Computación en Grilla de Escritorio para Evaluación de Algoritmos Criptográficos

Antonio Castro Lechtaler[1], Alejandro Repetto[1, 2], Martín Bianchi[1, 2], Marcelo Cipriano[1], Alejandro Arroyo Arzubi[1], César Cicerchia[1, 2], Eduardo Malvacio[1]

[1]EST – Facultad de Ingeniería – Instituto Universitario del Ejército
[2]CIDESO – DIGID –Ejército Argentino

{acastro, marcelocipriano}@est.iue.edu.ar;
{arepetto, mbianchi, cdcicerchia}@ejercito.mil.ar; aarroyo_arzubi@hotmail.com;
edumalvacio@gmail.com

Resumen

Como todos los componentes de un sistema de información, los sistemas criptográficos deben evaluarse para poder certificar sus características técnicas. Sin embargo, por sus características, son complicados de testear y, en general, los errores de implementación o puntos débiles se encuentran una vez ocurridos los incidentes.

Realizar pruebas sobre sistemas criptográficos requiere altos niveles de cómputo que raramente están disponibles en las organizaciones.

El proyecto ULTRACOM está desarrollando una plataforma de cómputo de alto rendimiento dedicada a la evaluación y certificación de sistemas criptográficos.

ULTRACOM utiliza la plataforma BOINC, de cómputo en grilla de escritorio, que permite otorgar grandes capacidades de cómputo a una red aprovechando los recursos disponibles, sin necesidad de adquirir servidores. Sobre dicha plataforma se están desarrollando APIs con el fin de enmascarar la complejidad de desarrollo y dejar a disposición un sistema apto para realizar pruebas de robustez de implementaciones de algoritmos criptográficos.

Palabras clave: criptografía, computación de alto rendimiento, cómputo distribuido.

Contexto

El proyecto ULTRACOM se desarrolla en un contexto de colaboración entre el CriptoLab, Laboratorio de Criptografía y Seguridad Teleinformática de la Escuela Superior Técnica - Facultad de Ingeniería del Ejercito (EST), y el Centro de Investigación y Desarrollo de Software del Ejército (CIDESO), perteneciente a la Dirección General de Investigación y Desarrollo (DIGID).

Estos dos centros de investigación presentan capacidades complementarias que permiten abordar el problema del criptoanálisis desde la perspectiva de la computación de alto rendimiento.

El CriptoLab posee gran experiencia en la investigación de sistemas criptográficos, incluyendo la mejora, la evaluación y el desarrollo de algoritmos y

matemáticas dedicada al problema de la seguridad de la información.

Por su lado, el CIDESO tiene experiencia en sistema militares operacionales que incluyen, en muchos casos, capacidades de computación de alto rendimiento.

Siendo el tema de la capacidad computacional un limitante crítico a la hora del desarrollo y evaluación de sistemas criptográficos modernos, la intersección de conocimientos entre ambas disciplinas da origen al proyecto ULTRACOM.

Este proyecto tiene aplicación directa tanto a nivel académico como a nivel operacional.

Introducción

ULTRACOM pretende desarrollar una capacidad de cómputo distribuida de amplia aplicación para problemas criptográficos.

La característica fundamental de un algoritmo criptográfico es su alta complejidad computacional. Es decir, requieren un alto nivel de cómputo para poder resolver el problema si no se tienen los inputs correctos (claves).

Matemáticamente se pueden calcular las complejidades computacionales de estos algoritmos. Sin embargo, la complejidad calculada es teórica y presenta un desafío extra el poder probarlo empíricamente.

Por otro lado, existen computadoras de uso específico para realizar grandes cálculos. Tanto computadoras paralelas como grillas pueden generar capacidades de procesamiento masivos capaces de mejorar los procesos de evaluación de algoritmos. Dichos equipos son costos de adquirir y complejos de operar.

ULTRACOM propone utilizar otra aproximación a la computación de alto rendimiento, a través de la implantación de Computación en Grilla de Escritorio (*Grid Desktop Computing*). Dentro de esta categoría de cómputo masivo, se destaca el *framework* BOINC (*Berkeley Open Infrastructure for Network Computing*), un sistema completo de código abierto desarrollado por la Universidad de Berkeley a fines de los 90's.

BOINC permite aprovechar la capacidad de cómputo ociosa de ordenadores de escritorio a través de un *middleware* [1], que recibe trabajos computacionalmente complejos y los divide en tareas que distribuye sobre los nodos.

Esta infraestructura presenta tres características fundamentales: el procesamiento es voluntario; es monopropósito; y es abierta.

La lógica de voluntarios indica que los equipos participantes de la grilla están bajo un esquema de administración descentralizada. Cada usuario (equipo) define el aporte computacional que desea hacer a la red, tanto en procesamiento como en almacenamiento. Asimismo, a través de un software cliente decide a qué proyecto dar su apoyo, y lo pude dividir su aporte en múltiples proyectos.

Por otro lado, la infraestructura está orientada a resolver problemas puntuales, debiendo desarrollarse una serie de módulos para cada problema en particular que se desee resolver. Es decir, es monopropósito. Una vez configurada para un proyecto, modificarla para que sea utilizada en otro implica un gran esfuerzo.

Por último, es abierta. Esto quiere decir que los nodos, además de estar administrados por terceros fuera del

control de la organización, no se pueden identificar, no se conocen, y tienen libertad de asociarse y darse de baja de la grilla de modo transparente.

ULTRACOM aborda una estrategia que permite adaptar estas tres características básicas de BOINC, generando una herramienta de evaluación de sistemas criptográficos con el fin de ser utilizado para la selección y certificación de algoritmos antes de ser incorporados a sistemas de software de uso civil o militar. Por esto, ULTRACOM podrá ser usado tanto dentro del laboratorio, como fuera, en aplicaciones que necesiten verificar la robustez de sus algoritmos criptográficos.

La lógica voluntaria de BOINC, a los efectos de ULTRACOM puede ser mantenida o enmascarada, según se considere más oportuno. Si se decide enmascarar, se puede implementar el procedimiento realizado en [2].

Si se decide trabajar en un entorno abierto, nuevamente, no es un limitante para ULTRACOM. El proyecto puede ser publicado en intranets, evolucionando de esa forma a un esquema de intragrid, tal como lo indica [3].

Sin embargo, el enfoque monopropósito sí plantea un desafío para los objetivos del proyecto. La generalización de la plataforma, aunque sea dentro de los límites de los problemas criptográficos, requiere una adaptación del *framework* original de BOINC [4].

En particular, la solución propuesta avanzó hacia la adaptación del componente denominado *work generator* y de la estrategia del algoritmo distribuido.

Esta adaptación permitió hacer una prueba de factibilidad técnica que aseguró la línea de investigación de ULTRACOM.

La concepción de los dos componentes modificados parte de la abstracción de los problemas criptográficos más comunes: aquellos que las pruebas se realizan mediante esquemas de fuerza bruta controlada.

Este tipo de pruebas se ejecuta mediante a la prueba sistemática de valores de entradas en los algoritmos criptográficos hasta obtener algún resultado particular. En general se pueden probar semillas o valores iniciales en algoritmos de generación de número aleatorios, potenciales claves o pares de números primos que conforman la estructura básica en infraestructuras de cifrado asimétrico.

La generalización de este problema siempre consta en la iteración controlada de rangos de valores, por lo que el tipo de entrada que esperan recibir los algoritmos presenta una taxonomía genérica con rangos de valores a probar. La lógica de BOINC permite particionar el espacio de pruebas del problema en subespacios independientes que pueden ser ejecutados por los voluntarios.

Así se genera un único proyecto con un ejecutable que se despliega sobre los voluntarios y recibe dos parámetros de entrada: el algoritmo a ejecutar y los parámetros de ejecución.

Los parámetros, aprovechando la generalización mencionada, son subdivisiones (tareas) del espacio de prueba del problema (trabajo).

El archivo ejecutable, también se incorpora como parte de los parámetros de entrada. El cliente de BOINC tiene la capacidad de incorporar un código ejecutable por proyecto. ULTRACOM supera esta limitación haciendo que el

código ejecutable del proyecto a su vez ejecute un código externo que se pasa como parámetro. Así, generando un solo proyecto "ULTRACOM" se pueden ejecutar múltiples códigos a través de una llamada tipo *system*, que permite ejecutar un ejecutable a través de otro.

Líneas de Investigación, Desarrollo e Innovación

Se abordarán las siguientes líneas de desarrollo:

a- Generación de API ULTRACOM
b- Incorporación de nuevas estructuras de sistemas criptográficos

La línea a- pretende generar una API de programación que permita a cualquier desarrollador poder utilizar la capacidad de cómputo distribuido sin necesidad de tener conocimiento profundo sobre los detalles de BOINC. Mediante una API, se prevé generar una abstracción que permita desarrollar el algoritmo distribuido, usando algunas interfaces dadas y una serie de archivos de configuración que permitan dar información al *work generator* sobre estrategias de partición del trabajo en tareas. Esta línea se focaliza en aumentar la usabilidad del sistema y complementa a trabajos realizados por la EST y el CIDESO [5].

La segunda línea de investigación tiene como objetivo ampliar el alcance de ULTRACOM, realizando abstracciones más generales de modo de abordar nuevos problemas criptográficos.

Resultados y Objetivos

Al momento se logró la prueba de factibilidad técnica de la aproximación propuesta, demostrando que se podía generalizar el uso de la plataforma BOINC a través del paso como parámetro de una porción de código a ejecutar [4] en la forma de un programa.

Además se probó conceptualmente el proyecto pudiendo poner en marcha pruebas sobre los algoritmos Trivium32 y TriviumToy32 [6] sobre la misma red de nodos distribuidos utilizando un solo servidor / proyecto.

El próximo paso está en vistas de estabilizar la solución y generar una interface de programación (API) para lograr un metalenguaje de programación que permita acceder de manera más amigable a las capacidades de cómputo distribuido. Esta generalización es fundamental para lograr un impacto mayor, habilitando el uso para investigadores con conocimientos limitados en tecnologías de cómputo masivo.

El objetivo final es que la plataforma ULTRACOM pueda ser utilizada y explotada por cualquier investigador cuyo nivel de conocimiento sea el suficiente como para programar su algoritmo, sin necesidad de conocer la complejidad de cómputo que subyace en el sistema.

Formación de Recursos Humanos

ULTRACOM, al ser un proyecto de colaboración entre el CriptoLab, laboratorio orgánico de la Facultad de Ingeniería del Ejército y el CIDEO, presenta una alta participación de alumnos de la carrera de grado de Ingeniería en Informática.

Desde 2011, se trabaja con alumnos de tercero, cuarto y quinto año en cuestiones relacionadas con la computación de alto rendimiento y criptografía, formando recursos técnicos con capacidades de investigación y desarrollo.

Además, del proyecto participan investigadores con distintos niveles de

experiencia, lo que permite una transferencia de conocimientos y formación en la carrera de investigación técnica y docente.

Referencias

[1] G. McGilvary, How to Create a BOINC Project, Edimburgo, 2012.

[2] A. J. M. Repetto, «Hybrid Architecture for Constructive Interactive Simulation: Evaluation and Outcomes,» de *Interservice/Industry Training, Simulation, and Education Conference*, Orlando, FL, 2010.

[3] L. Ferreira, V. Berstis, A. J. y M. Kendzierski, Introduction to grid computing with Globus, Riverton, 2003.

[4] A. Castro Lechtaler, A. Repetto, M. Bianchi, A. Arroyo Arzubi, C. Cicerchia, E. Malvacio y M. Cipriano, «Computación Distribuida para Seguridad Informática,» de *CACIC*, La Matanza, Provincia de Buenos Aires, 2014.

[5] A. Repetto y M. Bianchi, «Computación Distribuida para Seguridad Informática,» de *WICC*, 2012.

[6] A. Castro Lechtaler, M. Cipriano, E. García, J. Liporace, A. Maiorano y E. Malvacio, «Model Design for a Reduced Variant of a Trivium Type Stream Cipher,» de *XIX Congreso Argentino de Ciencias de la Computación*, Mar del Plata, 2013.