Cyber security : The role of artificial intelligence in the future of cyber security

What should be learned in this seminar:

High level overview of machine learning

How machine learning can be used ina cbybersecurity context

Artificial intelligence

Artificial intelligence in cyber security

Pitfalls & best practices

What is machine learning?

* Field of study that gives computers the ability yto learn without being explicitly programmed
* Development of algorithms that can draw inferences and make predictions based on data
* Evolved from pattern recognition and computational learning theory; closely related data mining and statistics
* Benefits of machine learning include automation, being unbiased, and being able to improve over time

The machine learning process

Data -> model -> Prediction

Code -> Algorithm -> Results

How can machine learning be used in a cybersecurity setting?

1. Applying upervised machine learning to security
   1. Supervised machine learning naturally suited to classification (yes/no) problems; transactions can be viewed under a good/bad lens:
      1. Spam
      2. Online fraud – given financial transaction that is fraud in the internet, even your picture can be copied/captured and used in bad things
      3. Malware – Can destroy your file/data inside your computer
      4. Part of networking – Malicious URLs/domains/IPs
         1. It is a malice, ip network connections to a given url. Phising sites.
         2. Created by programmers with abnormal behaviour, based on psychological studies.

If we have applied supervised, we must have the unsupervised machine learning security

1. Network traffic – Abnormal amount of traffic in a particular host, particular abnormalities in the network or inside the providers
2. Failed log-in attempts – Sometimes we see the GUI and not the URL, that is a phishing site if the URL is malicious
3. User accessing resources –
4. Access patterns - That are too regular is easy to know. You should change the pattern to prevent hacking of data.
5. Working during hours outside – It’s either his/her normal behaviours, even outside the company, you are accessing the files outside
6. User connecting to or from unusual geographic locations- No sense locations,

From this data, the machine learning learns the normal behaviour and anything outside that normal behaviour may be malicious. So don’t use the unsupervised machine learning

Automation is AI, Our phones is AI. Do not expose to the public

What is Artificial Intelligence?

AI is the intelligence of machines and robots and the branch of computer since that aims to create it.

AI is the computational part of the ability to achieve goals in the human and computer interface

It can help decide like humans.

From AI to Cybersecurity, Why Use AI in cybersecurity

When we talk about AI, people often refer to a world dominated by robots in a science fiction universe.

But AI is rooted in reality and is used in many fields, such as online shopping, surveillance systems and many others.

ML Allow the computer to learn to make prediction or result based on the given data.

AI has already proven that this is effective in treatment of millions malicious. 400000 new malicious programs detected each day. According to the independent testing we call that AV test or Antivirus test.

So how to block this particular threats in the artificial lintelligence by using this Ai?

We must install AV to block malware inside the system

Security vendors regularly look for ways to implement artificla intelligence technology to their cyber security tools.

We use Antivirus to protect our machines/ systems by installing the anti virus in our computer/servers/machines

What are the pitfalls and best practices when applying machine learning to cybersecurity

Challenge: Good data is critical

Garbage ->

When you throw your codes, you must destroy it, it can be used. You must delete.

Problem is we recycle

You must ultimately ask the right question for the right answer

Pitfall: Becoming obsessed with classifier

But if the data or the particular codes or ml codes, we must know this.

Data -> Features -> Classifiers

Order importance right to left

Amount of time spent left to right

It is easy to access the new features from existing samples to build more interesting features.

Classifier , we need to identify diff targets in malicious behaviours and malware inside the machine. We need to have diff targets.

Parang tao lang an, di mo pwedeng sabihing magloloko yung tao kung may sakit yun.

Kung yung data na kinuha mo may virus, mabilis lang. To protect that, we need different antiviruses bc 40000 per day, new malicious.

From trend micro, naddetect ang virus from china, china magaling gumawa ng virus. According to studies of trendmicro

If you don’t classify/identify your targets, the malicious behaviour, it will be a danger.

“Eh ayaw ko makisaksak sa virus”

You should not be afraid, since you will be the one to create a solution for that malware

Supervised learning pitfalls

2 parts of pitfalls, trap dangerous

AV – You trap the virus so no more

Training set caputures what you know about; inference from training set expand your capabilities, but don’t help with the “uknow unknons”; your model may be a glorified signature…

* We must use the best AV, even in phones, because it is still a machine. We must use digital signature.

So everything we use must be original, not fake.

Malicious behaviour is subjective ( not everyoneagrees) Further, wheteher somethings is malicious is not so much about actions, but more about the intent behind those actions.

Machine learning can avoid, but not always as we hope, because of new paradigm.

Unsupervised learning pitfalls

3 parts of unsupervised learnings in dangers

UL used to find abnormal behaviours, but that’s not the same as malicious behaviors.

The users.

People often act abnormally for legitimate reasons (travels, deadlines, new project, role, promotion)

It’s not always easy to measure normal behaviour. (Geolocation isn’t always accurate…)

Best practices:

* Data >> Features >> Classifier
* Identify/classify those threats against ML or AI
* Know what success means

Not bc u hacked u are successful, u destroy the system itself. When you hack/threat.

* Don’t set and forget it; adversaries adapt!
* Think about model deployment; not everyone touching system will have deep machine learning knowledge.
  + Studying not only the front end but also the backend

Today’s digital ecnomoy is based on trust

Intelligent automation supported by AI

Visualizations taps into the human ability to zero in on patterns

Liquid workfoce model reduces challenges by enabling more workfoce like crowd sourcing

Conclusion

Technology is destructive only in the hands of people who do not realize that they are one and the same process as the universe.

Only people is destructive, not machine, bc te AI and ML is based on humans.

2 anti viruses detect each other as virus

You must always choose the best application. You must delete one of the antiviruses if you have two and remain what you choose.

You must update update update your antivirus.

Do not use free trials, you must used licensed antivirus.

You must use digital signature, do not pirate, but the software. Bc free trials only scan, no features.

Maybe it’s possible, maybe not. Because sometimes virus are codes. To protect that codes, it should be secured with a cyber security tool. We say we are IOT, all in the cloud. Those is the cloud should be secured.

You should protect both the hardware and the software. If IOT, you need to secure all. If it is possible to put in a virus.

If we want to puruse cloud computing industry, what do we need to do in order to.

We want our system to be safe, new cloud computing, what do we need to do

Study where you should put it. Always License everything you use and it should be ISO certified. Because you will store it there. All clouds/servers are ISO certified, even our phones are iso certified. And we should study digital signatures. Wag basta basta mag titiwala

May iba pa pong antivirus para sa ransomware

Meron ,madami naman para sa ransomware, you can type that I nthe internet, akakakita kayo ng antiviruses. May mga company. Usually avira gamit ng mga company.