CS 856 Paper Reviews
W Anthony Young - 20161423
November 9, 2004

Paper Title: Secure Routing for Structured P2P Overlay Networks

Section I. Overview

A. Reader Interest

1. Which category describes this paper?

( ) Practice / Application / Case Study / Experience Report
(X) Research / Technology
( ) Survey / Tutorial / How-To

2. How relevant is this paper to the readers in the area? Please explain your rating under III. Detailed Comments.

( ) Very Relevant
(X) Relevant
( ) Interesting - but not very relevant
( ) Irrelevant

B. Content

1. Please explain how this paper advances this field of research and / or contributes something new to the literature. Please explain your answer under III. Detailed Comments.

2. Is the paper technically sound? Please explain your answer under III. Detailed Comments.

( ) Yes
(X) Appears to be - but didn't check completely
( ) Partially
( ) No

C. Presentation

1. Are the title, abstract, and keywords appropriate? Please explain your answer under III. Detailed Comments.

(X) Yes
( ) No

2. Does the paper contain sufficient and appropriate references? Please explain your answer under III. Detailed Comments.

(X) References are sufficient and appropriate
( ) Important references are missing; more references are needed
( ) Number of references are excessive

3. Does the introduction state the objectives of the paper in terms that encourage the reader to read on? Please explain your answer under III. Detailed Comments.

(X) Yes
( ) Could be improved
( ) No

4. How would you rate the organization of the paper? Is it focused? Is the length appropriate for the topic? Please explain your answer under III. Detailed Comments.

(X) Satisfactory
( ) Could be improved
( ) Poor

5. Please rate and comment on the readability of this paper.
Please explain your answer under III. Detailed Comments.

( ) Easy to read
(X) Readable - but requires some effort to understand
( ) Difficult to read and understand
( ) Unreadable

Section II. Summary and evaluation

A. Summary (provide here a summary of the paper)

This paper presents some methods of securing an overlay network from tampering by malicious hosts. The authors begin with a motivation for their work as well as a description of some DHT-based routing protocols. The system model that the authors assume is presented as well as reasons why the security protocols they are about to introduce are necessary.

The authors next discuss why node ID's must be distributed securely. This is mainly to avoid Sybil type attacks where attackers can control the routing table information in a joining node. The solution to this problem is to use a central certification authority to distribute node ID's. Two ways to bind ID's to physical nodes (by paying money or by binding to identities) are presented.

The discussion turns to secure maintenance of routing tables. In order to avoid two situations - faking proximity information and faking valid table update information - nodes maintain a second constrained routing table that is used if routing fails on the primary table. An outline of how the routing tables are formed is presented.

The final type of security offered by the authors' framework is secure message forwarding. Faulty nodes can route messages to the wrong place, pretend to be the destination node or drop messages altogether. The authors propose performing a failure test after routing a message to determine if the message was successfully sent to the proper node. If the test fails, the sender tries a redundant path. The use of self-certifying data to reduce overhead is discussed by the authors.

The paper concludes with a discussion of related work and some final thoughts.

B. Evaluation

Please rate the paper. Please explain your answer under III Detailed Comments.

( ) Award Quality
(X) Excellent
( ) Good
( ) Fair
( ) Poor

Section III. Detailed Comments

This paper presents a framework for a secure routing overlay. It is fairly well written. The sections are well organized, and not much overlap between sections was noted. However, some of your discussions were vague and required several readings to understand. Please be more clear and specific in the future. Missing keywords made this article difficult to index.

No extraneous references were provided. All sources were cited appropriately and a thorough explanation of the work was presented. This paper lays out a useful framework for future researchers to further develop a secure overlay. It appears technically sound (see comments below). However, some discussions were vague and not enough detail was provided to determine if the ideas are sound.

Some extra comments for the authors:

-You ignore dynamic IP hosts and hosts on NAT's citing a wish to model "traditional" peer networks. However, isn't the peer network of today traditionally using dynamic IP's and NAT's?

- Can attackers simply perform DoS attacks on the certificate servers to bring the network to its knees?

-Why are the methods of node ID assignment not suitable for small overlay networks?

Paper Title: The Sybil Attack

Section I. Overview

A. Reader Interest

1. Which category describes this paper?

(X) Practice / Application / Case Study / Experience Report
( ) Research / Technology
( ) Survey / Tutorial / How-To

2. How relevant is this paper to the readers in the area? Please explain your rating under III. Detailed Comments.

( ) Very Relevant
(X) Relevant
( ) Interesting - but not very relevant
( ) Irrelevant

B. Content

1. Please explain how this paper advances this field of research and / or contributes something new to the literature. Please explain your answer under III. Detailed Comments.

2. Is the paper technically sound? Please explain your answer under III. Detailed Comments.

( ) Yes
(X) Appears to be - but didn't check completely
( ) Partially
( ) No

C. Presentation

1. Are the title, abstract, and keywords appropriate? Please explain your answer under III. Detailed Comments.

(X) Yes
( ) No

2. Does the paper contain sufficient and appropriate references? Please explain your answer under III. Detailed Comments.

(X) References are sufficient and appropriate
( ) Important references are missing; more references are needed
( ) Number of references are excessive

3. Does the introduction state the objectives of the paper in terms that encourage the reader to read on? Please explain your answer under III. Detailed Comments.

(X) Yes
( ) Could be improved
( ) No

4. How would you rate the organization of the paper? Is it focused? Is the length appropriate for the topic? Please explain your answer under III. Detailed Comments.

(X) Satisfactory
( ) Could be improved
( ) Poor

5. Please rate and comment on the readability of this paper.
Please explain your answer under III. Detailed Comments.

( ) Easy to read
(X) Readable - but requires some effort to understand
( ) Difficult to read and understand
( ) Unreadable

Section II. Summary and evaluation

A. Summary (provide here a summary of the paper)

This paper presents the Sybil attack: a method of forging multiple identities for a single host in a distributed computing environment. The author begins with an introduction that motivates the problem and outlines the work to be completed.

Next the author presents the distributed computing model that is to be used for the remainder of the paper. This model is fairly standard in its connection of users to a communication cloud, etc. The author then makes several claims regarding the ability of users to create many false identities in a system, proving them with logical conclusions.

The authors present some related work and conclude with some summary comments.

B. Evaluation

Please rate the paper. Please explain your answer under III Detailed Comments.

( ) Award Quality
( ) Excellent
(X) Good
( ) Fair
( ) Poor

Section III. Detailed Comments

This paper describes the Sybil attack. Since this is the name of the attack, the title is appropriate. Also, the abstract gives a good introduction to the problem the authors are about to present. Keywords are missing and were hence not evaluated. The introduction motivated the problem and presented the work that will be discussed in terms that draw the reader into the paper.

This paper is relevant as it describes a method of attack that cannot be prevented using current system models and challenge activities. The contribution to the literature is unclear, other than challenging researchers to help solve the problem. This paper is fairly easy to read, although some of the proofs take some time to dissect and understand. The sections are well organized though, and the writing style is clear and easy to read.

Although the paper appears technically sound, I have one major question:

-You assume that all machines operate under similar resource constraints. Is this really an acceptable assumption? My at home is significantly faster and has much more RAM than my PC at school and work.