DPPG - A Dynamic Password Policy Generation System

Gayatri Pachare
BE Scholar
B.I.T. Ballarpur,Chandrapur
gayatripachare1212@gmail.com

Awanti Deshmukh
BE Scholar
B.I.T. Ballarpur,Chandrapur
awantideshmukh24@gmail.com

Prof.Saraswati.B.Sahu
Assistant Professor
B.I.T.Ballarpur,Chandrapur
Sarusahu2006@gmail.com

Abstract: For securing the login, passwords of users from intruders and hackers, the website owners and administrators are providing certain guidelines to the users to create secure and strong passwords using a mechanism called Password Checkers. These guidelines which are provided helps the users to create strong passwords, these guidelines are also becoming the raw input for the hackers as they clearly show based on which policy the password was generated which increases the risk for brute force attacking with more ease. There by increasing the success rate probability for the brute force attackers. To overcome and to decrease the success probability for brute force attacking the Dynamic Password Policy Generator is being devised.The profiles of users are built and maintained by the system automatically bases on the interaction with the monitored database in training phase. This DBSAFE system will help both the administrator as well as the users to feel secured in terms with their data security.

Keywords – Dynamic Password, Authentication, ARP, Sniffer;

*****

I. INTRODUCTION

A Dynamic Password policy generation system is used To keep password users from creating simple and common passwords, major websites and applications provide a password-strength measure, namely a password checker. While critical requirements for a password checker to be stringent have prevailed in the study of password security, we show that regardless of the stringency, such static checkers can leak information and actually help the adversary enhance the performance of their attacks. To address this weakness, we propose and devise the Dynamic Password Policy Generator, namely DPPG, to be an effective and usable alternative to the existing password strength checker. DPPG aims to enforce an evenly-distributed password space and generate dynamic policies for users to create passwords that are diverse and that contribute to the overall security of the password database. Since DPPG is modular and can function with different underlying metrics for policy generation, we further introduce a diversity-based password security metric that evaluates the security of a password database in terms of password space and distribution. The metric is useful as a countermeasure to well-crafted offline cracking algorithms and theoretically illustrates why DPPG works well.

II.LITERATURE SURVEY

[A].Dynamic password policy generation system

A part of aimlessly selected passwords are used as training data and the rest are used as target data. All this data is taken from a leaked set of passwords. A threat model is also developed

[B].Generating pronounceable security passwords

The "Sandia System” is a pronounceable password generator which uses the next following methodology. different templates are created.

[C]. Administrative password generation

The method includes obtaining a tag associated witha client computer, and generating a password using the tag. The password is used for an application accessible by the client computer

[D]. Password Management with Storage Optimized Honeyword Generation.

Problem Formulation

common password composition strategy simply limits.the character set diversity of passwords, some scholars have advanced the mnemonic password strategy on the basis of the general password composition strategy. The purpose of the mnemonic password policy is to help users create passwords that are secure and easy to remember. The similarities between MneGenEx, MnePerEx, MnePer, MonEx, MneSchEx, and MneYanE are that the user selects sentences or phrases that contain at least eight words (It is safer to choose what makes sense to ourselves and is unlikely to be used by others), and then replaces each word with numbers, letters, and special symbols, usually using the first letter of each word. For example, using the MneGenEx strategy, select the sentence ‘‘Four score and seven years ago our fathers brought forth on this continent, then ‘‘Four’’ =>’4’ (‘4’ replace ‘‘Four’’), ‘‘and’’=>’&’, ‘‘seven’’=>’7’, ‘‘forth’’=>’4’, the rest of the words are replaced by the first letter of the word.Then we get the password ‘‘4s&7yaofb4otc’’ The KbCg password policy allows user to select an easy-to-remember password as pwd1 firstly, then the user moves one or more keys on the keyboard as a password based.

Objective

A password, sometimes called a passcode,[1] is a memorized secret, typically a string of characters, usually used to confirm a user's identity.[2] Using the terminology of the NIST Digital Identity Guidelines,[3] the secret is memorized by a party called the claimant while the party verifying the identity of the claimant is called the verifier. When the claimant successfully demonstrates knowledge of the password to the verifier through an established authentication protocol,[4] the verifier is able to infer the claimant's identity.

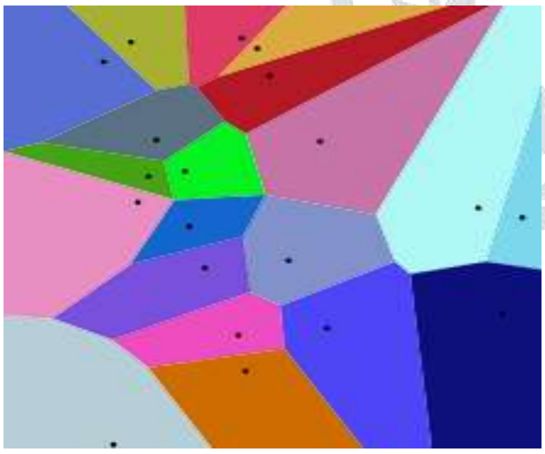
III. PROPOSED METHODOLOGY

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. Either the password policy is merely advisory, or the computer systems force users to comply with it. Some governments have national authentication frameworks[1] that define requirements for user authentication to government services, including requirements for passwords.

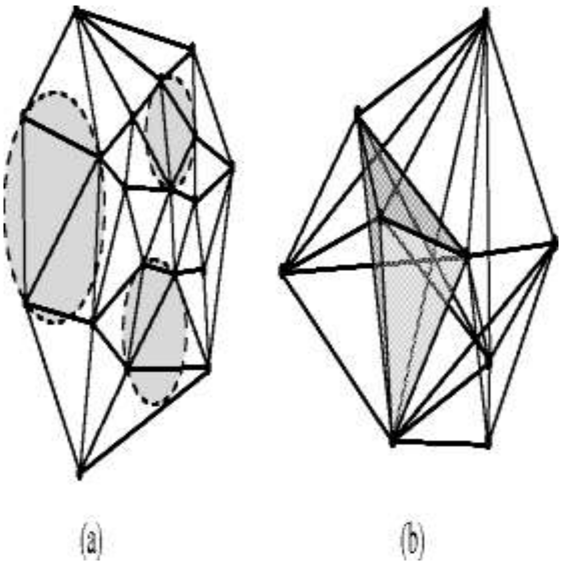
Voronoi Clustering

In mathematics, a **Voronoi diagram** is partition of plane into regions close to each of a given set of objects. In the simplest case, these objects are just finitely many points in the plane (called seeds, sites, or generators). For each seed there is a corresponding region consisting of all points of the plane closer to that seed than to any other. These regions are called Voronoi cells.

The Voronoi diagram is named after geogray, and is also called a **Voronoi tessellation**, a **Voronoi decomposition**, a **Voronoi partition**, or a **Dirichlet tessellation**.Voronoi cells are also known as **Thiessen polygons**. Voronoi diagrams have practical and theoretical applications in many fields, mainly in science and technology, but also in visual art.



Delaunay Triangulation



Given a point set P in the plane, the Delaunay triangulation is a particular triangulation of the points in P, which satisfy the empty circum-circle property: the circum-circle of each triangle does not contain any other point p∈P. This structure for a set of 3D points is the tetrahedralization of the points in which the circum-sphere of each tetrahedron does not contain any other point of the point set. Figure 1 shows Delaunay triangulation of some 2D and 3D points.

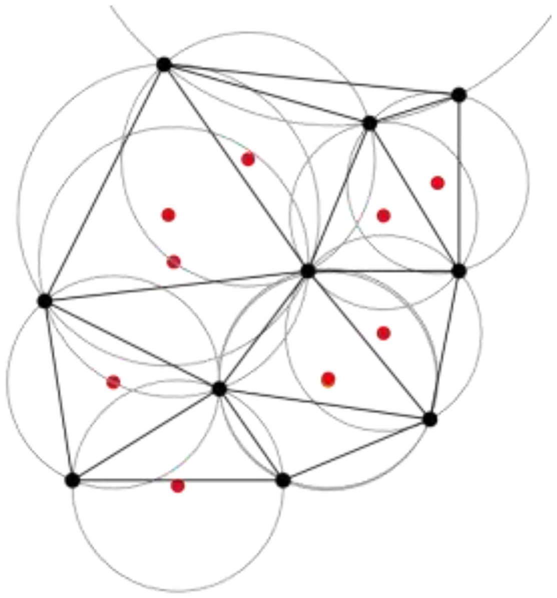
A password sometime called a passcode,[1] is a memorized secret, typically a string of characters, usually used to confirm a user's identity.[2] Using the terminology of the NIST Digital Identity Guidelines,[3] the secret is memorized by a party called the claimant while the party verifying the identity of the claimant is called the verifier. When the claimant successfully demonstrates knowledge of the password to the verifier through an established authentication protocol,[4] the verifier is able to infer the claimant's identity.

Delaunay Triangulation Relationship with Voronoi Diagram

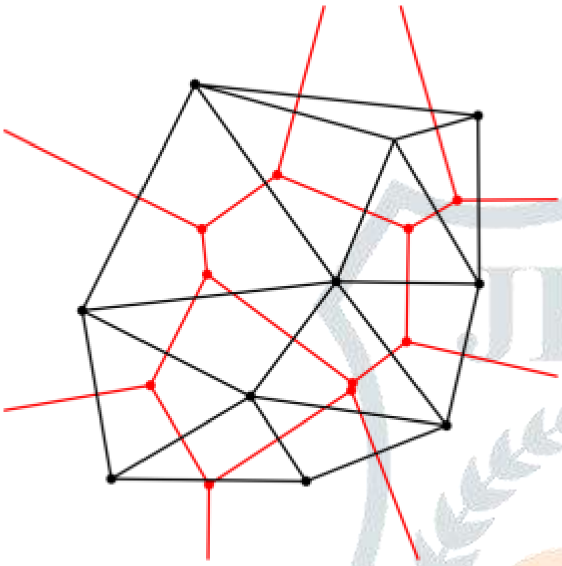
The Delaunay trigulatio of a discrete point set **P** in general position corresponds to the dual graph of thevorooic diagram for **P**. The circumeter of Delaunay triangles are the vertices of the Voronoi diagram. In the 2D case, the Voronoi vertices are connected via edges, that can be derived from adjacency-relationships of the Delaunay triangles: If two triangles share an edge in the Delaunay triangulation, their circumcenters are to be connected with an edge in the Voronoi tesselation.

Special cases where this relationship does not hold, or is ambiguous, include cases like:

- Three or mor collion points, where the circumcircles are of infinite radii.
- Four or more points on a perfect circle, where the triangulation is ambiguous and all circumcenters are trivially identical



Fig(1).The Delaunay triangulation with all the circumcircles and their centers (in red).



Fig(2).Connecting the centers of the circumcircles produces the voronoi diagram(in red).

Modules

Module 1:- EXISTING MODEL

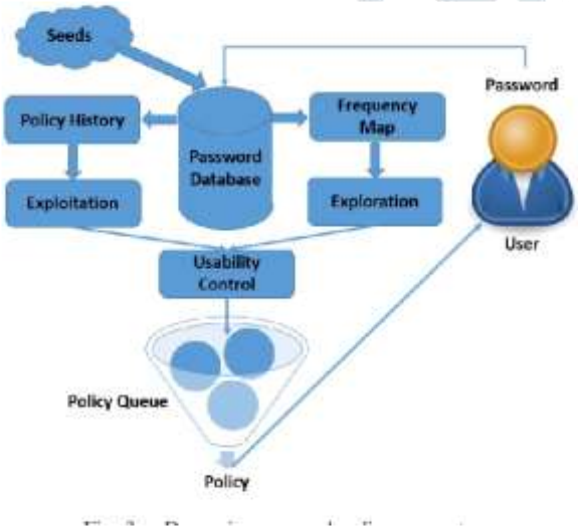


Fig- Existing DPPG Model

Firstly the system administrators can induce explicit passwords which work as seeds in the database. The seeds can form a list certain desired password characteristics to insert in the generated password. Now DPPG starts to generate password policies on the basis of these seeds. Users can type their desired password characters which will also be stored in the password database. Also the user will be given which are all the good and bad characters which has to be used and avoided for generating the random password. For generating the password policies intelligently, DPPG maintains a global characteristics frequency map and a history of generated password policies that can approximate the current password distribution.[2] There are two different ways for DPPG to enlarge the usable space of passwords. The exploitation mode balances password distribution with the help of password history

Module 2:- Implementation

This section illustrates the working of user registration and login into any website. Fig. 1 shows that how the password is stored in the database. Firstly, the user registers on the website

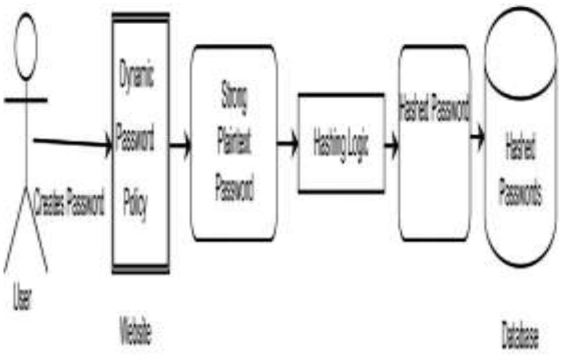


Fig.(1). Storing password in the database.

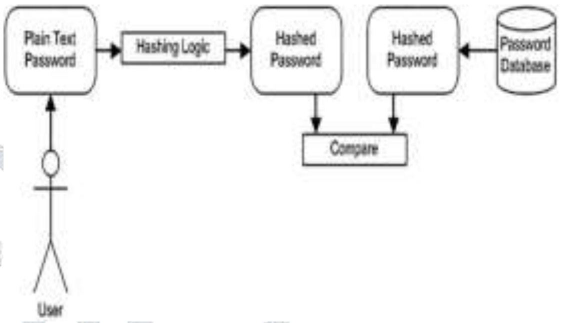


Fig.(2). Comparing the hash of input password with the hash of the stored password in the database.

in which user has to provide various details like username, new password, security code, etc. We are focusing on password which is chosen by the user based on the password policy generated by the algorithm, which is dynamic.

users to create strong passwords. For example, following are the password policies for creating a strong and dynamic password:

- Minimum of 8 characters in length.
- Maximum of 20 characters in length.
- Choose from the given good characters.
- Avoid bad characters.

The created password is strong and complex as it follows the policy which is dynamic. The generated strong plain-text password is hashed using a hash algorithm which is a slow hash function then it is stored in the database. After successful registration to the website, when a registered user login to the website, the provided password, is hashed again using the same hash function and since the user-id is a primary key(as it is unique) in the database, using this, it searches for the stored hashed password in the database. It is shown in Fig. 2. Since the methodology is the combination of generating the strong password by enforcing dynamic password policy and hashing with the standard Password-Based Key Derivation Function-2, it makes the proposed system more secure related to others.

Advantages of generating password policy dynamically

As policies of the static password policy generator are not dynamic, it exerts a bias on the characteristics of the password. The password stored in the database follows a specific pattern enforced by the password strength checker.

Simple and intuitive way rather than searching with complicated models. We judge the effect of exploiting present economic password strength checkers from attacker's view as passwords of same strengths will almost have the same pattern using which attackers can hack [2]. In DPPG each user will be getting unique passwords created by server and hence the user does not know what policy the other user gets unlike conventional method [2].

Conclusions

This paper reviews the methods and algorithms introduced in the literature to construct the Delaunay triangulation of 2D and 3D dynamic point sets (where the points are added or deleted) and kinetic point sets (where the position of the points vary over time). Static DT has been used in geosciences for many years to model the real world objects. However, dynamic kinetic DT are essential and for simulating the real world processes.

DPPG generated passwords though have a good memorisable rate, the user gets restricted in choosing passwords and not easy at every instance of password. People can argue that a potential solution to the password checker limitations is to have better web technologies to hide the policies and detect malignant password strength querying. However, it can result in delay in strength feedback and high false-positive rates in detection.

References

[1]. Albers, G. (1991). Three-Dimensional Dynamic Voronoi Diagrams, Ph.D. Thesis, University of Wurzburg, Wurzburg, Germany, (In German).

[2]. Albers, G., Mitchell, J.S.B., Guibas, L.J. and Roos, T. (1998). Voronoi Diagrams of Moving Points, International Journal of Computational Geometry and Applications, 8: 365-380.

[3]. Albers, G. and Roos, T. (1992). Voronoi Diagrams of Moving Points in Higher Dimensional Spaces, In Proceedings of the 3rd Scandinavian Workshop On Algorithm Theory (SWAT 92), Helsinki, Finland, Lecture Notes in Computer Science (LNCS), Vol. 621, Springer-Verlag, pp. 399-409.

[4]. Aurenhammer, F. (1991). Voronoi Diagrams - A Survey of a Fundamental Geometric Data Structure, 23(3): 345-405.

[5]. Bajaj, C. and Bouma, W. (1990). Dynamic Voronoi Diagrams and Delaunay Triangulations, In Proceedings of the 2nd Annual Canadian Conference on Computational Geometry, Ottawa, Canada, pp. 273-277.

[6]. Bowyer, A. (1981). Computing Dirichlet Tessellation, The Computer Journal, 24(2): 162-166.

[7]. Brown, K.Q. (1979). Voronoi Diagrams from Convex Hulls, Information Processing Letters, 9(5): 223–228.

[8]. Cignoni, P., Montani, C. and Scopigno, R. (1998). A Fast Divide and Conquer Delaunay Triangulation Algorithm, Computer-Aided Design, 30(5): 333-341.

[9]. De Fabritiis, G. and Coveney, P.V. (2003). Dynamical Geometry for Multiscale Dissipative Particle Dynamics, Computer Physics Communications, 153: 209-226.

[10]. Devillers, O. (2002). On Deletion in Delaunay Triangulations, International Journal of Computational Geometry and Applications, 12(3): 193-205.