- Episode 43 –

AI and Cyber Security

Criminal in my computer?

Script : Hemant Lagvankar

Concept and Coordination : Dr. B.K.Tyagi

Artificial Intelligence (AI) is a buzz word in the cyber world. It can play a vital role to overcome the challenges raised by the technology itself. Cybersecurity is one of the challenges and increasing cyber crimes is the dark side of technology. The future application of AI in cybersecurity will ensure in curbing hackers.

Cybercrimes has become a daily news item. It is not just a problem faced in one country but across the world. It has become a big threat for governments, banks, multinational companies through online attacks by hackers. A lot of individual and organizational data is exploited by hackers.

In this connection, research in the area of AI and cybersecurity has gained more importance in recent times, and it is everlasting as it is a dynamic and sensitive issue linked to human life.

This episode describes how novel AI techniques help to improve cybersecurity.

List of Characters :

Hacker : A young man (age about 25 years)

Mr. Pandey : A middle aged man (about 45 years old)

Narrator : Preferably female voice to maintain the balance of the script

Police Commissioner : Age about 57-58 years

Mrs. Malhotra : Superintendent of Police from cyber cell unit (age about 45 years)

Mr. Ashish Dayal : An AI expert in police department (age about 35 years)

(A person who is a hacker dials a number to other person. Mobile phone rings. Sound of ringtone is heard. The call is taken and a dialogue between two persons starts.)

Hacker : Hello…. Good morning Sir!

Pandey : Yes….

Hacker : Am I talking with Mr. Chaturvedi?

Pandey : No, not Chaturvedi…. I am Mr. Pandey!

Hacker : Ohhh…. Sorry Sir! Actually sir, I want to talk to you only….by mistake I said Mr. Chaturvedi!

Pandey : Okay… but who are you?

Hacker : Sir, I am calling you from 'Smart Pay'. I hope you are using our app regularly!

Pandey : Yes… I frequently use it.

Hacker : Yes, Sir! That's why I am calling you Sir!

Pandey : Okay.

Hacker : Sir, are you satisfied with our service? Do you have any difficulties in operating our app for transactions?

Pandey : No, not as such!

Hacker : So Sir, you are satisfied with our app 'Smart Pay' and the service that we provide to you, correct?

Pandey : Yes…

Hacker : Fine, Mr Pandey! You are our valued customer. So we want to give you a surprise gift for the last five transactions which you have made in this month.

Pandey : Okay, but I did not see such offer in the app.

Hacker : Sir, I told you, we want to give you a surprise!

Pandey : Okay.

Hacker : Sir, please confirm whether the same phone number you have registered for our 'Smart Pay' app or some other number…

Pandey : The same number on which you are speaking!

Hacker : Great! Then Sir, please check the notification in our app… right now!

(Notification bell rings. Mr. Pandey has received the notification)

Pandey : Yes! I have received the notification. But it is showing Rs. 18999.00 and asking to pay!

Hacker : Of course Sir! It is saying that, you need to pay to your wallet. Just press the option pay and you will see the amount in your wallet!

Pandey : Okay! Let me do that!

(Again notification bell rings. Mr. Pandey has received the sms)

Pandey : Ohh my god! Hello, hello…. Hey Mr. …… Hello….

(The busy sound of the phone is only heard)

Narrator : ***(A sad tune of music is at background)*** So friends, have you listened? Have you understood what has happened? Mr. Pandey was cheated. The phone call was a fraud and Mr. Pandey was the victim of this call from a hacker. He was compelled to pay nineteen thousand rupees in one click. I am sure that, most of us have read such incidences in news and some of you might have experienced such financial losses also….

(The background music changes gradually)

Friends, this is just the tip of the iceberg. The world is going digital at an unprecedentedly fast pace, and the change is only going to go even faster. The digitalization means everything is moving at lightning speed – business, entertainment, trends, new products, etc.

More ironically, according to the study carried out in 2017, India has emerged as the third most vulnerable country in the world in terms of risk of cyber threats, such as malware, spam phishing, bots, network attacks, web attacks, ransomware, and cryptominers.

The study also pointed out that with the threat landscape becoming more diverse, attackers are working harder to discover new avenues of attack and cover their tracks while doing so.

(Change over music)

(A scene of police commissioner's cabin. A meeting is called by the commissioner to discuss the increasing issues of cyber crimes and cyber security. Superintendent of Police Mrs. Malhotra along with Mr. Dayal who is AI expert in the police department have arrived in the cabin.)

Mrs. Malhotra : (Knocking the door of cabin) May I come in Sir?

Commissioner : Yes, come in!

Mrs. Malhotra : (Salutes to Commissioner. Sound of boots striking on ground) Superintendent of Police, Cyber Security Cell Mrs. Tanuja Malhotra, reporting Sir!

Commissioner : Yes, officer. Jai Hind!

Mrs. Malhotra : Jai Hind Sir.

Commissioner : Have a seat Mrs. Malhotra!

Mrs. Malhotra : Thanks Sir. I am reporting you with Mr. Dayal who is AI expert in our department.

Commissioner : Hello young man! Have a seat.

Dayal : Jai Hind Sir!

Commissioner : Jai Hind…. So, Mrs. Malhotra, as you know… I have called this meeting with a very specific agenda.

Mrs. Malhotra : Yes Sir!

Commissioner : You are very well aware that, recently, we have experienced unauthorized transactions of about 150 crore through a dark web network. Of course, CBI is looking after it. But, with increase in dependency on information technology, networking, social media, online business, etc. we are facing the issues of cybercrimes. Every day these cases are increasing.

Mrs. Malhotra : I know Sir!

Commissioner : Also, Mrs. Malhotra it is not restricted only to the financial issues, but it has become a threat to national security as well.

Mrs. Malhotra : Yes Sir! I can understand!

Commissioner : So, Mrs. Malhotra… I want to know what can be our strategy to tackle this burning issue. What can be our preparation?

Mrs. Malhotra : Yes, Sir. We will surely discuss it. That's why I have asked Mr. Ashish Dayal to work on this issue as he has expertise in the field of artificial intelligence and I think he is the right person who can guide us about what can we do using artificial intelligence to tackle this problem.

Commissioner : Correct! Then please go ahead…

Mrs. Malhotra : Ashish, now you can take over….

Dayal : Yes Madam! I will start my presentation from the beginning… that is how these cybercrimes are taking place.

Mrs. Malhotra : Okay.

Dayal : When everything is going smoothly, all of a sudden… you come to know that the hackers have attacked the system and asking for a leg and an arm as a ransom. In this scenario, you lose not just the money but, also the trust of your customers. The negative message that goes in the market put down your brand image.

Commissioner : Hmmm.

Mrs. Malhotra : This also creates fear in the minds of common people… a fear of insecurity!

Dayal : Yes! Due to vulnerability, from our studies, we came to know that, small businesses are on constant radar with 43% of the attacks being made on small enterprises.

Commissioner : Mr. Dayal, this study will definitely give us some lead to overcome the issue.

Dayal : Yes Sir! It is observed that, the biggest challenge for us is the malware proliferation. Malware is growing at a rapid pace of more than one lakh of unique pieces a day, which is humanly difficult to control.

Mrs. Malhotra : Then can artificial intelligence help in solving this issue?

Dayal : I will come to this point, Madam. But, let me first elaborate the problem so that we can understand the scope of it which eventually guide us in overcoming –

Commissioner : Yes, go ahead!

Dayal : Sir, businesses are doing their best to fight off cyberattacks, but it's hard to predict what new campaigns will emerge and how they will operate. It's even harder to discern what the next big malware threat will be.

Commissioner : You mean to say, is it difficult to defend against unknown threats?

Dayal : Yes Sir, somewhat –

Mrs. Malhotra : And that's something that cyber criminals take advantage of.

Dayal : Sir, the Zeus trojan and Locky ransomware were once considered as major threats, but now it's things like Emotet botnet, the Trickbot trojan and Ryuk ransomware.

Mrs. Malhotra : It’s terrible!

Dayal : The terrifying part is that, the Emotet software usually acts as a distribution and packing system for other malicious payloads, but is also able to brute-force computer systems, generate email messages for the purposes of spam campaigns, create backdoors, and steal financial data. Emotet started life as a banking trojan, but has also evolved into a botnet, with its criminal operators leasing out its capabilities to those who want to distribute their own malware to compromise machines. For almost two-thirds of malicious payloads were delivered by Emotet in phishing attacks.

Commissioner : But what is the modus operandi in this case?

Dayal : Sir, like in the past, the malware is delivered via phishing emails that contain a malicious Microsoft Word document. The email subject lines are generally based around invoices, bank details and other financial subjects – that is, common terms to attract the attention of people.

Mrs. Malohtra : And what is there in the attachment?

Dayal : The email asks the user to 'enable content' in order to see the document; and if this is done then it allows malicious macros and malicious URLs to deliver Emotet to the computer or mobile of the user.

Mrs. Malhotra : Ohhh my god! This is like a trap!

Dayal : Yes! It’s a trap for the user and they tempt to open the document. Because Emotet is such a prolific botnet, the malicious emails don't come from any one particular source, but rather from infected Windows machines around the world.

Commissioner : That means it spreads like pandemic!

Dayal : Exactly Sir! If a machine falls victim to Emotet, it not only provides the malware a backdoor entry into the system and allowing attackers to steal sensitive information, but it also allows the attackers to use the same machine to spread additional malware – or allow other hackers to exploit compromised PCs for their own gain.

Commissioner : Hmmm! That's why it is said that, 'cyber attack is the biggest threat to mankind, even more of a bigger threat than the nuclear weapon!'

Mrs. Malhotra : That's right Sir!

Dayal : Sir, such attacks have been directed not only at the organizations in financial services, but also targeted at the food, media and transportation industries now!

Commissioner : Okay… Let's face the reality and think how to deal with this challenge!

Dayal : Sir, traditional technology relies too much on past data and it cannot improvise. It cannot keep up with the new mechanisms and tricks of hackers. More over, the volume of cyber threats people has to deal with daily is too much. The malware is growing at a rapid pace of more than 100,000 of unique pieces a day, which becomes difficult to control manually.

Mrs. Malhotra : If people take proper precautions and keep their data password protected then?

Dayal : Madam, you are right, but passwords have always been a very fragile control when it comes to security. Let's face reality, most of us are quite lazy with our passwords – often using the same one across multiple accounts, relying on the same password since ages, keeping account of them neatly as a draft message in our device, etc.

Mrs. Malhotra : But what is about biometric authentication?

Dayal : Well, as you said, biometric authentication has been tested as an alternative to passwords, but it is not very convenient; and hackers can easily circumvent this, too. For example, a face recognition system can be irritating to use when it can't recognize you because of a new hairstyle or when wearing a hat. Attackers can also get through it by using your images from Facebook or Instagram.

Commissioner : ***(With some irritating voice)*** Mr. Dayal, I was asking for the solution. ***(Taking pause)*** See officers, I don't want any negativity in the issue. We need to look into this issue very seriously and take necessary action immediately…. that's what I know!

Mrs. Malhotra : Sorry Sir… we understand your sentiments!

Dayal : Sir, in this situation, artificial intelligence is the possible solution….. Not completely, but it has a promising scope of dealing with malware proliferation by eliminating the need for manually created anti-viruses for each malware.

Commissioner : Okay!

Dayal : With artificial intelligence and machine learning, the 'bad' can be differentiated from the 'good' and we can defeat even the most alien malware attack that has never been seen before.

Commissioner : That's good!

Mrs. Malhotra : How does machine learning help in this case, Ashish?

Dayal : Actually madam, before 'machine learning' entered the mainstream, artificial intelligence programs were only used to automate low-level tasks in business and enterprise settings. Machine learning is fundamentally set apart from artificial intelligence, as it has the ability to evolve. Using various programming techniques, machine learning algorithms able to process large amounts of data and extract useful information. In this way, they can improve upon their previous iterations by learning from the data they are provided.

Mrs. Malhotra : But what is about artificial intelligence?

Dayal : Yes, I am coming to that! Actually, we cannot talk about machine learning without speaking about big data, one of the most important aspects of machine learning algorithms. Any type of artificial intelligence is usually dependent on the quality of its dataset for good results, as the field makes use of statistical methods heavily. With machine learning algorithms, AI was able to develop beyond just performing the tasks it was programmed to do.

Commissioner : So machine learning and artificial intelligence go hand in hand!

Dayal : Exactly Sir! In today's online-first world, companies have access to a large amount of data about their customers, usually in the millions. This data, which has both, large in the number of data points and the number of fields, is very huge. This huge data which is generating everyday is almost impossible to process manually.

Mrs. Malohtra : And there artificial intelligence comes into the picture!

Dayal : Correct! What artificial intelligence enables us to do is to respond in an intelligent way, understanding the relevance and consequences of a

breach or a change of behaviour, and in real time develop a proportionate response. Artificial intelligence can efficiently handle the vulnerabilities seen in the software and it can prioritize high-risk scenarios requiring immediate attention. A key benefit of machine learning and artificial intelligence in cybersecurity is that these identify and react to the suspected problems almost immediately, preventing potential issues from disrupting the routine work.

Commissioner : That's very important aspect!

Dayal : Artificial intelligence allows us to automate the detection of threat and combat even without the involvement of the humans, powering the data to stay more secure than ever. Since artificial intelligence is totally machine language driven, it assures complete error-free cybersecurity services. The technology has the potential to detect attacks in their earliest stages or anticipate them before they occur.

Mrs. Malhotra : That's great!

Dayal : And Sir, like we also think about what could be the next possible move of the criminals, the technology can also help us to do so.

Mrs. Malhotra : How?

Dayal : Artificial intelligence and machine learning can detect and track more than 10,000 active phishing sources and react and remediate much quicker than humans can. As we know, there is no restriction of its understanding of phishing campaigns to any specific geographical area. But, Artificial intelligence and machine learning scan phishing threats from all over the world, and artificial intelligence has made it possible to differentiate between a fake website and a legitimate one quickly.

Commissioner : That means artificial intelligence is really good at the ability to adapt and respond to a constantly changing world. Am I correct?

Dayal : Absolutely Sir! Machine learning and artificial intelligence actually study the phishing patterns of hackers. Therefore with the help of artificial intelligence, it's now possible to spot the phishing activity almost immediately, blocking the potential damage of a malicious intrusion and preventing login credentials being stolen, malware being deployed or otherwise enabling attackers to gain access to the network.

Mrs. Malhotra : But what happens if any new pattern of hacking takes place?

Dayal : Very good question, Madam! The promising enhancement of security by artificial intelligence comes from its behavioral analytics ability.

Mrs. Malhotra : Means?

Dayal : It means is that machine learning algorithms can learn and create a pattern of your behavior by analyzing how you usually use your device and online platforms. The details can include everything from your typical login times and IP addresses to your typing and scrolling patterns. If at any time, the artificial intelligence algorithms notice unusual activities or any behavior that falls outside your standard patterns, it can flag it as being done by a suspicious user or even block the user. The activities that tick off the artificial intelligence algorithms can be anything from large online purchases shipped to addresses other than yours, a sudden spike in document download from your archived folders, or even a sudden change in your typing speed.

Commissioner : But Mr. Dayal, I have a fundamental question.

Dayal : Yes Sir!

Commissioner : The hackers are also intelligent. They also have the same technology which we are having. So can they supersede us?

Dayal : Sir, actually this is the biggest challenge in the field of artificial intelligence that it is equally accessible to everyone, including the hackers. Hackers are also using artificial intelligence to make multi-dimensional attacks in high volumes. They are using artificial intelligence to mutate the malware. They also leverage the technology to find out the most vulnerable cross-section of people who can be an easy target.

Commissioner : So, there is a constant battle between attackers and defenders!

Dayal : Yes Sir, but now there are systems which immediately inform the suspicious activity as the hackers came out with a new variant in the wild. For that some specialized machine-learning signatures and models are designed to orient to these variants when they appear. The AI-based network-monitoring tool can also track what users do on a daily basis, building up a picture of their typical behaviour. By analyzing this information, the artificial intelligence systems can detect anomalies and react accordingly.

Commissioner : Okay….That's great! So you mean to say we are fully equipped with the technology and can defend such phishing attacks using artificial intelligence.

Dayal : Yes Sir! But, it is equally important that the users should also be careful while doing any online activity, particularly while doing transactions!

(Change over music)

Narrator : So friends, machine learning and artificial intelligence are the two strong arms which we have to defend phishing attacks. But as the experts say, everything is not 'rosy' about artificial intelligence. We, at personal level must also be careful. Because it is not a distant probability that cannot happen to you… One in every 130 emails contains a malware! So, be careful… otherwise who knows there may be a criminal in your computer also!

(Music piece. Episode ends)

Written by

Hemant Lagvankar (हेमंत लागवणकर)
hemantlagvankar@gmail.com