ST. MARY'S UNIVERSITY OF SAN ANTONIO

An Expert System for Network Router Configuration

Vision Document

Michael A. Perez

Spring 2015

1. INTRODUCTION

PURPOSE

This document is the first in a collection of software engineering documents on the proposed software system, an Expert System for Network Router Configuration. In this Vision document we present the system at a high level of description with the intent that this should be used as a guide throughout the system development life-cycle to keep the project within scope, warding off feature creep. A discussion of the problem to be solved will be given first, leading to targeted user needs and goals. From these needs and goals, we will visually capture major features using UML Use-case diagrams. From which we will derive informal requirements or Software Product Features. Requirements will be formalized in the next volume of this collection, theSystem Requirements Specification (SRS) document.

PROBLEM DESCRIPTION

According to a published solicitation by the United States' Department of Defense Advanced Research and Projects Agency (DARPA) in 2006, incorrectly configured network devices are a common cause of insecure computer networks[1]. In the enterprise world, flawed configurations might result from fat-fingered input, poor quality network analysis, or distributed network devices with mismatched or uncomplimentary configurations. However, in the context of a 1st world residence, typical of a small office/home office (SOHO), a single wireless router is solely responsible for implementing network configuration and policy. While an enterprise network is carefully designed using some engineering process, a SOHO network can be characterized as ad-hoc in terms of design. Most SOHO router manufacturers understand this and provide "quick setup" firmware pre-installed. The default settings on these routers are acceptable for typical SOHO use cases but the typical SOHO user is ignorant of most of these settings. And, in indeed, the default administrative password is rarely changed leaving many SOHO routers vulnerable to attack[2]. However, for the power SOHO user, there are 3rd party firmwares available, for example, Linux-based OpenWRT, DD-WRT, and Tomato. These firmwares are designed to replace a SOHO wireless router's pre-existing firmware from the manufacturer and provide new or improved features for the router that otherwise would only be available on more expensive router [3,4]. As open-source software supported by an active community, an added feature of these firmwares is support for older, inexpensive hardware and turnarounds for security fixes that are quicker than one could expect from an original manufacturer who has dropped support or has become defunct[5]. Among the three firmwares mentioned, OpenWRT is currently the only one fully open-source and free providing the lowest barrier to full access. Configuring OpenWRT, on the other hand, is a manual and knowledge intensive process requiring a domain expert in order to get the most benefit from the features provided by OpenWRT.

A solution may include an Expert System, a system that emulates the decision-making ability of a human subject matter expert (SME) by reasoning about collected facts to infer knowledge. Expert systems should not be confused with cognitive modeling programs, which attempt to simulate human mental architecture in detail. Instead, expert systems are practical programs that use heuristic strategies developed to solve specific classes of problems such the software program TurboTax by Intuit.

STATEMENT OF SCOPE

The goal of this project is a small step towards bringing down the accessibility barrier to using 3rd party firmware on consumer-grade, network routing devices, specifically OpenWRT version 10.03.1. Applications of conversational-mode expert systems such as TurboTax have proved successful at empowering the common people in doing for themselves that which they otherwise would need an expert. To achieve the stated goal, we will apply the conversation-mode of an expert system to gather information about a SOHO network from a user. The Expert system will read in production rules from a knowledge base along with the user's responses and infer a new status message to display to the user, a new question to ask of the user, and /or a new UCI command to append to a growing configuration script. After the conversational information gathering is complete, the system will allow the user to review and apply generated configuration scripts. The configuration script will be applied remotely via SSH and implemented using the Unified Configuration Interface (UCI) command-line utility developed by OpenWRT developers. At this stage of the system development, no 3rd party firmware installation help with be provided nor will the system account for every possible configuration scenario. This project will start off small by getting the user up and running with typical 3rd party firmware usage scenarios such as:

- *multi-family dwellings where the various wireless routers in close proximity may interfere with each other,*
- *a repeater network,*
- *a client-bridge network,*
- *VPN,*
- *and port forwarding.*

2. USER DESCRIPTION

This section justifies the system's existence by examining market demographics, the user's environment, the user's goals and needs, and existing alternatives.

USER/MARKET DEMOGRAPHICS

Users of the system are ISP home customers and are either tech-savvy or not. The intended goal of the system is to make accessible the configuration of the OpenWRT firmware for users who 1) have never been exposed to 3rd party firmware for their SOHO routers, 2) are not familiar with Linux, and 3) are not familiar with network configurations.

USER ENVIRONMENT

The system is meant to be used in a residential ISP network. In such a network, a single router, typically supplied by the ISP to the customer, sits between the ISP network and the customer's home network. A home network consists of laptops, desktops and related computing devices such as wireless printers and network-accessible storage. It would also include network-enabled consumer devices such as gaming consoles like the Microsoft XBOX, and network-enabled mobile devices such as smartphones and tablets. Sometimes the ISP supplied router provides wired access only and the customer may use their own personal wireless router, sitting in-line with the ISP-supplied router, to supply wireless access to the home network. This end-user supplied router is the target router to be configured by the system. Admittedly, targeting this device may not be effective at port forwarding if the ISP-supplied router has

port-forwarding settings of its own. Configuration takes place rarely, such as when the user replaces the router device or when the user self-troubleshoots network connections. Currently, end-users use the factory installed web-based front-end to configure the device's port forwarding, SSID, access permissions, security, DHCP, and other network settings. This may take 5 minutes to an hour, depending on the settings to be changed, skill level of the user, and familiarity with the configuration tool.

Key User/Market Goals and Needs

GN01: Provide big payoff for configuring router

The major goal for this project to get normal users to configure security for their wireless router and minimize the number of vulnerable wireless routers on the internet. To motivate users to engage with a technological gadget they otherwise would not, a big payoff or reward must be provided. Open-source firmware such as OpenWRT can provide this payoff by providing features to users that would otherwise cost them thousands of dollars.

GN02: Bridge the Knowledge Gap

It will not be enough to just provide a big payoff, we will have to make configuration accessible to the user.

Alternatives and Competition

Formally verified configurations of networks at the Autonomous System node level within the BGP protocol space have been around over a decade[6,7,8]. However, requiring the system user to use formal logic to define their network configuration is tantamount to requiring the user be a good low-level programmer. Our project instead will be accessible to the typical residential ISP costumer.

There exist many freely available and high quality software tools to monitor traffic. However, they require the training and expertise of a network administrative professional.

Truly there is nothing on the market today that does what we aim to do here

PIKT is a complex tool used for administrator functions including automated network configuration of a single server host by copying files in place from a repository. This may complement this system well in the future but we will not focus on version control for this project.

The TCS Security Blanket product offers automated hardening, or lockdowns, of Linux and Solaris operating systems, specifically, Solaris 10 and Red Hat Enterprise Linux 5 and its derivatives. The enterprise edition allows central control over several hosts. It performs the hardening according to profiles which may be based on industry standards (e.g. DCID 6/3) typically developed by authoritative agencies or they may be custom profiles developed in-house. This product offers high-level policy specifications, verification of policy compliance, and automatic configuration. However, like PIKT, it offers these features for the host computers on the network not the router. Each device coming onto the network will need to be locked down individually and with consumers going through networked devices at least every two years this may not be desirable. Also, Security Blanket is targeted at the enterprise and not the home market. The stand-alone version would be a great substitute to this project for home users with only secure lockdowns of their networks in mind but it will put a great burden on the user to understand network, computer security terminology.

3. Product Overview

An overview of the system is given here in the context of a product perspective, market position, a summary of capabilities, assumptions and dependencies, and a preliminary project plan to include tasks/milestones, schedule, and budget.

Product Perspective

The product is a a freely available, open-sourced system for the general public. It uses the CLIPS inference engine developed by NASA at its core. The CLIPS inference engine accepts a flat file as a knowledge-base. It is important to note that this initial development of the system focuses on the OpenWRT firmware but only the knowledge-base is tied to this firmware, generating Unified Configuration Interface (UCI) commands. Other firmware, based on OpenWRT or not, may be targeted by user-defined knowledge-base flat files.

Summary of Capabilities

The product will determine a set of commands to configure OpenWRT firmware running on a SOHO router. Determination will be based solely on a user interview given by the system. User-defined knowledge-bases, in flat files, may be substituted as a video game cartridge can be swapped out of a Nintendo video game console.

Assumptions and Dependencies

The product will depend on the host platform's connection to router and the version and support for UCI of the OpenWRT firmware installed

Preliminary Development Plan

In an effort to minimize cost, the system will utilize and incorporate technology and software for which new or additional licensing is kept to a minimum. The software engineering strategy devised for this project should be driven by the methods and tools used, and the nature of the project [PRESSMAN5thEd.]. Methods include maintaining a single vision though out the project lifecycle, a software development plan consisting of an enumeration of tasks to be completed, a process model defining how the tasks will be completed, and a schedule defining when they will be completed. Other methods include documenting a Test plan as requirements and software are developed, developing a hierarchy of requirements from customer goals/needs to product features to software specifications. Tools used will be fairly generic and will include Gantt charts or PERT analysis, UML modeling tools, and general office productivity software. The project's high-level requirements can be grouped into standalone components indicating a modular nature of the project.

Based on these observations an incremental development process model will be used in developing a software development plan to build modules of the system and integrate them together, adding functionality as the project progresses. Certain modules provide base functionality while others provide advanced or added functionality. This will be considered when scheduling tasks. In addition, the V-model for development will be used in creating test plans as the project produces artifacts from high level to low level.

Major milestones and deliverables are listed below:

1. *Proposal (This Vision Document)*
2. *Define Acceptance tests for each Goal/Need and Product Feature.*
3. *Committee Accepts Proposal*
4. *Stable Product Features*
5. *User Manual (derived from UseCase Workflow/Alt. Flow/Exceptions)*
6. *Stable Analysis Document (UML Analysis Diagrams)*
7. *Preliminary System Design Document (UML Design Diagrams)*

a. *Design System Test Cases (black-box tests)*

8. *System Analysis Presentation to Committee*
9. *Design and Implement Each Module*

a. *Detailed Module Design*
b. *Update Detailed System Design*
c. *Implement and test module for stability*

i. *Design/Implement Unit test cases (white-box tests)*

d. *Integrate with existing modules*
e. *Repeat for next module*

10. *Fully Detailed System Design Document*
11. *Final Report and Presentation*

4. KEY USE CASES

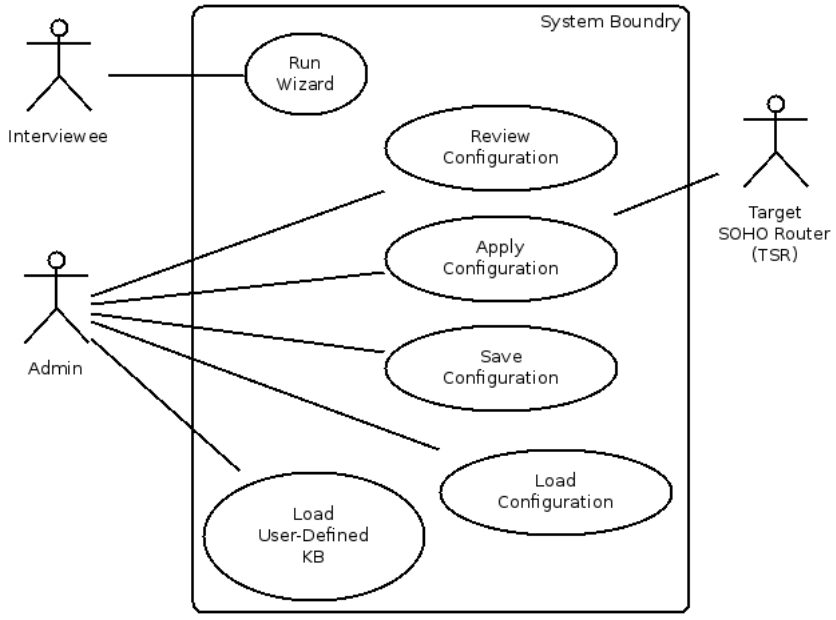

FIGURE 1: KEY USE-CASE DIAGRAM

UC01: **Run Wizard**

RUN WIZARD

Brief Description	The Wizard takes the interviewee step by step through the interview process to define the user's home network and determine how it should be configured.
Traceability	GN02, GN03
Preconditions	Wizard is not currently running. A knowledge base is selected.
Normal Flow	The user starts the wizard. The wizard prompts the user with a yes/no or multiple choice question. The user answers the question or cancels the wizard. If the wizard needs more information to determine a configuration for a SOHO router, it repeats from step 2 If the user canceled the wizard, nothing will be saved. The wizard will start from the beginning if the user starts it again
Alt. Flow	
Post Conditions	A set of shell script commands are generated to configure the target router unless the wizard was canceled.
Primary Actors	Interviewee

UC02: **Review Configuration**

REVIEW CONFIGURATION

Brief Description	Though the user is not expected to understand any of it, the set of shell script configuration commands to be run on the target router will be presented for the user's review.
Traceability	GN04
Preconditions	Wizard has completed to the end OR the user has loaded a previously saved configuration
Normal Flow	The system prompts the user with the configuration commands that will be applied to the target SOHO router. The user may review all the commands before applying them against the target SOHO router.
Alt. Flow	none

Post Conditions	The user may edit the commands, save the configuration to the file system, and apply the configuration to the target SOHO router.
Primary Actors	Admin

UC03: **Apply Configuration**

APPLY CONFIGURATION

Brief Description	Using SSH, remotely apply the configuration commands to the target SOHO router in the same LAN segment.
Traceability	GN01
Preconditions	Target router is installed with OpenWRT with SSH server enabled. System and target router are on the same LAN segment. User has SSH login credentials to the target router. A configuration file is already loaded here after the wizard has run or because the user has loaded a previously saved configuration.
Normal Flow	The user opts to apply the configuration currently being reviewed. The system prompts the user for the IP address of the target router. By default, the IP address of the network gateway is used. The user accepts the default or enters in a new IP address. The user is then prompted for the SSH username and password of the remote target SOHO router. Alternately, a public/private key pair may be used instead of a username and password credentials. Using SSH, the system remotely logs into the target router and runs the configuration script.
Alt. Flow	
Post Conditions	The SSH connection is closed. The target router is configured according to the configuration commands run by the script. The user's network connection may be interrupted.
Exception	

5. Feature Attributes

These attributes characterize all product features. Their values should be adjusted to reflect their current state as the project progresses.

Status: *Proposed, Rejected, Adopted, Implemented*

The Status attribute tracks progress during definition of the project baseline and subsequent development.

Priority: *Critical, Useful, Enhancement*

The Priority attribute ranks features by relative benefit to the end user and satisfaction of business goals and needs.

Effort: *Low, Medium, High*

The Effort attribute estimates the amount of time, lines of code, function points, or just general level of effort.

Risk: *Low, Medium, High*

The Risk attribute measures the probability that a feature will cause undesirable events such as cost overruns, schedule delays, or even cancellation.

Stability: *Low, Medium, High*

The Stability attribute measures the level of understanding of a feature.

Release: *Proposal, Plan, Module1, Module2, Module3, Module4, Module5, …, Final*

The Release attribute indicates the intended product version in which the feature will be introduced.

Assigned-To: *Person's name*

The Assigned-To attribute indicates the role or team that is responsible for further elicitation, software requirements, or implementation. Unless otherwise noted, the value for this attribute will be the author.

Traceability

The Traceability attribute tracks the source of the requested feature, e.g., one or more goals and needs from section 2 or a Use Case from section 4.

6. Software Product Features

The following software product features support the realization of one or more of the previously defined use cases.

SPF01: **Prompt user with yes/no question**

Prompt user with yes/no question

Attribute	Value	Notes
Status	Implemented	
Priority	Critical	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF02: **Prompt user with multiple choice question**

Prompt user with multiple choice question

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF03: **Start wizard**

START WIZARD

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF04: **Cancel wizard**

CANCEL WIZARD

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF05: **Determine if enough information from user has been collected**

DETERMINE IF ENOUGH INFORMATION FROM USER HAS BEEN COLLECTED

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF06: **Package configuration as repeatable script**

PACKAGE CONFIGURATION AS REPEATABLE SCRIPT

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF07: **Configuration script view**

CONFIGURATION SCRIPT VIEW

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF08: **Load configuration file from disk**

LOAD CONFIGURATION FILE FROM DISK

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF09: **Configuration script editor**

CONFIGURATION SCRIPT EDITOR.

Attribute	Value	Notes
Status	Proposed	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	Low	
Release		
Assigned-To		
Traceability	UC01	

SPF10: **Save edits to configuration script**

SAVE EDITS TO CONFIGURATION SCRIPT.

Attribute	Value	Notes
Status	Proposed	
Priority	Useful	
Effort	High	
Risk	High	
Stability	Low	
Release		
Assigned-To		
Traceability	UC01	

SPF11: **Remotely apply configuration script via SSH to the target SOHO router (TSR) that resides in the local LAN segment.**

REMOTELY APPLY CONFIGURATION SCRIPT VIA SSH.

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF12: **Determine gateway IP address of current LAN segment**

DETERMINE GATEWAY IP ADDRESS OF CURRENT LAN SEGMENT.

Attribute	Value	Notes
Status	Proposed	
Priority	Useful	
Effort	Low	
Risk	Medium	
Stability	High	
Release		
Assigned-To		
Traceability	UC01	

SPF13: **Select IP address of target router**

SELECT IP ADDRESS OF TARGET ROUTER.

Attribute	Value	Notes
Status	Proposed	
Priority	Useful	
Effort	Medium	
Risk	High	
Stability	Low	
Release		
Assigned-To		
Traceability	UC01	

SPF14: **SSH login with username/password credentials**

SSH LOGIN WITH USERNAME/PASSWORD CREDENTIALS.

Attribute	Value	Notes
Status	Adopted	
Priority	Critical	
Effort	High	
Risk	Medium	
Stability	Medium	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF15: **SSH login with public/private key pair credentials**

SSH LOGIN WITH PUBLIC/PRIVATE KEY PAIR CREDENTIALS.

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF16: **Generate Public/Private key pair**

GENERATE PUBLIC/PRIVATE KEY PAIR.

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF17: **Select Knowledge-base to use for wizard**

SELECT KNOWLEDGE-BASE TO USE FOR WIZARD.

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

SPF18: **Load default knowledge-base**

LOAD DEFAULT KNOWLEDGE-BASE.

Attribute	Value	Notes
Status	Implemented	
Priority	Useful	
Effort	High	
Risk	Low	
Stability	High	
Release	Final	
Assigned-To		
Traceability	UC01	

7. OTHER PRODUCT REQUIREMENTS

Non-functional requirements and their priorities are described here at a high-level. Applicable standards, hardware, or platform requirements; performance requirements; and environmental requirements. The quality ranges for performance, robustness, fault tolerance, usability, and similar

characteristics that are not captured in the Feature Set are defined here. If useful, attributes such as priority, stability, effort, and risk are described.

Applicable Standards

Whenever possible, encryption will be used when sending or receiving configuration data from the network. Consideration for a high Shannon Entropy will guide selection for keys, passwords, and/or algorithms. Follow procedures to ensure configurations are applied only by authorized users.

Constraints and Dependencies

The system requires TCP/IP network compatible devices.

There is some method available to remotely configure the router.

The system is cross-platform, able to run on Microsoft Windows, Mac OS X, and Linux with X Windows.

Performance Requirements

The system shall have a peak load of 1 active users.

The system shall have a maximum response time of 60 seconds for target router ping query before timing out.

Documentation Requirements

Define any specific documentation requirements, including user manuals, online help, installation, labeling, and packaging requirements.

User Manual

As defined in section 1, a key feature of this system is the accessibility to novice users. Therefore, a user manual will be provided. The Normal and Alternative flows from the Use Cases will guide the creation of the user manual.

Installation Guide

A guide will be written in which the installation will outlined.

Labeling and Packaging

The system is developed and packaged as a single unit. Any ancillary systems (i.e. database, server software, etc.) are not provided.

Licensing Installation

N/A