Secure Authentication Scheme using Dual channels in RAP Environments.

[1] N. Neelima, [2] M. Usman Gani Khan
[1]PG Scholar, [2]Assistant Professor
[1, 2] Department of Computer Science and Engineering
[1, 2] SSITS, JNTUA, India.

Abstract: Authentication performs an important role in keeping any online banking system, and many banks and different services secure those which rely on username/password for user verification. To remember usernames and passwords became difficult task. Additionally, traditional authentication methods have failed time and again, and they are not immune over many attacks those can introduced against users, networks or authentication servers. From many years, the reports of data breach emphasize that attacker have created various high-tech tricks to crack users data which leads to a severe threat. In this paper, we proposed an efficient and practical user authentication technique for personal devices that uses various cryptographic primitives, like encryption, digital signature, and hashing. The benefit with this technique is that from the greater use of ubiquitous computing and different wearable and portable devices which enables users to perform a safe authentication protocol. The technique which we proposed do not needed an authentication server to manage static username and password tables to identify and verify the login user's legitimacy. In addition to keeping password-against related attacks securely it also opposes replay attacks, shoulder-surfing attacks, and phishing attacks and data breach incidents.

Index Terms **- Security, authentication, password related attacks, one-time password**

I. INTRODUCTION

Former authentication models like username and/or password led to danger threat to online banking services, financial systems and their users. Many present authentication systems permits user to select a constant and unique username which is treated as label. This label is typically attached to user for a longer period. Unfortunately, users use the same user id in various websites and systems [1]. Additionally, most of the users continue to use the similar password over online accounts and systems [2]. As per recent study [3,4], 51% of surveyed users use the same password again on several websites and above 77% of users slightly change or reuse prevailing passwords with simple techniques. We have considered this as RAP (Rouge Access Point) environment. This common practical led to security issues like insider attacks. Malicious administrators or insiders, who have access to username and password tables, can leverage the data to access other services and websites. Malicious insiders will be benefited by selling this sensitive data on dark web by using Bitcoin and Zerocoin payment systems which are untraceable. Besides, this practice allows a phisher to use credentials of user's on multiple websites [5].

Phishing is a kind of social engineering attack where a malicious user otherwise called as phisher, attempts fraudulent activity to get legitimate users' credentials by masquerading as trustworthy entity or public organization. A phishing attack is carried out with the use of various means of communication like emails or instant messages, and it generally directs the victim to duplicate website that looks like real message [6]. Such type of attackers will target a user group or an individual user and harvest their usernames and passwords and try to login to critical systems like online banking. One of the major problems that allow phishing attacks is use of static credentials. In this paper, we depict how smart personal device improves not only security but also improves user's experience by introducing a one-time username authentication coupled with a secure verification code for every login session. The users need not to remind more usernames or recall critical passwords. We highlight the prime contributions of this paper in below:

i. We model and implement a new scheme that combines encryption and signature where user needs not to recall usernames and passwords. This scheme gives better security levels and reduces risks related to legacy authentication methods.

ii. We proposed user-centric access control concept, which plays a key role in authentication and improves security. In user-centric access control, users have self-accessed so that they are able to set permission for their account for every login session.

iii. We examine the preciseness of introduced scheme of authentication and provide its efficiency and feasibility. Specifically, we analyse this authentication scheme's security in different ways such as phishing attacks, password-oriented attacks, shoulder-surfing attacks, replay attacks and so on.

iv. We also show how our scheme obeys the One-Time Pad (OTP) property for session key and verification code, which improves the authentication security.

v. We evaluate the proposed scheme of authentication performance in terms of communication/computation overhead. This paper is organized as follows. Section 2 describes the related work, Section 3 describes about the literature work and section 4 is about the model and the conclusions are drawn in Section 5.

II. RELATED STUDY

A software-based technique called Google Authenticator or 2-Step Verification provides a second layer of defense [7, 8]. This creates two step verification codes that utilized in addition to account password. One more technique that is widely used is RSA Secure ID [9], which is software or hardware token that creates a new verification code (a six-digit number) at constant intervals. The created code relies on seed which is particular for every token and registered with the authentication server. To complete authentication successfully the server's clock is to be synchronized with the authenticated token's built-in clock. Varied from prevailing works, we exploit dynamic authentication credentials along with user-centric access control to clear the constant credential problem. Our approach is to introduce one-time usernames using smart devices and cryptographic primitives like encryption, digital signature and hashing. The aim is to create a username and password set uniquely for every session where different security vulnerabilities in traditional, constant username and password can be tackled [10].

2. 1 Types of Attacks

In this section, we analyzed the proposed authentication scheme's security under various attacks, and show how to use cryptographic primitives and security services in our work and can counter these attacks. To do cryptographic computations we consider the registered device with secure environment. We have shown few of the security attacks in Figure 1 and we described briefly about phishing attacks, password related attacks etc. [11].

2.1.1 Security Attacks

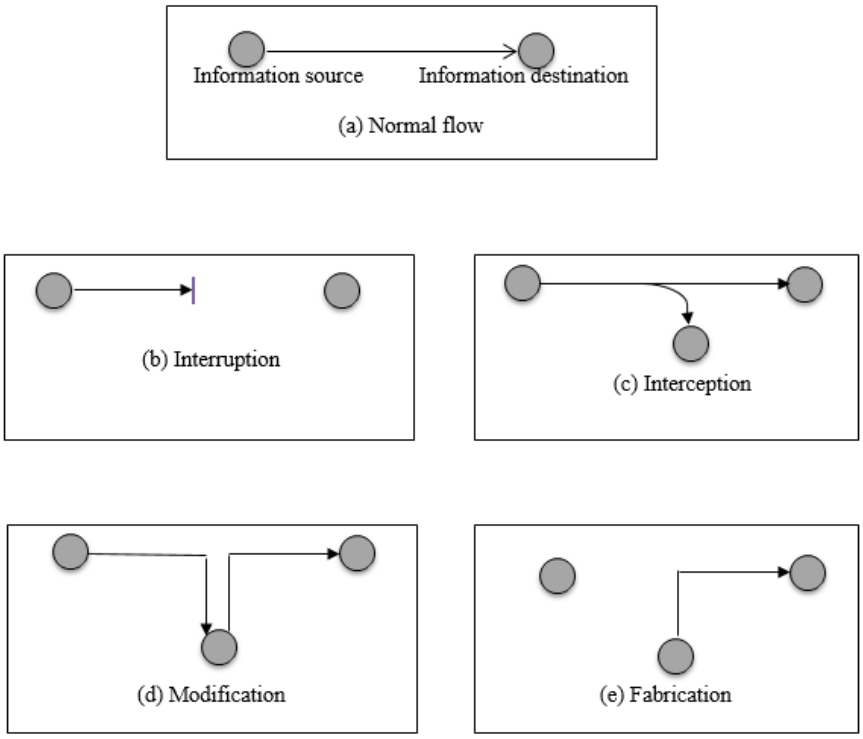

Figure 1: Security Attacks

2.2 PHISHING ATTACKS

Most of the phishing attacks are modeled to steal credentials like username and password by masquerading as a trustworthy entity.

Figure 2: Fishing Attack

2.3 PASSWORD-RELATED ATTACKS:

Protection against various password oriented attacks namely shoulder-surfing attacks and direct observation attacks. Now the client is prevented from using static usernames and passwords which are found with the use of thermal imaging or by finding the pressed keys using mechanical vibration analysis. Issues like using client's birthday as password ,using the similar password everywhere, or forgetting the password are ignored because we are dependent on group of dynamic username and password that is unique for every login session[12].

2.4 SHOULDER-SURFING ATTACKS

Using a static username and password combination also suffers from the shoulder-surfing attack, which is commonly used to harvest sensitive information, such as the password. A malicious attacker uses various direct observation techniques finds the victim and get its credentials. To capture a password a one straight forward method look after the victim's shoulder Shoulder-surfing attacks can also be performed long distance away with the aid of vision enhancing devices [13].

Figure 3: Shoulder surfing Attack

2.5 REPLAY ATTACKS

A client can update on-time username and its session key on client side for every authentication request. Also the ticket expires in a short time period. Time stamping with User Login List ULL gives an effective way to prevent replay attack. Note that server creates a valid verification code in very short period (for instance 5 minutes), for verifying client's identity. So that we claim that the server refuses replay attacks.

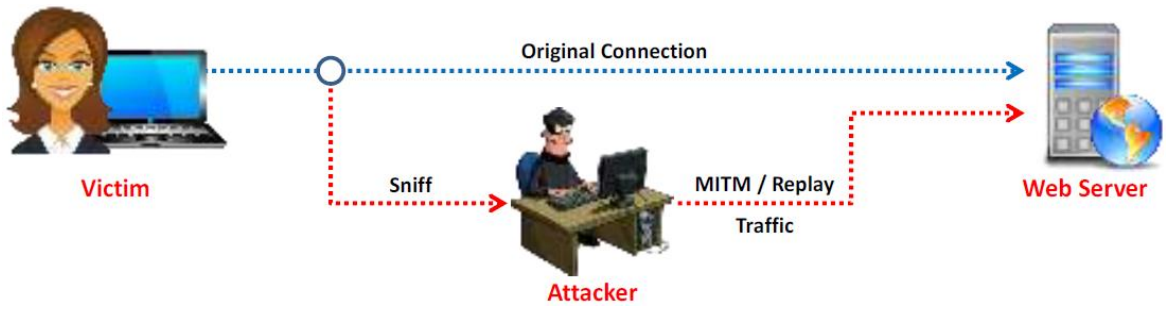

Figure 4: Replay Attack

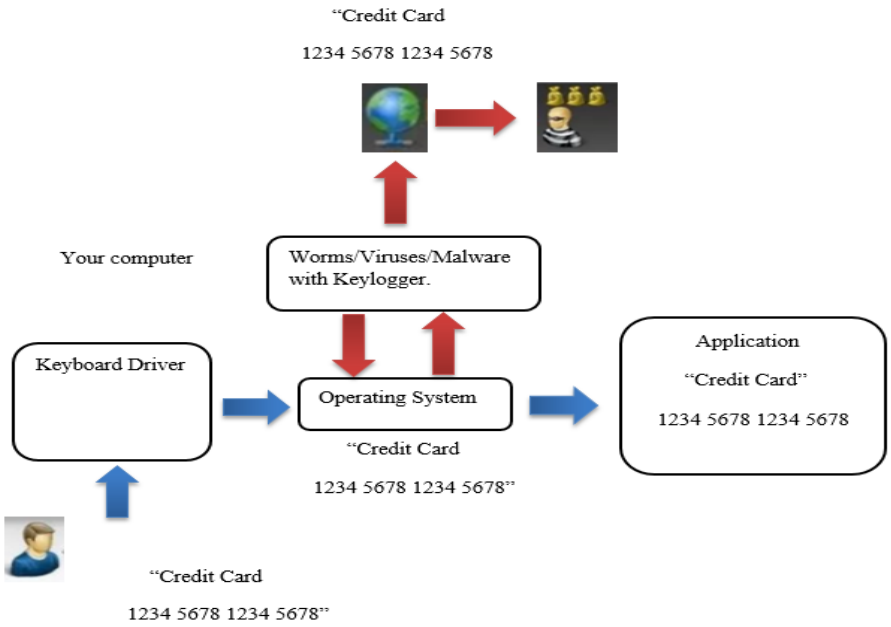

Figure 5: Key logging Process

III. LITERATURE WORK

The goals of this study are to model a new authentication scheme by using dynamic usernames and to show the necessity to store credentials of user's at centralized place. We conceive that present design shall oppose many attacks and risks such as key logger attacks, shoulder-surfing attacks, data breach incidents, reusing password and other human factors. Key logger attacks are turning complex and focus on constant authentication schemes. A key logger is a plug-in hardware device or can be a software code that is considered as a malicious process resides in victim's system. The main aim of using key loggers is to capture and keep track of each keystroke typed on victim's system [14]. This system contains information related authentication like usernames and passwords. Generally, it is difficult to find key logger software and hardware specifically in public computers. Some highly developed key logger software is rooted in operating system and do not displayed in the processes list of task manager. Although many countermeasures could mitigate the risk of key logger attacks, many new issues, tools, and techniques are still evolving In 2011, with 80% accuracy, researchers illustrated that it is feasible to capture keystrokes of a nearby computer utilizing the accelerometer found in many smartphones.

This yield emphasizes the belief that there is no solution to control the problem with key logger in username and password system and is essential to enhance the former schemes of authentication. Another issue which affects the former authentication schemes' security is Shoulder-surfing attack. This attack occurs when an attacker use direct observation technique like looking on somebody shoulder or to capture the sensitive data with hidden cameras. But shoulder surfing is efficient way to focus on traditional authentication schemes and retrieve passwords, PINs and other sensitive information. It is easy to perform shoulder surfing attack since this does not need a greater experience and no specified knowledge on it. Modern authentication schemes must consider the shoulder-surfing attacks resistance and shrink the attack surface. One more issue is data breaches which is becoming popular in today. Data breaches have greater impact over users and financial institutions. Most of data breach issues has usernames and passwords in disclosure and various leading experts treat data breaches as it has a big security problems facing by security professionals and system administrators. The causes with data breach are turning out into severe, and it is tough to estimate the damage on breached organization and the users' accounts in various online services. In October 2013, Adobe faced a breach that results in leaking about 153 million user's records. Every user record has an internal ID, email address, a username and a password which is encrypted, along with a password hint in plaintext. Unluckily as the password cryptography was poorly designed there is possibility of plaintext decryption with ease. One more instance to be noticed here is that the data breach of 13 million user accounts from a website in March 2015 [15]. The leaked data has names, email addresses and also passwords of plaintext.

A malicious cracker could leverage the credentials that are leaked to focus users' online banking accounts and do malicious activities like sharing financial related data or transferring money overseas. The combination of username/password is the major cause of data breach revealed from

Verizon report 2014. The similar report shows that 76% of data breaches, attackers are able to gain control by stealing user's credentials. As per security firm Hold Security, a cyber-gang breached around 420,000 web and FTP sites to yield more than 1.2 billion credentials; this will be the one of the biggest data breaches reported to media. All earlier mentioned data breaches, attacks, and issues leads to a severe threat called domino effect of reusing password. The domino effect is the output of a password file handover by malicious user, who then utilize it to crack other online account. One more issue with the same combination is that a huge number of usernames and passwords are to be maintained by user at internet. The enhancement of e-banking and g-government has led to a greater increment in the number of credentials managed by user. Tele Sign research, for instance, reported that an active web user an average of 24 passwords on a daily basis. Unfortunately, the similar study mentioned that 73% of accounts are using duplicate passwords. Additionally, 68% of surveyed respondents that they need online firms to provide a new security solution to keep their personal data secure.

IV. PROPOSED MODEL

Under this section, we are covering major components of our system model, threat model, design goals and notations.

A. SYSTEM MODEL

As shown in figure 1, our system model has two main entities are client and server. The registered devices and user's terminal are included under client side. Every entity's primary functions are clearly summarized in the below:

_ ***Registered devices:*** A device is said to be registered as those devices which perform cryptographic operations like a smart phone or a smart watch. Every user wants to register a device with server so that the user could get the services from server. A legitimate user is able to have services by providing no static username and password. Here, we are assuming that a user was already underwent registration of a smart device with server.

_ ***User's terminal****:*

An electronic device is treated as user's terminal like a laptop or desktop and it is used for server login in order to view or proceed transactions.

_ ***Server:***

The server relates to an entity like a bank and is connected with HSM (Hardware Security Module) that protects the private key and allows crypto-processing. The server distributes its public key and verification code to the clients and offer services.

B. THREAT MODEL

In this paper, we consider the semi-honest model [15], in which precise specification is followed by the server and clients as well but both try to learn more information possibly. The notable thing here is that this model does not have a powerful attacker who has control on device and access the private key will be our future work.

C. DESIGN GOALS

Under this section, the goals whichever satisfied by the protocol are identified and are shown in the following.

_ **Correctness:**

If client and server follow the protocol precisely, both can get an exact authentication result.

_ **Security:**

The protocol keeps the client's privacy data securely. At one side, the encrypted text is given, the attacker unable to retrieve client's original input data. On the other side, the exact result is kept in hide from an attacker.

_ **Verification:**

The message of client and verification code is being verified by the server successfully. Few of the notations used in our work are shown in Table 1.

Abbreviation	Description
M	One Time Login Ticket
OTU	One Time Username
HSM	Hardware Security Module
ACL	Access Control List
TVP	Ticket Validity Period
VC	Verification Code
k	Session Key
T	Timestamp
ULL	User Login List
H(.)	Hash Function
E(.)	ECIES Encryption
D(.)	ECIES Decryption
Enc(.)	AES Encryption
Dec(.)	AES Decryption

Table 1: Notations used in our work.

V. AUTHENTICATION PROTOCOL DESCRIPTION

This section is specified for our proposed protocol's description, which can be utilized in various domains like online banking, e-government and e-Health systems. To demonstrate our protocol we are using online banking system. We initiate by providing the ticket information, then the details of protocol steps completely.

A. SESSION TICKETS

A user resorts to its registered device to create a ticket for every session whenever the user needs to login his account he can login. The ticket is generated by registered device and sends it to server to verify it and is encrypted by using server's public key. As shown in Figure 6, a login ticket has mainly an OTU-One Time Username, a session key s, a Ticket Validity Period TVP, a timestamp T, and an Access Control List ACL. The ticket details are depicted in below:

1) ONE-TIME USERNAME

It has eight characters including capital and small letters, numbers, special characters. The one-time username must be generated randomly using the registered device. We select 8 characters because mostly the systems are configured to handle 8 characters.

2) SESSION KEY

A registered device like smart phone randomly creates a session key for every login session. The session key is a symmetric key that is used for encryption of verification code between user and the server.

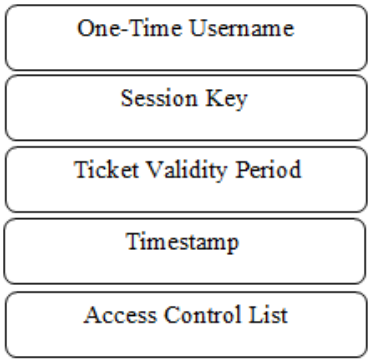

Figure 6: Ticket Information

3) TICKET VALIDITY PERIOD

To restrict the ticket's lifespan it is considered as a security parameter. In our model, we enable user to mention the validity period of ticket; anyways, security administrators can set a maximum lifetime for tickets**.**

4) TIMESTAMP

It is an instance of time at which the registered device grants a ticket. The timestamp is represented in a consistent format that makes the server to compare two different tickets easily and keeps the track of user's login activities over time.

5) ACCESS CONTROL LIST

The user mentions the list of access control. In respect to our design in this paper, it is a list of permissions attached to a ticket and it varies for every login session. To remain simple, we considered two permission modes.

_ Active mode permission:

The active mode enables users to make actions on the account. Let's take online banking system as an example. Here, whenever user chooses this permission, it provides him full control over the account. It also includes various privileged activities like performing transactions, requesting banking services and adding or deleting fund transfer beneficiaries in the account.

_ Passive mode permission:

This mode limits the users only to view the transactions, not to perform any further active operation. Specifying permissions offers a user-centric access control model and makes the users engage in setting permission to ticket. It has more benefits like good security with the utilization of least privilege principle. Such model follows the principle of providing those principles to user account which are essential for user's work. The data flow diagram of our work is shown in Figure 7.

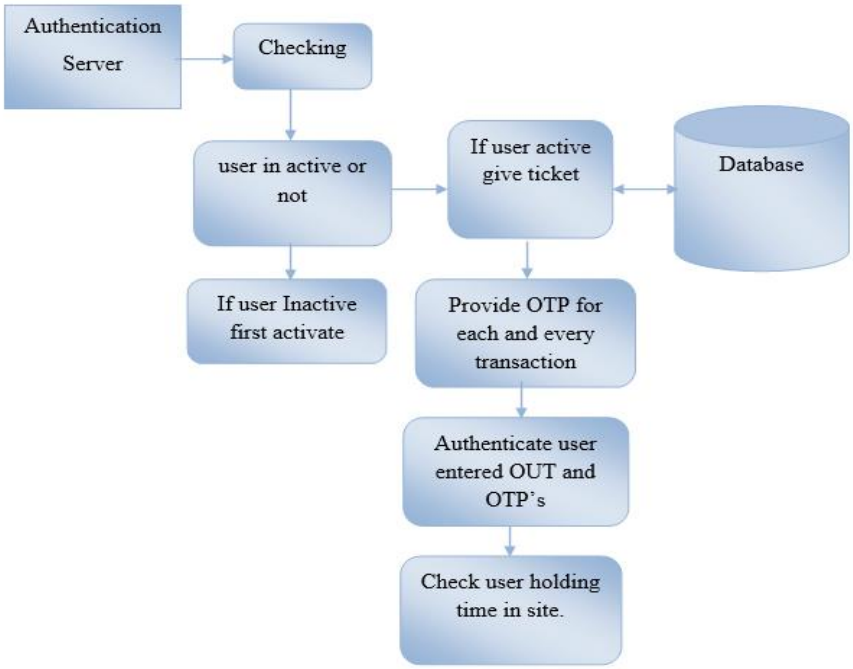

Figure 7: Data flow diagram of our work.

VI .CONCLUSION

The drastic growth in online banking and e-commerce systems led to a greater increment in number of usernames and passwords managed by single user. The previous used protocols are username and password suffers from different security related issues. Most of the users initiate using untrusted credentials time and again in different accounts and systems. Leaking or compromising one account could cause an attacker to infiltrate other systems and endanger users' security and privacy. In this paper we propose a new authentication technique which enables users to prevent many issues like reminding usernames and passwords for various websites and systems. The authentication model that we introduced will shows the way for user-centric access control that helps in reducing the risks of many attacks. There are many research ways that can be further explored in our research work in future. Firstly, we perform investigation by using light weight cryptographic techniques in our model. Next we plan to scrutinize the design of different user-centric access control models. We also intended to study the schemes for enhancing the authentication techniques like use of visual decryption and visual signature verification. Eventually, reporting on usability of the proposed authentication scheme should be further investigated in our future work.

REFERENCES

[1] A. Alhothaily, A. Alrawais, X. Cheng, and R. Bie. Towards more secure cardholder verification in payment systems. In Z. Cai, C. Wang, S. Cheng, H. Wang, and H. Gao, editors, Wireless Algorithms, Systems, and Applications, volume 8491 of Lecture Notes in Computer Science, pages 356–367. Springer International Publishing, 2014.
[2] A. Alhothaily, A. Alrawais, X. Cheng, and R. Bie. A novel verification method for payment card systems. Personal and Ubiquitous Computing, 19(7):1145–1156, 2015.
[3] A. Alrawais, A. Alhothaily, and X. Cheng. Secure authentication scheme using dual channels in rogue access point environments. In Wireless Algorithms, Systems, and Applications, pages 554–563. Springer, 2014.
[4] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng. An attributebased encryption scheme to secure fog communications. IEEE Access, 2017.
[5] K. Aravindhan and R. Karthiga. One time password: A survey. International Journal of Emerging Trends in Engineering and Development, 1(3):613–623, 2013.
[6] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Security and Privacy (SP), 2012 IEEE Symposium on, pages 553–567. IEEE, 2012.
[7] B. Borchert and M. Gunther. Indirect nfc-login. In Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for, pages 204–209. IEEE, 2013.
[8] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung. Fourthfactor authentication: somebody you know. In Proceedings of the 13th ACM conference on Computer and communications security, pages 168–178. ACM, 2006.
[9] Rsa securid, 2016. Available at http://www:centera:us/security/rsasecurid/index:htm, Date last accessed 15-Feb-2016.
[10] N. Chou, R. Ledesma, Y. Teraguchi, J. C. Mitchell, et al. Client-side defense against web-based identity theft. In Symposium on Network and Distributed System Security (NDSS), 2004.
[11] F. F. I. E. Council. Authentication in an internet banking environment. Financial Institution Letter, FIL-103-2005. Washington, DC: Federal Deposit Insurance Corp.(FDIC). Retrieved March, 18:2005, 2005.
[12] Cronto visual transaction. Available at https://www:cronto:com/, Date last accessed 2-Feb-2017.
[13] W. Dai. Crypto++ 5.6. 0 benchmarks, 2009. (Date last accessed 15- July-2014).
[14] D. Damopoulos, G. Kambourakis, and S. Gritzalis. From keyloggers to touchloggers: Take the rough with the smooth. Computers & Security, 32:102–114, 2013.
[15] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In Symposium on Network and Distributed System Security (NDSS), 2014.

N. Neelima is a PG scholar in the school of Computer science and Engineering in SSITS, JNTUA. She received her Bachelor's degree in 2015 from JNTUA University in the stream of Computer Science and Engineering. Her research interests include Networks Security and computer networks.

M Usman Gani Khan is currently working as Assistant Professor in the department of Computer Science and Engineering in SSITS, JNTUA. He received his master's degree from JNTUA in 2016 and Bachelor's degree in 2014. He has 2 years of experience and has taught various subjects in computer science stream His research interests are Knowledge Engineering, Network Security, and Recommender Systems. He also published various National and International Journals.