

FICHA DE PROYECTOS DE INVESTIGACIÓN

Año: 2011

Título del proyecto:

Diseño e implementación de un sistema de seguridad “honeypot” para redes de telefonía Voz sobre IP que utilizan el protocolo SIP.

Director del Proyecto:

Do Carmo, Rodrigo Daniel
rdocarmo@ubp.edu.ar

Equipo de Investigación:

Biasutto, Gustavo

Dependencia:

Centro de Investigación Aplicada y Desarrollo en Informática y Telecomunicaciones (CIADE-IT).

Área Temática:

Informática y Telecomunicaciones.

Evaluación:

Ministerio de Ciencia y Tecnología de Córdoba.

Financiamiento:

Ministerio de Ciencia y Tecnología de Córdoba.

Resumen:

INTRODUCCIÓN Y DELIMITACIÓN DEL OBJETO PROBLEMA

Con la difusión de Internet distintos tipos de servicios nuevos han aparecido, por ejemplo, la telefonía IP. Para este caso en particular, han surgido nuevas problemáticas respecto a la seguridad, debido a que al ser implementado sobre una red de computadoras es posible el

Sede Campus:

Av. Donato Álvarez 380 - (5147) Argüello, Córdoba
Tel. (+54 351) 414 4444 - Fax (+54 351) 414 4400

Sede Centro:

Lima 363 - (5000) Córdoba
Tel. (+54 351) 414 4555 - Fax (+54 351) 414 4500

República Argentina



espionaje y el fraude. Técnicamente los ataques más importantes que han sido reportados son: denegación de servicio, rastreo de llamada, secuestro de llamada, obtención de contraseña, publicidad no solicitada, intrusiones basadas en el servidor principal, ataques relacionados con los protocolos de medios, ataques relacionados con los protocolos de soporte, penetración de cortafuegos, "spoof" del identificador de llamadas y ataque "phishing".

En este trabajo se propone desarrollar una solución que disminuya (e elimine en gran medida?) la vulnerabilidad que los sistemas de telefonía IP presentan frente a los mencionados ataques. La solución que se propone es el desarrollo de un "honeypot", entendiéndose como tal a un programa de computadora que simula ser un teléfono IP, registrado como cualquier otro teléfono interno a la red y sin ningún tipo de restricción de seguridad, con el fin de registrar las actividades de los atacantes hacia éste y advertir de las mismas. El vocablo inglés "honeypot" significa literalmente "tarro de miel" y es una manera de hacer alusión a un tipo de sistema que atrae a los atacantes. Por su vasta difusión en la jerga técnica, en otras áreas de aplicación, se lo dejará en ese idioma.

Este proyecto se propone como una continuación del trabajo realizado en la Universidad Blas Pascal como tesis de grado, habiendo participado además en una demostración en la conferencia IEEE IPTComm 2010 en Munich, Alemania, además de un artículo ("paper") aceptado para ser publicado para la próxima conferencia IEEE IM 2011. En este proyecto se plantea continuar con el desarrollo del programa, exponiéndolo a ataques reales a fines de recolectar grandes cantidades de información, con el fin de seguir desarrollando y refinando los algoritmos que se utilizan y conseguir la mayor exactitud posible.

Palabras clave:

Vulnerabilidades – Ataques – VoIP – Modelo – Llamadas.

Abstract:

Voice over IP (VoIP) and the Session Initiation Protocol (SIP) are establishing themselves as strong players in the field of multimedia communications over IP, leveraged by low cost services and easy management. Nevertheless, the security aspects are not yet fully mastered. We propose an architectural design together with an open-source implementation of a VoIP SIP-specific honeypot that can be deployed as a user-agent back-end in a VoIP enterprise domain. Because of the fact that the honeypot extensions do not represent real users, every activity targeting them is perceived as suspicious. The honeypot answers the calls and records them along with the SIP trace. The honeypot is able to classify many kinds of anomalies and report them to the administrator or automatically control the security policy of the domain under protection. We aim, by this contribution, to encourage the deployment of such honeypots at large scale and the collection of attack traces.

Sede Campus:

Av. Donato Álvarez 380 - (5147) Argüello, Córdoba
Tel. (+54 351) 414 4444 - Fax (+54 351) 414 4400

Sede Centro:

Lima 363 - (5000) Córdoba
Tel. (+54 351) 414 4555 - Fax (+54 351) 414 4500

República Argentina



Key words:

Vulnerabilities – Attacks – VoIP – Model – Calls.



Sede Campus:

Av. Donato Álvarez 380 - (5147) Argüello, Córdoba
Tel. (+54 351) 414 4444 - Fax (+54 351) 414 4400

Sede Centro:

Lima 363 - (5000) Córdoba
Tel. (+54 351) 414 4555 - Fax (+54 351) 414 4500

República Argentina