GEORGE MASON UNIVERSITY

CYBER SECURITY ENGINEERING

CYSE 492/493 INDUSTRY-SPONSORED SENIOR DESIGN PROJECTS

MAY 10, 2018

GEORGE MASON UNIVERSITY | Volgenau School of Engineering

FROM THE PROGRAM DIRECTOR

The Senior Advanced Design Project or “capstone” presentations are the culmination of the final experience for the first graduating class of the first Bachelor of Science in Cyber Security Engineering (BS CYSE) degree program in the country. The CYSE 492/493 Senior Advanced Design Project is a two-semester project sponsored by industry. The students work with sponsoring organizations 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 and make significant contributions with guidance from our faculty and subject-matter experts. The students apply the cumulative technical, communication, and teamwork skills that they have learned toward one exciting and meaningful project. I am pleased to acknowledge how fortunate we are to have sponsorships from BAE Systems, Booz Allen Hamilton, General Dynamics, Leidos, and Vencore. They have provided not only technical projects, but also guidance in our curriculum.

I would especially like to acknowledge Professor Gino Manzo for his efforts as the instructor for the Senior Advanced Design Project. He has brought expertise and rigor to the projects. His direction has facilitated a rich and impressive group of projects for our students. In addition, he was instrumental in creating the BS CYSE Industrial Advisory Board. The board has also provided invaluable insight into cyber security engineering and the needs of our constituents.

The Senior 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 with the pursuit of master’s degrees. 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, PhD
Director, BS Cyber Security Engineering Program
Professor, Systems Engineering and Operations Research Department

FROM THE INSTRUCTOR

Welcome, and thank you for attending our very first industry-sponsored Senior Design Capstone Poster Paper Event! Today, we are celebrating the achievements of 30 students who have diligently worked on five 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 also the customers. With advice from subject-matter experts, the teams complete meaningful engineering projects.

Each 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 the project plan and then executing the plan. Throughout two semesters, they are guided in technical areas by the subject-matter experts and mentored by the instructor in a host of professional and business skills such as 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 scheduling conflicts and meeting deliverables. Students are responsible for managing the customer relationship and solving the many real-life issues that undoubtedly occur.

This program is only possible with the dedicated support from our sponsors and subject-matter experts. Thank you for engaging with our program and helping make our students more valuable. I also want to 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.

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.

Gino Manzo
Industry-Sponsored Senior Design Capstone Instructor
Professor of Practice

AGENDA

2–2:30 p.m. ..... **Sign-in, review posters**

2:30-3:30 p.m. ..... **Welcome**
Professor Gino Manzo

Remarks
Dr. Peggy Brouse
Dr. Kenneth Ball, Mason Engineering Dean

Short team presentations

3:30–4:30 p.m. ..... **Review posters**

4:30 p.m. ..... **Best Paper Awards**

5 p.m. ..... **Adjourn**

OUR SPONSORS

With gratitude and appreciation for your dedicated support.

BAE SYSTEMS

Booz | Allen | Hamilton

GENERAL DYNAMICS

leidos

VENCORE™

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/CUSTOMER

BAE SYSTEMS INC.
Doug Steil, Larry Bailey

BOOZ ALLEN HAMILTON CORPORATION
Patrick Schurr

GENERAL DYNAMICS CORPORATION
Robert Carey

LEIDOS INC.
Dan Kovaluk, David Szczesniak

VENCORE INC.
Barry Barlow

PROJECT/SUBJECT-MATTER EXPERT

Cross Domain Solution
Graham Archer

Cyber Security Automation through Machine Learning
Peter Fonash

Quantitative Model for Cybersecurity Products
Richard Lord

Android Custom ROM
Ammar Palla, Yaron Eidelman

Vulnerability Assessment for a Smart Grid to IoT Environment
Kai Zeng

Zabi Tora, Erika Strano, Jonathan Wiley, Simplice Njike, Ankur Goel

Cross Domain Solution

SPONSOR:
BAE SYSTEMS INC.

SME: ***Graham Archer***

CHALLENGE/PROJECT SUMMARY: *Our team will design and implement a mandatory access control security policy that will allow data to flow one way through a pipeline on BAE Systems' own operating system.*

STUDENT: ***Zabi Tora,*** *Fairfax, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To learn as much as possible and to hopefully help make the world as secure as possible in the future.*

CLASS COMMENT: *The class taught me how to work well in a team. Also, communication is very important when working with customers.*

STUDENT: ***Jonathan Wiley,*** *Washington, D.C.*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To help make an impact in the cybersecurity industry by raising the awareness of the need for secure platforms.*

CLASS COMMENT: *The importance of teamwork and the benefits of a team were highlighted in this course.*

STUDENT: ***Ankur Goel,*** *Fairfax, Virginia*

DEGREES: *BS, Bioinformatics; BS, Cyber Security Engineering*

ASPIRATIONS: *I fulfilled my dream in attending medical school, but due to complications I was forced to leave. My next big aspiration is to combine the medical field and cyber to protect hospitals.*

CLASS COMMENT: *This class introduced me to how the real world operates. Provides an understanding about deadlines, project reviews, customer meetings, and more.*

STUDENT: ***Simplice Njike,*** *Alexandria, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *I want to work as a professional security engineer.*

CLASS COMMENT: *The capstone class has taught me a lot of skills that would help in my future career. From the knowledge of work ethics to working on a project with customer`s requirements, I have learned how to communicate with my peers and my customers as well.*

STUDENT: ***Erika Strano,*** *Warrenton, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *I aspire to utilize both my technical and communication skills to demonstrate the capabilities of game-changing products.*

CLASS COMMENT: *This class taught me the importance of keeping constant communication with customers to ensure satisfaction.*

CROSS DOMAIN SOLUTION

Ankur Goel, Simplice Njike, Erika Strano, Zabi Tora, Jonathan Wiley

Sponsor: BAE Systems

Subject Matter Expert: Graham Archer

BACKGROUND

- A Cross Domain Solution (CDS) has the capability to validate, inspect and santitize incoming data.
- The three phases, validation, inspection, and sanitization are non-bypassable and one way.
- A CDS is a very secure layer-7 firewall/ router, that guarantees only clean, correct, and valid data is allowed to flow.
- Ensures secure information sharing between networks of various security classifications.
- CDS's are also known as "guards."

OBJECTIVE

- Establish a set of accept/reject criteria to allow data to flow one way through a pipeline of processes.
- It is to be implemented on the STOP OS, which allows for a secure and un-hackable CDS.

TOOLS

- We used an operating system developed by BAE Systems, called STOP OS, to implement our CDS.

Figure 1: This is the security label that is defined within STOP.

APPROACH

The CDS will:

1. Receive files delivered from a client computer.
2. Detect the presence of the new file and move the file into a filtering area.
3. Filter the file and ensure that it meets the established criteria.
4. Move accepted data to an output area, or
5. Move rejected data to a quarantine area.

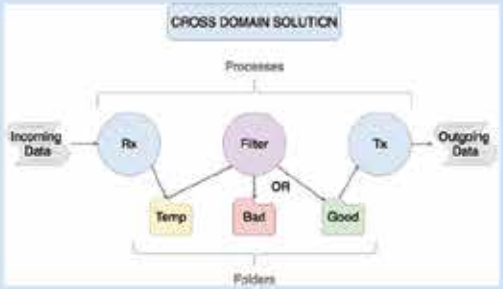


Figure 2: Design architecture of CDS. The three main processes are show, Rx, filter, and Tx. The flow is also noted from the beginning of the CDS to the end.

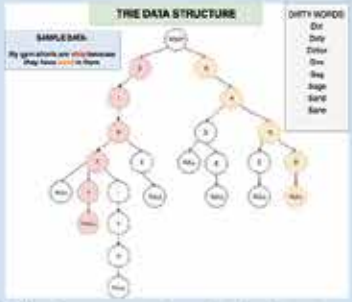


Figure 3: Visual representation of a trie data structure (left).

RESULTS AND CONCLUSION

- Successful implementation of a CDS.
- STOP OS's security labeling makes the CDS virtually un-hackable.
- Having a secure process that allows sensitive information to be transferred between agencies or within military operations prevents information from being leaked, spoofed, or compromised.

Figure 4: Code for the filtering algorithm

ACKNOWLEDGMENT

We would like to thank Doug, Larry, Aaron, and Ben for providing us the training and guidance necessary to complete this project. We would also like to thank the Cyber Security Engineering staff for supporting us during our ups and downs, and for pushing us to success. This project's success was made possible with the help of both entities.

References:

[1] BAE Systems. STOP training manual: an introduction to the stop operating system. BAE Systems, Reston, VA: BAE Systems, 2017

[2] S. Smith, "Shedding light on cross domain solutions," SANS Institute In-foSec Reading Room, Apr., 2018 W.-K.Chen, Linear Networks. and Systems.Belmont, Calif.: Wadsworth, pp. 123-135, 1993. (Book style)

May 10, 2018

Front, Ali Nasir, Sam Dura, Clara Currier. Back, Matt Burke, Richard Seidi (sponsor), Patrick Schurr (sponsor), Rod Wetsel (sponsor), Steve Zamory

Cyber Security Automation through Machine Learning

SPONSOR:
BOOZ ALLEN HAMILTON CORPORATION

SME: ***Peter Fonash***

CHALLENGE/PROJECT SUMMARY: *Automate security processes in support of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program.*

STUDENT: ***Steve Zamory,*** *Fairfax, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To fix machines that don't even know they're broken.*

CLASS COMMENT: *The class has provided a sense of what kind of information and responsibilities we will be exposed to in industry.*

STUDENT: ***Clara Currier,*** *Springfield, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Become a leader in the Department of Defense, publish a paperback graphic novel, and publish a paper in an academic journal.*

CLASS COMMENT: *Good practice with engaging customers and refining problem scope.*

STUDENT: ***Ali Nasir,*** *Fairfax, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Become a security expert and pursue the management career track.*

CLASS COMMENT: *This class provided great learning experience of proposal writing and dealing with RFPs. Learned about the 10K report.*

STUDENT: ***Matt Burke,*** *Fort Sill, Oklahoma*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Start a nonprofit business in the robotic agriculture area.*

CLASS COMMENT: *Enjoyed working with Enterprise toolsets.*

STUDENT: ***Sam Dura,*** *Fairfax, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To give back the knowledge and skill set I learned to the community.*

CLASS COMMENT: *Helped me to see a glimpse of the future.*

Booz | Allen | Hamilton

Cyber Security Automation through Machine Learning

Matt Burke, Clara Currier, Samuel Dura, Ali Nasir, Steve Zamory

Sponsored by Booz Allen Hamilton

SME: Peter Fonash

GEORGE MASON UNIVERSITY

Background

Federal agencies in the United States currently struggle to deploy consistent protocols for addressing cyber events, maintain their computer networks, and control access to their systems. Civilian agencies in particular may not have developed tools, expert staff, and guidelines required to protect their critical data. Recent incidents such as the data breach at the Office of Personnel Management underscore this need for a government-wide consolidation of defensive tactics, techniques, and procedures.

The Department of Homeland Security (DHS), responsible for maintaining the integrity of computer networks for a variety of federal agencies, has been tasked with providing a set of solutions and security enhancements to better defend federal networks and systems. This project is known as Continuous Diagnostics and Mitigation (CDM).

There are three phases in the CDM adoption process. Phase I targets asset management and accountability and is currently in its implementation stage. Phase II targets user credentials and privileges. Phase III focuses on mitigating potential vulnerabilities and responding to security incidents.

The sub-areas associated with phase III include:

- Incident response
- Boundary protection
- Generic monitoring

Phase II and Phase III workflows are incomplete and do not have concrete specifications for creating a process to deal with an event in their defined sub-areas. This project will target the workflows associated with events that would be generated by the sub-areas in Phase III.

Purpose

This project is intended to implement a cybersecurity automation tool suite in support of the DHS CDM project. Automation is a way to solve important problems in cyber defensive measures. Security operation can be understaffed and unable to digest every piece of threat intelligence and indicators that they come across. Indicator triage and processing are currently too slow and tedious to meet the level of alertness required to protect a system or network.

The end goals of the development of an automated toolset are:

- Lower alert fatigue and heighten the situational awareness of an operator.
- Lower the amount of case noise for smaller operations.
- Achieve some kind of predictive healing to the network through the use of threat intelligence.

Approach

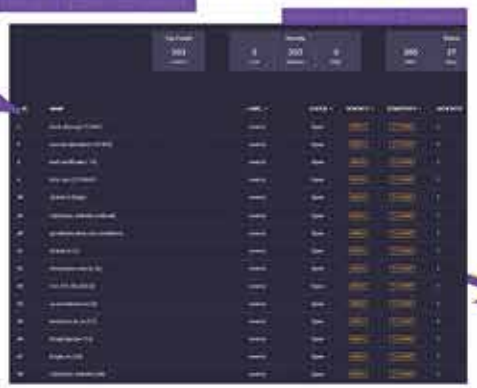
The system's main focus is dealing with the aggregation of threat intelligence data. Not only does the tool focus on this aggregation of threat intelligence data, but also the aggregation of multiple pools of threat intelligence data that are split between products.

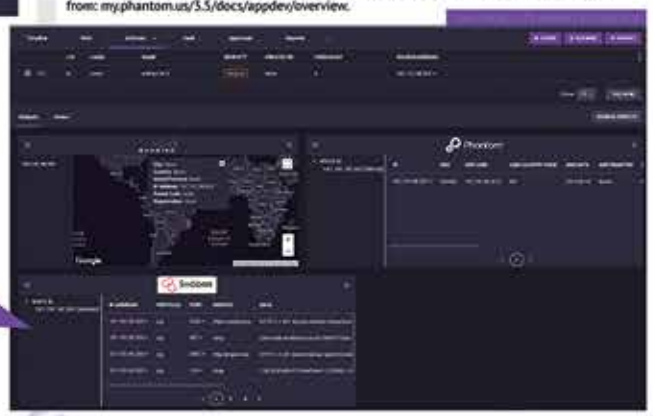
To cut down on costs, the system focuses primarily on open sources of threat intelligence. Using Pulsedive, a threat intelligence aggregator and feed, we were able to aggregate over 40 independent sources of threat intelligence. Our approach was then to track Indicators of Compromise (IoCs) across the multiple pools and see which IoCs were appearing on multiple lists. Our assumption is that if an IoC appears across multiple lists; the risk than an IoC may affect the network is multiplying. With this information, a feedcount metric for IoCs and a threshold for when an IoC crosses a certain amount of pools can be established.

The feedcount metric can be used to create medium- to high-risk tickets so that a security analyst could then cut down on the amount of time they spend on analysing threat intelligence data. Another possible path is using the orchestration tool to start an automated healing action on the network or at the very least present the automated action to be approved by an operator. We experimented with the use of Phantom, an orchestration tool to facilitate ticket processing and security automation. Utilizing Phantom's "playbook" feature can enable operators to use existing solution workflows in tandem with an enhanced and more comprehensive Indicator set.

System Overview

The system consists of several components working in concert. Threat indicators are pulled from 40 different feeds and assembled into an easily workable CSV format to be acted on by a Python script using REST. This data is then sent and ingested by the Phantom orchestrator to generate cases/tickets based on the indicator of compromise. Operators can then dive deeper on the indicator of compromise or have the orchestrator execute playbooks which execute the automated solution based on the threat.





In terms of infrastructure, Phantom Orchestrator runs on a virtual image. Pulsedive runs as a web application that runs separately from our infrastructure.

Results

The system successfully reduces the amount of threat intelligence noise, is able to perform semi-predictive actions on the network in anticipation of threats, and gives the security analyst alerts on growing threat trends in the wild. Through the FeedCount metric we are cutting down on multiple hits on the same piece of threat intelligence and providing this through the Pulsedive application integrated into the Phantom Cyber Orchestrator application store.

Conclusions

- Automated actions on networks need to be taken carefully as they can cause destruction rather than a healing effect.
- Certain automation workflows can be condensed through the use of tool sets (Pulsedive) in order to remove computational load.
- Sophisticated machine learning algorithms can be hard to develop without large datasets and horsepower.
- Programmed static rulesets can bring forth semi-intelligent decision making with automation.

Acknowledgements

We gratefully acknowledge the guidance from our sponsor's representative, Patrick Schurr. Additionally, our subject-matter expert, Peter Fonash, and Professor Gino Manzo provided valuable insight and suggestions. Threat indicators were graciously provided by Pulsedive.

References

S. Heckman, and L. Williams. "A model building process for identifying actionable static analysis alerts," in *Software Testing Verification and Validation, 2009. ICST'09. International Conference on*, pp. 161-170. IEEE, 2009.

U.S Department of Homeland Security. (n.d.) "Continuous diagnostics and mitigation program". Retreived from: www.us-cert.gov/sites/default/files/cdm_files/CDM_ProgramOverview.pdf.

Phantom App Developer Documentation. (n.d) "Phantom version 3.5 documentation". Retrieved from: my.phantom.us/3.5/docs/appdev/overview.

Allen Shen, Shival Puri, Hyun Kim, Jacob Dulaney, Richard Lord (sponsor), Ben Krause, Luis Gustavo Loayza

Quantitative Model for Cyber Security Products

SPONSOR:
GENERAL DYNAMICS CORPORATION

SME: ***Richard Lord***

CHALLENGE/PROJECT SUMMARY:

- *Current cybersecurity product selection for incorporation within a network is not based on meaningful measures, nor are its individual contributions to actual network or system security measured.*
- *This project goal is to develop a model that can be used to determine the qualitative value of similar security products against a given set of risk mitigation security controls.*

STUDENT: ***Allen Shen,*** *Herndon, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Learning and applying information security concepts and skills into the real-world workforce.*

CLASS COMMENT: *Good way to work with a real-world customer on a project with deliverables. Also, a great way to advance business and professional skills.*

STUDENT: ***Jacob Dulaney,*** *Virginia Beach, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Develop a good understanding of cybersecurity concepts while learning how to apply them professionally in the workplace.*

CLASS COMMENT: *Learning how to work in a team environment and learn how to manage myself, as well as others, in terms of time and resources.*

STUDENT: ***Ben Krause,*** *Virginia Beach, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Improve my skills and become a valued member of the cybersecurity community.*

CLASS COMMENT: *It was a good opportunity to learn how to act in a professional team environment and how to develop the necessary documentation for a project.*

STUDENT: ***Shival Puri,*** *Sterling, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Apply and advance my skills in cybersecurity to contribute to the success of major IT companies.*

CLASS COMMENT: *Enjoyed being able to learn how projects work in the real world and advance both my technical and business skills.*

STUDENT: ***Hyun Kim,*** *Seoul, South Korea*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Adapt to quickly changing IT industry to provide solutions to newly emerging security challenges.*

CLASS COMMENT: *It was a great opportunity to experience solving real-life problems working closely with a major IT company.*

STUDENT: ***Luis Gustavo Loayza,*** *Alexandria, Virginia*

DEGREES: *BS, Cyber Security Engineering; MS, Computer Forensics*

ASPIRATIONS: *Continue to learn about technologies and strategies to enhance cybersecurity and grow in a leadership role in cyber defense.*

CLASS COMMENT: *A great way to learn about the expectations of an engineer in the business world and the accountability of one's work.*

Quantitative Model for Evaluating Security Products

Jacob Dulaney, Hyunjoon Kim, Benjamin Krause, Luis Gustavo Loayza, Shival Puri, Allen Shen
Customer: Robert Carey (General Dynamics Information Technology)
Subject-Matter Expert: Richard Lord (GDIT)

GENERAL DYNAMICS
Information Technology

GEORGE MASON UNIVERSITY

PROBLEM STATEMENT

- Current cyber security products are not based on any meaningful measures
- The security tools are advertised on their qualitative features rather than their quantitative measure on how much they improve the security. Sales revolve around these qualitative features

BACKGROUND

- Advantages: can effectively compare different security products with similar features quantitatively by comparing the percentage of improvement in security
- Challenges: complex to develop one model that fits different organizations due to different requirements of each organization

OBJECTIVE

- A model that can be used to determine the quantitative value of similar security products against a given set of risk mitigation security controls at a high confidence and is applicable to all security tools
- Because of our lack of data to work with, our model was to be developed to be flexible to work with any type of data that could be gathered

Figure 1. Measuring Cyber Security

Date: May 10th, 2018

APPROACH

- In order to determine a minimum set of enterprise security controls applicable to cybersecurity devices, we researched standard logical controls related to business. Per the scope of our project, we did not review policy or physical controls
- Our research references previous work done by leaders in cybersecurity such as SANS Institute, the National Institute of Standards and Technology (NIST) and NSS Labs
- We broke up the Open Systems Interconnection (OSI) model into each of its 7 layers. We identified the most critical vulnerabilities of each layer to determine a minimum security control that could be measured in protecting against that vulnerability
- Rather than focus on the effectiveness of one type of cybersecurity device, we developed a controls matrix addressing the seven layer security stack. The controls matrix would allow for a global view of which combinations of devices can protect all seven layers
- We developed tests for each metric setting benchmarks of 80% minimum for a tool to be deemed satisfactory. For highly critical controls, the tool had to pass the metric tests 100% of the time

Figure 2. OSI Model

MODEL

- Layer - Selected layers from Open Systems Interconnect model that were relevant
- Control - Chose security controls that can be implemented at selected layer
- Security Device - Selected most commonly used and effective security tools and determined effectiveness in implementing selected controls

- Metric - Determined attribute of security device when covering selected control
- Test Methodology - Selected way in which metric effectiveness could be tested with necessary equipment
- Benchmark - Determined number at which security device would "minimally secure" selected control

Model Uses:

- Organizations can compare current security controls to those we have defined
- Companies will have better knowledge of what security tools cover each control
- Easier to define which security tools are actually needed - reduces chances of overlapping controls

OUTCOME

- The initial approach of creating minimum security stack of controls fulfilled the criteria needed to develop the model:
  - Create measurable criteria for the model
  - Control the scope of information that would be needed for testing
  - Process is replicable by any third party interested in customization of the model
- Based on the outcome of our research, the following improvements to our approach could solve the issues we faced:
  - Secure a data source before developing the model. The lack of testing data proved very difficult for our team
  - It would be beneficial to narrow the scope to a single tool/device and the role it plays in the network rather than attempt to include many devices for testing
  - Adjust the scope of the model to the data available if comprehensive testing data cannot be found
- We were unable to obtain the testing data necessary to refine our hypothetical benchmarks and testing methodology:
  - Declined by multiple organizations when approached about acquiring data
  - Without testing data, it was impossible to confirm what realistic benchmarks are or a defined testing methodology

CONCLUSIONS

- Creating a quantitative model to measure the effectiveness of a cyber security product is very difficult
  - Various organizations have thrown a lot more resources at this problem and have yet to effectively solve the problem
- The approach to creating a quantitative model should be to create a general, broad model where organizations and individualize it themselves
  - We ended up just evaluating based on a single tool. Companies can use this model to match to certain cyber security products
- Model was created based on methodology of security stack.
  - Metrics and benchmarks were also established but could not be tested fully due to circumstances with obtaining data.
- Future research can include a wide variations of uses everything from another potential risk management framework all the way from individual organization adopting the model for use for their own for things like auditing both internal and external systems for information assurance

ACKNOWLEDGEMENTS

We'd like to thank General Dynamics Information Technology for assistance with this project. We appreciate the support, time, and effect from our customer, Robert Carey, and our SME, Richard Lord. We would also like to thank Peggy Brouse for giving us this opportunity and Gino Manzo for supporting us throughout the project. We'd also like to thank David Raymond from Virginia Tech for his professional advice.

REFERENCES

Figure 1 - "2017 Cybersecurity Value Study." 2017 Cybersecurity Value Study - IcomtoSecurity, Fidelis Cybersecurity.

Figure 2 - Wilson, J. (2015, February 6). IOE/IOT KEY ENABLERS WILL BE UBIQUITOUS CONNECTIVITY & PREDICTIVE MAINTAINENCE. Retrieved April 23, 2018, from

Nadia Jehangir, Jake Steele, Ismail Ahmad, Chase Franklin, Yusif Atasoy, Alex Svinicki

Android Custom ROM

SPONSOR:
LEIDOS INC.

SMEs: ***Ammar Palla*** *and* ***Yaron Eldelman***

CHALLENGE/PROJECT SUMMARY: *Developing a custom ROM to remove the capability of six main hardware components for a Pixel 2.*

STUDENT: ***Ismail Ahmad,*** *Bealeton, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Focus on developing new skills in data science/machine learning fields.*

CLASS COMMENT: *The class provided valuable information that I can apply in my future career.*

STUDENT: ***Chase Franklin,*** *Springfield, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Work for a company as a security engineer while being able to research different and evolving cyber attacks.*

CLASS COMMENT: *You develop much better team skills.*

STUDENT: ***Yusif Atasoy,*** *McLean, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Become successful enough to retire before the age of 45.*

CLASS COMMENT: *I gained more than just technical experience and skills from it.*

STUDENT: ***Jake Steele,*** *Clifton, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Attend a research-intensive graduate program focusing on offensive cyber, eventually moving to a technical lead role.*

CLASS COMMENT: *Provided insight into a realistic project management scenario which I didn't have much experience in.*

STUDENT: ***Alex Svinicki,*** *Williamsburg, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Take part in a technical development role.*

CLASS COMMENT: *It helped me become better at management and helped me obtain technical knowledge.*

STUDENT: ***Nadia Jehangir,*** *Centreville, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Graduate from Mason within the CYSE program, including the computer forensics accelerated master's.*

CLASS COMMENT: *Learned new business skills that will supplement the technical skills I have learned in both programs.*

Securing an Android Custom ROM

Ismail Ahmad, Yusif Atasoy, Chase Franklin, Nadia Jehangir, Jake Steele, Alexander Svinicki
Sponsor: Leidos
Customer: David Szczesniak (Leidos)
SMEs: Yaron Eidelman, Ammar Palla (Leidos)

PROBLEM STATEMENT

- Mobile devices house a variety of features that lead to potential vulnerabilities, especially in high security environments
  - The scope of this project is significant because it can be useful in situations where certain components of a phone are needed to be blocked from use
- Users may want to disable certain features of a phone or protect integrity of the specific areas or events
  - Able to contain valuable data within a location that could otherwise be compromised with the use of a phones full capability

ARCHITECTURE OF AOSP

- An Android Custom ROM (Read-Only Memory) is the firmware of the phone
  - Android is an open source operating system, based off the Linux Kernel, so everyone has access to the code and can alter it
  - Customizing one's own ROM allows for users to alter features already present on the phone as well as add new features or increase functionality
- HAL (Hardware Abstraction Layer) allows to create hooks between the Android platform stack and the hardware
  - Components such as Camera, USB, WIFI, and Audio all contain hardware based components that are called from the HAL

Figure 1: Depicts the [illegible] of the Android framework

OBJECTIVES

- Develop an Android Custom ROM that disables the following components of the phone:
  - Camera
  - USB
  - WiFi
  - Bluetooth
  - Speaker
  - Microphone
- Phone should still be operable after the listed components have been disabled
- Sub-Objective:
  - Develop new ways to disable these components that have yet to be thought of by our SME team and use these methods to disable the components listed above
  - Create a test application that can test each component we disable to measure success

MATERIALS

- Android Phone – Google Pixel 2
- Gitlab
  - Android Open Source Project (AOSP)
  - Build Server
  - Build source using master branch, everyone on the team can individually

Figure 2: GitLab logo

Figure 3: The process of [illegible] code

Alternative Designs

1. Modifying configuration files in order to disable components from where they are called to operate
2. Specific components can be altered at a hardware level
   - Modify the HAL changing how each specific hardware is called
3. Alter manager files:
   - Directly alter the calling of a specific components manager service so when a service/application requests the component the service manager returns "null"
4. USB Condom:
   - We created a proof-of-concept device that will only allow charging to occur without data flow

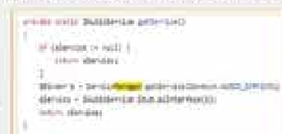


Figure 4: Above shows the [illegible] in order to return null for the microphone and speaker

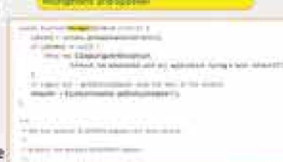


Figure 5: The above depicts the code for the bluetooth manager

Thank You

A special thank you to the following people who have helped us throughout our project; David Szczesniak, Yaron Eidelman, Ammar Palla who have given us guidance as well as the tools to complete the project as well as Dr. Peggy Brouse and Gino Manzo.

SOLUTIONS

- Ultimately the fastest solution we found was method 3 from "Alternative Designs"
  - Alter the service manager to return "null" when it went to request access to certain hardware components managers
  - Create a USB "Condom" that prevents data transfer between the USB port and the phones data
- Using these solutions was the most efficient & fastest method
  - Least error prone methods to use in the time span given to work on the project

RESULTS

- As expected, the edited code allowed us to disable the components
- When the service manager was asked to connect to a certain hardware component, the service manager would bounce back "null" and the application would not have access to the components
- The changes made to the service manager code retained the functionality of the phone which ultimately completed our objective
- The solutions we used maintained functionality of the phone without causing the phone itself to crash

CONCLUSIONS

- Achieved 6 of 6 devices disabled
- Completed Android Test Application in order to check for successful disabling of components
- Potential improvements and continuation of work
  - Toggled class developed within framework level to enable/disable our solutions based on environment
  - Without time constraints our optimal solution would be to develop an entirely new layer within AOSP as our shim
  - USB potentially disabled as a software solution

Date: May 10, 2018

Marco Perdomo, Eric Gum, Mathew Wilkes, Barry Barlow (sponsor), Douglas MacDonald, Natalie Parke, Nicholas Burley, Rida Saref, Andrew Van Pernis

Vulnerability Assessment for a Smart Grid IoT Environment

SPONSOR:
VENCORE INC.

SME: ***Kai Zeng***

CHALLENGE/PROJECT SUMMARY: *We are conducting a vulnerabilty assessment standard operating procedure for a smart grid Internet of Things (IoT) environment to encourage more secure IoT implementations.*

STUDENT: ***Nicholas Burley,*** *Carlisle, Pennsylvania*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To engineer cybersecurity applications and then move to the federal sector.*

CLASS COMMENT: *It was a challenging experience to gain knowledge and understanding about a topic I have never had hands-on interaction with.*

STUDENT: ***Douglas MacDonald,*** *San Diego, California*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Create a more secure world by working with the federal government.*

CLASS COMMENT: *A difficult series of challenges that taught a great many things about teamwork and cybersecurity.*

STUDENT: ***Natalie Parke,*** *Sterling, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To become a digital forensics examiner.*

CLASS COMMENT: *An interesting combination of academic and industry problems.*

STUDENT: ***Matthew Wilkes,*** *Haymarket, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To secure cyber physical systems through research and development.*

CLASS COMMENT: *Real-world problem-solving that challenged our educational background.*

STUDENT: ***Marco Perdomo,*** *Alexandria, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To become a network security expert.*

CLASS COMMENT: *Working with other cybersecurity majors on a task is always a positive experience.*

STUDENT: ***Andrew Van Pernis,*** *Springfield, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To improve cybersecurity for protecting customer data.*

CLASS COMMENT: *A challenging but informative experience working on a real-world problem.*

STUDENT: ***Eric Gum,*** *Woodbridge, Virginia*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *To work for the government doing offensive cyber operations.*

CLASS COMMENT: *The lectures have provided helpful information on resume building and working with a team.*

STUDENT: ***Rida Saref,*** *Casablanca, Morocco*

DEGREE: *BS, Cyber Security Engineering*

ASPIRATIONS: *Work with a government entity to improve the nation's security.*

CLASS COMMENT: *The class provided useful knowledge about the professional world, such as building a resume and how to be a team player.*

Vulnerability Assessment for a Smart Grid IoT Environment

Nicholas Burley, Eric Gum, Douglas MacDonald, Natalie Parke, Marco Perdomo, Rida Saref, Andrew VanPernis, Matthew Wilkes

Sponsored by Vencore, Inc.

SME: Dr. Kai Zeng

Introduction

In comparison to other electrical grids, the Internet-of-Things (IoT) environment of smart grids potentially possesses a more flexible network topology and increased demand-side management efficiency. Using an IoT environment in the electrical grid comes with many benefits, while also posing the risk of opening up the grid to security vulnerabilities. To assess these vulnerabilities, there needs to be a standard vulnerability assessment methodology; however, there is no accepted standard assessment for this environment causing a lack of proper security in smart grids. The basis of this project is to create a standard operating procedure (SOP) for conducting a vulnerability assessment for smart grid IoT environments. The SOP will be a step-by-step instruction for the proper execution of a vulnerability assessment directed towards the IoT network. The foundations of the SOP will come from the research of other vulnerability assessments conducted in electrical grid systems and testing for vulnerabilities using a simulated IoT environment. The environment to be tested is a limited form of JupiterMesh which is a robust, low-power industrial IoT wireless mesh network used in smart grids. Major protocols of this type of IoT environment is Routing Protocol for Low Power and Lossy Networks (RPL) which establishes connections between IPv6 nodes, and IEEE 802.15.4 which defines the operation of low-rate wireless personal area networks. The focus of the vulnerability assessment is to test for vulnerabilities in the usage of RPL on the network layer. A black hole attack is implemented on RPL in the environment to show RPL's vulnerabilities. After the attack, mitigation will be put into effect to attempt to solve the vulnerabilities.

Objectives

- Analyze and mitigate vulnerabilities in smart grid IoT environments and develop a standard for vulnerabilities in these environments to promote more secure and safe environments.
- Analyze the environment, implement an attack against the environment, and develop mitigations to detect and prevent the attack in the environment.
- Establish an Environment Standard Operating Procedure (SOP) based on the analysis and findings of a black hole attack on the environment provided by Vencore Labs to efficiently protect similar environments.

Image taken from: https://www.sensorsexpo.com/iot-ecosystem

Materials and Methods

Materials:

- CyberVan Environment - allows a user to access the JupiterMesh environment via web browser.
  - 8 Linux machines (Nodes 1-8) connected together through RPL and IPv6.
  - Collector node (C) distributes UDP traffic throughout the environment.

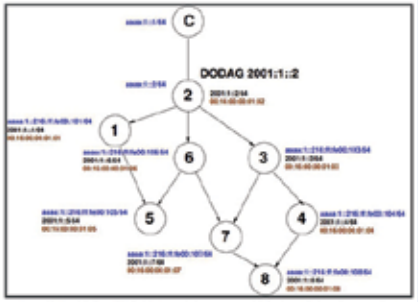


Figure 1: The DODAG of the environment with Nodes 1-8 as Linux "IoT" devices connected wirelessly. Node C is the collector node that is connected by ethernet to node 2 to distribute UDP traffic throughout the network.

Black Hole Attack - Attack against topology:

1. Choose a node to be the malicious node (Node 6 was chosen)
2. Modify the rank of node 6. The rank is a value that its neighbor nodes use to determine the preferred parents. Rank increases as it goes down the DODAG and increases as it goes up the network for each node. Modifying the rank allows greater impact on the topology. RPL code is modified to change the rank.
3. Block UDP traffic distributed by Node C. Ip6tables is a built in firewall for Linux and was used to block traffic.

Mitigation of Black Hole Attack:

- Preventing and detecting the changing of rank for nodes using rank verification.
  - Changing the code of RPL to check the rank of the node.
- Detecting packet loss.
  - IDS to detect increased packet loss over certain time intervals.

SOP Methods: A standard operating procedure is a document that defines the regularly recurring operations relevant to the quality of the investigation. The purpose of it is to carry out certain operations correctly and always in the same manner. The following defines key points in constructing our SOP:

- Identifying key areas of concern where our SOP will be useful (i.e. identifying key vulnerabilities in the CyberVan Environment)
- After identifying the key vulnerabilities, we identified the top three vulnerabilities and answered questions concerning what attacks might exploit those vulnerabilities
- Finally we defined measures to identify and mitigate the key vulnerabilities

Results

Black Hole Attack Results:

- The black hole attack was analyzed using tcpdump on each node to discover packet delivery.
- Modifying the rank proved effective. The code change resulted in the rank decrease for node 6 and the domino effect on its child nodes. Node 5's preferred parent changed to node 6. Node 7's preferred parent changed to node 6. Node 8's preferred parent changed to node 7. Node 4 no longer received data from node 8 because node 7 is now node 8's preferred parent.
- By using ip6tables on node 6, it cut off UDP delivery past node 6 and its child nodes. The ip6tables commands prevented traffic from being forwarded, sent, or received by node 6, meaning traffic sent or forwarded to node 6 was not delivered.
- Figure 2 represents the topology after the attack and the loss of data on the network.

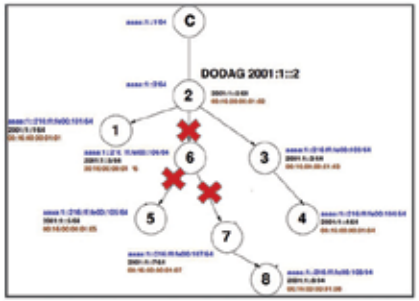


Figure 2: The red Xs represent loss of traffic between the nodes. Node 8 is still able to send traffic to node 7 but is dropped once it reaches node 6. Traffic is dropped for nodes 5, 7, and 2 to node 6. Notice there is no longer connections from 8 to 4, 7 to 3, and 5 to 1.

Mitigation Results:

- The proposed rank verification ensured verifying the parent rank before the node's rank is changed.
- The code (Figure 3) computes the parent's max rank and compares it to the parent rank value sent from DIO messages. The threshold sets a parameter for how much the rank can decrease. If the parent rank is too low, meaning the node can be lying, it returns a NULL value to choose another parent.
- Figure 4 shows the successful results of the rank verification of node 5. Node 5 set the preferred parent as node 1 because it no longer sends UDP traffic to node 6 due to it having an incorrect rank.

Figure 3: The code taken from node 5 that was modified to verify rank. The old code is commented and the new code implements the old code if the verification is successful. The execute_rank_increase function is part of Objective Function 0 which sets the requirements for computing ranks for nodes.

Results (continued)

Figure 4: Tcpdump of UDP traffic on Node 5. Notice that traffic is no longer sent from node 5 to 6. It only sends UDP traffic to node 1, a safe node. Tcpdump is a built in linux command to monitor traffic

Final SOP:

- The environment-based SOP consists of:
  - Potential vulnerabilities of JupiterMesh consisting of vulnerabilities found in:
    - IEEE 802.15.4
    - RPL
    - IPv6
  - Possible measures in identifying and mitigating these vulnerabilities.

Conclusion

- Successfully implemented the black hole attack that hindered the communications in the network topology by effectively changing the source code in specific nodes to exploit the rank of the network.
- By detailing the attacks and showing how they were conducted, we were successful in showing how a smart grid topology is prone to compromise.
- The mitigations were successful in detecting if the black hole attack occurs and correcting the attack against the network.
- We were able to create an SOP for the detection and mitigation of key vulnerabilities in this smart-grid environment.
- Future work would include computing the parent rank using hashing algorithms to prevent modification to the values used for parent rank computations.

References

- RFC 6552: Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL): https://tools.ietf.org/html/rfc6552
- A. Mayzaud, R. Badonnel and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", in International Journal of Network Security, vol. 18, no. 3, pp. 459-473, May 2016.
- R. Chadha, T. Bowen, C.J. Chiang, Y.M. Gottlieb, A. Poylisher, A. Sapello, C. Serban, S. Sugrim, G. Walther, L. Marvel, A, Newcomb, and J. Santos, *"CyberVAN: A Cyber Security Virtual Assured Network Testbed"*, IEEE MILCOM 2016.
- W. Meng, M. Ruofei, and H. Chen, "Smart Grid Neighborhood Area Networks: A Survey", *IEEE Networks*, Vol. 28 No. 1, Pp. 24-32. January 2014. Referenced From: https://ieeexplore.ieee.org/document/6724103/
- K. Weekly and K. Pister, "Evaluating Sinkhole Defense Techniques in RPL Networks", *IEEE*, October 2012.

Acknowledgement

- Customer: Vencore, Inc.
  - Barry Barlow
- Vencore Labs
  - James Sugrim
  - Alex Poylisher
- SME: Dr. Kai Zeng
- Instructor: Gino Manzo

SPECIAL ACKNOWLEDGEMENTS

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

Dr. Peggy Brouse

for her vision and continued support in making this class available for students.

Catherine Courtney

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

Hugh Miller

for providing ABET guidance and ensuring we are surpassing the ABET requirements.

Vani Sai Koppisetti

for being our Graduate Teaching Assistant and helping with all aspects of the class.

CROSS DOMAIN SOLUTION

Zabi Tora, Jonathan Wiley, Ankur Goel, Simplice Njike, Erika Strano

Subject Matter Expert: Graham Archer

Sponsor: BAE Systems

BACKGROUND

- A Cross Domain Solution (CDS) has the capability to validate, inspect and santitize incoming data.
- The three phases, validation, inspection, and sanitization are non-bypassable and one way.
- A CDS is a very secure layer-7 firewall/ router, that guarantees only clean, correct, and valid data is allowed to flow.
- Ensures secure information sharing between networks of various security classifications.
- CDS's are also known as "guards."

OBJECTIVE

- Establish a set of accept/reject criteria to allow data to flow one way through a pipeline of processes.
- It is to be implemented on the STOP OS, which allows for a secure and un-hackable CDS.

TOOLS

- We used an operating system developed by BAE Systems, called STOP OS, to implement our CDS.

APPROACH

The CDS will:

1. Receive files delivered from a client computer.
2. Detect the presence of the new file and move the file into a filtering area.
3. Filter the file and ensure that it meets the established criteria.
4. Move accepted data to an output area, or
5. Move rejected data to a quarantine area.

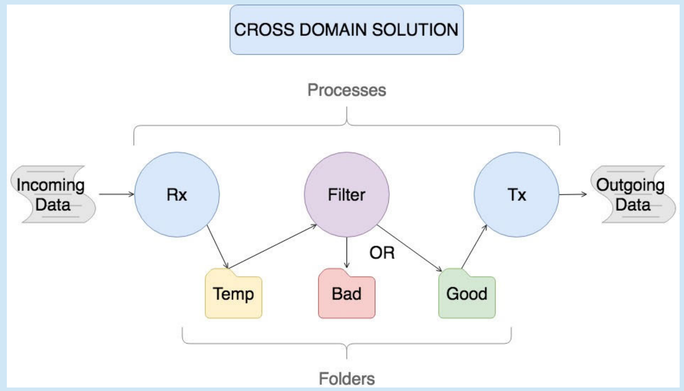


Figure 1: Design architecture of CDS. The three main processes are show, Rx, filter, and Tx. The flow is also noted from the beginning of the CDS to the end.

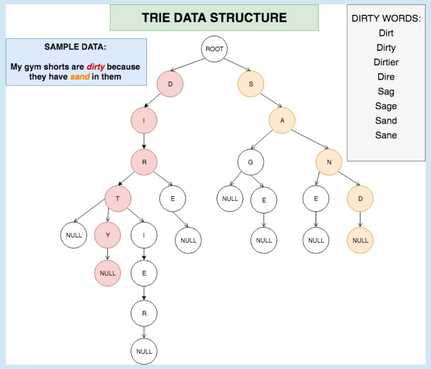


Figure 2: Visual representation of a trie data structure (left). Code for the filtering algorithm (right).

RESULTS AND CONCLUSION

- Successful implementation of a CDS.
- STOP OS's security labeling makes the CDS virtually un-hackable.
- Having a secure process that allows sensitive information to be transferred between agencies or within military operations prevents information from being leaked, spoofed, or compromised.

Figure 3: This is the security label that is defined within STOP.

ACKNOWLEDGMENT

We would like to thank BAE Systems for providing us the training and guidance necessary to complete this project. We would also like to thank the Cyber Security Engineering staff for supporting us during our ups and downs, and for pushing us to success. This project's success was made possible with the help of both entities.

References:

[1] BAE Systems. STOP training manual: an introduction to the stop operating system. BAE Systems, Reston, VA: BAE Systems, 2017

[2] S. Smith, "Shedding light on cross domain solutions," SANS Institute In-foSec Reading Room, Apr., 2018 W.-K.Chen, Linear Networks, and Systems.Belmont, Calif.: Wadsworth, pp. 123-135, 1993. (Book style)

Cyber Security Automation through Machine Learning

Matt Burke, Clara Currier, Samuel Dura, Ali Nasir, Steve Zamory
Sponsored by Booz Allen Hamilton
SME: Dr. Peter Fonash

Background

The United States Department of Homleand Security (DHS), responsible for maintaining the integrity of computer networks for a variety of federal agencies, is overseeing the integration of security enhancements known as Continuous Diagnostics and Mitigation (CDM).

Currently in its second phase, CDM is

Purpose

The purpose of our project is to reduce the amount of human effort needed to monitor computer networks for anomalies.

Introduction

The system uses machine learning to evaluate the network traffic based on threat indicators.

Machine Learning

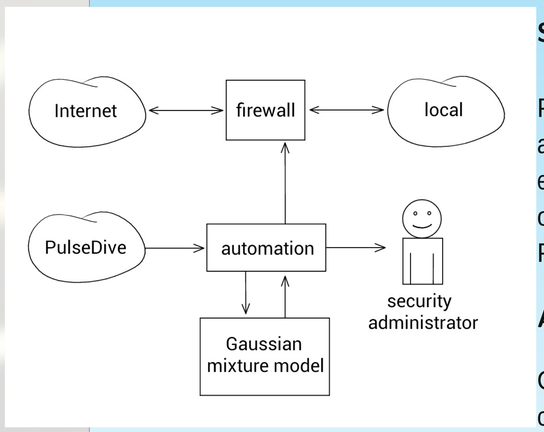
Machine learning is a term that describes a multitude of algorithms used to classify data.

Gaussian Mixture Models

One statistical method of classifying threat indicators is

System Overview

The system consists of several components working in concert. Threat indicators are



Situation data

Predictive information about the current network environment is drawn from open sources provided by Pulsedive.

Automation

One statistical method of classifying threat indicators is nit

Test Environment

The test environment consists of a demonstration version of a commercial automation system. that may be used t

Results

The system consists of several components working in concert. Threat indicators are

Summary

The purpose of our project is to reduce the amount of efforUnited St
a

Future Study

One statistical method of classifying threat indicators is nit

Acknowledgements

We greatfully acknowledge the guidance from our sponsor's representative, Patrick Schurr. Additionally, our subject-matter expert, Dr. Peter Fonash, provided valuable insight and suggestions. Threat indicators were graciously provided by Pulsedive.

References

I. Antoniou, V. V. Ivanov, and P. V. Zrelov. "On the log-normal distribution of network traffic," Physica D: Nonlinear Phenomena 167, no. 1-2 (2002): 72-85.

S. Heckman, and L. Williams. "A model building process for identifying actionable static analysis alerts," in Software Testing Verification and Validation, 2009. ICST'09. International Conference on, pp. 161-170. IEEE, 2009.s

Quantitative Model for Evaluating Security Products

Jacob Dulaney, Hyunjoon Kim, Benjamin Krause, Luis Gustavo Loayza, Shival Puri, Allen Shen
General Dynamics Information Technology; Robert Carey
SME: Richard Lord

BACKGROUND

- Current cyber security products are not based on any meaningful measures
- The security tools are advertised on their qualitative features rather than their quantitative measure on how much they improve the security. Sales revolve around these qualitative features
- Advantages: can effectively compare different security products with similar features quantitatively by comparing the percentage of improvement in security
- Challenges: complex to develop one model that fits different organizations due to different requirements of each organization

OBJECTIVE

- A model that can be used to determine the qualitative value of similar security products against a given set of risk mitigation security controls at a high confidence and is applicable to all security tools
- Because of our lack of data to work with, our model was to be developed to be flexible to work with any type of data that could be gathered

APPROACH

- In order to determine a minimum set of enterprise security controls applicable to cybersecurity devices, we researched standard logical controls related to business. Per the scope of our project, we did not review policy or physical controls
- Our research references previous work done by leaders in cybersecurity such as SANS Institute, the National Institute of Standards and Technology (NIST) and NSS Labs
- We broke up the Open Systems Interconnection (OSI) model into each of its 7 layers. We identified the most critical vulnerabilities of each layer to determine a minimum security control that could be measured in protecting against that vulnerability
- Rather than focus on the effectiveness of one type of cybersecurity device, we developed a controls matrix addressing the seven layer security stack. The controls matrix would allow for a global view of which combinations of devices can protect all seven layers
- After researching, we adopted the “rule of 5” to determine a minimum of 5 data points for reliable metrics
- We then developed tests for each metric setting benchmarks of 80% minimum for a tool to be deemed satisfactory. For highly critical controls, the tool had to pass the metric tests 100% of the time

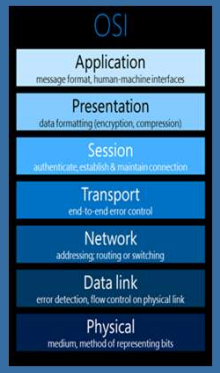


Figure 1. OSI Model

MODEL

Layer	Control	Security Device: Traditional Firewall	Application Firewall	Next Generation Firewall	Intrusion Detection System	Intrusion Prevention System	Web Proxy	Endpoint Protection	Network Access Control
Application	1. Monitor applications using signature based detection for known malware								
	2. Application level access controls to define and enforce access to application resources.								
	3. Monitor and block application inquiries and activity that deviates from normal behavior								

- Layer - Selected layers from Open Systems Interconnect model that were relevant
- Control - Chose security controls that can be implemented at selected layer
- Security Device - Selected most commonly used and effective security tools and determined effectiveness in implementing selected controls

Layer	Control	Metric	Test Methodology	Benchmark
Application	1. Monitor applications using signature based detection for known malware	1. How well the device can detect malware signatures	1. Test a set of malware with known signatures to determine if the tool detects them (estimated 20 unique malware to test)	At least 18/20
	2. Application level access controls to define and enforce access to application resources.	2. How well the device blocks access	2. Test whether users can access critical applications (estimate 5 applications to test)	At Least 4/5
	3. Monitor and block application inquiries and activity that deviates from normal behavior	3. How well the device blocks malware from executing	3. Test whether malware or code injection attacks can be executed (estimate 20 attacks)	At Least 18/20

- Metric - Determined attribute of security device when covering selected control
- Test Methodology - Selected way in which metric effectiveness could be tested with necessary equipment
- Benchmark - Determined number at which security device would “minimally secure” selected control

Model Uses:

- Organizations can compare current security controls to those we have defined
- Companies will have better knowledge of what security tools cover each control
- Easier to define which security tools are actually needed - reduces chances of overlapping controls

OUTCOME

- The overall approach failed due to being unable to obtain testing data. We were unable to test and refine the testing and evaluation methodology:
  - Declined by multiple organizations when approached about acquiring data
  - Without testing data, it was impossible to confirm what realistic benchmarks are or a defined testing methodology
- The initial approach of creating minimum security stack of controls fulfilled the criteria needed to develop the model:
  - Create measurable criteria for the model
  - Control the scope of of information that would be needed for testing
  - Process is replicable by any third party interested in customization of the model
- Based on the outcome of our research, the following improvements to our approach could solve the issues we faced:
  - Secure a data source before developing the model. The lack of testing data proved very difficult for our team
  - It would be beneficial to narrow the scope to a single tool/device and the role it plays in the network rather than attempt to include many devices for testing
  - Adjust the scope of the model to the data available if comprehensive testing data cannot be found

CONCLUSIONS

- Creating a quantitative model to measure the effectiveness of a cyber security product is very difficult
  - Various organizations have thrown a lot more resources at this problem and have yet to effectively solve the problem
- The approach to creating a quantitative model should be to create a general, broad model where organizations and individualize it themselves
  - We ended up just evaluating based on a single tool. Companies can use this model to match to certain cyber security products
- Future research can include a wide variations of uses everything from another potential risk management framework all the way from individual organization adopting the model for use for their own for things like auditing both internal and external systems for information assurance

ACKNOWLEDGEMENTS

We’d like to thank General Dynamics Information Technology for assistance with this project. We appreciate the support, time, and effect from our customer, Robert Carey, and our SME, Richard Lord. We would also like to thank Peggy Brouse for giving us this opportunity, and Gino Manzo for supporting us throughout the project. We’d also like to thank David Raymond from Virginia Tech for his professional advice.

References

Wilson, J. (2015, February 6). IOE/IOT KEY ENABLERS WILL BE UBIQUITOUS CONNECTIVITY & PREDICTIVE MAINTAINENCE. Retrieved April 23, 2018, from http://jimwilsonblog.com/?cat=176

Securing an Android Custom ROM

Yusif Atasoy, Nadia Jehangir, Chase Franklin, Jake Steele, Alexander Svinicki, Ismail Ahmad
Leidos
SME: David Szczesniak, Yaron Eidelman, Ammar Palla

BACKGROUND

- An Android Custom ROM (Read-Only Memory) is the firmware of the phone
  - Android is an open source operating system, based off the Linux Kernel, so everyone has access to the code and can alter
  - Customizing one's own ROM allows for users to alter features already present on the phone as well as add new features or increase functionality
- HAL (Hardware Abstraction Layer) allows to create hooks between the Android platform stack and the hardware
  - Components such as Camera, USB, WIFI, and Audio all contain hardware based components that are called from the HAL

Figure 1: Depicts the breakdown of the Android framework.

OBJECTIVES

- Develop an Android Custom ROM that disables the following components of the phone:
  - Camera
  - USB
  - WiFi
  - Bluetooth
  - Speaker
  - Microphone
- Phone should still be operable after the listed components have been disabled
- Our configurations to the phone should ultimately not affect how the phone functions as a whole, but only when the specific components are accessed
- Sub-Objective:
  - Develop new ways to disable these components that have yet to be thought of by our SME team

MATERIALS

- Android Phone – Google Pixel 2
- Gitlab
  - Android AOSP
  - Build Server
  - Build source using master branch,

everyone on the team can individually create branches from master and alter separate components.

Figure 2: GitLab logo

Figure 3: The process of altering and saving code.

METHOD

1. Modifying configuration files in order to disable components from where they are called to operate
2. Specific components can be altered at a hardware level
   a. Modify the HAL changing how each specific hardware is called
3. Alter manager files:
   a. Directly alter the calling of a specific components manager service so when a service/application requests the component the service manager returns "null"
4. USB Condom:
   a. We created a proof-of-concept device that will only allow charging to occur without data flow

```
private static IAudioService getService()
{
    if (sService != null) {
        return sService;
    }
    IBinder b = ServiceManager.getService(Context.AUDIO_SERVICE);
    sService = IAudioService.Stub.asInterface(b);
    return sService;
}
```

Figure 6: Above shows the direct sections of the android/media/AudioManager.java file that were altered in order to return null for the microphone and speaker

```
public BluetoothManager(Context context) {
    context = context.getApplicationContext();
    if (context == null) {
        throw new IllegalArgumentException(
                "context not associated with any application (using a mock context?)");
    }
    // Legacy api - getDefaultAdapter does not take in the context
    mAdapter = BluetoothAdapter.getDefaultAdapter();
}

/**
 * Get the default BLUETOOTH Adapter for this device.
 *
 * @return the default BLUETOOTH Adapter
 */
```

Figure 4: The above depicts the code for the bluetooth manager.

Thank You

A special thank you to the following people who have helped us throughout our project;
David Szczesniak, Yaron Eidelman, Ammar Palla who have given us guidance as well as the tools to complete the project as well as Dr. Peggy Brouse and Gino Manzo.

SOLUTIONS

- One of the solution approaches we utilized was intercepting the function call for the hardware api in the framework level
  - This allowed us to fool application level api calls down into thinking certain hardware components were missing or unavailable
- Ultimately our fastest solution was to alter the service manager to return "null" when it went to request access to certain hardware components managers
- There were a few alternative solutions that we considered:
  - Altering kernel source configuration files to prevent the higher levels from accessing the hardware components
  - Develop a "shim" to intercept and modify API calls in a way that will prevent the OS from accessing the components

RESULTS

- As expected, the edited code allowed us to disable the components
- When the service manager was asked to connect to a certain hardware component, the service manager would bounce back "null" and the application would not have access to the components
- The changes made to the service manager code did not affect any other functionality of the phone as well as application functionality

CONCLUSIONS

- Android Open Source Project contains all the code needed for a user to modify or improve functionality in their android device
- There are multiple ways to prevent the OS and the application layer from interacting with various components of an Android system
- Some of the methods that our team discovered were: the OS method, the SHIM method and the Kernel method
- The most feasible method was the kernel method, editing kernel code to disable the components
- Disabling components was ultimately done by altering the service manager code and in esence, returning "null" statements when requested

Vulnerability Assessment for a Smart Grid IoT Environment

Nicholas Burley, Eric Gum, Douglas MacDonald, Natalie Parke, Marco Perdomo, Rida Saref, Andrew VanPernis, Matthew Wilkes

Sponsored by Vencore, Inc.

SME: Dr. Kai Zeng

Introduction

In comparison to other electrical grids, the Internet-of-Things (IoT) environment of smart grids potentially possesses a more flexible network topology and increased demand-side management efficiency. Using an IoT environment in the electrical grid comes with many benefits, while also posing the risk of opening up the grid to security vulnerabilities. To assess these vulnerabilities, there needs to be a standard vulnerability assessment methodology; however, there is no accepted standard assessment for this environment causing a lack of proper security in smart grids. The basis of this project is to create a standard operating procedure (SOP) for conducting a vulnerability assessment for smart grid IoT environments. The SOP will be a step-by-step instruction for the proper execution of a vulnerability assessment directed towards the IoT network. The foundations of the SOP will come from the research of other vulnerability assessments conducted in electrical grid systems and testing for vulnerabilities using a simulated IoT environment. The environment to be tested is a limited form of JupiterMesh which is a robust, low-power industrial IoT wireless mesh network used in smart grids. Major protocols of this type of IoT environment is Routing Protocol for Low Power and Lossy Networks (RPL) which establishes connections between IPv6 nodes, and IEEE 802.15.4 which defines the operation of low-rate wireless personal area networks. The focus of the vulnerability assessment is to test for vulnerabilities in the usage of RPL on the network layer. A black hole attack is implemented on RPL in the environment to show RPL's vulnerabilities. After the attack, mitigation will be put into effect to attempt to solve the vulnerabilities.

Objectives

- Analyze and mitigate vulnerabilities in smart grid IoT environments and develop a standard for vulnerabilities in these environments to promote more secure and safe environments.
- Analyze the environment, implement an attack against the environment, and develop mitigations to detect and prevent the attack in the environment.
- Establish an Environment Standard Operating Procedure (SOP) based on the analysis and findings of a black hole attack on the environment provided by Vencore Labs to efficiently protect similar environments.

Image taken from: https://www.sensorsexpo.com/iot-ecosystem

Materials and Methods

Materials:

- CyberVan Environment - allows a user to access the JupiterMesh environment via web browser.
  - 8 Linux machines (Nodes 1-8) connected together through RPL and IPv6.
  - Collector node (C) distributes UDP traffic throughout the environment.

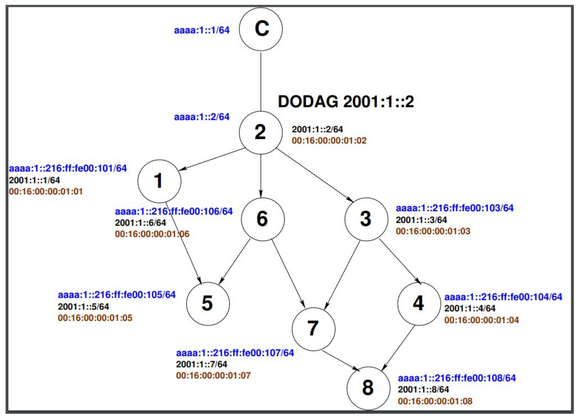


Figure 1: The DODAG of the environment with Nodes 1-8 as Linux "IoT" devices connected wirelessly. Node C is the collector node that is connected by ethernet to node 2 to distribute UDP traffic throughout the network.

Black Hole Attack - Attack against topology:

1. Choose a node to be the malicious node (Node 6 was chosen)
2. Modify the rank of node 6. The rank is a value that its neighbor nodes use to determine the preferred parents. Rank increases as it goes down the DODAG and increases as it goes up the network for each node. Modifying the rank allows greater impact on the topology. RPL code is modified to change the rank.
3. Block UDP traffic distributed by Node C. Ip6tables is a built in firewall for Linux and was used to block traffic.

Mitigation of Black Hole Attack:

- Preventing and detecting the changing of rank for nodes using rank verification.
  - Changing the code of RPL to check the rank of the node.
- Detecting packet loss.
  - IDS to detect increased packet loss over certain time intervals.

SOP Methods: A standard operating procedure is a document that defines the regularly recurring operations relevant to the quality of the investigation. The purpose of it is to carry out certain operations correctly and always in the same manner. The following defines key points in constructing our SOP:

- Identifying key areas of concern where our SOP will be useful (i.e. identifying key vulnerabilities in the CyberVan Environment)
- After identifying the key vulnerabilities, we identified the top three vulnerabilities and answered questions concerning what attacks might exploit those vulnerabilities
- Finally we defined measures to identify and mitigate the key vulnerabilities

Results

Black Hole Attack Results:

- The black hole attack was analyzed using tcpdump on each node to discover packet delivery.
- Modifying the rank proved effective. The code change resulted in the rank decrease for node 6 and the domino effect on its child nodes. Node 5's preferred parent changed to node 6. Node 7's preferred parent changed to node 6. Node 8's preferred parent changed to node 7. Node 4 no longer received data from node 8 because node 7 is now node 8's preferred parent.
- By using ip6tables on node 6, it cut off UDP delivery past node 6 and its child nodes. The ip6tables commands prevented traffic from being forwarded, sent, or received by node 6, meaning traffic sent or forwarded to node 6 was not delivered.
- Figure 2 represents the topology after the attack and the loss of data on the network.

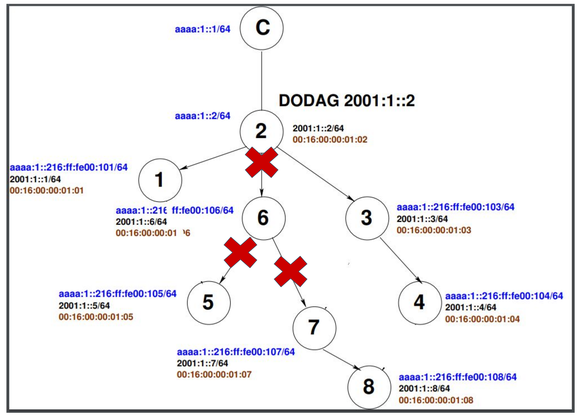


Figure 2: The red Xs represent loss of traffic between the nodes. Node 8 is still able to send traffic to node 7 but is dropped once it reaches node 6. Traffic is dropped for nodes 5, 7, and 2 to node 6. Notice there is no longer connections from 8 to 4, 7 to 3, and 5 to 1.

Mitigation Results:

- The proposed rank verification ensured verifying the parent rank before the node's rank is changed.
- The code (Figure 3) computes the parent's max rank and compares it to the parent rank value sent from DIO messages. The threshold sets a parameter for how much the rank can decrease. If the parent rank is too low, meaning the node can be lying, it returns a NULL value to choose another parent.
- Figure 4 shows the successful results of the rank verification of node 5. Node 5 set the preferred parent as node 1 because it no longer sends UDP traffic to node 6 due to it having an incorrect rank.

```
def compute_rank_increase(dodag, parent_rank):
    """Compute the rank increase for a node"""
    # this is static here, because our implementation does not receive much
    # feedback from lower layers
    rank_increase = (DEFAULT_STEP_OF_RANK * DEFAULT_RANK_FACTOR + DEFAULT_RANK_STRETCH) * dodag.MinHopRankIncrease
    #if parent_rank * rank_increase > INFINITE_RANK:
        #return INFINITE_RANK
    #else:
        #return parent_rank + rank_increase
    threshold = 0.9 #toleration for rank
    if parent_rank < (1024 * threshold): #1024 is the max rank for node 6, if node 6 rank is less than that times the threshold it is lying
        return None #fixes rank to correct topology based on correct max rank
    else: #if everything is good it will return back to normal operations
        if parent_rank * rank_increase > INFINITE_RANK:
            return INFINITE_RANK
        else:
            return parent_rank + rank_increase
```

Figure 3: The code taken from node 5 that was modified to verify rank. The old code is commented and the new code implements the old code if the verification is successful. The compute_rank_increase function is part of Objective Function 0 which sets the requirements for computing ranks for nodes.

Results (continued)

```
root@iot5:~/simpleRPL/RPL# tcpdump -nvei eth0 | grep UDP
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:34:29,108415 00:16:00:00:01:05 > 00:16:00:00:01:01, ethertype IPv6 (0x86dd), length 137: (flowlabel 0xc78ec, hlim 64, next-header UDP (17) p
ayload length: 83) 2001:1::5.52062 > aaaa:1::1.22222: [udp sum ok] UDP, length 75
18:34:49,115831 00:16:00:00:01:05 > 00:16:00:00:01:01, ethertype IPv6 (0x86dd), length 137: (flowlabel 0xc78ec, hlim 64, next-header UDP (17) p
ayload length: 83) 2001:1::5.52062 > aaaa:1::1.22222: [udp sum ok] UDP, length 75
18:35:09,123340 00:16:00:00:01:05 > 00:16:00:00:01:01, ethertype IPv6 (0x86dd), length 137: (flowlabel 0xc78ec, hlim 64, next-header UDP (17) p
ayload length: 83) 2001:1::5.52062 > aaaa:1::1.22222: [udp sum ok] UDP, length 75
18:35:29,130454 00:16:00:00:01:05 > 00:16:00:00:01:01, ethertype IPv6 (0x86dd), length 137: (flowlabel 0xc78ec, hlim 64, next-header UDP (17) p
ayload length: 83) 2001:1::5.52062 > aaaa:1::1.22222: [udp sum ok] UDP, length 75
```

Figure 4: Tcpdump of UDP traffic on Node 5. Notice that traffic is no longer sent from node 5 to 6. It only sends UDP traffic to node 1, a safe node. Tcpdump is a built in linux command to monitor traffic

Final SOP:

- The environment-based SOP consists of:
  - Potential vulnerabilities of JupiterMesh consisting of vulnerabilities found in:
    - IEEE 802.15.4
    - RPL
    - IPv6
  - Possible measures in identifying and mitigating these vulnerabilities.

Conclusion

- Successfully implemented the black hole attack that hindered the communications in the network topology by effectively changing the source code in specific nodes to exploit the rank of the network.
- By detailing the attacks and showing how they were conducted, we were successful in showing how a smart grid topology is prone to compromise.
- The mitigations were successful in detecting if the black hole attack occurs and correcting the attack against the network.
- We were able to create an SOP for the detection and mitigation of key vulnerabilities in this smart-grid environment.
- Future work would include computing the parent rank using hashing algorithms to prevent modification to the values used for parent rank computations.

References

- RFC 6552: Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL): https://tools.ietf.org/html/rfc6552
- A. Mayzaud, R. Badonnel and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", in International Journal of Network Security, vol. 18, no. 3, pp. 459-473, May 2016.
- R. Chadha, T. Bowen, C.J. Chiang, Y.M. Gottlieb, A. Poylisher, A. Sapello, C. Serban, S. Sugrim, G. Walther, L. Marvel, A, Newcomb, and J. Santos, "*CyberVAN: A Cyber Security Virtual Assured Network Testbed*", IEEE MILCOM 2016.
- W. Meng, M. Ruofei, and H. Chen, "Smart Grid Neighborhood Area Networks: A Survey", *IEEE Networks*, Vol. 28 No. 1. Pp. 24-32. January 2014. Referenced From: https://ieeexplore.ieee.org/document/6724103/
- K. Weekly and K. Pister, "Evaluating Sinkhole Defense Techniques in RPL Networks", *IEEE*, October 2012.

Acknowledgement

- Customer: Vencore, Inc.
  - Barry Barlow
- Vencore Labs
  - James Sugrim
  - Alex Poylisher
- SME: Dr. Kai Zeng
- Instructor: Gino Manzo