IJCSN International Journal of Computer Science and Network, Volume 4, Issue 2, April 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Restriction of Mobile Viruses Using Pre-Immunization and Adaptive Dissemination

Priti Naik

G.H.R.I.E.T.W. Nagpur,Mahharashtra, India

Abstract - Viruses and malwares can spread can spread from PC systems into versatile systems with the fast development of shrewd mobile phone clients. In a portable system, infections and malwares can result in protection information spillage, additional charges, and remote tuning in. Moreover, they can stick remote servers by sending a huge number of spam messages or track client positions through GPS. On account of the potential harms of portable infections, it is critical for us to pick up a profound understanding of the spread instruments of versatile infections. We propose a network model for simulating virus propagation through both Bluetooth, SMS, GPS and Wifi. Different from previous work, our work addresses the impacts of human behaviors, i.e., operational behavior and mobile behavior, on virus propagation. Our simulation results will provide further insights into the determining factors of virus propagation in mobile networks. Moreover, we examine two strategies for restraining mobile virus propagation, i.e., pre-immunization and adaptive dissemination strategies drawing on the methodology of autonomy-oriented computing (AOC). The experimental results will show that our strategies can effectively protect large-scale and/or highly dynamic mobile networks.

Keywords - *Access Control, Authentication, Attribute-Based Signatures, Attribute-Based Encryption, Cloud Storage.*

1. Introduction

We are mindful about the expanding number of Smartphone clients. These Smartphone ought to be secured by the infections and malwares engendering in the system. These infections proliferate from PC system to the versatile system. Portable infections can result in private information spillage and aggravate discussion by remote control. In some more genuine circumstances, infections can even stick remote administrations by sending a great many spam messages, and diminish the nature of voice correspondence. In perspective of this circumstance, there is an earnest requirement for both clients and administration suppliers to further comprehend the proliferation instruments of versatile infections and to convey proficient countermeasures.

A few models have been utilized to study the element methodology of infection proliferation. Substantial spread models can be utilized as test cots to: 1) gauge the size of an infection flare-up before it happens truly and 2) assess new and/or enhanced countermeasures for controlling infection proliferation.

In this undertaking, we propose a system model for portraying BT-based , SMS-based, GPS based and Wifi Based infections, which spread through Bluetooth and Short/Multimedia Message Services, individually, with a specific end goal to address the aforementioned weaknesses [1][9]. Not the same as existing work that spotlights on the impacts of system structures on infection engendering; our work is intended to increase further experiences into how human practices influence the spread progress of versatile infections. As of late, a few routines have been proposed to limit versatile infection proliferation focused around existing models.

In a few existing techniques some won't have the capacity to discover new infections because of the impediment of antivirus learning. Our work centers that the gadget at first bearing the application can give the criticism to the server which upgrades further gadgets not introducing that specific application. So as to verify that clients convenient upgrade their own particular recognition databases, the PDAs are dispersed with the notices or fixes by the administration suppliers or security organizations. A few methods endeavor to forward security notices or patches focused around the short range correspondence abilities of joined telephone yet their effect will be influenced by human portability designs and entomb contact frequencies among telephones. It would be hard to procure mark documents in a convenient way. Meanwhile, other scattering methodologies have likewise been utilized to disperse patches and the trouble remains when managing a substantial scale or very dynamic system. Therefore, we propose another technique that can effectively forward patches to whatever number telephones as would be prudent, even in substantial scale and/or alterably developing systems.

We propose a two-layer network propagation model that accounts for the behavior of users (i.e., operational and mobility patterns) in mobile networks. Based on our model, we examine the performance of a pre-immunization strategy that draws on the methodology of

autonomy-oriented computing (AOC) as reported in restraining mobile virus propagation. In order to evaluate the effect of patch distribution delay on virus propagation, we deploy the AOC-based pre-immunization strategy into a network at different times. Furthermore, we design an adaptive dissemination strategy by extending local reactive behaviors of entities.

We propose a two-layer system proliferation demonstrate that records for the conduct of clients (i.e., operational and portability designs) in portable systems. In light of our model, we look at the execution of a preimmunization methodology that draws on the procedure of self-governance arranged processing (AOC) in controlling versatile infection engendering. We outline a versatile spread system by broadening neighborhood responsive practices of elements.

2. Related work

The related work on mobile virus and their propagation models is reviewed first. Next, some virus defense methods that contain abnormal detection technologies for restraining virus propagation in mobile networks are introduced here.

2.1 Smartphone Malwares

The Smartphone infection, Cabir, was produced in 2004 by the infection composing gathering. It can self-duplicate yet does no harm to the telephones. Presently a day more than a hundred portable infections have started to be, huge numbers of which contain defenseless codes and reason different harms to the PDAs. The PDAs infection development is quick, when contrasted with the infection from the PC and Internet world. Such abruptly development of advanced cells will give a beneficial ground to the malware to spread. An influenced PDA can result in serious pay for both the clients and the cell administration supplier. If there should arise an occurrence of clients, the harm may contain the misfortune or robbery of private information, the obstruction of ordinary advanced mobile phone utilization furthermore financial misfortunes (e.g., the infection might furtively utilize the SMS/MMS services).In the cell base side, the versatile infections exhibit a genuine impact of Denial of Server.

2.2 Types of Viruses

There are numerous approaches to arrange Smartphone infections. These Smartphone infections are classified focused around the focuses on that the infection assaults (e.g. the call focus, the phone base station). As opposed to concentrating on what the infections try to assault or accomplish, we decide to sort the Smartphone infections focused around the various contamination vectors that the infection enters and/or retreats the gadget. The profit of our methodology is that it gives a non specific view on how an infection infiltrates into a Smartphone and how effectively it can spread in the Smartphone populace. We have distinguished the classes of disease vectors for Smartphone infection, which are recorded in provides for some graphic infections at present in presence for every contamination vector.

2.3. Virus Propagation through BT and SMS

As indicated by the correspondence channels of versatile infections, the infections fall into two classes specifically: BT based infections (e.g., Cabir, Lasco) and SMS-based infections (e.g., TXSBBSpy, Zombie, and Commwarrior). SMS-based infections can send duplicates of themselves to all telephones that are recorded in location books, by method for photographs sending, features, and short messages, and so forth. The spread of SMS based malwares takes after a long-range spreading example that is like the spreading of infections in PC, particularly like worm engendering in email organizes consequently, the operational conduct of clients is essential in SMS-based infection proliferation. Clients with mindfulness about the infections danger won't likely be tainted regardless of the fact that they get connection. So as to study SMS-based infection engendering, we consider certain the operational examples, for example, if the clients open an infection connection or not.

BT-based infection is a nearby contact driven infection since it contaminates different telephones just through Bluetooth and Wi-Fi gadgets inside a given radio range. Like contact based ailments as in people (e.g., SARS and H1N1), the proliferation of a BT-based infection takes after a spatially constrained spreading sample. Disease showing is a champion amongst the most broadly perceived systems for considering such contamination inducing. It acknowledge that individuals are homogeneous in a host gather, every one having a meet likelihood contact with others.

3. Proposed Approach

In the structure we are completing a two layer framework model for spreading disease through Bluetooth and SMS/MMS channel. The operation of human practices for instance, adaptable behavior and operational behavior [3] addresses the spreading of diseases. Other than we examine two techniques to avoid contamination in cell phones. i.e., Preimmunization and Adaptive Dissemination approachs through the strategy of Autonomy-Oriented Figuring (AOC) .It can characteristically place the disease before when contamination go into the cells and eradicate it.

3.1 Autonomy-Oriented Computing

Autonomic figuring proposes the overseeing to oneself physical appearance of dispersed transforming

resources, acclimating to sporadic changes while beating regular inconvenience to overseers and customers [6]. Started by IBM in 2001, this attempt finally plans to make machine structures prepared for association to oneself, to annihilation the quickly getting to be inconvenience of figuring organizations of structure, and to diminish the obstacle that multifaceted nature shows to further advancement. Using strange state courses of action the structure makes conclusion isolated's and it will as frequently as could be expected under the circumstances check likewise enhance its status hence so it can change itself to developing conditions. An autonomic enlisting skeleton is assembled of autonomic parts (AC) teaming up with each other.

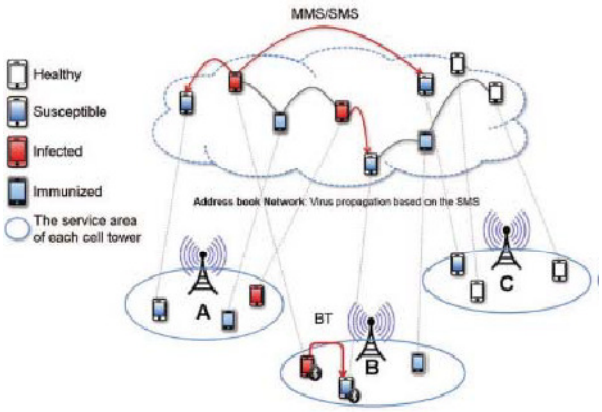

Fig 1. Modeling Mobile Virus Propagation

In this fragment, first a two-layer framework model for reproducing compact disease spreading through different correspondence channels is introduced. Next, we display organized spread blueprints on compact application diseases. The work presented in this fragment is an increase of the work in Modeling and Restraining the Propagation of Portable Viruses. Considering the examination of expansion segments, a crucial component helping disease spread lies in operations of customers after polluted messages are gotten from the framework through the applications being presented on the contraption. In case customers have enough data they won't open suspicious messages additionally their phones won't be smoothly debased. Convenience cases expect a key part in contamination spread in light of the way that as these diseases can simply corrupt neighborhood neighbors (whether they know these neighbors) inside a certain range. This can survey the impact of operational lead on convenient contamination duplication in social related frameworks, moreover the effects of versatile direct on the disease and diverse disease inciting in area contact frameworks.

3.2 Two-Layer Network Propagation Model

The vital musings behind our two-layer framework augmentation arranging are shown in Fig1. The lower layer addresses a geologically based cell tower framework. In this layer BT-based contaminations spreads to distinctive positions of cell phones as demonstrated. The upper layer contrasts with a wise framework fabricated from the area books of phones. SMS-based contaminations multiply in this layer imitating the social associations among versatile customers and affiliation gets up and goes.

3.3 The Structure of Geographical Network

Cell phones unite with each other through remote signs gave by cell towers. Customers with their phones can go in a land framework, moving from network to an exchange concentrated around their compact behavior. The same or differing towers give the crucial remote banners in these two cross segments. The inducing systems of BT-based and SMS-based contaminations can be reenacted in an area contact framework and a social related framework, independently.

3.4 The Structure of Logical Network

A true blue relationship framework among versatile customers can ascend out of the area books of cell phones. In such a framework, the distinctive centers identify with phones and associations additionally show the correspondences among them. Not the same as contamination spread through Bluetooth that is simply ready to do affecting nearby phones, a couple of contaminations may spread through SMS (e.g., Zombie). Consequently, they can in like manner attack remote phones. Thusly, SMS-based diseases perhaps spread as snappy as consider to worms in email frameworks.

3.5 SMS- Based Propagation Process

Social associations are exemplified in versatile frameworks in light of the area books of Pdas. In case a phone is polluted by this kind of disease, it characteristically sends its copies to distinctive phones as per the area book of the corrupted phone. Exactly when customers gets a suspicious message from distinctive contraptions, in perspective they could call their own security care they opens or eradicate as showed by the data about the dangers of compact diseases. Henceforth, the security cognizance of convenient customers is one of the dominating variables that delineate.

SMS based disease inducing. In our model, one sort of operational behavior is reproduced, i.e., whether a customer opens a suspicious message. To better depict the SMS based contamination expansion, taking after is acknowledged: On the off chance that a customer opens a spoiled message, the phone of this customer is polluted and subsequently sends contaminations to all phones concentrated around its address book. On the off chance that a customer does not open a spoiled message, its expect that the one with higher security care can

eradicates this corrupted message; A polluted phone passes on diseases to diverse phones simply once, and the corrupted phone can't pass on contaminations any more; On the off chance that a phone is settled (vaccinated), it won't pass on any contaminations paying little heed to the likelihood

E. BT- Based Propagation Process

Not the same as SMS-based infections, if a telephone is tainted with BT-based infection, then it naturally seeks an alternate gadget through accessible Bluetooth benefits inside a certain extent, and after that imitates the BT-based infection to that telephone. Consequently, clients' contact recurrence and portability designs which assume key parts in BT-based infection engendering. In our model, we coordinate a stochastic neighborhood disease progress among telephones with the versatile conduct of every client in a geological system, considering earlier research on human versatility. Taking into account our examination, an advanced cell can stay away from a BT based assault by turning off the Bluetooth administration. Be that as it may, SMS based infections regularly spread through the trust connections among companions. Past examinations likewise demonstrate that SMS-based infections are a larger number of perilous than BT based infections as far as proliferation rate and extension. In this segment, we portray two procedures to control SMS based infection engendering.

4. Methodology

Although we have used a homogenous model to simulate BT-based virus propagation in each tower, users' different travelling patterns will cause different dynamic spreading processes. Several studies have found that users' travelling patterns play a key role in virus propagation, similar to contact-based epidemics (e.g., SARS) in humans. Fig. shows three mobility patterns of users. The more accurate the mobility patterns of users are, the better predicting results about virus propagation will be.

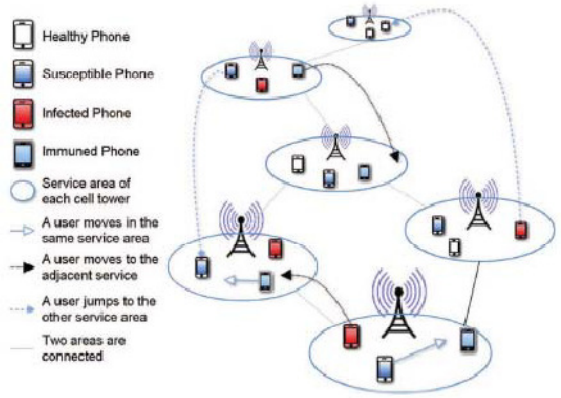

Fig 2 : Goals and Modeling Process of Autonomy-Oriented Computing

AOC has three objectives [10].The first objective is to repeat life-like conduct in reckoning. With complete learning of the essential instrument, improved exact conduct can be utilized as model for an universally useful critical thinking system. Replication of conduct is not the end, yet rather the methods, of these computational calculations; the second objective is to comprehend the crucial instrument of a certifiable complex framework by guessing and successive experimentation. The finish up result of these recreations is an advancement understanding of or clarifications to the genuine working system of the displayed framework; the third objective issues the ascent of an issue solver without human intercession. AOC framework essentially contains a populace of independent elements and whatever remains of the framework is alluded to as the earth. Focusing on substance and environment, the development of an AOC model includes three stages (see Figure 3). The primary stage, common framework recognizable proof, can be seen as the forerunner to genuine frameworks demonstrating and concerns the determination of a fitting similarity from the characteristic and physical world. There are two undertakings included: distinguish craved framework practices and recognize framework parameters.

The right similarity is the way to the accomplishment of the AOC based framework which deciphers itself through its practices.

4.1 Adaptive Patch Dissemination Strategy

After the decision of proper similarity, and points of interest like the aggregate substances to run and time to run the recreation need to be chosen. The second stage is the manufactured framework development, incorporates aggregate number of components present in the AOC-based framework. This stage is further separated into two noteworthy sub-stages: independent element demonstrating and environment displaying. The recognize helping substances errand is the first and the most imperative undertaking in which the originators are obliged to pick the level of point of interest to be demonstrated. The characterize neighborhood errand gives a certain estimation (e.g., separation) in the arrangement space inside which nearby connections can happen and nearby data accumulation is conceivable. The characterize substance representation undertaking handles how to describe an element, that likewise concentrate on its states and objectives and so on. The last assignment concerning the elements, characterize neighborhood practices and behavioral guidelines, characterizes the routes in which an Autonomous substance responds to different information which has been gathered inside its neighborhood and the courses in which it adjusts its nearby practices and behavioral standards. The assignments that worry nature are distinguishing environment attributes and characterize environment representation. The previous undertaking

concerns the part nature plays in passing on the information imparted between the self-sufficient elements. The recent undertaking addresses the characterization of nature. The third stage is the execution estimation, which is worried about the assessment criteria for looking at the simulated framework showed by the AOC-based framework. This identifies with critical thinking and gives a sign to change the current set of individual practices and behavioral standards.

5. Experiment and Results

In this experiment by considering 50, 100, 150 and 200 as number of nodes, these number of nodes we are considering into SMS based, BT based, Wifi Based and GPS based systems. We are configuring network nodes for all these models, we are differentiating these networks by varying its communication model. The BT based communication is based on inermeditory nodes where SMS based its based on node ids (i.e whom it has to communicate)

We are designing a routing protocol to manage the communication and as well as to organize detection and prevention mechanism to manage different malicious. Here malicious nodes produces an extra traffic to interrupt the communication services and mean time it redirects the actual source node routing and it changes the routing path.

In order to identify the node behavior and node propagation, we are creating a packet with some specified features, packet consist of packetid, sourport no, source address, message, destination port number, destination id, TTL etc. The packet will transfer a data across different nodes. Based on node behavior and node traffic we are identifying it as a susceptible node. Here we use packet scan type to identify the packet traffic level. Which ever the node sends more number of packets those nodes we treat it as malicious node. In such manner we are identifying malicious node. Other important factor is to prevent the node, according to the proposed idea, we have to block the virus propagation to the normal nodes. On this consideration the protocol will have to disable suscptialbe nodes by limiting propagation range by disabling RTS and CTS value as well as it will minimize its communication range and it will discard these nodes to communicate to other normal nodes. To evaluate prevention we are reducing communication range of malicious nodes and we are making nowhere in network.

6. Conclusion

In this paper, a two-layer system model for examining the spreading of SMS-based, BT based, GPS and Wifi infections [3] is indicated. Portable handsets gadgets are exploited person to malwares because of their adaptable correspondence and processing capacities, and asset requirements. This is backing in android Smartphone and precisely identifies and erases the infection of the substance before go into the portable working framework. It in the wake of using the applications gives the criticism so that the following client will think about the application. Future work can be improved the infection substance of information's go into the

Cell phone through Bluetooth and SMS channels it naturally channel the infection and information independently and erase the infection yet not the information. The result demonstrates that the Smartphone in spreading of infections through distinctive applications is being secured. As Android malware advances henceforth the viability of these sorts of measures will diminish. In any case, these systems are still important as they increase current standards of passage for repackaged and recently dispatched malware.

The understanding of associations between human practices and the engendering progress of portable infections would be useful to send security notices to various clients to enhance their security mindfulness, which can thus to assume a key part in limiting infection proliferation.

References

[1] Chao Gao and Jiming Liu, “Modeling and Restraining Mobile Virus Propagation,” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.12, NO.3, MARCH 2013.

[2] C. Gao, J. Liu, and N. Zhong, “Network Immunization with Distributed Autonomy-Oriented Entities,” IEEE Trans. Parallel and Distributed Systems, vol. 22, no.7, pp. 1222-1229, July 2011.

[3] C,Gao and J.Liu, “ Modeling and Predicting the Dynamics of Mobile Virus Spread Affected by Human Behavior”, Proc. IEEE 12th Int’l Symp. A World of Wireless, Mobile and Multimedia Networks (WoWMoM ’11), pp, 1-9, 2011.

[4] D. Balcan, V. Colizza, B. Goncalves, H. Hu, J. Ramasco, and A. Vespignani, “Multiscale Mobility Networks and the Spatial Spreading of Infectious Diseases,” Proc. Nat’l Academy of Sciences of USA, vol. 106, no. 51, pp. 21484-21489, 2009.

[5] D.-H. Shi, B. Lin, H.-S. Chiang, and M.-H. Shih, “Security Aspects of Mobile Phone Virus: A Critical Survey,” Industrial Management and Data System, vol. 108, no. 4, pp. 478-494, 2008.

[6] J.Liu, “Autonomy-Oriented Computing(AOC): The Nature and Implications of a Paradigm for Self-Organized Computing. ”Proc. Fourth Int’l Conf. Natural Computation(ICNC’08),pp.3-11,2008.

[7] X. Meng, P. Zerfos, V. Samanta, S.H. Wong, and S. Lu, “Analysis of the Reliability of a Nationwide Short Message Service,” Proc. IEEE INFOCOM, pp. 1811-1819, 2007.

[8] J.Cheng, S.H.Y. Wong,H. Yang, and S.Lu,”Smartsiren Virus Detection and Alert for Smartphones, ”Proc

.Fifth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '07),pp.258-271,2007.

[9] H.Kim, J.Smith, and K.G. Shin, "Detecting Energy-Greedy Anomalies and Mobile Malware Variants," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys 08), PP.239- 252, 2008.

[10] L.Xie, H.Song, T. Jaeger, and S.Zhu, "A Systematic Approach for Cell-Phone Worm Containment," Proc.17th Int'l World Wide Web Conf.(WWW '08), pp. 1083-1084,2008.

[11] Jiming Liu, Xiaolong Jin, Kwok ching Tsui, " Autonomous Oriented Computing(AOC): Formulating Computational Systems with Autonomous Components." IEEE Trans on system, man and cybernetics,pp.879-902,nov 2005.

[12] Vinit B. Mohata, Dhananjay M. Dakhane, Ravindra L. Pardhi, " MOBILE MALWARE DETECTION TECHNIQUES", International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 04, 2229-3345,Apr 2013.

[13] J. Balthrop, S. Forrest, M.E.J. Newman, and M.M. Williamson, "Technological Networks and the Spread of Computer Viruses," Science, vol. 304, no. 5670, pp. 527-529, 2004.

[14] R. Pastor-Satorras and A. Vespignani, "Epidemic Spreading in Scale- Free Networks," Physical Rev. Letters, vol. 86, no. 14, pp. 3200- 3203, 2001.

[15] Adebayo, Olawale Surajudeen, Mabayoje, Amit Mishra, Osho luwafemi, "Malware Detection, Supportive Software Agents and Its Classification schemes", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.6, November 2012.

[16] B. Miller, P. Pearce, C. Grier, C. Kreibich, and V. Paxson. What's Clicking What? Techniques and Innovations of Today's Clickbots. In DIMVA, 2011.

[17] N. Daswani and M. Stoppelman. The anatomy of Clickbot. A. In Proceedings of the _rst conference on First Workshop on Hot Topics in Understanding Botnets, pages 11{11. USENIX Association, 2007.

[18] N. Daswani, C. Mysen, V. Rao, S. Weis, K. Gharachorloo, and S. Ghosemajumder. Online advertising fraud. Crimeware: Understanding New Attacks and Defenses, 2008.

[19] http://en.wikipedia.org/wiki/Mobile_virus