PenTest magazine

MACHINE LEARNING, DEEP LEARNING AND CYBERSECURITY

The Crossroads of Artificial Intelligence
Machine Learning, and Deep Learning

Machine Learning In Information Security

Radical Solution
To Identify Web Spam Using Machine Learning AI

AND MORE...

03/2018 ISSN: 2084-1117

PenTest magazine

EDITORIAL TEAM

Managing Editor

Bartłomiej Adach

bartek.adach@pentestmag.com

Proofreaders & Betatesters

Lee McKenzie, Samrat Das, Francesco Consiglio, Greg Hanis, Craig Thornton, Avi Benchimol, Bernhard Waldecker, Da Co, Jonus Gerrits, Francesco Mura, Timothy Hoffman, David von Vistauxx, Steve Hodge

Special thanks to the Proofreaders & Betatesters who helped with this issue. Without their assistance there would not be a PenTest Magazine.

Senior Consultant/Publisher

Paweł Marciniak

CEO

Joanna Kretowicz

joanna.kretowicz@pentestmag.com

DTP

Bartłomiej Adach

bartek.adach@pentestmag.com

COVER DESIGN

Hiep Nguyen Duc

PUBLISHER

Hakin9 Media Sp. z o.o.
02-676 Warszawa
ul. Postępu 17D
Phone: 1 917 338 3631
www.pentestmag.com

Dear PenTest Readers,

In the current issue of PenTest Magazine we would like to focus mainly on the topic of Machine Learning and its impact on cybersecurity. As continuous evolution of technology generates more threats and vulnerabilities, which are becoming more and more sophisticated, Machine Learning offers an efficient defense due to its adaptability to the unknown circumstances. The authors present you how the ML's subcategories, such as supervised learning, unsupervised learning, classification, regression, and clustering, are used in the context of Big Data. In the time of an enormous and still growing amount of information, Machine Learning is an essential tool to deal with potential IT threats. However, it has to be emphasized that systems which are dependable on machine learning algorithms can also be vulnerable to hacking in a very sophisticated manner (for instance, altering the learning algorithm).

Moreover, we would like to draw your attention to SCADA systems. In the current issue, we have an interesting piece on how it is used in cyber security of a nuclear power plant. You can also find a practical article about pentesting of SCADA networks.

Furthermore, the issue contains pieces on securing the spectrum across various media, as well as some specific cases of CPU vulnerabilities, a global bank's penetration testing methodology, and common flaws in session management. Last but not least, we would like to introduce you to our new "Q&A Session With Cybersecurity Expert" section. - our first guest is Mr. Jigar Thakkar

Enjoy your reading,

PenTest Magazine's Editorial Team.

Contents

Artificial Intelligence and Cybersecurity

The Crossroads of Artificial Intelligence, Machine Learning, and Deep Learning

Chrissa Constantine

Chrissa is an Information Security Analyst and has a Master of Science in Information Security, CISSP and CE|H certifications. She held positions as a consultant at Apple and for a Silicon Valley start-up as a penetration tester. Chrissa enjoys hacking competitions, meeting new people, and learning new things.

Two methods are used to train an algorithm, *supervised* and *unsupervised*. The data or inputs accepted by supervised and unsupervised learning are differentiators for each technique. From a supervised perspective, the data provided to the algorithm is labeled and structured. Supervised data is historical data, and predictions must be made to create labels on future data.

What is Artificial Intelligence, Deep Learning, and Machine Learning?

Think of artificial intelligence (AI), deep learning (DL) and machine learning (ML) as the layers of an onion. Starting with the outer layer of the onion (Figure 1) as AI, as you move through the layers, you encounter ML, and then DL, which is a subset of machine learning.

The term *artificial intelligence* is frequently used as a marketing product term by many cybersecurity companies without consensus about what it means. Part of the issue in defining AI is that it relates back to human intelligence, which is hard to describe. Different researchers in the field of intelligence focus on various aspects of intelligence in their definitions (Sternberg, 2018).

Generally speaking, AI refers to a “broad field of science encompassing not only computer science but also psychology, philosophy, linguistics and other areas” (Bakhshi, 2017). However, some definitions of AI relate to computerized systems or machines as exhibiting behavior or performing tasks requiring intelligence like that of a human. In these definitions, intelligence refers to an “ability to plan, reason and learn, sense and build some kind of perception of knowledge and communicate in natural language” (Bakhshi, 2017).

Currently, AI can only do the task it was designed to perform, and specific algorithms are developed to solve problems. At this point, AI does not understand what it was trained to do, but the future of AI is to design systems that can learn and then solve any problem.

AI is a collection of technology that a spectrum of industries utilizes, such as agriculture, healthcare for medical diagnosis systems, transportation and logistics, finance, and cybersecurity. A powerful technique used for cybersecurity technology is machine learning.

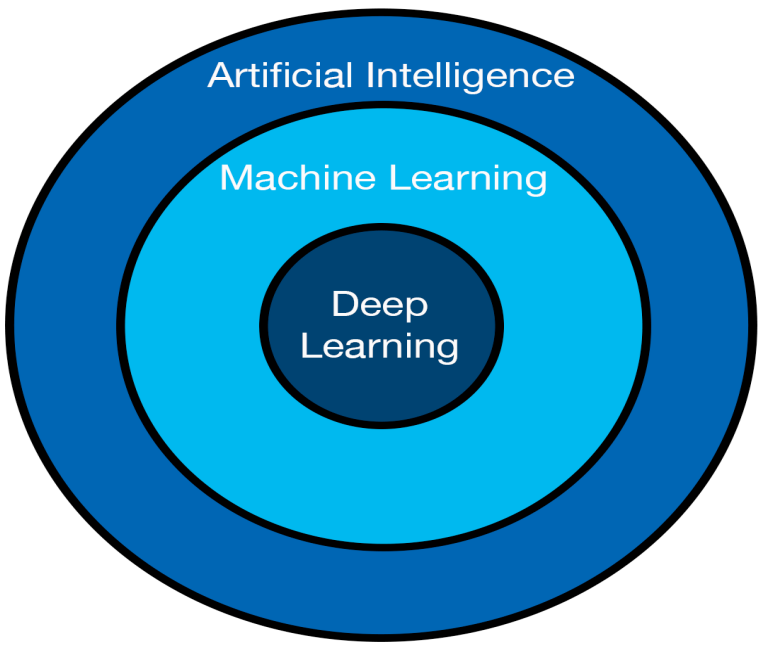


Figure 1. Relationship of AI to ML and DL

Historical Background

In 1956, John McCarthy coined the term artificial intelligence. AI uses algorithms or machines to perform tasks that intersect characteristics of human intelligence, such as planning, understanding natural languages, recognizing objects, learning and problem-solving (McClelland, 2017). In 1959, Arthur Samuel described AI as "the ability to learn without being explicitly programmed." Prior descriptions of AI systems include, "machine-driven decision engines that can achieve near-human-level intelligence" (Chio, 2018). However, there is contention about the definition of artificial intelligence due to varying definitions of what constitutes human intelligence. There are different thoughts about how AI should be understood. Some researchers and scientists believed that it would make the most sense to build systems that respond to rules and logic and that make their inner workings transparent. Others maintained that biology would be the inspiration of machine and that the machine would create the program. In today's systems, the evolution of AI has been for machines to program themselves. The rise of big data and dependence on computerization for many verticals has inspired the development of machine learning techniques that are very powerful. Machine Learning (ML) are mathematical techniques that enable information mining, pattern discovery and drawing inferences from data (Chio, 2018). Think about machine learning as a part of AI, but AI does not always utilize machine learning methods. ML can discern patterns from examining raw data and can then use models to make predictions.

Machine learning refers to an algorithm that can create abstractions (models) by training on a dataset and is a method of *training* an algorithm to accomplish a task. *Training* involves providing large data sets to the algorithm so the algorithm can adjust and improve. Machine learning modifies itself when exposed to more data. The *learning* part of machine learning refers to ML algorithms optimizing along a dimension, such as trying to minimize error or enhance the likelihood of predictions becoming true (Chio, 2018).

The functionality of the human brain is what inspired deep learning. DL uses algorithms and artificial neural networks to create models and uses multiple layers of networks to improve with training or iteration (Storkey, 2017). Artificial neural networks are algorithms that mimic the biologic structure of the brain and have discrete layers and connections. These layers are what give deep learning its name, and DL algorithms require vast amounts of data to obtain results.

Deep artificial neural networks can solve issues in image or sound recognition and in detecting fraud in the finance industry. Some current applications include recommendation systems or activity recognition. Google started to use deep

learning for the Google Brain project in 2011, but branched out and extended use of DL in over 1,000 projects. Microsoft uses DL for commercial speech recognition projects such as X-Box, search rankings, photo search, and translation systems. Facebook uses DL neural networks to translate 2 billion user posts per day in over 40 languages (McClelland, 2017). Deep learning can be used to detect and prevent insider threats and is used in anomaly detection because DL can identify patterns in data that has little consistency between sources.

Deep neural networks have thousands of simulated neurons arranged into various interconnected layers. Layers of inputs fed into each successive layer generate final outputs. These layers within the deep learning network enable it to recognize objects at multiple levels of abstraction. To capture and explain what is happening in DL, Google researchers modified a deep learning-based image recognition algorithm, Deep Dream, to generate or alter images. These images show how different DL is from human perception. Refer to Figure 2 for an example of a Deep Dream image made from a file upload by the author.

Figure 2. Image by Google's Deep Dream from file upload by author

On a daily basis, machine learning is used to enhance smartphones, smartwatches, home devices, and even in online searches. If you perform a search on Google, and it comes back with “Did you mean…?” that is a result of machine learning algorithms in Google search. Machine learning techniques are used to determine what activity is performed by a user based upon GPS, gyroscope and accelerometer sensors in a user’s phone. Applications based upon ML algorithms can be used to tell how far you walked, how many calories you burned, where you went, or give you directions and track your movements. Other examples of ML algorithms in use include image processing, which uses ML techniques for facial recognition or biometric recognition software. Machine learning can be used to retrieve data from image or medical applications and has many applications across a spectrum of industries. Moreover, it is more and more prevalent in our personal lives through the use of mobile phones, gaming consoles, and other computing or internet-enabled devices.

Is AI Ready?

Rapid advances in big data, data analytics, and machine learning are used to convert millions of scattered data points into databases for use in various cybersecurity arenas, such as threat intelligence analysis. AI continues to evolve and has a wide variety of applications. As AI develops capabilities to handle large, complex and unstructured data, it may be able to outperform people in areas such as threat intelligence.

The investment poured into the field of data science, and specifically AI, means that AI is featured in the news regularly. However, the key lies in being able to discover how AI can help corporations align with their strategic objectives. Any company using new technology must blend experience, knowledge, and insight into the integration of the tool into business practices. Some companies are struggling to implement organizational and process changes to integrate machine intelligence analysis into core business processes. A lot of what happens behind ML is a black box; unless an

executive has an advanced math degree, it can be challenging to understand how to adopt the new technology. The real struggle is to understand which machine intelligence capabilities to incorporate into the business.

Currently, AI is expensive and difficult to implement fully into businesses, and, at this time, AI is not ready to fully meet the demands of cybersecurity. The science fiction style concept of AI, the ability for a machine to mimic intelligent human behavior, does not exist at this time. However, machine learning can still be leveraged to support cybersecurity initiatives.

The technology stack using machine learning is growing. Large tech companies rely on machine intelligence and have products that depend upon AI or machine learning. Some of these companies have launched open source libraries and research. For example, OpenAI offers the public access to research and environments. Google's TensorFlow (uses machine learning) and Google Cloud AutoML were introduced to make AI accessible to businesses. Cloud AutoML uses machine learning and neural architecture technologies. Also, Microsoft, in partnership with Amazon Web Services, offers Gluon, an open-source deep-learning library for developers.

Other solutions, like IBM's Watson, use X-Force to learn security language and analyze information, and call their solution AI enabled. If the general premise is that AI must have a large dataset to provide a satisfactory answer, then IBM's Watson, which ingests tens of thousands of documented software vulnerabilities, security research papers and data from blogs, could be considered an expert system – a system narrowly focused on a particular problem. In traditional AI, expert systems were often used to support a medical diagnosis (Martin, 2016).

The evolvement of technology means that attack techniques are also evolving and are becoming more sophisticated in penetrating systems and evading traditional signature-based approaches to cybersecurity. However, ML can be used to offer a solution to these threats due to its ability to adapt and learn in new and unknown circumstances.

Cyber Threats – Offensive and Defensive Measures

In 2016, there were notable advancements in AI, and we also saw an increase in ransomware, malware attack vectors and other forms of attack from cybercriminals. Many organizations are turning to machine learning to provide a better deterrent against attack and to support cybersecurity analysis. The goal in utilizing AI systems would be to scale security operations, improve responsiveness in response to attacks or breaches, assist security personnel in decision making, and to minimize exposure to emergent threats. While there are some defensive applications of machine learning analysis and automation, there are also a rising number of offensive uses of the same technology.

Defenders and cybersecurity personnel attempt to use ML to detect attacks, but nothing prevents adversaries from also using this technology to their advantage. Attackers can use machine learning to evade spam filters or to learn more about a target to craft a perfect social engineering email or scam.

A survey by Cylance at Black Hat USA 2017 showed the majority of information security professionals (62 percent) believe that AI is going to be weaponized by hackers (Elazari, 2017). In a DEFCON 2017 lecture, a data scientist from Endgame demonstrated and publicly released a malware manipulation environment for OpenAI Gym, an open-source toolkit for learning algorithms (Elazari, 2017).

The systems that machine learning algorithms rely on may be vulnerable to hacking. Machine learning algorithms can be susceptible to an attack due to a lack of security design. (Chio, 2018) In other cases, a hacker may determine the data used as a training dataset and manipulate the input data to the algorithm. In day-to-day examples, search engine ML algorithms have been manipulated to boost ranking. Senders of spam try to trick the spam-filtering algorithm by using misspellings or by adding unrelated words or sentences to make them seem like a legitimate email.

While these examples happen daily, there can be more dangerous consequences. The credit card and financial industries are using machine learning to identify fraud. If an attacker knows the pattern of a shopper, then fraudulent purchases may occur that deviate only slightly from normal behavior, which would be undetected by a fraud-based anomaly detection system. Therefore, businesses seeking to leverage machine learning enabled technology need to

threat model and perform risk assessments when creating machine learning systems for cybersecurity purposes. Other vulnerabilities in these systems come from flawed designs, algorithmic limitations or a combination of both (Chio, 2018).

ML in cybersecurity falls into two categories – anomaly detection and pattern recognition. Both tasks are related but look at the issue from different perspectives. For pattern recognition, datasets are examined to discover various characteristics hidden within the data. These characteristics can then be used to teach an algorithm to recognize other data with similar features. Anomaly detection is used to establish a baseline of normalcy for describing a dataset and occurs when there are deviations from the norm.

Spam filtering, malware detection, and botnet detection have used machine learning algorithms to aid cybersecurity analysts. Access control is another area where ML can be used to detect and defend against breaches or information theft. ML, in this case, can include unsupervised learning and anomaly detection. These systems can infer access patterns by users or roles and can engage in various actions when an unexpected pattern is detected (Chio, 2018).

There are multiple attack vectors against machine learning, such as attacks that alter the learning process (attack the training dataset), attacks on integrity or availability, and targeted attacks.

Problems such as where the machine learning algorithms have made a difference and ones where machine learning has tried but failed to yield usable results, are two use cases for cybersecurity. The following sections describe areas where machine learning has made improvements in cybersecurity. There are many appealing aspects to using AI for cybersecurity, including minimizing human bias, assessing risk, and developing predictive capabilities to automate operational tasks.

Taxonomy of Cybersecurity Machine Learning

Machine learning is a scientific discipline, a form of artificial intelligence, and a sub-field of computer science (Dykstra, 2015). Algorithms for machine learning, "*learn"* because they do not need to be explicitly re-programmed when exposed to new datasets. Algorithms are more accurate when they have large datasets to process than when there is limited data. The algorithm is only as good at prediction as the quality of the datasets used for training.

ML systems improve with experience and can learn from previous observations to make inferences about future behavior and predictions about how to apply behaviors to new situations. Mathematics, statistics and the algorithms used to discover patterns, anomalies, and correlations within datasets vary in complexity and are the foundation of machine learning algorithms.

Figure 3 shows machine learning methods for training algorithms and associated cybersecurity tasks. There are some areas of overlap, such as in malware identification and detection, which can use both clustering and classification techniques.

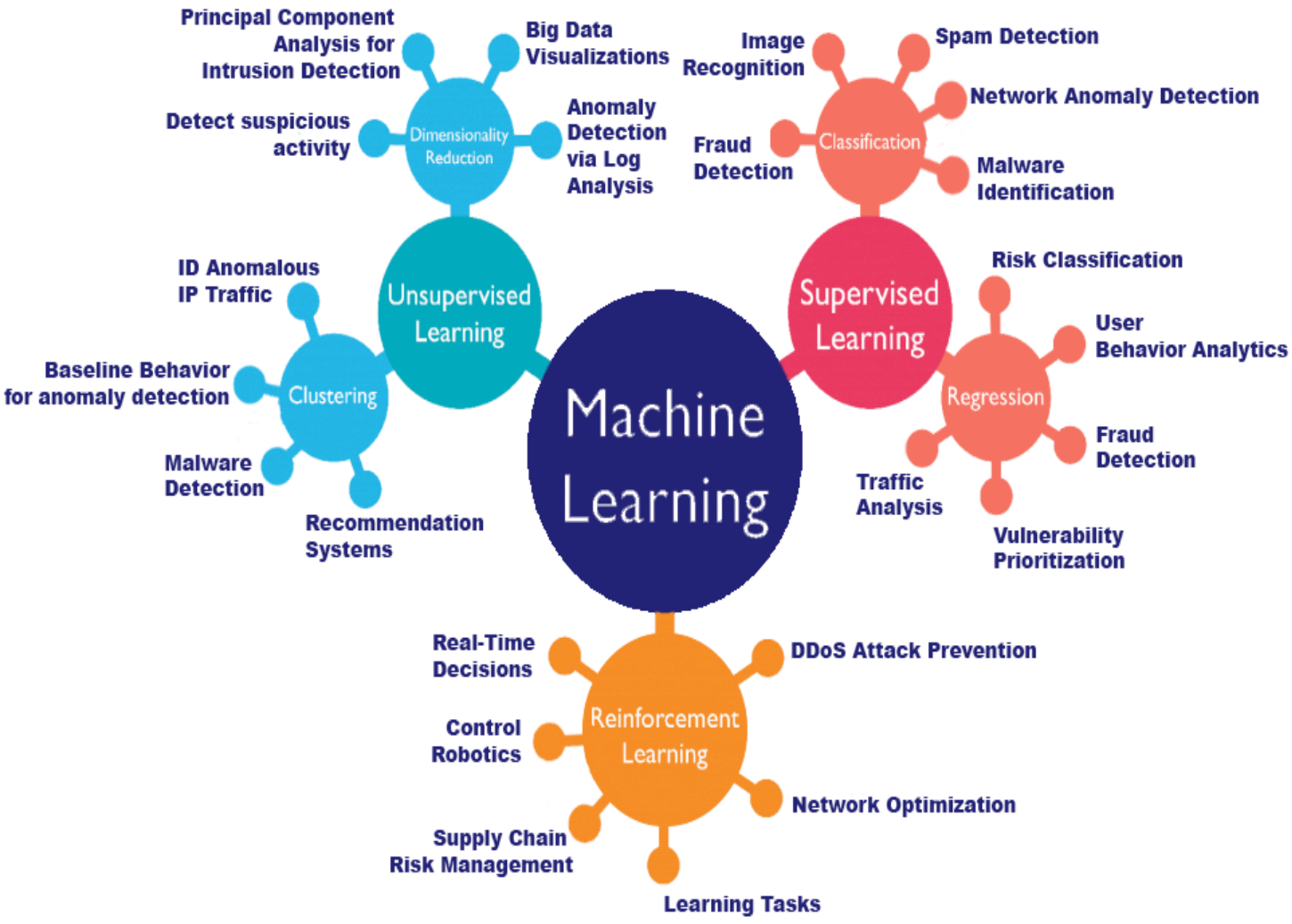


Figure 3. Machine Learning Techniques for Cybersecurity

Supervised vs. Unsupervised

Two methods are used to train an algorithm, *supervised* and *unsupervised*. The data or inputs accepted by supervised and unsupervised learning are differentiators for each technique. From a supervised perspective, the data provided to the algorithm is labeled and structured. Supervised data is historical data, and predictions must be made to create labels on future data.

Supervised learning algorithms are provided with labeled training data and tasked with learning what differentiates the labels. By learning what makes a category unique, the algorithm can be trained to apply a correct label to new, unlabeled data (Kanal, 2017). The criteria for choosing training data in supervised learning is data that is a representative training set. For example, if the ML algorithm must train to identify photos of fruit correctly, but the provided training set are animals, the algorithm cannot correctly identify and label the data.

Email spam detection algorithms can be used to understand one application of machine learning. ML enhances spam filtering because it can compare verified spam with a verified legitimate email to determine what is present in one or the other. This process of automatically inferring a label is called *classification* (Kanal, 2017).

Unsupervised methods use unlabeled datasets and apply these to new data to draw abstractions. (Chio, 2018) Historical data does not have a label, and there may be cases where it is unclear what label is being predicted, such as in instances of malware or botnets.

Forms of supervised learning include classification and regression. Forms of unsupervised learning include clustering (Chio, 2018). Machine learning analysis of large datasets incorporates clustering, dimensionality reduction (a technique of reducing and simplifying inputs) and association rule learning (rule-based method of ML to discover relationships between variables in large databases) (Marty, 2018).

Unsupervised learning refers to algorithms provided with unlabeled training data. If there is a lot of unlabeled data to examine, it may be challenging for people to determine what label to assign. However, it may be easier to have machines separate data into groups because they can identify patterns in large datasets better than humans. Data separation assumes relevant data is present. An example where it would be better to have a machine label data would be the case of network flow data. For this type of dataset, the data features would have to be assigned, such as IP address, network port, packet contents, timestamp, or other relevant data. Useful features are a prerequisite for applying machine learning techniques (Kanal, 2017). Too many non-informative features can lead to algorithm degradation, and too much noise hides relevant information.

Classification vs. Regression

Supervised learning uses c*lassification* or *regression* methods (Chio, 2018). Classification is considered learning where a training set of correctly identified observations is available. Classification determines which of a set of categories a new observation belongs, by a training set of data with observations whose category membership is known (Wikipedia, 2018).

Regression or prediction is used to learn the relationship between features of data based on existing knowledge about the dataset. In cybersecurity, regression is used for traffic analysis, user behavior analytics or fraud detection.

Classification can also be used to detect malicious network activity. The behavior can be used to identify types of activities such as scanning or spoofing. It can be applied on a web application firewall to detect various attack types, such as OWASP Top 10. There are many applications within cybersecurity for this type of analysis and use of regression or classification.

Forecasting is another conventional technique that uses historical data to predict future behavior and is a process of making predictions by analyzing trends in data. An example would be using the Holt-Winters algorithm to perform network anomaly detection.

Clustering

In *unsupervised* learning, data grouped into categories based upon a measure of similarity or distance is called *clustering*, and either a person or the machine learning algorithm is trying to find structure in unlabeled data. An example of clustering is finding malware families using executables and no other metadata (Dykstra, 2015).

With clustering, there is no information on the classes of data. Tasks using clustering include malware analysis and user behavior and analytics (Polyakov, 2017).

Feature Engineering

There is a branch of machine learning called feature engineering, which is used to extract maximum information from features to maximize the ability to categorize or predict unknown data. For brevity, these techniques are not in this article.

Requirements

Machine learning tools typically require the following:

1. **Data collection**. Most ML techniques collect data ahead of time and create a model with stored data.
2. **Data cleansing**. Raw data is often unusable for ML. Missing data, inconsistent data and mixed numeric and non-numeric data can create issues. This step requires combining multiple data sources into a single usable source.

3. **Feature engineering**. Once data is ready for use, the maximum information must be extracted from the data using features. Feature engineering occurs before the creation of the machine learning algorithm (Kanal, 2017).
4. **Model building and validation**. This step works on building the model to test to ensure it works on unlabeled data. Statistical techniques are used to validate the model. Models are predictions used by the ML system. Bayesian Analysis methods are used to train the system to create a better model. This phase may be run again and again to fine tune the system. During this phase, the system makes small adjustments over and over to get the model right.
5. **Deployment**. Machine learning deployment usually requires tuning and refinements, which is especially true in cases of network traffic, where historical observations do not typically match future activity.
6. **Monitoring**. After deployment, ML models must be monitored and run through previous steps to ensure accuracy.

The type of problem presented by cybersecurity needs to be analyzed to determine which machine learning algorithm can solve the issue. So, depending on whether the company wants to address an issue with malware or spam, various types of machine learning algorithm are better suited than the others. The steps above outline a basic model of how to incorporate or use machine learning. For example, if the issue is malware, the dataset needs to be collected from various security data sources, such as a SIEM or varied sources of log files, network traffic, email content or user behavior. Gather training data, and then the data is cleansed, normalized and readied for use. The machine learning model is then selected, the system tuned and the data used with an operational focus, such as creating visualizations and notifications and used for monitoring and management of devices. Meanwhile, the machine learning algorithm is tuned and refined over time, and the steps above are iterated over to ensure the accuracy of the model.

Conclusion

Artificial Intelligence and machine learning can increase the efficiency and precision of specific tasks. Traditional security systems used structured data, but there is a lot of unstructured data that cannot utilize traditional methods to derive intelligence for cybersecurity purposes. Machine learning can be leveraged to support new areas of detection and identification of malicious behavior or attacks.

Human intelligence is used to define AI, which creates issues because there is no standard definition of what constitutes human intelligence. The term is used in marketing campaigns and in various articles to describe new technology, but there are differences of opinion about what it means. As a result, there is a lot of misleading, and confusing information about artificial intelligence, machine learning, and deep learning.

Machine Learning is an effective method to support cybersecurity because of various use cases, such as spam detection, malware identification, user behavior analytics, traffic analysis, fraud detection, and image recognition. However, AI is still growing as a field and is not entirely actualized or realized in cybersecurity. There are opportunities in various domains of cybersecurity to apply ML to address challenges to complex issues.

The key is to connect obscure data points that humans cannot connect on their own to enable enhanced cybersecurity defenses using technology that excels in areas that are limited to humans. The bottom line is to understand what the technology can do for you and your business, not get swept up by the hype and marketing around the terms describing the technology.

Works Cited

Bakhshi, S. v. (2017, March). *Part 1: Artificial Intelligence Defined*. Retrieved from Deloitte: https://www2.deloitte.com/nl/nl/pages/data-analytics/articles/part-1-artificial-intelligence-defined.html

Chio, D. F. (2018). Chapter 1: Why Machine Learning and Security? In D. F. Chio, *Machine Learning and Security.* O'Reilly Media, Inc.

Dykstra, J. (2015). Situational Awareness and Data Analytics. In J. Dykstra, *Essential Cybersecurity Science.* O'Reilly Media, Inc.

Elazari, K. (2017, December 28). *Artificial Intelligence: Hackers on the brink of launching a wave of AI attacks*. Retrieved from WIRED: http://www.wired.co.uk/article/hackers-ai-cyberattack-offensive

Kanal, E. (2017, June 5). *Machine Learning in Cybersecurity*. Retrieved from Carnegie Mellon University: https://insights.sei.cmu.edu/sei_blog/2017/06/machine-learning-in-cybersecurity.html

Martin, S. (2016, November 16). *It's A Marketing Mess! Artificial Intelligence Vs. Machine Learning*. Retrieved from ITSP Magazine: https://itspmagazine.com/from-the-newsroom/its-a-marketing-mess-artificial-intelligence-vs-machine-learning

Marty, R. (2018, January). *AI and Machine Learning in Cyber Security: What Zen Teaches About Insights*. Retrieved from Towards Data Science: https://towardsdatascience.com/ai-and-machine-learning-in-cyber-security-d6fbee480af0

McClelland, C. (2017, December 4). *The Difference Between Artificial Intelligence, Machine Learning, and Deep Learning*. Retrieved from Medium: https://medium.com/iotforall/the-difference-between-artificial-intelligence-machine-learning-and-deep-learning-3aa67bff5991

Polyakov, A. (2017, November 30). *The Truth About Machine Learning In Cybersecurity: Defense*. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2017/11/30/the-truth-about-machine-learning-in-cybersecurity-defense/2/#31f3b718416c

Sternberg, R. J. (2018). *Human Intelligence: Psychology*. Retrieved from Encyclopaedia Britannica: https://www.britannica.com/science/human-intelligence-psychology

Storkey, M. D. (2017). Chapter 6: Artificial Intelligence (AI). In M. D. Storkey, *Futureproof: How to get your business ready for the next disruption.* Harlow: Pearson Education Limited.

Wikipedia. (2018, February 8). *Statistical Classification*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Statistical_classification

Machine Learning In Information Security

Raghunadha Kotha

Raghu started his career as a systems programmer building CAD systems, mathematical packages, and compilers/interpreters and designing IDS systems. He received the achievement award from Bell Labs for his work on configuration management tools. Raghu has had opportunities to work in senior roles in many aspects of Information Technology including Application Development, Information Management, and Enterprise Architecture. Over the past 13 years, he has been involved in Pen testing, malware analysis, malware creation, Security Operations/ Architecture, Machine Learning, and Security Governance. After holding the Head of Information Security position at a California bank, Raghu is currently working as a Sr. Security Architect at Charlotte based Stalwart Systems.

Machine learning techniques have been applied in many areas due to their scalability, adaptability, and potential to rapidly adjust to new data sets and unknown challenges. Information security is a fast paced field demanding a great deal of attention because of remarkable progress in social networks, cloud, IOT, web technologies, online banking, mobile environment, etc. Different machine learning methods have been adopted and deployed in such environments to address different security and non-security problems. We should leverage ML to defend against the bad guys.

Introduction

Information security is a Big Data problem. Humans generate huge amounts of data in the form of blog posts, social media, business data, e-mails, instant messaging, videos, darknet traffic, machine generated data and other sources. This explosion of data is fueled by the unprecedented growth of internet usage and smart phones. This ever-cheaper handheld technology enables us to create, capture, store, share, and manage information with unprecedented convenience and efficiency. Woven into this heap of noise are both our most guarded secrets and shadows of threats that seek to uncover them.

Big Data

To give you an idea of how much data we are producing, look at the research conducted by IDC and sponsored by EMC as shown in picture-01.

Picture-01

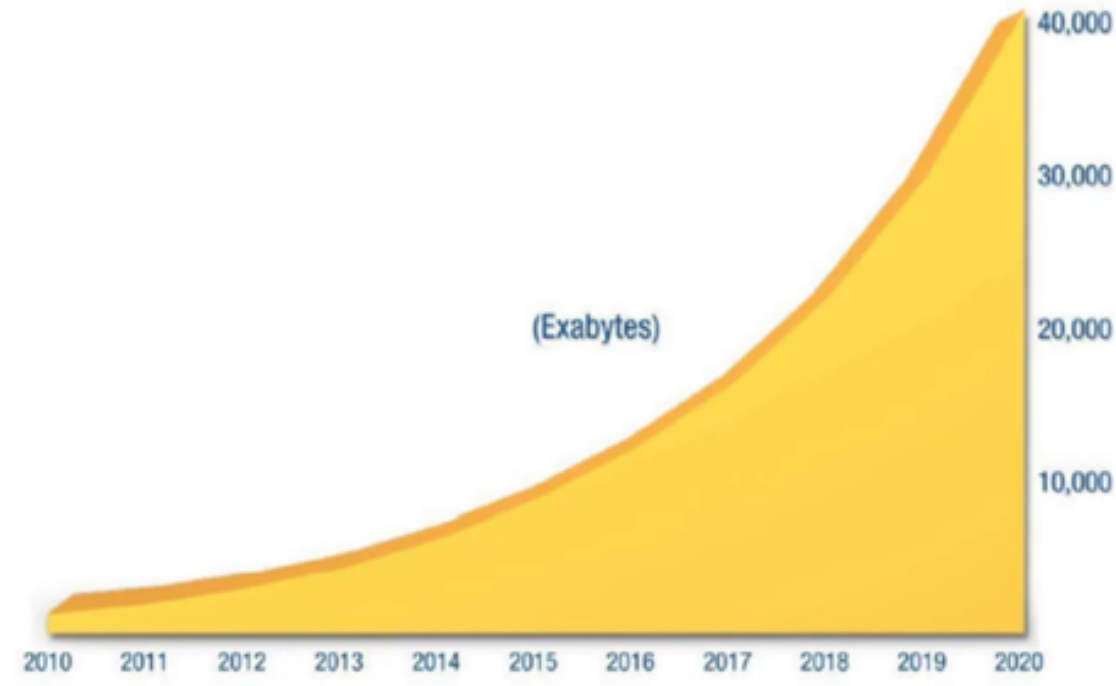
Every two days, we create as much information as we did from the dawn of civilization up until 2003, per Schmidt. To quantify his point, we can observe that prior to 2010, we have produced roughly 130 exabytes. This value skyrockets by 2010, by which we have produced around 1200 exabytes of data. By 2015, we have produced 7900 exabytes and project 41000 exabytes by 2020. To help us comprehend the amount of data in an exabyte, the Amazon rain forest contains roughly 1.4 billion acres of trees, every acre has about 500 big trees, so that makes it about 700 billion trees in the Amazon rain forest. If we chopped and pulped all those trees into paper and then filled every page with letters , the text would form one to two petabytes of data. An exabyte is 1000 petabytes. This is the magnitude of the data that humanity is producing. Whether we are aware or not, we are in the age of Data Exhaust.

5V's

To better understand big data, we can describe the concept in five dimensions, all starting with V's:

Volume – Refers to the vast amount of data generated every minute.

Variety – Refers to the different types of data we consume. In the past, we focused on structured data. Specifically, in the field of security, we deal with a tremendous variety of unstructured data to identify threats and adversaries. This data includes network packets, social media conversations, videos, images, darknet traffic, logs, IOT data and other kinds of data.



Source: IDC's Digital Universe Study, sponsored by EMC, December 2012

Velocity – Refers to the speed at which new data is generated and the speed at which this data moves around.

Veracity – Refers to the trustworthiness of the data. In information security, this is very important. If the data is not accurate, the tools which consume this data may produce lots of false positives, detracting from the confidence in the tools.

Value – Refers to the value we glean from this data. This could be qualitative or quantitative. If the data can save an organization from a breach, that brings a huge value for that organization and it the same time it can save the company from reputational damages.

It would be humanely impossible to process and analyze this huge data. Businesses become vulnerable to security breaches if they don't properly analyze the data. To identify attacks and breaches, the security industry added some tools to their arsenal.

Current State

To transform the 5V's into insight, the generated data needs to be analyzed by security tools to identify potential attacks and breaches. Traditionally, we used SIEM tools, which connect disparate, isolated systems and bring their logs/events together to paint a bigger picture. SIEM tools analyze these logs, correlate them based on the signatures, rules, behavior and produce actionable alerts for a potential attack or a breach. SIEM tools eventually evolved to index and search big data using key words and relationships. These tools provide good visualization to see behaviors, trends and predict attacks and breaches.

Future state

As a human data scientist, we can process data in the world is around 5000 exabytes. At present, machines are analyzing approximately 12000 exabytes. The data that is not being processed by machines due to capacity limitations can be processed by machine learning techniques. With the ability to process big data, ML (Machine Learning) and DL (Deep Learning) become beacons of hope for cyber security. Machine learning holds great promise for the security industry's ability to detect advanced and unknown attacks, particularly those leading to data breaches.

Machine learning techniques have been applied in many areas due to their scalability, adaptability, and potential to rapidly adjust to new data sets and unknown challenges. Information security is a fast paced field demanding a great deal of attention because of remarkable progress in social networks, cloud, IOT, web technologies, online banking, mobile environment, etc. Different machine learning methods have been adopted and deployed in such environments to address different security and non-security problems. We should leverage ML to defend against the bad guys.

Just to give you a glimpse on what myriad of things machine learning applications can do, take, for example, the task of online shopping. Almost every large online storefront will recommend items you may want to purchase. These recommendations are based on a few data points; for example, previous shopping history, your recent searches, or even based on who your friends are. Some other common applications of machine learning in today's technology include face recognition, voice recognition, email spam filtering, fraud detection, NLU (Natural Language Understanding), NLP (Natural Language Processing), video analysis, etc.

What is ML (Machine Learning)

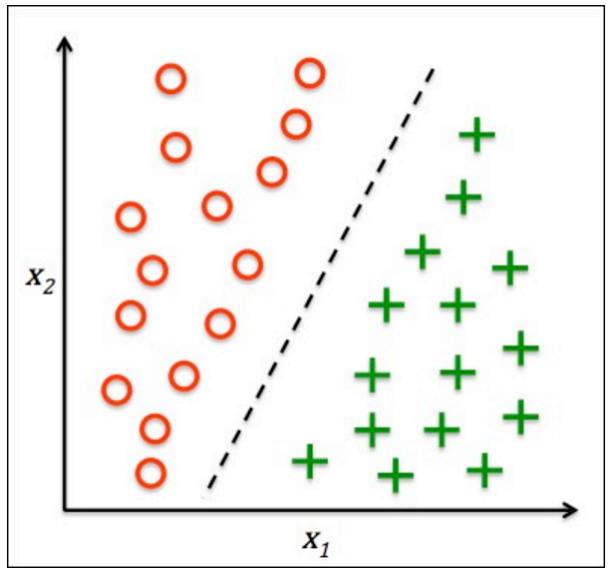
Now that we've established the need and potential benefits of machine learning, we must understand the concept behind the hype. According to Wikipedia –

Machine learning is the subfield of computer science that, according to Arthur Samuel in 1959, gives "computers the ability to learn without being explicitly programmed." Evolved from the study of pattern recognition and computational learning theory in artificial intelligence, machine learning explores the study and construction of algorithms that can learn from and make predictions on data – such algorithms overcome following strictly static program instructions by making data-driven predictions or decisions, through building a model from sample inputs.

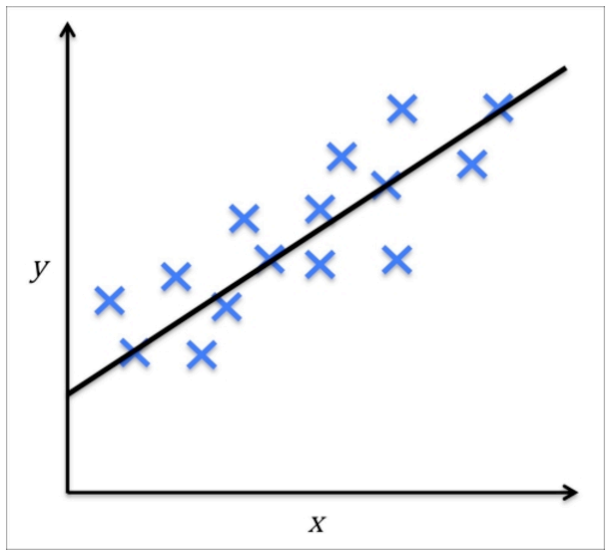
First, let us consider ML from a ten-thousand-foot view. Machine learning can be divided into the following categories:

Supervised learning - The main goal of supervised learning is to develop a model from labeled training data. This mode will allow us to predict future results. The term supervised refers to a set of samples where the desired output labels are already known. The supervised learning is further divided into the two categories:

Classification - Classification is a subcategory of supervised learning focused on predicting the categorical class labels of new instances based on trained observations. Those class labels are discrete, unordered values that can be understood as the group memberships of the instances. Consider the example of e-mail spam filtering - we can train a model using a supervised machine learning algorithm on a corpus of labeled e-mail, categorized by users as spam or ham (not-spam). Once the machine learns to predict spam or ham, the machine can prioritize the spam out of the user's inbox. A supervised learning task with discrete class labels, such as e-mail spam-filtering, is a good classification example.

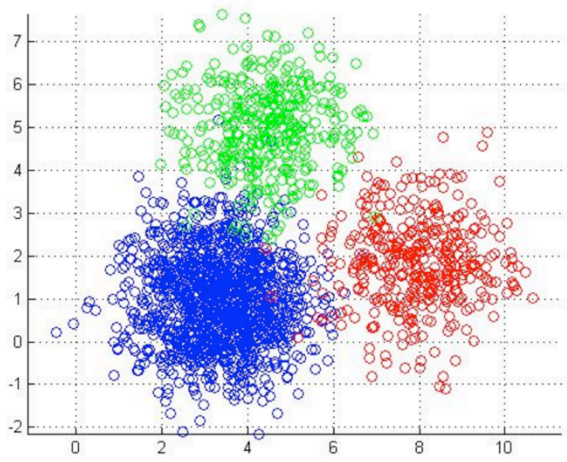


Regression - A second type of supervised learning is the prediction of continuous outcomes, which is also called regression analysis. In regression analysis, we are given a number of predictor (explanatory) variables and a continuous response variable (outcome), and we try to find a relationship between those variables that allows us to predict an outcome. For example, let's assume that we are interested in predicting the math SAT scores of our students. If there is a relationship between the time spent studying for the test and the final scores, we could use it as training data to teach a model to use study time to predict the test scores of future students who are planning to take this test.

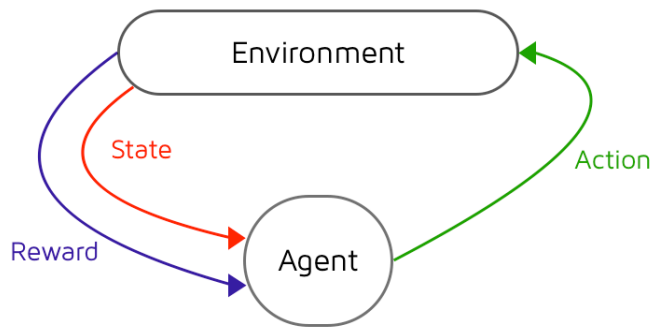


Unsupervised Learning - Unsupervised learning is a type of machine learning algorithm used to draw inferences from datasets consisting of input data without labeled responses. Unsupervised learning is sub categorized into or known as clustering.

Clustering - Clustering is an exploratory data analysis technique that allows us to organize a pile of information into meaningful subgroups (clusters) without having any prior knowledge of their group memberships. Each cluster that may arise during the analysis defines a group of objects that share a certain degree of similarity but are more dissimilar to objects in other clusters. For example, it allows marketers to discover customer groups based on their interests in order to develop distinct marketing programs.



Semi Supervised Learning or Reinforce Learning - Another type of machine learning is reinforcement learning. In reinforcement learning, the goal is to develop a system (agent) that improves its performance based on interactions with the environment. Since the information about the current state of the environment typically also includes a so-called reward signal, we can think of reinforcement learning as a field related to supervised learning. However, in reinforcement learning this feedback is not the correct ground truth label or value, but a measure of how well the action was measured by a reward function. Through the interaction with the environment, an agent can then use reinforcement learning to learn a series of actions that maximizes this reward via an exploratory trial-and-error approach or deliberative planning. A popular example of reinforcement learning is a chess engine. Here, the agent decides upon a series of moves depending on the state of the board (the environment), and the reward can be defined as win or lose at the end of the game.



Now we know what are the different categories of Machine Learning and their sub categories, their definitions and non-information security use cases, let us try to identify where we can use ML in Information Security without going into the algorithm details.

ML Use cases

With the rapid evolution of web, mobile, cloud, IOT technologies, attack techniques are also becoming more sophisticated in penetrating systems and evading generic signature-based approaches. Machine learning techniques offer potential solutions that can be employed for resolving such challenging and complex situations due to their ability to adapt quickly to new and unknown circumstances. Diverse machine learning methods have been already successfully deployed to address wide-ranging problems in computer and information security. Now let us identify different applications of machine learning in Information security. Those are:

- Malware detection
- User behavior analysis
- Mitigating the Denial of Service Attacks
- Web application FW

- Detect Malicious URL
- SPAM Filtering
- Reputation in Cyber Space
- User Identification
- Detecting Identity Theft
- Information Leakage Detection and Prevention
- Social Network Security
- Detecting Advanced Persisted Threats
- Detecting Hidden Channels
- Writing malware

In the next article, I will take one use case from the above mentioned use cases and will explain how to write a working ML code.

References

Raschka, Sebastian. Python Machine Learning. S.l.: Packt Limited, 2015. Print. Wikipedia contributors. "Machine learning." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 4 May. 2017. Web.

THE DIGITAL UNIVERSE IN 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East – IDC and EMC study.

Radical Solution To Identify Web Spam Using Machine Learning AI

Ajay Gowtham

Ajay is passionate about cyber security, Exploit development and Penetration testing activities. He is working with the world's largest accounting and finance staffing firm (S&P 500 and Fortune 500) as lead cyber security consultant for one of the largest UK manufacturing clients. He is an active participant in private bug bounties, International level Research member and holding CVE IDs for a few security vulnerabilities. Also, he published a few 0-day security advisories for the security community.

Machine Learning (ML) is a subfield within Artificial Intelligence (AI) that builds algorithms that allow computers to learn to perform tasks from data instead of being explicitly programmed. ML allows computers to learn and progressively perform computer tasks in an efficient manner with the help of data. Data is feed into the computer that allows the machine learning to construct a pattern using an algorithm and predict the future state output accurately, with less programming. This enhances the computer to perform automated tasks and cognitive thinking ability to solve complex problems with ease. The below split makes it easier to understand the sequential process.

How is Machine Learning trained?

- Feed appropriate data
- Clean, prepare and manipulate data sets
- Train model
- Test data
- Improve and upgrade results

Unpacking - Succeeding with Machine Learning for humans

- Would you be alive if you were caught up in 9/11 attack?
- Would you have survived the sinking of the Titanic?
- Do you need to find your lost friend in the tsunami among 1 million pictures?
- Do you want to predict the next stock market crash?
- Do you want to know how much body weight you may gain after 10 years?

Ice-breaking fact:

Yes, Machine learning (ML) has answers for the questions above and many more not mentioned. The more data you give the machine, the higher output results.

Tools and library files utilized for this experiment

- **The Jupyter Notebook** - The Jupyter Notebook is an open-source web application that allows you to create and share documents that contain live code, equations, visualizations and narrative text.
- **Py3** - Python is a powerful high-level, OOPS programming language.
- **Pandas** - Pandas is an open source library providing high-performance, easy-to-use data structures and data analysis tools for the Python programming language.
- **Scikit** - Scikit-learn is a free software machine learning library for the Python programming language.
- **NumPy** - NumPy is a Python library for large, multi-dimensional arrays and matrices, along with a large collection of high-level mathematical functions to operate on these arrays.

Our Experiment - Reshaping the future of InfoSec with Machine Learning

Abstract: Web search engines serve both legitimate and illegitimate data, such as unsolicited spam content, pirated software packed with malware/backdoors and pirated movies/songs. Usually, the piracy software is used by attackers to spread malware/Trojans by binding with pirated software.

Expectation = Good Data @ Speed

Attackers use spam data/banned movies or pirated movies, songs screened on bad reputed sites to increase the web page's ranking by subverting the web search engine's algorithms used to rank search results. This affects web search engine reputation and increases threats to end users, such as spamdexing. Existing search engines have little or no effect on automatically classifying web spam by type.

“It takes just one spark of genius to ignite a secure revolution.”

What: This experiment helps evaluate the spam content online of pirated movies, software piracy and spam content fuelled sites, etc., and provides a solution to keep spam sites from delivering malicious content to users to serve the refined content with high quality.

How: The experimental results are demonstrated using the multinomial naive Bayes classifier algorithm with the search engine optimizing user experience and online safety.

Why: Let's consider a case study of Google's search engine, released as an update called Penguin (2012 - release year), which is used for the Page Ranking method to identify Spam content in links or sites.

Google Search Engine - Case Study:

This is purely based on web-page ranking in which if a web-page has a low ranking, then it's categorized as a Spam related site or a low-quality content site.

The page ranking concept is used by calculating parameters like browser logs, query logs, ad-click logs, etc.

There are two types of ranking in Search Engine Ranking.

- Static Ranking – Ownership of the web page.
- Dynamic Ranking – Based on relevant content delivered for the respective search query.

If any of the pages has keyword stuffing, link schemes, cloaking or doorway pages, or duplicate content by direct, then that will be ranked low and categorized as Spam. Based on the above spam related calculation, a web-page ranking is created. Penguin detects the number of tags, links, and authoritativeness of the page and ranks the page accordingly. It analyses the number of links pointing to the respective page as one of the page ranking criteria.

In other words, Page rank is the basic concept Google has been using to determine the importance of a page or domain by analysing and counting the number of links pointing to it, thereby giving a rank from 0 to 10.

Since the Google Penguin update looks for SEO techniques to analyse and determine a web-page ranking, it's a disadvantage for a small company that relies on those SEO techniques to make a profit. This makes the Penguin update a less valuable one, even though it has a few more advantages.

Since there is an update with Google, why are we experimenting using machine learning?

There are still a lot of search engine companies, like Google, Yahoo, Bing, Ask.com, AOL, and Baidu that use multiple strategies or don't work on automatically classifying web spam by type.

Conquering the first frontier: However, our proposed experiment would help to identify the spam content on websites in a large scale, automated way at the first step.

Where can we implement this model? Maximizing growth opportunities, adapting your strategy to different markets. In a search engine, website search zone, ERP applications, pharma Industry, finance Industry, etc.

Setting the Scene with Three Scenarios – The Rise of Machine Learning

All these stories illustrate how machine intelligence is at the very heart of humans. When business works better with automation, the world works better with machines.

Scenario #1 – Intelligent Automation in Search Engines:

Objective: Need to find the list of illegitimate movie sites with less false positive nature.

Consider millions of websites indexed in a search engine that serves pirated movies. That means you can watch the latest movies online. Now you have assigned a task to identify legitimate/illegitimate movie sites in a short span of time.

Do you have an appetite for bad data?

Let's put this in a different way. All the sites are made up of coding and words chained together to form sentences. Why don't we split the sites by categorizing them as good vs bad data through automation?

That's exactly what we do through this experiment.

So what's next?

The data analytics platform could be used to narrow down our results. Let's consider, we are implementing it in the Google search engine. In the backend, Google operates its analytics platform, strong data of all websites. It is designed for Google customers experienced using digital analytics.

Jackpot, what have we got?

Upon identifying the legitimate/illegitimate movie sites, we can use the digital analytics platform by feeding all the *found illegitimate movie sites list into that*. Now, the filters can be used; the users who spend more time (more than half an hour) on those sites need to be targeted to remove from the Search engine/ action*, what could be taken against the site owner. The list is ready to attack, spamdexing sites!

**here the 'action' defines that removal of DMCA/ authorized subjected owner copy right removal.*

Scenario #2 – Intensive Automated Search in The Pharma Industry:

Objective: Need to identify the banned medicines on a large scale.

Consider thousands of curated lists of medicine names that are available with some information, and you need to identify good/bad medicine in less than a week.

Do you take one of these banned drug combinations?

We treasure hunted, what have we got? As previously mentioned, the corpus of data can be drilled by using the below ML program to grab the good vs bad data using a trained data set on medicine description/drug information/ingredients and filtering will get us the data to take action* on.

**here the 'action' is defined as the removal of medicine manufacturer/legal actions to be taken care of.*

Scenario #3 – Identify banned books from book collections:

Objective: Need to identify banned books on a large scale.

Gems hunted, what have we got? Imagine, a huge list with good vs banned books. Similar to before, the corpus of data can be drilled by using the below ML program to grab the good vs bad data using a trained data set on book description/author information/publisher details and filtering will get us the data to take further steps on it.

Applause – Bringing Future Ready; Predicting Future Achievement:

- As above mentioned, the below ML helped us to grab the good vs bad data from search engines, huge banned medicine data, banned books, etc.
- Similarly, this can be obtained for various applications to solve the problems.
- We solve one problem, we make human life easier.

What are its special features, distinctive machine intelligence (Pros)?

A single pane of glass shows the risk on global stands of Search Engines, by providing clear insights into the real time user experience and business performance.

☑ **Ultimate Pain Reliever:** Reduced False positive

☑ **Expectations come true:** 360-degree Structured Outcomes

☑ **Life Time Saver:** Time consuming activity is reduced

☑ **Future Forecasts:** Overall business model can be adjusted in real-time.

☑ **Presence of mind for Machines:** Decision making by data, not by assumptions

What are limitations with Machine learning (Cons)?

☑ **Expertise Required:** Need expertise in ML, AI domain

☑ **Efforts are important:** Difficult to train the data set more for accurate results

Making It Happen with ML (An AI Experiment):

https://ajaygowtham.github.io/Machine-Learning-to-Identify-Spam-Websites-SEO/

Note: Data sets are stored in a private bay, due to limited set of data that are present and this experiment is in test bed stage.

Let the Journey Begin (In a Nutshell):

Import required libraries are depicted in the image below:

```
import numpy as np
import pandas as pd
import matplotlib
from pylab import *
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.cross_validation import train_test_split
from sklearn.naive_bayes import MultinomialNB
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.metrics import average_precision_score
```

Load dataset into pandas Data Frame (2D data structure) and the data frames are given as status and message:

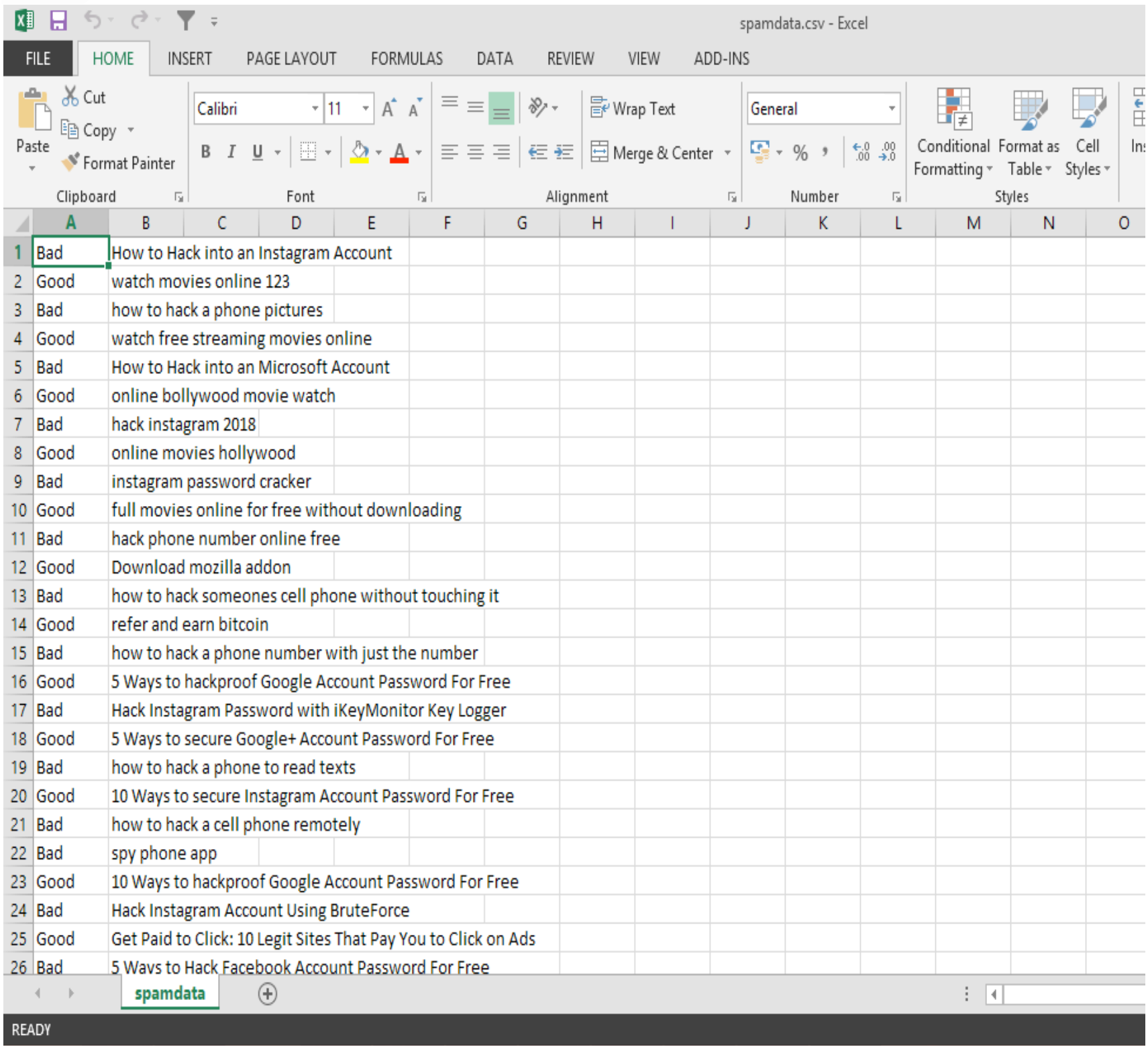
```
df=pd.read_csv('data1/spamdata.csv',names=['Status','Message'])
```

Trained Data Set:

Assorted good and bad data are split up as given below:

- Good Data – provides non-spam content to the users
- Bad Data – provides spam content to the users

Consider a search engine that consists of millions of assorted websites with good (healthy websites do not harm the users) and bad content (published by bad actors to abuse users' computers/illegitimate content). Here, to address the problem in large scale, such as a search engine, we use the web content text as a main pattern source to classify the millions of websites to identify good/bad reputed site. From the trained data set, we split the data into two categories by labelling it Good ('1' integer value) or Bad ('0' integer value).



	A	B
1	Bad	How to Hack into an Instagram Account
2	Good	watch movies online 123
3	Bad	how to hack a phone pictures
4	Good	watch free streaming movies online
5	Bad	How to Hack into an Microsoft Account
6	Good	online bollywood movie watch
7	Bad	hack instagram 2018
8	Good	online movies hollywood
9	Bad	instagram password cracker
10	Good	full movies online for free without downloading
11	Bad	hack phone number online free
12	Good	Download mozilla addon
13	Bad	how to hack someones cell phone without touching it
14	Good	refer and earn bitcoin
15	Bad	how to hack a phone number with just the number
16	Good	5 Ways to hackproof Google Account Password For Free
17	Bad	Hack Instagram Password with iKeyMonitor Key Logger
18	Good	5 Ways to secure Google+ Account Password For Free
19	Bad	how to hack a phone to read texts
20	Good	10 Ways to secure Instagram Account Password For Free
21	Bad	how to hack a cell phone remotely
22	Bad	spy phone app
23	Good	10 Ways to hackproof Google Account Password For Free
24	Bad	Hack Instagram Account Using BruteForce
25	Good	Get Paid to Click: 10 Legit Sites That Pay You to Click on Ads
26	Bad	5 Ways to Hack Facebook Account Password For Free

Classified Good vs Bad data split as follows:

	Status	Message
0	Bad	How to Hack into an Instagram Account
1	Good	watch movies online 123
2	Bad	how to hack a phone pictures
3	Good	watch free streaming movies online
4	Bad	How to Hack into an Microsoft Account

The data shown below is a mixture of multiple raw words and line patterns. However, as an algorithm, it works effectively only in the numbers (i.e., integer values).

```
In [8]: df_x
```

```
Out[8]: 0                How to Hack into an Instagram Account
        1                             watch movies online 123
        2                          how to hack a phone pictures
        3              watch free streaming movies online
        4                How to Hack into an Microsoft Account
        5                          online bollywood movie watch
        6                                hack instagram 2018
        7                            online movies hollywood
        8                         instagram password cracker
        9          full movies online for free without downloading
        10                      hack phone number online free
        11                              Download mozilla addon
        12     how to hack someones cell phone without touchi...
        13                             refer and earn bitcoin
        14       how to hack a phone number with just the number
        15     5 Ways to hackproof Google Account Password Fo...
        16     Hack Instagram Password with iKeyMonitor Key L...
        17     5 Ways to secure Google+ Account Password For ...
        18                    how to hack a phone to read texts
```

The content should be transformed into numbers without losing too much data.

Analyzing the feature:

Bag of words is a Vector Space Model in which each word will be considered unique and, based on that, it will be used in document classification in vectorization. In this model, the words in the given input will be given vector values (regardless of meaning of the word, grammar of the word, etc.) when it has more than a single occurrence. Therefore, here we use a count vector instead of bag of words technique by splitting the test and training data. For instance, *Referring to the In[11]: input, the "Download" word is only repeated once, which is reflected as output for the function cv.get_feature_names() in array format,* i.e.,

```
array ([1, 0, 1, 0, 0, 0, 0, 0, 1, 0],

            [0, 1, 1, 1, 0, 0, 0, 1, 0, 0],

            [0, 0, 0, 0, 1, 1, 1, 0, 0, 1]], dtype=int64)
```

Similarly, the features are extracted from the words. Here, it counts the numbers of words in corpus and assigns as array format as shown below:

```
In [9]: cv=CountVectorizer()

In [10]: x_train, x_test, y_train, y_test = train_test_split(df_x, df_y, test_size=0.2, random_state=4)

In [11]: x_traincv = cv.fit_transform(["Download hack tools", "How to hack Facebook", "Watch Pirated movies online"])

In [12]: x_traincv.toarray()

Out[12]: array([[1, 0, 1, 0, 0, 0, 0, 0, 1, 0],
                [0, 1, 1, 1, 0, 0, 0, 1, 0, 0],
                [0, 0, 0, 0, 1, 1, 1, 0, 0, 1]], dtype=int64)

In [13]: cv.get_feature_names()

Out[13]: ['download',
          'facebook',
          'hack',
          'how',
          'movies',
          'online',
          'pirated',
          'to',
          'tools',
          'watch']
```

Again, using the count vectoring to the trained data sets all are converted into integers as shown below, which is ready available to feed into a machine learning algorithm.

```
In [17]: cv1=CountVectorizer()

In [21]: x_traincv=cv1.fit_transform((x_train).values.astype('str'))

In [22]: a=x_traincv.toarray()

In [23]: a

Out[23]: array([[0, 0, 0, ..., 0, 0, 0],
                [0, 0, 0, ..., 0, 0, 0],
                [0, 0, 0, ..., 0, 0, 0],
                ...,
                [0, 0, 0, ..., 1, 0, 0],
                [0, 0, 0, ..., 0, 0, 0],
                [0, 0, 0, ..., 0, 0, 0]], dtype=int64)

In [24]: a[0]

Out[24]: array([0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0], dtype=int64)
```

```
In [338]: x_traincv.toarray()

Out[338]: array([[0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.87110198,
                  0.        , 0.        , 0.        , 0.49110216, 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        ],
                 [0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.88995571, 0.        , 0.        , 0.45604696, 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        ],
                 [0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.52898678, 0.        , 0.        , 0.        , 0.46178696,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
                  0.        , 0.        , 0.        , 0.        , 0.        ,
```

The above experiment used text data analyzing, which could dominate the final results. For example, words such as “and”, “to”, etc., that are high in number, may dominate the output of the ML experiment. So here, Tfidf vectorizer is used to classify if it’s a good or bad reputed site using the text/sentences present in the website. This allows to add less weightage to repetitive words, such as “and”, “to”, etc. Tfidf helps to increase the edge words by increasing more features to the above vector.

Here, we are using Tfidf vectorizer function and re-running the program again would sync the complete data and results as below in next section:

```
import numpy as np
import pandas as pd
import matplotlib
from pylab import *
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.cross_validation import train_test_split
from sklearn.naive_bayes import MultinomialNB
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.metrics import average_precision_score
from sklearn.feature_extraction.text import TfidfVectoriz
```

Implementation in a large scale search engine would allow the operation to be performed in the background. Crawling sites with huge trained data sets helps to eliminate the bad reputed websites that serve malicious web content, spam websites, or pirated movies/songs.

So, what is Tfidf vectorizer – How does it help in this experiment?

The term frequency-inverse document frequency (Tfidf) is a statistic that shows the importance of a word to a specific document relative to all of the words in corpus. The Tfidf value increases appropriately to the number of times a word appears in the document, but is offset by the frequency of the word in the corpus.

```
In [43]: cv1=TfidfVectorizer(min_df=1, stop_words='english')

In [44]: x_train, x_test, y_train, y_test = train_test_split(df_x, df_y, test_size=0.2, random_state=4)

In [45]: x_traincv = cv.fit_transform(["Download hack tools", "How to hack Facebook", "Watch Pirated movies online"])

In [46]: x_traincv.toarray()

Out[46]: array([[0.62276601, 0.        , 0.4736296 , 0.        , 0.        ,
                 0.        , 0.62276601, 0.        ],
                [0.        , 0.79596054, 0.60534851, 0.        , 0.        ,
                 0.        , 0.        , 0.        ],
                [0.        , 0.        , 0.        , 0.5       , 0.5       ,
                 0.5       , 0.        , 0.5       ]])
```

In a scenario like smaller data -text, count vectorizer would be helpful. As this experiment is to address the problem in larger scale, Tfidf is used here.

```
In [51]: a

Out[51]: array([[0, 0, 0, ..., 0, 0, 0],
                [0, 0, 0, ..., 0, 0, 0],
                [0, 0, 0, ..., 0, 0, 0],
                ...,
                [0, 0, 0, ..., 1, 0, 0],
                [0, 0, 0, ..., 0, 0, 0],
                [0, 0, 0, ..., 0, 0, 0]], dtype=int64)

In [52]: a[0]

Out[52]: array([0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
                0], dtype=int64)

In [53]: cv1.inverse_transform(a[0])

Out[53]: [array(['and', 'bitcoin', 'earn', 'refer'], dtype='<U12')]
```

The feature extraction of the data is successfully completed as shown below,

```
In [346]: x_train.iloc[0]

Out[346]: 'refer and earn bitcoin '
```

Now, a machine learning algorithm multinomial (sklearn.naive_bayes.MultinomialNB) classifier is used to classify the data by integer method.

Technology to Drive the Change: How does the Multinomial Naive Bayes Algorithm work in our experiment? Feature is property (i.e., attribute of object) that is “category” column which is a characteristic phenomenon measured using “text data” column.

Hack	$\frac{2+1}{8+14}$	$\frac{1+1}{7+14}$
Into	$\frac{1+1}{8+14}$	$\frac{0+1}{7+14}$
An	$\frac{0+1}{8+14}$	$\frac{1+1}{7+14}$
Website	$\frac{2+1}{8+14}$	$\frac{0+1}{7+14}$

The input data is analysed by considering the word frequency in “text data” column by assigning numerical values, to classify as spam or non-spam.

Text Data	Category
“Hack this website ”	Spam
“Data network to PC”	Non-Spam
“steal this api-key”	Spam
“Hack into a social website”	Spam
“why to Hack an network”	Non-Spam

By considering the below given Bayes’ Theorem formula,

$$P(A|B) = \frac{P(B \mid A) \times P(A)}{P(B)}$$

The probability of hypothesis spam or non-spam from the axioms of conditional probability are calculated as given below:

$$P(Spam \mid Hack\ into\ an\ website) = \frac{P(Hack\,\mathrm{int}\,oanwebsite \vee Spam) \times P(Spam)}{P(Hack\,\mathrm{int}\,oanwebsite)}$$

As stated above, if the probability is calculated for whole corpus statement such as

P (Spam | Hack into a website), the whole value will become 0.

The output would be null value - which is shown as

P (Spam | Hack into a website) = 0

It can be avoided by considering a numerical value to each word frequency, which can be achieved using naïve Bayes algorithm.

Naive Bayes Algorithm:

Assuming each word in the data set is assigned with unique values, the probability calculations will result in obtaining the actual result. For instance, the below probability is calculated by assigning a value to each word in a sentence instead of considering the whole sentence, thus increasing the probability to predict the accurate result.

By rewriting the probability to calculate spam/non-spam:

P (Hack into an website | Spam) = P (Hack) × P (into) ×P (an) ×P (website)

It can be rewritten as:

P (Hack into an website | Spam) = P (Hack| Spam) × P (into| Spam) ×P (an| Spam) ×P (website| Spam)

Similarly, for Non-Spam, the probability will be:

P(Hack into an website | Non- *Spam) = P(Hack*| Non- *Spam) × P(into*| Non- *Spam) ×P(an*| Non- *Spam) ×P(website*| Non-*Spam)*

We are calculating the probability of a single word from the input by using the below formula, in the spam category:

P (Hack | Spam) = (Count of new word in spam category i.e., Hack + Total number of new word appearance in both spam and non-spam) / (Total no. of unique word in spam category + Total unique word)

P (*Hack | Spam*) = (2+3) / (8+14) = 5/22

Accordingly, we can obtain the other probabilities necessary for comparing to predict spam/non-spam – output data:

P (*Hack into an website |Spam*) with **P (*Hack into an website | Non-Spam*)**

List of unique words in the data set as referenced above = {hack, this, website, data, network, to, PC, steal, this, api-key, a, social, why, an}

P (Hack into a website | Spam) = P (How | spam) × P (into | spam) ×P (an | Spam) × P (website| Spam)

= (3/25)*(2/25)*(1/25)*(3/25)

$=4.61 \times 10^{-5}$

= 0.0000461

P (Hack into a website |Non-Spam) = P (How |Non-Spam) × P (into |Non-Spam) ×P (an | |Non-Spam) × P (website |Non-Spam)

= (2/23)*(1/23)*(2/23)*(1/23)

$=1.43 \times 10^{-5}$

= 0.0000143

By comparing the results above, P (How to Hack an website | Spam) gives a higher probability, which directly shows that the sentence belongs to the Spam category.

Again, circling back to the above theory, the below demonstrated “pred” prediction is the series of streamlined data:

```
In [244]: mnb=MultinomialNB()

In [245]: y_train=y_train.astype('int')

In [246]: mnb.fit(x_traincv, y_train)
Out[246]: MultinomialNB(alpha=1.0, class_prior=None, fit_prior=True)

In [247]: x_testcv=cv1.transform(x_test)

In [248]: pred=mnb.predict(x_traincv)

In [267]: pred
Out[267]: array([1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1,
                 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1,
                 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0,
                 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0,
                 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0])

In [263]: actual=np.array(y_test)

In [264]: actual
Out[264]: array([0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1,
                 0, 0, 0], dtype=object)

In [289]: count=1

In [290]: for i in range (len(pred)):
              if pred[i]==actual[i]:
                  count=count+ 1
```

To test this experiment, as above defined – referencing again here,

Good (‘1’ integer value)

Bad (‘0’ integer value)

Pause for a second, wheeling back…

Conclusion: Preparing people to embrace automation

As the nature of work has changed, so too have the methods of automation. Artificial Intelligent process and Machine learning automation tools can help businesses improve the effectiveness of services faster and at a lower cost than current methods, but with important limitations.

The Machine Learning automation has the potential to change today’s workplace as dramatically as the machines of the Industrial Revolution changed the office floor. Just as with prior waves of automation, we can expect that Artificial Intelligence will likely drive significant changes in the jobs that people do. In our case, instead of people manually checking millions of sites, they can save their energy and complete time-consuming tasks more easily and can focus on other advanced productivity.

So, this helps us to achieve better data quality and reduce operational costs.

We see the bigger picture in implementation of our experiment with Search engine delivering a wide range of benefits.

Tasting our medicine output:

Circling back to our experiment and cross validating the output using the function (x_test.iloc[0]) – successfully identifies the bad content (spam one) as given below,

```
In [278]: x_test.iloc[0]

Out[278]: 'How to Hack into an Facebook Account '
```

Introduction to Cyber Security for Nuclear Power Plant

Md. Tawhidur Rahman Pial

Mr. Tawhidur Rahman is a security professional with over 12 years of experience in Cyber security consultancy, Digital forensic, Framework Design, Policy Making, project development and execution, integration of various technologies, lawful interception system, Telecommunication network interrogation & active tracking system, command control and communication, critical infrastructure security, tactical & intelligence solutions etc. He has 48 Global vendor certificates like C|CISO, CEH, ITILFV3, ISO/IEC 27001 LA, COBIT 5, CLPTP, CCTA, CFIP, CCIP, Counterintelligence, OSINT…. etc. he also certified from He is working now as Team Leader of Government of Bangladesh E-Government Computer Incident Response Team and previously he was working for Government Joint Defense organization as a cyber security consultant.

One way to protect power plants from intruders is to harden the system. Here I don't just talk about hardening the operating system, but the system as a whole. Writing and applying security policies is one of the major steps of IT-security. The second and perhaps even more important step is to implement these policies. Employee training is crucial, since the human element will always be the weakest element. It is much easier to obtain information from a friendly employee that had no conscious understanding of IT-security than trying to find a weak point in a computer system and penetrating it for the wanted information.

Introduction

The development of nuclear energy accompanied the invention of the computers, which brought about a development that we would call the Third Industrial Revolution. This development generated a complex of economic, political, social effects that is in some cases, like in the case of power plant safety, considered national security. In this context, power plants belong to the ICS category. Industrial control system (ICS) is a vague term to describe several types of control systems used in industrial production, such as in electric, gas or water plants, as well as supervisory control and data acquisition (SCADA) systems, distributed control systems [use fully qualified domain names (FQDN)] (DCS), and other control systems (Wikipedia, 2011). All of these are defined as critical infrastructures and are considered national security objects. These infrastructures need to be protected from cyber incidents, which is defined by the NIST as "an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits (FIBS PUB, 2006)." [2] These threats might be

intentional malicious attacks or unintentional, caused by untrained or careless employees. In addition, modern networking and communication technologies used to improve also create new cyber vulnerabilities. Care must be exercised in the selection, implementation, and operation of cyber-vulnerable ICS technologies.

What is Nuclear Plant Security and how is it defined?

Nuclear plant security involves the securing of critical business and operational functions performed by cyber assets affecting the bulk electric system necessitate having security management controls. To protect critical cyber assets (each company should define these assets individually), companies should design and implement an information protection plan, define employee roles and responsibilities, as well as provide security training. In this context, we need to look at some of the possible threats and attacks. One such attack is the SCADA attack. SCADA hacks, SCADA attacks, or system vulnerabilities pose significant threats to power plants. They combine traditional exploits with industrial control systems, which allows attackers to weaponize malicious code, as demonstrated with Stuxnet worm in 2010 to attack the Iranian power plant, which was using Simetic 7 from Siemens. SCADA systems control everything from valves on oil and gas pipelines to energy grids, and heat sensors in power plants, but they are usually not connected to the internet. "*SCADA systems run in small private networks hidden away from the rest of the world, usually perfectly secure against reasonably determined hackers. Ergo, SCADA software and hardware by its very nature is not as secure, because it is nowhere near as well known or scrutinized and is heavily dependent on physical security to keep it safe. However, the environments that SCADA systems monitor are usually mission critical; their failure would have serious or even catastrophic consequences*." (Wiley & Sons, 2008)

So what does an attacker need for a successful attack? This is a legitimate question to ask, if considering ways of preventing an attack. There are two ways to attack a SCADA system. One, if the system is connected to the internet for vendor updates and maintenance, finding leaks and security holes in the connection and network structure; second, the intruder attacks by collecting information about what SCADA systems are being used (software and hardware), which vendor they use and preferably the locations of the terminals and then implanting the attack.

A SCADA hack can be remote access hacks. Gathering information about the system over social networking and asking untrained employees about security, intruders can collect valuable information bit by bit to bring down the system. Sometimes, web pages of vendors give out a great deal of information about the clients they take on, and the system software used. With a little research and reading through press releases, hackers can find out the hardware used. The next step is social engineering over the phone or in person. With this information, remote control stations can be broken into, networks from the remote access point used and a SCADA hack made possible.

I came to the conclusion that it is not important how these attacks happen, let's simply assume for a minute that they do happen.

With this in mind, I would like to emphasize what to do and how to prevent these attacks. One way to protect power plants from intruders is to harden the system. Here I don't just talk about hardening the operating system, but the system as a whole. Writing and applying security policies is one of the major steps of IT-security. The second and perhaps even more important step is to implement these policies. Employee training is crucial, since the human element will always be the weakest element. It is much easier to obtain information from a friendly employee that had no conscious understanding of IT-security than trying to find a weak point in a computer system and penetrating it for the wanted information. The following are suggestions for prevention measures mentioned in Allsopp's book of unauthorized access.

Prevention measures Information Protection

Document and implement a process for the protection of information pertaining to or used by critical cyber assets. The roles of whom should write these policies and who should implement them on site should be clearly defined.

Identification. In a security plan, all assets and mechanical equipment that are identified as being computer operated need to be identified.

Classification. This equipment and these systems then need to be assigned a security level and a security zone.

Protection. A plan that drafts the constant maintenance and ongoing protection should be drafted.

Roles and Responsibilities

Roles and responsibilities of employees should be well defined and briefed. Responsible managers should document and direct SCADA security. This can be done with the help of the company's employee and mechanical system architecture. The most important part is to define these roles and responsibilities on the vendor's side as well as on the nuclear plant side.

Physical Security

One might argue that physical security has nothing to do with IT-security. I believe it has everything to do with it. If I can't penetrate a local remote access station, how can I penetrate the system in the first place? First, I have to beat the physical security before I can get to the systems. The biggest challenge is to convince IT-security managers, that have little training or no knowledge of real life threats. The implementation of processes, tools and procedures to monitor physical access to the power plant and its critical cyber assets, as well as all access points to the computer systems, should be clear. Security measures could include identification:

- Bio-metric, keypad, token, or other devices that are used to control access to the cyber asset through personnel authentication.
- Surveillance cameras.
- Alarm systems inside the building and outside.
- Maintenance and testing of the implemented security measures, as well as software and hardware used.
- Electronic media control. No unnecessary technology allowed into the plants, like cell phones, cameras, etc. (Nuclear Plant Security, 2009)

Cyber asset security

The main concern should be the implementation of the security measures and a regular check of the implemented methods. It is important to:

- Keeping the system updated and patched
- Account and password management
- Software integrity checks
- Employee training
- Acting according to international standards
- Always being inspection ready and up to par

- Identifying and handling vulnerabilities

Conclusion

It is very critical that all power plant operations, as well as other ICSs, are protected from cyber-attacks to maintain the mission of the systems. SCADA systems are often believed to be safe, but several lab tests have shown vulnerabilities that could cause tremendous financial and physical damage to a nuclear plant. Threats come from the inside as well as outside, intentional and unintentional, but the key is to have clear defined rules, regulations and policies in place. Identifying system vulnerabilities, training employees and having an incident prevention, as well as incident response, plan is of great importance. Of course, any advice looks good on paper, but a good security manager knows that there is no system that is completely secure or no system that cannot be penetrated. The job is to keep testing the system, finding weak points and exploiting them, and preferably cataloging them, not hiding them or ignoring them.

Bibliography:

- Allsopp, W. (2009). *Unauthorised Access: Physical Penetration Testing For IT Security Teams*. New York: John Wiley & Sons. [only in Annotated Bibliography, not in References - In this book Wil Allsopp has created a thorough reference for those looking to advance into the area of physical penetration testing. The book thus serves as a guidebook for in-house security managers seeking to institute better policy safeguards." - From the Foreword, by Kevin Mitnick. Most IT security teams concentrate on keeping networks and systems safe from the outside - usually with the entire focus on firewalls, server configuration, application security, intrusion detection systems, and the like.]

- Basta, A., & Halton, W. (2008). *Computer Security and Penetration Testing.* Boston: Course Technology. Covered many subjects concerning penetration testing and gave a general overview of network monitoring and penetration testing.

- Graves, K. (2010). *CEH® Certified Ethical Hacker Study Guide.* Indianapolis: Wiley Publishing, Inc. This book is a study guide for a certificate as an ethical hacker. Network security, penetration testing and incident handling are some of the subjects discussed.

- Hold, M., & Anthony, A. (2008). *Nuclear Power Plant and Security Vulnerabilities.* Washington: Congress EH® *Certified Ethical Hacker Study Guide.* This paper discussed the overall plant security, threat models and scenarios, as well as incident emergency response.

- *Nuclear Power Plant Security.* (2009, August). Retrieved July 28, 2011, from Nuclear Energy Institute: http://www.nei.org/keyissues/safetyandsecurity/factsheets/powerplantsecurity/ General information about nuclear plant security emphasizes physical plant security measures' and breaches.

- Oriyano, S.-P., & Gregg, M. H*acker Techniques, Tools, and Incident Handling.* It discussed general information in the first two chapters. Then, it goes on to review the technical overview of hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on the Web.

- Weiss, J. (2010). *Protecting Industrial Control Systems from Electronic Threats*. New York: Momentum Press, LLC. This book discussed the measures that can be taken to protect industrial control systems by listing and demonstrating the threats and suggesting how to handle them. Safari books online :http://search.safaribooksonline.com/book/technology-management/9780470145012 http://www.msnbc.msn.com/id/42237805/ns/technology_and_science-security/t/nuclear-plant-software-called-vulnerable-attack/

- NIST Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf This is a great sample for writing security policies. It is similar to the ISO 2700 series.

Pentesting SCADA Networks

Anandharaj Velu

Anandharaj Velu holds Master of Technology (M.Tech) in Computer Networks and Information Security and works as an Information Security Engineer at IARM Information Security PVT Ltd, Chennai, India.

The SCADA system makes prompt notifications to an operator that a batch of product is showing a high incidence of errors. This helps the operator to pause the operation and view the SCADA system data through an HMI to determine the cause of the issue. The operator reviews the data and discovers that a particular machine was malfunctioning. With the SCADA system's ability to notify the operator of an issue, he/she can resolve the problem and prevent further loss of product.

Introduction

Industrial control system (ICS) is a general term for various types of control systems. They are supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and system configurations, such as Programmable Logic Controllers (PLC). They are often found in the following industries:

- Nuclear power plant systems
- Oil and gas pipelines
- Electrical grid systems
- Rail control systems
- Air traffic control systems
- Security systems
- Webcams
- Sewage and water systems
- Financial systems and ATMs
- HVAC systems

SCADA systems have been around since the mid-1960s. This system evolved from the electric utility systems in the 1940s. Though it is a very old system, it's recently in the spotlight for security because of upgrading and increasingly being migrated to corporate networks. These systems run on low bandwidth, and over disparate networks. ISCADA networks run over cable, fibre and wireless IP networks. Though many people don't understand how to compromise a SCADA serial network, there are people who know how to hack, and therein lies the problem; once closed system is now increasingly open to abuse.

SCADA

SCADA system has software and hardware for industrial organizations to:

- Monitor, gather, and process real-time data
- Control industrial processes locally or at remote locations
- Directly interact with devices through human-machine interface (HMI) software
- Record events into a log file

SCADA systems are very important to maintain efficiency, process data for smarter decisions, and communicate system issues to mitigate downtime. The basic SCADA architecture has programmable logic controllers (PLCs) and remote terminal units (RTUs). PLCs and RTUs are microcomputers that communicate with factory machines, HMIs, sensors, and end devices, and then route the information from those objects to computers with SCADA software. The SCADA software processes, distributes, and displays the data to operators and other employees which helps them to analyze the data and make important decisions.

SCADA COMPONENTS

1. **Human Machine Interface (HMI):** It is a Windows/Linux workstation to manage and control PLCs on the network through client software. If an HMI is compromised, an attacker can gain access to everything on your SCADA network.

2. **Programmable Logic Controller (PLC):** PLC is a physical system that manages the sensors and actuators. PLC is connected with a power supply and network that uses TCP/IP to communicate over Ethernet networks. It could have an LCD panel showing controller status, operator messages, etc. Due to the usage of third party tools and TCP/IP, we have seen that PLCs are accessible via web browsers, Telnet, SSH - exposing it to all kinds of application and network layer attacks. If the PLC is compromised, a malicious attacker can manipulate the input/output of your devices, which results in serious damage to the organisation.

3. **End Devices (Sensor, Valve or Pump):** End devices installed at the remote site. They report to PLCs over communication links such as radio, serial connections, Ethernet or direct modems. If compromised, an attacker can compromise the integrity of the environment.

4. **Sensors and actuators:** Allows interaction with the physical world (pressure sensor, valves, motors, etc.).

5. **Data historian:** Records all the data from the production and SCADA networks. Collects and stores data regarding process statistics, sensor readings, inputs/outputs and other measures. Data is stored in a database such as MSSQL or Oracle.

6. **Remote Terminal Unit (RTU):** RTU collects data and correlates it between physical sensors and SCADA processes.

Note: *You may discover other devices such as database servers, serial device interfaces, etc.*

Penetration testing approach:

Penetration testing should be performed on a periodic basis depending on the criticality of the targeted system. This can be performed as a broad penetration test encompassing several control systems (such as an entire testing or staging control network), a targeted penetration test with a restricted scope of a single control system (management server to its controlled devices), or to test a single component of a larger system, such as a historian or a reclosure. NESCOR recommends performing this type of assessment in testing or staging environments on an annual basis or after any major systems upgrades or changes to the systems in question.

When we perform penetration testing, our main goal is to identify as many vulnerabilities as possible, and to determine the impact of those vulnerabilities being exploited by threat. While we perform penetration testing for clients that rely on SCADA/ICS systems, we should follow self-imposed restrictions and special procedures because **ensuring safety of the public, personnel, and systems that are critical to continued operations should be our main concern rather than testing of the entirety of an organization's network.**

Target System Setup

Penetration tests should be performed on non-production systems and devices that are installed and configured for functional operation in testing environments. The closer the target systems are configured to their production counterparts, the more accurate result you will receive.

Embedded Device Penetration Tasks

Penetration testing of embedded devices, microprocessor based devices that are reasonably exposed to physical attack, hardware that is commonly deployed in areas where attackers could easily gain physical access, such as on customer premises, or in substations, should be tested using the tasks listed below.

These tasks target electronic components inside these field deployed devices, namely those microchips that store data (EEPROM, Flash, RAM, MCU on-chip storage), buses that pass data between components (parallel buses and serial buses), and input interfaces used for administrative or debugging purposes (serial ports, parallel ports, infrared/optical ports). The following table will help map specific components that should be considered for each Smart Grid product domain.

Tool List

Here are the tools that I have personally used in a SCADA assessment and have found do their job well.

- smod: ModBus penetration testing framework
- plcscan: Python script for scanning PLC devices
- NMAP Scripts: NMAP script to scan PLC devices
- Wireshark: Network sniffer
- mbtget: Perl script to read data from PLC
- Plcinject: Tool to inject code into PLCs
- CSET: The Cyber Security Evaluation Tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks.

Port scanning can crash systems if not careful!

- Don't use the -O or -A flags in nmap because most problematic on embedded devices not running Windows or Linux. You can do ARP scans locally on each subnet and use MAC to ID devices
- When Scanning with SYN scans, you have to always specify -sT in your scans
- By default Nmap scans too fast, to avoid this you should use nmap's -T2 setting to set this at 0.4 seconds
- Service fingerprinting usually safe, but can occasionally cause problems so you have to use nmap's -sV selectively on new subnets
- Always run nmap with sudo
- It's always good practice to use -v when scanning

Low Risk port scans

```
sudo nmap –n –PR –sn
```

- Risk = Almost None (only does ARP request (IP -> MAC) which is required by TCP)
- Value = retrieves MAC address if IP is live, which can be used to fingerprint
- Note = this must be done from the SAME subnet as the IP being scanned

```
sudo nmap –n –sn
```

- Risk = Very Low (only sends ICMP and TCP80/443 ping requests)
- Value = shows if IP address is responding to pings
- Note = if done on same subnet, will retrieve MAC address

```
sudo nmap -n -sT --scan-delay 1 --top-ports 100
```

- Risk = Low (scans each host's TCP ports serially with 1 second delays)
- Value = Medium (tests for most common TCP servers...but not ICS protocols)

Medium to High Risk port scans

```
sudo nmap –n –sT --max-parallelism 1 -p
```

- Risk = Medium Low (scans each host's TCP ports serially as fast as possible)
- Value = Medium High (tests for whatever services you specify but quickly)

```
sudo nmap –n –sT --max-parallelism 1 -p- -sV ...
```

- Risk = Medium (scans each host's TCP ports serially as fast as possible)

- Value = High (scans all possible TCP ports)

```
sudo nmap –n -sT -p- -A ...
```

- Risk = High (likely to crash most old gear and even some modern)
- Value = High (scans all possible ports, fingerprints everything, and runs NSE)

```
sudo nmap –n -sT -sU -p- -A ...
```

- Risk = Extremely High (likely to crash most old gear and even some modern)
- Value = High (scans all possible ports, fingerprints everything, and runs NSE)

Conclusion

SCADA systems are widely used to monitor and control industrial processes. They provide the functionality of real-time monitoring, logging/archiving, report generation, and automation among other things. Due to modern technology and usage of third party tools, SCADA Networks are vulnerable and targeted so it is highly advised for penetration testing. we should follow self-imposed restrictions and special procedures because ensuring safety of the public, personnel, and systems that are critical to continued operations should be our main concern than testing of the entirety of an organization's network.

References

NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security
https://inductiveautomation.com/what-is-scada
http://research.aurainfosec.io/scada-penetration-testing/
https://github.com/hslatman/awesome-industrial-control-system-security
http://www.samuraistfu.org/resources
https://github.com/enddo/smod
https://github.com/tangjiajia9/plcscan
https://www.wireshark.org/
https://github.com/sourceperl/mbtget
https://github.com/SCADACS/PLCinject
https://ics-cert.us-cert.gov/Assessments
https://nmap.org/download.html

Meltdown and Spectre - Feature Exploits As CPU Vulnerabilities

Jeremy Walker and Chris Berberich are Managing Director(s) at CYBIEN. CYBIEN specialization is in Information Security and Regulatory compliance, focusing on both policy and technology risk assessment aspects of compliance with the specific regulations including: NCUA requirements, Gramm-Leach-Bliley Act [GLBA], Federal Financial Institutions Examination Council [FFIEC], National Institute of Standards and Technology [NIST], International Organization of Standardization or International Standards Organization [ISO], and Payment Card Industry Data Security Standards [PCI-DSS] requirements and general good business practices.

Jeremy Walker

Jeremy Walker has a well-rounded Information Technology background. He has over 13 years of combined experience designing, maintaining, and securing military and agency Information Technology systems. His work experience includes roles with the Federal Government as a Cyber-security engineer where he performed security assessments and compliance testing for government acquisition programs. He has spent time overseas in support of multiple “3” letter agencies.

Chris Berberich

Chris Berberich has extensive knowledge working with applications, network equipment (internal and external), network security, network operating systems and networking protocols. He has performed over 700 Penetration Tests regarding audit related, web applications, black and white testing Penetration Tests and Compliance Audits (PCI, HIPPA, SOC, DIACAP, SSAE 16, ISO 27011, NCUA (related) and FISMA).

Spectre (CVE-2017-5753 & CVE-2017-5715), which is a close relative to Meltdown, impacts Intel, AMD, and ARM CPUs by calculating branch prediction and speculative execution, resulting in a data leak from compromised processes. Spectre is perpendicular to Meltdown, which exploits CPUs to allow out-of-order execution of user instructions to read kernel memory. Spectre permits an attacker to bypass additional application(s) to access random portions of its memory, and the exploit occurs with a read through on those applications.

Meltdown and Spectre are feature exploits, not chip design flaws, and both are garnering massive attention due to the industries they affect and the price hike in processors in the past few months. They both have the potential to read the kernel secret location(s) used by the device(s) and application(s) (including browsers) that store sensitive information located in the kernel memory, including potentially sensitive data; however, they cannot read memory on a disk drive. Additionally, the exploits require an extensive understanding of where the sensitive data is located and require substantial processing/decoding.

Let's clarify what Meltdown and Spectre cannot do:

- The exploits do not allow takeover or modification of machines and operating systems.
- They do not allow data access and retrieval of stored data sets on disk drives (rules out DDoS Attacks).

The Meltdown (CVE-2017-5754 (rogue data cache load)) and Spectre (CVE-2017-5753 (bounds check bypass) & CVE-2017-5715 (branch target injection)) vulnerabilities could potentially impact the key processor vendors. Both vulnerabilities deal with CPU data caching and are true side-channel attacks, and like WPAD attacks, they are both feature exploits.

Meltdown (CVE-2017-5754) provides access to all physical memory, including kernel memory, and using a "user" mode ring 3 process, allows any process running on the device(s) access to the physical memory.

Meltdown affects Intel chips and ARM processors, allowing an attacker to take control of the application, accessing all system memory, including memory allocated for the kernel.

Meltdown exploits a race condition, inherent in the design of many modern CPUs using out-of-order/dynamic execution. Out-of-order execution is a performance feature in many modern, high performance processors that allow the processors to execute based on input and execution cycles rather than in a linear manner dictated by the code and was implemented to overcome latencies in older processors.

Race conditions occur between memory access and privilege checking during instruction processing. Additionally, combined with a cache side-channel attack, which is very important to an attacker, Meltdown allows a process to bypass the normal privilege checks that isolate the processes from accessing data belonging to the operating system and/or other running processes. Depending on the size of data cached, the time allotted to retain the data is very high, which makes these attacks very hard to exploit. The CVSS v3 Base Score: 5.6 Medium, reason being is the attack vector is exploited locally and the attack itself is very complex. However, considering some cloud-based virtual clusters can contain hundreds or more individual instances.

Again, Meltdown fits in with side-channel attacks, and very specific knowledge is required about the target (an old IT employee) or about the target application. Meltdown is not trivial to execute, and it presents the side effects caused by out-of-order execution. An out-of-order execution allows the vulnerable CPUs to give access to an unprivileged process, where data can be extracted from the privileged kernel.

Meltdown uses exception handling or suppression to run instructions given by the user where the PC will assign a "secret value" and will allow the CPU to store physical memory.

Meltdown can be broken into three steps:

Step 1

Read the value secret and define how to load the data using a virtual address and translating it into a physical address. The CPU will also check the permission(s) bits of the virtual address, whether the virtual address is accessible.

Step 2

Transmit the secret quietly on the network and then use the instruction classification(s) from Step 1 which is “executed out-of-order” and must be used in a way that it becomes transparent. Also note, the offshoots differ from the original Meltdown in that they are two core attacks as they use two CPU cores against each other and leverage the way memory is accessed in multi-core systems.

Step 3

The attacker can use Prime Plus Probe (contains attacker address) or Flush Plus Reload (shares address from cache) to determine the accessed cache line and hence the secret stored at the chosen memory location, and by repeating these stages for different memory locations, the attacker can dump the kernel memory, including the entire physical memory.

Example Code for Attack:

```
WCHAR gdk_keysym_to_unicode(gkeysym
Input) {
if (IsUpper(Input)) {
return gkeysym2unicode_UpperCase(Input);
}
else {
return gkeysym2unicode_LowerCase(Input);
}
}
```

Meanwhile, Spectre (CVE-2017-5753 & CVE-2017-5715), which is a close relative to Meltdown, impacts Intel, AMD, and ARM CPUs by calculating branch prediction and speculative execution, resulting in a data leak from compromised processes. Spectre is perpendicular to Meltdown, which exploits CPUs to allow out-of-order execution of user instructions to read kernel memory. Spectre permits an attacker to bypass additional application(s) to access random portions of its memory, and the exploit occurs with a read through on those applications. Mitigation will require microcode updates to fully mitigate, in addition to software patches. The CVSS v3 Base Score: 5.6 Medium, reason being is the attack vector is exploited locally and the attack itself is very complex.

Spectre emulates a hypothetical "secret value" which it needs to execute specific instructions to leak the passwords that are still being stored in "cache" from the victim process. Spectre lacks the privilege escalation characteristic of Meltdown and requires manipulating the victim process's software environment. The Spectre exploit involves encouraging someone to perform processes that would not normally occur during the execution of a program being attacked and which leak the victim's data via a side channel attack.

So, we avoid confusion, Spectre occurs when an attacker manipulates the processor into executing instructions sequences that should not have executed normally during the program execution.

During the Spectre Exploit, the attacker begins by locating a sequence of instructions within the process that when performed will act as a "secret" transmitter leaking the victim's memory. After this sequence is performed, the attacker will then attempt to trick the CPU into executing an instruction sent by the attacker. If all goes well for the attacker, "secret" data can be obtained.

Like Meltdown, Spectre can be broken into three steps as well:

Step 1

For Spectre to be successfully exploited, the attacker needs to be patient, because the attacker will need to ping the vulnerable device and begin sending malicious instructions to the processor. This is the most important step in the attack as the attacker will need to perform memory reads to determine the destination of the attack on the victim's device.

Again, as in Meltdown, the attacker will need to set up a side channel, which will be used to steal the victim's information.

Step 2

Now the processor will execute instructions, so that data can be transferred. This happens when an attacker tricks a victim into performing an action they normally would not.

Step 3

Now the attacker needs to recover the compromised data, and they do this by using flush plus reload or evict plus reload.

There are a few ways to exploit the vulnerability; here is an example of Spectre using code. We'll cover one of them here, using a JavaScript program that successfully reads data from the address space of the browser process running it.

Exploiting the Speculative Execution feature: Speculative Execution consists of a chip's logic trying to preemptively calculate multiple branches of code to precompute possible code branch outcomes. The chip will attempt to recognize a local program involving multiple logical branches, where the device(s) will begin attempting to calculate the algorithms for all the branches even before a program itself decides between them. For instance, IF statements can be used to trick the program- If ABC is true, compute XYZ; if ABC is false, compute 123, while doing so the chip will start calculating both functions XYZ and 123 at the same time, before the chip knows whether ABC is true or false. Note that this attack uses side channel, which then can be used to extract the "secret information" from devices such as PCs, laptops and mobile phones. These types of devices face further threats that do not require external devices due to the attacker executing code from who knows where. There are some software-based attacks as well here. So, exploit the software for vulnerabilities under OWASP guidelines to auditing software, such as a buffer overflow, and/or use after free vulnerabilities.

Here is an example, "in the wild Java Script", that could potentially exploit Spectre:

```
1. if (index < simpleByteArray.length) {
2. index = simpleByteArray[index | 0];
3. index = (((index * TABLE1_STRIDE)|0) & (TABLE1_BYTES-1))|0;
4. localJunk ^= probeTable[index|0]|0;
5. }
```

--Disclaimer: We did not write this script, and the script can be found on numerous websites. –

Mitigation:

Affected users with hardware susceptible to Meltdown should install the software patches that have been issued by Microsoft, Apple, Linux, etc. These patches are now readily available for Meltdown. The Linux patch is known as kernel page-table isolation (KPTI), and KPTI restores the security assumption about kernel/user memory isolation, preventing the processor from reading anything sensitive. Bottom line, for a device to be considered secure, that device must protect its memory.

Microsoft issued a critical out-of-band security update to mitigate one of the two Spectre CPU vulnerabilities, CVE-2017-5715: Branch Target Injection, for Windows 7, 8.1, 10, Server 2008 R2 and Server 2012 R2. Additionally, more information, including download instructions, can be found on Microsoft's web site at KB4078130: Update to disable mitigation against Spectre, Variant 2. ESET's software is not affected by this update, and we recommend affected users follow guidance from Microsoft and other operating system vendors in applying patches for the Meltdown and Spectre CPU vulnerabilities. @ https://www.welivesecurity.com/2018/01/05/meltdown-spectre-cpu-vulnerabilities/

A Tale of Two Worlds: Integrating Automated Mainframe Vulnerability Scanning into a Global Bank's Penetration Testing Methodology [Case Study]

Ray Overby

Ray Overby is the Founder and President of Key Resources, Inc., (KRI), a software and security services firm specializing in mainframe security. A recognized world authority in mainframe security, risk and compliance for IBM z System environments, Ray's 35+ years of experience in Enterprise z Systems, in both hands-on technical and strategic roles, along with his multidimensional and solutions-driven approach, assures he is highly valued by clients. He has been published in both business and computer journals and provides training seminars on mainframe security vulnerability assessments.

This Case Study focuses on the integration of mainframe vulnerability data into the overall risk assessment reports managed by a bank's Penetration Testing team. Increasingly, mainframe operations teams at large institutions are looking to shift the responsibility for overseeing mainframe vulnerability management to the penetration testing and risk management teams.

A PCI Audit

A set of mainframe systems programmers had been performing automated mainframe vulnerability assessments at a large multi-national bank for several years. Then came a comprehensive PCI audit. Based on the results from the PCI audit, the Operations Director stated that his team had reached a point where they could no longer be held responsible for the results from the vulnerability scanning of the mainframe and requested that the corporate Penetration Testing team take over the responsibility.

"We never even thought we could have vulnerabilities on the mainframe, but once we began automated scanning, we found the volume and the severity to be much greater than anticipated," said the bank's CISO.

The bank's IT management understood that the individuals responsible for mainframe PCI compliance were running up against an industry-wide problem; mainframe security patches and vulnerabilities are not widely communicated by vendors and do not have CVSS scores associated with them. This is a problem because PCI requires businesses to evaluate and rate the risks involved with vendors' patches and security updates. Some vendors provide a database of integrity and security patches to apply, but there's usually no description of what those patches will fix nor a CVSS score – there's not enough information to accurately assign a risk ranking. Organizations are left with a few imperfect options. They can blindly trust vendors that the patch won't adversely impact their systems, spend valuable time regressing the code to figure out what the integrity fix actually does, or simply not apply the patch or upgrade. If updates are corrupted, they can create operational issues like lengthy downtimes, which spells disaster for an organization. Also, the organizations operational teams might ignore a security update because they're just not sure what it's protecting against or whether it's worth the risk.

Integrating Two Disparate Processes

The bank's IT management knew that the only way to break down the silos between their enterprise operations and penetration testing teams and respond to the PCI Audit results was through an integrated and automated process that took the vulnerability scanning results from all of the operational and technology layers and created consistent, automated reports.

The problem: Not only did everyone on the Penetration Testing team only know network and PC penetration testing methodologies, no one understood the issues with building mainframe vulnerability risk rankings and why analytics–driven reporting was necessary to analyze and score the vulnerabilities found on the mainframe. Also, a primary challenge they faced in shifting this process was the education of the penetration testers on mainframe language and scheduling processes.

A task force was formed to determine the best approach to integrate their penetration testing processes with the mainframe vulnerability scanning processes, keeping PCI reg's in mind.

Being tasked with overseeing mainframe vulnerability management was daunting to the Penetration Testing team. Applying PCI to the mainframe requires a specialized set of skills – one that takes a long time to perfect. PCI requires a deep technical understanding of platforms and their security systems. Most internal security specialists, auditors, and CIOs are now coming from distributed systems expertise and not mainframe expertise. The average person coming from a distributed network background finds the complexity of the Enterprise Security Managers on the mainframe overwhelming. Most external auditors and penetration testers don't have a background in mainframe security and thus don't know how to exploit even the simplest vulnerability.

How does a PCI penetration test differ from a vulnerability scan?

The differences between penetration testing and vulnerability scanning, as required by PCI DSS, still causes confusion within the industry. The differences are summarized as follows in the PCI Data Security Standard (PCI DSS) Version: 1.0, Dated March 2015.

	VULNERABILITY SCANNING	PENETRATION TESTING
Purpose	Identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.	Identify ways to exploit known vulnerabilities to circumvent or defeat the security features of system components.
When	At least quarterly or after significant changes.	At least annually and upon significant changes.
How	Typically, a variety of automated tools combined with manual verification of identified issues.	A process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.
Reports	Potential risks posed by known vulnerabilities, ranked in accordance with NVD/ CVSS base scores associated with each vulnerability. Note that external vulnerability scans must be performed by an ASV and the risks ranked in accordance with the CVSS. Internal vulnerability scans may be performed by qualified personnel (does not require an ASV) and risks ranked in accordance with the organization's risk-ranking process as defined in PCI DSS Requirement 6.1. An external vulnerability scan is conducted from outside the target organization. An internal vulnerability scan is conducted from inside the target organization.	Description of each vulnerability verified and/or potential issue discovered. More specific risks that vulnerability may pose, including specific methods how and to what extent it may be exploited. Examples of vulnerabilities include but are not limited to SQL injection, privilege escalation, cross-site scripting, or deprecated protocols.
Duration	Relatively short amount of time, typically several seconds to several minutes per scanned program.	Engagements may last days or weeks depending on the scope of the test and size of the environment to be tested. Tests may grow in time and complexity if efforts uncover additional scope.

Integrated into Risk Management Process

Despite their network-based background, the bank's Penetration Testing team is now capable of running automated mainframe vulnerability checks, fully assuming responsibility for scanning of the firm's mainframe systems for vulnerabilities and using the reported results as part of the consolidated risk report, which automatically assigns the appropriate risk ranking and builds a corporate wide mitigation plan. All of the technology platforms are covered in one risk ranking report. This analytics–driven automation was needed to analyze **ALL** vulnerabilities in the complete context of their attack surface and meet the PCI requirement that businesses evaluate and rate the risks involved with vendors' patches and security updates.

"*The integration process was easier than we originally thought,*" said the bank CIO. "*There were some bumps along the way, but overall it proceeded very smoothly, and our audit team couldn't be happier with the results.*"

Once both teams came to agree that mainframe scanning responsibilities were better off centralized with the Penetration Testing team, they met with the bank's CISO to determine the challenges and frictions in migrating these responsibilities from one team to the next and identified what they needed in order to build out a mainframe education program for the penetration testers. The first step in integrating the mainframe and penetration testing methodologies together was to find mainframe systems programmers who wanted to work with and train the penetration testing team members. Training covered both mainframe operating system fundamentals, as well as specific vulnerability testing procedures and mitigation processes.

The Penetration Testing team learned how to utilize the analytics–driven data and CVSS scoring that was being generated by the mainframe scanning software and reported in a Vulnerability Analysis Report. The data was extracted from the XML generated by the mainframe software and incorporated into a consolidated risk report (including distributed and mainframe CVSS scores) and ranked in accordance with the organization's risk-ranking process as defined in PCI DSS Requirement 6.1. Also, the bank solution now met PCI Testing Procedure 11.2.1 *"Perform quarterly internal vulnerability scans and rescan as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scan must be performed by qualified personnel."*

The Software

The mainframe scanning software uses the CVSS methodology to rank identified system integrity vulnerabilities. The CVSS ranking is based upon a proprietary algorithm using Impact and Exploitability metrics.

Code vulnerabilities caused by poor coding techniques exist in every z/OS system and the External Security Manager's (ESM) can do nothing to protect a mainframe once a hacker has exploited a vulnerability to elevate their privileges to authorized access. Code vulnerability exploits are especially damaging; a single attack could compromise all of the data, while also crashing the system itself.

The mainframe scanning software operates on the principles of Interactive Application Security Testing (IAST) and is an innovative new approach to automated security testing. The methodology allows for real-time, automated scanning of binaries and is 99.9% accurate. By building and improving on traditional testing approaches, this approach to scanning not only identifies code, but points to the exact offset in the code where the vulnerabilities exist.

The scanning software is also significantly more efficient than traditional scanning methods, making it a perfect fit for fast-paced development and corporate environments. With traditional, manual testing methods, security experts might perform a manual scan once a year on predetermined dates.

A READ level mainframe code vulnerability is defined as a vulnerability that, when exploited, will completely comprise some or all memory on your system. It is common practice to place sensitive data into fetch protected memory. Data placed into fetch protected memory includes clear text passwords, encryption keys, and other similar sensitive data. This sensitive data could also include installation defined sensitive data. Severe security code based READ level vulnerabilities will typically score at least 7.0 or higher using the CVSS V3 calculator.

ON THE WIRE:

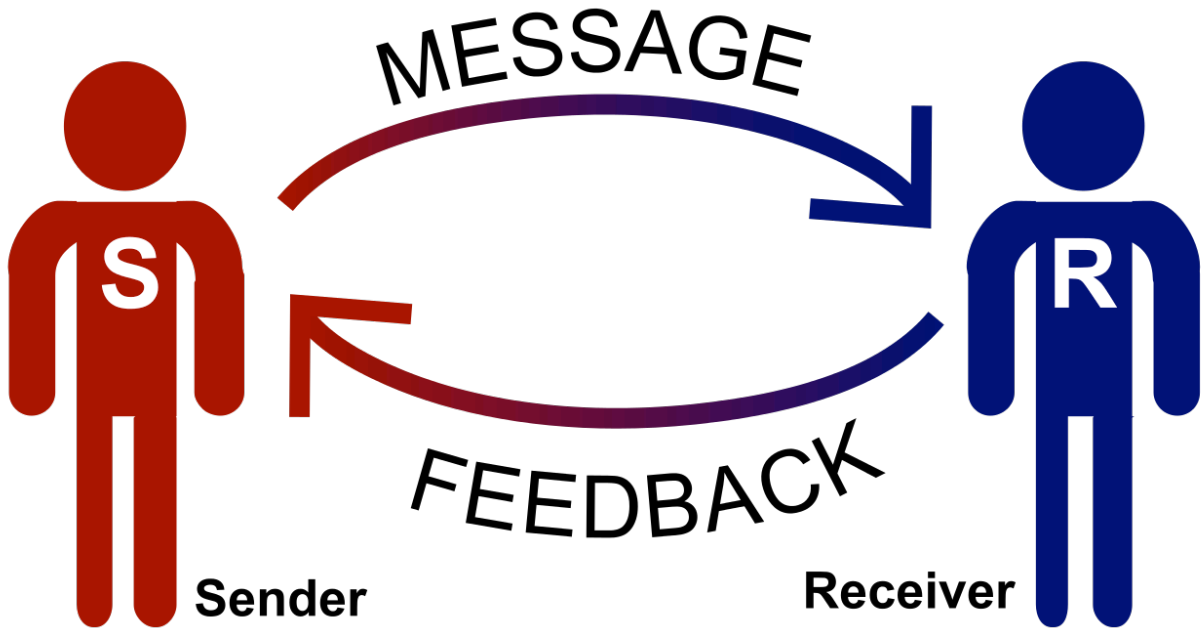
Securing The Spectrum Across Various Media

Robert Brooks Authement

Robert Brooks Authement is the owner and operator of BRIQ| HAUS LTD. Security & Intelligence. Interest in hacking led to interest in electronic warfare, militaries, and government. After a tour to Washington DC where he was provided some on-site training and witnessed two large scale protests, Robert's vision for success with his private sector security firm, Briq Haus Ltd., can only be augmented by the inclusion of his material in PenTest Magazine.

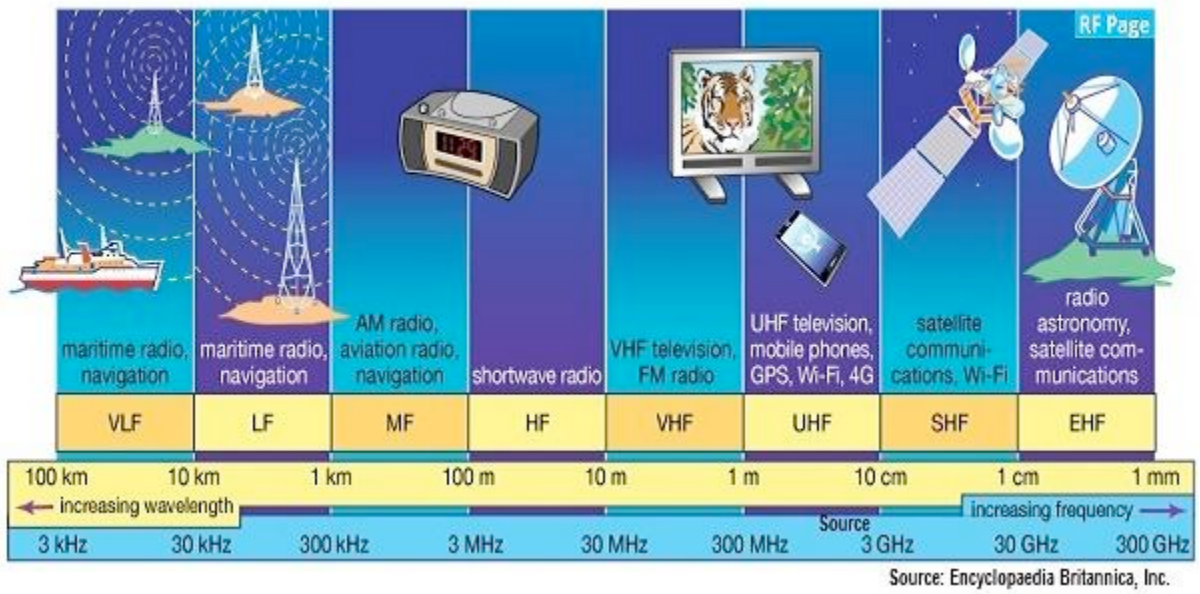
A quick Google search will yield incredible amounts of comparative information between wired and wireless technologies, so much so that the waters are immediately muddied by the countless applications to consider when devising a security strategy. There must a way to reduce the *signal to noise ratio* in discerning the best plan for securing your communications and operations. That is what we aim to do here today, by reducing the noise and focusing on the solid signals emitted by some of the higher likelihood probable technologies you may use specifically in modern deployment for your computer network, communications framework, or broadcast platform.

Communication Principle



Notwithstanding basic knowledge, a communication principle describes the process by which a message is sent from one source, received by another source, and in this transition the original meaning of the sender is transmitted as clearly as possible and interpreted correctly by the receiver. In the diagram above, we may see the sender and receiver not represented by human stick figures, but by radio and electrical charts describing antennae, modulators, transmitters and receivers. The same principle is applied to satellites in space and dish receivers at base stations on the surface of the planet, or even to radio repeaters placed on high peaks to extend *line of sight* in radio transmissions. As you can tell by these few examples, the field becomes complicated very quickly, and the number of technologies employing a communication principle, either by **wired** or **wireless** means, is astronomical.

For the human range of visible light, we are observing only a fractional piece of the entire energy spectrum. To be precise, visible light makes up approximately .18% of the energy spectrum, which is to say one fifth of one percent of the available energy being emitted from stars. There is a lot going on above and below that tiny band of technicolor brilliance. Just outside of the visible light spectrum at the low end we have **infrared** or heat-vision, which is used by snakes and moths to find food sources and potential mates. Above the visible band is **ultraviolet,** which bees use to see their paths to and from the hive and sources of nectar. In early days, what people may have called *supernatural* turned out to be entirely natural methods described and repeatable by scientific means. Just because you can't see it, doesn't mean that it isn't there!



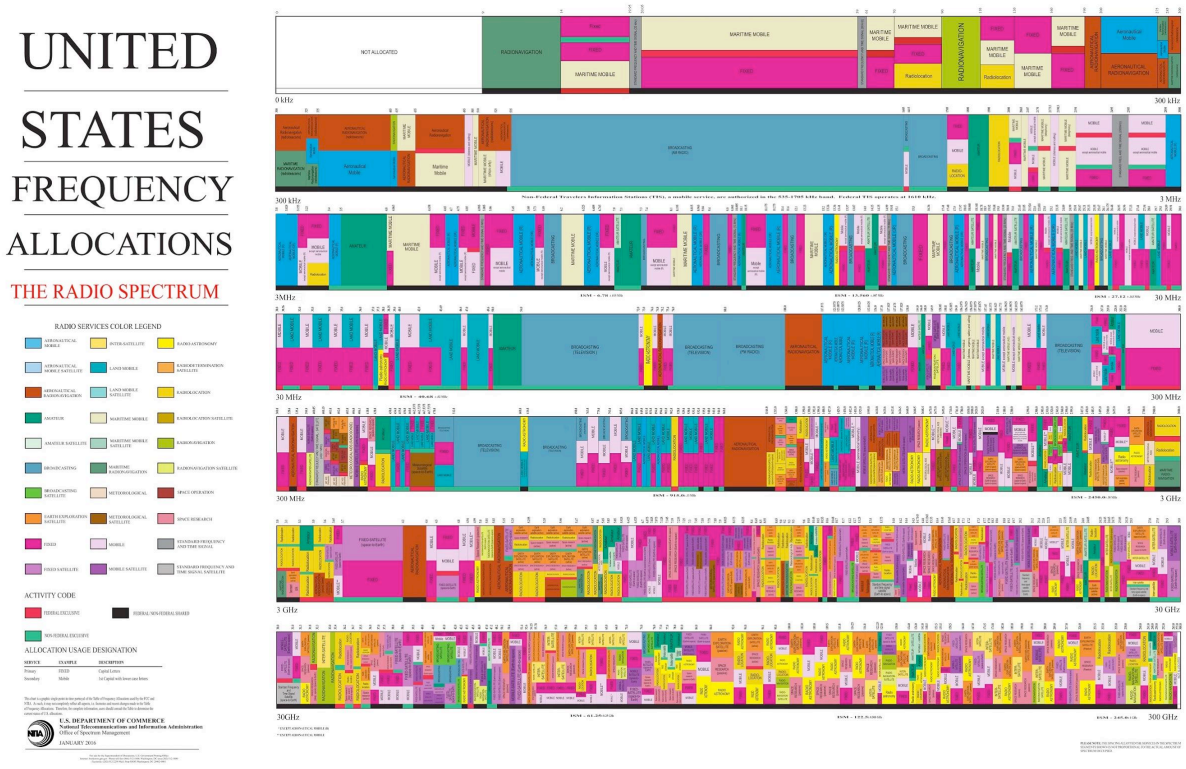
Similarly we can see, in the diagram above demonstrating exclusively wireless transmission technologies, that there are a wide variety of applications. Maritime navigation radio can use a lower frequency because of their method of travel and medium of transmission. For example, submarine sonar technology easily uses only a sonic signal (the sound of a *ping*) to echolocate their position in relation to the seascape below, and to locate other vessels in the water. Water is supremely conducive to sound, therefore sound was an excellent wireless technology to be used for submarines. Later in this article is a fascinating story about security in regard to submarine technology.

Up the spectrum, starting in the low frequency to high frequency range, we have the traditional standard radio technologies with which consumers are most familiar. AM and FM radio, used by car radios for music and news transmission utilize signal repeaters and scanning technology that aids the receiver in tuning into the strongest signal source for clear reception and audio. It is not unfamiliar to hear static electricity as snaps and pops on the car radio while driving in a thunderstorm, as the antenna is picking up the electromagnetic spray from errant lightning bolts, which creates a noise in the reception. This is the beginning of a concept in security, but more on that later.

VHF and UHF, or very high frequency and ultra high frequency, are used for television transmission and for modern cell phone radio signals. These are propagated by fiber fed base stations that are placed in a grid to cover as much area as possible, thereby granting customer subscribers ubiquitous access to cell phone and data coverage. For a while, before the cell phone providers were well established, one of the competing points was *how much coverage* they offered. Famously, Verizon featured commercials where some innocuous nerd walks about asking, "Can you hear me *now*?" The statistic for cell phone coverage from one provider or another and available access to US citizens is 99%, but many

parts of the world and developing nations in whatever stage may not boast such prolific technologies. Startups and ventures abound in the lands of opportunity, which similarly creates a demand for securing these operations.

Beyond these frequencies are space communications, such as satellite relay and electromagnetic telescopy. These systems are highly sensitive, and can detect very minute signals propagating through the vacuum of space. There are many, numerous and varied technologies used by commerce, consumer, government, and military users. The following chart conveys the mind-numbing vastness of applications being used in the United States spectrum.



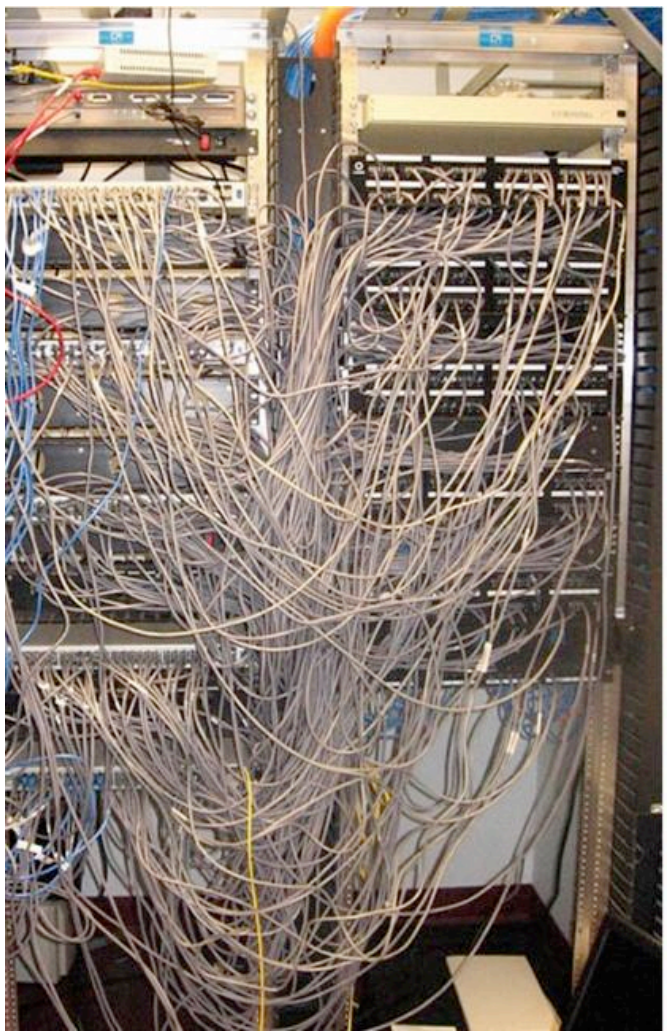
Wired VS. Wireless

The Communication Principle describes how a signal or message is sent from one source to a receiver. This signal can be spoken words, such as sound passing through the air as compression, radio signals, as briefly introduced above, or even the electricity traveling through wires in the utility grid. True to form, the electrical grid has many of the same terms and operational concepts as radio transmission, but with some simplification. In a wired system, we can always see that the information travels from one point of origination to the connected point of reception. For purposes of security, this is a great boon. Well, to be honest, there are pros and cons of each. Let's look at these in more detail.

Specifications	Wired network	Wireless network
pace of operation	Higher	lower compare to stressed networks, but advanced Wi-Fi technologies inclusive of lte, lte-a and wlan-11ad will make it feasible to acquire pace par equal to wired community
System Bandwidth	High	low, as frequency spectrum may be very scares aid
Cost	Less as cables are not expensive	more as Wi-Fi subscriber stations, Wi-Fi routers, Wi-Fi get right of entry to factors and adapters are steeply-priced
Installation	stressed out community set up is cumbersome and it calls for greater time	Wireless network installation is easy and it requires less time
Mobility	Limited, as it operates in the area covered by connected systems with the wired network	now not constrained, as it operates within the complete Wi-Fi community coverage
Transmission medium	transmission medium copper wires, optical fiber cables, Ethernet	Electromagnetic waves or radio waves or infrared
Network coverage extension	calls for hubs and switches for community coverage limit extension	Greater region is included by Wi-Fi base stations which can be related to one another.
Applications	lan (Ethernet), guy	wlan, wpan(ZigBee, Bluetooth), infrared, cell(gsm,cdma, lte)
channel interference and sign strength loss	interference is less as one stressed community will not have an effect on the other	Interference is higher because of boundaries among Wi-Fi transmitter and receiver e.g. climate situations, mirrored image from walls, and so on.
QoS (Quality of Service)	Better	terrible due to excessive value of jitter and postpone in connection setup
reliability	High evaluate to Wi-Fi counterpart, as synthetic cables have higher overall performance due to lifestyles of stressed technology in view that years.	Reasonably high, that is because of failure of router will have an effect on the whole network.

Wired technologies have some risks. For example, copper wire theft in the United States, according to a Department Of Energy report from 2008, is costing figures to the tune of $1 billion annually! Not only is this a high cost of loss for corporations and providers, but it creates risk at the work site where nefarious scavengers and tweaker scrappers will trespass and burglarize bundles of copper wire and other copper applications such as drain pipes and grounding wires off towers. Therefore, implementing a wired system may be cheaper in terms of project estimation, but leaving copper around may require more investment in protecting the site against copper thieves! In my own opinion, as a field security researcher, corporations and policy makers frequently overlook or ignore real-world risk of this caliber. It is on them when things grow legs and go missing, affecting their bottom line. Don’t be like them; have a plan for protecting your critical infrastructure and valuable materials.

Insulated wire runs very little risk of signal interception or hacking. Underground wire is the most secure, and, of course, most costly in terms of expenditure and infrastructural displacement, but once it's underground, it is highly unlikely that someone will cut the line or splice into it without drawing overt attention to their crime. However, we also see, as in the case of the amateur data-center operator, sometimes what you end up with is *wire-spaghetti* or just a massive mess and jumble of wires and cables everywhere. This can be frustrating and confusing and become contra-progressive when a clear connection scheme is not specified.



Now let's be honest about the risks. I love to reference the tale of Operation Ivy Bells. This was a combined effort between the US Navy, NSA, and CIA. A sort of early *phreaking* device had been designed that could read the signals being emitted from submarine communication cables operated by the Soviets. A US submarine deployed the device in 1971, which sort of fit around the cables and read the signal through the insulation. Of course back then, divers were required to revisit the site (extremely classified) to retrieve the tapes from the recordings and replace them with new reels. It turns out that the Soviets did not encrypt (or scramble) their communications, being overconfident in their cable's secrecy. This breach of Soviet security went on unabated for nine years, and demonstrates how even a secured end-to-end communication system can still be hacked by plucky hostile foreign intelligence.

Contrary to the operation, would you believe an American NSA agent, Robert Pelton, because of $65,000 debt, accepted payment of $35,000 from the Russian KGB to reveal the secrets of Operation Ivy Bells. In 1981, American surveillance satellites saw a grouping of Soviet ships and a salvage vessel anchored above the site of their submarine tap. When they returned to change the tapes, lo and behold, the device was missing, claimed by the Soviet salvage team. The device would later be proudly displayed at the Great Patriotic War museum in Moscow. Quite a trophy, and perhaps the only means by which to prove how realistically desperate counter-operating opposing forces will become in the heat of war time. The same goes for competitive firms and criminal elements. People will stop at nothing to breach your security.

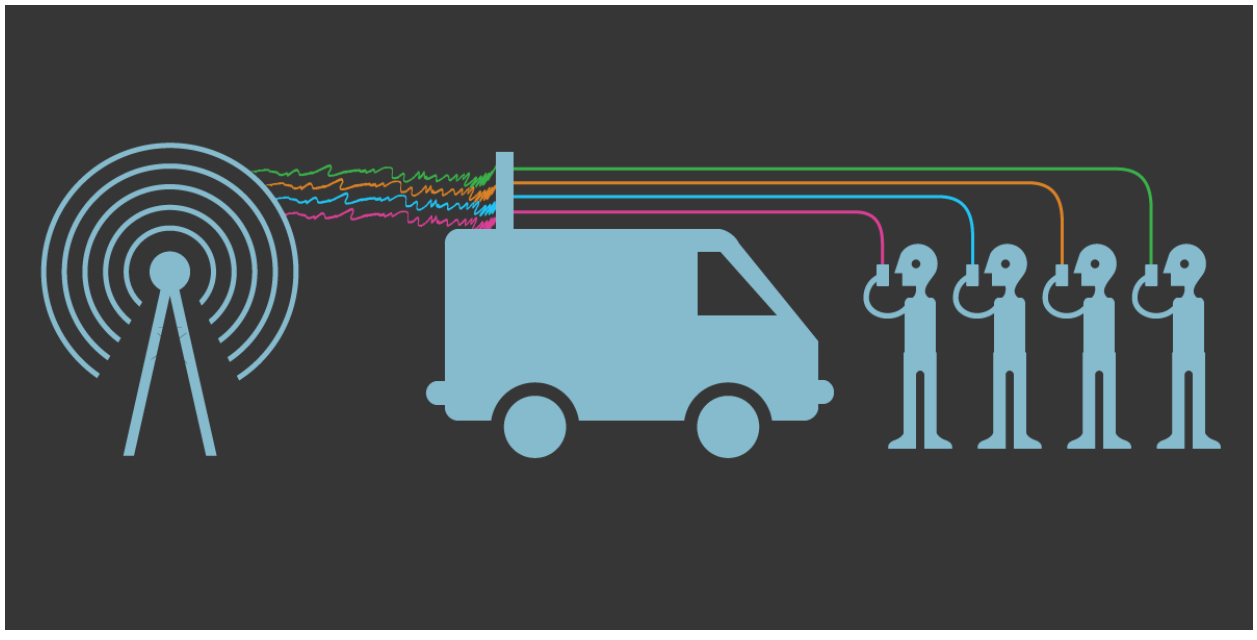
Wireless technology, and specifically digital technology, offers a lot more risks in terms of signal interception. Is convenience and mobility enhanced by wireless and radio technologies? Yes, of course, one hundred percent! The propagation of waves and signals creates more issues due to the fact that anyone could set up a base station with a transceiver to intercept, alter, and rebroadcast the radio signal. This is the basic principle behind the absolute *most effectively devastating* and successfully implemented hack of all time: **The Byzantine Attack**. It is best considered that

in the heat of ancient naval conflict, a lone pirate could blow the horn signalling to the opposing team that she or he was the admiral, and for all ships to follow! These bogus orders would be ignorantly obeyed by the fleet, not realizing they had been bamboozled. To this day, this attack works perfectly and if you don't believe me, run an instance of Ettercap at a public wifi spot. You'll see just how easy it is to launch a man-in-the-middle attack.

So encryption becomes necessary. Of course, in the case of our misfortunate (and then later more fortunate) Soviet friends, not encrypting even their *wired* system led to a breach. With radio and wireless technologies, *anything and everything* not being encrypted end-to-end can be sniffed remotely and read aloud in cleartext. In terms of operational security for radios and walkies, it would be required to have sets that do the encryption from hand-held to hand-held. The principle of computer science as we know it today arose from the need to encrypt and decipher coded messages during World War II. I can not stress enough the vital necessity of strong encryption for your operations, whether they be from disk to disk, wire to wire, or transmitter to receiver. If you want any security, then you need some encryption.

Security Implications

There are some means of guarding against traffic hijacking sniffers and hackers, however. Beam or burst transmissions are used to send a brief and highly compressed signal in direct line of sight from a narrow transmission point to a specific receiver. These are employed by militaries and space technologies, and are on the whole the absolute most secure. FHSS, or Frequency Hopping Spread Spectrum, was developed long ago in 1941 by an Austrian actress Hedy Lamarr and George Antheil. It was utilized to prevent signal discovery, deciphering, or jamming. In effect, by rapidly changing the radio frequency of the signal, a hacker or man-in-the-middle has a difficult time of capturing and then altering the transmission. Even to this day some top class wireless data radios are used in secure data transmission of various utility applications. Industrially hardened radios are required for security in operational communications for data transmission and distribution automation.



Aside from our reference to running Ettercap at public wifi spots, which was surreptitiously discovered to not work in Starbucks locations due to their implementation of client-side isolation in their router (which you should never, ever do because, well reasons), there are other real-world specific instances of wireless hacking, which is actually still a fairly hot topic in privacy advocacy groups. The Stingray cell phone surveillance system is a particularly nasty technology deployed by agencies and law enforcement, which basically eliminates any semblance of secure communication or privacy for a consumer level user. As we see in the simple diagram above, which basically depicts the exact concept of a man-in-the-middle or Byzantine Attack, the officer or operator in the van is capturing the signal from the source transmitter, rebroadcasting the transmitter's cell ID, and capturing the IMSI (international mobile subscriber identity), and thereby relaying all traffic to and from the subscriber to the cell tower. We can easily visualize the man-in-the-middle, but requiring more discernment is observing in what means this can compromise the target.

All communications can be routed to opposing force controlled operator, whose intentions are aligned with the agenda of the hacker (or in this case, police or investigative agency or bureau). The IMSI will reveal the location of the phone, and assuming the target is carrying the phone, it will reveal their physical location and proximity as well. All signals coming into and out of the phone can be captured, as in the case of an old-fashioned *wiretap*, or even worse, the signal can be altered. Therefore, apps downloaded can by augmented trojans or RATs (remote access tools) to further escalate the privileges of the raider. The use of the Stingray technology is highly contested by privacy advocates, as it well should be. The cost for the deployment of a Stingray system, I discovered from some deep delving once upon a time, is upwards of $100,000. It is, therefore, cost prohibitive except for even lucrative police forces and agencies. Let's say it this way: if your local police cannot afford to have body cameras, they cannot afford a Stingray system. It is likely, as time goes on, this may in fact change.

Other wireless technologies, such as the radio for drones and even Bluetooth technology, are all vulnerable to the man-in-the-middle attack. Wired technologies are also vulnerable, but far less so. Which is better? You alone can decide which technology to deploy in your operation. My only recommendation is to bear in mind, a penny invested in security may yield a vast return in stopped loss and thwarting or otherwise preventing sensitive asset hijack. If you got wires, keep them neat, survey and guard your work site, and protect your infrastructure by burying the installation if possible. If you use wireless, make sure you get yourself some industrially hardened radio equipment and similarly protect your end-nodes. In both cases, use a strong encryption protocol with as many bits as your bandwidth and processing can handle. Be safe, be strong, and always be faster than the opposing force.

As a final note, something also of some dispute and debate can finally be put to rest by this statement by the ***National Center For Biotechnology Information****:* The results of this study and International Commission of Non Ionization Radiation Protection (ICNIRP) reports showed the people who spend more than 50 minutes a day using a cell phone could have early dementia or other thermal damage due to the burning of glucose in the brain. *This is not to mention the necessity of guarding* ***AGAINST*** *unwanted or hostile radio transmissions. Describing the ways in which radio technology is used offensively, especially against biological or neurological systems, and the means by which to protect oneself and operations against these styles of attacks, are beyond the scope of this article.*

References:

I.) Internet Backbone - https://en.wikipedia.org/wiki/Internet_backbone

II.) Bluetooth - https://en.wikipedia.org/wiki/Bluetooth

III.) Wired VS. Wireless Technologies For Communication Networks In Utility Markets - https://www.utilityproducts.com/articles/print/volume-16/issue-04/product-focus/transmission-distribution/wired-vs-wireless-technologies-for-communication-networks-in-utility-markets.html

IV.) Signal To Noice Ratio - https://en.wikipedia.org/wiki/Signal-to-noise_ratio

V.) Operation Ivy Bells - https://en.wikipedia.org/wiki/Operation_Ivy_Bells

VI.) Stingray Phone Tracker - https://en.wikipedia.org/wiki/Stingray_phone_tracker

VII.) Effect Of Ultra High Frequency Mobile Phone Radiation On Human Health - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4930268/

VIII.) Basic Radio Awareness - https://www.taitradioacademy.com/topic/digital-vs-analog-radio-1/

Common flaws within session management

Alex Archondakis

Alex is a Penetration Tester, security blogger and public speaker. His cyber security skills were originally self-taught and he currently works with various technologies, whilst mainly focusing on Web Application and External Infrastructure testing.

Idle timeout is often not set on an application which increases the chance of both a skilled hacker and an opportunist hacker gaining access to a user's account; this could be through a user leaving their account logged in on a public computing environment, like a library. Session management vulnerabilities mixed together can lead to critical flaws within an application.

Web applications have quickly integrated their way into our daily lives with over a billion websites published to date with this number quickly increasing. We use web applications to keep in contact with our friends, pay our bills and host our family photos but how do these applications keep track of who is who and how do they stop other people accessing our information?

Weak authentication and session management is number two on the OWASP top ten vulnerability list in 2017. In this article, we will be looking at some of the most common flaws within the session management of an application, how a hacker would exploit them and what impact they can have on your business.

Session management defines the exchange between the user and web application to regularly share the session ID to keep the session alive. There are many mechanisms available to keep a session state but we will be focusing on the use of session cookies.

Session cookies are set upon visiting an application and then an authenticated cookie is set upon logging in. They are used to keep the user logged in and identify them. Developers often do not implement the correct attributes and management to properly secure the session cookies and stop them being stolen by an attacker. If an attacker is able to successfully steal a valid session cookie, they can replay them and gain control of the user's session.

When an authenticated session cookie is set, it should have the secure and HTTPOnly attributes implemented into the cookie. The secure attribute is set by the server when sending a new cookie; its purpose is to stop cookies being observed by third-parties when being sent over an unencrypted transmission (HTTP) by only allowing the cookie to be sent to a secure page (HTTPS). The below example shows a session cookie set with secure, path and HTTPOnly.

```
HTTP/1.1 200 OK
Server: Apache
Set-Cookie:  PHPSESSID=39f7akdsjfkfnvbnodskkfngklvdb68; Path=/; secure; HttpOnly
```

The HTTPOnly flag is set to prevent client-side script attacks accessing the session cookie. If cross-site scripting flaws existed within an application and a user was tricked into exploiting this flaw, the browser would not reveal the session cookie.

Session cookies should be properly invalidated both client and server side when a user logs out of an application, otherwise, if an attacker were able to gain access to the user's session cookie, they would be able to easily replay it and gain full access to that account, from here the attacker could potentially change the email address to their own and request a new password resulting in account compromise and denial of service to the legitimate user. The impact of this is variable dependent on the privilege levels of the compromised account.

As discussed earlier in the article, usually a session cookie is set when visiting an application and then another authenticated session cookie is set when logging in, this is security best practice, however, sometimes developers use the same cookie for both unauthenticated and authenticated session management, this is called session fixation. This makes stealing a session ID a lot easier for an attacker.

Idle timeout is often not set on an application which increases the chance of both a skilled hacker and an opportunist hacker gaining access to a user's account; this could be through a user leaving their account logged in on a public computing environment, like a library.

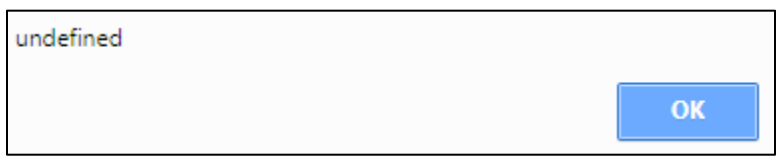
Session management vulnerabilities mixed together can lead to critical flaws within an application; let's take the following scenario from a real test:

The attacker is able to exploit a stored cross-site scripting vulnerability within the application by injecting malicious JavaScript into a comment box, any user that views these comments will trigger the JavaScript. The application does not enforce the HTTPOnly attribute on the session cookie and has not enforced idle timeout and the session cookie is not deleted properly after logout. Below is an example of a cookie set without HTTPOnly, path or secure.

```
HTTP/1.1 200 OK
Server: Apache
Set-Cookie:  PHPSESSID=39f7akdsjfkfnvbnodskkfngklvdb68;
```

So, the attacker is now able to steal any user's session cookie after they visit the comment box and replay it to hijack the user's session. This will be valid indefinitely as the cookie is not deleted when the user logs out nor is there any timeout policy. Below is a proof of concept by using the command <script>alert(document.cookie</script> to trigger an alert box with the victim's sessionID, not that an attacker would be able to craft malicious code to send the session ID back to them.

If the HTTPOnly flag is set on the cookie, we will get the following response when trying to execute this command:



Now, the attacker has got complete account compromise on many user accounts and could change the user's password, email address and perform any actions that are permitted within the hijacked account's privileges.

Changing the password and/or email address would lead to a denial-of-service for the user as they will no longer be able to access their account, which would result in loss of reputation for the company that owns the application.

An attacker, performing actions on a user's behalf, could exploit the trust relationship between users and trick others into clicking on links that contain malicious code or redirecting them to phishing pages.

Q&A Session With Cybersecurity Expert: Jigar Thakkar

Could you quickly introduce yourself to our readers?

I'm Jigar Thakkar, a SecurityResearcher protecting companies' data from malicious hackers, a full time bug bountyhunter on different platforms like HackerOne (19th rank with 9100+ reputation points, best in the world of all time.), BugCrowd and also an active member of Synack RED Team.

You have graduated not a long time ago. Do you miss the student life sometimes?

Of course not, because this subject - "cyber security" - is fun for me. I always want to know about the different kind of techniques related to hacking. Normally, I spend my free time with my laptop only.

Do you think that studies prepared you well for the cybersecurity market?

The answer is "yes", but partially. If you are not familiar with the coding and other programming language stuff then still you will be able to do the hacking. Because apart from this there are several things that you have to focus on during the security testing, Like If you are good with logical things then you will be able to bypass the business logic issues. This type of issue does not need any study. We have to learn this from our own experience. But, of course, if you studied well, then this will definitely help you to think beyond into any application to find high security vulnerabilities.

Did you take part in any projects during studies? If yes, do you consider such activity important?

Actually, no, I did not take part in any projects during my studies. I was an independent security researcher at that time and I was looking for the vulnerabilities for the big companies like Facebook, Google, Microsoft and all.

Did you start your career during your studies or did you decide to focus on the education first? What do you think is better and why?

Actually, during my studies I knew my path was to become a security consultant. I always focus on both things. Education is also important for me. If you split your time as per your requirements, then this would be very helpful for you.

Let's move to one of the most arguing questions. Certificates - do you think they are important or not?

I would like to give the answer by yes and no both. Yes, because as we know, each and every company wants an expert and if you have the certification then a company will know that he/she must have this kind of knowledge. During the training of that certification there are several scenarios you will learn. Companies have this kind of information that if you are certified with this certification then you definitely know about this. Sometimes it is a requirement that you must have this or that certification to apply for this job. No, if you do not have any certification it's not like you are not a good security consultant. But it is very hard to prove that you are a deserving person for this job.

Cybersecurity is constantly evolving and new tools and techniques are developed everyday. How do young people keep in touch with the newest technologies? Do you have your favourite platforms to learn?

- Attend the hackers conferences, like Blackhat, Defcon, Nullcon, etc.

- Enable Google Alerts for the specific subject.

- Connect with HackerOne + https://hackerone.com/hacktivity

How about the contact network e.g. *LinkedIn*? Do you think it helps to look for new jobs and opportunities or maybe you heard of someone it helped?

Yes, of course, *LinkedIn* really helps us look for new jobs and opportunities.

Which part of the cybersecurity market is worth focusing on right now?

If I have the one word to say then its obviously "Mobile Security" because nowadays we can see the digitalization everywhere. So it's very hot subject to focus on.

Have you got any final tips for younger colleagues who are currently studying or starting their career?

To become an information security analyst as a career is a very good choice but for this, you must do 100% every day because every day you will see some new stuff. So you need to learn and understand new stuff always. This means you will always be a learner in your life if you choose this as your career. But one thing I want to say that if you really have an interest in this, then it would definitely be good fun for you.

Jigar's LinkedIn profile: https://www.linkedin.com/in/jigar-thakkar-88355053