[[1]](#footnote-1)

RSA Integer Factorization Attacks, a Comparative Analysis

**Oscar  
Jessid  
Camilo  
David**

Resumen

This short paper contains a general description about cyber-attacks classification, this classification seeks to define a satisfactory domain that allows an adequate information management, which includes data treatment and storage.

*keywords*—Cyber-Attack, RSA, cryptography, factorization/factoring, Information security.

# INTRODUCCIÓN

I

nformation technologies, had become the principal axis of many basic aspects on daily life. Continuously an information chain is fed, in which each of its links has so many relation between them that the dangers of exposed private information are ignored. One of the main objectivs of cryptography is to achieve a high degree of trust, so the users of a particular service can have security for the data they bring, and a degree of privacy approved by themselves: keep the required secret.

Even when many countries

Aunque muchos países manejan ciertas políticas de seguridad nacional para proteger la información privada, tanto de los sectores estatales como de la población civil, la responsabilidad de la seguridad informática no solo puede recaer sobre ellos. Es necesario que tanto los entes privados y la ciudadanía tomen recaudos pertinentes, en otras palabras, que no se delegue como una responsabilidad estatal [1].

Este artículo busca mostrar las principales formas que existen de ciberataques, que tiene objetivo lograr una identificación de los peligros reales a los cuales se pueden ver enfrentada la información personal de alguien. Al obtener la categorización, se podrá observar que uno de las formas de romper los protocolos de seguridad, es encontrar una factorización adecuada para N en el algoritmo RSA, se implementaran alguno de estos algoritmos y se realizará un análisis de sus tiempos de ejecución.

# Formas Comunes de Ciberataques

Se puede denominar ciberataque a cualquier actividad relacionada con cualquiera de los métodos diseñados para romper la seguridad informática. Existen varias formas de categorizar los ciberataques, la siguiente esa una clasificación muy intuitiva que busca hacerse la idea de los principales peligros a los cuales está expuesta la información. Por otra parte, se definen 5 características para todo ciberataque [2]:

* Actores: Al menos dos actores están involucrados en un ciberataque. El termino adversario no suele usarse, pero si se idéntica los roles de defensa y ataque.
* Assets targeted: Información sobre el sistema informático y redes.
* Motivación: Con relación a la información: espía, accesos no autorizado, robo, seguridad nacional, propaganda, etc.
* Effect on targeted assets: Con relación a la información: alteración, borrado, corrupción, fraude o destrucción.
* Duración: Tiempo que dura el ciberataque.

## Ataques de negación del servicio (DDoS):

Con un nombre muy intuitivo, este tipo de ataques tiene como característica principal, hacer un alto volumen de solicitudes con el fin de colgar algún servicio. Sin embargo, es solo un ataque de bloqueo, generalmente no se busca romper ningún protocolo de seguridad, solamente saturar algún servicio en particular para hacer que caiga y no se encuentre disponible durante cierto tiempo. Para este tipo de ataques suelen usarse paquetes modificados con IPs falsas para evitar la ubicación del origen, o se hacen uso de troyanos para controlar el nacimiento del ataque remotamente [3]. Existen tres tipos de ataques por DDoS:

* Consumo de recursos: El atacante intenta consumir los recursos del servidor hasta agotarlos.
* Alteración de la configuración: Se intenta modificar la información de hardware.
* Alteración física de los equipos: Destruyendo físicamente hardware prioritario para la utilización de un servicio.

## Ataques a redes inalámbricas:

Para tener acceso a una red cableada es indispensable contar con acceso a esa red física, lo que limita cualquier intento de tener accesos al canal de comunicación. Al tener una red que no usa cableado, aumenta la inseguridad considerablemente. No solo facilita escuchar la información que se transmite, sino también es probable que se puedan inyectar nuevos paquetes o modificar los ya existentes.

Las redes inalámbricas tienen dos problemas en concreto. Los puntos ocultos suelen ser un gran problema, puesto que generalmente los empleados suelen instalar sus propios puntos de acceso dentro de las maquinas por cuestiones de comodidad. Este tipo de instalaciones pueden crear huecos enormes en la red. El otro problema importante, es la falsificación de los puntos de acceso. Es normal que se instalen puntos de accesos que difundan su propia SSID para permitir que cualquiera pueda conectarse a la red o inducir a conectarse a una red en concreto [4].

## Ingeniería social:

La idea de este enfoque es encontrar alguna contraseña en específico basándose en los datos personales de la persona que administra cierta sesión. Se recolecta datos que son públicos, y mediante técnicas de inteligencia artificial, para este caso minería de datos, se encuentra un diccionario con las posibles contraseñas que pudo haber escogido la administración basado en su información personal.

## Ataques basados en factorización de N en RSA:

# Algoritmos de Factorización

## Fermat:

Si se tiene un *N* el cual es difícil de factorizar, eso implica que los *p* y *q* escogidos tienen un tamaño similar en bits. Si *p* y *q* son muy cercanos es posible usar el método de factorización de Fermat. Se puede representar *N* de la siguiente manera:

(1)

Donde, y . Al despejar *y* se obtiene lo siguiente:

(2)

En base a lo anterior el algoritmo de factorización de Fermat es el siguiente:

1. Entrada: *N,* inicializar los valores:
2. Si , ir al paso 4.

Sino,

1. Si , ir al paso 2.

Sino, ir al paso 5.

1. Termina el algoritmo.

Si , con y . Cuando , el algoritmo de factorización de Fermat puede encontrar los factores de N eficientemente.

## Factorizacion Pollard y Williams:

Los números primos de RSA deben ser escogidos con la propiedad que y , tienen almenos un factor primo mayor a , *p* puede encontrarse eficientemente usando las factorizaciones de Pollard () y Williams (), el algoritmo es el siguiente:

1. Inicialización, escoger aleatoriamente.

Escoger un entero positivo *k,* de la siguiente forma:

Un valor grande de B ayudará a encontrar un mejor resultado, pero aumentará significativamente el tiempo que toma encontrarlo.

1. Calcular,
2. Calcular
3. Si , *f* es un factor no trivial de *N*, ir al paso 6.
4. Escoger un nuevo *a* y repetir desde el paso 2.
5. Termina el algoritmo.

## Lenstra´s Elliptic Curve Method (ECM):

## Quadratic Sieve Attack:

Given 2 numbers X y Y:

# Conclusiones

Referencias

[1] M. Chertoff, US Departman of Homeland Security, The Cybersecurity Challenge, Regulation & Governance 2, pág. 480 - 484, 2008.

[2] M. Kadivar, Copenhagen School, Cyber-Attack Attributes, Technology Innovation Managenment Review, November 2008.

[3] A. Reshamwala and Dr. S. Mahajan, Prediction of DoS Attack Sequences, International Conference on Communication, Information & Computing Technology, Mumbai, India, 2012.

[4] I.P. Mavridis and Ph. Mylonas, Real-life Paradigms of Wireless Network Security Attacks, Panhellenic Conference on Informatics, Greece, 2011.

[?] S. Y. Yan, Cryptanalytic Attacks on RSA, Cap. 3, 2008.

1. [↑](#footnote-ref-1)