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

Extension of the Behavioural Characterization of Proximity Malware in DTN

Syeda Mehjabeen Fatima
Student,
Department of CSE,
Shadan Women's College of Engineering & Technology,
Khairatabad, Hyderabad.

Usha Puligadda
Associate Professor,
Department of CSE,
Shadan Women's College of Engineering & Technology,
Khairatabad, Hyderabad.

Khadarbi Shaik
HOD,
Department of CSE,
Shadan Women's College of Engineering & Technology,
Khairatabad, Hyderabad.

Abstract:

With the universal presence of short-range connectivity technologies (e.g., Bluetooth and, more recently, Wi- Fi Direct) in the consumer electronics market, the delay tolerant- network (DTN) model is becoming a viable alternative to the traditional infrastructural model. Proximity malware, which exploits the temporal dimension and distributed nature of DTNs in self-propagation, poses threats to users of new technologies.

In this paper, we address the proximity malware detection and containment problem with explicit consideration for the unique characteristics of DTNs. We formulate the malware detection process as a decision problem under a general behavioral malware characterization framework.

We analyze the risk associated with the decision problem and design a simple yet effective malware containment strategy, look-ahead, which is distributed by nature and reflects an individual node's intrinsic trade-off between staying connected (with other nodes) and staying safe (from malware).

Furthermore, we consider the benefits of sharing assessments among directly connected nodes and address the challenges derived from the DTN model to such sharing in the presence of liars (i.e., malicious nodes sharing false assessments) and defectors (i.e., good nodes that have turned malicious due to malware infection).

Keywords:

Delay-Tolerant Networks (DTNs), Detection, Wi-Fi.

INTRODUCTION:

Mobile consumer electronics permeate our lives. Laptop computers, PDAs, and more recently and prominently, smart-phones, are becoming indispensable tools for our academic, professional, and entertainment needs. These new devices are often equipped with a diverse set of non-infrastructural connectivity technologies, e.g., Infra-red, Bluetooth, and more recently, Wi-Fi Direct.

With the universal presence of these short-range connectivity technologies, the communication paradigm, identified by the networking research community under the umbrella term Delay-tolerant Networks (DTNs), is becoming a viable alternative to the traditional infrastructural paradigm. Because of users' natural mobility, new information distribution applications, based on peer-to-peer contact opportunities instead of persistent connection channels among nodes, are considered to be the game changer for future network applications.

The popularity of new mobile devices (e.g., smart phones), the adoption of common platforms (e.g., Android), and the economic incentive to spread malware (e.g., spam) combinedly exacerbate the malware problem in DTNs. Malware is a piece of malicious code which disrupts the host node's functionality and duplicates and propagates itself to other nodes via contact opportunities.

In the traditional infrastructural model, the carrier serves as a gatekeeper who can centrally monitor network abnormalities and inhibit malware propagation; moreover, the resource bottleneck for individual nodes naturally limits the impact of the malware.

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

However, the central gatekeeper and natural limitations are absent in the DTN model. Proximity malware, which exploits the temporal dimension and distributed nature of DTNs in self-propagation, poses serious threats to users of new technologies and challenges to the networking and security research community. A common malware detection method currently in practice is pattern matching. More concretely, a sample of malware is first reported by an infected user. The sample is analyzed by security specialists, and a pattern which (hopefully) uniquely identifies the malware is extracted; the pattern can be either code or data, binary or textual. The pattern is then used for the detection of malware1. The analysis and extraction often involve extensive manual labor and expertise. The overhead, the lack of generality, and high false positive rate in one round of analysis make it unsuitable for promising DTN applications on smart devices.

The quest for a better malware detection method comes to the very question of how to characterize proximity malware in DTNs. In this paper, we consider an approach to characterize proximity malware by the behaviors of an infected node observed by other nodes in multiple rounds. The individual observation can be imperfect for one round, but infected nodes' abnormal behaviour will be distinguishable in the long-run. Methods like pattern matching can be used in one round of observation for the behavioral characterization of proximity malware. Instead of assuming a sophisticated malware containment capability, such as patching or self-healing , we consider the simple capability of "cutting off communication". In other words, if a node i suspects another node j of being infected with the malware, i may cease to connect with j in the future. We want to explore how far such a simple technique can take us. Our focus is on how individual nodes make such cut-off decisions based on direct and indirect observations. A comparable example from everyday experience is fire emergency. An early indication, like dark smoke, prompts two choices. One is to report fire emergency immediately; the other is to collect further evidence to make a better informed decision later. The first choice bears the cost of a false alarm, while the second choice risks missing the early window to contain the fire. . In the context of DTNs, we face a similar dilemma when trying to detect proximity malware: Hypersensitivity leads to false positives, while hyposensitivity leads to false negatives.

In this paper, we present a simple, yet effective solution; look ahead, which naturally reflects individual nodes' intrinsic risk inclinations against malware infection, to balance between these two extremes. Essentially, we extend the naive Bayesian model, which has been applied in filtering email spams, detecting botnets and designing IDSs and address two DTN specific, malware-related, problems: Insufficient evidence versus evidence collection risk.

• In DTNs, evidence (such as Bluetooth connection or SSH session requests) is collected only when nodes come into contact. But contacting malware-infected nodes carries the risk of being infected. Thus, nodes must make decisions (such as whether to cut off other nodes and, if yes, when) online based on potentially insufficient evidence. Filtering false evidence sequentially and distributed.

• Sharing evidence among opportunistic acquaintances helps alleviating the aforementioned insufficient evidence problem; however, false evidence shared by malicious nodes (the liars) may negate the benefits of sharing. In DTNs, nodes must decide whether to accept received evidence sequentially and distributed. Our contributions are summarized as follows: We present a general behavioral characterization of

• proximity malware, which captures the functional but imperfect nature in detecting proximity malware. Under the behavioral malware characterization, and

• with a simple cut-off malware containment strategy, we formulate the malware detection process as a distributed decision problem. We analyze the risk associated with the decision, and design a simple, yet effective, strategy, look ahead, which naturally reflects individual nodes' intrinsic risk inclinations against malware infection. Look ahead extends the naive Bayesian model, and addresses the DTN specific, malware-related, "insufficient evidence versus evidence collection risk" problem.

RELATED WORK:

There are several common malware detection method currently in practice is pattern matching, which is a supervised data matching technique. The existing pattern matching suffers from the following drawbacks 1.

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

Processing overhead the lack of generality,2. High false positive rate in one round of analysis make it unsuitable for DTN applications in real-time. Proximity malware and mitigation schemes has been proposed which helps to collect Bluetooth traces and demonstrated that malware could effectively propagate via Bluetooth with simulations.Some existing developed Bluetooth malware model., which showed that Bluetooth can enhance malware, propagation rate over SMS/MMS. Additionally some technique enhanced malware propagation through proximity channels in social networks and wide-area wireless networks. Late some techniques discussed optimal malware signature distribution in heterogeneous, resource-constrained mobile networks. In traditional, non-DTN, networks proposed to detect malware with learned behavioral model, in terms of system call and program flow. The final implementation extends the Naive Bayesian model, which has been applied in filtering email spam's, detecting botnets and designing IDSs and address DTN-specific, malware-related, problems.Random waypoint method has been applied,recent finding on these techniques these models may not be realistic. optimal malware signature distribution in heterogeneous, resource-constrained mobile networks. In traditional, non-DTN, networks proposed to detect malware with learned behavioral model, in terms of system call and program flow.

EXISTING SYSTEM:

Existing worms, spam, and phishing exploit gaps in traditional threat models that usually revolve around preventing unauthorized access and information disclosure. The new threat landscape requires security researchers to consider a wider range of attacks: opportunistic attacks in addition to targeted ones; attacks coming not just from malicious users, but also from subverted (yet otherwise benign) hosts; coordinated/distributed attacks in addition to isolated, single-source methods; and attacks blending flaws across layers, rather than exploiting a single vulnerability. Some of the largest security lapses in the last decade are due to designers ignoring the complexity of the threat landscape.The increasing penetration of wireless networking, and more specifically wifi, may soon reach critical mass, making it necessary to examine whether the current state of wireless security is adequate for fending off likely attacks.

Three types of threats that seem insufficiently addressed by existing technology and deployment techniques. The first threat is wildfire worms, a class of worms that spreads contagiously between hosts on neighboring APs. We show that such worms can spread to a large fraction of hosts in a dense urban setting, and that the propagation speed can be such that most existing defenses cannot react in a timely fashion. Worse, such worms can penetrate through networks protected by WEP and other security mechanisms. The second threat we discuss is large-scale spoofing attacks that can be used for massive phishing and spam campaigns. We show how an attacker can easily use a botnet by acquiring access to wifi-capable zombie hosts, and can use these zombies to target not just the local wireless LAN, but any LAN within range, greatly increasing his reach across heterogeneous networks.

DISADVANTAGES:

» Viruses can cause many problems on your computer. Usually, they display pop-up ads on your desktop or steal your information. Some of the more nasty ones can even crash your computer or delete your files.
» Your computer gets slowed down. Many "hackers" get jobs with software firms by finding and exploiting problems with software.
» Some the applications won't start (ex: I hate mozilla virus won't let you start the mozilla) you cannot see some of the settings in your OS. (Ex one kind of virus disables hide folder options and you will never be able to set it).

PROBLEM DEFINITION:

Although many schemes have been proposed to defend against malware attacks on the Internet and in wireless sensor networks, they assume persistent connectivity and cannot be directly applied to DTNs that have intermittent connectivity. The packets injected by outsider attackers can be easily filtered with authentication techniques. However, authentication alone does not work when insider attackers inject packets and replicas with valid signatures. Thus, it is still an open problem is to address inject attacks in DTNs. Most existing malware detection schemes are not a DTN specific; several existing failed to identify the malware exactly within the DTN. And several techniques suffered from several trust management problems.

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

This also suffers from the insufficient evidence versus evidence collection risk and Sequential and distributed online evidence filtering is very complicated.

PROPOSED SYSTEM:

In this paper, we present a simple, yet effective solution, look ahead, which naturally reflects individual nodes' intrinsic risk inclinations against malware infection, to balance between these two extremes. Essentially, we extend the naive Bayesian model, which has been applied in filtering email, spams detecting botnets, and designing IDSs.

We analyze the risk associated with the decision, and design a simple, yet effective, strategy, look ahead, which naturally reflects individual nodes' intrinsic risk inclinations against malware infection. Look ahead extends the naive Bayesian model, and addresses the DTN specific, malware-related, "insufficient evidence versus evidence collection risk" Proximity malware is a malicious program that disrupts the host node's normal function and has a chance of duplicating itself to other nodes during (opportunistic) contact opportunities between nodes in the DTN.

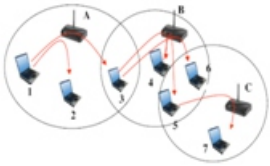
We consider the benefits of sharing assessments among nodes, and address challenges derived from the DTN model: liars (i.e., bad-mouthing and false praising malicious nodes) and defectors (i.e., good nodes that have turned rogue due to malware infections). We present two alternative techniques, dogmatic filtering and adaptive look ahead, that naturally extend look ahead to consolidate evidence provided by others, while containing the negative effect of false evidence. A nice property of the proposed evidence consolidation methods is that the results will not worsen even if liars are the majority in the neighborhood traces are used to verify the effectiveness of the methods.

Two DTN specific, malware-related:

1. Insufficient evidence versus evidence collection risk. In DTNs, evidence (such as Bluetooth connection or SSH session requests) is collected only when nodes come into contact. But contacting malware-infected nodes carries the risk of being infected. Thus, nodes must make decisions (such as whether to cut off other nodes and, if yes, when) online based on potentially insufficient evidence.

2. Filtering false evidence sequentially and distributedly. Sharing evidence among opportunistic acquaintances helps alleviating the aforementioned insufficient evidence problem; however, false evidence shared by malicious nodes (the liars) may negate the benefits of sharing. In DTNs, nodes must decide whether to accept received evidence sequentially and distributedly.

ARCHITECTURE DIAGRAM:



IMPLEMENTATION:

Service Provider:-In this module, the Service Provider browses the required file and uploads to the particular end user (End User A, End User B, End User C, End User D) via Delay Tolerant Router.

DTN Router:

The Delay Tolerant Network Router consists of Warm Filter, which is responsible for forwarding file for destination (End User A, End User B, End User C, End User D). The Warm Filter scans each and every file in the router and then forwards to dedicated destination, If found any malware in the scan then it forwards to the Evidence Aging collector. In Router can view the files scanned and transmitted with their tags File Name, Destination node details.

Malware Files:

Proximity malware is a malicious program that disrupts the host node's normal function and has a chance of duplicating itself to other nodes during (opportunistic) contact opportunities between nodes in the DTN. When duplication occurs, the other node is infected with the malware.

Evidence Aging Collector:

The Evidence aging collector is responsible to scan and block the malicious infected file.

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

A defector starts as a good node but turns evil due to malware infections; the assessments collected before the defector's change of nature, even truthful, are misleading. To solve the problem of outdated assessments, old assessments are discarded and to save the end user by infected malware file in a process called evidence aging.EAC can view the Virus Name, attacker IP, attacked time, Result.End User:-In this module, the End user can Recieve the data file from the Service Provider and end user who will receive file contents scanned by the warm filter in the Delay Tolerant Network Router.
Attacker:-In this module, the Attacker browses the malicious file and uploads to the particular end user (End User A, End User B, End User C, End User D). The malicious nodes those are able to transmit malware to the destination.

CONCLUSION:

Behavioral characterization of malware is an effective alternative to pattern matching in detecting malware, especially when dealing with polymorphic or obfuscated malware. Naive Bayesian model has been successfully applied in non-DTN settings, such as filtering email spams and detecting botnets. We propose a general behavioral characterization of DTN-based proximity malware. We present look ahead, along with dogmatic filtering and adaptive look ahead, to address two unique challenging in extending Bayesian filtering to DTNs: "insufficient evidence versus evidence collection risk" and "filtering false evidence sequentially and distributedly." In prospect, extension of the behavioral characterization of proximity malware to account for strategic malware detection evasion with game theory is a challenging yet interesting future work.

REFERENCES:

[1] Trend Micro Inc. (2004) SYMBOS CABIR.A. [Online]. Available: http://goo.gl/aHcES

[2] [Online]. Available: http://goo.gl/iqk7

[3] Trend Micro Inc. (2009) IOS IKEE.A. [Online]. Available: http://goo.gl/z0j56

[4] P. Akritidis, W. Chin, V. Lam, S. Sidiroglou, and K. Anagnostakis, "Proximity breeds danger: emerging threats in metro-area wireless networks," in Proc. USENIX Security, 2007.

[5] A. Lee. (2012) FBI warns: New malware threat targets travelers, infects via hotel Wi-Fi. [Online]. Available: http://goo.gl/D8vNU

[6] NFC Forum. About NFC. [Online]. Available: http: // goo.gl/zSJqb

[7] Wi-Fi Alliance. Wi-Fi Direct. [Online]. Available: http: //goo.gl/fZuyE

[8] C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, and X. Wang, "Effective and efficient malware detection at the end host," in Proc. USENIX Security, 2009.

[9] U. Bayer, P. Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda, "Scalable, behavior-based malware clustering," in Proc. IEEE NDSS, 2009.

[10] D. Dash, B. Kveton, J. Agosta, E. Schooler, J. Chandrashekar, A. Bachrach, and A. Newman, "When gossip is good: Distributed probabilistic inference for detection of slow network intrusions," in Proc. AAAI, 2006.

[11] G. Zyba, G. Voelker, M. Liljenstam, A. M´ehes, and P. Johansson, "Defending mobile phones from proximity malware," in Proc. IEEE INFOCOM, 2009.

[12] F. Li, Y. Yang, and J. Wu, "CPMC: an efficient proximity malware coping scheme in smartphone-based mobile networks," in Proc. IEEE INFOCOM, 2010.

[13] I. Androutsopoulos, J. Koutsias, K. Chandrinos, and C. Spyropoulos, "An experimental comparison of naïve bayesian and keyword-based anti-spam filtering with personal e-mail messages," in Proc. ACM SIGIR, 2000.

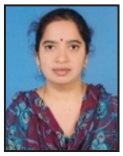
[14] P. Graham. Better Bayesian filtering. [Online]. Available: http://goo.gl/AgHkB

[15] J. Zdziarski, Ending spam: Bayesian content filtering and the art of statistical language classification. No Starch Press,2005.

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

Authors:

Ms. Syeda Mehjabeen Fatima
has completed her B.E. in CSE Department from Muffakham Jah College Of Engineering and Technology, Osmania University, Hyderabad. Presently she is pursuing her Masters in Computer Science in Shadan Women's College of Engineering and Technology, Khairatabad, Hyderabad, India.



Usha Puligadda
has completed B.E from TKR College of Engineering, M.Tech (CSE) from JNTUH. She is having 11 years of experience in Academic, Currently working as Assistant Professor at Shadan Women's .College of Engineering and Technology ,Hyderabad, AP. Her research includes data mining, data warehouses, databases, software testing methodologies(STM).

Khadarbi Shaik
has completed B.E from TKR College of Engineering, M.Tech (CSE) from JNTUH. She is having 11 years of experience in Academic, Currently working as Assistant Professor at Shadan Women's .College of Engineering and Technology ,Hyderabad, AP. Her research includes data mining, data warehouses, databases, software testing methodologies(STM).