The Datagram newsletter

August, 2017 Volume 2, No. 8

From the Chair...

A new Machine Learning (ML) web page has been added to our web site. The web page contains books, articles, research and resources centered around machine learning in the abstract and machine learning specific to cyber security.

The effort to find a clear and simple explanation of machine learning and its applications was not successful. This is our effort at an explanation.

Machine learning is the general research area which defines algorithms able to "learn." The learning is a feedback loop, commonly called "training"; given an answer, the loop returns a value that shows the extent of the difference between the output results and the expected answer. The ML then modifies its behavior. This continues iteratively.

One implementation of ML is in its use in neural nets (NN). Think of an oreo cookie. The outer chocolate wafers are the input and output to the inner "'brain." The brain's neurons are simulated. Where a neuron

Continued on page 2

Next meeting:

August 23, 2017

6:30 PM Dinner and Networking
7:00 - 8:00 PM Presentation
8:00 - 8:30 PM Q & A
8:30 - 9:00 PM Meet & Mingle

Dinner: FREE

ATEP, 15445 Lansdowne Road, Tustin, CA, Room #D106
(Room number subject to change)

Speaker: Ron Monard, Esq.

This Month's Topic: Law, Legal, Cyber, Software Technologies

In the coming years we will see advancement in automated vehicle technologies and the roll out of such cars for consumer use. Although hailed as an innovation to decrease accidents, there will be a rise of legal issues with driverless cars, beginning with the complexity of separating fault between the automated car system and the driver. Manufacturers, service providers and consumers need to ensure that they understand the legal developments around the technology in order to be prepared for the legal responsibility these vehicles could present. The law will expect the manufacturers to have invested

Continued on page 2

About the Speaker

Ron Monard is an attorney in Orange County and a professor at Webster University. He is also an Arbitrator with the Better Business Bureau settling disputes between auto manufacturers and the consumers on automotive cases involving the Lemon Law. He currently sits on the Steering Committee of the Orange County Sheriff Department's OC Shield Program which helps to foster partnering between the Sheriff's Department and key critical infrastructure entities in the county.

He is a graduate of the FBI's Citizen Academy and has been a long-standing member of the FBI's InfraGard Program. This fall he is helping Webster University laumch their new Master level and Certificate program in Cyber Security.■

Contact Information

Website: sites.ieee.org/ocs-cssig

Meetup.com/CyberSecuritySIG

Newsletter Editor:
stargazer@stargazerpub.com

From the Chair, Cont'd.

has input signals, a processing center (the "thinking" part), and output signals, where neuron accepts input from many sources and outputs to other neurons and the external world. In a similar way, our simulated neuron is connected to one or more input and output devices and to one or more other neurons. Our neurons are the ML software investigated by ML researchers.

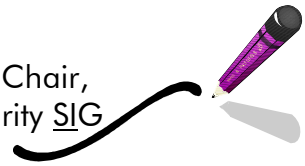
The training phase causes the neurons to adjust the weights on input signals. The input weights are adjusted on each neuron until training is complete.

Think of a directed graph. Connectivity is established by the arcs. Each arc contains some value. Nodes in the graph represent ML processing elements. The software traverses the graph, delivering arc values to each ML processing element and accepting (remembering) the generated value. Internally to the ML processing element, the weights of its inputs are adjusted, processing is done, and an output is put onto each exiting arc.

The machine learning web page contains detailed papers on the mechanics of the ML nodes and NN implementation, as well as articles which identify cybersecurity use and warnings.

Art

(reluctant) Chair,
CyberSecurity SIG



This Month's Meeting, Cont'd.

significantly in protections and will likely look to a mix of manufacturers, insurers and drivers to allocate the cost of that liability as the connected car market matures.■

July Meeting Report:

How Cyber Security is Redefining the 21st Century IoT World of Digital Health

Many people enjoy the convenience of checking their medical records online or via an app on their phones or tablets. There are over 165,000 mobile health apps, 12% of which account for 90% of all consumer downloads. Nearly half of these are generated by just 36 apps. The down side for this convenience is that 90% percent of these apps, which are projected to become a regular part of our care over the next five years, are vulnerable to critical security risks.

CyberSecurity SIG Vice-Chair Gora Datta gave a very informative presentation to a standing-room-only audience on the status of cybersecurity and the healthcare industry today. In 2004 and 2005, President George W. Bush issued executive orders requiring patients to have access to their records electronically. In 2010, companies and doctors' offices began to convert patient data to digital format. This was accomplished in three stages:

- Stage 1 – Capture coded data
- Stage 2 – Share information with other government agencies
- Stage 3 – Convert data to knowledge

Several factors are driving this change to digital information:

- Increasing global population
- Aging population
- Higher life expectancy
- Increasing number of chronic diseases
- Emergence of personalized medicine
- Global reach of diseases
- Technological advances

In 2016, the US GDP was $18.5 trillion. It is projected to rise to $23 trillion by 2022. U.S. healthcare spending is currently 18% of the GDP, or $3.3 trillion. This is expected to rise to $4.6 trillion in 2020, which will constitute 20% of the GDP. Surprisingly, out of 14 developed countries, the U.S. is ranked 13th when it comes to population health outcomes and risk factors.

These factors will cause a change in the payment model. In the 20th century, the model was fee for service, which is volume-based. In other words, payment is predicated on the number of services provided. The 21st century payment model will be pay for performance,

which is value-based. Payment will be predicated on improved health, higher quality of service/ experience, and lower cost.

The Internet of Things (IoT), which includes mobile phones, is largely responsible for this shift. By 2020, we will have an IoT-connected world, with a projected 50 billion devices being used. Young people today are used to having information instantaneously because of phones, tablets, and social media.

This has blurred the lines regarding the concept of privacy and has increased the risk of vulnerability. The online presence will rise from 2 billion people today to over 4 billion by 2020. This greatly increases the chances for cyber attacks on patient data.

People ask why any hacker would want their individual medical information. It's not that the data is valuable in and of itself. Hackers know it is valuable to the patient. They will hold the data hostage and request payment to release it. If the patient doesn't pay—and sometimes the demand is in the thousands—they will destroy the data and neither the doctor nor the patient will have access to the records or the prescriptions the patient needs.

This is in direct violation of the HIPAA laws, which state that healthcare information cannot be accessed, used, or disclosed in any manner that comprises the security or privacy of that information.

What makes this data so hackable is that many doctors' offices and other healthcare facilities are still running XP, which is completely vulnerable to cyber attack. Contrary to popular belief, Macs are just as vulnerable. In the past two months alone, there have been 33 breaches of healthcare offices or agencies and other companies. Involving millions of patient/customer records.

Ransomware damage cost $325 million in 2015 and is expected to rise to $5 billion in 2017 2017, which is a 15 times increase. In 2016, the global cost was $3 trillion and is expected to go up to $6 trillion by 2021.

Cybersecurity spending overall is currently around $80 billion and is expected to be over $1 trillion by 2021. This provides a lot of opportunity for those hoping to go into the cybersecurity field. The unemployment rate is zero, and the average starting salary is $200,000 per year. There are currently around 1.2 million jobs, and this is expected to rise to 3.5 million by 2021.■

Cyberattackers Hit HBO

Cyberattackers hacked into several upcoming episodes of HBO TV shows in early August, reported Time-Warner, HBO's parent company. This included script outlines for the popular series, *Game of Thrones*.

For complete details, go to http://www.technewsworld.com/story/84723.html ■

2017 CyberSecurity SIG

Chair	Arthur Schwarz
Co-Chair	Gora Datta
Treasurer	Brandon Young
Programming	Irvin Lemus
Newsletter	Carol J. Amato
Web Design	Ginson Samuel
Audio-Visual	Open

Place Your Ads in The Datagram

Do you have information about an academic program, seminar, work-shop, symposium, presentation, or job listing related to cybersecurity? Consider placing an ad in The Datagram.

Ads are currently FREE and will be published for three months, after which they are renewable. They will appear simultaneously on the CyberSecuritySIG's website at sites.ieee.org/ocs-cssig for maximum exposure.

Submit a camera-ready, business-card-sized (3.5" x 2") JPG file to Carol Amato at stargazer@stargazerpub.com.

Please Provide Feedback on Our Website

We want your feedback on our new website. If you like what you see or have any changes to suggest, tell us and others. If you have any changes in mind, please let us know. We are open to any suggestions and would appreciate your comments. ■