Zero-knowledge proof
Prueba de conocimiento-cero

Carlos Vaughn O'Connor

En forma abstracta una prueba de conocimiento-cero es una prueba interactiva con un prover y un verifier, donde el prover convence (con alta probabilidad) al verifier qué declaración es verdadera sin revelar ninguna información adicional. Tal prueba es usada en métodos de autenticación. En este artículo brindamos una explicación de qué se entiende por una prueba de conocimiento-cero y dos ejemplos que creemos les aclararán las dudas. Con este artículo NEX IT Specialist ha contribuido a www.wikipedia.org con la versión en español de Prueba de Conocimiento-cero (Zero Knowledge Proof).

El concepto criptográfico de prueba de conocimiento-cero o protocolo de conocimiento-cero es un método interactivo para que un ente pruebe a otro que una declaración (usualmente matemática) es verdadera, sin revelar nada más que la veracidad de la afirmación. Aparece el concepto de "probador" (en inglés "prover") y "verificador" (en inglés "verifier") y se establecen una serie de pasos (protocolo)

Una prueba de conocimiento-cero debe satisfacer las siguientes tres propiedades:

1. Completitud: si la declaración es correcta, el "verificador" honesto (esto es, aquel que sigue el protocolo correctamente) quedará convencido del hecho por un "probador" honesto.
2. Ser lógica: si la declaración es falsa, ningún "probador" deshonesto podrá probar al "verificador" honesto que es verdadera. Excepto, con una probabilidad muy baja.
3. Conocimiento-Cero: si la declaración es verdadera, ningún "verificador" deshonesto aprende algo más que este hecho. Esto se formaliza mostrando que cada "verificador" deshonesto tiene algún "simulador" que, dado el argumento a probar (y ningún acceso al "probador"), puede producir una copia que "parece ser como" una interacción entre el probador "honesto" y el "verificador" deshonesto.

Las dos primeras de estas son propiedades definen el caso más general de "sistemas de pruebas interactiva"

La investigación en pruebas de conocimiento-cero ha estado motivada por sistemas de autenticación donde una parte quiere probar su identidad a la otra a través de alguna información secreta (por ejemplo un password), pero no quiere que el segundo ente conozca nada de cuál es su secreto.

Los pasos típicos en una prueba de conocimiento-cero es que el "probador" da un mensaje de "compromiso" (commitment message) que es seguido por un "desafío" dado por el "verificador" (challenge). Finalmente una respuesta que da el "probador" al desafío. Este protocolo se puede hacer varias veces y dependiendo de las respuestas obtenidas el "verificador" puede aceptar o no la prueba.

Veamos dos ejemplos muy simples pero muy ilustrativos:

Ejemplo 1.

¿"Dónde está Waldo"? es un juego que aparece en libros donde cada página contiene un dibujo muy detallado con muchísimos personajes. El fin del juego es encontrar a Waldo, un personaje predefinido (ver imágen a continuación).

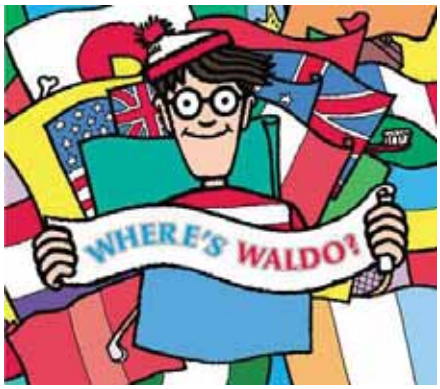
Veamos la siguiente historia que nos ejemplifica este problema de criptografía muy interesante:

Nuestra historia involucra a Alice y Bob (recordar que estos son nombre siempre usados en la mayoría de las ejemplificaciones de temas de criptografía).

Alice y Bob se hallaban jugando a "¿Dónde está Waldo?". Alice de repente exclama: "se donde está Waldo". Bob le responde: "eres una mentirosa". ¿Cómo puede Alice probarle a Bob que identificó a Waldo sin revelar su ubicación en el dibujo?.

Solución simple:

Antes que nada permitamos a Alice tener acceso a una fotocopiadora. Ahora realizan el siguiente protocolo: fotocopian el dibujo específico, Alice corta la imagen de Waldo de la fotocopia (Bob no está autorizado a mirar). Se queda con la imagen de Waldo y destruye el resto. Con esto demuestra a Bob que sabía donde estaba Waldo y revela casi nada nuevo ya que Bob conoce de antemano la imagen de Waldo.



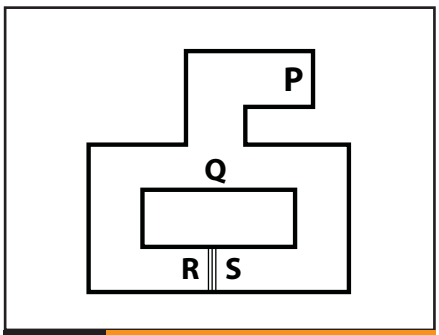
Una discusión más completa puede verse en la web page de Moni Naor, Dept. of Computer Science and Applied Mathematics, Weizmann Institute of Science (Referencia 1).

Ejemplo 2:

La cueva de Alí Babá (no deje de leer las Referencias 2 y 3.).

Alice quiere probarle a Bob que ella conoce las palabras secretas que abren la puerta R-S en la cueva. Pero, no desea revelar el secreto.

El compromiso de Alice es ir a R o S. Una típica rueda del protocolo sería: Bob va a P y espera que Alice vaya a R o S. Bob se dirige a Q y grita a Alice que salga por la derecha o la izquierda. Si Alice no conociese las palabras secretas que abren la puerta R-S habría sólo una chance del 50% de que ella acertara al salir por izquierda o derecha. Si ella realmente conoce el secreto, no importa cuantas veces se repita el proceso siempre saldrá del lado correcto. Y, no reveló la frase "ábrete sésamo".



La Cueva de Alí Babá

Referencias

1. *http://www.wisdom.weizmann.ac.il/~naor/PUZZLES/waldo.html*

2. *J.-J. Quisquater , L. Guillou and families, with T. Berson: How to explain zero-knowledge protocols to your children. In G. Brassard, ed., Advances in Cryptology -- Crypto '89, vol. 435 of Lectures Notes in Computer Science, Springer-Verlag, pp. 628-631, 1990.*

3. *FAQ de RSA Laboratorios de RSA Security: http://www.rsasecurity.com/rsalabs/node.asp?id=2152*