Certificados y Propuesta de Voto y firma anónimos

René Mérou

17 de septiembre de 2002

Guión comentado de la ponencia dada el domingo a primera hora en la NcN.

Introducción

Mi guión tenía 3 partes:

1. Comentar que en la NcN dábamos "certificados" de asistencia.
2. Introducir primero para qué podían ser útiles el voto y la firma anónimos.
3. Describir el funcionamiento del sistema y la propuesta en particular para implementarlo en la NcN.

Mi guión estaba poco comentado, sólo algunas frases claves y en general era más bien un esquema de los puntos que tocar y relaciones de unos con otros para una ponencia que debía durar sólo media hora. Pero aquí miraré de comentarlo para que quede clara mi propuesta y la podamos comentarlo en el foro y buscarle las pegas.

1. Certificados

Todos aquellos que lo solicitaron tuvieron a su disposición el servicio de firmas de claves públicas de la NcN. El sistema es sencillo, primero los asistentes traían un documento que les acreditase su identidad e indicaban de alguna forma cuál era su clave pública. Después del evento me encargué de crear el par de claves de la NcN validas por unos pocos días, firmar las claves públicas de los asistentes, y por último destruir la clave.

De esta forma los asistentes tuvieron más firmas en sus claves públicas que aumentaban la seguridad de que eran suyas y de paso confirmaban que habían asistido a la NcN.

Se me pasó el avisar a los asistentes un par de días antes como habíamos pensado, así hubiésemos podido echar una mano a quien no tuviese mucha experiencia en el tema y que llegado el momento, tuviese una clave pública

que pasarnos. Tomo nota para la próxima vez que me encargue de algo así con claves GPG / PGP.

2. ¿Por qué?

La pregunta de por qué tanto defender la privacidad es digna por si sola no de un documento sino de muchos que ya hay en Internet y muchos que aun vendrán porqué se trata de un tema muy polémico que varía con las leyes a medida que pasa el tiempo.

Además mi intención era abarcar no sólo el tema central de la privacidad, también el anonimato y comentar los atentados del 11S para dar un poco de perspectiva.

2.1. Fundamentalismo Islámico

Desde los terribles atentados del 11S los gobiernos están cediendo cada vez más antes las peticiones de las agencias de seguridad y espionaje. Ya tiempo atrás venían pidiendo que se modificasen los marcos legales para permitirles acceder a las comunicaciones cada vez de forma más invasiva.

Y es natural, es su misión buscar posibles peligros y plantear defensas para evitarlos. Lo que pasa es que hay que intentar ser razonable igual que cuando el jurado escucha al fiscal y al abogado defensor y no aceptar según que métodos porque eso nos haría cómplices.

De todos son conocidos ya los intentos de que se obligase a los usuarios a proteger sus comunicaciones con un chip de cifrado controlado por unas determinadas manos allá en los USA. En la vecina Francia hubo un tiempo en que cifrar las comunicaciones era delito.

De todas formas soy un poco escéptico sobre esos intentos de poner puertas en medio del campo. Además, todos sabemos lo fácil que es entrar en la mayoría de las casas donde los usuarios normales de ordenadores suelen utilizar un sistema operativo de Microsoft. De cuyos padres hemos oído repetidamente que no se venden ni ceden a las enormes presiones que reciben para que pongan puertas traseras que permitan a la policía o a determinadas agencias gubernamentales entrar fácilmente y hurgar lo que quieran. Y al final de tanto no rendirse, la verdad es que no parece que nuca haya sido demasiado difícil hackear les ni que se hayan esforzado demasiado en corregir los problemas una vez enterados. ¿Se trata simplemente de mal trabajo pero sin mala intención? Me vuelvo a confesar escéptico.

Volviendo a los atentados, parece que ahora tienen más vía libre. Parece que ya no es tan desvergonzado entrar en los sistemas informáticos de cualquier parte del mundo para robarles las claves privadas o obligar a que los servidores de acceso a Internet a que guarden una cantidad ingente de información de los usuarios que simplemente navegan o envían correos electrónicos.

Por cierto, alguien sabe ¿por qué esa fecha determinada? ¿Por qué eligieron el 11 de septiembre precisamente? Pensando para la ponencia di con una posible

respuesta: 11S son caracteres que unidos son el símbolo del dolar $.

No digo que sea la respuesta, tiene pegas como por ejemplo el que no sean letras arábicas pero quizás sea un mensaje de cara a occidente. Pero me sorprendió la posibilidad que todavía no he encontrado comentada en ningún medio de comunicación o en Internet.

Así pues, el primer por qué de la propuesta de firma y voto anónimos era promocionar el uso del GPG como forma de defender la privacidad.

2.2. GPG

Normalmente todo el mundo envía cartas firmadas y cerradas pero cuando lo hace por medios informáticos, a pesar de ser sencillo dar el equivalente informático al correo no se suele hacer y es cuando más se necesita.

Era mi impresión (y sigo pensando igual) que el uso del GPG está bastante poco extendido incluso entre los técnicos que trabajan en la seguridad informática.

No es nada fácil convencer a quien no está muy familiarizado con la informática para que use el GnuPG o el PGP. Suelen verlo como algo difícil a pesar de que no lo es y no confían demasiado.

Dado esa dificultad en la promoción el problema me rondó aun más por la cabeza.

2.3. Anonimato

Estuve hablando con alguien del entorno de Amnistía Internacional. Resulta que utilizan un sistema curioso para evitarles las persecuciones.

Los miembros de Amnistía suelen enviar miles y miles de cartas a los gobiernos que permiten barbaries contra los derechos humanos como por ejemplo aquellos que realizan limpiezas raciales. La idea es evidenciarles delante de la comunidad internacional y de esa forma presionarles.

Ningún miembro de dicha organización en uno de los países destinatarios donde pueden ser perseguidos envía cartas a su propio gobierno, si las envían lo hacen hacia otros gobiernos en el exterior.

Conversando salio el tema del anonimato. También es un tema difícil, mucha gente piensa que un anónimo es algo despreciable, un acto de falta de valor que desmerece completamente el escrito hasta el extremo de pensar que es mejor tirarlo a la papelera sin leerlo. Y eso es un error, sin minusvalorar los que tienen firma y corren un riesgo para declarar algo, el anónimo no tiene por qué ser un engaño o un intento de hacer daño.

Hay que recordar que la propiedad de anonimato no tiene que tener ningún estigma social, de hecho lo utilizamos en nuestras instituciones democráticas a la hora de votar y entonces es casi sagrado. Pienso que se necesita un cambio de mentalidad al respecto.

3. Sistema de firma y voto anonimos

Teniendo todo aquello en mente y dándole vueltas se me ocurrió una posible implementación de un sistema que permite el voto anónimo y un tipo de firma especial. Se trata de una firma que permite saber solamente a que grupo de firmantes pertenece el dueño del documento firmado y si ha firmado varias veces. Así mismo permite votar cumpliendo con las condiciones básicas de una votación:

1. Sólo un determinado grupo de personas pueden votar, los llamados "votantes".
2. Sólo pueden votar una vez.
3. No se conoce cada voto a qué votante pertenece.

Tiene además otra característica, no permite saber quienes han votado y quienes no. Esa información es utilizada actualmente por ejemplo por los partidos políticos en las votaciones electorales y no sé si les gustaría la idea de tener que recurrir a otros métodos para conocerla, pero pienso que aporta un nivel más de privacidad.

3.1. Solución propuesta

La solución propuesta es usar el GPG para firmar pero quitándole a las firmas todo identificativo salvo el grupo al que pertenece. Por ejemplo si se trata de un colegio de ingenieros pues el nombre del colegio, si se trata de un hospital y es para los que trabajen allí pues podría servir: "empleado del hospital La salud".

Si se recogen las firmas públicas de todos los miembros del grupo con capacidad de firma de la forma adecuada se puede garantizar que se cumplan las condiciones requeridas. También el voto debe seguir un proceso que tenga las necesarias garantías.

Recogida de firmas

El proceso de recogida de firmas se detalla en la figura 1.

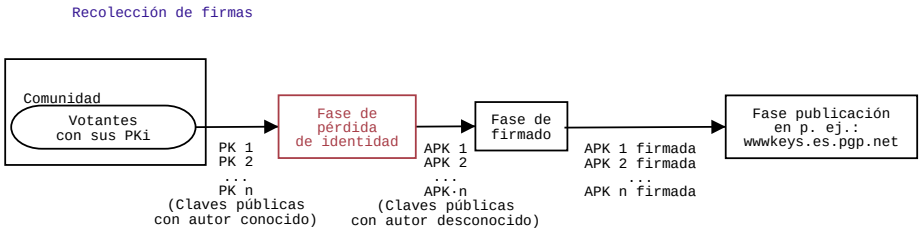

Figura 1

La recogida de firmas digitales tiene el propósito de permitir luego a los votantes / firmantes que puedan demostrar que el documento o voto es de un miembro del grupo. Este proceso como muestra la figura 1 tiene una serie de

fases sencillas que llevadas a cabo en el orden establecido garantizan el correcto funcionamiento.

Primero se crean los pares de claves por parte de los usuarios, luego estos hacen llegar las claves a través de una fase de pérdida de identidad a una autoridad con capacidad de certificar que la clave pública es de un miembro del grupo y por último se publican.

La clave del proceso está en que en la fase de perdida de identidad no puedan entrar nadie que no pertenezca al grupo y sólo puedan entrar una vez. Y es importante que haya suficiente fiabilidad en la fase de firmado para evitar que se firmen claves privadas de personas ajenas al grupo.

Implementación propuesta

Para hacer la primera prueba en la NcN se propuso utilizar un sistema de recogida de disquetes indistinguibles en una caja cada uno de ellos con una clave de un participante que previamente se hubiese chequeado su pertenencia a la lista de asistentes y su identidad con el DNI. Estos disquetes una vez recogidas todas las claves públicas serían firmadas por la NcN.

A partir de aquí cualquier anónimo que llegase con una firma garantizaba que el firmante era uno de los asistentes a la NcN.

Recolección de votos

Para la recolección de votos hay dos propuestas diferentes adaptadas a unas condiciones diferentes en el marco de las votaciones.

Propuesta 1

Esta propuesta evita al 100 % la posibilidad del pucherazo exponiendo la lista de votos y las firmas de los votantes.

Esto permite a todos los votantes comprobar si su voto está correctamente contabilizado en la lista. Si los votantes no son todos los miembros sino que se delega por grupos para que un votante "representante" de cada grupo ejerza su voto en nombre del grupo este método ofrece la interesante posibilidad de comprobar que el representante realmente votó lo que se le encomendó votar.

La figura 2 detalla los pasos que hay que seguir y una vez más hay que tener cuidado de asegurar la fase de pérdida de identidad del voto.

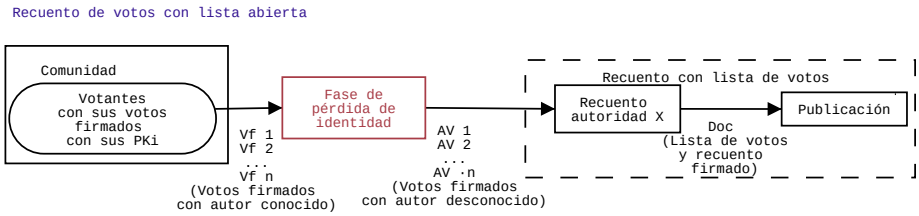

Figura 2

Propuesta 2

La segunda propuesta es para solucionar un problema grave que puede tener la primera en algunas condiciones especiales. Por ejemplo si se implementa en una votación para elegir un gobierno. Es sólo un decir, para que sirva de ejemplo. En este caso la votación es problemática, es muy importante garantizar que nadie

ha sido obligado a votar en un sentido determinado. Y si las listas son abiertas el votante puede revisar si su voto está correctamente contabilizado, pero esa comprobación también la podría hacer otra persona que le estuviese obligando.

Quizás hay otras posibles salidas para evitar que el voto pueda ser reconocible por otra persona como, por ejemplo, que la clave de reconocer su voto no sea la clave pública con que lo firma, pero aun no he dado con ninguna que no tenga pegas.

Así pues, la segunda propuesta es no publicar los votos. Pare ello se pide la colaboración de que una serie de autoridades para que lleven su propio ordenador con su propio software al que se le entregue los votos firmados. Y una vez contabilizados estos y llegado a un acuerdo en los resultados se exponen firmados por las distintas autoridades sin incluir los votos particulares.

La figura 3 detalla los pasos que hay que seguir y también tiene como punto crítico, que debe asegurarse, la fase de pérdida de identidad del voto.

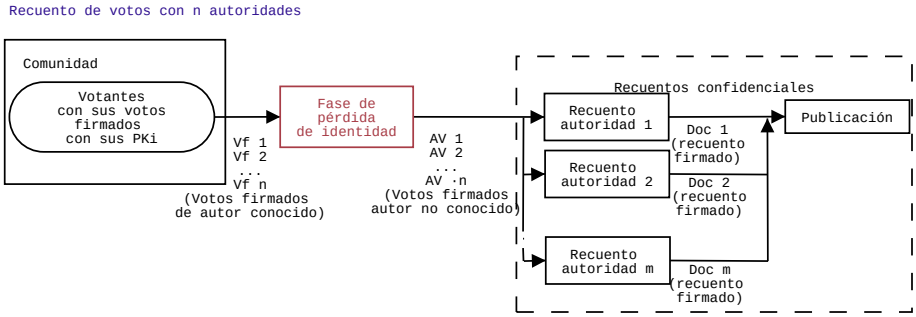

Figura 3

Esta solución tiene a su vez una pega, los votantes que no se fíen de las n autoridades, no quedan seguros de que no haya un complot, un acuerdo de engaño entre todas las autoridades. La única forma es que se les permita a muchos de ellos ser autoridades, que el numero de autoridades que comprueban pueda ser moderadamente grande.

Implementación en la NcN

La propuesta inicial era recoger todas las firmas en unos disquetes y luego hacerlo de nuevo con otros disquetes para cada votación. Y en todas utilizar el sistema de listas abiertas por no ser un peligro real el que se obligase a alguien a votar y por el coste de tener n autoridades reconocidas entre los asistentes. No valía la pena, era sólo para probar que el sistema funcionase y al final no se llevó a cabo.

Notas finales

El sistema propuesto constituye sólo una hipótesis de trabajo que no pretende ser la solución definitiva. De echo se presentó en público finalizando con una petición a los asistentes de críticas para ver si por algún defecto que se me escapase no era viable. La petición de críticas sigue abierta y espero que en foro

de la NcN aparezcan comentarios de quien piense que puede contribuir.

La idea es que se critique esta solución propuesta y se le añadan detalles o controles pero también hay cabida para comentar otras soluciones implementadas que traten de cualquiera de los dos temas: votaciones y firmas anónimas.

Preguntas

1- De todas las preguntas hay una que destaca: *¿Usó Bin Laden el GPG / PGP?*

Mi opinión:

No creo que lo hiciese. La razón es que dudo que tuviese confianza en ese sistema.

Un problema que seguramente podría resolver es encontrar un ingeniero en informática que pudiese explicarle el nivel de seguridad que puede darle pero tengo la impresión de que aun así no le daría confianza.

Al ser una tecnología extranjera de origen kafir (no musulmán) la confianza es un problema grave para un fundamentalista integrista Islámico. Luego está el problema de si los káfires tienen o no una forma de romper el propio sistema que no han hecho pública.

De todas formas es sólo una opinión, como lo es el que Bin Laden está muerto. Soy escéptico frente a la posibilidad de que siga vivo pero prefiera no volver a amenazar y llamar a la yijad a los musulmanes de todo el mundo con más y más nuevos vídeos.

Puede que a alguno le interese seguir amenazando con el fantasma de Bin Laden para tener más fácil el cambio de las legislaciones.

Esté o no vivo, utilizase o no el PGP o el GnuPG, no es razón para dejas que impongan cambios en las legislaciones que coarten la base de nuestras libertades: nuestra privacidad.

2- Otra pregunta era sobre sistemas distribuidos donde la idea es perder el rastro de las claves en la multitud de ordenadores que actuen como una sól base de datos. (Siento no recordar el nombre, sólo recuerdo el esquema de la idea).

Respuesta:

Tengo la impresión de que es más difícil asegurar la confianza a un sistema unitario o de pocos ordenadores que contengan la información crítica, pero tendría que estudiar más el tema porque lo desconozco. Lo correcto sería dedicarle más tiempo para evaluarlo pero no lo tengo y dejo eso pendiente, si alguien está interesado en el tema debería informarse también sobre este sistema que me digeron que está funcionado.

Por hacer

Dejo varios puntos por hacer, pero el más importante es probarlo en la vida real. Adquirir experiencia al respecto e ir adaptandolo a la realidad y mejorándolo con las críticas.