SMS Mobile Botnet Detection Based on Multi Agent System

Abdullah Alzahrani, Natalia Stakhanova, and Ali A. Ghorbani

Faculty of Computer Science, University of new Brunswick

ISCX Information Security Centre of Excellence

UNB

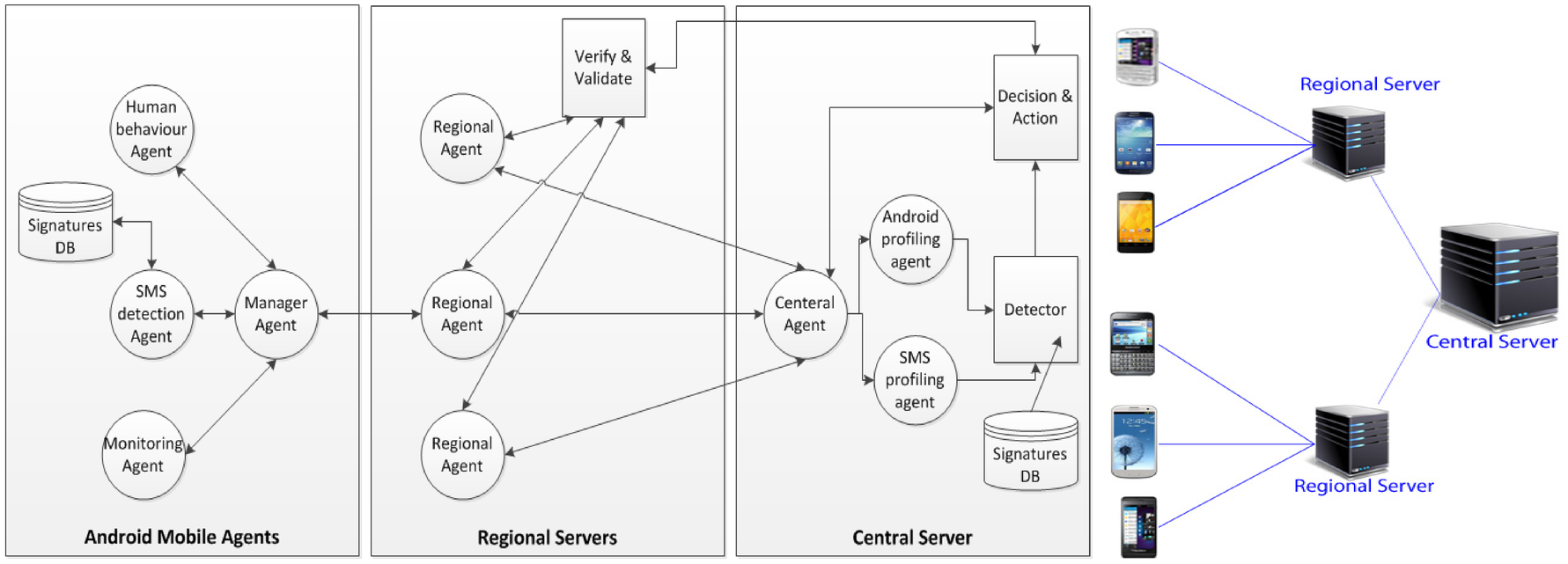
Problem Statement

- Mobile botnet is a group of compromised smart phones that share the same command and control (C&C) infrastructure and that are controlled by bot master for performing a variety of malicious attacks.
- With the ubiquitous of short message services (SMS) to every smart phones, SMS messages are used to transfer all C&C commands.
- **We propose a hybrid model of SMS botnet detectors, which is a combination of signature-based and anomaly-based approaches that use multi-agent technology to detect SMS botnet.**

Objectives

- Designing and implementing the four agents with different responsibilities on android mobile devices.
- Developing regional agents to interact with android devices and the verify-and-validate module to perform more authentication, which will investigate any misuse of agent behavior.
- Designing and implementing three services agents to maintain regional communication, to handle suspicious SMS, and to send android profiling data from a regional server.
- Developing detection module to detect malicious SMS with the usage of a behavior-based profiling technique which employs an anomaly detection approach.
- Designing and implementing decision and action modules to make informal decision and send the action to be performed by certain agents.

System Design



Android Smartphones

First, the SMS detection agent will perform signature detection on saved SMS and other agents will observe smartphone behaviors and resources. Then performing certain actions when it is received from regional agent.

Agents	Responsibilities
Manager Agent	•Register to regional agent provider •Read smart phone status •Interact with regional agent •Receive commands from regional agent •Manage the interaction between local agents •Send data to android profiling agent •Unsubscribe from regional agent
SMS Detection Agent	•Register to SMS profiling service via regional agent •Obtain copy of SMS signatures •Read current SMS and scan for any malicious SMS. •Perform signature detection on received SMS before it gets to SMS app •If SMS is malicious, notify the user and then delete the SMS •If SMS is suspicious, send a copy of suspicious SMS to SMS profiling agent
Monitoring Agent	•Read phone status •Report access to browse or other apps •Check WiFi Status and Internet access. •Spot any setting changes •Monitor the phone status including battery usage, running apps •Report to manager agent
Human-behavior Agent	•Observe user connectivity time. •Maintain the whitelist. •Report daily usages of android mobile. •Respond to manager agent

Regional Servers

Regional provider servers are created for authentication and security aims. The Regional server has two main components which are regional agent providers and a verify-and-validate module.

Agent	Responsibilities
Regional Agent	•Report changes to central Agent •Register smart phone device and add it to the subscribe list •Update and delete manger agents •Validate the manager agents certificate •Communicate with other agents, in case of agent movement, using broadcasting •Get profile updates then send it to Android profiling agent provider. •Obtain a copy of SMS then forward it to SMS profiling agent provider

Module0	Capabilities
Verify-and-validate	•Issue agents certificates •Manage and verify registered agents •Investigate suspicious manager agents. •Handle agent movement between regional agents •Send commands to regional agent to delete and block manager agents •Maintain agents' security

Central Server

Three agents and two modules used to process the data to detect suspicious SMS, make decision, and perform actions

Agents	Responsibilities
Central Agent	•Obtain profile updates and send them to Android profiling service provider. •Get a copy of SMS and then forward it to SMS profiling service provider •Create, update, block, delete, and control regional agents •Managing and updating the regional agents •Send actions to the regional agents •Update the database signatures •Send commands to start new agents •Manage the interaction between local agents
Android Profiling Agent	•Maintain a profile database for all subscribing smart phones •Update the received changes •Respond to detection module requests •Request more information from manager agents via regional servers
SMS Profiling Agent	•Handle the received suspicious SMS and then send it to detection module •Maintain the updated signature for each SMS detection agent

Module	Capabilities
Detection	•Read the suspicious SMS •Obtain all the android mobile profiles that contain the same SMS •Perform anomaly detection on profiles •If detected as Malicious, content analysis is required to check the URL.
Decision-and-Action	•Block the phone number •Broadcast the suspicious number •Update the signature DB