Konfidi: Trust Networks Using PGP and RDF

Andrew Schamp
Calvin College
3201 Burton SE
Grand Rapids, MI 49546
ams5@calvin.edu

Dave Brondsema
Calvin College
3201 Burton SE
Grand Rapids, MI 49546
dpb2@calvin.edu

ABSTRACT
We ought to write this last.

General Terms
source, sink, concatenation, aggregation

Keywords
Semantic Web, Trust Network, FOAF, RDF, PGP, reputation, propogation, distributed, inference, delegation, social, GPG

1. INTRODUCTION
We should write this second to last.

2. RELATED WORK
2.1 Representing Trust Relationships
There seems to be a general lack of psychological research on trust inference and representing trust relationships. In fact, most works in the fields of mathematics and computer science seem to adopt an arbitrary model appropriate to the algorithm under consideration. As Guha points out[3], there are compelling reasons for a trust representation scheme to express explicit distrust as well as trust.

Konfidi likewise has chosen a somewhat arbitrary model, but in designing the system we have made every effort to allow for adaptation to different models as research in this area develops.

2.2 Trust Networks and Inferences
There are a number of mathematical papers discussing a number of propagation strategies and algorithms for weighted, directed graphs[1]. For the most part, however, they are concerned with describing the networks mathematically, and did not have much in the way of practical application.

Jennifer Golbeck, at the University of Maryland, is doing graduate research on trust and reputation systems[2] that is similar to our work on this project. Like us, she uses an extension of FOAF to represent trust relationships and a rating system[3]. She has written a number of papers[4], and created TrustMail[5], an email client that uses the trust network that she is building. She is more concerned with the academic side of things, since this field is still growing rapidly, and less in the pragmatic side of things, as she prefers to help determine a good system of standards in the area.

2.3 The Semantic Web
In addition to Golbeck's work, a number of others have explored the usefulness and implications of expressing trust relationships in the Semantic Web.

2.3.1 Friend of a Friend (FOAF)
The FOAF project[6] is an RDF vocabulary used to represent personal data and interpersonal relationships for the Semantic Web. Users created RDF files describing Person objects which can specify name, email address, and so on, but more importantly, they can express relationships between Person objects.

2.3.2 FOAF Whitelisting
Dan Brickley has made a non-academic attempt to investigate the use of FOAF, particularly the mbox_sha1 property, to automatically generate email whitelists. By hashing the sender's address using SHA1, privacy is protected (and the address cannot be gathered by spiders), and so users can share whitelists of non-spam emailers. Then for all incoming mail, the sending address is hashed and the whitelist searched for the resulting value, and then is filtered accordingly. This use of FOAF is promising, but since it is localized, it is difficult for updates to propagate[7].

[1]See such-and-such, and so-and-so, for example

[2]See "Trust and Reputation in Web-based Social Networks" at http://trust.mindswap.org/

[3]Though both our ontologies and are ratings are different in significant ways, which we will address later.

[4]list of Golbeck papers here

[5]For more information about TrustMail, and to download a demonstration, visit the website at http://trust.mindswap.org/trustMail.shtml

[6]See http://www.foaf-project.org/ for more information about FOAF

[7]See http://www.w3.org/2001/12/rubyrdf/util/foafwhite/intro.html for more information about the whitelisting experiments

2.4 Email Filtering by Inferred Trust

Boykin and Roychowdhury discuss ways to infer relationships based on existing data (From:, To:, Cc: headers)[1]. This seems to work fairly well but there is often not enough data to make the spam/not-spam decision. They clearly state a cryptographic solution would be ideal.

2.4.1 Spam Filtering

Domain-level solutions, such as SPF and DomainKeys, are mostly to prevent phishing and also assume that a domain's administrator can control and monitor all its user's activities. Greylisting and blacklisting often have too many false positives and false negatives. User-level filtering, which dmail does, is not very common. Challenge-response to build a whitelist is tedious for sender and reciever and does not validate authenticity. Content-level testing is the most common, but bayesian filtering and other header checks are reactionary and must be continuously updated, and are becoming less effective as spammers create emails that look more and more real.

3. MOTIVATION

This project began as an exploration of whether we might use the PGP web-of-trust to filter email spam at the client's end. A mail client plugin would filter incoming mail, and check to see if there was a path from the sender to the recipient, in which the recipient had signed someone's key, who had signed another key, which eventually lead to the sender's key. If there was a path within a certain length, the message would be marked as trusted, if not, it would be marked as not trusted. This approach required that most users digitally sign email messages, and it depended on users to be aware of known spammers and keep from signing their keys. However, it soon became clear that the recommended PGP keysigning practices require only the careful verification of the key-holder's identity. Thus, any information about whether a user was trusted to send good email, and not spam, was information over and above the information expressed in the PGP web-of-trust itself, so any attempt to encode such information in the web-of-trust would be inadequate.

A more serious flaw in this thick-client approach is that, given the key-centric nature of the web-of-trust, paths between users can only be constructed from the sender backward to the recipient. When a key is retrieved from a keyserver, all of the signatures on that key are included with it, showing which keys have signed that key, and providing a number of possible links in a chain. However, using the existing keyserver infrastructure, there is no easy way to tell which other keys a particular key has signed. If these paths are built backward using a breadth-first search from the sender to the recipient, a spammer or other malicious user could generate a large number of fake keys that are inter-signed, and then use these keys to sign the sender's key. By adding this artificial information, the client's searching capabilities would be crippled, and the web-of-trust would be polluted with fabricated keys, users, and signatures. The PGP system of key-signing and verification was designed to be robust against this sort of impersonation, by requiring photo-identification and fingerprint exchange before any key-signing, but a deluge of false information would put undue strain on the keyserver infrastructure, and would amount to a denial-of-service, of sorts.

So, for our idea to be viable, it must first deal with these two issues, namely, representing trust information not directly in the PGP web-of-trust but rather in some other system closely coupled with it, and not being susceptible to denial-of-service attacks caused by generated false webs. We had other requirements, too. A system like this must be widely (even universally) adopted in order to be useful. As such, it must be easy for the technically unsavvy, like Aunt Sally, to use, while at the same time avoiding any diminished security stemming from being easy-to-use. It must also be available in any of the many widely-used email clients.

4. DESIGN

Say something here.

4.1 Representation

Our schema for representing trust data went through several iterations before stabilizing in its current form. It seemed that we had the choice of two general kinds of representations: one that used discrete values for varying levels of trust and returned a discrete binary (yes or no) answer, or one which used a (theoretically) continuous range of trust values and returned an answer within that range. Now, either kind of representation could be roughly mapped onto the other, however, we felt that a continuous range would allow more finely-grained control over the data. This had its advantages in setting up our test data, but it also took into consideration our thoughts about the way trust between people works.

4.1.1 Distrust

This is closely related to another important concern, that our representation give some account of distrust. If our trust network contained trust values ranging from neutral to complete, then everyone in the network is trusted, explicitly, or by inference on some level at or above this. If the system makes a trust inference between Alice and Bob at one level, but Alice really trusts Bob at a different level, she can explicitly state this previously implicit trust to have a more accurate result (for herself and for others who build inference paths of whom she is a member). But, suppose that Alice feels strong negative feelings about Bob. In this case, she would still only be able to represent this relationship as one of neutral trust. So, the trust network must account for distrust in some reasonable way.

One of the difficulties of using explicit distrust in an inference network, however, is that it is unclear how inferences should proceed once a link of distrust has been encountered. Suppose Alice distrusts Bob, and Bob distrusts Clara. As Guha points out[3], there are at least two interpretations of this situation. On the one hand, Alice might think something like "the enemy of my enemy is my friend" and so decide to put trust in Clara. On the other hand, she might realize that if someone as scheming as Bob distrusts Clara, then Clara must really be an unreliable character, and so decide to distrust Clara. Further, suppose Bob expressed trust for Dave. At first consideration, it might seem reasonable to simply distrust everyone that Bob distrusts, including Dave. But suppose there were another path through

different nodes indicating some minimal level of trust for Dave. Which path should be chosen as one which provides the correct inference?

One solution to this problem is simply to traverse one link of distrust, and then record that distrust and stop, seeking an alternate path. To overcome the problem of chosing the correct path for the inference, some kind of weighted average can be taken of all of the paths between Alice and Dave, thereby producing an answer according to whether the majority of people in the neighborhood Dave trust him or not.

We explored a method similar to this one, but in the absence of sufficient psychological research affirming a model of this type, we sought a simpler solution. In the end, we decided on a model that corresponds to another intuition about how trust works between people, that it is more of a continuum of both trust and distrust than a measure of just one or the other. For example, if Alice trusts Bob at some moderate level (say, .75 of a scale of 0 to 1), then it seems that she also *distrusts* him at some minimal level (say, .25). If Alice trusts Bob neutrally, then she trusts him about as much as she distrusts him. If she distrusts him completely, then she doesn't trust him at all. But in all of these cases, there is a trade-off between trust and distrust. Only in the extremes is either of them eliminated completely. So, we decided that our trust model should represent a range of values from 0 to 1, treating 0 as complete distrust, 1 as complete trust, and 0.5 as neutral, and calculate trust inferences accordingly[8].

4.1.2 Trust Topics

We thought that if other attributes about a trust relationship could be expressed, in addition to the rating system, then a system like Konfidi would be useful in many wider scopes than email spam prevention. The most important of these is the trust topic, or in other words, what the trust is about. A natural feature of interpersonal trust relationships is that there can be many different aspects of the same trust relationship.

(you can make an Alice-Bob-Clara-Dave diagram for this business)

For example, suppose Bob is a master chef, but is terribly gullible about the weather forecast. Alice, of course, knows this, and so wants to express that she trusts Bob very highly when he gives advice for making souffle, but she does not trust him at all when he volunteers information about the likelihood of the next tornado. Suppose she only knows Bob in these two capacities. Any trust inference system should not average the two trust values and get a somewhat neutral rating for Bob, for that would lose important information about each of those two trust ratings[9].

Suppose also that, given only the above trust ratings, the system tried to make an inference on a subject that was not specified. Perhaps Alice has some general level of trust for Bob that should be used when there is no specific rating for the topic in question. See the discussion in Future Work for our proposal for a system of topics that might account for this situation.

4.1.3 Rating System

With these considerations in mind, we decided that a relationship-based system would meet our needs while avoiding some of the disadvantages of other representations. According to this system, each trust relationship is an object, and the trusting party and the trusted party are specified as such[10]. Trust relationships are related to objects representing trust items. Each of these items has a topic and a rating associated with that topic. Each rating is on a scale from 0 to 1 inclusive, with 0 representing complete distrust, 1 representing complete trust, and 0.5 representing neutral.

Because the trust relationship is represented as its own object, other attributes may be added later, such as the dates the relationship began, annotations, etc. as the need arises.

4.2 Infrastructure

As Konfidi developed, it seemed that two important but separate components were needed to fulfill the two major needs of our project. First, we needed a way to store data specifying trust relationships. Second, we needed a way to represent the network specified in the data, and traverse it to calculate trust values[11]

4.2.1 Data Management

One need was for a system to store trust network data, verify signatures on that data, and allow for updates of existing files and their signatures.

If Konfidi were to be useful as a system of trust management, then the operations it performs and the results it returns must be trusted by the users. Thus, to prevent malicious users from submitting faulty or incorrect trust data for others, Konfidi will require every file submitted to be digitally signed by the key of the user who is indicated as the trusting party. Konfidi will then verify the signature before accepting the data as legitimate and passing it along to the trust management system.

4.2.2 Trust Management

This part of the design is the core element of Konfidi. Storing and managing the data would not be of much use in this context unless we did something with it. So, this part would handle requests for trust ratings, traverse the internal representation to find a path, and provide a response.

We should say more about this. Why did we choose the design we did? I can barely remember...

5. IMPLEMENTATION

put a shiny diagram in here

5.1 OWL Schema

Explain OWL, RDF, and how it fits into FOAF as needed.

[8]This also makes many propagation algorithms simpler, as we'll discuss later.

[9]In fact, it would lose the only information that made these ratings useful in the first place.

[10]Thus, each relationship is one-way, but since the truster is responsible for the accuracy of the information, that is fine.

[11]should we leave the FOAF stuff to "implementation", and just discuss "data" here? I think so.

5.2 FOAF Server

URI based lookup

communications with trust server

5.3 Trust Server

5.3.1 Frontend

generic interface

short introduction about coupling for the following subsections reasons for it (scalability)

5.3.2 Trust Backend

this does the dirty work

bit about the different strategies

5.3.3 PGP Backend

bit about the importance of verifying a PGP link (identity is good)

6. FUTURE WORK

6.1 Psychological Research

6.2 Additional Features

multipart signing of the results query, and signature checking between components

6.3 Other Clients

6.3.1 Firefox + Mime

6.3.2 MTA Integration

6.4 Topic Hierarchy

7. OTHER ISSUES

7.1 Anonymity

Since authentication is a key part of Konfidi, it is effectively impossible to act anonymously within the system. To enter the PGP web of trust you must prove your identity to someone. Political and religious discussions (especially in intolerant countries), corporate whistleblowing, crisis hotlines, and other sensitive discussions have grave reasons to be conducted anonymously. If authentication becomes a defacto standard of communication it will be difficult to conduct these communications. Two potential alleviations would be to 1) have policies regarding when documents will be signed and when they won't (e.g. banks will always sign) and 2) using an anonymizing proxy service that is trusted by most people. There are obvious drawbacks to both of these.[2]

7.2 Privacy

Should there be any? How will it be controlled? Encrypted FOAFs.

7.3 Ethics

Dependency on a trust system, trust in the system, etc.

8. CONCLUSIONS

9. ACKNOWLEDGMENTS

We would like to thank the following people: Jim Laing for assisting with test data, Prof. Vander Linden for advising us on this project, Profs. Fife, Frens and Plantinga for their advice on specific matters.

10. REFERENCES

[1] P. O. Boykin and V. Roychowdhury. Personal email networks: An effective anti-spam tool, 2004.

[2] J. Fenton. Distinctions between message authentication and user authentication. 2005.

[3] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Propagation of trust and distrust, 2004.