INSTITUTO TECNOLÓGICO DE CELAYA

MATERIA:
TÓPICOS AVANZADOS DE SEGURIDAD EN REDES CONVERGENTES

ALUMNA:
SANTANA DE LOS RÍOS CAROLINA

NÚMERO DE CONTROL:
13030622

TÍTULO:
INVESTIGACIÓN AUTENTICACIÓN MÚLTIPLE

FECHA DE ENTREGA:
21 DE SEPTIEMBRE DEL 2017

1) Investigar los distintos mecanismos para autenticación en dos pasos

+ Como funciona: OTP, PIV, U2F, OATH, Open PGP.

Autenticación en dos pasos

También conocido como: Doble Factor de Autenticación (2FA). Se trata de una medida de seguridad para que sea más difícil que un usuario sin autorización acceda a una cuenta. [1]

Este tipo de verificación se activa sobre un servicio web, en donde además de ingresar la contraseña, también será necesario un código único para concluir el acceso. Dicho código generalmente es enviado al teléfono móvil del usuario por medio de un SMS, aplicaciones móviles, llamadas telefónicas, entre otros. [1]

OTP

Contraseña de un Solo Uso (*One-Time Password*), válida solo para una autenticación.

OTP soluciona las deficiencias relacionadas con la implementación de una contraseña estática. Entre las mejoras se incluyen:

- Las contraseñas OTP son vulnerables a ataques de REPLAY (transmisión de datos maliciosa o fraudulentamente repetida).
- Hace al sistema más fuerte ante ataques de fuerza bruta (obtener una clave probando todas las combinaciones posibles). [2]

PIV

Verificación de Identidad Personal (*Personal Identity Verification*), permite la gestión de identificaciones, desde la verificación de identidad hasta la emisión y uso de seguros de credenciales. Se brinda a los usuarios una experiencia más ágil, seguridad más robusta implementando el uso de credenciales confiables y otros aspectos avanzados, los cuales son sencillos de adquirir, instalar y mantener. [3]

U2F

Segundo Factor Universal (*Universal 2nd Factor*), estándar de la verificación en dos pasos por hardware, evita al usuario tener que lidiar con mensajes o códigos complicados. [4]

Creado con el objetivo de brindar más seguridad a las cuentas de usuario sin complicaciones, se ha conseguido con las llaves USB que actualmente se consiguen en el mercado.

Existen cuatro tipos de llaves (las cuales pueden ser encontradas en Amazon España):

1. FIDO U2F Ready
2. FIDO U2F Dedicated
3. YubiKey NEO
4. YubiKey Nano

Como dato adicional, el inicio de sesión de google es compatible con este sistema, siempre en combinación al clásico login de usuario y contraseña

OATH

Autorización Abierta (*Open Authorization*, *OATH u OAuth*), estándar abierto con flujos simples de autorización para páginas web o aplicaciones informáticas. Permite la autorización segura de una API (conjunto de subrutinas, funciones y procedimientos que ofrece cierta librería para ser utilizado por otro software como capa de abstracción) [5] para aplicaciones de escritorio, móviles y web.

Permite a un usuario del tipo A compartir su información en el sitio A (proveedor de servicios) con el sitio B (consumidor), sin compartir toda su identidad. En otras palabras, para desarrolladores de consumidores, OATH ofrece un método para interactuar con datos protegidos y publicarlos. Por otro lado, para desarrolladores de proveedores de servicio, OATH proporciona a los usuarios el acceso a sus datos al mismo tiempo que protege las credenciales de su cuenta.

Este mecanismo es utilizado por Google, Facebook, Microsoft, Twitter y Github para permitir a los usuarios compartir información sobre sus cuentas con aplicaciones de terceros o sitios web. [6]

Open PGP

Estándar para encriptación de email más utilizado [7]. Derivado del software PGP (Privacidad Bastante Buena, *Pretty Good Privacy*), programa que protege los datos distribuidos a través de internet mediante el uso de criptografía de clave pública (método que usa un par de claves para el envío de mensajes), así como facilitar la autenticación de documentos gracias a firmas digitales (mecanismo criptográfico

que permite identificar al propietario de un mensaje y que éste no ha sido alterado). [8]

2) Beneficios que hay con esta autenticación

Capa de seguridad extra que se proporciona a las cuentas personales, debido a que es más seguro que el clásico login de usuario y contraseña. Aunque la contraseña no sea segura y un atacante la ha adivinado, si se tiene la autenticación por dos pasos, nadie más podrá acceder a la cuenta. [1]

3) ¿De qué vulnerabilidades nos estaremos protegiendo?

Ataques de phishing, su objetivo es obtener información personal y bancaria de los usuarios; con éste, se puede obtener la contraseña de una cuenta y, si no tiene habilitada la autenticación por dos pasos, un ciberdelincuente podría acceder a ella. [1]

Ataques de fuerza bruta, consiste en obtener una clave probando todas las combinaciones posibles. La mayoría de los usuarios elige utilizar una contraseña no muy segura que repite en varios sitios, la autenticación en dos pasos es un método para mantener segura la cuenta.

Ataques de REPLAY, transmisión de datos maliciosa o fraudulentamente repetida. [2]

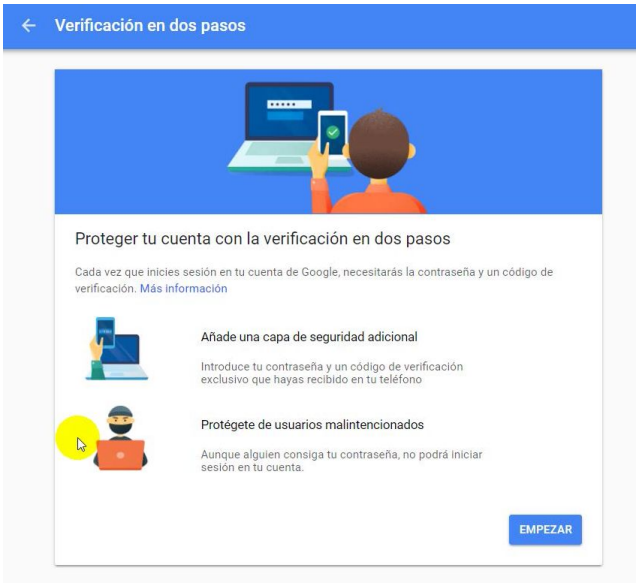
4) Comenzar a implementar una solución con Google

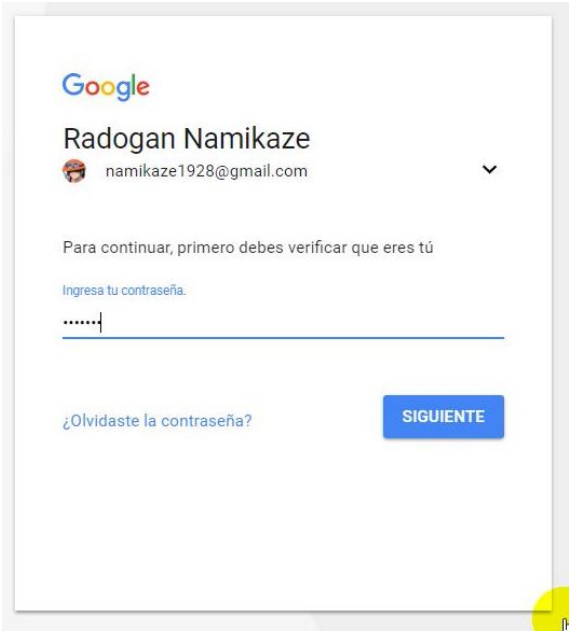
Capturas de pantalla:

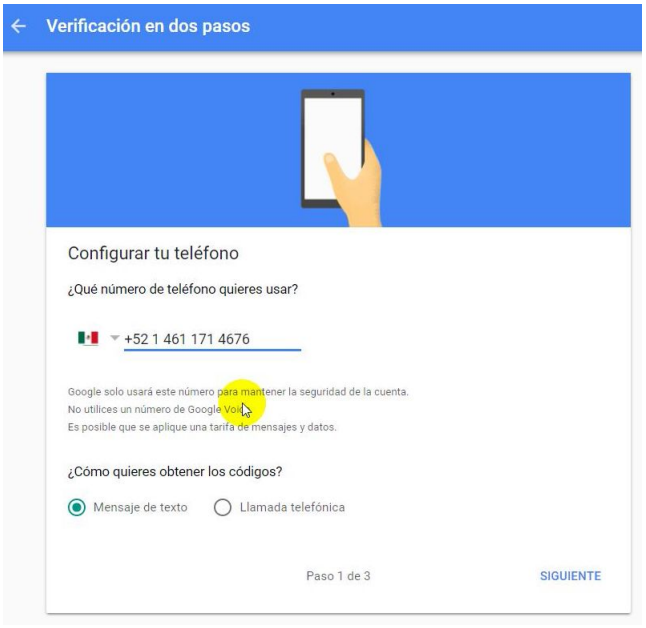
Únete a millones de otras personas que protegieron sus cuentas con la verificación en dos pasos

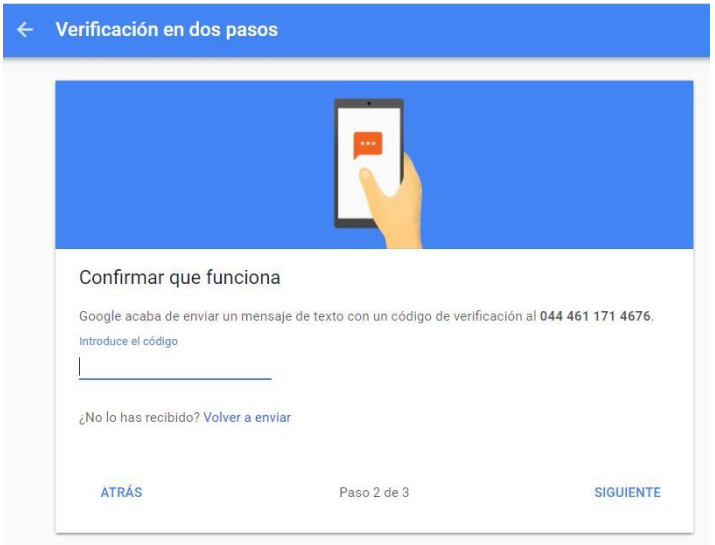
Comenzar

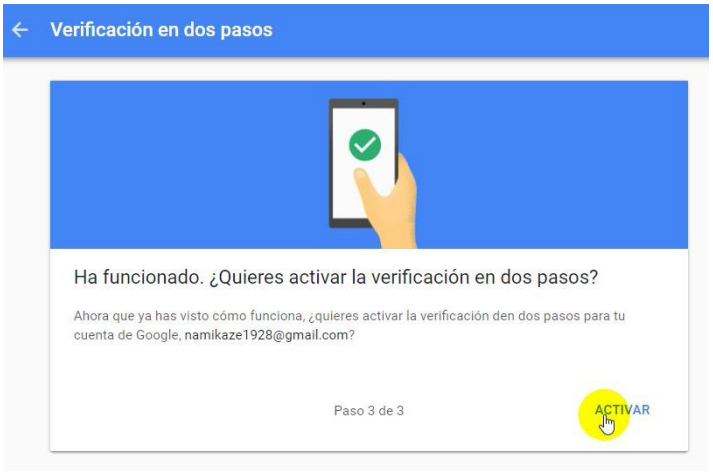
Ver cómo se protege la cuenta



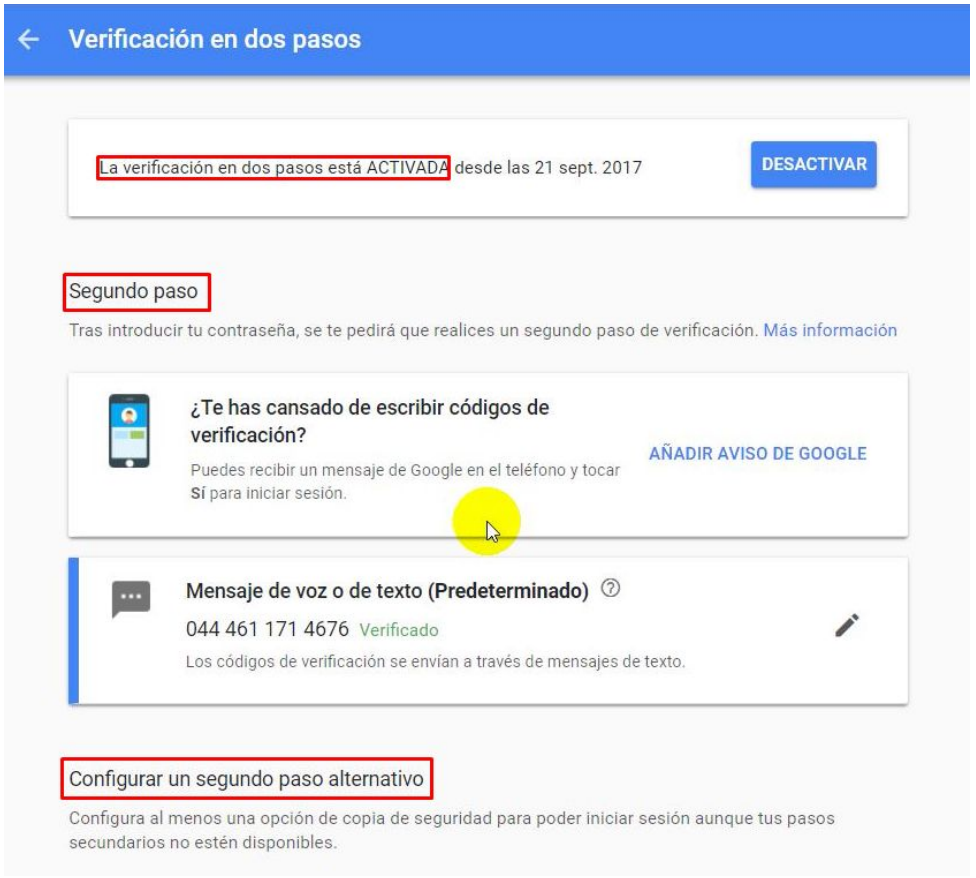








Lo siguiente es el 2do paso. Sin embargo, no pude implementar las dos opciones recomendadas por google, por lo que opté por las opciones alternativas.



Con esto se ha finalizado el 2do paso.

5) Investigar inicio de sesión en servidor propio más validación de yubico.

Yubico proporciona una “Yubikey”, se trata de un dispositivo llave que se puede conectar al puerto USB de la computadora con el fin de proveer una capa más de seguridad cuando se accede a las cuentas. La empresa asegura que son seguras, fáciles de usar, inmune a: ataques de repetición, *man in the middle*, y otra serie de amenazas.

Está disponible para las siguientes plataformas, la Yubikey es implementada durante el logueo al sistema: Ubuntu, Fedora, CentOS, RedHat, Centrify, Linux, macOS, Windows, MicroFocus y Citrix [9]. Existen opciones de logueo para cada una de estas plataformas, para Ubuntu se requiere lo siguiente [10]:

- Se requiere configurar la Yubikey para que responda al “llamado”. Yubico proporciona un manual, el cual hay que seguir para que la Yubikey se pueda utilizar durante el proceso de logueo: https://developers.yubico.com/yubico-pam/Authentication_Using_Challenge-Response.html
- Configurar el bloqueo de pantalla cuando la Yubikey es removida. El siguiente foro tiene una pequeña explicación de cómo realizar las configuraciones para la Yubikey Neo: http://forum.yubico.com/viewtopic.php?f=23&t=1143
    - Ejecutar el comando:
      sudo nano /usr/local/bin/yubikey

- Escribir lo siguiente dentro del archivo:

```
#!/bin/bash
# Double checking if the Yubikey is actually removed, Challenge-Response won't trigger the screensaver this way.

if [ -z "$(lsusb | grep Yubico)" ]; then
        logger "YubiKey Removed or Changed"
        # Running the LightDM lock command
        export XDG_SEAT_PATH="/org/freedesktop/DisplayManager/Seat0"
        /usr/bin/dm-tool lock
fi
```

- Guardar y cerrar el archivo. Crear el archivo ejecutable:
  sudo chmod +x /usr/local/bin/yubikey
- Encontrar las propiedades de la Yubikey para una asignación adecuada. Para esto, el descriptor USB debe estar activado. Se pueden encontrar detalles en el foro de Yubico:
  https://forum.yubico.com/viewtopic.php?f=23&t=1143#p4772
- En una ventana de terminal nueva, ejecute el siguiente comando:
  udevadm monitor --environment --udev
- Desconecte la Yubikey y obtenga la lista de IDs. Busque las siguientes IDs:

```
ID_VENDOR_ID
ID_MODEL_ID
ID_SERIAL_SHORT
```

- Los IDs serán usados para reconocer la Yubikey. Lo siguiente es crear el siguiente archivo:
  sudo nano /etc/udev/rules.d/85-yubikey.rules
- Escribir en el archivo lo siguiente:

```
# Yubikey Udev Rule: running a bash script in case your Yubikey is removed
ACTION=="remove", ENV{ID_VENDOR_ID}=="1050", ENV{ID_MODEL_ID}=="0010",
ENV{ID_SERIAL_SHORT}=="0001711399", RUN+="/usr/local/bin/yubikey"
```

- Cambie el ID de acuerdo a su llave. Guarde y cierre el archivo. Finalmente, el servicio UDEV tiene que recargar las reglas:
  sudo udevadm control --reload-rules
  sudo service udev reload

Además, Yubico cuenta con autenticación por factores múltiples, implementa un dispositivo que puede ser habilitado para usarse con su cuenta y requiere de un segundo paso antes de poder acceder. Esto ayuda a proteger de keyloggers y otras amenazas.

Este tipo de autenticación cuenta con las siguientes opciones principales [11]:

- *LastPass Authenticator*, genera códigos de autenticación de una sola vez o envía una notificación *push* a un teléfono inteligente
- *Google Authenticator*, genera códigos de autenticación de una sola vez en un teléfono inteligente. Puede ser usado en conjunto con *Microsoft Authenticator*

- *Toopher*, envía notificaciones push a un teléfono inteligente para verificar un logueo
- *Duo Security*, genera códigos de autenticación de una sola vez o envía una notificación *push* a un teléfono inteligente
- *Transakt*, envía una notificación de aceptación o rechazo a un teléfono inteligente
- *Grid*, hoja de cálculo imprimible de números y letras usado para ingresar distintos valores al momento de loguearse.
- *Yubikey*, dispositivo USB que genera códigos de autenticación de una sola vez.

6) Investigar servicio autenticación en Radius (Freeradius) y OTP.

Radius

Este servidor puede soportar varios métodos para autenticar usuarios. Cuando se proporciona el nombre de usuario y la contraseña original, puede soportar PPP, PAP o de la GRIETA (de UNIX), así como otros mecanismos de autenticación. [12]

FreeRadius es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. [13]

OTP

OTP de Gemalto, solución para garantizar que las llaves OTP no sean comprometidas, al mismo tiempo que ofrece una fácil implementación y uso. [14]

SafeNet genera contraseñas de un solo uso y altamente seguras, garantizan que sólo los usuarios autentificados adecuadamente tengan acceso autorizado a las aplicaciones y datos críticos. [15]

Referencias

[1] Osi.es. (2017). *Verificación en dos pasos, ¿qué es y cómo me puede ayudar?* | Oficina de Seguridad del Internauta. [online] Available at: https://www.osi.es/es/actualidad/blog/2017/01/17/verificacion-en-dos-pasos-que-es-y-como-me-puede-ayudar [Accessed 21 Sep. 2017].

[2] Mohamad, J. and Patel, D. (2017). *Autenticación con contraseña de un solo uso.* [online] Es.wikipedia.org. Available at: https://es.wikipedia.org/wiki/Autenticaci%C3%B3n_con_contrase%C3%B1a_de_un_solo_uso [Accessed 21 Sep. 2017].

[3] Seguridad-online.com.ar. (2017). *Desde los equipos de escritorio hasta las puertas*. [online] Available at: http://www.seguridad-online.com.ar/index.php?mod=Home&ac=verNota&id_nota=1978&id_seccion=96 [Accessed 21 Sep. 2017].

[4] Pérez, D. (2017). *Llaves de seguridad USB: qué son y cómo funcionan*. [online] El Androide Libre. Available at: https://elandroidelibre.elespanol.com/2015/04/llaves-de-seguridad-usb-que-son-y-como-funcionan-con-google.html [Accessed 21 Sep. 2017].

[5] Es.wikipedia.org. (2017). *Interfaz de programación de aplicaciones*. [online] Available at: https://es.wikipedia.org/wiki/Interfaz_de_programaci%C3%B3n_de_aplicaciones [Accessed 21 Sep. 2017].

[6] Es.wikipedia.org. (2017). *OAuth*. [online] Available at: https://es.wikipedia.org/wiki/OAuth [Accessed 21 Sep. 2017].

[7] OpenPGP. (2017). *OpenPGP*. [online] Available at: http://openpgp.org/ [Accessed 21 Sep. 2017].

[8] Lucas, M. (2017). *Pretty Good Privacy*. [online] Es.wikipedia.org. Available at: https://es.wikipedia.org/wiki/Pretty_Good_Privacy#OpenPGP [Accessed 21 Sep. 2017].

[9] Yubico. (2017). *Featured Solutions* | Yubico. [online] Available at: https://www.yubico.com/solutions/#computer-login [Accessed 21 Sep. 2017].

[10] Courbet, M. (2017). *Use of Yubikey Neo for login 2FA and lock screen*. [online] Askubuntu.com. Available at: https://askubuntu.com/questions/635266/use-of-yubikey-neo-for-login-2fa-and-lock-screen [Accessed 21 Sep. 2017].

[11] User Manual. (2017). *Protecting Your Account with Multifactor Authentication*. [online] Available at: https://helpdesk.lastpass.com/es/multifactor-authentication-options/ [Accessed 21 Sep. 2017].

[12] Tecnologías, S. (2017). *¿Cómo el RADIUS trabaja?*. [online] Cisco. Available at: https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html#authenticandauthor [Accessed 21 Sep. 2017].

[13] Cayu.com.ar. (2017). *Servidor FreeRadius* [Cayu - Wiki de Sergio Cayuqueo]. [online] Available at: http://cayu.com.ar/wiki/doku.php/manuales:servidor_freeradius [Accessed 21 Sep. 2017].

[14] Gemalto.com. (2017). *OTP de Gemalto*. [online] Available at: http://www.gemalto.com/latam/identidad/inspiracion/autenticacion-robusta/info-on-otp [Accessed 21 Sep. 2017].

[15] Gemalto. (2017). *Autenticación con OTP (contraseña de un sólo uso)*. [online] Available at: https://safenet.gemalto.es/multi-factor-authentication/authenticators/one-time-password-otp/ [Accessed 21 Sep. 2017].