Server Assemble Location Authentication in Internet using Positioning Algorithm

[1] A. Alekhya, [2] Dr. K. S.Yuvaraj
[1]PG Scholar, Department of MCA, St. Anns College of Engineering & Technology, Chirala, Andhra Pradesh, India
[2]Assistant Professor, Department of MCA, , St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India

ABSTRACT

Server Assemble Location Authentication mechanism to providing real time server location verification. Its uses and enhancing server authentication is browsers to automatically interpret server location data. Server Location Verification (SLV) is find Planet Lab to explain to SLV is compatible with the increasing trends of geographically distributed content dissemination over the internet without causing any interoperability conflicts. New notion of server location pinning within TLS to support SLV to evaluate their combined impact using a server authentication options framework. The propose system novel Wi-Fi indoor positioning and tracking framework which employs the spatial analysis and image processing methods. To specifically leverage Channel ID-based authentication in combination with server invariance to create a novel mechanism that we call SISCA Server Invariance with Strong Client Authentication. With the uses of signing and symmetric modules to secure verification process put forth. Sign module is responsible for signature generation of input data along with UMAC and unique signing key. Security design and implement is efficient cryptographic protocol that security keystroke integrity by utilizing chip Trusted Computing Platform (TPM). The protocol prevents the forgery of fake key events by malware under reasonable assumptions. The verification method is lightweight framework for restricting outbound malware traffic in Nearest Neighbor (NN) algorithm of the fingerprinting method to identify the initial position estimate of the smart phone user.

Keywords : Indoor Positioning, Wi-Fi, Smartphone, LBS, Fingerprinting, Geographic Information Systems; Global Positioning Systems

I. INTRODUCTION

Millions of systems are affected by malware all over globe which disrupt the data of host. Specifically malware is computer contaminant and defined as program or software designed with intent to harm the user of system by affecting the sensitive information and gain access to system [1]. An attacker is successfully impersonating a legitimate server to the browser by presenting a valid certificate for that server as long as she holds the corresponding private key [2]. In previous years, quite a few incidents involving miss used certificates were made public. Even in the case where the attacker simply presents an invalid certificate not accepted by the browser she will still succeed in her attack if the user defies the browser's security warning [3]. We construct a lightweight cryptographic protocol that prevents malicious bots from injecting keystroke events into a host's applications [4]. This keystroke integrity service also prevents certain types of tampering on the host's kernel. We implement our prototype with an enabled on-chip TPM and experimentally evaluate both the computation and communication overheads [5]. Our cryptographic operations have low computation overhead and reasonable bandwidth overhead [6]. The widely use of Wi-Fi access points for Internet connection in hotels, offices, coffee shops, airports and many other fixed places makes Wi-Fi become an attractive technology for the positioning purpose [7]. Location positioning systems using wireless area local network (WLAN) infrastructure are considered as cost-effective and practical solutions for indoor location estimation and tracking [8]. There is almost no extra hardware or other infrastructure investment, which is different from other indoor positioning technologies such as low-energy Bluetooth sensor networks or radio-frequency identification (RFID) systems [9].

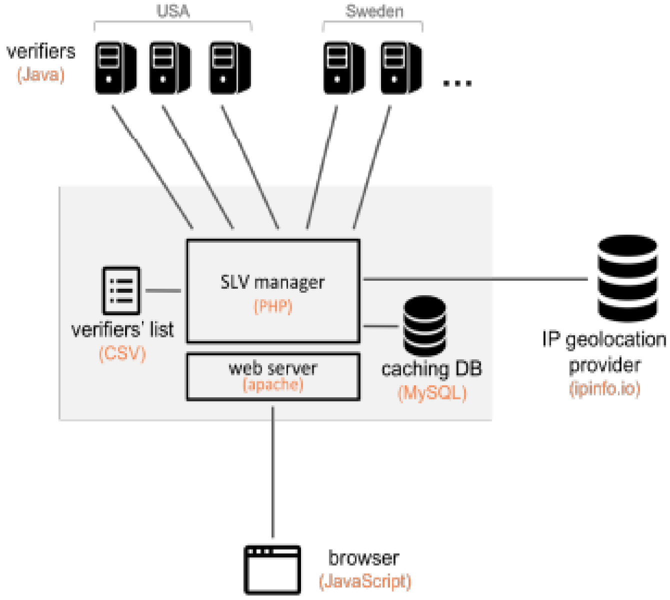

Fig 1. System architecture to implemented prototype

This enables SLV to address all phrasing attacks regardless of where in the hierarchical lookup procedure an adversary may spoof the name resolution SLV itself does not contact any DNS systems for name resolutions. If the browser receives a spoofed IP address via DNS due to a phrasing attack that IP address is the one passed to SLV for verification. Accordingly, a fraudulent IP address from a local phrasing attack would be presented to SLV for location verification [10].

II. RELATED WORK

This could be in the form of GPS coordinates along with lateral and longitudinal distances that accurately delineate the space boundaries. To claim a space, the owner submits their space defined certificate (self-signed or CA-signed) to a public log and monitors the log to detect any other entity claiming ownership of their space [11]. To validate a space ownership, Geo PKI relies on CAissued Extended Validation (EV) certificates, associated to a real world street address [12]. An attacker would thus need to either compromise a CA to issue an EV certificate to tie its public key to the fraudulently-claimed space, or forge legal documents proving such ownership [13]. Trusted platform module hardware chip was originated by efforts of Trusted Computing Group which comprises Intel, HP, IBM, Microsoft, Compact in 1999 with purpose to use hardware to enhance the level of trustiness and strengthen security of system or network [14]. TPM acts as device with provision for credential storage, software integrity, secure storage of cryptographic information and device identity. Along with trusted software TPM utilize hardware that which offers resistance to malware attacks with enhance trusted infrastructure [15]. In addition to conventional taint tracking solutions such as hardware memory bit or extended software data structure our TPM-based solution uniquely supports the cryptographic operations to enforce data confidentiality and the integrity of taint information. The important feature about TPM is its on-chip secret key. Therefore, the client device can be uniquely authenticated by a remote server [16]. And the relative distance between wireless devices and access points can be roughly estimated based on Wi-Fi signal strength using signal propagation models. It is also well known that the accuracy of indoor position estimation based on Wi-Fi signal strength is affected by many environmental and behavior factors such as walls, doors, settings of access points, orientation of human body. In practical applications, a good approximation of heterogeneous environmental signal surfaces could help to improve the indoor positioning accuracy [17].

III. SYSTEM ARICTURES

A new Wi-Fi based indoor positioning method was developed in this research for improving the positioning accuracy of the fingerprinting approach based on the nature of the spatial correlation of Wi-Fi signal propagation [18]. Another characteristic for the new method to be based on is the spatial correlation of the Wi-Fi signal propagation, that is, the proportion of the RSSI values observed and their corresponding distances calculated is trustworthy for two points which are close to each other [19]. It is obvious that the distance between a wireless device and an access point is the key for Wi-Fi positioning using the relate ration method. The received signal strength doesn directly lead to an estimated distance to an access point. In general, it does follow a trend that the signal strength decreases with an increase of distance as is expected, but it is not a simple linear path loss model [20].

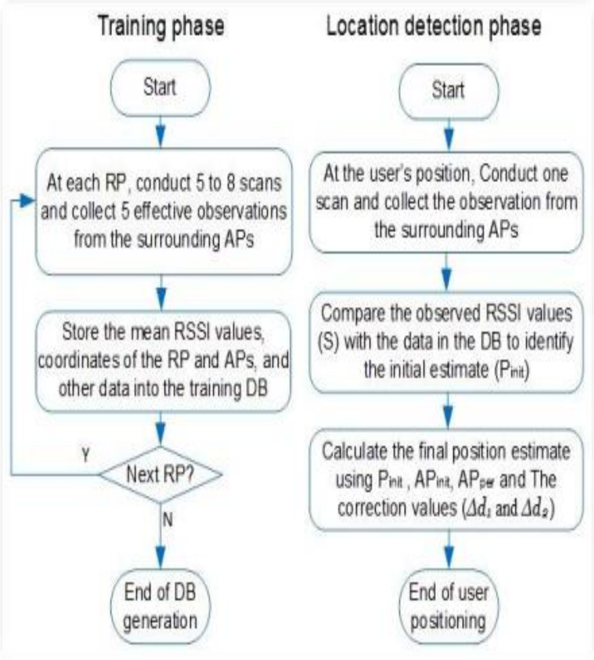
Training phase
Location detection phase
Start
At each RP, conduct 5 to 8 scans and collect 5 effective observations from the surrounding APs
Store the mean RSSI values, coordinates of the RP and APs, and other data into the training DB
Y
Next RP?
N
End of DB generation
Start
At the user's position, Conduct one scan and collect the observation from the surrounding APs
Compare the observed RSSI values (S) with the data in the DB to identify the initial estimate (P_{init})
Calculate the final position estimate using P_{init}, AP_{init}, AP_{ser} and The correction values (Δd_1 and Δd_2)
End of user positioning

Fig 2. Overall procedure of the new method

1. PROPOSED MODEL

The system comprises of three main modules input, sign, and verify module. The input module is responsible for accepting input from user is passed to sign module for signature generation [21]. Initially Sign and verify undergo key update and generation step for symmetric and communication keys. These key is prove the provenance of data and make system more secure against malware by providing verified data as output [22].

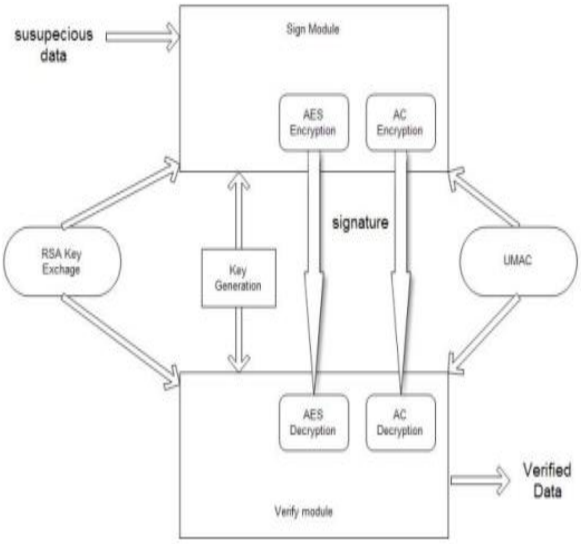

Fig. 3. Fig:- Proposed System Architecture

2. TRACKING PROVENANCE OF OUTBOUND TRAFFIC

Our cryptographic provenance verification method in a network setting in particular for ensuring the integrity of outbound packets as they flow through the host network stack [23]. We describe the design and implementation of a lightweight traffic optimizations framework. It used a building block for constructing powerful personal firewalls based malware detection tools. Malware disabling or bypassing personal firewalls on a host renders the firewalls useless [24]. Malware may communicate with the outside world with the intent of exporting sensitive data. Legitimate outbound network traffic passes through the entire network stack in the host's operating system. We develop a robust cryptographic protocol for enforcing the proper provenance of a packet on a host [25].

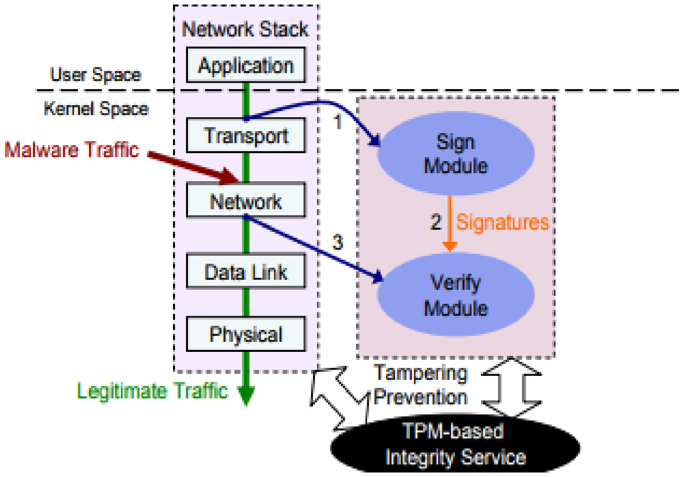

Fig. 4. Traffic checkpoints are placed at the Sign and Verify modules

A. POSITIONING ALOGORITHM

Several positioning algorithms have been developed for Wi-Fi positioning and can be categorized as geometric techniques, statistical methods, fingerprinting and machine learning algorithms. We introduce another algorithm based on image filtering technique and then integrate it with two widely used algorithms [26]. Trilateration and knearest-neighbor in signal space into our indoor positioning system relying on a Wi-Fi surface which keeps at least three image pixels that meets the multi-value filtering requirements

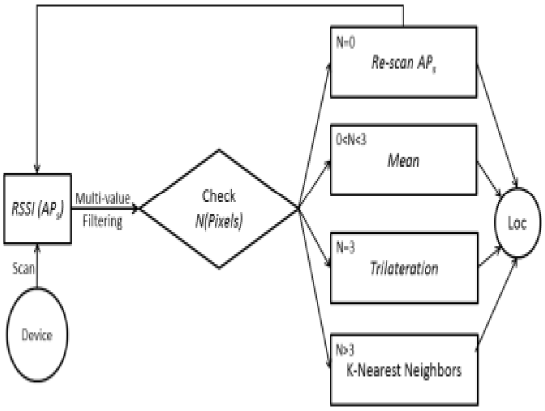

Fig 5: The proposed heuristics-based indoor positioning algorithm.

B. KEY EXCHANGE:

1) The Sign module initiates the connection with the Verify module. The two modules exchange their public keys.
2) The Verify module receives and decrypts a0 and a1 with its private key. It then generates two random numbers b0 and b1. The Verify module encrypts b0 and b1 using the Sign module's public key [27].
3) Both the Sign and Verify modules have a0, a1, b0, and b1. They compute the signing key as a0 ⊕ b0 and the symmetric key for their communication encryption

C. CREATE ADVANCED CPV MODEL

The overall idea of execution of Advanced CPV model is operations that performed data source verification between sign module and verify module. Initially both of the modules undergo RSA key exchange by exchanging their public keys. Each of modules generates two random numbers which exchanged in encrypted manner [28]. These four numbers are used to generate signing key and symmetric key by undergoing XOR operation. Following are steps for key generation described in detailed. The signing key along with AES and ACA is used to generate signature for input data. Symmetric key is used for is used for data verification in verify module. The two algorithms use keys for encrypting the data and send securely to verify module for verification [29].

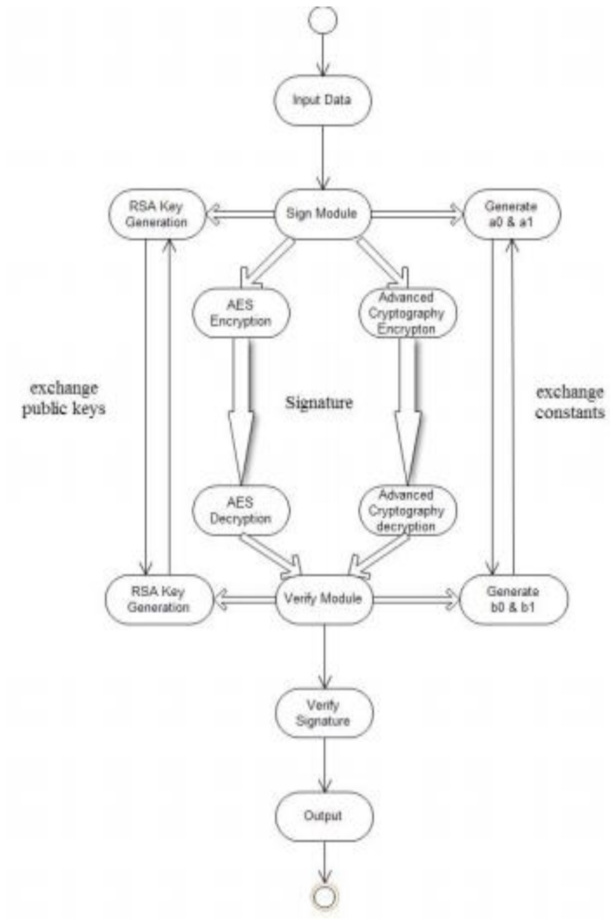

Fig. 6.Execution of the Model

IV. PERFORMANCE RESULT

In the online phase the indoor position of the user can be estimated via raster multivalve-attribute filtering on Wi-Fi signal surfaces and above introduced heuristics based positioning algorithm. One mobile device was put at the location Q, the red circle represented the estimated position based on our proposed method while the blue circle was the GPS location which still located on the outside of this building. After conducting several rounds of experiments The commercial Keaau RTLS, the NN algorithm and the new method were tested in the same testing environment. The accuracy of 3.8 m of NN is slightly better, however, it cannot be drawn by this minor difference that NN is better than Keaau RTLS in general.

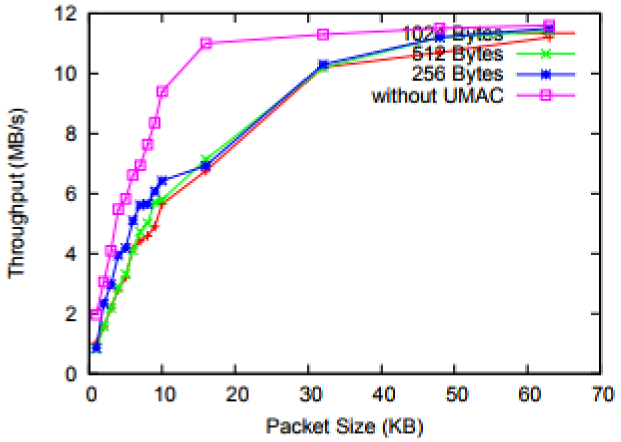

Fig. 7. Comparisons with partially signed packets at the bottom

V. CONCLUSION AND FUTURE WORK

SLV leverages established networking principles that location information can be inferred from timing measurements, and existing methodological guidelines for use of timing measurements to achieve server location verification the recently proposed Channel ID-based authentication, cannot prevent such attacks. Instead, strong client authentication needs to be complemented with the concept of server invariance, which is a weaker and easier to enforce property than server authentication. Advanced CVP approach gives satisfactory guarantee of data with trusted computing platform which includes the most trustiness in the provenance of data integrity, confidentiality and availability. We demonstrated CPV's application in identifying stealthy malware activities of a host, in particular how to distinguish malicious/unauthorized data flow from legitimate one on a computer that may be compromise. In future work, we aim to take the signal directionality into consideration and try more advanced spatial interpolation and clustering methods to achieve better accuracy from meter to decimeter. In addition, a crowd sourcing WiFi signal collection and sharing platform will be developed to engage more users' contribution for advancing indoor positioning technology in our campus.

VI. REFERENCES

[1]. A. M. Abdou, A. Matrawy, and P. C. van Oorschot, “Location Verification on the Internet: Towards Enforcing Location-aware Access Policies Over Internet Clients,” in IEEE CNS, Oct. 2014

[2]. ADKINS, H. An update on attempted man-in-the-middle attacks.

[3]. AUBOURG, J., SONG, J., STEEN, H. R. M., AND VAN KESTEREN, A. XMLHttpRequest (W3C Working Draft).

[4]. A. Baliga, P. Kamat, and L. Iftode. Lurking in the shadows: Identifying systemic threats to kernel data. In IEEE Symposium on Security and Privacy, pages 246–251. IEEE Computer Society, 2007.

[5]. B. Blackburn and R. Ranger. Barbara Blackburn, the World’s Fastest Typist, 1999.

[6]. M. Christodorescu, S. Jha, and C. Kruegel. Mining specifications of malicious behavior. In ESEC-FSE ’07: Proceedings of the 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on the foundations of software engineering, pages 5–14, New York, NY, USA, 2007. ACM

[7]. A. Bose and C. H. Foh. A practical path loss model for indoor wifi positioning enhancement. In Information, Communications & Signal Processing, 2007 6th International Conference on, pages 1–5. IEEE, 2007

[8]. M. Brunato and R. Battiti. Statistical learning theory for location fingerprinting in wireless lans. Computer Networks, 47(6):825–845, 2005.

[9]. N. Bulusu, J. Heidemann, and D. Estrin. Gps-less low-cost outdoor localization for very small devices. IEEE personal communications, 7(5):28–34, 2000.

[10]. R. Dhamija, J. D. Tygar, and M. Hearst, “Why phishing works,” in ACM CHI, 2006, pp. 581–590

[11]. N. Vratonjic, J. Freudiger, V. Bindschaedler, and J.-P. Hubaux, “The inconvenient truth about web certificates,” in Economics of info sec and priv III. Springer, 2013, pp. 79–117.

[12]. J. A. Muir and P. C. van Oorschot, “Internet geolocation: Evasion and counterevasion,” ACM Comput. Surv., vol. 42, pp. 4:1–4:23, 2009.

[13]. T. H.-J. Kim, V. Gligor, and A. Perrig, “GeoPKI: Converting Spatial Trust into Certificate Trust,” in Springer EuroPKI, 2013, pp. 128–144

[14]. Anirudha Vikhe, P. S. Desai, “Data Provenance Verification for Secure Host Using Advanced Cryptographic Algorithm”, INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS, VOL 88-NO.11, FEB. 2014

[15]. Huijun Xiong, Chehai Wu, Deian Stefan, Danfeng Yao Member, Data-Provenance Verification For Secure Hosts , IEEE Transactions On Dependable and secure computing vol.9 no.2 year 2012.

[16]. M. J. De Smith, M. F. Goodchild, and P. Longley. Geospatial analysis: a comprehensive guide to principles, techniques and software tools. Troubador Publishing Ltd, 2007.

[17]. F. Evennou and F. Marx. Advanced integration of wifi and inertial navigation systems for indoor mobile positioning. Eurasip journal on applied signal processing, 2006:164–164, 2006.

[18]. R. Faragher and R. Harle. An analysis of the accuracy of bluetooth low energy for indoor positioning

[19]. A. Cayley. On a theorem in the geometry of position. Cambridge Mathematical Journal, 2:267–271, 1841.

[20]. N. Chang, R. Rashidzadeh, and M. Ahmadi. Robust indoor positioning using differential wi-fi access points. IEEE Transactions on Consumer Electronics, 56(3):1860–1867, 2010.

[21]. B.Baliga, P. Kamat, and L. Iftode. Lurking in the shadows: Identifying systemic threats to kernel data. In IEEE Symposium on Security and

Privacy, pages 246–251. IEEE Computer Society, 2007.

[22]. W. Cui, R. H. Katz, and W. Tian Tan. Design and implementation of an extrusion-based break-in detector for personal computers. In ACSAC, pages 361–370. IEEE Computer Society, 2005.

[23]. A. Dinaburg, P. Royal, M. Sharif, and W. Lee. Ether: malware analysis via hardware virtualization extensions. In CCS '08: Proceedings of the 15th ACM conference on Computer and communications security, pages 51–62, New York, NY, USA, 2008. ACM.

[24]. S. Garriss, R. Caceres, S. Berger, R. Sailer, L. van Doorn, and ´ X. Zhang. Trustworthy and personalized computing on public kiosks. In MobiSys '08: Proceeding of the 6th international conference on Mobile systems, applications, and services, pages 199–210, New York, NY, USA, 2008. ACM.

[25]. J. Goebel and T. Holz. Rishi: Identify bot contaminated hosts by IRC nickname evaluation. In Proceedings of the First USENIX Workshop on Hot Topics in Understanding Botnets, April 2007

[26]. H. Xiong, P. Malhotra, D. Stefan, C. Wu, and D. Yao. Userassisted host-based detection of outbound malware traffic. In Proceedings of International Conference on Information and Communications Security (ICICS), December 2009.

[27]. G. Xu, C. Borcea, and L. Iftode. Satem: Trusted service code execution across transactions. In Proceedings of the 25th IEEE Symposium on Reliable Distributed Systems (SRDS), pages 321–336, Washington, DC, USA, 2006. IEEE Computer Society

[28]. J. M. McCune, A. Perrig, and M. K. Reiter. Safe passage for passwords and other sensitive data. In NDSS. The Internet Society, 2009.

[29]. M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis. My botnet is bigger than yours (maybe, better than yours). In Proceedings of the First USENIX Workshop on Hot Topics in Understanding Botnets, April2007

ABOUT AUTHORS:

A.ALEKHYA is currently studying her MCA department St. Ann's college of Engineering & Technology, chirala, A.P. She received her Bachelor of Sceince From A.N.U.

Dr.K.S.YUVARAJ ph.D is currently working as in technology as a associative professor in MCA Department, St.Ann's college of Engineering & Technology, chirala, A.P.

His research includes Network and Datamining.