Subject: [ASIACCS 2012] Paper #163 "Adaptive Semi-Private Email Aliases"
From: asiaccs-pcchairs@cs.unc.edu
Date: 2/23/2012 6:56 PM
To: Beng Heng Ng <bengheng@eecs.umich.edu>

Dear Beng Heng Ng,

We are happy to report that your submission,

  Adaptive Semi-Private Email Aliases

has been accepted as a FULL PAPER for presentation at ASIACCS 2012. This is a significant accomplishment, since only roughly 30% of submissions were accepted in either full or short form.

The reviews for your paper are appended below. Please take the reviewers' concerns into account in preparing your final version. You will receive instructions in the near future for preparing your final version, but in the meantime, please do not hesitate to let us know if you have any questions.

- ASIACCS PC Co-Chairs

==========

ASIACCS 2012 Review #163A
Updated Friday 13 Jan 2012 8:56:13pm EST

Paper #163: Adaptive Semi-Private Email Aliases

Overall merit: 6. Accept
Reviewer expertise: 3. Knowledgeable

===== Paper summary =====

This paper presents a new system, called SEAL, to generate email aliases to mitigate the email-address leakage and spam problem. SEAL works as a separate service layer, augmenting traditional email servers by managing aliases (creation, state change, and demolition) and resolving address mappings (from temporary to permanent addresses). The authors implemented a prototype system and used it for students in a class to communicate with an online forum.

===== Comments for author =====

Overall, this is a cute paper and I enjoyed reading it. The ideas are not completely new, with some of they rooted from several previous work. However, the authors add interesting twists to make the new system more usable and practical than previous ones. Although the paper does not solve all usage issues, e.g., the easiness for others to memorize addresses and the abuse by spammers, I imagine it is still quite useful for many purposes. Personally, I would like to try out their system.

Strengths:

-An interesting paper and well written
-Ideas quite simple, but very practical
-A complete, real system built, used already, with reasonable evaluations

Weaknesses:

-There are two usage issues with deployment.

The first issue is remembering and distributing email aliases to friends, colleagues, or families to use. The use of long, hash generated aliases prevents others from using those to initiate email conversations to you, other than using them for reply. For example, if I have such aliases, I may not even want to distribute them to known friends since they are unlikely to type those. Maybe this is not the type of scenarios that the authors want to address. The email aliases are perhaps mostly useful for being distributed for unimportant purposes such as forum posting or newsletter sign up etc. For this reason, the major difference between this work and previous is that this work allows a flexible time range for an alias to expire, instead of imposing on a fixed expiration date.

The second issue is the abuse by spammer accounts. It is true that spammers will still need to register an account to send emails, but with a lot of aliases, they could conveniently change to new email addresses if the old ones are blocked or blacklisted (without the cost of registering new accounts).

Other comments:

I would like to see more evaluation results based on real deployment and measurement. The paper reported some results regarding which site leaked user emails based on their system, which I find quite interesting. It would be nice to see more deep investigation in this direction vs. the benefit of using the system over longer period of time.

SEAL does require secure SMTP connections and how widely is this supported in practice now? Please clarify.

What's the overhead of alias translation in email latency? How many concurrent aliases can a user have?

What's the impact of CAPTCHA, and if a CAPTCHA is sent to a legitimate user, do they bother to really solve it and retry again?

==========

ASIACCS 2012 Review #163B
Updated Monday 16 Jan 2012 1:32:09pm EST

Paper #163: Adaptive Semi-Private Email Aliases

Overall merit: 4. Borderline
Reviewer expertise: 2. Some familiarity

===== Paper summary =====

The paper covers a hard subject, how to thwart spam while still retaining some usability. The authors have added valuable contributions to this subject.

===== Comments for author =====

This system requires the recipient to initiate the lifecycle changes for the keys and to identify the spam. You should think of ways of hiding this or making this interaction more automatic. Maybe coloring the email for several days and if it is not "uncolored" it is spam and the state should change? Maybe the random bit of the email address can be hidden in the headers somehow? Is it possible to guess the private address from the public address, particularly since this is affiliation preserving? What about multiple seal services that don't coordinate? Do mutual users that are trusted have to do anything?

Since my private email address is sometimes in the body of email, there can be inadvertent spillage of the private email address and then bets are all off and the system has failed that address.

Bottom line, anti-spam is good enough for most people with little or no effort on their part. People that can add additional authentication in a standard way, can get their spam score lowered, again without compromising the receiver's experience.

==========

ASIACCS 2012 Review #163C
Updated Thursday 9 Feb 2012 4:17:39pm EST

Paper #163: Adaptive Semi-Private Email Aliases

Overall merit: 4. Borderline
Reviewer expertise: 2. Some familiarity

===== Paper summary =====

The paper propose a scheme of email alias with access control policies. Users can control an email alias is unrestricted, partly restricted, fully restricted or disable. By using email alias, users can reduce the propagation of the email address and thus reduce the spam.

===== Comments for author =====

The paper propose an interesting scheme of email alias which can control the email address propagation and also authenticate the users' organization. The seems to be a reasonable approach. The evaluation results show the system developed under the aforementioned design works quite well.

For human senders, the major concern is that although the email alias is easy for its owner to use, but hard for the senders to maintain, because they might need to keep update the alias according its life cycle. There are quite a bit extra work for the sender to make sure the alias they actively use has not been disabled by its owner yet. They have to keep up to date to the latest alias if the owner keep changing the alias.

For the automated sender, it is not fully clear (partially admitted by the authors) that what type of changes they can make. It is quite common that they might need to update the source email addresses. It is also not clear to the reviewer that, whether the owner of an alias can extend its expiration date, etc so that they can keep trusting the automated sender.