AI Weaponization by Hackers

The risks of cyberspace security now and in the future
ANTHONY ENGLISH
CEO/CISO, Bot Security Inc.
Canada
Panelists

Fook Hwa Tan
Chief Quality Officer
The Netherlands

Dragan Pleskonjic
Senior Director of Application Security at IGT (formerly GTECH), Adjunct Professor,
Initiator and Founder of the R&D projects:
INPRESEC (Intelligent Predictive Security),
Glog, Security Predictions
Serbia
Artificial Intelligence

Definition

• **Artificial intelligence AI** (also machine intelligence, MI) is intelligence displayed by machines, in contrast with the natural intelligence (NI) displayed by humans and other animals.*

• In computer science, AI research is defined as the study of “intelligent agents”: any device that perceives its environment and takes actions that maximize its chance of success at some goal.*

• Colloquially, the term “artificial intelligence” is applied when a machine mimics “cognitive” functions that humans associate with human minds, such as “learning” and “problem solving.”*

• **Strong AI** — Claim that computers can be made in a way to “think” as humans. To be more precise, it is a claim that there is a class of computer programs which, when implemented, make computers mimic human thinking.

• **Weak AI** — Claim that computers are important tools in modelling simulations of human behavior.

* https://en.wikipedia.org/wiki/Artificial_intelligence
Artificial Intelligence

Umbrella term to describe machines/constructs capable of learning and human-type reasoning and perception.

The use of algorithms to examine and learn from data to make predictions/decisions. Performance improves over time with exposure to more data.

The use of multi-layered neural networks to build algorithms that are used to perform tasks better as part of this process. Large data sets are utilized.
Artificial Intelligence

Examples of AI in Use Today

• Self driving cars, smart cars, other vehicles, flying objects
• Speech and image recognition and analysis
• Medical diagnosis, pharmacy
• Virtual personal assistants
• Recommendation services: shopping, movies, music, books, etc.
• Purchase and market prediction, advertising
• News generators (e.g., fake news and deep fakes)
• Military uses
• ...
Question Time!

- How do you define Artificial Intelligence?
- What recent example of AI weaponization has caught your attention?
AI and ML, some fun (1)

Difference between machine learning and AI:

If it is written in Python, it's probably machine learning

If it is written in PowerPoint, it's probably AI

2:25 AM · Nov 23, 2018 · Twitter Web Client

8.5K Retweets  865 Quote Tweets  24.1K Likes
AI Weaponization
Current Uses of AI in Cybercrime

- Hackers are turning to AI and using it to weaponize malware and attacks to counter the advancements made in cybersecurity solutions (e.g., criminals use AI to conceal malicious code in benign applications).
- Criminals are using AI to crack passwords faster.
- Breaking CAPTCHA
- Data poisoning
- Generative Adversarial Networks (GAN’s)
- Manipulating bots

**Future concern:** One of the biggest concerns regarding AI’s use in malware is that new strains would be able to learn from detection events. If a strain of malware was able to determine what caused its detection, the same behavior or characteristic could be avoided the next time around.
Impact of AI in Cybercrime

• Given the black market for cybercriminal tools and services, AI can be used to make operations more efficient and profitable. In identifying targets for attacks, cybercriminals can start and cease attacks with millions of transactions in just minutes, because of fully-automated attack infrastructure.

• Can AI be hacked? The hacking of artificial intelligence is an emerging security crisis. Pre-empting criminals attempting to hijack artificial intelligence by tampering with datasets or the physical environment, researchers have turned to adversarial machine learning.

• Will AI take over cyber security? The answer is probably no; however, AI will drastically change the kinds of work cyber engineers are doing. While AI may be great for processing large amounts of data or replacing autonomous manual tasks, it will never be able to replace a security analyst's insights or understanding of the field.
Fighting Cybercrime with AI

Dragan Pleskonjic – My current research and development focuses on:

- **Glog** is a solution that is able to give remediation advice based on context or, even more, to automatically fix the security vulnerabilities in software code. It uses machine learning and AI.

- **INPRESEC (Intelligent Predictive Security)** – Exploring the paradigm shift in Information Security and Privacy with Artificial Intelligence and Machine Learning. Novel approach to cyber security to predict the most likely cyber-attacks and to plan optimal proactive cyber security defensive measures.

- **Security Predictions** – Exploring the ways to harness the “wisdom of crowds” and experiment if and how crowd-sourced security intelligence can be used to predict future security and privacy threats, attacks, and events.
Question Time!

- What AI weaponization countermeasures do you see as being needed soon or now?
- Do you see AI weaponization as going beyond computer systems as the main pathway for attacks?
AI Future
AI Evolutions & Their Impact

Rival schools of thought within Machine Learning

- **Symbolists** view learning as the inverse of deduction and take ideas from philosophy, psychology, and logic.
- **Connectionists** reverse engineer brain and are inspired by neuroscience and physics.
- **Evolutionaries** simulate evolution on the computer and draw on genetics and evolutionary biology.
- **Bayesians** believe learning is a form of probabilistic inference and have their roots in statistics.
- **Analogizers** learn by extrapolating from similarity judgments and are influenced by psychology and mathematical optimization.

- What we really want is a single algorithm combining the key features of all of them: the ultimate master algorithm.

AI Evolutions & Their Impact

The ultimate Master algorithm

• What we really want is a single algorithm combining the key features of all of them: the ultimate master algorithm. For some this is an unattainable dream, but...

• If it exists, the Master Algorithm can derive all knowledge in the world — past, present, and future — from data. Inventing it would be one of the greatest advances in the history of science. It would speed up the progress of knowledge across the board, and change the world in ways that we can barely begin to imagine.

• The Master Algorithm is to machine learning what the Standard Model is to particle physics or the Central Dogma to molecular biology: a unified theory that makes sense of everything we know to date, and lays the foundation for decades or centuries of future progress.

• The Master Algorithm is our gateway to solving some of the hardest problems we face...

• Source: The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World, Pedro Domingos
Question Time!

- What AI weaponization evolutions do you see as future threats?
- What is the best way to manage AI and its use as a weapon for hackers or for nation-states?