How to insert auto play: https://support.office.com/en-us/article/Insert-or-link-to-a-video-on-YouTube-8340ec69-4cee-4fe1-ab96-4849154bc6db

Hacking into the school

https://www.youtube.com/watch?v=U2_h-EFIztY&index=2&list=PLZbXA4lyCtqpGOS2KC1mAAKaGwbup-DQt

<iframe width="560" height="315" src="https://www.youtube.com/embed/U2_h-EFIztY?

list=PLZbXA4lyCtqpGOS2KC1mAAKaGwbup-DQt" frameborder="0" allowfullscreen></iframe>

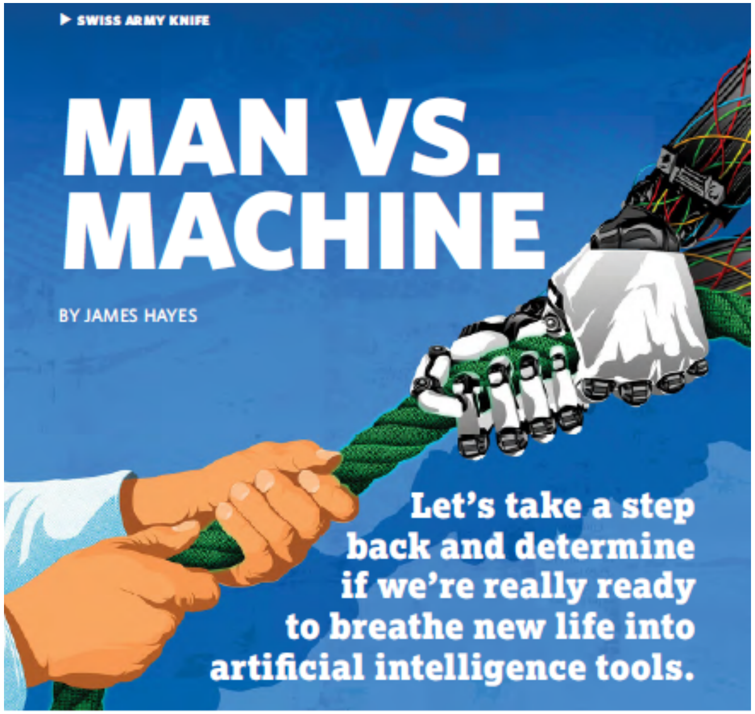
Artificial Intelligence and Cyber Security

"Man vs. Machine"
An ISC2 Article Review
InfoSecurity Professional Sept/Oct 2017

Hampton Roads Chapter
ISSA

Agenda

- Artificial Intelligence (AI)
- Machine Learning (ML)
- AI use in counter threats
- Evaluation Point
- Risks



▶ SWISS ARMY KNIFE

MAN VS. MACHINE

BY JAMES HAYES

Let's take a step back and determine if we're really ready to breathe new life into artificial intelligence tools.

Artificial Intelligence

- Definition: https://www.merriam-webster.com/dictionary/artificial%20intelligence
  - a branch of computer science dealing with the simulation of intelligent behavior in computers
  - the capability of a machine to imitate intelligent human behavior
- AI is not just about robots. It is also about understanding the nature of intelligent thought and action using computers as experimental devices (Buchanan, Bruce G. *A (Very) Brief History of Artificial Intelligence*. AI Magazine 26(4): Winter 2005, 54.)
- The first book collecting descriptions of working AI programs was Edward Feigenbaum and Julian Feldman's 1963 book, *Computers and Thought.*

Machine Learning

- Definition: http://www.expertsystem.com/machine-learning-definition/
  - Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. **Machine learning focuses on the development of computer programs** that can access data and use it learn for themselves.

```
<iframe width="560" height="315" src="https://www.youtube.com/embed/NHWjlCaIrQo" frameborder="0" allowfullscreen></iframe>
```

AI and ML in Cyber Security

- "…While AI is how we hope to make machines 'intelligent,' ML is the behind-the-scenes computation that makes AI possible. [In the cybersecurity market now] ML is the fastest-growing area [related to] AI, which is why there is such buzz around it—and also why there is confusion about what ML can do [in comparison with] 'true' AI."
- Cybersecurity solutions are already taking advantage of ML, Herberger reports, by using behavioral analysis to enhance attack mitigation systems. As a result, mitigation systems can perform more advanced threat analytics on a much larger scale.
- AI "can provide new tools for threat hunters, helping them protect new devices and networks even before a threat is classified by a human researcher. Machine learning techniques, such as unsupervised learning and continuous retraining, can keep us ahead of the cybercriminals."

Evaluation Points

Advantages

- Less manual data analysis, more predictive threat analysis
- Large amounts of data can be synthesized quickly
- Once trained, provides 24 X 7 X 365 coverage (no sick leave or vacations)

Disadvantages

- Still new Technology – Not proven
- High learning curve - staff
- Not an out of the box solution – takes time to train the system
- Process/procedure changes

Risks

- An organization could place too much trust in an AI, which results in bad judgment calls
- An organization could ignore its insights, so the AI learns that prolific ‘bad’ behavior is actually normal
- Productivity impact: Using a fully autonomous AI solution without proper tuning can enable it to make decisions which negatively impact business productivity
- Double edge sword: AI-based products can uncover the harsh reality of what is actually going on within an organization (Facebook, Amazon, etc.)
- Potential adverse action by AI/ML
  - Example: Oct. 19, 1987 Black Monday stock market crash

Humans vs. Machines

Computers

- Calculations
- Instructions
- Objectivity

People

- Purpose
- Perspective
- Passion

Humans and Machines

Summary

- “The term ‘AI’ generally applies to more far-reaching and complicated uses that could potentially mimic human thought processes. For the most part, cyber practitioners with firsthand experience will know the difference—but confusion will certainly mount at the board level if hype increases.”
- AI and ML are “closely related, but they are not the same thing…In many ways, ML is an enabler for AI.”
- Technology simply has not matured enough to allow a fully ‘hands-off’ approach
- The optimal use of AI is the Machine and Human Partnership

Summary cont.

- Due process must be conducted when implementing AI/ML systems
- Risks can be mitigated by appropriate tuning and setup and, at least, semi-frequent use of a system; so again, organizations will get out of [AI-based cybersecurity] what they put in.
- The fundamental reason for using these AI-based approaches is because they are more capable and flexible than the more simplistic rule- or heuristic-based mechanisms deployed to date. By analyzing much larger volumes of data and then being trained with human feedback as they surface possibly ‘questionable’ behavior, over time these systems become smarter, and can account for a broader range of allowable behaviors

Questions???