IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Detecting Targeted Malicious Email by Spam Filtering Using Naïve Bayesian Classification

Mrs. M. Rajeswari[1], Radhika Rama Rao[2], Priyadharshini .R[3], Aarthi .R[4]

Assistant Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, India [1]

Student, Department of Information Technology, Panimalar Institute of Technology, Chennai, India [2,3,4]

Abstract: In recent years, Targeted Malicious Email (TME) has become more dangerous. Beyond spam and phishing designed to trick users into revealing information, TME exploits computer networks and gathers sensitive information. It targets on single users and is designed to appear legitimate and trustworthy. In this paper, we propose a new email filtering technique using random forest classifier. A compromised router detection protocol is developed to identify congestive packet losses. We also develop feature extraction procedure to identify TME specific features. Naive Bayesian classification is used to classify mails as either TME or trusted mail.

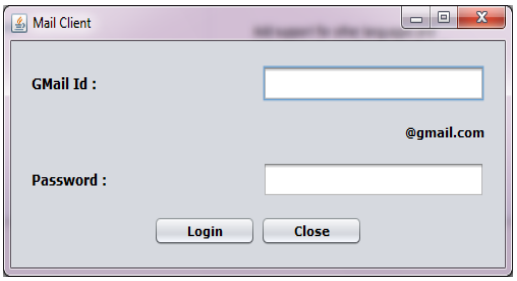
Keywords: Targeted Malicious Email, router detection protocol, feature extraction, Naive Bayesian.

I. INTRODUCTION

Nowadays email has deeply entrenched in our society as most of the research efforts have been made for making email technology more convenient, intuitive to use and costing virtually nothing. Thus, an email system has become an important and essential communication approach for millions of people since one can conveniently transfer messages electronically to anyone within seconds at visibly zero cost [1]. In order to use email, one has to use a mail client to access the mail server. The mail client and mail server use a variety of protocols for exchanging information with each other [2]. The users can access email in several ways, but most popular ones are Post Office Protocol (POP), Interactive Mail Access Protocol (IMAP) and Webmail.

POP is designed to support offline mail processing. With POP protocol, messages are delivered to the mailboxes and users can access their mailboxes and download messages from the mail server to their computers by using mail client programs. Once the messages are delivered to the computer the messages are deleted from the mail server. IMAP is more complex and recent development which is designed for the users to stay connected to one or more email servers while reading, creating and organizing messages. With IMAP, the mails can be accessed by connecting to the servers only. The mails cannot be viewed when one is offline. Webmail offers complete access to one's email without any email being downloaded to one's computer. Email can be accessed with one's web browser however, webmail depends on a web browser (e.g. Firefox, IE, Opera, Chrome, Safari, etc.) which can take some time to load, access the webmail page, login and load the GUI.

The users of email face various difficulties due to the attacks which may destroy the whole system. In this paper we propose a new email-filtering technique based on email's persistent-threat and recipient-oriented features with a random forest classifier which outperforms the two traditional detection methods, Spam Assassin and Clam AV, while maintaining reasonable false positive rates. Here, detection of targeted malicious packet (email) for normal network into modern network is described. We develop a compromised router detection protocol that dynamically infers the precise number of congestive packet losses that will occur.



According to the statistics in [7], around 90% of email messages are spam. Spam is not only irritating and nuisance; it is also a persistent problem which can cause significant harm negatively affecting the internet users and administrators. It has also increasingly become extremely dangerous as 83% of spam contains a URL so phishing sites and Trojan infections are just one click away [8]. email spam is not only wastage of time but it also consumes storage on the server and blocks communication channels until the recipient takes some action on it. Also there is a chance of deletion of an important email while deleting spam emails. Spam email is also a great malware carrier in order to infect computers with viruses.

TME on the other hand is more dangerous than spam and phishing. Spam and phishing is easy to detect as it is mass generated sent to millions of people. It is possible to gather mails with similar characteristics and message content probably for identifying spam. But TME is designed to target a single individual and is difficult to detect. So, we develop an alternative filtering procedure by using TME specific feature extraction. Thus, using all the methods described above the detection of TME is done.

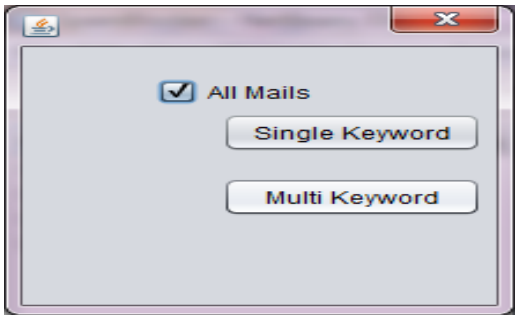
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

II. PROPOSED METHODOLOGY

The main problem in the current scenario is the attacks on the mail. Sometimes this may lead to destruction of the entire system. Our main aim is to detect TME and acknowledge about it to the user. We develop a compromised router detection protocol that identifies congestive packet losses. To identify the TME we propose a specific feature extraction algorithm. A simplified view of our classification consists of pre-processing the mail for leveraging company information. Persistent threat and recipient oriented features are extracted and the associated mails are classified using random forest classifier. We use Non-Targeted Malicious Email (NTME) and TME datasets to construct TME filter technique and provide context for the new features incorporated for TME detection. In this paper, we also propose Naive Bayesian classification for classifying the mails.



III.RELATED WORKS

(1) STEMMING ALGORITHM

Stemming is reducing the word to the root form, where lemmatization is concerned with linguistics. Lemmatization is “go”, ”gone”, ”goes”, ”going”, ”been” and “went”, where stemming a word would be reducing a word from "gone" to "go", so it can be matched to other stemmed words such as "going", as "going" stemmed would also be "go".

A better example is: "engineering", "engineers", "engineered", "engineer"

These four words would not match up if they were tested for equality, however by stemming these words we can reduce them to a more basic form,

engineering	-->	engineer
engineers	-->	engineer
engineered	-->	engineer
engineer	-->	engineer

Now the stemmed words will match for equality. So, now if we try searching using the word engineer, documents on engineering, engineers and engineered would be returned from a stemmed index/database.

Stemming usually means to cut off characters from the end of the word, e.g. walked -> walk, walking -> walk. However, this does not necessarily produce a real word, e.g. a stemmer could also change house and houses to ”hous". Also, cutting of characters isn't enough for irregular words, e.g. you cannot get from "went" to "go" by just cutting of characters. A lemmatizer solves these problems, i.e. it always produces real words, even for irregular forms. It usually needs a table of irregular forms for this.

IV. CLASSIFICATION

In this paper, the classification method used to classify the mails is:

(2) NAIVE BAYESIAN CLASSIFICATION

A Naive Bayesian classifier is a simple probabilistic classifier based on applying Bayesian theorem with strong (Naive) independence assumptions. A more descriptive term for the underlying probability model would be "independent feature model". Naive Bayesian belongs to a group of statistical techniques that are called 'supervised classification' as opposed to 'unsupervised classification.' In 'supervised classification' the algorithms are told about two or more classes to which texts have previously been assigned by some human(s) on whatever basis.

In simple terms, a Naive Bayesian classifier assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature, given the class variable. For example, a fruit may be considered to be an apple if it is red, round, and about 4" in diameter. Even if these features depend on each other or upon the existence of the other features, a Naive Bayesian classifier considers all of these properties to independently contribute to the probability that this fruit is an apple.

Depending on the precise nature of the probability model, Naive Bayesian classifiers can be trained very efficiently in a supervised learning setting. In many practical applications, parameter estimation for Naive Bayesian models uses the method of maximum likelihood; in other words, one can work with the Naive Bayesian model without believing in Bayesianian probability or using any Bayesianian methods.

In spite of their Naive design and apparently over-simplified assumptions, Naive Bayesian classifiers have worked quite well in many complex real-world situations. In 2004, analysis of the Bayesianian classification problem has shown that there are some theoretical reasons for the apparently unreasonable efficacy of Naive Bayesian classifiers. Still, a comprehensive comparison with other classification methods in 2006 showed that Bayesian classification is outperformed by more current approaches, such as boosted trees or random forests.

An advantage of the Naive Bayesian classifier is that it only requires a small amount of training data to estimate the parameters (means and variances of the variables) necessary for classification. Because independent variables are assumed, only the variances of the variables for each class need to be determined and not the entire covariance matrix.

Example:

Problem: Classify whether a given person is a male or a female based on the measured features. The features include height, weight, and foot size.

DOI 10.17148/IJARCCE.2016.53167

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

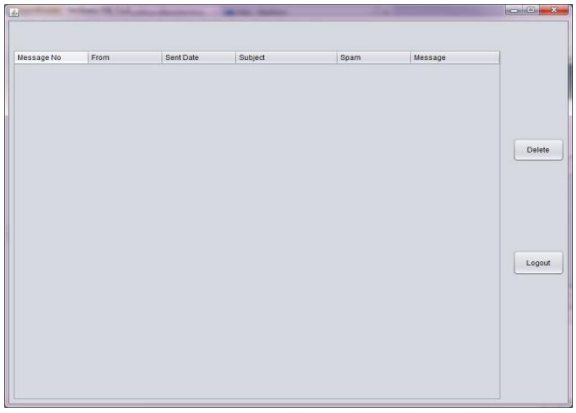
Training: Example training set below.

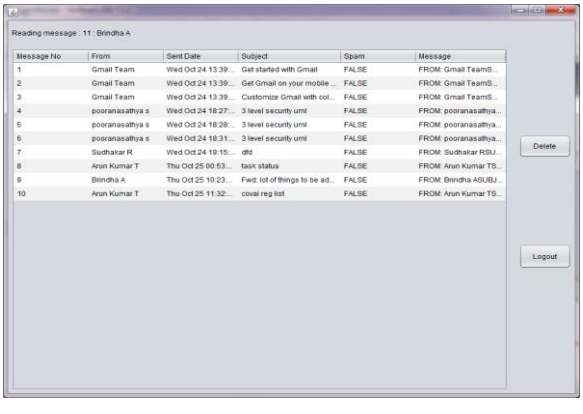
Gender	Height (ft)	Weight (lbs)	Foot size(inches)
male	6	180	12
male	5.92 (5'11")	190	11
male	5.58 (5'7")	170	12
male	5.92 (5'11")	165	10
female	5	100	6
female	5.5 (5'6")	150	8
female	5.42 (5'5")	130	7
female	5.75 (5'9")	150	9

The classifier created from the training set using a Gaussian distribution assumption would be:

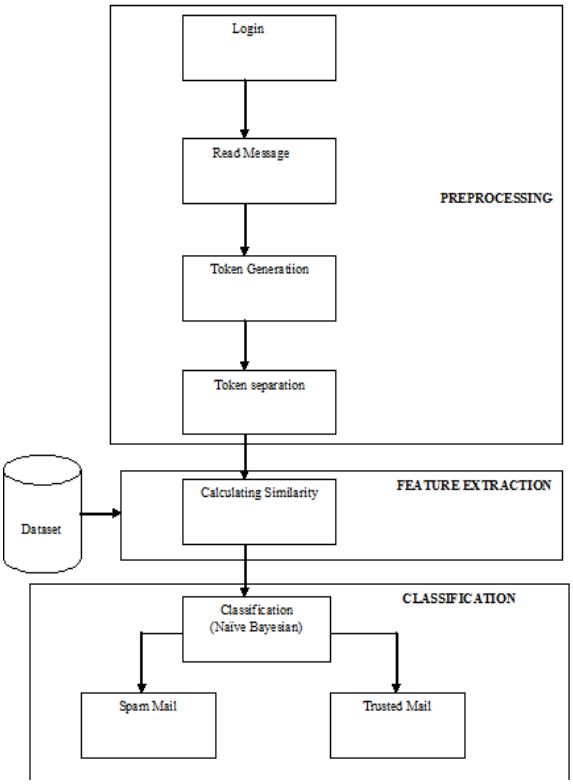
Gender	mean (height)	variance (height)	mean (weight)	variance (weight)	mean (foot size)	Variance (foot size)
male	5.855	3.5033e-02	176.25	1.2292e+02	11.25	9.1667e-01
female	5.4175	9.7225e-02	132.5	5.5833e+02	7.5	1.6667e+00

Let's say we have equiprobable classes so P(male)= P(female) = 0.5. There was no identified reason for making this assumption so it may have been a bad idea. If we determine P(C) based on frequency in the training set, we happen to get the same answer.





V. SYSTEM ARCHITECTURE



The detection of TME is done by using Naive Bayesian classification. The user must login using mail id and password. During the training, a model is built based on the characteristics of each category in a pre-classified set of e-mail messages. The training dataset should be selected in such a way that it is varying in content and subject. Each sample message is labeled with a specific category. We first perform pre-processing to extract tokens and determine the number of occurrences of each token in each category. Spam filtering is based on calculating the fuzzy similarity measure between the received message and each category i.e. spam and legitimate. The token with the maximum number of occurrences is assigned with a value of 1, and all other tokens are assigned with proportional values. The mails are then classified using Naive Bayesian classification which detects the mails with highest probability of spam. The mails are classified as spam mail and trusted mail.

VI. PREVIOUS STUDY

LEARNING TO FILTER SPAM E-MAIL: A COMPARISON OF A NAÏVE BAYESIAN AND A MEMORY-BASED APPROACH
Ion Androutsopoulos, GeorgiosPaliouras, Vangelis Karkaletsis, Georgios Sakkis, Constantine D. Spyropoulosand Panagiotis Stamatopoulos

We investigate the performance of two machine learning algorithms in the context of anti spam filtering. The increasing volume of unsolicited bulk e-mail (spam) has generated a need for reliable anti-spam filters. The Naive Bayesian classifier has recently been suggested as an

effective method to construct automatically anti-spam filters with superior performance. We investigate thoroughly the performance of the Naive Bayesian filter on a publicly available corpus, contributing towards standard benchmarks. Both methods achieve very accurate spam filtering, outperforming clearly the keyword-based filter of a widely used e-mail reader.

Drawbacks:
Filters of this type have so far been based mostly on keyword patterns that are constructed by hand and perform poorly.

DETECTING TARGETED MALICIOUS EMAIL THROUGH SUPERVISED CLASSIFICATION OF PERSISTENT THREAT AND RECIPIENT ORIENTED FEATURES
Rohan Mahesh Amin
Persistent threat features, such as threat actor locale and weaponization tools, along with recipient oriented features, such as reputation and role, are leveraged with supervised data classification algorithms to demonstrate new techniques for detection of targeted malicious email. Finally, detection of targeted malicious email using persistent threat and recipient oriented features results in significantly fewer false negatives than detection of targeted malicious email using conventional email filtering techniques.

Drawbacks:
This improvement in false negative rates comes with acceptable false positive rates.

INTELLIGENCE-DRIVEN COMPUTERNETWORK DEFENSE INFORMED BY ANALYSIS OF ADVERSARY CAMPAIGNS AND INTRUSION KILL CHAINS

Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin, Ph.D.z
Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. . The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but also the threat component of risk.
An

Drawbacks:
An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insouciant for certain methods.

INTEGRATED NETWORK ELECTRONIC WARFARE: CHINA'S NEW CONCEPT OF INFORMATION WARFARE
Deepak Sharma
The People's Liberation Army (PLA) considers active offence to be the most important requirement for information warfare to destroy or disrupt an adversary's capability to receive and process data. Launched mainly by remote combat and covert methods, the PLA could employ information warfare pre-emotively to gain the initiative in a crisis. Specified information warfare objectives include the targeting and destruction of an enemy's command system, shortening the duration of war, minimizing casualties on both sides, enhancing operational efficiency, reducing effects on domestic populations and gaining support from the international community. The PLA sees CNO as critical to seize the initiative and achieve "electromagnetic dominance" early in a conflict, and as a force multiplier.

Drawbacks:
Although there is no evidence of a formal Chinese CNO doctrine, PLA theorists have coined the term "Integrated Network Electronic Warfare" to outline the integrated use of electronic warfare, CNO, and limited kinetic strikes against key command and control, communication and computers nodes to disrupt the enemy's battlefield network information systems.

VII. CONCLUSION

A new email filtering technique focused on persistent threat and recipient- oriented features outperforms other available techniques. Targeted malicious emails (TME) for computer network exploitation have become more insidious and more widely documented in recent years. We develop a compromised router detection protocol that dynamically infers the precise number of congestive packet losses that will occur. We develop an alternative filtering procedure by using TME specific feature extraction. Our protocols automatically predict congestion in a systematic manner and that it is necessary. In this paper, we propose Naïve Bayesian classification for classifying mails as spam and trusted.

REFERENCES

[1] M. W. Wong, "Sender authentication what to do," A Messaging Anti-Abuse Working Group Whitepaper. [Online]. Available: www.openspf.org/blobs/sender-authentication-whitepaper.pdf
[2] P. Loshin, Essential Email Standards: RFCs and Protocols Made Practical. Hoboken, NJ, USA: Wiley, 1999.
[3] J. Myers and M. Rose, "Post Office Protocol—Version 3," STD 53, RFC 1939, May 1996. [Online]. Available: http://www.rfc-editor.org/ info/rfc1939
[4] G. V. Cormack and T. R. Lynam, "Spam corpus creation for TREC," in Proc. 2nd CEAS, Palo Alto, CA, USA, Jul. 2005.
[5] "When was the first spam email sent? What did it advertise?" Accessed: May 4, 2014. [Online]. Available: http://email.about.com/od/emailtrivia/f/first_spam.htm
[6] M. Crispin, "Internet message access protocol—Version 4rev1," RFC 2060, Dec. 1996. [Online]. Available: http://www.rfc-editor.org/info/rfc2060
[7] Messaging Anti-Abuse Working Group, Email Metrics Program: Report #15—First, Second and Third Quarter 2011, Messaging, Malware and Mobile Anti-Abuse Working Group (MA3AWG), San Francisco, CA, USA, Tech. Rep.
[8] M. Wong and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing User of Domains in E-Mail," tech. memo, Internet Soc., 2006; www.ietf.org/rfc/rfc4408.txt.
[9] M. Sahami et al., A Bayesian Approach to Filtering Junk Email, tech. report WS-98-05, Am. Assoc. Artificial Intelligence, 1998.
[10] R. Beverly and K. Sollins, Exploiting Transport-Level Characteristics of Spam, tech. report MIT-CSAIL-TR-2008-008, Computer Science and Artificial Intelligence Lab, MIT, 2008.

[11] D. Erickson, M. Casado, and N. McKeown, "The Effectiveness of Whitelisting: A User-Study," Proc. Conf. Email and Anti-Spam, 2008; www.ceas.cc/2008/papers/ceas2008-paper-20.pdf.
[12] M. Tran and G. Armitage, "Evaluating the Use of Spam-Triggered TCP Rate Control to Protect SMTP Servers," Proc. Australian Telecom. Networks and Applications Conf. (ATNAC 04), ATNAC, 2004, pp. 329–335.
[13] C. Li, W. Jiang, and X. Zou, "Botnet: Survey and case study," in Proc. 4th ICICIC, Kaohsiung, Taiwan, Dec. 7–9, 2009, pp. 1184–1187.
[14] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," Comput. Netw., vol. 57, no. 2, pp. 378–403, Feb. 2013.
[15] N. Ianelli and A. Hackworth, "Botnets as a vehicle for online crime," Coordination Center, CERT cMellon University, Canegie CERT, 2005.
[16] P. Bacher, T. Holz, M. Kotter, and G. Wicherski, "Know your enemy: Tracking botnets (using honeynets to learn more about bots)," Honeynet Project, Tech. Rep., 2008.
[17] R. Puri, Bots & Botnet: An Overview. Singapore: SANS Institute InfoSec Reading Room, 2003.
[18] P. Wang, L. Wu, B. Aslam, and C. C. Zou, "A systematic study on peerto- peer botnets," in Proc. 18th ICCCN, Aug. 3–6, 2009, pp. 1–8.
[19] Z. Zhu, G. Lu, Y. Chen, Z. Fu, and R. P. K. Han, "Botnet research survey," in Proc. 32nd IEEE Int. Annu. COMPSAC, Turku, Finland, Jul. 28–Aug. 1, 2008, pp. 967–972.
[20] M. Feily, A. Shahrestani, and S. Ramadass, "A survey of botnet and botnet detection," in Proc. 3rd Int. Conf. SECURWARE Emerging Inf., Syst. Technol., Athens, Greece, Jun. 18–23, 2009, pp. 268–273.
[21] H. S. Nair and S. E. Vinodh Ewards, "A study on botnet detection techniques," Int. J. Sci. Res. Publ., vol. 2, no. 4, pp. 1–3, Apr. 2012.
[22] E. Alparslan, A. Karahoca, and D. Karahoca, "Advances in data mining knowledge discovery and applications," in BotNet Detection: Enhancing Analysis by Using Data Mining Techniques. Rijeka, Croatia: INTECH, ch. 17, Sep. 12, 2012.
[23] L. Zhang, S. Yu, D.Wu, and P.Watters, "A survey on latest botnet attack and defense," in Proc. 10th IEEE Int. Conf. TrustCom, Security Privacy, Nov. 16–18, 2011, pp. 53–60.
[24] S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, and S. A. Khayam, "A taxonomy of botnet behavior, detection and defense," IEEE Comun. Surveys Tuts., vol. 16, no. 2, pp. 898–924, 2nd Quart. 2013.
[25] A. Karim et al., "Botnet detection techniques: Review, future trends and issues," J. Zhejiang Univ.–SCIENCE C, vol. 15, no. 11, pp. 943–983, Nov. 2014.
[26] R. Beverly and K. Sollins, "Exploiting transport-level characteristics of spam," in Proc 5th CEAS, Mountain View, CA, USA, Aug. 2008.
[27] A. Sperotto, G. Vliek, R. Sadre, and A. Pras, "Detecting spam at the network level," in Proc. 15th EUNICE/Open Eur. Summer School/IFIP TC6.6 Workshop Internet Future, Barcelona, Spain, Sep. 7–9, 2009, pp. 208–216.
[28] M. Ye, T. Tao, F.-J.Mai, and X.-H. Cheng, "A spam discrimination based on mail header feature and SVM," in Proc. 4th Int. Conf. WiCOM, Netw. Mobile, Dalian, China, Oct. 12–14, 2008, pp. 1–4.
[29] C.-H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Syst. Appl., vol. 36, no. 3, pp. 4321–4330, Apr. 2009.
[30] J. Sheu, "An efficient two-phase spam filtering method based on emails categorization," Int. J. Netw. Security, vol. 9, no. 1, pp. 34–43, Jul. 2009.
[31] H. Gomes, C. Cazita, J. M. Almeida, V. Almeida, and J. W. Meira, "Characterizing a spam traffic," in Proc. 4th ACM SIGCOMM IMC, Taormina, Sicily, Italy, Oct. 25–27, 2004, pp. 356–369.
[32] S. T. Vuong and M. S. Alam, Advanced Methods for Botnet Intrusion Detection Systems, P. Skrobanek, Ed. Rijeka, Croatia: InTech, 2011.
[33] C. Kanich, K. Levchenko, B. Enright, G. M. Voelker, and S. Savage, "The heisenbot uncertainty problem: Challenges in separating bots from chaff," in Proc. 1st USENIX Workshop LEET, Apr. 2008, p. 10.
[34] S. Lab., March 2011 Intelligence Report. Symantec Report 2011, Symantec Corp., Mountain View, CA, USA. 2011.
[35] A. Ramachandran, N. Feamster, and D. Dagon, "Revealing botnet membership using DNSBL counter-intelligence," in Proc. 2nd USENIX SRUTI, Jul. 7, 2006, vol. 2, pp. 49–54.