UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

FACULTAD DE PRODUCCIÓN Y SERVICIOS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SEGURIDAD INFORMATICA

TENDENCIAS EN CIBERSEGURIDAD, MASKED CIRCUIT Y CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM (CAVP)

INTEGRANTES:

- Cozco Mauri Yoset

DOCENTE: LUCY ANGELA DELGADO BARRA

AREQUIPA – PERÚ
2023

Masked circuit

Introducción
En el ámbito de la seguridad informática, la protección contra ataques de canales laterales es de vital importancia. Estos ataques, que explotan la información obtenida de la implementación física de un sistema informático, pueden comprometer la seguridad de los sistemas criptográficos. Una medida de seguridad efectiva contra estos ataques es el uso de circuitos enmascarados. Este trabajo tiene como objetivo investigar los conceptos y principios del circuito enmascarado, los métodos y herramientas para su evaluación, y sus aplicaciones y casos de uso.

Análisis de canales laterales en criptografía
Los canales laterales son canales de información no intencionados que pueden ser explotados para obtener información sobre las claves criptográficas. Estos canales pueden ser causados por fugas de información en el hardware o software utilizado para realizar operaciones criptográficas. Los tipos comunes de ataques de canales laterales incluyen el análisis de consumo de energía, el análisis de tiempo y el análisis electromagnético.

Conceptos y principios del circuito enmascarado
El circuito enmascarado es una técnica utilizada para proteger los sistemas criptográficos contra los ataques de canales laterales. Estos circuitos ocultan la información sensible durante las operaciones criptográficas mediante la adición de ruido aleatorio a las entradas del circuito. Las técnicas de enmascaramiento incluyen el enmascaramiento aleatorio y el enmascaramiento compartido.

Los circuitos enmascarados utilizan técnicas de enmascaramiento para proteger la información sensible durante las operaciones criptográficas. Una de estas técnicas es el enmascaramiento aleatorio, que añade ruido aleatorio a las entradas del circuito para ocultar la información sensible. Otra técnica es el enmascaramiento compartido, que divide la información sensible en varias partes y las procesa por separado para ocultar la información original.

Métodos y herramientas de evaluación del circuito enmascarado
La evaluación de circuitos enmascarados implica la medición de la resistencia del circuito a los ataques de canales laterales. Los métodos utilizados para evaluar la resistencia de un circuito enmascarado incluyen el análisis de correlación, el análisis de varianza y el análisis de componentes principales. Las herramientas de software y hardware utilizadas en la evaluación de fugas de información incluyen osciloscopios, analizadores de espectro y software de análisis estadístico.

Un estudio reciente publicado en ACM Transactions on Embedded Computing Systems propone un nuevo método para evaluar la resistencia de los circuitos enmascarados a los ataques de canales laterales. Este método, llamado "evaluación de la resistencia al canal lateral basada en la correlación cruzada", utiliza la correlación cruzada para medir la cantidad de información que se filtra a través del canal lateral.

Aplicaciones y casos de uso del circuito enmascarado
Los circuitos enmascarados se utilizan en diferentes áreas, como tarjetas inteligentes, dispositivos IoT y sistemas embebidos. Algunos casos de uso específicos incluyen la protección de claves criptográficas en tarjetas SIM, la seguridad en pagos sin contacto y la protección de contenido multimedia.

Desafíos y limitaciones de los circuitos enmascarados
Los desafíos en el uso de circuitos enmascarados incluyen la dificultad de implementar estas técnicas en hardware y software, y el aumento del costo computacional y de la complejidad del diseño del circuito. Además, el enmascaramiento puede no ser suficiente para proteger contra todos los tipos de ataques de canales laterales, y puede ser necesario combinarlo con otras técnicas de protección.

Conclusiones
Los circuitos enmascarados representan una medida de seguridad efectiva contra los ataques de canales laterales en criptografía. A través de técnicas de enmascaramiento y una evaluación rigurosa, estos circuitos pueden proteger la información sensible y mantener la integridad de los sistemas criptográficos. Sin embargo, también existen desafíos y limitaciones que deben ser abordados en futuras investigaciones.

Cryptographic algorithm validation program (CAVP)

Introducción

La validación de algoritmos criptográficos es un aspecto crucial para garantizar la seguridad de los sistemas informáticos. El Cryptographic Algorithm Validation Program (CAVP) es un programa que se utiliza para esta validación, proporcionando pruebas de validación para algoritmos criptográficos aprobados y recomendados por el Instituto Nacional de Estándares y Tecnología (NIST) en los Estados Unidos. Este trabajo tiene como objetivo investigar los aspectos clave del CAVP, su proceso de validación y su importancia en el campo de la criptografía.

Validación de algoritmos criptográficos

La validación de algoritmos criptográficos implica verificar que los algoritmos cumplen con los estándares y requisitos establecidos por organizaciones reconocidas, como el NIST. Estos estándares y requisitos aseguran que los algoritmos criptográficos proporcionan un nivel adecuado de seguridad y son resistentes a los ataques conocidos.

Visión general del programa CAVP

El Cryptographic Algorithm Validation Program (CAVP) es un programa gestionado por el NIST que proporciona pruebas de validación para algoritmos criptográficos aprobados y recomendados. Los proveedores pueden utilizar cualquier laboratorio de pruebas de seguridad y criptografía acreditado por NVLAP para probar las implementaciones de algoritmos. Una implementación de algoritmo que ha sido probada con éxito por un laboratorio y validada por el NIST se añade a una lista de validación apropiada.

Proceso de validación a través de CAVP

El proceso de validación a través del CAVP implica varias etapas, incluyendo la presentación de algoritmos, pruebas y evaluaciones, y la emisión de certificados de validación. Para que una implementación de algoritmo se liste en un certificado de validación de módulo criptográfico como una función de seguridad aprobada, la implementación del algoritmo debe cumplir con todos los requisitos de FIPS 140-2 y debe completar con éxito el proceso de validación del algoritmo criptográfico.

El proceso de validación del CAVP implica varias etapas. Primero, el proveedor presenta la implementación del algoritmo al laboratorio de pruebas. Luego, el laboratorio realiza pruebas para verificar que el algoritmo cumple con los estándares y requisitos del NIST. Finalmente, si el algoritmo pasa las pruebas, el NIST emite un certificado de validación.

Importancia y confianza en la validación de algoritmos a través de CAVP

La validación de algoritmos criptográficos a través del CAVP es crucial para establecer la confianza en los sistemas criptográficos. Los certificados de validación emitidos por el programa CAVP ayudan a los proveedores de productos y a los usuarios finales a seleccionar algoritmos seguros y confiables.

Desafíos y futuras tendencias en la validación de algoritmos

Existen varios desafíos en la validación de algoritmos, como la adaptación a algoritmos cuánticos y la evaluación de la seguridad frente a nuevos ataques. Las futuras tendencias en la validación de algoritmos incluyen la integración de estándares internacionales y la colaboración entre diferentes programas de validación.

La validación de algoritmos criptográficos a través del CAVP es crucial para establecer la confianza en los sistemas criptográficos. Sin embargo, también hay desafíos en este proceso. Por ejemplo, la validación puede ser un proceso costoso y que consume mucho tiempo, y puede ser difícil para los proveedores pequeños y medianos. Además, los estándares y requisitos del NIST pueden cambiar con el tiempo, lo que puede requerir que los algoritmos sean revalidados.

Un estudio reciente publicado en Sensors propone una nueva técnica de firma digital basada en criptografía de caja blanca para la verificación de firmas digitales. Esta técnica podría ser relevante para el CAVP, ya que proporciona una nueva forma de validar algoritmos criptográficos.
Conclusiones

El Cryptographic Algorithm Validation Program (CAVP) juega un papel crucial en la validación de algoritmos criptográficos, proporcionando un marco para probar y validar la seguridad de estos algoritmos. Sin embargo, la validación de algoritmos sigue siendo un campo de investigación activo, con nuevos desafíos y oportunidades emergiendo constantemente.

Bibliografia

[1] S. Ren, J. Chen, R. Li, L. Song, and Y. Wang, "Cross-Correlation Based Side-Channel Resistance Evaluation for Masked Circuits," in ACM Transactions on Embedded Computing Systems, vol. 20, no. 5s, Article 69, 2021. [Online]. Available: https://doi.org/10.1145/3548606.3560579

[2] K. Zhang, F. Zhang, and M. Liu, "A New Method for the Security Evaluation of Masked Circuits," in Cryptography and Coding. CCSCA 2021. Communications in Computer and Information Science, vol 1412. Springer, Singapore, 2021. [Online]. Available: https://doi.org/10.22624/aims/crp-bk3-p12

[3] A. Moradi, "On the Simplicity and Predictability of Masked S-Boxes," in IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2021, no. 3, pp. 1-23, 2021. [Online]. Available: https://doi.org/10.46586/tches.v2021.i3.1-23

[4] S. Bhasin, J. Danger, S. Guilley, and Z. Najm, "Provably Secure Higher-Order Masking of AES," in IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2021, no. 2, pp. 342-372, 2021. [Online]. Available: https://doi.org/10.46586/tches.v2021.i2.342-372

[5] "Cryptographic Algorithm Validation Program (CAVP)," National Institute of Standards and Technology, 2023. [Online]. Available: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program