Example

Project Status Report

Section 1. Project Description

Project Name:	NEMESIS: Automated architecture for thread modeling and risk assessment for cloud computing
Principal Investigator:	Krishna Kavi
Student Researcher(s):	Patrick Kamongi
Originating University:	University of North Texas

Section 2. Project Plan

Original Statement of Work

Briefly summarize the work originally planned for the project, task budgets, and deliverables for the 5 most important tasks planned for this project.

Task#	*Description*	*Budget*	*Deliverable*
Task-1	Understand STRIDE model	$10K (3 mos)	Detailed report on our Ontologies and Vulcan framework
Task-2	Build a prototype of NEMESIS framework using VULCAN ontology system	$25K (9 mos)	Bayesian model used to define threat probabilities
Task-3	Evaluate NEMEISIS system with sponsor provided system configurations	(included in Task-2)	Demonstrations to show the capabilities of NEMESIS
Task-4	Explore optimizations to the search process	$10K (3 mos)	Report on suggested optimizations and formal review with sponsor

Section 3. Project Progress

Progress to Date and Accomplishments

What has this project accomplished since the last reporting period? Include major accomplishments, publications, presentations at significant venues, products created (software, hardware, data, designs, etc.), student placements, other. Insert most recent progress at top.

March 30, 2016

- Designed and implemented ontology knowledge bases for vulnerabilities
- Gathered preliminary results of NEMESIS capabilities to validate security assessment techniques
- Vulnerability prediction techniques based on probability and machine learning techniques partially complete

December 31, 2015

Example

Progress to Date and Accomplishments
• Developed a limited prototype of Nemesis Architecture and used it to assess the risk of any type of Software as a Service (SaaS) application, for example running on top of an OpenStack private cloud (IaaS + PaaS). • Nemesis-architecture extension work is on-going to address two other dimensions of IT Product vulnerabilities, notably the unknown vulnerabilities and current cyber threat intelligence on how the vulnerabilities are being exploited. • Continuing to adjust risk estimation for cloud assets to understand potential business impacts as a result of a security breach.

Section 4. Other Project Information

Additional Commentary
Use this area to include any additional information of interest to the project sponsor(s) and Center membership.
Preliminary results of this work have been submitted to the International Conference on Software Engineering Advances ICSEA 2016.