Correo basura, fraude, autenticación y privacidad

Traducción de Textos

Curso 2007/2008

Versión	Cambio
1.0RC	Revisión de todo el texto
0.9	Traducido el noveno párrafo
0.8	Traducido el octavo párrafo

Autor:

Rubén Paje del Pino

i010238

Índice de contenido

1. Primer párrafo (12-XI-07)

No es nuevo para la mayoría de lectores que el correo electrónico se está volviendo inmanejable. Por un lado tenemos los correos comerciales no solicitados (spam) que venden una variedad de productos dudosos, que abarca desde farmacéuticos a cuentas de banco abandonadas. Por otro lado tenemos a los llamados "phisers" que intentan robar nombres de usuarios y sus contraseñas para hacer transacciones bancarias por Internet. Y finalmente tenemos a los virus, gusanos y demás software nocivo. Aunque existen posibles soluciones para esos problemas, algunas de estos tiene un potencial para hacer más daño que otra cosa.

2. Segundo párrafo (12-XI-07)

Un método sencillo para luchar contra el correo basura es idear algún método para poder autenticar al remitente o bien saber quien envió realmente el correo, podríamos saber que hacer con él, aceptarlo si conocemos quien lo envía o bien – si es correo basura- podemos identificar a quien quiera que lo enviara y podemos atacarle a él mediante acciones judiciales. Es algo que puede parecer sencillo pero no funciona por numerosas razones. Fundamentalmente la mayoría de la gente acepta – y quieren aceptar – que el correo electrónico de más o menos cualquiera. Justo mientras escribo esta columna, recibí no menos de 5 correos legítimos escritos directamente a mi, desde nuevos remitentes. No tiene sentido cierta seguridad sobre identificación de alguien desconocido si de cualquier manear estás dispuesto a aceptar el correo que nos envían. Esencialmente identificar es solo un concepto que le afecta un contexto compartido – sinque este autentique la identidad del remitente, como oposición a la única identificación del remitente, que dice muy poco.

3. Tercer párrafo (13-XI-07)

Los remitentes de dichos correos basura pueden autenticarse también. Hasta hoy pueden comprar muy barato dominios, en un hipotético mundo de correos autenticados ellos comprarían por muy poco identidades autenticadas. De hecho, una evidencia anecdótica sugiere que los remitentes de los correos basura han sido los más rápidos en adaptarse al prototipo de la autenticación en los correos autenticados. Nosotros así nos encontramos con la siguiente paradoja: ¡si utilizamos dicha técnica contra el correo basura, estadísticamente somos como los que lo realizan"

4. Cuarto párrafo (13-XI-07)

A parte de eso, se recuerda que mucho correo basura tiene su origen en máquinas pirateadas. Alguien que "tiene tu máquina puede robar tu identidad electrónica con bastante facilidad, incluyendo (por supuesto) cualquier llave criptográfica que posea.

5. Quinto párrafo (13-XI-07)

Si las técnicas de autenticación no funcionan contra el correo basura, ¿nos ayudarán a

protegernos de el fraude? Aquí , al menos, hay una razón para ser optimistas: un ataque de fraude es un intento de imitar, si podemos autenticar realmente al remitente de el correo, ¿pudiéramos no estar seguros?

6. Sexto párrafo (13-XI-07)

Desafortunadamente, el propósito de las técnicas de autenticación del correo no resolverán el problema. Lo que querría realmente es probar que "este es el interesado a quien doy mi dinero", todo este método permite establecer que el remitente posea un nombre de dominio verosímil. Esto no indica nada sobre tus relaciones anteriores. Este ataque ya ha ocurrido no es imaginación, ya que uno de los primerísimos ataques de fraude eran correos que parecía que los enviaba paypal.com aunque desde el dominio deal paypa1.com

7. Séptimo párrafo (13-XI-07)

Pensemos en otra estrategia en la cual, cuando se abra una cuenta, el banco le envía una copia de su certificado. De hecho, este certificado podría ser usado para autenticar cualquier correo del banco. Observe esta diferencia crucial: un certificado está sujeto a una transacción previa, en vez de a un nombre.

8. Octavo párrafo (13-XI-07)

El correo autenticado puede resolver algunos problemas; como mínimo, dificulta que los gusanos se extiendan a través del correo, ya que la máquina afectada será claramente identificada. Además, hay algunas situaciones en las que se utiliza una lista de remitentes conocidos. En una de las estrategias que son mejores la supuesta identidad se utiliza para activar algún tipo de mecanismo desafío-respuesta. Los mails con algún tipo de desafío nos darán una cierta protección en este caso, aún cuando sin él los "jue jobs" con éxito – las suplantaciones de las legítimas identidades de los usuarios – son relativamente infrecuentes. Los remitentes del correo basura podrían tener seleccionado pares de direcciones de origen-destino para evitar las listas de remitentes que están permitidos.

9. Noveno párrafo (19-XI-07)

Sin embargo, existen algunas graves desventajas, siendo algunas logísticas con algunos de los presupuestos, los servicios de redireccionado de correos de entrada como acm.org no funcionará correctamente, las personas que estarían enviando correos desde cualquier lugar que afirmara ser de acm.org. Otras propuestas plantean problemas con las listas de correo, tal como son las que añade información administrativa a los correos de salida.

10. Décimo párrafo (18-XI-07)

Pero el problema más importante es el de la privacidad. Si en la práctica todos los correos

tienen que estar firmados, entonces estos son fáciles de controlar (algunos proyectos anti-spam de pago tienen el mismo problema). El tribunal supremo de los Estados Unidos ha recordado de que "los panfletos, los folletos e incluso los libros anónimos han jugado un papel importante en el progreso de la humanidad. En distintas épocas de la historia los grupos y las sectas perseguidas han prohibido criticar las prácticas y las leyes opresivas anónimamente. Es evidente que el anonimato algunas veces ha sido utilizado con los fines claramente muy positivos". ¿Queremos por tanto un mundo electrónico sin tales ventajas?