Rhodes University

Computer Science Department

Project Proposal

Radu Courage Samuel
Email-g11r3764@campus.ru.ac.za
Cell: +2772 850 2466

March 2011

1 Project Title

A less attack-prone, Internet deployment of iLanga

2 Supervisors

1. Mosioua Tsietsi
   e-mail:M.Tsietsi@ru.ac.za
2. Prof Alfredo Terzoli
   e-mail: A.Terzoli@ru.ac.za

3 Objective of Research

The primary goal of this project is to secure iLanga from attacks such as those that have been experienced in the past and to identify other potential threats to it. We will try to mitigate these threats by considering the traditional aspects of security, that is, Confidentiality, Integrity and Availability (CIA). Confidentiality ensures that only authenticated users can use the system and that their information is not disclosed to unauthorised individuals. Integrity ensures that the system behaviour and data are not modified without being detected. Availability ensures that the telephony system is always available for use by legitimate users when they need to

communicate. The secondary goal is to develop a guide with best security practices that will apply to iLanga and similar VoIP systems. This guide will help administrators to carefully consider security when deploying such systems.

4 Background

In the past, iLanga has been compromised and at the beginning of this project it was shut down to avoid further exploitation rendering it unavailable to its users. The problem can be largley attributed to malicious elements on the Internet. The most prevalent threats to VoIP deployments today are the same security threats that exist in traditional data networks [1, 2]. Among these threats are brute force attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS). Brute force attack is a technique whereby an attacker simply guesses username and password until he finds a combination that works. DoS and DDoS attack are characterised by an attempt to prevent the legitimate use of a service. Additionally, in the telephony world, there is a new threat known as Spam over Internet Telephony (SPIT) which refers to unsolicited bulk calls or instant messages [3].

5 Phases

The project has five phases. These are as follows

1. Phase 1
   Assesment of the current state. This includes recording the versions of each component that makes up iLanga.

2. Phase 2
   Historical attacks associated with each component version. We will consider how other similar threats have been mitigated.

3. Phase 3
   Securing the system by introducing countermeasures. An iterative approach will be used to deploy each countermeasure

4. Phase 4
   Re-implementing the secure version of iLanga.

5. Phase 5
   Testing the system - penetration testing.

6 Proposed Experiments

The following tests are proposed to test the security and stability of the system

1. Asterisk PBX server test
    - Testing for known weaknesses
2. MySQL Database test
    - testing known weaknesses
3. Kamailio proxy server test
    - testing for known weaknesses

7 Requirements

- Laptop/ Desktop 2.0GHz or better
- Ubuntu Linux operating system
- Asterisk PBX server
- MySql Database 5.5 version
- Kamailio proxy server

8 Timeline

Project Milestones 2011	
7th March	Project Proposal
31 March	Field trip(iLanga architecture)
31 April	Reading and writting
30 May	Reading and writting
24 June	Literature Review Submission
30 July	Implementation
31 August	Experiments
31 September	Deductions
30 October	Final project report
14 November	Research website complete

References

[1] Blake, E. A. Network security: Voip security on data network–a guide. In *Proceedings of the 4th annual conference on Information security curriculum development* (New York, NY, USA, 2007), InfoSecCD '07, ACM, pp. 27:1–27:7.

[2] Endler, D., and Collier, M. *Hack Exposed VoIP: Voice Over IP Security Secrets & Solutions*. McGraw-Hill, 2007.

[3] S Dritsas, J Mallios, M. T. G. F. M. D. G. Threat analysis of the session initiation protocol regarding spam, 2007.