ESPC
Email Sender & Provider Coalition

Home About ESPC Members Press Room Project Lumos Resources Contact Us

Response to Project "Lumos: A Solutions Blueprint for Solving the Spam Problem by Establishing Volume Email Sender Accountability"

With the announcement of the white paper, "Project Lumos: A Solutions Blueprint for Solving the Spam Problem by Establishing Volume Email Sender Accountability", the ESPC solicited industry feedback regarding the proposed architecture and its' implementation.

By and large, as reflected in the extensive media of Project Lumos, we received comments in support of authentication and reputation systems. The ESPC would like to thank all the individuals who provided their comments and recommendations. The following is a summary of the feedback we received specific to Project Lumos, and our subsequent responses.

As a point of clarification, Project Lumos uses the term "ESP" or "email service provider" to indicate an operator of the mail server whether it is the corporate IT department, a small independent domain with its own mail server, or an email service provider that delivers on behalf of a client base.

1. **Can you clarify the basis for "identity"? There are references to both IP address and certificate verification. Where certificate verification is used, what is being verified?**

   The concept of "identity" in Project Lumos is used to describe the verified and unique identification of a person, commercial organization, or non-commercial organization. A real world example of identity certification for an individual is a passport. For a business, identity could be certified with a tax ID. We see the use of IP as a first step - short-term solution - for verification.

   The Project Lumos Road Map offers a more detailed description of the evolution of the certification process. Within the Project Lumos solution, the attribute that is verified is the hash. The authenticity of the content and the origin of the message are verified by hashing the entire message and signing the hash.

2. **How will Project Lumos limit the ability of spammers who use many accounts to send small volumes of spam from each account?**

   Project Lumos does not consider an email account a viable source of identity. A cornerstone of Project Lumos is the link between identity and reputation; even anonymous users have a reputation. So you can send small volumes of spam, but it is still spam based on the reputation associated with the identity sending the email.

   If the security system were breached by an entity with a low grade identity for the purpose of gaining access to many accounts, the identity would last for a short period of time, and would not be sustainable. Further, the economics of performing the steps required to continue to obtain multiple low grade identities is economically prohibitive.

3. **How will Project Lumos limit the impact of Trojaned machines?**

   While the focus of Project Lumos is not the security of machines, Project Lumos creates significant obstacles that do not exist today for preventing illicit activity like accessing machines for the purpose of spreading viruses and sending spam.

Currently, almost any machine can become a Trojan mail server. Many owners of Trojaned machines have no idea that their machine is configured to send mail, let alone that it is doing it. Within the Project Lumos structure, the only machines that can become Trojan mail servers are machines that were set up by their owners to be mail servers with a secure identity. This greatly reduces the number of available Trojans, and increases the difficulty in creating a Trojan. The infiltrator must now not only find a machine, but also find its identity and the identity of a sender.

Since operating a Trojan involves stealing an identity, the reputation associated with that identity will rapidly render the identity useless. Though the registries will operate a dispute resolution process to repair the identities of the owners of Trojaned machines.

And finally, the identity will make it much simpler for law enforcement and others to find the Trojaned machines and investigate the circumstances that led to the security breach.

4. **Comment on the following: Project Lumos allows for email gateways to process incoming mail based on the level of security of the senders certification. Consequently, there is the potential for the "slippery slope" with regards to correlating the size of an organization to the trustworthiness of their message.**

   The Sender Classification is only valuable if the sender is new to the registry, or has not yet been rated by the registry. In this situation, recipients will more than likely set their expectation of the sender performance based on the sender classification. Section 4.2.1.1 provides a more detailed description of Certified Sender Classifications.

   However, once the sender establishes a performance rating, the sender's classification becomes fairly irrelevant. The sender's reputation becomes the relevant measure. So, a Class A sender classification and a low performance rating is not as valuable as Class C sender classification with a high performance rating.

   Additionally, if the smaller sender uses an email service provider with a good performance rating, the smaller sender benefits from the reputation of the email service provider in establishing their own, independent reputation.

5. **How could Project Lumos incorporate a category for messages with consent in the form of stamps?**

   The categories for consent are proposed categories and are extensible to include stamps. We will incorporate additional categories based on what is relevant for the industry.

6. **Can existing complaint based systems be used in developing an early reputation system?**

   Yes. Existing systems could be used to create a preliminary reputation system. This could easily be incorporated in Phase I, and is an excellent suggestion.

   Use of these systems does not necessarily rule out the need for a registry though. A registry could perform the role of the aggregator of existing systems' information.

7. **Is it necessary to have an identity separate from the IP address?**

Yes. Small senders and small businesses do not have their own IP address, and many of them send email through multiple ESPs.

The individual sender's reputation is more important that the ESP's reputation.

8. **Comment on the following: If Project Lumos adopted a proof of individual consent, the problem of having only one metric to describe all behavior of a sender would be lessened.**

   Without identity, it is impossible to know who has consented to what.

   Project Lumos addresses the concept of a Mail Categorization in section 4.2.2.2 Table 3. Rather than attempt to define consent, Project Lumos provides a foundation to define the sender and the type of message. Thereby, the receiving mail gateway can make an improved decision about delivery of the email message.

   Also, Project Lumos is extensible. So, once identity and reputation systems are in place, it is possible to build a consent system as well.

9. **Comment on the following: Small volume and individual email senders could have their emails labeled and certified by the outbound email provider or ISP. This would also alleviate the need for updating the very large number of email clients.**

   This is exactly our intention. You are describing an anonymous or small sender using an ESP.

10. **Comment on the following: In addition to, or rather than using the proposed Email Content Assertions, include an optional mechanism whereby the sender can make an additional assertion about the content or intent f the email. Where possible, Project Lumos and TEOS should aggress on the labeling mechanism.**

    The Content Labeling component of Project Lumos could be enriched to include additional information. We are reviewing complimentary proposals and systems.

Privacy Policy

©2003-2014 Email Sender and Provider Coalition. All Rights Reserved.