ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Web Based Security Analysis of OPASS Authentication Schemes Using Mobile Application

Mohammad Sharique
M.Tech,
Dept of Computer Science Engineering,
K.G.Reddy College of Engg and Technology,
Hyderabad, Telangana, India.

Mr.M.SaidiReddy
Associate Professor,
K.G.Reddy College of Engg and Technology,
Hyderabad, Telangana, India.

Abstract:

In this paper, we have a tendency to style a user authentication protocol that involves user's telephone and short message service to forestall Arcanum stealing and recycle attacks. Reusing Arcanum's across completely different websites could cause users to lose their data that is keep in websites once the password hacked or compromised by wrongdoer. Second, hackers will install malicious software system to induce the passwords, once user writing their username and Arcanum into unknown public computers. During this paper, developing net based mostly security analysis of 1 Time Arcanum authentication schemes exploitation mobile application. Opus solely needs every taking part web site possesses a singular number, and involves a telecommunication service supplier in registration and recovery phases. Through Opus, users solely have to be compelled to bear in mind a semi-permanent Arcanum for login on all websites. Once evaluating the Opus image, we have a tendency to believe Opus is economical and reasonable compared with the standard net authentication mechanisms.

Keywords:
Password Reuse Attack, Password Stealing Attack, User Authentication.

INTRODUCTION:

OVER the past few decades, text watchword has been adopted because the primary mean of user authentication for websites. Individuals choose their username and text passwords once registering accounts on an internet site. So as to log into the web site with success, users should recall the chosen passwords. Generally, password-based user authentication will resist brute force and lexicon attacks if users choose sturdy passwords to produce comfortable entropy. However, password-based user authentication includes a major downside that humans don't seem to be consultants in memorizing text strings. Thus, most users would select easy-to-remember passwords (i.e., weak passwords) even though they recognize the passwords could be unsafe. Another crucial downside is that users tend to apply passwords across varied websites.

To develop net primarily based security analysis of DUOS authentication schemes mistreatment mobile application. Watchword primarily based authentication could be a user friendly authentication mechanism and additionally simple probability to hack (dictionary attacks, phishing attacks, watchword stealing and apply attacks, malware) the accounts. So, we'd like to boost the protection levels of associate application. For that we tend to area unit implementing protocol primarily based communication between net and mobile application and that we area unit projected new approach authentications that have higher security level compare to the other authentication mechanism.

- Problem Definition: Text watchword is that the hottest type of user authentication on websites attributable to its convenience and ease. However, users' passwords area unit vulnerable to be purloined and compromised below totally different threats and vulnerabilities. Firstly, users typically choose weak passwords and apply constant passwords across totally different websites.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Habitually reusing watchwords causes a domino effect; once associate antagonist compromises one password, she's going to exploit it to realize access to additional websites. Second, typewriting watchwords into untreated computers suffers password outlaw threat. Associate antagonist will launch many watchword stealing attacks to grab passwords, like phishing, key loggers and malware.

EXISTING SYSTEM:

A user will perform the bulk of browsing interactions from the computer and solely perform terribly sensitive interactions from the personal digital assistant (Personal Digital Assistant). Session scientific instrument permits a user to completely make the most of the convenience of employing a computer.

- Catch primarily based Login System
- Text positive identification primarily based Login System
- Cryptography primarily based Login system
- Image primarily based Login System.
- Biometric primarily based Login System

DISADVANTAGE:

- Increasing possibilities for Forget the positive identification with totally different websites.
- Reusing passwords causes a event.
- Hacker Applying Random-Key Function/Method for Hacking the user positive identification.

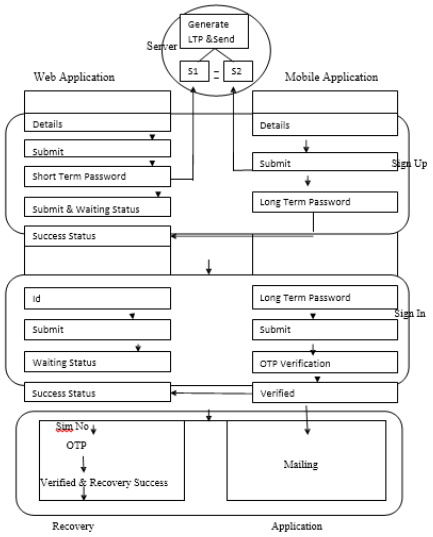
PROPOSED SYSTEM:

The main Objective of OPass is free users from having to recollect or kind any passwords into typical computers for authentication. in contrast to generic user authentication, oPass involves a replacement part, the cellular phone, that is employed to get one-time passwords and a replacement channel, SMS, that is employed to transmit authentication messages.

ADVANTAGES:

- Anti-malware
- Phishing Protection
- Secure Registration and Recovery
- positive identification use hindrance and Weak positive identification rejection
- cellular phone Protection

ARCHITECTURE DIAGRAM



LITRETURE SURVEY:

PERFORMANCE EVALUATION OF PUBLIC-KEY CRYPTOSYSTEM OPERATIONS IN WTLS PROTOCOL:

WTLS (Wireless Transport Layer Security) is a vital normal protocol for secure wireless access to net services. WTLS employs public-key cryptosystems throughout the hand shake between mobile shopper and WAP entranceway (server).Several cryptosystems at totally different key strengths may be employed in WTLS. The trade-off is security versus process and UTC. During this paper, Associate in nursing analytical accomplishment model for public-key cryptosystem operations in WTLS protocol is developed.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Totally different acknowledgment protocols, totally different cryptosystems and key sizes are thought-about. Public-key crypto systems are enforced victimization state-of-the–art performance improvement techniques, yielding actual performance figures for individual cryptosystems. These figures and also the analytical model are accustomed count the value of victimization public-key cryptosystems in WTLS. Results for various cryptosystems and acknowledgment protocols are relatively pictured and taken. It's been ascertained that ECC (Elliptic Curve Cryptography) performs higher than its rival RSA cryptosystem in WTLS. Performance of some stronger computer code curves, that don't seem to be thought-about in WTLS normal, is additionally analyzed. Results showed that a number of those curves can be employed in WTLS for top security applications with an appropriate degradation in performance

PRIVACY-PRESERVING PUBLIC AUDITING FOR DATA STORAGESECURITY IN CLOUD COMPUTING:

Cloud Computing is that the long unreal vision of computing as a utility, wherever users will remotely store their data into the cloud therefore on fancy the on-demand top quality applications and services from a shared pool of configurable computing resources. By information outsourcing, users may be alleviated from the burden of native information storage and maintenance. However, the fact that users not have physical possession of the presumably large size of outsourced information makes the info integrity protection in Cloud Computing a really difficult and doubtless formable task, particularly for users with affected computing resources and capabilities. Thus, facultative public auditability for cloud information storage security is of important importance in order that users will resort to Associate in nursing external audit party to ascertain the integrity of outsourced data once required. To firmly introduce a good third party auditor (TPA), the subsequent 2 elementary needs have to be met: 1) TPA ought to be able to expeditiously audit the cloud data storage while not difficult the native copy of knowledge, and introduce no extra on-line burden to the cloud user; 2) The third party auditing method ought to usher in no new vulnerabilities towards user information privacy. During this paper, we tend to utilize and uniquely combine the general public key primarily based similarity appraiser with random masking to attain the privacy-preserving public cloud data auditing system that meets all higher than needs. To support economical handling of multiple auditing tasks, we tend to further explore the technique of linear mixture signature to increase our main result into a multi-user setting, wherever TPA will perform multiple auditing tasks at the same time. Intensive security and performance analysis shows the projected schemes ar provably secure and extremely economical.

AN IMPROVED DYNAMIC PROVABLE DATAPOSSESSION MODEL:

Cloud computing is changing into more and more in style. Many corporations, organizations and individuals choose to source their computing demands and storage demands. so as to confirm the integrity of the knowledge within the Cloud, particularly the dynamic files which are often updated on-line, we have a tendency to propose an improved dynamic obvious knowledge possession model: It divides file into blocks, generates a tag for each block, computes a hash price for every tag, uses tags to confirm the integrity of the file blocks, and uses hash values to confirm the integrity of the tags. Compared with previous works, it reduces the machine and communication complexness from to constant. Though shopper wants to store some secret values which can produce some additional storage expense, it solely takes up about0.02% of the initial file size. Thus it is acceptable in most cases.

HYBRID PROVABLE DATA POSSESSION AT UNTRUSTED STORES IN CLOUD COMPUTING:

In recent years, cloud computing has gradually become the thought of web services. Once cloud computing environments become additional good, the business and user are going to be a colossal quantity of

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

knowledge hold on within the remote cloud storage devices, hoping to realize random access, data collection, scale back prices, and facilitate the sharing of different services. However, once the info is hold on within the cloud device, a long time, enterprises and users inevitably can have security concerns, fearing that the knowledge is really hold on within the cloud continues to be in the device or too long while not access to, has long been the cloud server removed or destroyed, resulting in businesses and users within the future can't access or restore theater files. Therefore, this theme goal to analysis and style for data storage cloud computing environments that area unit tried. Stored within the cloud for knowledge storage, analysis and develop a security and economical storage of proof protocol, can also delegate or authorize others to public verifiability whether or not theater truly hold on within the cloud storage devices.

ROBUST DYNAMIC PROVABLE DATA POSSESSION:

Remote knowledge Checking (RDC) permits purchasers to efficiently check the integrity of knowledge hold on at untrusted servers. This enables knowledge homeowners to assess the chance of outsourcing detain the cloud, creating RDC a valuable tool for knowledge auditing. Robust DC theme incorporates mechanisms to mitigate arbitrary amounts of knowledge corruption. Specially, protection against little corruptions (i.e., bytes or perhaps bits) ensuresthatattacks that modify a couple of bits don't destroy AN encrypted file or invalidate authentication info. Early RDC schemes have focused on static knowledge, whereas later schemes like DPDP support the complete vary of dynamic operations on the outsourced knowledge, including insertions, modifications, and deletions. Hardiness is required for each static and dynamic RDC schemes that relyonspot checking for potency. However, underneath AN adversarial setting there's a basic tension between economical dynamic updates and therefore the encoding required to realize hardiness, as a result of change even a tiny low portion of the file might need retrieving the whole file.

We have a tendency to establish the challenges that require to be overcome once making an attempt to feature hardiness to a DPDP theme. We have a tendency to propose the first DC schemes that offer hardiness and, at a similar time, support dynamic updates, whereas requiring little, constant, shopper storage. Our initial construction is economical in cryptography, however has high communication value for updates. Our second construction overcomes this disadvantage through a mix of techniques that features RS codes supported Cauchy matrices, decoupling the cryptography for hardiness from the position of symbols in the file, and reducing insert/delete operations to append/modify operations once change the RS-encoded parity knowledge.

A SECURITY ANALYSIS OF AMAZON'S ELASTIC COMPUTE CLOUD SERVICE:

Cloud services like Amazon's Elastic reason Cloud and IBM's Smart Cloud square measure quickly changing the means organizations square measure managing IT infrastructures and square measure providing online services. Today, if a corporation desires computing power, it will merely pip out on-line by instantiating a virtual server image on the cloud. Servers is quickly launched and shut down via application programming interfaces (API), giving the user a greater flexibility compared to traditional server rooms. In this speak, I will be able to explore the final security risks related to exploitation virtualserverimagesfrom the general public catalogues of cloud service suppliers. Especially, we have a tendency to investigate thoroughly the security issues of public pictures that square measure on the market on the Amazon EC2 service. i will be able to describe the style and implementation of an automatic system that we have a tendency to wont to instantiate and analyze the protection of public AMIs (Amazon Machine Images) on the Amazon EC2 platform, and supply elaborated descriptions of the protection tests that we have a tendency to performed on every image. Our findings demonstrate that each the users and also the suppliers of public AMIs is also prone to security risks like unauthorized access, malware infections, and loss of

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

sensitive data. The Amazon net Services Security Team has acknowledged our findings, and has already taken steps to properly address all the protection risks we have a tendency to gift during this speak.

PUBLIC VERIFIABLE PROOF OF STORAGE PROTOCOL FROMLATTICE ASSUMPTION:

Proof of storage (PoS) is AN interactive protocol allowing a shopper to verify that the server possesses the first information while not retrieving it. All of the existed Pops protocols square measure supported the hardness of resolution or discrete-log issues, which cannot resist quantum attacks. During this paper, we have a tendency to first propose a linearly homomorphy signature theme (LHHS) from lattice assumption, and generate HTVs from LHSS. Then we have a tendency to construct the primary lattice-based PoS protocol from the new HTVs. Outpost protocol is public verifiable and might be prove dun-forgettable in random oracle model presumptuous that SIS issues laborious. Quality analysis shows that the in the main computation price in Lopes square measure occur in code section. The communication costing prove and verify phases is freelance to the size of the file. The shopper or the friend solely must store the verifiable tags rather than the first file blocks.

APPROACHES:

User Authentication:

- Online customers should have access to a pc and a technique of payment. In our system, the user interactions area unit login, registration, communication, on-line payments and dealing. User details area unit handled in backend common information.
- In pc security, a login or logon is that the method by that individual access to a ADP system is controlled by distinctive and authenticating the user concerning credentials bestowed by the user.
- A user will log in to a system to get access and might then log off or close once the access isn't any longer required. To log off is to shut off one's access to a ADP system when having antecedently logged in.

Protocol Communication:

- All communications between devices need that the devices agree on the format of the information. The set of rules shaping a format is termed a protocol. Here we tend to area unit creating the protocol communication between the user mobile devices exploitation mobile Application and also the websites by HTTP protocol. A protocol accustomed request and transmit files or knowledge, particularly sites and webpage parts, over the web or different network.

Long term password generation:

The long run parole generation permits you to form random passwords that square measure extremely secure and intensely tough to crack or guess as a result of associate ex gratia combination of lower and grapheme letters, numbers and punctuation symbols. Our long run parole generated and sends to your mobile once you complete check in method.

Context Generation:

To access your application you must complete your login method with each internet and mobile application .During login method, your internet application details ought to match to mobile application for palm login. For this method we tend to area unit generating one context request with internet application and pass the request to mobile application.

It has valid period of time. It expires if period of time limit reached. Context generate once login id input was given at computing machine. It requests the mobile application to simply accept and await response context.

Context Verification:

Mobile application accepts the context request once enter correct id & long run countersign and verifies the IMEI for confirmative right user and sends generate

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

response context whereas accretive request if detects the situation victimization GPS mobile in mobile and maintains as a log.

Short term password generation:

If the response context was verified the short term countersign was generated at mobile facet that distinctive is exclusive} for unique sites and that was verified at protocol. the location needs short term countersign was analyzed base on context and therefore the authentication was succeeded.

Recovery Phase:

In the probability of mobile missing, we have a tendency to are providing recovery choice to secure our application. Victimization IMEI variety of our mobile and therefore the opass.apk we are able to simply recover our system.

Application Maintenance:

- Application maintenance may be a discouraging task for enterprises. They're fraught to scale back spends on maintenance. Whereas making certain optimized performance of their IT systems and applications. Final module of our project as application maintenance. That is, to keep up our application with a lot of and a lot of security. Like PIN code analysis and OPASS verification.

CONCLUSION:

In this paper, we have a tendency to plan a user authentication protocol named oPass that leverages cell phones and SMS to thwart word stealing and word recycle attacks. We have a tendency to assume that every web site possesses a singular number. We have a tendency to conjointly assume that a telecommunication service supplier participates within the registration and recovery phases. The planning principle of oPass is to eliminate the negative influence of human factors the maximum amount as potential.

Through oPass, every user solely has to bear in mind a long-run word that has been accustomed shield her telephone. Users square measure free from writing any passwords into untrusted computers for login on all websites. Compared with previous schemes, oPass is that the 1st user authentication protocol to stop word stealing (i.e., phishing, key logger, and malware) and word recycle attacks at the same time. The explanation is that oPass adopts the one-time word approach to confirm independence between every login.

REFERENCES:

[1] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.
[2] S. Gawand E. W. Felten, "Password management strategies for online accounts," in SOUPS '06: Proc. 2nd Symp. Usable Privacy . Security, New York, 2006, pp. 44–55, ACM.
[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666, ACM.
[4] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords," in CCS '09: Proc. 16th ACM Conf. Computer
Communications Security, New York, 2009, pp. 500–511, ACM [5] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in SSYM'99: Proc. 8th Conf. USENIX Security Symp., Berkeley, CA, 1999, pp. 1–1, USENIX Association.
[6] A. Perrig and D. Song, "Hash visualization: A new technique to improve real-world security," in Proc. Int.Workshop Cryptographic Techniques E-Commerce, Cutesier, 1999, pp. 131–138.
[7] J. Thorpe and P. van Oorschot, "Towards secure design choices for implementing graphical passwords," presented at the 20th. Annu. Computer Security Applicat. Conf., 2004.
[8] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

longitudinal evaluation of a graphical password system," Int. J. Human-Computer Studies, vol. 63, no. 1–2, pp.
102–127, 2005.
[9] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in AVI '06: Proc. Working Conf. Advanced Visual Interfaces, New York, 2006, pp. 177–184, ACM.
[10] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in CCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170, ACM.
[11] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient method for securely managing passwords," in WWW '05: Proc. 14th Int. Conf. World Wide Web, New York, 2005, pp. 471–479, ACM.
[12] K.-P. Yee and K. Sitaker, "Passpet: Convenient password management and phishing protection," in SOUPS '06: Proc. 2ndSymp. Usable Privacy Security, New York, 2006, pp. 32–43, ACM.
[13] S. Chiasson, R. Biddle, and P. C. van Oorschot, "A second look at the usability of click-based graphical passwords," in SOUPS '07: Proc. 3rd Symp. Usable Privacy Security, New York, 2007, pp. 1–12, ACM.
[14] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in CHI '09: Proc. 27th Int. Conf. Human Factors Computing Systems, New York, 2009, pp. 889–898, ACM.
[15] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and thememorable space of graphical passwords," in SSYM'04: Proc. 13th Conf. USENIX Security Symp., Berkeley, CA, 2004, pp. 10–10, USENIX Association.
[16] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in SS'07: Proc. 16th USENIX Security Symp. USENIX Security, Berkeley, CA, 2007, pp. 1–16, USENIX Association.
[17] P. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Information Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.
[18] R. Dhamija, J. D. Tygar, andM. Hearst, "Why phishing works," in CHI '06: Proc. SIGCHI Conf. Human Factors Computing Systems, New York, 2006, pp. 581–590, ACM.
[19] C.Karlof,U. Shankar, J. D.Tygar, andD.Wagner, "Dynamic pharming attacks and locked same-origin policies for web browsers," in CCS '07: Proc. 14th ACMConf. Computer Communications Security, NewYork, 2007, pp. 58–71, ACM.
[20] T. Holz, M. Engelberth, and F. Freiling, "Learning more about the underground economy:Acase-study of keyloggers and dropzones," Proc. Computer Security ESORICS 2009, pp. 1–18, 2010.
[21] N. Provos, D. Mcnamee, P. Mavrommatis, K. Wang, and N. Modadugu, "The ghost in the browser: Analysis of web-based malware," in Proc. 1st Conf. Workshop Hot Topics in Understanding Botnets, Berkeley, CA, 2007.
[22] Phishing Activity Trends Rep., 2nd Quarter/2010 Anti-Phishing Working Group [Online]. Available: http://www.antiphishing.org/
[23] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," Financial Cryptography Data Security, pp. 1–19, 2006.
[24] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda, "Panorama: Capturing system-wide information flow for malware detection and analysis," in CCS '07: Proc.e 14th ACM Conf. Computer Communications Security, New York, 2007, pp. 116–127, ACM.
[25] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X. Zhang, "Trustworthy and personalized computing on public kiosks," in Proc. 6th Int. Conf. Mobile Systems, Applications Services, 2008,
pp. 199–210, ACM.
[26] RSA SecureID [Online]. Available: http://www.rsa.com/node. aspx?id=1156/
[27] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proc. IEEE, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[28] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, pp. 770–772, Nov. 1981.
[29] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters,"
in Selected Areas Cryptography, 2003, pp. 175–193, Springer.
[30] TS 23.040: Technical Realization Short Message Service (SMS) 3GPP [Online]. Available: http://www.3gpp.org/
[31] I. T. Report, ITU Internet Rep. 2006: Digital.Life [Online]. Available:
http://www.itu.int/
[32] TS 35.201: Specification 3GPP Confidentiality Integrity Algorithms Document 1: f8 and f9 Specification 3GPP [Online]. Available: http:// www.3gpp.org/
[33] TS 35.202: Specification 3GPP Confidentiality Integrity Algorithms Document 2: KASUMI Specification 3GPP [Online]. Available: http:// www.3gpp.org/
[34] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, Stronger password authentication using browser extensions," in
SSYM'05: Proc. 14th Conf. USENIX Security Symp., Berkeley, CA, 2005, pp. 2–2, USENIX Association.
[35] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," Advances Cryptology—ASIACRYPT 2000, pp. 531–545, 2000.
[36] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is SSL?)," in Advances Cryptology— CRYPTO 2001, 2001, pp. 310–331.
[37] B. Blanchet, ProVerif: Cryptographic Protocol Verifier Formal Model [Online]. Available: http://www.proverif.ens.fr/
[38] B. Blanchet, "An efficient cryptographic protocol verifier based on prolog rules," in Proc. 14th IEEE Computer Security Foundations Workshop, 2001, pp. 82–96.
[39] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in Proc. 17th ACM Conf. Computer Communications Security, New York, 2010, pp. 162–175, ACM.
[40] T. Delenikas et al., SMSLib API—Java Library for Sending/Receiving SMS [Online]. Available: http://smslib.org/
[41] M.Wu, S. Garfinkel, and R. Miller, "Secure web authentication with mobile phones," in DIMACS Workshop Usable Privacy Security Software, Citeseer, 2004.
[42] E. Barkan and E. Biham, "Conditional estimators: An effective attack on A5/1," in Selected Areas in Cryptography. NewYork:Springer, 2006, pp. 1–19.
[43] M. Mannan and P. van Oorschot, "Using a personal device to strengthen password authentication from an untrusted computer,"
Financial Cryptography Data Security, pp. 88–103, 2007.
[44] J.McCune, A. Perrig, andM. Reiter, "Bump in the ether: A framework for securing sensitive user input," in USENIX Annu. Tech. Conf., 2006, pp. 185–198.
[45] C. Yue and H. Wang, "SessionMagnifier: A simple approach to secure and convenient kiosk browsing," in Proc. 11th Int. Conf. Ubiquitous Computing, 2009, pp. 125–134, ACM.
[46] D. Wendlandt, D. G. Andersen, and A. Perrig, "Perspectives: Improving ssh-style host authentication with multi-path probing," in
Proc. USENIX 2008 Annu. Tech. Conf., Berkeley, CA, 2008, pp. 321–334, USENIX Association.
[47] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "Emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies," in Proc. 2007 IEEE Symp. Security Privacy, 2007.
[48] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," in ACM Computing Surveys, Carleton Univ., 2010.