INSTITUTO POLITECNICO NACIONAL

LUIS ENRIQUE ERRO SOLER

ALUMNOS:

- ABARCA DE LA CRUZ SHADANI ELIZABETH
- CIRA BLANCAS PAULINA MICHELLE
- NERI GARCIA BRYAN ISRAEL
- PALACIOS MENDOZA JIRETH SINAI
- RESENDIZ RANGEL EMILIO
- ROJO BELTRAN AXEL
- SANTIN VILLANUEVA LAURA YARITH
- VELAZQUEZ VELES ISAAC

PROFESOR: JORGE OSCAR ROSALES

Proyecto Aula

GRUPO: 3IM5

MATERIA: GEOMETRIA ANALITICA

TURNO: MATUTINO

Resolución de Problemas

introducción

Matemáticas es una base importante para muchos dominios y disciplinas. Del mismo modo, las matemáticas son las bases fundamentales en la informática. Como desarrollador de software, uno debe ser bueno para tratar con el sistema numérico y la geometría. Lidiar con los problemas relacionados con la seguridad cibernética puede ser realmente fácil si tienes un buen control sobre las Matemáticas y será una tarea un poco más fácil. Entender los problemas, son necesarios para estar confiados al realizar una actividad electrónica en nuestros computadores. Para los matemáticos, los números primos son un reto. Para los informáticos, pueden serlo todo. Los usos inseguros por parte del usuario, un sistema de seguridad puede fallar de dos maneras: por el estándar matemático en el que se basa; o por cómo se aplica este estándar a un programa concreto. En el primer caso el problema es puramente matemático. Los estándares de cifrado se basan en claves por problemas sin resolver. En cambio, construir una aplicación práctica, el diseño y la puesta en marcha de un programa de seguridad, tradicionalmente ha quedado como un método para la resolución de problemas. Expertos creen que los retos en seguridad en el futuro, exigen más colaboración entre matemáticos e ingenieros: nuevas matemáticas también para los desarrollos.

objetivos

El objetivo principal es el de permitir:

- Escuchar, ver y discutir las opiniones de los usuarios.
- Compartir información relevante del tema.
- Poner en práctica los retos informáticos sobre los cuales se manejen un sistema matemático.
- Contribuir a un mejor desarrollo dentro de los adolescentes.
- Intercambio de información
- Compartir conocimiento.
- Encontrar soluciones a los problemas de seguridad cibernética aplicando conocimientos matemáticos.
- Buscar problemas y solucionarlo en ayuda a una formula.
- Un estudio y trabajo en equipo.
- En base a un análisis matemático encontrar una solución para un problema.

Modelo Matemático

• Las Matemáticas ofrecen herramientas que permiten analizar, evaluar y gestionar amenazas con el objetivo de minimizar el impacto de las mismas. Nos concentramos en temas que relacionen las matemáticas junto a una ciberseguridad es por ello que extendimos la investigación tomando como referencia el uso de técnicas criptográficas tiene como propósito prevenir algunas faltas de seguridad en un sistema computacional, que actualmente es más utilizado.

Modelos matemáticos para observar la propagación de malware.

La Criptografía es una rama de las matemáticas que, al orientarse al mundo de los mensajes digitales, proporciona las herramientas idóneas para solucionar los problemas relacionados con la autenticidad y la confiabilidad.

La seguridad, en general, se considera como un aspecto de gran importancia en cualquier corporación que trabaje con sistemas computacionales. El hecho de que gran parte de actividades humanas sean cada vez más dependientes de los sistemas computarizados, hace que la seguridad sea aún más importante.

El esquema propuesto en RSA se explica así:

Mediante un programa de cómputo cualquier persona puede obtener un par de números, matemáticamente relacionados, a los que se denominan llaves. Una llave es un número de gran tamaño, que usted puede conceptualizar como un mensaje digital, como un archivo binario, o como una cadena de bits o bytes. Las llaves, públicas y privadas, tienen características matemáticas, su generación se produce siempre en parejas, y se relacionan de tal forma que, si dos llaves públicas son diferentes, entonces, las correspondientes llaves privadas son diferentes y viceversa. En otras palabras, si dos sujetos tienen llaves públicas diferentes, entonces sus llaves privadas son diferentes. La idea es que cada individuo genere un par de llaves: pública y privada. El individuo debe de mantener en secreto su llave privada, mientras que la llave pública la puede dar a conocer.

El proceso de autentificación se efectúa de la siguiente forma:

Dos puntos I y II mantienen comunicación, conociendo I la llave pública de II. Desde el punto II, se envía un documento firmado digitalmente y un criptograma asociado que sólo es posible hacerse utilizando su clave privada. Entonces I, utilizando la llave pública de II genera un criptograma reflejo, compara ambos criptogramas y, si son iguales, el documento es auténtico.
Si alguna parte del documento o parte de la firma se modifica, aunque sea ligeramente, entonces, el procedimiento de autentificación indicará que el documento no es auténtico. Si una llave pública autentifica un documento firmado, entonces el documento fue firmado con la correspondiente llave privada, es decir, si un individuo tiene asociada la llave pública que autentifica el documento, entonces, el documento fue efectivamente firmado por ese individuo.

Evolución en seis meses de las vulnerabilidades y los ataques

Time	Ataques	Vulnerabilidadades
0	100,00	1.000,00
1	500,00	1.500,02
2	1.100,0	2.250,04
3	2.000,0	3.375,10
4	3.350,1	5.062,73
5	5.375,2	7.594,25
6	8.412,9	11.391,66

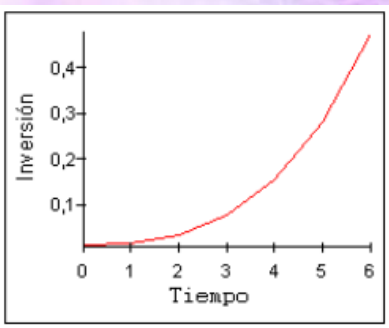
1 ANÁLISIS Y RESULTADOS El período de tiempo considerado en el modelo, estuvo comprendido de cero a seis meses con una periodicidad mensual. En primer lugar, se analizó el comportamiento de las vulnerabilidades, los ataques y la seguridad.

Comportamiento semestral

2 Se observa que el comportamiento de las vulnerabilidades sigue siendo mayor que los ataques, ya que se simuló el comportamiento con un factor de crecimiento acelerado de la información de 0.9, mientras que el factor de crecimiento normal de ataques fue de 0.4.

Comportamiento de los incidentes

Time	Nuevos_Incidentes	Incidentes_Conocidos
0	100,00	10,00
1	120,00	20,00
2	250,00	40,00
3	540,00	80,00
4	1.060,01	160,00
5	1.905,03	320,00
6	3.197,57	640,00



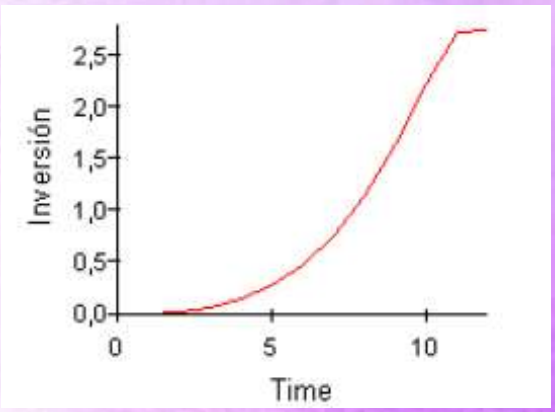
Tiempo	Inversión
0	0,015
1	0,018
2	0,0375
3	0,081
4	0,159
5	0,286
6	0,48

Diferencia de los nuevos incidentes frente a los incidentes conocidos.

3 Se presenta el comportamiento de los incidentes en donde es claro que los nuevos incidentes superan a los incidentes conocidos. El conocimiento por experiencia de incidentes no asegura la seguridad en la organización, la cual sigue siendo igual o más vulnerable.

El comportamiento de la inversión en seguridad

4 se presenta el comportamiento de la inversión en seguridad, la cual muestra que la organización se ve obligada a invertir continuamente.



Comportamiento de la inversión en 12 meses.

5 Se muestra que la inversión en seguridad se estabiliza a partir de los 12 meses y sigue siendo constante a medida que pasan los meses, posiblemente porque los incidentes conocidos superan a los incidentes nuevos.

6 Comportamiento de los incidentes.

Si las organizaciones no cuentan con alternativas que guíen los esfuerzos de protección, por más dinero que inviertan en seguridad nunca alcanzarán niveles de seguridad satisfactorios. Debido al alto costo de la seguridad de la información y al hecho de que una segura por completo es una meta casi imposible de alcanzar. Aprender a determinar la cantidad de inversión en seguridad tomando como referencia diversos factores.

La seguridad informática en tiempos de COVID-19

Actualmente vivimos una situación dificil causada por la pandemia. Hoy en día no solo somos vulnerables en cuanto a la salud, también somos víctimas fáciles para los ciberataques, y más en estos momentos que nos encontramos en casa.
Muchas personas desconocen el riesgo que puede provocar el manejo de medios digitales, es por ello que son los más vulnerables a los fraudes realizados a través de internet.
A pesar de que con el paso de los años el uso de internet se ha generalizado en todos los sectores de la población, no todos tienen el mismo conocimiento sobre los riesgos asociados a un mundo digitalizado.
En los últimos años, y más especialmente en los últimos días, se ha incrementado notoriamente los fraudes cibernéticos. Es por ello que existen unas medidas para la prevención de estos ataques:

- Comprender que solo se tiene que utilizar un dispositivo propio o en el que confíen para realizar cualquier tipo de actividad.
- Evitar guardar información confidencial comprometida en cualquier dispositivo, como puedan ser las contraseñas, números PIN, imágenes comprometidas u otros datos sensibles.
- Evitar colocar información sensible en un mensaje de texto o un correo electrónico, ya que los hackers conocen esas tácticas.
- No instalar aplicaciones adicionales que no se sabe su procedencia y sin antes consultarlo con otra persona y verificar de que se trata y cuál es su finalidad.
- Siempre conectarse a una red segura y de confianza y no desde una red pública.
- Cerrar las sesiones inmediatamente después de utilizarlas en cualquier dispositivo.
- Hacer caso omiso de correos electrónicos sospechosos y no abrir enlaces de ningún tipo si no se conoce con exactitud el destino.

Para una empresa de antivirus el costo de trabajo y su colocación por antivirus es de $500 y los costos fijos son de $2000 al día. Si se vende cada antivirus en $1000. ¿Cuántos antivirus se deberán colocar y vender cada día con objetivo de garantizar que la empresa se mantenga en el punto de equilibrio?

X= número de antivirus

Y= dinero= $

C.V. = $500 C/U

C.F.= $2000

PRECIO= $1000 C/U

X=?

UTILIDAD= 0

ECUACION COSTO Y=500X+2000
INGRESO Y=1000X
UTILIDAD Y= 1000X-(500X+2000)
ECUACION UTILIDAD Y=500X-2000
500X-2000=0
X= 2000/ 500
X= 4
Y= 500 (4) +2000= 4000
Y= 1000 (4) = 4000

Supóngase que el costo total diario (en dólares) de producir x antivirus está dado por: Y= 3.5x +400

a) Si cada antivirus se vende a $6. ¿Cuál es el punto de equilibrio?
   COSTO TOTAL
   Y= 3.5x +400
   INGRESO
   Y= 6
   UTILIDAD
   Y= 6x-(3.5x+400)

   Y= 400/2.5
   Y=160

b) Si el precio incrementa a $7 por antivirus ¿Cuál es el nuevo punto de equilibrio?

X= 7x- (3.5x +400)
X= 3.5x +400=0
X= 400/3.5
X= 114

Si se sabe que al menos 200 antivirus pueden venderse al día. ¿Qué precio deberá fijarse con el objeto de garantizar que haya perdidas?

Y=3.5 (200) + 400 = 1100
PRECIO= 1100/ 200
Y= 5.5 x

Referencias

Gil Vera, Víctor Daniel; Gil Vera, Juan Carlos. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. 07/01/2021, de Universidad Tecnológica de Pereira Colombia Sitio web: https://www.redalyc.org/pdf/849/84953103011.pdf

José Adán Ascencio Díaz. (2020). La seguridad informática en tiempos de COVID-19. 07/01/2021, de Soporte Técnico Data Warden Sitio web: https://datawarden.com/new/la-seguridad-informatica-en-tiempos-de-covid-19/

EducacionIT. (2018). ¿Cuál es la verdadera importancia de las matemáticas para la ingeniería de software?. 07/01/2021, de Programador Profesional Sitio web: https://blog.educacionit.com/2018/08/27/cual-es-la-verdadera-importancia-de-las-matematicas-para-la-ingenieria-de-software/

Ing. Yran Marrero . (2003). La Criptografía como elemento de la seguridad informática. 07/01/2021, de SCIELO Sitio web: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012