FACULTAD DE CIENCIAS

DEPARTAMENTO DE...

PHD THESIS:

EL TÍTULO DE LA TESIS ES MUY IMPORTANTE, ASÍ QUE, NO OLVIDES PONER UNO QUE SEA INTERESANTE Y ADECUADO PARA TU TESIS

A Thesis submitted by Amy Wong for the degree of Doctor of Philosophy
in the Mars University

Supervised by:
Hubert J. Farnsworth

Índice general

Índice de figuras

1 Resumen

Hace décadas comunicarse mediante un dispositivo que estuviera conectado a una red cableada y tras mucha espera resultaba algo fantástico. Hoy en día tenemos la posibilidad de realizar un gesto en cualquier lugar y ponernos en contacto con alguien a cientos o miles de kilómetros. En este sentido, las comunicaciones han evolucionado de una forma increíble. La seguridad en estas comunicaciones basada en la criptografía es un elemento primordial para salvaguardar la privacidad de los usuarios y la del contenido.

La criptografía no se ha quedado atrás y durante el último siglo su devenir ha seguido el mismo camino. Desde los métodos más primitivos basados en cambiar una letra por la anexa; hasta complejos sistemas criptológicos (criptosistemas) que aprovechan ciertas propiedades matemáticas para preservar niveles de seguridad elevados con la necesidad de menos recursos (computacionales y de almacenamiento). Optimizar los recursos es esencial para ser competitivo y para ello la metodología de criptografía basada en curvas elípticas reduce exponencialmente la cantidad de almacenamiento necesaria respecto a otros algoritmos. De la mano va la tecnología NFC (*Near Field Comunication*), la cual ha simplificado los dispositivos de comunicación a algo tan pequeño y barato que ha conquistado el planeta en forma de multitud de aplicaciones.

En este Trabajo Fin de Grado (TFG a partir de ahora), comprenderemos la posibilidad de elaborar sistemas seguros con dispositivos de comunicación de bajo coste y criptología avanzada. A su vez, se implementará una aplicación para *smartphones* que, gracias a algorítmos avanzados de criptografía, permitirán a un usuario crear y utilizar un *tag* NFC como dispositivo de autenticación de alta seguridad en un sistema ficticio.

Palabras clave: *Criptografía, Curvas elípticas, NFC, autenticación.*

Abstract

Hace décadas comunicarse mediante un dispositivo que estuviera conectado a una red cableada y tras mucha espera resultaba algo fantástico. Hoy en día tenemos la posibilidad de realizar un gesto en cualquier lugar y ponernos en contacto con alguien a cientos o miles de kilómetros. En este sentido, las comunicaciones han evolucionado de una forma increíble. La seguridad en estas comunicaciones basada en la criptografía es un elemento primordial para salvaguardar la privacidad de los usuarios y la del contenido.

La criptografía no se ha quedado atrás y durante el último siglo su devenir ha seguido el mismo camino. Desde los métodos más primitivos basados en cambiar una letra por la anexa; hasta complejos sistemas criptológicos (criptosistemas) que aprovechan ciertas propiedades matemáticas para preservar niveles de seguridad elevados con la necesidad de menos recursos (computacionales y de almacenamiento). Optimizar los recursos es esencial para ser competitivo y para ello la metodología de criptografía basada en curvas elípticas reduce exponencialmente la cantidad de almacenamiento necesaria respecto a otros algoritmos. De la mano va la tecnología NFC (*Near Field Comunication*), la cual ha simplificado los dispositivos de comunicación a algo tan pequeño y barato que ha conquistado el planeta en forma de multitud de aplicaciones.

En este Trabajo Fin de Grado (TFG a partir de ahora), comprenderemos la posibilidad de elaborar sistemas seguros con dispositivos de comunicación de bajo coste y criptología avanzada. A su vez, se implementará una aplicación para *smartphones* que, gracias a algorítmos avanzados de criptografía, permitirán a un usuario crear y utilizar un *tag* NFC como dispositivo de autenticación de alta seguridad en un sistema ficticio.

Keywords: *Cryptography, elliptic curves, NFC, authentication.*

2 Introducción

Cuando una persona envía un mensaje a un destinatario con información que considera comprometida o personal, pretende realizarlo con el mínimo riesgo de que dicho mensaje llegue de forma alterada y que sea al destinatario indicado. Además, éste quiere que el canal sea seguro y que nadie más intercepte la información; y si ocurriese tal caso, que personas ajenas no sean capaces de interpretar el mensaje y usarlo en su contra de forma perjudicial -o simplemente no desea difundir la información a alguien que no sea el destinatario-. También es evidente la necesidad de sistemas que eviten de la mejor forma posible la suplantación de usuarios; apoyándose en la criptografía, la autentificación resulta indespensable.

Existe la consideración generalizada que aquellos elementos más seguros a la hora de identificar y autenticar a un usuario de un sistema son aquellos que implican el uso de parámetros biométricos. Por ejemplo, el algoritmo para el reconocimiento del iris patentado por el investigador de la universidad de Cambridge, John Daugman, se basa en el iris como elemento único e intransferible para cada persona [11]. De forma análoga se utilizan algoritmos basados en la estructura facial o huellas dactilares. Por otra parte, Manuel Lucena López, doctor en informática de la universidad de Jaén, asegura en su publicación [8] que esta clase de requerimientos biométricos se pueden reducir a problemas de autenticación basada en dispositivos. Es decir, una tarjeta puede actuar con el mismo compromiso de seguridad que dichos elementos biológicos.

Al igual, en los sistemas criptográficos (criptosistemas), la implementación más segura suele ser la menos eficiente. En la actualidad, la competencia hace de la optimización un objetivo en el que se invierten millones de capital. En el campo de la automoción competitiva, un incremento de la velocidad punta de 3km/h puede implicar reducir el tiempo de un competidor en unas décimas vitales que podrían suponer la diferencia entre ser primero o ser segundo. Dentro de la criptología y la seguridad de comunicaciones también está afectado por este hecho y no está exento de la voracidad por optimizar el trinomio de recursos, tiempo y resultados. Dentro de este contexto la tecnología tan asequible co-

mo NFC (*Near Field Comunication*), - dispositivos para la comunicación de información empleando radiofrecuencia de corto alcance- que ha conquistado numerosos ámbitos, será el soporte de estudio de este Trabajo de Fin de Grado (TFG a partir de ahora) como dispositivo de autenticación.

Como suele ser habitual, un dispositivo 'barato' tiene ciertas desventajas. Respecto a la seguridad criptográfica con NFC el mayor inconveniente suele ser el tamaño de almacenamiento - inferior a 500 bits generalmente-. Este problema implica utilizar criptosistemas que puedan trabajar con tamaños reducidos de información sin comprometer la seguridad. La evolución en la criptografía es considerable desde que en la Segunda Guerra Mundial el proyecto ULTRA tratara de descifrar los mensajes del ejército alemán; quienes se encontraban a la vanguardia de la criptografía.

3

APP: Autenticación en un sistema ficticio

3.1. Introducción

Anteriormente se han explicado los conocimientos y términos generales relacionados con la seguridad en la autenticidad NFC basada en criptología con curvas elípticas. A continuación se muestra la aplicación de dichos conocimientos en un proyecto software experimental. El objetivo es demostrar la capacidad de los dispositivos NFC para, de la mano de la criptografía con curvas elípticas, llegar a desarrollar un sistema de autenticación óptimo y fiable.

Tanto los nombres, librerías, herramientas, así como el resto del material utilizado se describirán a continuación. A su vez, siguiendo un estándar de desarrollo software basado en metodologías ágiles, se mostrará la utilizada para éste proyecto. Para ello, el autor y director de este TFG (Fidel Abascal y Domingo Gómez) hemos actuado y ejercido tanto de cliente como de contratado para el desarrollo de la aplicación.

Dentro de un ámbito ficticio, una empresa llamada **Alpha - Consultora S.A.**[*], nueva potencia local dentro del campo de la seguridad bancaria, que ha cosechado unos excelentes resultados a lo largo de sus 2 años de existencia. Cuenta con más de 40 trabajadores y su crecimiento y expansión es notoria. Tanto es el éxito de esta empresa que, para dar cabida a su plantilla, ha decidido trasladarse a una nueva sede más moderna, amplia y mejor ubicada. La empresa, antes de instalarse en la nueva sede, decide contratar a unos expertos en seguridad para gestionar el control de accesos mediante un sistema de tarjetas y lectores en las entradas; teniendo en cuenta una inversión mínima pero garantizando un alto grado de seguridad.

Tras buscar incesantemente recurren a la empresa **F-NFC**. Una vez realizado el estudio por parte de F-NFC, se pone en consonancia un acuerdo para elaborar una aplicación que

[*]Cualquier similitud con la realidad es mera coincidencia

genere información que autentifique a un usuario de la empresa *Alpha* y sea reconocido de forma unívoca para permitir su acceso a la sede. La infraestructura de la empresa propietaria de la nueva sede corresponde a la figura 3.1.

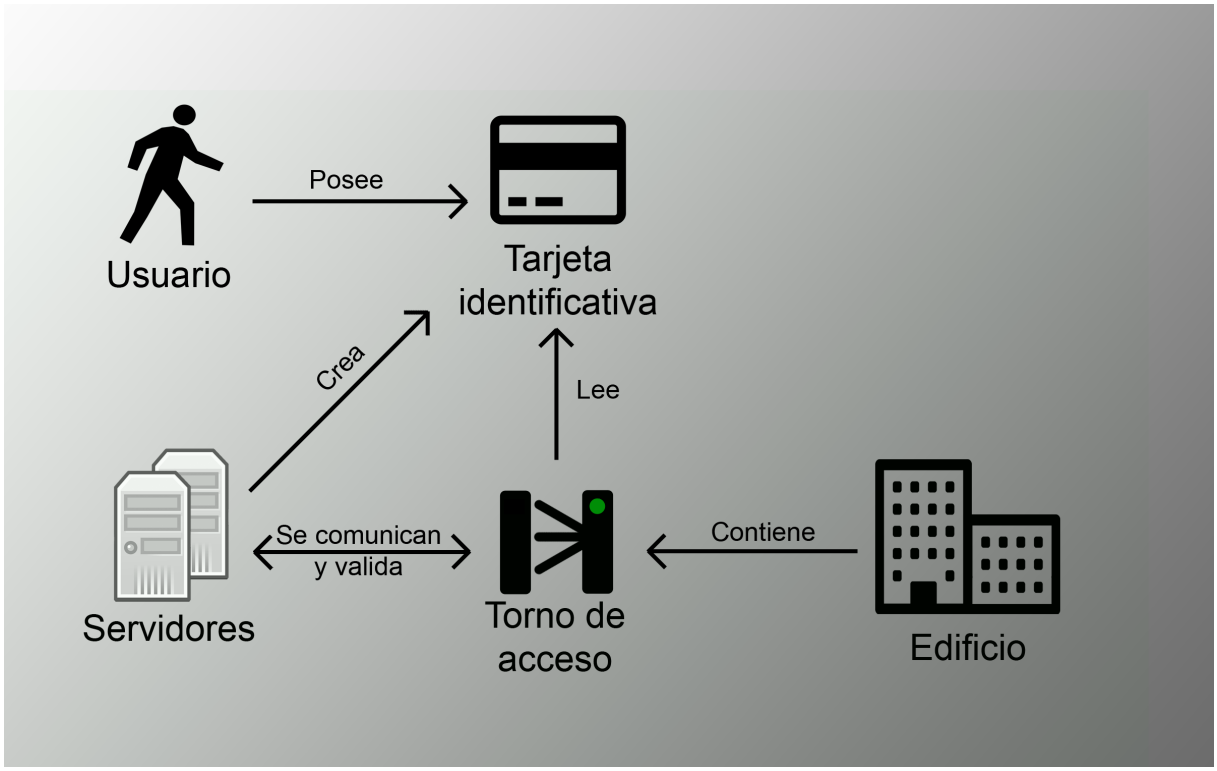

Figura 3.1: Infraestructura del sistema ficticio.

Los detalles de implementación de la aplicación seguirán un objetivo didáctico y experimental que cumplirán los requerimientos de la situación propuesta; adecuándose a la carencia real de la infraestructura anteriormente mencionada. Se explicará en las secciones siguientes en detalle todos los puntos implicados en la consecución de este objetivo. Más concretamente en el apartado de escenario de la aplicación 3.4.

3.2. Material utilizado

Para el desarrollo del proyecto se ha utilizado, ante todo, software de carácter libre junto a imágenes, textos, estructuras y contenido sin restricciones de uso. Ya sea debido al tipo de licencia de cada elemento o por ser de autoría propia.

El desarrollo se ha realizado en el lenguaje de programación *Java* con el kit de desarrollo *Java* (JDK) 1.8.65 (*Java 8 update 65*) de *Oracle Corporation* [1].

El entorno de desarrollo integrado o *IDE* de la aplicación es el oficial de Google para el desarrollo para dispositivos *Android*: *Android Studio*, versión 1.5.1 [5]. Este programa provee las herramientas básicas de desarrollo; entre ellas, un administrador de los kit de desarrollo o *SDKs* para las diferentes versiones y varios elementos descritos a continuación:

- Plataformas SDK
  - API 22: Para la versión Android 5.1.1.
  - API 21: Para la versión Android 5.0.1.
- Herramientas SDK
  - Android Build Tools : Para la construcción de la aplicación.
  - Android SDK Platform Tools v23.1: Soporte para el desarrollo.
  - Repositorio de ayuda Android, rev 30.
  - Libreria de ayuda Android, rev 23.2.1 : Ayudas en la retrocompatibilidad de elementos de interfaz de usuario.
  - Google USB Driver, rev 11 : Conexión entre el servicio de ejecución de la aplicación y los dispositivos USB.
  - Intel x86 HAXM, rev 6.0.1 : Aceleración *hardware* para la emulación.

Estos componentes de *Android Studio* hacen posible el desarrollo de la aplicación objetivo. Este programa, con carencias notorias en ciertos apartados, ha hecho complicado, de cierta forma, la selección de componentes a instalar, versiones y etcétera debido a diversos motivos de compatibilidades de librerías y actualizaciones desfasadas entre los componentes y el propio IDE.

La esencia de la aplicación reside en la criptografía mediante curvas elípticas. Para la implementación de ello ha sido necesario utilizar una librería externa llamada *Bouncy Castle* [10] versión 1.54. Dicha librería suple las deficiencias de la implementación base de la propia API (*Application Programming Interface*) de *Java*. La cual tiene limitaciones claras a la hora de la generar curvas elípticas. Gracias a ésta librería se ha podido realizar la parte crítica de la aplicación con una mejora de rendimiento notoria si hubiera que haber utilizado la API de *Java*.

Respecto al almacenaje de datos se ha optado por utilizar una pequeña base de datos en *SQLite* [12] descrita más adelante. Para el almacenamiento de unos pequeños registros que utilizará la aplicación. El uso de una base de datos de mayor capacidad y funcionalidades no se ha contemplado factible.

En cuanto a los elementos gráficos de la aplicación, un alto porcentaje son de elaboración propia mediante programas de edición de imágenes. El resto son de libre uso comercial. La iconografía de la aplicación es autoría de *Google Inc.* [6]. Dichos iconos han de ser vectoriales debido a la optimización del tratamiento de imágenes y su renderizado, por lo que en este aspecto, *Google* provee estos iconos en formato *SVG* y *PNG*; también *Android Studio* de forma nativa pero no actualizada. A la hora de incluir estos elementos externos se ha transformado las descripciones vectoriales *SVG* (*Scalable Vector Graphics*) en formato *XML* (*eXtensible Markup Language*) interpretable de forma sencilla por *Android Studio*. En el apartado de diseño y aspecto de la aplicación 3.5 se comenta en detalle el resto de la disposición, motivación y elaboración gráfica de la aplicación.

La API de objetivo del proyecto *Android* ha sido la número 22. Desarrollada para la versión 5.1. (*LOLLIPOP MR1*). Se ha decidido utilizar esta esta API debido a las mejoras sustanciales en cuanto al trabajo del adaptador NFC implementadas desde la versión 5.0 [3] y mejoradas en ésta [4].

Para el testado de la aplicación *Android Studio* dispone de la tecnología *AVD* para la virtualización de dispositivos *Android*. Sin embargo, el rendimiento es pobre en comparación con el testeo y *debug* en un dispositivo físico. Por lo que se ha utilizado un dispositivo *Android smartphone One Plus One* de la compañía americana *Never Settle*, el cuál dispone de la versión *Android* 5.1.1 y *Cyanogen OS* 12.1.1 en el momento de la elaboración de la aplicación.

Figura 3.2: Smartphone One Plus One - Never Settle

Por último, el proyecto ha necesitado de dos elementos físicos principales: el dispositivo *Android* mencionado anteriormente y de tarjetas NFC. Debido a la carencia de un presupuesto, se ha optado por utilizar etiquetas adesibles (desde ahora NFC-T) de bajo coste por etiqueta. Se trata del chip *NTAG213* que siguen el estándar ISO 14443-3 [7]. Las características de estas etiquetas son las siguientes:

- Tipo de etiqueta : ISO 14443-3A
- Descripción : NXP MIFARE Ultralight (Ultralight C) - NTAG213
- Tecnología : NfcA, Ndef, MifareUltralight
- Formato de datos: NFC Forum Type 2
- Diámetro: 25 mm
- Identificadores del chip
    - Valor ATQA: 0x0044

- Valor SAK: 0x00
- Firma: NXP Public Key

▪ Tamaños y capacidad

- Memoria: 45 páginas de 4bytes por página (180 bytes)
- Tamaño: 137 bytes
- *UID* (Identificador del contenido): 7 bytes [2]
  - *Byte 7*: Valor *UTF-8*, codificación
  - *Byte 6*: Valor *0*, reservado para uso futuro
  - *Byte 5-0*: Tamaño del código del lenguaje *IANA*
- Tamaño utilizable: 130 bytes (Tamaño menos *UID*)

Estas etiquetas se pueden adherir en una superficie que le haga de soporte. Por ejemplo, se podría plastificar junto a dos tapas que cubran el chip y tener la apariencia de una tarjeta común. Su apariencia es la siguiente:

Figura 3.3: NFC Tag - NTAG213

Hubiera sido preferible utilizar chips *MIFARE* [9] de alta capacidad y mayores funcionalidades como los *MIFARE classic* 1K y 4K del productor *NXP*. Estos chips están implementados en una enorme cantidad de aplicaciones en todo el mundo, un ejemplo claro de su uso son el de las tarjetas de crédito y la mayoría de chips NFC actuales que impliquen la necesidad de encriptación (RSA comúnmente) y seguridad. En estas tarjetas es realmente complicado acceder a su contenido ya que se precisan ciertas claves para la lectura y decodificación. Sin embargo, en las utilizadas en este proyecto se escribe en texto plano (siguiendo el objetivo didáctico); en el apartado de seguridad y criptología 3.6 se explica cómo afectaría esta carencia al sistema final.

Todos los elementos descritos en este apartado conforman lo necesario para simular la estructura descrita en la figura 3.1 y la implementada definida en el apartado 3.4.

3.3. Metodología

Metodología ágil basada en iteracciones continuas debido a la comunicación continua con el cliente...

Diagrama gantz

Figura 3.4: Diagrama Gantt - Subdivisión de elementos de la aplicación para su desarrollo

3.4. Escenario

La idea principal del escenario de la aplicación se ha comentado en el aparatado 3.1, en donde se comenta que el objetivo de la aplicación es meramente didáctico y experimental. Alejándose de los modelos pragmáticos del desarrollo profesional.

La complejidad añadida de implementar un sistema cercano a la realidad aplicaría un coste elevado de recursos sin tener relevancia notoria en la finalidad comentada. Elementos tales como: servidores, *WebServices*, *frameworks* de desarrollo, certificación, optimización, etcétera. Dado que la esencia de este TFG se centra en el elemento teórico y didáctico de la criptología en curvas elípticas, la creación de una aplicación de carácter altamente profesional le añadiría beneficios nimios. Los cuales no compensan la complejidad agregada, por lo que se han realizado labores de simulación y descarte de las partes que se han considerado prescindibles.

La arquitectura de la aplicación representada en la figura 3.1 muestra un escenario típico que da pie a la implementación de este tipo de seguridad. Dentro de este proyecto virtual se dispone de un edificio el cuál posee tornos o puertas de acceso. Estas puertas son capaces de leer el contenido de las tarjetas NFC de cada usuario del sistema. El contenido de las tarjetas se transmite a los servidores de validación de la empresa (sin la necesidad de que se encuentren físicamente dentro del mismo edificio). Los servidores validarán la información recogida en el torno de acceso y validará o no el contenido. Si resulta validado el torno recogerá de los servidores la nueva información a escribir en la tarjeta para hacer válida el paso la próxima vez. Finalmente, el usuario por medio de ésta tarjeta unipersonal podrá acceder al edificio autenticándose en la entrada.

Descrito el escenario virtual, es necesario comentar el que éste proyecto se ha realizado. Contando con los elementos de 3.2 se agruparán los funcionalidades del escenario virtual en el dispositivo *Android*. Por lo tanto, no habrá conexiones a servidores externos y toda la estructura se compondrá únicamente del dispositivo *Android* y las tarjetas NFC. A su vez, contará con las siguientes funciones que simulan labores del escenario virtual:

- Información sobre los usuarios del sistema: En lugar de contar con un acceso a una base de datos que recoja la información, se utiliza una pequeña base de datos dentro del dispositivo que contiene la información básica de los usuarios (identificador y nombre del usuario).
- Información del sistema de encriptación: El dispositivo también contiene la información básica del sistema criptológico implementado (labor de información de servidores).
- Validación: Tras leer el contenido de la tarjeta NFC, denegará o validará la información obtenida (labor de validación y acceso).
- Labores de administración del sistema: El dispositivo será capaz de restaurar los valores por defecto del sistema, junto a la información inicial. También permitirá crear nuevas definiciones del sistema de seguridad. Por último, también asignará usuarios al sistema de seguridad que no se encuentren dentro (labor de creación de tarjetas).

Todos los elementos de información se describen en el apartado 3.8 sobre la base de datos de la aplicación; y las funcionalidades del sistema dentro del apartado 3.7 de requisitos y funcionalidades.

3.5. Requisitos y funcionalidades

La toma de requisitos, especificaciones y funcionalidades de la aplicación real, que cumple con los simulados en el contexto virtual descrito en la introducción 3.1, se ha llevado a cabo mediante constantes reuniones.

Siguiendo la metodología ágil basada en iteracciones comentada en el apartado 3.3, desde el primer momento se ha ido mostrando el avance del proyecto al supuesto cliente. Éste ha validado según sus requerimientos iniciales o ha concretado cambios que se adecuen en el marco de las funcionalidades principales. Iteracción a iteracción se ha ido implementando los pasos siguiendo hitos a validar. El diagrama *Gantt* mostrado en la figura **??** muestra en detalle la división de las tareas y apartados del proyecto realizado en este TFG.

Los casos de uso de la aplicación se muestran a continuación :

–

3.6. Diseño y aspecto

iconografía vectorial [6] Material design intento de material desing (iconos, sombras, disposición de elementos, etcétera Colores que dan seguridad

3.7. Seguridad y criptología

hablar de qué ocurre al tener texto plano en las nfc-t en vez de las mifare classic

3.8. Base de datos

Tablas, contenido por defecto.

Bibliografía

[1] Oracle Corporation. Software java.

[2] NFC Forum. Nfc forum specifications.

[3] Google Inc. Android apis - about version 5.0.

[4] Google Inc. Android apis - about version 5.1.

[5] Google Inc. Android studio - the official ide for android.

[6] Google Inc. Material design icons.

[7] ISO/IEC. Iso/iec standard 14443-3.

[8] Manuel José Lucena. Criptografía y seguridad en computadores. *versión 0.7*, 5, 1999.

[9] MIFARE. Mifare ic - contactless smart cards.

[10] Legion of the Bouncy Castle Inc. Bouncy castle - api criptográfica.

[11] Mohamad Ramli, Nurul Akmar, Muhammad Saufi Kamarudin, and Ariffuddin Joret. Iris recognition for personal identification. 2008.

[12] SQLite. Sqlite - public domain embedded sql database engine.