AI and Its Impact on Cybersecurity

Part 1: The AI Explosion – Where Did It Come From?

Artificial Intelligence, or AI, has dominated news cycles, online forums, and social media for the past several years. Unless you have been living off the grid in a remote cabin growing your own food, enjoying creation, the sun, moon and stars, which sounds very nice, you have either used or interacted with AI knowingly or not. The reporting around AI just like most things goes from one extreme to the other. The goal of this series is not to come down on one side of the debate, to help you do that, to discuss the pros or cons or any of the other issues surrounding the use of AI being discussed. The goal is to educate you the reader about what AI is, as best as it can be described, how it works and how it is being used. Just like anything else AI can be used as a tool for useful purposes, or it can be used for nefarious purposes. Just like a hammer can be used to frame a house, it can also be used to smash the glass on a jewelry store display case so a thief can steal precious gems.

Understanding AI can be difficult and so what we propose here is to make it understandable by everyday technology users, which in today's world is pretty much all of us. The goal is to use easy to understand everyday language and examples to help everyone understand what AI is, what it does and how it is being used. No fancy technical jargon (if we can help it), no computer science degree needed. Let us start with a little history of AI, where it all started and how it morphed into what we see today.

From Sci-Fi to Reality

If you are on downhill side of life like I am, you will remember the Sci-Fi TV series Lost in Space, which if you are a bit younger than I am, you may remember the 1998 movie adaptation. If you are still too young to even remember that you probably don't need to be reading this! In that series the family blasted off into space to explore accompanied by a robot named Robot, of course. Robot, more formally known as B-9, was the mechanical protector and informational database that was sent along to help the family succeed. Robot had a "human" voice, was aware of what was safe and what was dangerous maybe even with a touch of emotion. The 1940s and 1950s were filled with sci-fi robots and computers. Even into the 1960s and 1970s, examples like the voice activated computer in Star Trek or the "human-like" computer in 2001: A Space Odyssey. So how did we go from the imagination of screen writers to having an AI assistant in the palm of our hands?

Well, screen writers and authors usually take cues and ideas from real life, and the early sci-fi writers were no different. In 1950, a very smart man named Alan Turing wrote a paper called "Computing Machinery and Intelligence." You can see where he was going with this! This paper laid out the theory and is considered the intellectual starting point of AI. You may have heard of a test named after him used today called the Turing Test. If you read anything on AI, you will hear how the developers of the current AI models use this test to measure how "smart" their models are. This

test is used to see if a machine can exhibit intelligence that is indistinguishable from human intelligence. That is why it is also called the “Imitation Game.”

Based on Turing’s paper and work, others began to develop what was then called Machine Learning. Arthur Samuel and Christopher Strachey, in the early 1950s, both developed checker playing machines that learned how to play checkers, first by following the fixed set of rules of the game, but then by analyzing moves and outcomes so that it could learn how to play, anticipate moves and eventually win. You can thank these men for the ability to kill time at work playing either checkers or chess on your computer!

In 1956, several more very smart men gathered at Dartmouth College for The Dartmouth Summer Research Project on Artificial Intelligence. Yes, 1956 was when the term Artificial Intelligence was coined at this conference. While no major breakthroughs occurred during this conference, it was here that we got the term that has been so prominent in our everyday language over the past couple of years and where leading minds in the field came together to set the course for the development of AI.

It is important to note that one of the men at this meeting in 1956 at Dartmouth was John McCarthy, a computer and cognitive scientist. He is widely considered as one of, if not the, founding father of artificial intelligence. If you want to learn more about modern AI’s origins, a study of John McCarthy and his peers would be a great place to start.

Perceptron

Closing out the decade of the 1950s was the Perceptron. A very fifties sci-fi, cool name for a machine that was developed by yet another very smart person, Frank Rosenblatt. The Perceptron was an early computer that used what they call neural networks to give weight or priority to certain data, in effect ranking it from high to low in a sense. For example, if you had data in your computer on what an apple is and what an orange is, color, shape, taste, etc. and then fed data into the computer like round, red and sweet, the neural network would give weight to each of those entries and compare it to known data. The thinking might go something like this. Both are round so that criteria is given low weight, one is red and one is orange, these colors are close, so a little higher weight is given and then finally an apple is sweet, and an orange is tart. The taste of these two are very different so a high weight is given to taste. Based on the weights, or the neural network, the computer would tell you that you have an apple. This is the precursor to what we know today as the modern algorithm.

Our next step is taking the theoretical and developmental work during this time and making it useful and implementable into daily life and work. This takes us into the 1960s. As with most other technological developments, the early users were governments and research institutions. Governments have the money to fund these types of programs and out of this early machine learning era came programs like DARPA, The Defense Advanced Research Projects Agency that focused on developing technology for use by the military.

The Shift into Mainstream

The 1970s proved to be a challenging time for advancement in machine learning. Not due to a lack of want, but due to the high expectations of what machine learning could do coupled with a lack of

computing power. During this time limitations in hardware kept machine learning from advancing at the rate scientists hoped for. I remember our middle school had a calculator cart that would rotate through the math classes. These calculators could only do addition, subtraction, multiplication, and division. While it seemed like computers were coming of age, they were still limited in what they could do. This period during the 70s is often referred to as the AI Winter.

However, in the 1980s machine learning began picking up steam again. With advancements in computing power and computer chip development, industry began looking to machine learning for help with practical problem solving. These new "Expert Systems" were being developed with large amounts of data and rules in the attempt to mimic human decision-making. These were the early forms of the AI that we have today. Some systems were created to help doctors with medical diagnoses or assist geologists in finding oil fields.

Developments and advancements made in the use of algorithms, or weighting the data, along with increasing computing power made these early AI systems more effective. One of the earliest widespread uses of these new algorithms was in email spam filters, search engines, and e-commerce sites. These will be discussed in later parts of this series.

The Major Turning Point

AI maintained its usefulness through the 90s and into the 2000s, gaining momentum mainly through increased computing power and storage. It wasn't until a paper written in 2017 by eight scientists at Google entitled "Attention is All You Need" that AI took a major leap from what can be described as a step by step plodding method, known as RNN or recurrent neural network if you want to look it up, to a more holistic or complete analysis known as Transformer Architecture.

For example, the RNN model would look at a sentence word by word. Take this sentence; "I loved the pizza so much that I ate the whole…." The RNN model would read "I," process it and pass a bit of information to the next step, reading the word "loved." It would progress through the sentence this way relating each word to the previous word until it gets to the end and *predicts* the last word of the sentence, "thing" or maybe even "pizza." The issue with this model is that it has a short memory and so longer sequences, longer paragraphs, are harder for the model to remember thereby making it more difficult to predict at the end. In other words, this model lacked attention. See what I did there?

What the paper by Google theorized was that if you could focus, or pay attention to the entire sequence, the entire paragraph all at once, instead of word by word, then the model would be able to see relationships to words that are far apart instead of forgetting them like the RNN model could. Since the transformer model can see the whole sequence at once, it is much faster and more efficient to train. The RNN model had to plod along step by step in small bits to be able to retain relationships between words. The Transformer model also can calculate or weight how important every other word is to the current word, while the RNN model just looked at the previous word.

This idea of focusing on the entire sequence of data existed before the Google paper, however scientists and developers did not think it was possible to run only the Transformer model, they believed the RNN and Transformer model would have to run together. This would require a large amount of computing power. It was also a sort of perfect storm. At the same time as the paper was written, advancements in computer chip development, mainly GPUs (Graphics Processing Units),

was occurring that allowed developers to start running and training models using only the Transformer model or focusing on the entire sequence all at once. With these modern, more powerful GPUs, the idea of paying attention to the complete set of data was now possible and by running huge databanks of GPUs, massive datasets could be used to train these new AI models very quickly. Thank you Nvidia!

This is a very basic and brief history of where AI came from. It seemed to just appear in late 2022 with the mainstream release of ChatGPT by OpenAI, and this is when it really came to the forefront of the population. However, these new Transformer models, or attention AI models were already being used and trained as early as 2017 and 2018. Even at its release in 2022 OpenAI, the developers of ChatGPT stated that it was not fully ready and still in developmental stages, or what is called a research preview. We will also talk a bit more about this later when we discuss how these models are trained.

Hopefully this gives you a better understanding of the history of artificial intelligence, where it came from, how it evolved and maybe even surprised you in that you were using AI way back when Windows 98 came out with chess and checker games included! The next part of the series will discuss AI in more detail. We will look at data and how it used to train models, what exactly is an LLM, what is the difference between AI and automation and how these newer faster Transformer, or attention models are making an impact in the everyday life of technology users; search engines, use of algorithms (YouTube, Instagram) and advertising. Until then, think about heading over to our website, www.knowphishing.com, and signing up for our weekly newsletter that helps everyday technology users keep their data safe. We discuss current data security issues, how to set up hardware for maximum security, how to spot and identify attempts to steal your data and more! We do it all using easy to understand information and instructions. Thank you for your “attention”!!!