AFRL-RI-RS-TR-2021-043

APCERTO: MOBILE APP SECURITY ORCHESTRATION PLATFORM

APCERTO

MARCH 2021

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2021-043 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
JAMES SIDORAN
Work Unit Manager

/ S /
JAMES PERRETTA
Deputy Chief, Information
Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MARCH 2021	FINAL TECHNICAL REPORT	JUL 2017 - JAN 2021

4. TITLE AND SUBTITLE

Apcerto: Mobile App Security Orchestration Platform

5a. CONTRACT NUMBER
FA8750-17-2-0218

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
69220K

6. AUTHOR(S)

Marika Robertson

5d. PROJECT NUMBER
DHSA

5e. TASK NUMBER
PC

5f. WORK UNIT NUMBER
RT

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Apcerto
20130 Lakeview Plz Ste 405
Ashburn VA 20147-5904

8. PERFORMING ORGANIZATION REPORT NUMBER
NA

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2021-043

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Past work commercialized a mobile app security certification tool that 1) performed critical security validation of Android mobile apps as measured against the National Information Assurance Partnership (NIAP) Mobile Application Protection Profile (MAPP), called Apcerto Bayesian Classifier." The Bayesian classifier was designed with the capability to produce a unique threat model based on machine learning that projects the probability of an attack or intrusion based on the mobile app's design and configuration. This work extends the classifier into an end-to-end mobile application orchestration platform by building out application programming interface (API) connections to other mobile app lifecycle components, such as identity management, cyber hardening, and Enterprise Mobility Management (EMM).

15. SUBJECT TERMS

Bayesian classifier, mobile app security, Enterprise Mobility Management (EMM), mobile application orchestration platform, National Information Assurance Partnership (NIAP) Mobile Application Protection Profile (MAPP)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**JAMES SIDORAN**
U	U	U	UU	16	19b. TELEPHONE NUMBER (*Include area code*) **N/A**

TABLE OF CONTENTS

1. Summary

This Technical Status Report covers Apcerto's activities under the Cooperative Agreement FA8750-17-2-0218 during the complete period of performance from July 13, 2017 – January 21, 2021. It provides a task by task overview of all completed and undertaken activities, special accomplishments, and other findings.

2. Introduction

In 2017, at the start of Apcerto's R&D Cooperative Agreement, there were multiple commercial offerings available for mobile app vetting in the market – most of them suitable for public facing mobile applications only, which do not touch Government networks. Apcerto believed that sensitive but unclassified level mobile use cases should be vetted against the well established NSA National Information Assurance Partnership (NIAP) Mobile Application Protection Profile (MAPP) set of security controls plus Agency-defined requirements that best represent the unique risk profile of that organization.

Originally funded by the Defense Information Systems Agency (DISA), and developed by MIT, Apcerto's then newly commercialized mobile app security certification tool already 1) performed critical security validation of Android mobile apps as measured against the National Information Assurance Partnership (NIAP) Mobile Application Protection Profile (MAPP); and 2) was designed with the capability to produce a unique threat model based on machine learning that projects the probability of an attack or intrusion based on the mobile app's design and configuration, herein referred to as the "Apcerto Bayesian Classifier" Apcerto has patented the Bayesian Classifier and no other app vetting solutions support this approach.

Apcerto applied for and was awarded the subject Research and Development Agreement to further enhance the product's functionality for the government. Apcerto's goals and subsequent product enhancement efforts included the following:

(1) further fine-tuned incorporation of all current and future NIAP PP standards
(2) integration of our security tool with Enterprise Mobility Management (EMM) platforms to achieve continuous monitoring and increased level of automation
(3) enhancing of the Apcerto Bayesian Classifier to anticipate future threats and vulnerabilities, and deliver predictive security
(4) expanding the "Apcerto Bayesian Classifier" capability for application in iOS space
(5) layering additional app vetting tools into the framework, for Apcerto to process the findings through its patented risk rating algorithms and aggregate the results into a comprehensive vulnerability assessment and risk score, results in higher detection of malware and actionable mitigation responses to threats

In conducting the development work towards achieving the above-listed objectives, and conducting numerous consultations with mobile app security executives, practitioners and evangelists within the Federal Government, Apcerto became acutely aware of one additional consideration: **mobile app security is best not addressed in a vacuum and separate from mobile app development phase**. Rather security functionality must be embedded early on in the mobile app lifecycle, in alignment with the DevSecOps principles. Therefore, Apcerto adopted

another major objective of integrating with an app development platform to develop a cohesive unified mobile app development and security ecosystem. This direction further evolved into transforming Apcerto into an end-to-end mobile application orchestration platform by building out application programming interface (API) connections to other mobile app lifecycle components:

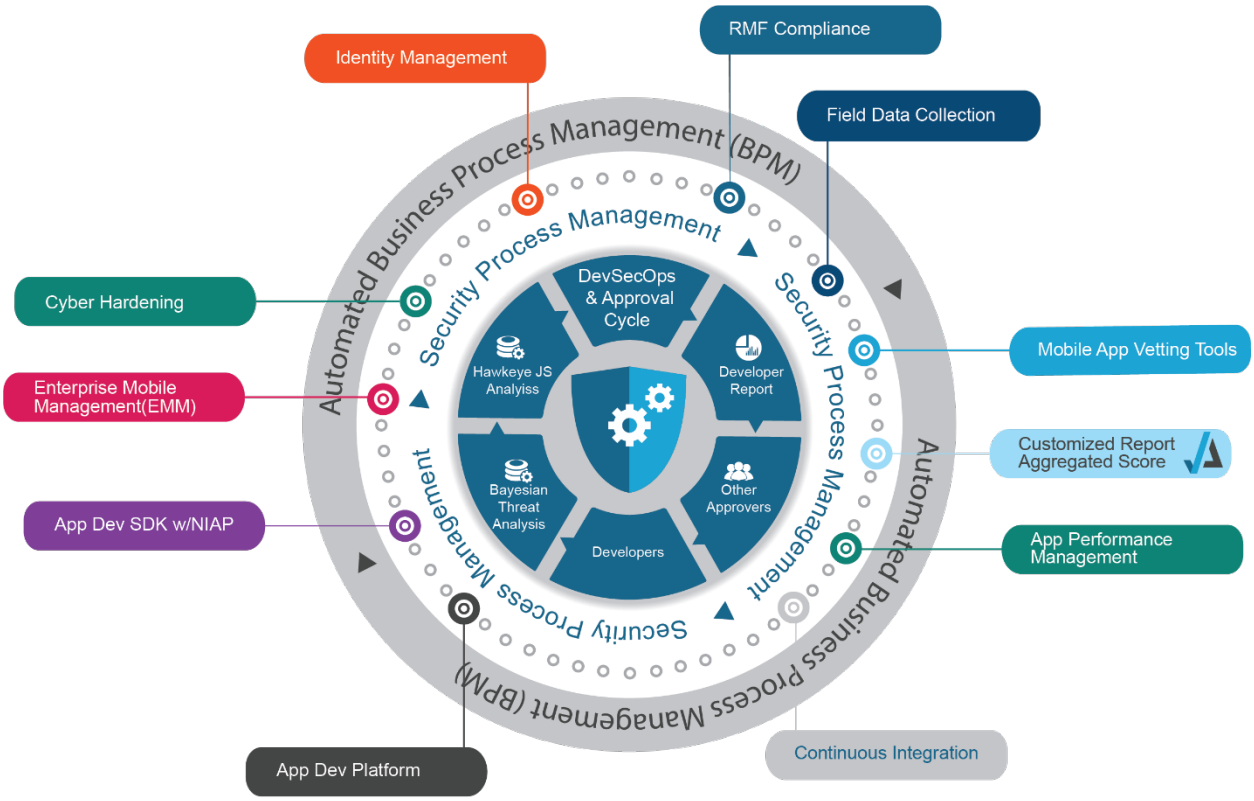

Figure 1: Apcerto Mobile Application Orchestration Platform

In this Final Technical Report, a detailed description is provided for all efforts and development initiatives undertaken by Apcerto through the Performance Period of the subject R&D Agreement.

3. Project Methods Assumptions and Procedures

3.1. Support to NIST for Static Analysis Technology Exposition (SATE) VI Mobile Track

Upon award of the Cooperative Agreement to Apcerto, it was identified by DHS S&T that an initial priority element within Apcerto's research and development effort is to provide support to DHS S&T's partnership with the National Institute of Standards and Technology (NIST) for the Static Analysis Tool Exposition (SATE) VI research project in its newly introduced mobile application testing tool analysis component. The core of the SATE activity was to invite static analysis tool vendors to participate in analyzing software with known vulnerabilities. The end goal of the activity was to measure the accuracy of those tools in successfully identifying the vulnerabilities.

Under this effort, seven (7) mobile application vetting vendors participated on a voluntary basis in an 'experiment' of inspecting fabricated malicious or compromised apps and submitting their results to NIST for analysis and evaluation.

Apcerto's platform provided an automated testbed for the normalization of the collected vendor test results, and translation of their respective outputs to a scoring system. Apcerto produced a single standardized report to compare and contrast vendor testing methodologies and highlight industry best practices.

The SATE Mobile Track testing included running seven (7) test cases aimed at measuring the efficiency of mobile app vetting solutions. Each test case included a number of mobile vulnerabilities, the detecting of which each vendor would be measured against. In this process, Apcerto provided support to NIST in evaluating the vendor results by implementing an automated natural language. Specifically:

- Apcerto implemented a natural language algorithm based on requirements to include all NIAP Mobile Protection Profile and eleven CWE's
- Apcerto integrated each vendor tool's report into the Apcerto platform, and implemented a common framework for all vendor reports
- Apcerto implemented the REST interface to receive scores from each vendor
- Apcerto created a virtual cloud environment to run vendor algorithm testing
- For each test case and each vendor tool, Apcerto provided JSON reports for each of the NIAP and CWE's implemented
- Finally, Apcerto compared each report against expected results

With test case retrieval and result set submission being facilitated through the Apcerto orchestration platform, NIST was able to conclude that the seeded "vulnerabilities were identified at approximately 35% when looking at all participant groups across all vulnerabilities and all test cases. Furthermore, the identification of CWEs was at roughly half the rate of NIAP vulnerabilities."[1] Apcerto's primary conclusion was that since all vendors were allowed to submit data in their tool-native formats, it resulted in bigger than expected challenges in machine-aided review of the results. It would be our recommendation that in future iterations of similar experiments, a more formalized and structured submission format would be prescribed to the vendors to improve the automation and response times of this analysis.

3.2. Fine-Tuning and Automating the App Vulnerability Analysis Mapping to NIAP Protection Profile Standards

NIAP Protection Profile is the de facto standard for mobile application security baseline in the federal government. Many agencies, particularly DOD, wish to have their enterprise and classified / sensitive information-containing apps to be vetted against these criteria to provide a safer mobile infrastructure. This was recently further solidified by the Defense Department in

[1] NIST Report "Static Analysis Tool Testing (SATE) VI: Mobile Track Report" by Michael A. Ogata

officially signing a memo to establish NIAP as the baseline security standard for mission-critical mobile apps.

Apcerto's objective was to ensure accurate interpretation of the NIAP criteria within Apcerto's app analysis and provide the highest level of automation possible in mapping the app vetting results to the NIAP security profile. At the beginning of the research program, Apcerto's technology enabled automated mapping to 22 out of (then) 26 NIAP Protection Profile criteria. However, there was a level of vagueness in the interpretation of some of the criteria which resulted in "warn" or "unknown" results. Our goal under this task was to further define the criteria and increase levels of automated mapping to the NIAP criteria with reliable "fail/pass" results.

In order to achieve these results, Apcerto undertook the following activities:

- Analysis of current Apcerto NIAP mapping capabilities, identification of ambiguities and gaps
- Discussions and collaboration with NIAP to ensure accurate interpretation of the NIAP business rules
- Collaboration and discussions with a NIAP certified laboratory, Acumen Security (since acquired by Intertek, a leading Total Quality Assurance provider to industries worldwide)
- Consultations with Stephen M. Dye, a mobile security policy expert and creator of technical policy and implementation guides for the DoD cyber security purposes. Mr. Dye co-authored the Mobile Application, Operating System and Mobile Application Store (MAS), Mobile Device Manager (MDM) Security Requirements Guide (SRG) for the DoD, and also authored the AirWatch MDM Secure Technical Implementation Guide (STIG). He has continued to support the policies through interfacing with multiple government departments, and companies in the mobile eco system and application testing space.
- Collaboration with Monkton, a company that developed the Rebar middleware development environment to enable building of secure and compliant mobile solutions. Using this development environment, Monkton developed a mobile application which was then put through the NIAP Protection Profile certification process conducted by the Acumen Security lab. Upon putting the Acumen-certified app through the Apcerto app platform, we were be able to further evaluate our framework NIAP mapping capabilities and identify gaps where further definition was needed.
- Re-evaluation of the existing scoring system and transition to a 100-point scale for more accuracy - a task very complex nature requiring numerous algorithm adjustments. As Apcerto continued its NIAP scoring related development efforts, each additional open source tool and technique used needed to be integrated in a rational way with the NIAP scoring engine, which was updated and evolved along the way as a result.

At the conclusion of this task, Apcerto performed an internal test of the now improved app vetting platform and its NIAP automation capabilities. Apcerto performed a vulnerability assessment on three (3) Android mobile applications provided to us by Glacier's (Core, Messenger, and Voice). Through joint evaluation of the business rules around Android risk vectors within our framework, it was identified that certain software and coding adjustments were still necessary for more accurate NIAP mapping results. These fixes were completed accordingly.

3.3. iOS Mobile Application Security Vetting Capability Development

The Apcerto platform evaluates the risk of vulnerability in mobile device apps by using static and dynamic analysis techniques. The tool uses features extracted from the app under examination and uses machine learning algorithms to calculate its risk level before the app's release to an enterprise app store. At the start of the program, Apcerto offered risk evaluation capability within Android OS only, but lacked similar functionality for the Apple mobile operation system, iOS platform, which is being widely used in federal and commercial space.

Under this effort Apcerto's goal was to expand existing capabilities to perform static and dynamic analysis within the iOS platform. This included generating Bayesian and other machine learning algorithms to assess the riskiness of an iOS app, as well as use features of the analysis to run against the NIAP PP.

It was intended to develop evaluation models for machine learning, based on a mixture of good, bad and "in-between" apps. Apcerto aimed to study known iOS malware categories and identify apps with this behavior. Using the gathered research data, Apcerto intended to create algorithms to score coverage for iOS based on the NIAP PP security criteria. Using the features available from the new analysis tools, we would create feature vectors for all good and bad applications in our corpus and train our algorithms. Due to the lack of a sufficient volume of binary or source codes for iOS apps with known good and bad behaviors, Apcerto was unable to create a successful machine learning evaluation model, which necessitated a change in direction towards identifying existing commercial and open source app vetting tools with iOS capability to explore the potential of integration with an existing software.

The process of enhancing Apcerto's native capability to vet iOS-based apps and evaluate them for risky behaviors against the industry prevalent security standards, proved to be a long term effort around decomposing an app at both a dynamic and static level. Using both static tools (such as Infer, Biplist, Class-dump, Tailor, JTool, Clang Static Analyzer, Antlr) and dynamic (Frida) open source tools allowed us to statically analyze several application characteristics at the source code level. This analysis allowed us to look specifically at what the coder is doing that may or may not be risky. To understand added libraries and overall low level API interactions, the Frida tool allowed us to create a dynamic run time call graph of the running application. To fully enable run-time iOS analysis, a longer term effort would be needed to build these capabilities in a more scalable and automated way, outside of the scope of this agreement.

Finally, Apcerto was successful in automating the integration between the commercially available NowSecure app vetting platform and incorporating their existing iOS capability into the Apcerto app vetting tool.

3.4. Integration with Enterprise Mobility Management (EMM) Platforms

In its Mobile App Security Orchestration Platform design and development, Apcerto recognized the critical need to partner with different domains of the mobile security ecosystem and the indisputable advantages in bringing them together in a unified platform. For example, by integrating with enterprise mobility management solutions, Apcerto could address the DHS S&T objective of continuous monitoring and increased level of automation.

Therefore, Apcerto set out to integrate with three (3) major EMM platforms: VMware AirWatch, MobileIron, and IBM MaaS360. The objective was for Apcerto tie directly into the each of the EMM systems to get notifications when apps are being requested for download. This would trigger obtaining the application's .apk or binary file for ingestion into Apcerto, performing security analysis, and producing a detailed report. The EMM system would then automatically receive the app's vulnerability score, and marking of the app as good, bad or malware.

In addition to coding all common EMM functionality, the following specific steps were taken toward the completion of Apcerto integration with each of the individual EMM platforms:

For its integration with VMware AirWatch, Apcerto obtained access to VMware Workspace ONE (AirWatch) for development and testing, provisioned the VMware partner environment CN877, and designed a workflow to integrate the Apcerto framework to EMM frameworks using REST API's. For the benefit of a security analyst, Apcerto created automated workflows for new apps to appear in the enterprise app store; for AirWatch customers we created an automated apps scoring workflow.

The steps in the integration with MobileIron included studying the MobileIron Event Notification Service and Common Platform Services API Guide, evaluation of the MobileIron app approval workflow, establishing access to the app exchange submission portal, and system integration into the MobileIron web application.

In partnership with IBM, Apcerto created an automated apps scoring workflow between our platform and MaaS360. Upon establishing access to the IBM Security AppExchange Submission Portal, Apcerto created a Postman collection to access the IBM Approve Services, and completed the system integration of IBM MaaS360 tasks into web application, which is now live on production portal and available to IBM customers through the IBM App Catalog. The offering was launched Beta in order to get more customers adopt and send feedback.

3.5. Integration with App Development Platforms

Similar to the recognized need to integrate with different domains of the mobile security ecosystem, Apcerto perceived the inevitable connection point between mobile app security and mobile app development. In order to enable mobile app life cycle from a to z, Apcerto sought out to integrate with an app development platform to offer automated workflows between the security and development functions of a mobile app's lifecycle.

Apcerto identified the Kony (now Temenos) no-code/low-code app development environment as the most suitable commercially available system to fold into the Apcerto platform. By syncing up the often disjointed app development and security elements, Apcerto orchestrated a seamless and automated workflow from app conception, to app dev in an agency-branded component marketplace (with reusable elements), to testing, to distribution, to continuous monitoring. This enables agencies build reliably secure mobile apps at scale.

Our integration effort included creating a methodology for Apcerto to understand a non-Java native app and creating an associated score, as well as creating automated workflows to send developer assets (code/apk) to Apcerto. In addition, Apcerto integrated with Kony static code Hawkeye analysis tool, and incorporated the Kony static code Hawkeye JavaScript output into Apcerto report.

3.6. Commercialization and Public Outreach Task

Apcerto's communication and commercialization efforts intend to promote all 5 emerging technology performers (Apcerto, Lookout, Qualcomm Technologies, RedHat, United Technologies Researcher Center (UTRC)) in receipt of the DHS S&T CSD BAA research and development awards in July, 2017, as well as pursue 'transition to market' goals set by DHS S&T. Apcerto's commercialization and public outreach task under our project took shape as a multi-prong approach to include the following components to include (i) industry events, (ii) written media / PR, (iii) audio-visual media / PR. Below is a listing of major outreach activities and products completed within this task.

Throughout the course of the contract, Apcerto attended and/or exhibited several emerging technology promotional forums, technology conferences, workshops, and IT summits, including:

- The ACT-IAC Executive Leadership Conference 2017, Williamsburg VA
- The ATARC Federal Mobile Technology Summit, Oct 2017, Washington DC
- Recurring Department of the Veterans Affairs – Underwriters Laboratory (UL) Medical Device Cybersecurity Project Team Call
- DHS S&T Mobile Tech Forum hosted by the Federal CIO Council's Mobile Technology Tiger Team, April 2018, Washington DC
- Secure Mobile Application Development Workshop, hosted by DHS S&T Mobile Security Research and Development (R&D) Program, August 2018, Washington DC. Apcerto prepared a live demonstration of its secure app development platform. This presentation aimed at showcasing the automated workflow through Apcerto platform – from its integrated no code/low code omni-channel development environment, through patented Apcerto app vulnerability checking algorithms, to third party integrated app vetting tools, back to Apcerto for producing an aggregated security score and detailed report, and finally to a major Enterprise Mobility Management (EMM) system for distribution to end users. Apcerto engaged with the audience in a Q&A session and generated new potential customer leads for pilot project engagement.
- ATARC Federal Mobile Technology Summit, Aug 2018, Washington DC. This educational, one-day symposium examined the mobile tools and techniques being used by the Federal Government to provide agencies with greater efficiency and cost savings.

Apcerto engaged in live presentations of its secure app development platform, lead generation through potential customer conversations, and exploration of potential partnerships with fellow exhibitors.

- Mobile World Congress Americas (MWCA), Sept 2018, Los Angeles CA. At this event with over 1,000 expected exhibitors, per the requirement by Apcerto's DHS S&T Program Manager, Apcerto secured an exhibition booth for DHS S&T to showcase its twelve (12) front running performers and their innovations in mobility and cybersecurity research and development
- DHS S&T Cybersecurity and Innovation Showcase, March 2019, Washington DC. This S&T flagship event attended by over 700 industry and government representatives presented a tremendous opportunity for Apcerto to build awareness about its innovative technology platform and forge new partnerships with other R&D focused organizations in the cyber security field.
- ATARC Federal DevSecOps Summit, March 2019, Washington DC. Apcerto participated as a Technology Showcase Partners at this educational, one-day symposium with focus on examination of DevOps tools and techniques being used by the Federal Government to provide agencies with greater efficiency and cost savings.
- RSA Federal Summit Presented by ATARC, March 2019, Washington DC. Continuing the tremendous momentum of the RSA Conference in San Francisco, ATARC presented its first annual RSA Federal Summit on March 26, 2019 at the Marriott Metro Center in Washington, D.C. where Apcerto participated as an Exhibiting Partner. This educational, one-day event provided a platform for subject matter experts from the Federal Government to discuss the latest tools, trends and techniques in Cybersecurity. A MITRE-ATARC Cybersecurity Collaboration Symposium allowed for representatives of the government, academia and industry to brainstorm and whiteboard a variety of security topics including CDM and RMF: Complementary Roles in Agency Cybersecurity; Cybersecurity and Federal Data Protection; and Cybersecurity Threat Defense of the Future.
- ATARC Federal Cloud and Infrastructure Summit, June 2019, Washington DC. Apcerto participated as a Technology Showcase Partners at this educational, one-day symposium with focus on examination of Cloud integration and techniques being used by the Federal Government to provide agencies with greater efficiency and cost savings.
- DevSecOps: Mobile Application Development Workshop, hosted by DHS S&T Mobile Security Research and Development (R&D) Program, July 2019, Washington DC. This event featured presentations and hands-on tutorials from three of the Program's mobile application (app) security development performers. Apcerto, in tandem with Kony, presented at this workshop on our Mobile App Security Orchestration Platform/Certification Tool for mobile application development and app vetting. Apcerto's presentation covered our solutions for normalizing and rating mobile apps based on predefined standards and embedding security throughout the mobile app development platform.
- Mobile World Congress Americas (MWCA), October 2019, Los Angeles, CA.

Under this Task, Apcerto also conducted extensive outreach to most major U.S. Civilian and DOD agencies to gather data on their current mobile application development and security efforts, major challenges and explore potential pilot use cases.

3.7. Federal Mobility Landscape Survey Project

As a final component of the Research and Development Cooperative Agreement between Apcerto and DHS S&T, Apcerto was guided to conduct a Federal Mobility Landscape Study on the current status, challenges, successes, and vision for the future in the Federal Mobility landscape.

To conduct this study, Apcerto created a comprehensive questionnaire to survey the primary mobile application development and security stakeholders in both Civilian and Defense agencies, targeting both executive and practitioner level individuals to ensure a wide range of perspectives, including:

- Information Technology Executives
- Mobile Application Development experts
- Mobile Security experts

The survey (attached to this report) was distributed over a period of two months to 5,000 plus target responders and received a total of 68 responses. Upon analyzing the received responses, ATARC made several key conclusions, as provided below, and also produced a White Paper to summarize the emerging trends (provided as an attachment to this report)

Key Conclusions from Federal Mobility Landscape Survey:

- 68 total responses received from 24 different federal agencies
- Over half responders are technology executives (indicates higher level visibility into issues and focus areas)
- Overall mobility status rated at 6.26 out of 10 – encouraging but with room for improvement
- Overwhelming hinderance to larger mobility adoption is security concerns
- Agency focus in terms of using mobile apps is 2/3 on enterprise internal/productivity versus 1/3 on public facing (this raises a question whether a higher percentage of public facing app use would drive faster change towards a mobile friendly Government)?
- Overwhelming leaning towards iOS platform / devices over all others (twice more than second closest Android)
- IoT seems not on the radar for most agencies
- COVID-19 impact: while more agencies have remained static in mobility policy, than implemented change – the latter have tackled better definition of mobility policy, and to a lesser extent opening it up (likely tied back to those security concerns)
- Agencies rely on in house teams more for app development (80%) than for app security (66%). Similar trend is supported by acquisition vehicles being used more for security than dev tools/services
- Use of agency specific security standards for app security is relatively high (18%), showing that a lot of custom security features are needed / policies must vary from agency to agency

4. Results and Discussion

As a result of the research and development work conducted by Apcerto, and as detailed in Section 3 of this report, the following list represents major accomplishments fulfilled under this Agreement:

(1) Apcerto provided support to NIST in conducting its mobile security tools' capabilities evaluation and comparison analysis under the Static Analysis Technology Exposition (SATE) VI Mobile Track. By implementing an automated evaluation process, Apcerto helped NIST achieve a quicker and more efficient methodology for performing their tools analysis. Apcerto also helped identify a recommendation for improved analysis for the next SATE Mobile track iteration.

(2) Based on many consultations and extensive analysis of the code, Apcerto accomplished the complex algorithm adjustments required for re-evaluation of the existing scoring system and transition to a 100-point scale for more accuracy. In addition, Apcerto completed the integration of several open source tools and techniques into its NIAP scoring engine, which further updated and evolved its vulnerability detection and NIAP PP mapping capabilities.

(3) Apcerto was successful in expanding its application security vetting capability to iOS mobile apps, by automating the integration between the NowSecure app vetting platform and incorporating its iOS capability into the Apcerto app vetting tool.

(4) To advance the automation and ability for Enterprise Mobility Management (EMM) platforms to categorize employee requested apps as good / bad / malware, Apcerto demonstrated integration capability with three major EMM systems: VMware AirWatch, MobileIron, and IBM MaaS360.

(5) Apcerto successfully integrated with a no-code/low-code application development platform, Temenos (previously Kony), in order to create a seamless DevSecOps methodology for embedding app code vulnerability evaluation checkpoints all along the development process. This created automated workflows between the security and development functions of a mobile app's lifecycle.

(6) Under its commercialization and public outreach task, Apcerto attended and presented at over a dozen emerging technology conferences, workshops and demonstration events. Among the outreach initiatives, Apcerto supported the participation of other DHS emerging tech performers at the reputable Mobile World Congress Americas in two consecutive years.

(7) As the final task under this Agreement, Apcerto successfully completed a Federal Mobility Survey Project, studying and reporting on the current status, challenges, successes, and vision for the future in the Federal Mobility landscape.

5. Conclusions

Based on the completed development work towards achieving the objectives as detailed in this Technical Report, as well as on numerous consultations with mobile app security executives, practitioners and evangelists within the Federal Government, Apcerto has made the following conclusions:

- Mobile app security should not be addressed in a vacuum and separate from mobile app development phase. Rather security functionality must be embedded early on in the mobile app lifecycle, in alignment with the DevSecOps principles.
- For best results in increasing app development efficiency and security, it is advantageous to utilize a cohesive unified mobile app development and security ecosystem, with built-in application programming interface (API) connections to other mobile app lifecycle components.
- While Apcerto greatly updated and evolved the automation in its vulnerability detection and NIAP PP mapping capabilities, it was evident that a certain minimum level of manual oversight and interpretation is necessary for reliable results to be produced by the NIAP scoring engine.

6. References

Ogata, Michael, "Static Analysis Tool Testing (SATE) VI: Mobile Track Report" *NIST Report,* 2018

7. List of Symbols, Abbreviations, Acronyms

ATARC	Advanced Technology Academic Research Center
BAA	Broad Agency Announcement
CDM	Continuous Diagnostics and Mitigation
CIO Council	(Federal) Chief Information Officers Council
COVID-19	Coronavirus Disease of 2019
CWE	Common Weakness Enumeration
DHS S&T	Department of Homeland Security, Science & Technology
DoD	Department of Defense
EMM	Enterprise Mobility Management
JSON	JavaScript Object Notation
MAS	Mobile Application Store
MDM	Mobile Device Manager
MWCA	Mobile World Congress Americas
NIAP PP	National Information Assurance Partnership Protection Profile
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework
SATE	Static Analysis Tool Exposition
SRG	Security Requirements Guide
STIG	Secure Technical Implementation Guide