¿Para qué se usa el key-value store en pung?

Para que los metadatos puedan estar protegidos si se pierde la seguridad de la infraestructura de la red.

¿Cuáles son 2 ventajas del esquema de aliasing propuesto? (vs. La alternativa de implementar pung sin aliasing)

Existe una gran probabilidad de ocultar la metadata si de alguna forma se compromete la infraestructura, es decir, da privacidad a los metadatos.

Permite escalabilidad, el rendimiento aumenta de forma lineal con el número de servidores.

¿Cuál es una ventaja de Dissent vs Pung?

Facilita la encriptación de la información.

¿Cuál es una desventaja de Dissent vs Pung?

Ciertas claves puedes ser idénticas, ya sea con diversas entradas, lo cual puede ser explotado por los terceros que quieren acceder a dicha información, con una tabla de string y respuestas.

¿Qué video escogió y por qué?

Primer video:

The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information

Ya que deseo conocer cómo se realiza el secuestro de las cookies y como poder solucionarlo.

¿Qué problema describe el video?

Habla de cómo los archivos cookies son encriptados, como navegan por la red, y como pueden ser interceptados por un tercero para comprometer su información.

¿Considera usted que el problema descrito es serio o grave?

La intercepción de cookies por un tercero es grave, ya que en la actualidad las cookies siempre tienen información sensible de una u otra forma, es por eso que existen muchas leyes que comprometen a los servicios en línea, repositorios, etc. A preguntar al usuario si este desea manejar el uso de cookies para ese servicio, ya que de lo contrario puede estar violando la privacidad del mismo.

¿Qué se puede hacer para solucionar/evitar el problema descrito?

Una opción fácil, es que los usuarios estén conscientes de que fin se le dará a la información personal que comprometen en línea, para que este trate en lo posible de exponer material que no quiera que sea invadido por alguien más, como por ejemplo contraseñas, así mismo, podría tener nuevas prácticas como tener varias contraseñas, o de carácter más fuerte, por si ocurre una falla en la seguridad toda su información no sea expuesta.