ENGW3301 Project 1: Discourse Community Analysis

ISAAC BOEHMAN, Northeastern University

Through use of didactic language targeting multiple audiences unified by a common interest in original research with practical applications, the academic journal ”Transactions in Information and System Security”, published by the Association for Computing Machinery, exemplifies the multi-disciplined pragmatic focus of the security community as a whole.

General Terms: Discourse Community Analysis

Additional Key Words and Phrases: Advanced Writing, Discourse Community, speech community, Swales, Gee

ACM Reference Format:
Isaac Boehman, 2014. ENGW3301 Project 1: Discourse Community Analysis. *ACM Trans. Info. Syst. Sec.* 1, 1, Article 1 (May 2014), 5 pages.
DOI:http://dx.doi.org/10.1145/0000000.0000000

1. INTRODUCTION

”Transactions in Information and System Security” (TISSEC) is a scholarly journal published by the Association for Computing Machinery (ACM). In this paper, I will examine how language is used to convey the values of pragmatism leading to data-driven conclusions in the security field as a whole. I will examine the individual contributions in Volume 16 Issue 4 of TISSEC to build up a case for the stated thesis. I will do so by examining the persona of individual contributions contrasted with the collection as a whole. Similarly, the audience of the individual contributions will be analyzed and contrasted with the audience targeted by the collection at large. Next the context of the collection will be analyzed to answer questions of what prior knowledge is necessary to successfully read these contributions. Finally, the thesis and purpose of the journal will be analyzed to determine how they are supported and given credence by the previous sections.

2. PERSONA

2.1. Language

The language and tone throughout the various contributions included in the issue of TISSEC is consistently didactic. This is not surprising considering TISSEC is a scholarly journal published by ACM, whose focus is to advance computing as a science and profession [Association for Computing Machinery 1947], with the focus of TISSEC directed at publishing ”original research in all areas of information and system security, including technologies, systems, applications, and policies” [Transactions in Information and System Security 1998].

This work is supported by the parents of Isaac Boehman in combination with the Stafford Loans offered by the United States Department of Education

Author’s addresses: I. Boehman, Student, Northeastern University.

DOI:http://dx.doi.org/10.1145/0000000.0000000

2.2. Stylistic Patterns

A number of stylistic patterns are used throughout each contribution in this issue of TISSEC.

One such pattern is the use of a first-person point-of-view. Normally one would expect for scholarly writing to be done in the third-person point-of-view, however as each of the contributions are presenting original research findings performed by the authors themselves, they are able to write as such because they themselves were involved in the primary sources being used in their article. For example, use of the word ”we” is extremely common throughout each contribution in this issue, due to each contribution being authored by numerous individuals.

Another example of a stylistic pattern used throughout the contributions is the use of italics to emphasize the keywords or key-phrases that are being introduced or defined. This sort of emphasis signals subconsciously to the reader that this term and definition are important and makes it easy for readers to scan through a contribution to look for a key term they encountered that they are unfamiliar with. If the term is not defined in the paper, meaning it is not in the paper somewhere italicized and defined, then the reader will know they need to look it up elsewhere. Likewise, parenthesis are another stylistic pattern used heavily throughout the contributions wherever additional information such as abbreviations or short explanations of a concept are required.

Additionally, each individual contribution provided an abstract at the beginning of their article. This provides a one to two paragraph overview of the contents of the paper and is extremely useful when searching through a large amount scholarly research papers as they provide a sense of what the paper contains, and using that, you are able to determine whether or not this paper will be useful to you without needing to read the entire paper first. Similarly, the use of section headings, subheadings, and subsubheadings is another pattern that can be seen throughout each of the contributions. Authors of the contributions use these headings to title individual sections of the article with relevant names. These titles then provide an easy means for readers to skim through a paper to find exactly the section that they are interested in or are specifically looking for. For example, while writing this paper, I needed to determine what the purpose of each contribution was in this issue of TISSEC. By reading the abstract, skimming the section titles, and, if present, reading the conclusions, I was quickly able to get an idea of what each contribution was trying to convey. Without these headings, this process either would have taken a much longer time or I would have simply stuck with reading the abstracts. Plus, the use of section headings allows for a sort-of mental reset for the reader, which then allows the author to re-use any words they may have previously used to start paragraphs or sentences.

There are no advertisements contained within this issue, or within any issue, of TISSEC. Neither are there any editorials or opinion pieces. The journal simply presents a collection of around four to five different articles (each around 30 pages) detailing the latest research being done in the security field.

Finally, it’s readily apparent that the contributions are all formatted in the same manner. This is absolutely no accident and is due to the considerable amounts of submissions that each ACM-published journal receives. ACM provides a template for authors of submissions to use when documenting their research and findings, allowing authors to focus just on the content of their contributions and to not have to worry about styling. Then, when publishing the issue, those putting together the issue of the journal do not have to perform nearly as much work to format each contribution in a consistent style. This not only makes things easier for authors and editors, but also makes things easier on the readers as well. By abstracting away the formatting and styling into a template, ACM makes it much easier for readers to focus on the content of the individual contributions instead of being distracted by changing, inconsistent styling. Additionally, it very clearly demonstrates the pragmatic nature of the computing field as a template very cleanly solves the issue of having to comb through submissions in a wide variety of different formats. Were templates not used, the turnaround time for submissions would extend even longer than the already lengthy process, around one year for submissions to TISSEC.

3. AUDIENCE

TISSEC is an academic journal focused on topics in security. This much can be gathered by just looking at the name of the journal itself, ”Transactions in Information and System Security”. As such, issues of TISSEC are written to the security community at large. In other words, the collection is written to an audience unified through its focus on topics in security. However, the topic of security itself is quite a broad, all-encompassing topic, meaning that was akin to saying a journal is written to the ”literature community”. Because security is such a broad topic, this leads to the individual contributions contained in an issue focusing on a very specific area in the security domain, i.e. the individual contributions are all written to their own specific audiences while the collection as a whole is written towards the security community itself. For example, the contribution ”Exposure: A Passive DNS Analysis Service to Detect and Report Malicious Domains” [Bilge et al. 2014] is focused on machine learning in network security to provide better detection of security threats, while ”Sophisticated Access Control via SMT and Logical Frameworks” [Arkoudas et al. 2014] is written towards an audience involved with access control and policy analysis with experience with typed first-order logic. Both of these contributions are targeted towards different specific audiences, yet are also targeted towards those interested in security as a whole.

Each individual contribution is highly technical and very in-depth and detailed. It comes as no surprise then that one would make the connection that this journal is not written towards those outside of this discourse community, but is written to the community itself. Additionally, we can also make the claim that each contribution in the journal is targeted towards the experts (or at least, equals) in the field related to the contribution. This is readily apparent once you begin to look at where each of the authors belongs to. For example, the ”Exposure” paper reference above is written by Leyla Bilge of Symantec Research, Sevil Sen of Hacettepe University, David Balzarotti of Eurecom (a French graduate school), Engin Kirda of Northeastern University, and Christopher Kruegel of the University of California Santa Barbara. As you can see, four out of the five authors are affiliated with different universities from around the world, while one is associated with a very large security company’s research department. These are not novice researchers, but seasoned professionals.

As the collection is targeted towards experts or equals, there is a large amount of specialized lexis that is used throughout each contribution that goes undefined. Were this lexis to be defined, the bodies of work would swell to even longer lengths and become bogged down defining everything. By forgoing these definitions, each contribution is able to achieve a high-level of discourse, allowing for the rapid communication of new ideas and research to others in the field, facilitating discussions, posing questions, and advancing the field as a whole, which fits in very well with the overarching goal of TISSEC to present original research with practical applications.

4. CONTEXT

As has been stated before, TISSEC is produced to publish original research papers in all areas of information and system security. This tells us that the security field is quite large and actively researched since new issues are published routinely throughout the year. This purpose, combined with being written to an audience of experts, proves just how necessary it is for specialized lexis to be used throughout contributions with assumed knowledge of said lexis.

The content of each contribution to this issue of TISSEC is highly detailed and highly technical. Each contribution is around 30 pages single-spaced text with a handful of images, charts, tables and equations interspersed throughout. The length of each contribution along with their high level of detail requires a significant amount of background knowledge from the readers. This is even more so when you consider the basic structure of each contribution. All start with an abstract and introduction section. Then, there's a section of background information and previous or related works, though these are sometimes included in the introduction itself. Next follows the presentation of the research, followed by an analysis and/or empirical evaluation of said research, which leads to data-backed conclusions or practical applications of the presented research. Since there is so much to present in the paper, not a lot of space can be dedicated to providing detailed background information on the topic at hand. As such readers of TISSEC must have at a minimum a basic understanding of various security concepts, such as access control, encryption, networking, and operating systems. Additionally, the reader will need a basic understanding of whatever subtopic of security an individual contribution is about. For example, the contribution ”Off-Path TCP Injection Attacks” [Gilad and Herzberg 2014] assumes that the reader is familiar with the basic operation of the TCP protocol, particularly with how connections are established. Without this background knowledge, a reader will either consistently context switch to look something up, or quickly become discouraged and abandon reading the paper entirely, as the contribution very quickly begins to dive into the intricacies and quirks of the protocol that lead to the security vulnerabilities documented in the paper. This is not an isolated incident as each of the contributions followed a similar format as shown above.

5. THESIS

TISSEC is ”devoted to the study, analysis, and application of information and system security” [ATI]. This thesis is supported by the contributions that advance their respective fields which make up each issue of the transaction. By focusing on a variety of broad subtopics in the security field (security technologies, secure systems, security applications, security policies), TISSEC is able to address a very wide audience in a very large field at a very high level of discourse to accomplish their goal of advancing the field as a whole.

6. PURPOSE AND CONCLUSION

6.1. Purpose

As a whole, TISSEC sets out to inform, analyze, and evaluate original research with practical applications. ”Practical applications” is not just a buzz word, but a requirement for a submission to be accepted into the journal for publication. Submissions that do not have practical relevance to the construction, evaluation, application, or operation of secure systems will be rejected. [TISSEC 1998]. Through an intensive peer-review process (which takes around 11 months), submissions are vetted to ensure that they will embody the purpose of the journal as a whole. For example, the contribution ”An Anti-Phishing System Employing Diffused Information” [**?**] was submitted January 2013, revised August 2013 and November 2013, and finally accepted in February of 2014, for a total of 13 months in peer-review. It is clear that the editors of this journal take their role as gatekeepers very seriously.

Additionally, all conclusions arrived at in each of the contributions are backed by data

6.2. Conclusion

It should fairly clear by now that TISSEC is a very serious scholarly journal that seeks to advance the security field at large. While written towards a very broad audience, each individual contribution is written towards a specific audience of experts in a particular subtopic of the security field. This has been shown through examples of language use, stylistic patterns, and the context in which the journal is published.

ACKNOWLEDGMENTS

The author would like to thank the Internet for its vast array of resources.

REFERENCES

ACM Transactions on Information and System Security (TISSEC). ACM, New York, NY, USA.

Konstantine Arkoudas, Ritu Chadha, and Jason Chiang. 2014. Sophisticated Access Control via SMT and Logical Frameworks. *ACM Trans. Inf. Syst. Secur.* 16, 4, Article 17 (April 2014), 31 pages. DOI:http://dx.doi.org/10.1145/2595222

Association for Computing Machinery. 1947. ”Welcome – Association for Computing Machinery”. http://www.acm.org/. (1947). ”Accessed: 2014-05-11”.

Leyla Bilge, Sevil Sen, Davide Balzarotti, Engin Kirda, and Christopher Kruegel. 2014. Exposure: A Passive DNS Analysis Service to Detect and Report Malicious Domains. *ACM Trans. Inf. Syst. Secur.* 16, 4, Article 14 (April 2014), 28 pages. DOI:http://dx.doi.org/10.1145/2584679

Yossi Gilad and Amir Herzberg. 2014. Off-Path TCP Injection Attacks. *ACM Trans. Inf. Syst. Secur.* 16, 4, Article 13 (April 2014), 32 pages. DOI:http://dx.doi.org/10.1145/2597173

TISSEC. 1998. Information for Authors. http://tissec.acm.org/content/process/information-for-authors/. (1998). ”Accessed: 2014-05-11”.

Transactions in Information and System Security. 1998. ”ACM :: Home”. http://tissec.acm.org/. (1998). ”Accessed: 2014-05-11”.

Received May 2014; revised May 2014; accepted May 2014