Security Keys: Modern Security Feature of Web

Deepika Kamboj
KIET Group of Institution,
Ghaziabad

Varsha Gupta
KIET Group of Institution,
Ghaziabad

ABSTRACT
Security providing devices that are used to protect against multiple threats like man-in-the-middle attack and phishing are known as "security keys". With the help of security keys, user can register himself with any kind of online services that works with this protocol. If we install these security keys in some devices, deployment, implementation and use becomes very easy. We can also see the security keys in some browsers like chrome, Mozilla, even in some online services as well. These keys provide more satisfaction to user with the help of higher security level. This work is all about security keys which are second-factor devices that are used to improve the state of the art for authentication purpose for real consumers in terms of privacy, security, and usability.

Keywords
Authentication, client, keys, signature, registration

1 INTRODUCTION
There are many research papers which have been proposed to work on some other security feature rather than passwords. But till no such efforts is successful. Even most of the service providers works on password-based authentication with one other feature i.e. OTP (One Time Password). One Time Passwords also not provide complete security in some of the common attacks. In this way deployment of OTPs is limited in case of reliability and security perspective. Each and every client who is working on the internet wants security of information but sometimes he or she do not know that someone else may be a intruder is collecting the information. Information is an asset that must be protected [11]. At the same time, other authentication and security factors related to response and challenge based protocols also suffer from some deployment problems. On the other hand smart cards and NID (National ID) cards require some pre-installation before use. Protocol is proven to be secure under CDH assumption in both the random oracle model and the ideal cipher model [8].Over forty years of research have demonstrated that passwords are plagued by security problems [2] and openly hated by users [3]

The security is achieved in the formal security model of Bellare et al. [9].This work is related to one other security factor provided by "Security Keys". These Security keys help the user in better way than OTPs in terms of usability, authentication, privacy etc. Here we will see how security keys increase the security level and how they provide satisfaction to user.

2 RELATED WORKS
Now we will have an overview of related work. Some schemes can do better than passwords on security—as expected, given that inventors of alternatives to passwords tend to come from the security community. The concept of using combining functions to determine the combined effect of vulnerabilities in a network[12].Network security involves the authorization of access to data in a network, which is controlled by the network administrator [10]. Some schemes do better and some worse on usability—suggesting that the community needs to work harder there.[1] Before that let's see some basic knowledge that will help us to understand the work done.

One Time Passcodes: Even though One Time Passwords provides higher security than simple passwords, still we suffer from some problems. First, OTPs are vulnerable to some cyber-attack like man-in-the-middle attack and phishing. Second, OTPs require the availability of phones and internet as they are send via messages or emails. OTPs offer a sub-optimal user expertise as they typically need the user to manually copy codes from one device to a different. Security Keys are unit immune to phishing and man-in-the-middle by design; our preliminary study conjointly shows that they supply a far better user expertise.

Smartphone: Many of the efforts were taken to take the leverage of user's mobile phone to provide more security, whether it is in industry or academics. At the time of promising, they face lots of challenges: Like, on a general purpose, protection of application logic from malware is very difficult. Even though, sometimes user's phone gets unreachable or data connection problem is there or battery related issue

may be there. There is no requirement of batteries in security keys.

Smart Cards: Security Keys work into the what you have class of authentication schemes and have a detailed relationship to smart cards. Whereas Security Keys are often enforced on prime or top of a smart card platform like JavaCard, Security Keys defines a specific protocol for which smart cards area unit only one attainable implementation platform.

TLS: TLS is a Transport Layer Security (TLS) protocol which is used to provide security, data integrity and privacy between two communicating parties. Now a Days TLS is the only security protocol which is widely deployed today. On the other hand TLS is used for Web browsers and some other kind of applications which requires data to be securely transmitted over a network like VPN Connections, Voice over IP, File Transfer and instant messaging. TLS basically consists of two types of protocols:

- TLS Record Protocol and
- TLS Handshake Protocol

Protocol is proven secure Password-Based Group Key Exchange in a Constant Number of Rounds against dictionary attacks under the DDH assumption, in the ideal-cipher and random oracle models [4]. Proposed the use of probability scores for each vulnerability to represent the likelihood that one attacker or the percentage of attackers that will exploit the vulnerability [13].Record protocol is used to provide secure connection and Handshake Protocol permits the client to authenticate server and vice versa.

Electronic Identification Cards: EID or Electronic Identification Cards works as an identity of every citizen or any organization. With the help of these EIDs people even get benefits of many services provided by the government. For its authenticity EIDs provide users with Electronic Documents where digital signatures can be used.

Even though these cards have been failed in most of the authentication mechanism which are used globally. One main reason of their failure is requirement of a hardware or card reader, which makes them hard to deploy. Second possible reason is these cards are controlled completely by the government which cannot be accepted in other countries. This problem can be resolved with our approach of security keys. These keys are pre-installed in devices and can be access anywhere without the control of any single entity.

3 THREAT MODEL

A classical way to break password-based schemes is the partition attack [5]. An integrated framework for measuring various aspects of network security, metrics developed based on the framework will lead to novel quantitative approaches to vulnerability analysis, network hardening, and attack response [12]. Here we outline some major attacks that we will consider in our design.

3.1 Attackers

Web Attackers: If attacker's aims is to acquire information owned by the web and/or stored in the network. This information may exist in the form of customer information, business-critical information, or intellectual property. Web attackers are very effective in information stealing that 25% of all data breaches.

Network Attackers: Network attacks are defined as some kind of attack or process, means that is used to maliciously get the network security. There are lots of reasons for which attackers want to attack corporate networks. These individual attackers who perform network attacks are basically known as hackers, network attackers or crackers. Some examples that network attackers can perform are given below:

- Stealing hardware
- Stealing data
- Illegally using user accounts and privileges
- Modifying stored data

Related-Site Attackers: Some other kind of attackers' compromise with sites which consist of weak security practices in case of stealing the user's credentials. Often all the users reuse credentials across all the sites related-site attackers will use the stolen credentials on secure sites in hopes of accessing the user's accounts Network Attackers. Network security in the physical layer requires failure detection, attack detection mechanisms, and intelligent counter measure strategies [7].

3.2 Attack Consequences

Here we will discuss the two consequences of most concerning attacks:

Session Duplication: In most of the cases, an attacker can get the credentials that help him to get the access on user's account from anywhere using any computer. For an Example, an attacker is able to login into someone's account, if he can get the cookies or passwords (if password was not changed).

Session Riding: If an user is using his/her computer and at the same time attacker get the access over that and tries to modify that, then this kind of attack is known as session riding. Example, if the website requires user to start a new session with the help of providing proof of a hardware device which can't be controlled by the attacker, in that case only attacker is able to ride the active sessions of user's.

These two consequences can be made difficult using Security Keys. A generic password-based authenticated key exchange protocol, based on any such primitive, with a formal security proof [6].

4 SYSTEM DESIGN

Here we are settled on the following goals:

Easy for Users: Use of security keys is easy, fast. It should be difficult to access Security Keys incorrectly or insecurely.

Privacy: Security Keys must not permit chaseoff any kind. Additionally, if a Security key lost, it must be difficult for an attacker to get some useful information from a security key.

Security: Security keys must protect users against phishing, man-in-the-middle attack and reuse.

Easy for Developers: Integration of security keys into websites should be easy.

4.1 System Overview

Security keys can be used for user's authentication or user's identity. Security keys help in following commands which are present in web pages as browser APIs.

Register: Using this command, Every time security keys generate a new asymmetric key pair and also returns a new public key. This public key is associated with user's account.

Authenticate: Using this command, the Security Key help in testing the user presence and works on its private key to provide a response. Then server verifies that the response is valid, and thus authenticates the user.

4.2 Detailed Design

Registration: The relying party the server generates a random challenge. The user's browser combines the server's challenge into a Client Data structure, which is to be covered in short time. The browser sends the server's web source and a hash of the Client Data to the Security Key. As a result, the Security Key generates a new key pair along with a key handle. The Security Key merges the key pair with the relying party's web source and then returns the produced public key, key handle, an attestation certificate, and a signature over 1. The internet source, 2.hash of the client data, 3. Keyhandler and 4.Public key. The web browser then sends this data, along with the client data, back to the website. The site verifies the signature and associates the public key and key handle with the user's account.

Authentication: The relying party requests that the Security Key exercise a particular key. This particular key already registered for a user account. The relying party forwards the desired key's handle and a challenge to the web browser. The browser generates the client data (see above) and sends the hash of the sender's data along with the key handle and the internet origin to the Security Key. If the Security Key does not recognize the key handle or doesn't agree that it associates with the web source that requested the signature, it rejects the request. Otherwise, it generates a signature of the client data. The Security Key signs two additional attributes: a Test of User Presence (TUP) succeeded, and a counter value. The

description shown below gives the User Presence. The counter value is a 32-bit counter that increments with every signature the Security Key perform; its presence allows the server to detect possible cloning of Security Key, e.g., when counter value seems to decrease from one signature to the next. The browser forwards the signature, attached with the counter value and TUP to the server. Server then verifies the signature against the public key it has registered and authenticated the user if the signature matches.

Client Data: The client data binds the server-generated challenge to the browser's view of its connection to the server. Specifically, the client information includes request type (register or authenticate), the challenge, and, when possible, the TLS channel ID of the connection. Binding the TLS channel identifier permits the server to find the presence of a TLS Man in the Middle. When a server gets a signed TLS channel ID, it can compare it with the TLS channel ID.

Test of User Presence: (TUP) allows the caller to check a human is present or not during command execution. It has two purposes: First, it gives a mechanism for confirmation of commands. Second, it permits internet applications to implement a policy which is based on that check For example, Transactions for a dollar amount more than $1,000

needs confirmation," or Credentials should be presented again by a human after 3 months." Test of User Presence implementation is based upon the device manufacturer. If one vendor uses a touch sensor, others can employ a mechanical button, while another one makes a device which stays powered up only for a very short time after inserting into a USB port, which requires the user to re-insert the device for every operation.

5 IMPLEMENTATION

Security Keys needed proper end-to-end support. For providing this support many components are implemented.

5.1. Client-side Support

For the client-side support security keys, carried out as a part of web browser.

Registration Method

Registration of a security key is requested by the server-side by the help of updated browser API (application programming interface).

u2f.register()

API keep the record of the register keys, that help a web browser to check the eligibility of a security key. Eligibility i.e. one security key can register only once.

When a request takes place for registration, Browser check the record of registered keys, if key is not registered then register command send to the Security key. After the registration command, client send its data and registration message to the server. Server handle the verification of registration signature and client data of its own request. In the end, Server verify that signed certificate according to its ownrequirement. If all the parameters are correct, then private key of server stored by key the handler k_h and public key k_{pub} stored for the users.

Signature Method: A signature of for the security key is requested by the web server, with the help of enhanced browser API.

As described above client send a signature command to the eligible key. After the signature command, client sends signature and its data to the server. Verification of key with the public key k_{pub} is held by server, if verification is successful then counter increased. Servers check the client data according to its requirement and verify it. If all the verification is positive, user authentication is provided.

5.2 Security Key Symbol Implementation

In the implementation of security key there are two major and basic actions: Registration i.e. to generate new keys and Signature i.e to generate the cryptographic sign.

Registration Operation

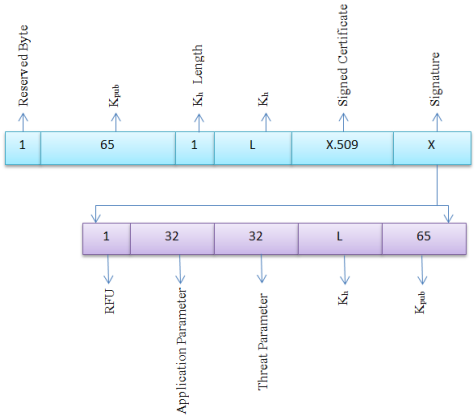

Fig. 1. Security Key Authentication Message

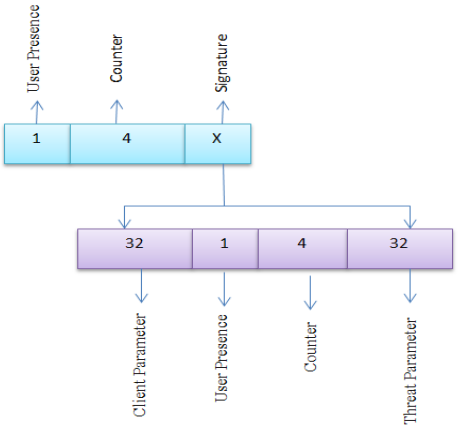

Fig 2: Security Key Registration Message

Registration operation is the combination of two parameters first is client i.e. application parameter and a threat. Above already explained that new combo of keys (k_{pub}, k_{pvt}) developed by security key for the clients.

Signature Operation

In signature parameter three types of parameter are used first application parameter, a key handle k_H and a threat. Signature operation performs to provide authentication. Major operation performs during authentication for the retrieval of the application parameter and k_{pvt} for k_h. After it security key verify the k_h and application parameter with retrieved parameters, if any one of them does not match, operation is refused with an error message. In such manner, server tries to utilize k_h.

If the valid private key k_{pvt} for k_h retrieved by the security key, then it is verified that developed for the

required application parameter. The above process increase the counter value that shows the presence of user and signature provided to the server which is combination of user presence indication, updated counter value and the threat parameter. An authentication message is output of the signature operation.

Store and Retrieve Operations: Store and retrieve are considered as database operations where storing a secret key works like an index into a table, and then this index is returned as K_h. On the other hand retrieving a K_h finds the value in the table at particular address index.However, an implementation like database decreases usability and privacy: a predictable index for K_h displays total accounts for which a Security Key is being used. Additionally, the usersmust aware of the storage of Security Keys so that it doesn't run out of space in key database.

In our implementation, store is implemented as a key wrapping operation: the private key k_{pvt} and the application parameters are encrypted using a secret key K wrap. By implementing store and retrieve as key wrap/unwrap operations; the Security Key reference implementations can store an unlimited number of key handles: the storage is implemented by the server.

function store(k priv , app)

app 0 ← Encrypt(app) K app

plaintext ← Interleave(k priv , app 0)

H K ← Encrypt(plaintext) K wrap

return H K

end function

function retrieve(H K , app)

app 0 ← Encrypt(app) K app

plaintext ← Decrypt(H K) K wrap

(kpriv , app 00) ← Deinterleave(plaintext)

constant-time check(app 0 == app 00)

return k priv

end function

Comparative Study

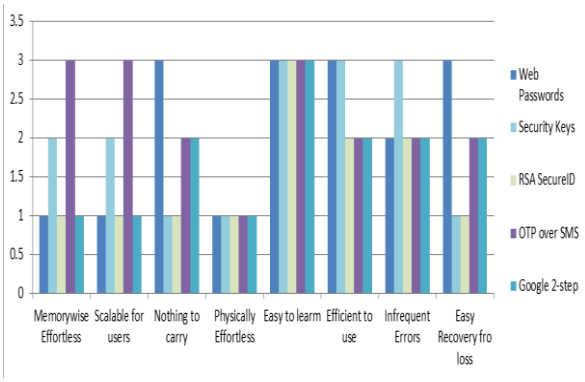

Fig. 3. Comparative study in terms of usability

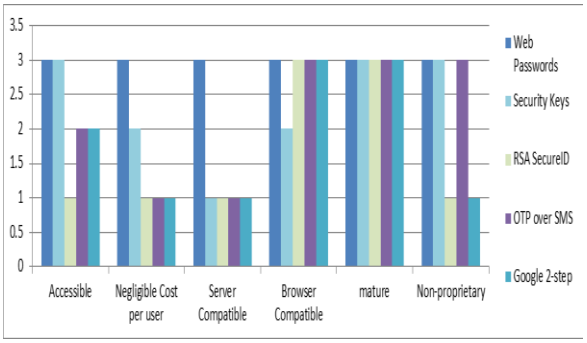

Fig. 4. Comparative study in terms of Deployment

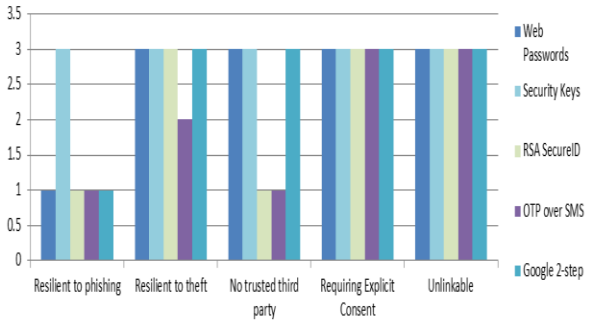

Fig. 5. Comparative study in terms of Security

6 CONCLUSION

Authentication on the web can be enhance by a unique technique presented in the above paper i.e. security keys. Many attacks (phishing, password reuse, man-in-middle) can be prevented by the uses of these security keys. Initial analysis of sign in data estimates the advantages of security keys for the user and the organization. The security key protocol can be standardized by FIDO Alliance organization as the Universal Second Factor (U2F) open standard. Browser and login system of major web service providers supports security keys. Above study may contribute a important role in academic foundations and in authentication.

7 REFERENCES

[1] Bonneau, J., Herley, C., van Oorschot, P.C., Stajano, F.: The Quest to Re-place Passwords: A Framework for Comparative Evaluation ofWeb Authentication Schemes. In: 2012 IEEE Symposium on Security and Privacy. (May 2012)

[2] R. Morris and K. Thompson, “Password security: a case history,” Commun. ACM, vol. 22, no. 11, pp. 594–597, 1979.

[3] A. Adams and M. Sasse, “Users Are Not The Enemy,” Commun. ACM, vol. 42, no. 12, pp. 41–46, 1999.

[4] Michel Abdalla, Emmanuel Bresson, Olivier Chevassut and David Pointcheval,
Password-based Group Key Exchange in a Constant Number of Rounds,
Public Key Cryptography - PKC 2006, Moti Yung, YevgeniyDodis, AggelosKiayias, and Tal Malkin (Eds.), LNCS 3958, pp. 427-442, Springer-Verlag, April 2006

[5] C. Boyd, P. Montague, and K. Nguyen. Elliptic Curve Based Password Authenticated Key Exchange Protocols. In ACISP ’01, LNCS 2119, pages 487–501. Springer-Verlag, Berlin, 2001.

[6] Dario Catalano, David Pointcheval and Thomas Pornin, Trapdoor Hard-to-Invert Group Isomorphisms and Their Application to Password-based Authentication,
Journal of Cryptology, vol. 20, no. 1, pp. 115-149, Springer-Verlag, IACR, 2007.

[7] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008.

[8] RatnaDutta and RanaBarua, Password-based Encrypted Group Key Agreement,
International Journal of Network Security, vol. 3, no. 1, July 2006.

[9] M. Bellare, D. Pointcheval and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in B. Preneel, editor, Eurocrypt 2000,

[10] Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323

[11] Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," In Proceedings International Conference on Advnaced Communication Technology, 2004.

[12] Lingyu Wang, AnoopSinghal, SushilJajodia,"Toward Measuring Network Security Using Attack Graphs," Proc. QoP 2007, Oct 29, 2007.

[13] Tania Islam, Tao Long, Lingyu Wang, AnoopSinghal, and SushilJajodia, A Probabilistic Network Security Metric Based on Attack Graphs, Technical Report, Concordia University,