1. Introduction

The spam problem is extremely widespread, and is not merely confined to the problem of junk mail, but is symptomatic of cumulative problems with the underlying e-mail infrastructure. The current system for e-mail fails to allow for reliable tracking of e-mail messages from receiver to source, and accurate correlation between real and virtual identity (i.e. real names and aliases). These weaknesses allow spam and several types of more malicious e-mail to be pervasive. It makes it much easier to introduce worms, viruses and junk e-mail into the system without fear of consequences.

Existing proposals for solutions fail to provide a way of making Spammers accountable for their actions. Spammers frequently evade costs by signing up for an account, failing to pay their early bills and spamming, meanwhile the account is cancelled and the company loses the money from the access as well, existing filter based approaches in the market fail to do anything about the Spam they have found. What appears to be necessary is a way of providing both privacy and accountability in the current email system.

This paper will introduce a potential means for industry-wide note comparisons on spammers and other untrustworthy e-mailers. As part of the system I have assumed the existence of a Public Key Infrastructure, the details of which will be discussed in Section 3. By allowing ISP’s and law-enforcement certain information about a users past
history with e-mail, we can prevent the high-turnover, anonymous mass-emailing that occurs so frequently on the internet today, and thereby take control of our e-mail and our networks.

1.1. Motivation

From a legal perspective, currently the burden is almost entirely on law enforcement systems to bring spammers to justice, and thus far they have indicated that the tools for spam-law enforcement do not presently exist (FTC, 2004). The Can Spam Act provides for penalties for spam of up to $11,000 (FTC, 2004), but it seems entirely possible that providing the documentation to law enforcement of the abuses of a single spammer could easily cost a company $11,000. It seems equally likely that it could easily cost the taxpayer more than this for a complete investigation.

From an economic perspective the $11,000 maximum fine pales in comparison to the estimates of the cost of spam. The University of Indiana spent $1.2 million on its e-mail system in 2000, but they will have to upgrade in 2004 at a cost of around $300,000 because of increases in e-mail volume (Hansell, 2003). Apparently almost 45% of each day’s 3 million e-mail is spam. Ferris Research estimates the cost was nearly $10 billion in the United States in 2003, while The Radicati Group estimates the worldwide cost may be as high as $20.5 billion (Hansell, 2003).

According to IDC, the number of e-mail mailboxes is expected to increase 138%, reaching 1.2 billion by 2005. (Online Publishing News, 2001). SpamCop, one of the largest spam reporting services logged 412 million spam emails in the past year (SpamCop.net, Inc., 2004b). It is unclear as to how well this represents the total Spam problem as it is based only on reports of Spam received by individuals registering for
their free service. It appears that e-mail usage is growing, and the Spam problem is unlikely to go away on its own.

2. Related Works

2.1. Public Key Infrastructure

There have been volumes written and done about Public Key Infrastructure (PKI), and the details are mostly beyond the scope of this paper. In brief, PKI works as follows. A key-pair is generated of two keys A & B, such that only A can decrypt what B has encrypted and B can decrypt what A has encrypted. The relationship allows for a public key system. One of the keys (arbitrarily the private key) is kept secret, in this case A, and the other one is made publicly available. In order to send a private message to the holder of the key pair, a user on the internet can sign the message with the public key (B), which can then only be decrypted with the private key (A).

In order to send someone an encrypted message, you only need their public key, while reading encrypted messages requires the appropriate private key. The private key can additionally be encrypted or stored on smart media, etc. for security. If you wish to digitally sign the message as well, you can encrypt it also with your own private key, or add a signature based on a hashed and encrypted version of the message, so the message is readable even if the signature verification isn't part of the e-mail client.

For further explanations of the workings of PKI, David Henry (Henry, 1999), and Trevor Perrin (Perrin, 2003) have written considerably about them. Later we shall assume that every ISP is capable and has been given the legal authority to assign a uniquely identifiable certificate for use in something similar to existing S/MIME e-mail systems.
2.1.2. Anonymity and Accountability in Self-Organizing Communities

Additionally much work has been done on Anonymity and Accountability in Self-Organizing Communities (A2S0C) (Farkas, 2002), from which many concepts have proven useful, except that in most cases the paradigm presented in this paper is not self-organizing, but rather is based on the current decentralized independently organized system more common in the existing e-mail system. Most important of the concepts of A2S0C used herein is the concept of Layered Accountability, which describes 2 layers on which users can be held accountable.

The lowest layer, Layer 2, allows for accountability within the community. It allows for checking of various access and control rights that should be granted to a certain real user associated with a virtual identity. It would also prevent, for example, a new virtual identity from gaining access to things which the Real Identity has lost access to, by way of linking all the virtual identities together. It prevents the user from creating a new virtual identity independent of their existing virtual identities, without anyone in the community having access to their real identity.

Layer 2 provides virtual identity, i.e. it can determine if virtual user 1 and virtual user 5 belong to the same person. Basically they are all linked back to a root virtual identity, which is separate from the real identity and is not directly associated with the real identity within Layer 2.

Layer 1 maintains external accountability. It would be necessary in the case of law enforcement action or illegal behavior. The Self-Organizing Community component involves a system of checks and balances that allow for the system to not be totally trusted. By encrypting the Layer 1 associations with multiple keys, this system allows for
robustness and security even if the Trusted Computing Base (TCB) which maintains the Layer 1 associations is compromised. Within an organization the same general framework can be applied to a user credentialing system, only the business will likely set its own policy for the selection of the individuals with the authority to access the information contained in Layer 1.

3. Assumptions

Many assumptions have been made in the development of this framework. Among the assumptions is a fully operational PKI e-mail system. It appears natural that PKI be used for the purpose of assurance of a unique and accountable identity. The mathematics and the cryptography have been developed to full maturity; it only lacks a viable implementation and cost/benefit structure. I feel that analysis of the cost vs. benefit is rapidly approaching the critical mass at which spam and other e-mail nuisances will make it necessary for the introduction of a PKI.

I have assumed that all ISP’s and private organizations choosing to participate in this particular e-mail system have issued identity-validating certificates, based on whatever account information the ISP obtained in order to establish the account, i.e. some sort of national identifier. Additionally, I assume a functional Certificate Revocation List System (CRL).

By providing for this assurance, and minimally guaranteeing that every e-mail is sent by an authorized user (i.e. encrypted private keys and/or smart cards or smart chips), we are given a number of options that have led me to believe that something similar to, but more restricted than, the Credit Reporting Bureaus is appropriate for the e-mail system.
4. Framework

In the PKI environment we have so carefully chosen, the first step an ISP and/or organization (from here on referred to simply as ISP) would have to take would be to verify that no customer had any outstanding Spam complaints against them before issuing any certificates and a corresponding e-mail account. An E-mail Credibility Authority would generate credentials in a process not unlike the way in which a bank decides whether to risk making a loan to an individual.

In order to handle complaints under this PKI system each ISP would have to establish complaint thresholds and a complaint logging system, both of which could easily be automated up to a point. It might be reasonable to implement two thresholds, or a rate-based threshold. If distinct complaints are increasing faster than some reasonable rate, i.e. exponentially then immediate suspension might be reasonable, or once distinct complaints reached some arbitrarily high number above the human involvement threshold. Once the first threshold of complaints has been reached I would suspect that human involvement would become necessary, as in any judiciary process there needs to be some sort of verification of the charges before proceeding. If the complaints were indeed valid, or the rate or secondary complaint limit had been reached - the certificates would of course be invalidated immediately.

As per their customer agreement, the company should be allowed to report minor credibility violations to the ECA of their choice. This ECA would function as a mediator between the FTC and the ISP and an aggregator of blacklists through a public CRL.

Instead of relying on the ISP itself to cancel the account and the certificate, both the ECA and the ISP would record the certificate on their CRL’s and the ECA would
confidentially be transferred the Layer 1 data associated with the certificate. The ECA could then report their most significant violators (those with the most aggregated, distinct complaints) to the FTC.

As a customer service the ISPs must propagate the CRL’s. This is a difficulty inherent in most certificate-based authentication systems, and is marginally out of the scope of this paper. However, it seems possible that a distributed system, where each ISP maintained its own CRL could be possible. By using the forthcoming E-mail Sender ID technology proposed (Microsoft, 2004) a solution might be possible. Sender ill allows DNS records to contain lists of authorized hosts allowed to transmit e-mails by IP address. IP Spoofing aside, the SMTP server could be modified to only allow the transmission of emails with currently valid certificates (i.e. ones neither expired nor on any local CRL). Higher security could be maintained by the client checking either or both of the CRL’s at the ISP or the ECA.

Additionally when a complaint is received either from an ISP or the ECA, the FTC or whomever the ECA’s have decided to entrust the keys with can provide the keys necessary to unlock the Layer 1 real identities and report them to the authorities. Once legal action has been taken against someone it seems likely that most ISP’s would choose to permanently black list the Layer 1 identities from using e-mail, to prevent themselves from being mired in ill-repute.

5. Practical Evaluation

5.1. Economic & Legal Evaluation

As liability becomes an increasing concern to the ISP this sort of "Credibility" check could becomes critical. It would also serve to prevent Spam law violators from
obtaining new accounts, as they will have to find new employees to register accounts
under, and eventually the supply of people willing to have their credibility tarnished
seems likely to diminish, especially as the use of electronic communication becomes
increasingly important to commerce.

Because of the massiveness of the current system, I have chosen the Credit
Reporting Agency as a model for credentialing e-mail accounts. The four major CRA's
keep records on virtually every person in America with a financial life. There are
frequently discrepancies between the four agencies, but obviously the FTC would be able
to exhume whatever they needed once the got a complaint about a major e-mail abuser.
Additionally, just like with credit, allowing e-mail and computer system access can be a
security risk. Part of assessing risk is gaining knowledge for the purpose of assigning
trust. An E-mail Credibility Authority would provide a semi-private record of what are
essentially credibility errors, much like credit reports provide potential creditors with
"potential risk" information. By allowing ISP's to check for previous spamming, fraud
or other illegal activities relevant to allowing e-mail access they can determine whether
or not to issue a new account, with less concern about lawsuits.

5.2. End-User & Implementation Evaluation

It would likely be best for most all of this system to be completely transparent to
the end user. That is certainly no small goal, even given the assumptions made earlier
there are many issues related to this which have yet to be investigated (see section 6).
There are many systems for Key management and distribution, which are all beyond the
scope of this document. It seems possible for them to be integrated into existing e-mail
clients such that the only noticeable difference will be whatever time is lost to the process
of encrypting the information and generating the keys, and these losses are likely to be both inevitable and insignificant and computing power continues to grow.

From a system administrator's perspective, many commercial ISP's already have significant staff being devoted to Spam. If successful, perhaps fewer people will be needed solely to address the Spam problem as the economic and legal costs to the spammer increase, and instead they can focus on e-mail security rather than being overwhelmed with garbage collection.

6. Future Work

There are already many illegal uses of Social Security Numbers and other personal identifiers, however, in particular the Credit Reporting Agencies all make ready uses of it. There are legal and privacy concerns which are beyond the scope of this paper, but which merit solutions. Additionally, it seems that separating identity into Layers as suggested previously (Farkas 2002) is an adequate way to address many privacy concerns.

Internationally, PKI will be very challenging to implement, even domestically it will not be easy. Establishing trust between international certification authorities, particularly in countries without Spam regulations has the potential to disrupt considerable commerce and trade activities if not properly handled. The assumptions made will probably require at least as much work if not more work to implement than the framework I have attempted to layout.

I think it should be noted that except for actual evidence of computer crimes that care must be taken that type of system should not be used in any way for documenting personal e-mail or intruding on individual privacy, but to make the international e-mail
infrastructure safer and more secure. The system does have the potential for abuses and therefore, like the Credit Reporting Agencies, it must also have a system for arbitration and dispute resolution. Like credit, e-mail and internet access is becoming economically important to our domestic infrastructure, and excluding people because of unfairly made accusations could be dangerous and ethically serious.

7. Acknowledgements

This research was made possible by a NSF Grant and the resources of the NSF REU Program at the University of South Carolina, Columbia, SC.