Ingeniería Eléctrica
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

Estudiantes: _____

_____

_____

Radio Frequency Identification (RFID)

Introducción

RFID es una tecnología de comunicación inalámbrica que permite transmitir información sobre la identidad de un objeto (código ID, ubicación, color, tamaño, etc.) a través de una etiqueta o *tag*. A grandes rasgos, el *tag* consiste en una antena capaz de recibir y emitir información en la banda de las radiofrecuencias.

En esta experiencia se usará un lector/escritor RFID Rysccorp y el *software* Proxmark3, que funciona en GNU/Linux.

Desarrollo

Conexión de los dispositivos e ingreso al *software*

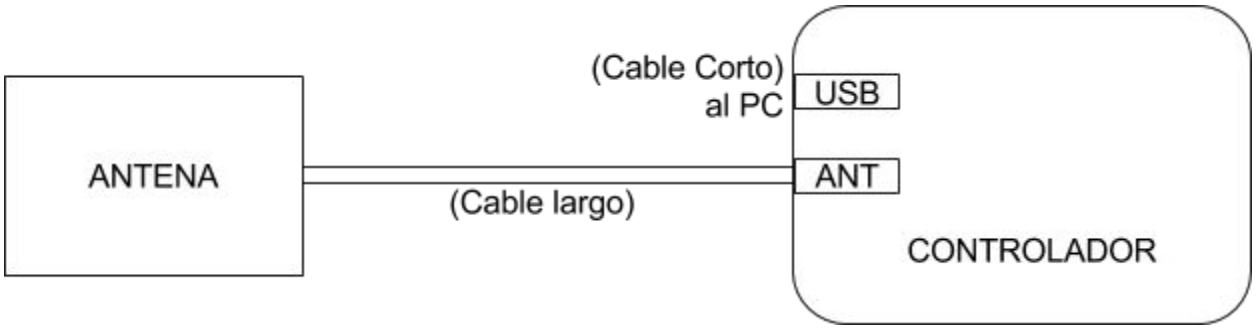

Figura 1 - Diagrama de conexiones del lector/escritor RFID

1. Iniciar el PC en Ubuntu y abrir una línea de comandos (Terminal).
2. Compruebe que la tarjeta "*J. Westhues ProxMark-3 RFID Instrument*" ha sido reconocida usando el comando **lsusb**, que muestra los dispositivos USB conectados al PC.
3. Navegue hasta la carpeta ".../pm3-r623/client", donde se encuentra el software Proxmark3. Para esto use los comandos **cd + Nombre_carpeta** (para entrar a las carpetas) y **ls** (para mostrar los archivos y carpetas dentro de la carpeta actual).
4. Para iniciar el *software*, usar el comando **sudo ./proxmark3**, *password*: buhoazul

Lectura de una tarjeta

Usando el comando **hf 14a reader**, leer las TUI del grupo y anotar los datos de cada tarjeta:

		Key A	Access Bits	Key B
Sector	**Block**	**Data**		
0	0	33bd9d3f2c980200648f841441502212		
	1	090f1808000000000003010000400b		
	2	00000000400c400c400c000400040005		
	3	a0a1a2a3a4a5787788c17de02a7f6025		
1	4	418d50c98d7f962462004c800000ffcc		
	5	1fa1014100d101c060000000049a2a9f		
	6	1fa1014100d101c060000000049a2a9f		
	7	2735fc18180778778800bf23a53c1f63		
2	8	3065061730077220296012505b74c05d		
	9	68c701da24c027ece0ee9a99c0caadb1		
	10	c82591842f0b8304a2a068d1f4e016e7		
	11	2aba9519f574787788ffcb9a1f2d7368		

Figura 2 - Ejemplo de los datos almacenados en una tarjeta RFID MIFARE. Notar que en el último bloque de cada sector se encuentra la pass (Key A) para editar el sector correspondiente.

Dependiendo del modelo de su tarjeta, la Universidad guardó su nombre en el sector 2 o el 18. Acceda a estos sectores de una de sus TUI para encontrar los datos hexadecimales almacenados y conviértalos a ASCII. Usando el entorno "help", encontrar el comando necesario para la lectura de un sector. *Hint*: comienza con **hf mf**. Nota: la password puede ser `a0a1a2a3a4a5` o `ffffffffffff` (passwords default). Anotar el comando usado y los datos accedidos:

También hay otra información en otros sectores de su tarjeta TUI (sobretodo si es un modelo más reciente), Búsquelos y mencione que otra información logró encontrar y en qué sector y/o bloque.

Escritura de una tarjeta

Ahora que sabe leer la información desde una tarjeta, se procederá a escribir información encima de otra del tipo “Mifare Classic 1k” (tarjeta blanca). Para esto encuentre el comando necesario para escribir sobre bloques. *Hint*: comienza con **hf mf**. Clone su TUI en los sectores que lo permitan. Luego de realizar esto pruebe la tarjeta clonada en una de las puertas magnetizadas de la facultad. ¿Que sucedió y por qué?¿Son Vulnerables las TUI?

Lea el bloque 0 de la tarjeta blanca e intente cambiarlo. ¿Qué relación tiene con la UID?

Borre los cambios realizados en la tarjeta blanca, ordene su puesto y dele un abrazo a los aux <3.

Referencias

1. J. Scambray, S. McClure & G. Kurt, *Hacking Exposed Linux 3rd Edition*, ISECOM.
   - Disponible (Web): http://bit.ly/1PPodVk
2. V. D. Hunt, A. Puglia & M. Puglia, *A Guide to Radio Frequency Identification*, Willey.
   - Disponible (Web): http://bit.ly/1RzXwRL
3. K. Finkenzeller, *RFID Handbook 3rd Edition*, Willey.
   - Disponible (Web): http://bit.ly/1H8sBqa