

Project Plan

Risk Mitigation Metric for Multi-Factor Authentication Systems

Project Manager: Bob O’Brien

Technical Lead: Stephen Paul King

# Project Scope

The objective of this project is to implement a proof-of-concept demonstration system which showcases the use of a novel Risk Mitigation Metric (RMM) module which relies upon the Maximum Relative Entropy (MrE) probability calculation algorithm to improve the ability to evaluate the risks associated with accessing some target asset that is “defended” by a multi-factor authentication system. The demonstration system will be used with both simulated and “real life” attempts to log into a series of (fictitious) software applications in order to demonstrate the capabilities and advantages of the MrE-based RMM.

# Customer / Agent

The Customer is the Defense Advanced Research Projects Agency (DARPA) – a branch of the Department of Defense of the United States of America.

BIT Systems (BITS) will be acting as agent/representative of DARPA and will manage routine communications and interactions on DARPA’s behalf during the project.

# Assumptions

The following assumptions are made:

* 1. The demonstration product resulting from this effort is just that: a demonstration product. Development of a production-strength product is beyond the scope of this project. It is assumed that the resulting product will not be used as-is for any real-world security application.
  2. At project start time, it is assumed that we will be able to identify a satisfactory collection of Identify Authenticator products which meet the needs of the project. (Meeting the needs of the project requires that these authenticators return more than a simple “pass / fail” result – that they instead return some sort of “reliability” score.)
  3. It is assumed that the availability of Clarkson University resources – particularly Dr. Giffon – as well as those of other contracted individuals will be sufficient throughout the life of the project.

# Limitations

The following Limitations are identified:

* 1. In order to meet delivery time and budget, the demonstration will be implemented within an environment based upon Microsoft’s .NET platform. The runtime environment for the resulting product must provide a .NET environment, and specifically must be able to support the Infer.NET probability calculation library.
  2. The project team is widely distributed geographically. This will place practical limits on communication schedules.

# Risk and Issue Tracking

A Risk and Issue Log will be maintained via Excel Spreadsheet. It will be reviewed at least weekly by the entire project team under the direction of the Project Manager. This document is located at **<gdrive>/ProvenSecure/Projects/CFT2/Risks and Issues.xlsx**

(Note: Until we migrate documentation to a location that provides for proper change / version control, update access to this document is limited to the Project Manager. Others team members can view it – and are encouraged to. But changes will be made in a controlled fashion by the Project Manager. Any team member with Risks, Issues, or comments that need to be documented should notify the project manager immediately – don’t wait for a status meeting.)

# ProvenSecure Project Team

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Responsibilities** |
| Project Manager | Bob O’Brien | Perform overall Project Management activities (manage schedule and budget, assign resources)  Prepare key project documentation, status reports and milestone completion reports  Act as Scrum Master during development sprints |
| Technical Lead | Stephen Paul King | Oversee project progress from a technical perspective  Act as “Product Owner” during development sprints. Guide selection of appropriate work to be included in sprints, and accept completed work at the end of sprints |
| Administrative Lead | Bill Whitescarver | Interact with Customer for Adminimstrative issues  Sign necessary contracts, orders, etc. |
| Architect / Developer | Allen Francom | Design the overall demonsration “bench” system and its components (except for the MrE calculation engines)  Act as Designer/Developer during development sprints |
| Technical Advisor | James Whitescarver | Assist in defining solutions for technical & theoretical problems as they arise.  Offer advice regarding the design of the overall architecture of the demonstration bench. |
| Technical Advisor | V Rao Bhamidipati | Assist in defining solutions for technical & theoretical problems as they arise.  Offer advice regarding the design of the overall architecture of the demonstration bench. |
| “Hardware” Systems Manager | Roman Anderson | Implementing Windows Virtual Machine testing environment. |
| Technology Advisor / Tester | Paul Dube | Research potential retail-market authenticators for appropriateness in this effort  Perform “live” testing of finished demonstrator |

# External / Contract Participants

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Company/ Organization** | **Name** | **Responsibilities** |
| University Research Lead | Clarkson University | Dr. Adom Giffin | Prepare white paper required for completion of Milestone 1  Contribute to the design of the MrE algorithm engine being coded into the RMM |
| Architect/Developer | (independent contractor) | Renaldus Urniezius | Design and code the MrE algorithm engine  Participate in integrating the MrE engine into the RMM |
| Technical Advisor | (independent contractor) | Dr. Joseph Skufca | Provide technical advice and assistance as needed to MrE algorithm development  Provide technical advice and assistance as needed to the team integrating authenticators into the demonstration base. |

# Customer Representatives

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Company/ Organization** | **Name** | **Responsibilities** |
| Administrative Contact | BIT Systems | Thomas Jacques | Administrative issue POC |
| Technical Contact | BIT Systems | Kyle Dausin | Technical issue POC |
| Customer Program Manager | DARPA | insert name here | list project-related responsibilities here |

# Schedule & Budget

## Overall Summary Information

|  |  |
| --- | --- |
| Expected Start Date | 24-Jun-2013 |
| Expected Completion Date | 11-Oct-2013 |
| Total Scheduled Effort (hours) | 2694 |
| Total Project Budget (Labor, Materials, Travel, etc.) | $ 125,830 |
| Milestone Summary Document | <gdrive>/ProvenSecure/Projects/CFT2/CFT2 Milestone Analysis (FINAL REVISION) (gdoc)  PSSCFT2 google group members here: <https://docs.google.com/document/d/18yPVXdeXFKqoE_vwiv-auVcMLErU_obGg3BYVlLG_50/edit#heading=h.d6oejpf1y3jy> |
| Schedule Document | <gdrive>/ProvenSecure/Projects/CFT2/working schedule.xlsx  Team members in the PSSCFT2 google group can view the current project schedule here: <https://docs.google.com/file/d/0ByI-WJm63WrwU3U0RVFjU0htQ2c/edit?usp=sharing> |

# Communication Plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Frequency** | **Delivery Method** | **Who Is Responsible** | **Comments** |
| Internal Team Status Meeting | weekly | Google+ Hangout | Bob O’Brien | Internal status will initially be reported and discussed at weekly Sunday evening meeting. If team deems it necessary, we will move to a dedicated meeting at a different date/time for this purpose. |
| Milestone Completion Reporting | As needed (approx. 2 week intervals) | .PDF format document | Stephen Paul King | Bob O’Brien will prepare project-related status reports. Stephen will review, add any technical comments that are necessary, and submit as evidence of completed milestone. |
| Payment Invoices | As needed (milestone completion) | .PDF format document | Bill Whitescarver | Bob O’Brien will generate invoices. After review to ensure completeness, Bill will forward to BITS for payment. |
| Final Project Report | End of project | .PDF formant document | Stephen Paul King | Final report describing the results of the testing and performance of RMM and MrE will be developed by Clarkson and ProvenSecure jointly. |

# Summary Description of Approach

The effort will begin with two concurrent tracks:

* **Milestone 1** involves Dr. Giffon of Clarkson University researching and writing a White Paper outlining the value of the Maximum Relative Entropy approach to probabilistic analysis within the context of multi-factor authentication software systems. While the project team already has very definite ideas regarding the benefits and best use of an MrE engine, it is hoped that this additional research – focused on the specific domain of authentication analysis – will yield additional insights that will then be incorporated into functional requirements of the proof-of-concept application that we are constructing.
* **Milestone 2** involves the “technical” team doing the functional analysis required to develop a set of use cases that will make up the high level specifications of the system we are building. Once we are satisfied that we have at least defined enough such “User Stories” (using the Agile/Scrum parlance), we will be able to select the ones to be addressed in the first development sprint. Those, in turn, will be further analyzed to identify “Tasks” that will make up the actual development goals of the sprint. Milestone 2 is complete when we have sufficient specification (stories and tasks) to fully define the work requirements for the first development sprint. It is important to note that functional analysis will not end with Milestone 2. User stories may be refined, and new ones added, particularly as results from the white paper analysis are considered. Task identification will be ongoing as well – not being required until just before a story is scheduled within a sprint for implementation.

**Milestones 3, 4, 5, and 6** represent the actual development iteration cycles of the project. Each of the four cycles will be conducted using the Scrum approach, which consists of the following:

1. A Planning Meeting held before the sprint starts to identify which stories are to be included, review the tasks, and ensure the estimates for the tasks seem reasonable.
2. Each day of the sprint will begin with a “Virtual Standup”. Scrum methodology calls for very brief face-to-face meeting of all those involved in the design and coding of the system. In our case, geography prevents us from being physically face to face, and time zones may prevent us from even all meeting together. Nonetheless, the Project Manager / Scrum Master (Bob O’Brien) will communicate with each developer/architect/designer daily to ensure the tasks in the sprint are being worked completed, the burn-down chart (the list of completed and outstanding activity) is being updated, and any problems are dealt with.
3. Nine days of each sprint will be used for “development”. On the tenth day, the system will be delivered to the testing platform. The Product Owner (Stephen King) will exercise the system and “Accept” or “Reject” specific user stories based on the performance of the test system. Rejected Stories are returned to the backlog.
4. If this is the not the last sprint, the Planning meeting for the next sprint will now be conducted and stories for the next sprint selected.
5. At the end of the tenth day, all source code will be catalogued. Documentation required for the Milestone Summary (backlog details, upcoming sprint task details, status summary, updated schedule and budget) will be prepared as well.

Sprint1 (Milestone 3) will be focused on creating the code necessary to define and capture the various risk ratings that will be used to define “environmental” situations surrounding a hypothetical login attempt. We will also use Sprint 1 to get our virtual test environment activated.

Sprint 2 (Milestone 4) will be focused on completing the end-to-end processing that will drive all of our testing. It will, however, use “stubs” instead of actual calls to authenticators and the RMM. In the meantime, RMM core design will continue at Clarkson.

In Sprint 3, we will replace stubs with actual calls to authenticators, and instantiate the “real” RMM code.

Sprint 4 will involve final tuning of the RMM and MrE engine, and – if time permits – addressing some “nice to have”s that we may have identified along the way.

In the event that any issues arise with code after Sprint4 is delivered, one or more “mini-sprints” of 1 to 3 days duration will be scheduled and run to deal with problem corrections. These will take place concurrently with the data gathering activities during Milestone 7 and will not generate any additional “milestones” or invoices.

The code delivered at the end of Sprint 3 included Image and Audio capture, but did not include the full interaction required with the AT&T Face, BetaFace, or AT&T Voice authenticators. Slight changes in the Bench design will still allow us to start capturing images and voiceprints prior to Sprint 4 for use in analytic data gathering.

Following the last sprint, **Milestone 7** will consist of final delivery of the proof of concept system to the testing platform (and most likely to a secondary platform independently managed by BIT Systems). It will then be exercised using a combination of “real user” interaction and “synthesized” interactions to produce statistically significant number of events covering the range of conditions we desire to test. Final performance reporting will be drafted. Final copies of source code and other documentation will be delivered along with the proof-of-concept executable image, and the project will be closed down.

The delivered “Bench Test” software will consist of a single executable image that acts as a wrapper for four “tools” in addition to the Risk Mitigation Module (RMM):

* The **Security Auditor Tool** which will be used to demonstrate the types of risk parameterization possibilities that would be incorporated into a “real” system that uses this approach to authentication and security.
* The **User Emulation Generator Tool** that will create large numbers of virtual login attempts that will be fed through the RMM. Large numbers of test cases are needed to improve statistical reliability of the RMM results.
* The **Batch Processing Tool** that will actually run the cases amassed by the User Emulation Generator Tool
* The **Login Simulator Tool** will provide a “real” login experience, and can be used to assess the performance of the RMM-base authentication validation.

# Revision History

LEAVE THIS INSTRUCTION IN PLACE. Insert a new row immediately below the header row when recording a new revision. This will ensure that the current revision is the first line in the table.

|  |  |  |
| --- | --- | --- |
| **Revision Date** | **Revision Author** | **Revision Details** |
| 25-Aug-2013 | Bob O’Brien | V4.0 – Added notes in Summary description revising “end of Sprint 3” expectations and adding post-Sprint 4 “mini-sprints”. |
| 11-Aug-2013 | Bob O’Brien | V3.0 – Added notes in Summary Description about possible start of some testing at end of Sprint 3. |
| 27-Jul-2013 | Bob O’Brien | V2.0 – Added general objectives for the four sprints |
| 14-Jul-2013 | Bob O’Brien | V1.2 – Added brief description of deliverable bench product; completed team roster |
| 13-Jul-2013 | Bob O’Brien | V1.1 – Corrected misspelled names |
| 12-Jul-2013 | Bob O’Brien | V1.0 – Initial Version completed |
| 05-Jul-2013 | Bob O’Brien | V0.1 – Initial Version |