UNIVERSITY OF CENTRAL FLORIDA

CAP6135 Malware & Software Vulnerability

On Limitations of Designing LRPS: Attacks, Principles and Usability

By Sagar Patel
04/21/2014
EECS Department

Agenda

- Introduction
- Leakage-Resilient Password System
- Brute Force Attack
  - Principle 1
  - Principle 2
- Statistical Attack
  - Principle 3
  - Principle 4
  - Principle 5
- Quantitative Analysis Framework
- Paper Weakness

Introduction

- Secret leakage is one of the most common security threats, in which an adversary steals the password by capturing user’s input.
- An ideal LRPS allows user to generate a one-time password (OTP) for each authentication sessions.
- A strong adversary may use a hidden camera or malicious software to record complete interaction between user and computer.

Leakage-Resilient Password System

- Its a challenge response between a user and server
- User and server agree on a common root secret (password)
- User uses the root secret to generate *responses* to *challenges* issued by the server to prove his identity
- The common system parameters of the most existing LRPS systems can be described by a tuple (D, k, n, d, w, s)

Threat Model & Experimental Setting

- Two types of passive adversary models
- The weaker passive adversary model assumes that the adversary is not able to capture complete interaction between user and the server.
- The strong passive adversary model in which secret leakage during human-computer authentication is unavoidable

Threat Model & Experimental Setting

- **Security strengths of existing schemes and the process is given as follows:**
  - Generate a random password as the root secret
  - Generate challenge for authentication round
  - Generate response based on the password
  - Analyze the collected challenge-response pairs after each authentication round.
  - Repeat last three steps until exact password is recovered.

Brute Force Attack

- **Brute force attack is pruning-based learning process.**
- **Its procedure is described as follows:**
  - List all possible candidates for the password in the target system.
  - For each independent observation of a challenge response round, remove the invalid candidates from the candidate set.
  - Repeat the above step until the size of candidate set reaches a small threshold.

Brute Force attack

- **The power of brute force attack is given by two statements:**

- **Statement 1:** The verification algorithm used in brute force attack for candidate verification is at least as efficient as the verification algorithm used by server for response verification.
- **Statement 2:** The average shrinking rate for the size of valid candidate set is the same as one minus the average success rate of guessing attack.

$$m = [\log_{1/d} X]$$

P1: Large Root Secret Space Principle

- **An LRPS system with secret leakage should have a large candidate set for the root secret.**
- Undercover is a typical scheme based on the *k*-out-of-*n* paradigm.
- In each authentication round, the user is asked to recognize if there is a secret image is shown in the current window.
- The default parameters are: k = 5, n = 28 and w = 4 + 1
- On average, 53.06 rounds are sufficient to recover the exact secret, and the size of the candidate set can be reduced to less than 10 after 43.55 rounds.

P1: Large Root Secret Space Principle

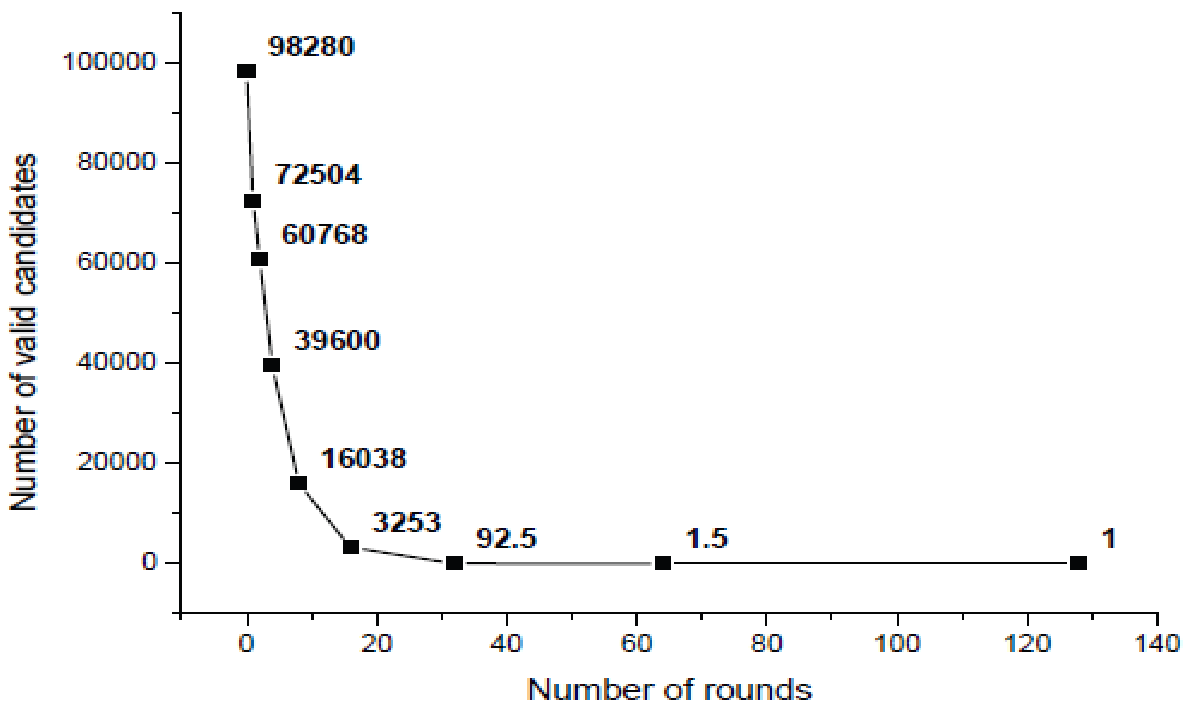

Figure 1. The average number of valid candidates shrinks for Undercover.

P2: Large Round Secret Space Principle

- **An LRPS system with secret leakage should have a large candidate set for the round secret.**
- Predicate-based Authentication Services (PAS) is used as a counterexample to show that a round secret with a small candidate set can be easily recovered.

$$x = 1 + ((I - 1) \bmod len)$$

- For example: There are two secret pairs ,(<2,3>,sente) and (<4,1>,logig) and I = 15. So, $x = 5$ and the predicates are (<2,3>,e) and (<4,1>,g)

P2: Large Round Secret Space Principle

- **The default parameters are p = 2, and there are 25 cells in each challenge table and 26 possible letters for the secret character.**
- **On average, 9.4 rounds are sufficient to recover the exact round secret.**

P2: Large Round Secret Space Principle

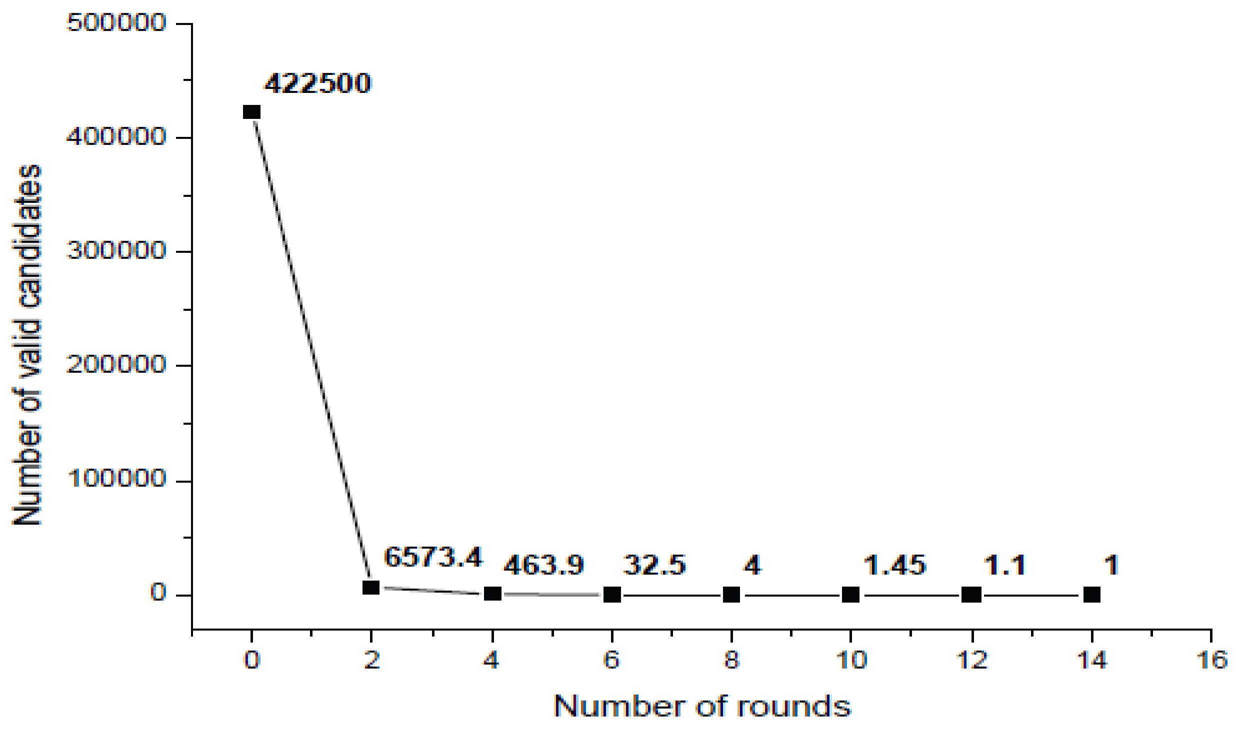

Figure 2. The average number of valid candidates shrinks for PAS.

Statistical Attack

- Statistical attack is an accumulation-based learning process.
- Compared to brute force attack, statistical attack has fewer limitations as it can be applied to schemes with a large password space.
- The efficiency of statistical attack is *design dependent* and varies with different schemes and different analysis techniques.
- There are two statistical analysis techniques that are able to extract the root secret of most existing schemes.

Statistical Attack

- **The first technique is probabilistic decision tree.**

- **The procedure is as follows:**
  - Create a score table for each possible individual element or affordable-sized element group in the alphabet of the root secret.
  - For each independent observation of a challenge response pair, the adversary enumerates every *consistent* decision path that leads to the current response

Statistical Attack

- A *decision path* is an emulation of the user's decision process that consists of multiple decision nodes.

- Consider a scheme which shows a four-element window:

$$\langle S1{:}1,\ S2{:}2,\ S3{:}1,\ D1{:}1\rangle$$

- Its decision path is :

$$X = \langle S1{:}1\rangle \| \langle D1{:}1;\ S3{:}1\rangle$$

Statistical Attack

- **The second technique is Counting-based statistical analysis**

- **The procedure is as follows:**
  - Create / counting tables for / response groups. The adversary creates a counting table for each possible response if affordable
  - For each independent observation of a challenge-response pair, the adversary first decides which counting table is updated according to the observed response
  - Repeat the above step until the number of entries with different score levels reaches a threshold

P3: Uniform Distributed Challenge Principle

- **An LRPS system with secret leakage should make the distribution of the elements in each challenge as uniformly distributed as possible.**
- Undercover is the counterexample to show secret leakage.
- 2-element counting table is used to recover secret from the challenge.
- On average, it is sufficient to recover the exact secret within 172.7 rounds.

P4: Large Decision Space or Indistinguishable Individual Principle

- **An LRPS system with secret leakage should make each individual element indistinguishable in the probabilistic decision tree if the candidate set for decision paths is enumerable.**
- A high-complexity CAS scheme is used as an counterexample.
- Given a response with the answer, they enumerate all consistent decision paths leading to this answer, and update the score table according to the conditional probability.

P4: Large Decision Space or Indistinguishable Individual Principle

- For an 8 × 10 grid specified by the default parameters, there are 43758 possible decision paths in total, with average path length of 14.5539.
- On average, it is sufficient to discover the exact secret within 640.8 rounds, and discover 90% secret elements after 264.7 rounds
- So, it is necessary to increase the number of candidate decision paths if it is infeasible to make each individual element indistinguishable in the probabilistic decision tree

P4: Large Decision Space or Indistinguishable Individual Principle

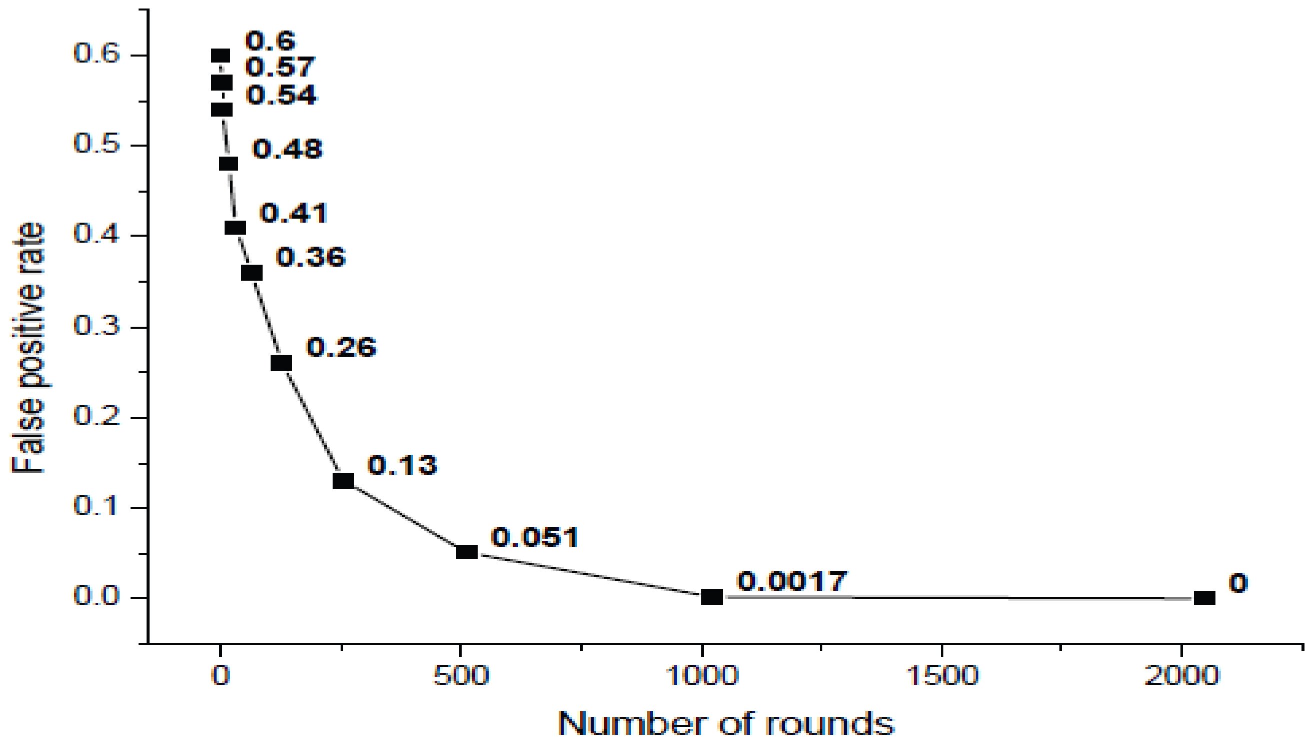

Figure 4. The average false positive rate decreases for the high-complexity CAS scheme.

P5: Indistinguishable Correlation Principle

- **An LRPS system with secret leakage should minimize the statistical difference in low-dimensional correlations among each possible response.**
- SecHCI is used as a counterexample to show how it works while brute force and probabilistic decision tree are infeasible.
- The user calculates r as,

$$r = [(x \bmod 4)/2]$$

- 2-element counting tables is used to recover secrets.

P5: Indistinguishable Correlation Principle

- Since the default parameters are large for SecHCI system, k = 14, n = 140, brute force attack is not applicable.
- On average, it is sufficient to recover the exact secret with 14219.4 rounds and recover 90% secret elements after 10799.8 rounds.

P5: Indistinguishable Correlation Principle

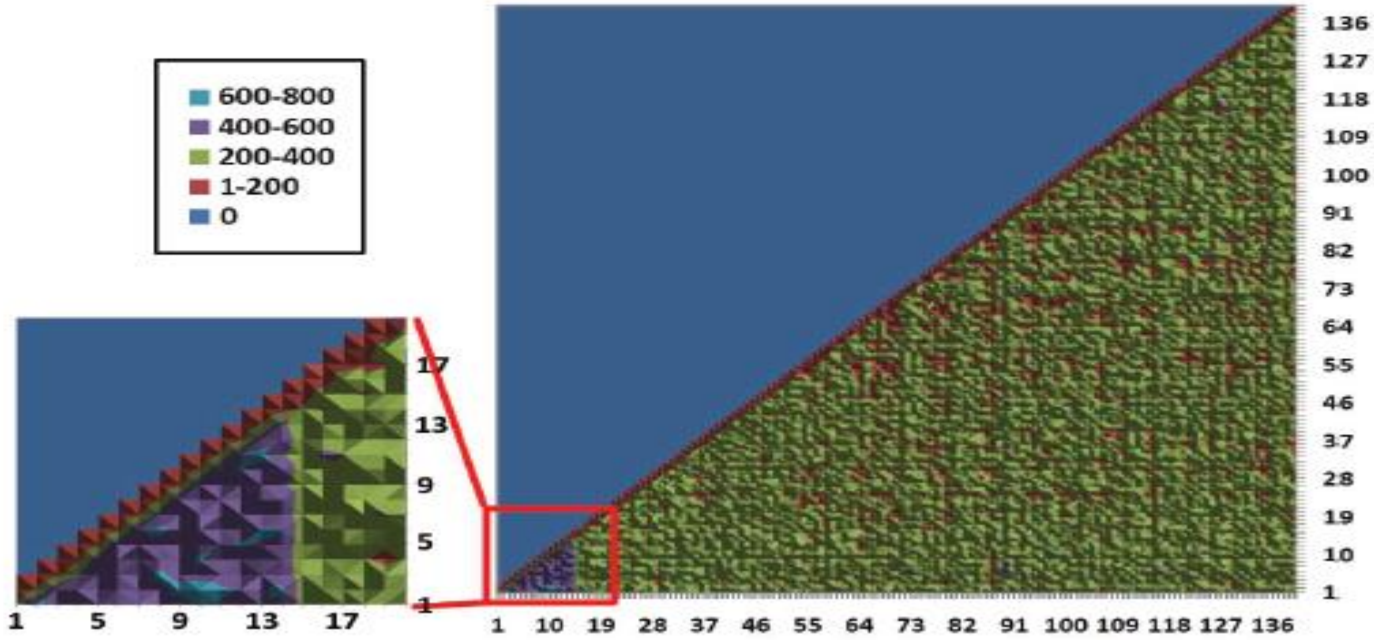

Figure 5. The pair-based score distribution is distorted for SecHCI. The first 14 elements are the secret icons, whose pair-based scores are distinguishable from the scores of other icons.

Quantitative Analysis Framework

- **This framework decomposes the process of human-computer authentication into atomic cognitive operations in psychology.**

- **There are four types of atomic cognitive operations commonly used:**
  - Single/parallel recognition
  - Free/cued recall
  - Single-target/multi-target visual search
  - Simple cognitive arithmetic

Quantitative Analysis Framework

- **There are two components in our quantitative analysis framework:**
  - *Cognitive Workload* (C)
  - *Memory Demand* (M)
- **Cognitive workload is measured by the total reaction time required by the involved cognitive operations**
- **Memory demand is measured by the number of elements that must be memorized by the subject, which is the prerequisite of any password system**

Weaknesses

- Based on the framework and security analysis, the tradeoff between security and usability is strong, which indicates the inherent limitation in the design of LRPS systems

- Error rate is currently not included in the analysis framework as it is difficult for experimental psychology to provide the general relation between thinking time and error rate

UNIVERSITY OF CENTRAL FLORIDA

Thank You!