1. **Diez riesgos sobre la "Infraestructura de Clave Pública"**

Bruce Schneier y Carl Ellison publican un ensayo de ocho páginas sobre los riesgos de la "Infraestructura de Clave Pública", tal y como se define en la actualidad. El documento fue publicado originalmente en el primer número del año 2.000 de la revista "Computer Security Journal".

El documento, analiza en profundidad diez riesgos de las estructuras PKI actuales. Las PKI constituyen, entre otras cosas, las bases actuales de las entidades de certificación, por ejemplo:

1. **¿En quien debo confiar?**
   Hoy en día existen multitud de entidades de certificación pero, ¿quien te garantiza que los datos que certifican son correctos (por ejemplo, un email o un nombre?. ¿Quien las ha situado en el contexto comercial en el que se encuentran?. **Solución de ANF AC**
2. **¿Quien tiene acceso a mi clave?**
   La criptografía de clave pública o asimétrica supone la existencia de dos claves: una pública y disponible de forma universal, y otra privada y bajo el control exclusivo del usuario.
   Pero, hoy en día, la clave secreta o privada no está segura. Los sistemas operativos y los navegadores adolecen de multitud de problemas de seguridad, además de existir virus y troyanos. Por tanto, no se puede garantizar que un documento firmado con una clave secreta constituya una firma confiable. **Solución de ANF AC**
3. **¿Cómo de seguro es el ordenador verificador?**
   Como ocurre con el caso anterior, el ordenador que realiza la verificación del certificado puede haber sido manipulado. Puede, por ejemplo, haberse instalado una entidad de certificación espúrea en el navegador, algo absolutamente trivial. **Solución de ANF AC**
4. **¿Qué "Jesús Cea" es el correcto?**
   Habitualmente los certificados se expiden a un nombre determinado, sin tener en cuenta que pueden existir diferentes personas con dicho nombre. En caso de disponer de información adicional, como su dirección de correo electrónico, tenemos que saber también si ésta es correcta o no, amén de vincular al usuario con datos que pueden quedar anticuados en un plazo breve. **Solución de ANF AC**
5. **¿La entidad de certificación es realmente una autoridad?**
   Por lo general, una entidad de certificación tradicional emite un certificado cubriendo datos sobre los que no tiene control. Por ejemplo, un certificado fusionando el nombre y la dirección de correo electrónico de un usuario no tiene en cuenta si el usuario se llama real y legalmente así, ni considera la posibilidad de que el email cambie o el ISP dé de baja la cuenta y la reasigne a otro usuario (o que todo el ISP desaparezca, por ejemplo). **Solución de ANF AC**
6. **¿El diseño de seguridad considera al usuario?**
   Son muy pocos los usuarios, por ejemplo, que verifican los certificados del servidor remoto cuando establecen una conexión SSL con su navegador. **Solución de ANF AC**
7. **¿Autoridades de certificación o autoridades de certificación con autoridades de registro? Solución de ANF AC**
8. **¿Cómo identifica la autoridad de certificación al usuario?**
   Antes de emitir un certificado, la autoridad de certificación debe tener la certeza de que los datos que certifica son correctos. **Solución de ANF AC**
9. **¿Los certificados son seguros?**
   El uso de certificados no garantiza la seguridad. Una cadena es tan fuerte como su eslabón más débil. **Solución de ANF AC**
10. **¿El diseño de seguridad considera el proceso de firma?** Son muy pocas las autoridades de certificación que intervienen durante el proceso de firma, no queriendo asumir responsabilidad alguna y dejando a las partes sin garantías ciertas del proceso. **Solución de ANF AC**

Más Información:
Ten Risks of PKI: What You're Not Being Told About Public Key
Traducción al castellano
Servidor de ANF