each, one on each side ($\{s, d, f\} \rightarrow left$ and $\{j, k, l\} \rightarrow right$).

Haptic modalities incorporated. Haptic feedback is given with every keypress and its intensity is varied in every alternate block sequence. All odd numbered blocks (1,3,..) will have a set haptic intensity and the even blocks (2,4,..) will have 50% of the haptic intensity set in odd blocks.

Detail Operation of NEUROCRYPT System

NEUROCRYPT authentication system is composed into two phases – training phase (step $1-5$ in Algotithm 1) and authentication phase (step $6-8$ in Algotithm 1).

Conclusion and Future Work

We propose NEUROCRYPT, a *novel* authentication system based on implicit memory and retention. NEUROCRYPT uses visual, auditory and haptic modalities to strengthen the learning and improve the implicit retention of the trained passcode. In the future, we aim to develop a comprehensive prototype using which we plan to assess the individual and combined effect of the visual, auditory, haptic modalities and their effect on implicit learning of long passcode sequences. Intensive user studies and case studies on this scheme will also give the usability perspective and allow us to identify user pain points. This will aid in further research and the development of better authentication schemes.

Algorithm 1: NEUROCRYPT Authentication System

1. **For training:** users willing to use NEUROCRYPT undergo a training session in which they are trained with a 30 item long system assigned passcode sequence. The 6 keys that correspond to the six columns in the game are of the set $S = \{s, d, f, j, k, l\}$. This 30 character long secret passcode sequence is generated from the set of Euler cycles from a directed graph $G = (V, E)$ with each unique character in S as the vertexes.
2. A 30 item long secret passcode sequence is generated from the set of Euler cycles from a directed graph $G = (V, E)$ with each unique character in S as the vertices and is stored in $\sum$.
3. The system assigned passcode P_a is repeated thrice intermittently in an 18 character random sequence to make a 108 character sequence S_b called sub-block.
4. S_b is followed by 4 more randomly generated S_b to make S. S is repeated 7 times in the training phase. The user gets a 20 seconds break after every S called block.
5. The game speed increases with better performance H by the user in the training session. H is defined as the number of correct responses by the user for the number of cues rolled down. The final game speed at the end of the training session is recorded.
6. **For authentication:** the user is presented with P_a along with two distinct untrained sequences P_1 and P_2 from $\sum$. Each of the sequences in $M = \{P_a, P_1, P_2\}$ is presented to the user six times (two groups of three repetitions) with random ordering six times with no break.
7. The users performance in P_a and performance in the untrained sequences P_1 and P_2 are H_p and H_{r_1} and H_{r_2} respectively.
8. The system declares that authentication was successful if $H_p > Avg(H_{r_1}, H_{r_2}) + \sigma$, where σ is large enough to minimize chance occurrences but small enough to prevent authentication failures. We will be able to identify a reasonable value for σ after running the simulations.

References

Bojinov, H.; Sanchez, D.; Reber, P.; Boneh, D.; and Lincoln, P. 2012. Neuroscience meets cryptography: designing crypto primitives secure against rubber hose attacks. In *21st USENIX Security Symposium (USENIX Security 12)*, 129–141.

Gobel, E. W.; Sanchez, D. J.; and Reber, P. J. 2011. Integration of temporal and ordinal information during serial interception sequence learning. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 37(4): 994.