McAfee expert explained how deepfake and AI are drilling through the cyber security wall

'Hundred listeners are not equal to one', this proverb might not be accurate when it comes to cyber security.

'Hundred hearing is not equal to one', this idiom may no longer be accurate when it comes to the situation of cyber security before the 'threat' from deepfake in the future, you will no longer be able to believe I saw it with my own eyes!

Recalling a bit of concept, deepfake is a program that uses artificial intelligence, allowing users to swap someone's face in a video with someone else's face. In fact, it helps users create fake content by inserting the faces of celebrities into the video for the purpose of libeling or gaining illicit profits. That is the reason why deepfake becomes a top threat to entertainment companies, celebrities, and above all, is network security.

1. Google and DeepMind apply AI to predict the output of wind farms

Steve Grobman, chief technology officer at network security company McAfee, and Celeste Fralick, one of the world's leading data scientists, have now issued a warning in an important speech at the conference. RSA's secret in San Francisco recently said that Deepfake technology has developed much more sophisticated than humanity still thinks, and it is really a great threat in the future. To prove it, these two scientists showed a video, which showed that Celeste Fralick's words are spoken from a descriptive image that resembles Steve Grobman's face, even though Grobman has not yet ever say those words. Thus it can be seen that we are easily fooled by deepfake, so in this age, what the eyes see in the ears is not necessarily correct!

'I used your public comments to create and train a machine learning model that allowed me to develop a deepfake video, with the words I said but that came from someone else's mouth. This is just one of many ways

that AI and machine learning can be used for nefarious purposes. It makes me think of a bad scenario that AI can be used by attackers, things like social engineering and scams, where our competitors can now create content. Auto target ', Celeste Fralick said.

1. China continues to launch the virtual female radio announcer run by the world's first AI

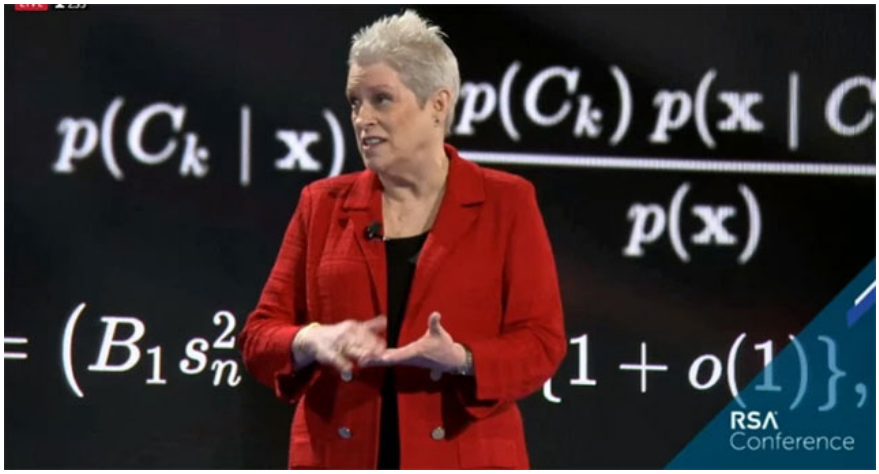
In fact, the deepfake and AI itself have become a powerful supporter for hackers to create personalized online phishing attacks and have a higher success rate and can proceed. with the scale of automatic attacks.

'To be fair, most people don't realize how dangerous AI and machine learning can be, and the boundary between being applied to good or evil is also fragile. There is a technical area that my team is participating in, called adversarial machine learning. There, we conducted research on the ways in which bad guys can invade or poison the machine learning hierarchy, 'added Celeste Fralick.

In an interview on Monday 4 March, Steve Grobman said that he and Celeste Fralick were able to create deepfake videos in just one weekend without trying hard to make it perfect. This suggests that when a qualified deepfake attacker has identified the target, creating sophisticated AI-based fabricated videos is not difficult at all.

One of the most common ways to deceive a real person and an AI-created model is to take a nearly realistic picture, and then change a very small part of the image's details in a way that the average person usually will not be recognized. Fralick gave an example, in which a photo of a penguin can be interpreted and deduced by AI as a frying pan, only in a few small steps.

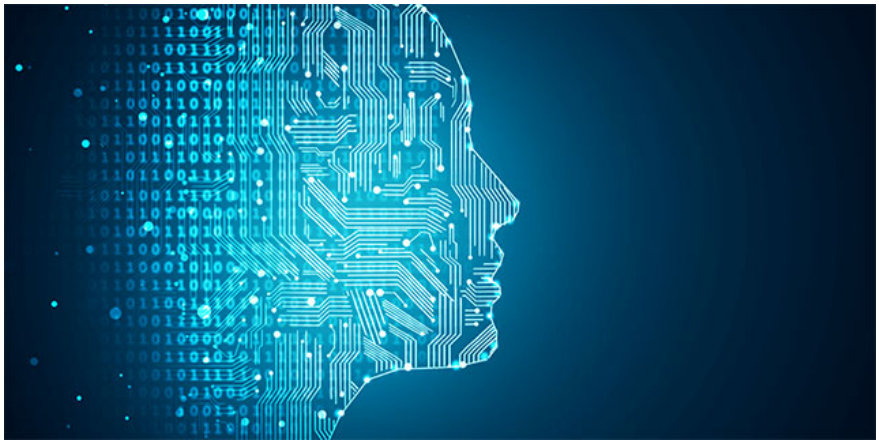
What Celeste Fralick wonders here is whether the same techniques that are being used to confuse the image classifier can continue to be used to confuse their network models. whether or not, specifically here is the False positive (false authentication error).



1. AI engineer Facebook talks about deep learning, new programming languages ??and hardware for artificial intelligence

The false positive has several types, such as the negligence of some anti-spyware programs that make users mistakenly believe that their device has been attacked by spyware, but there is no problem. The term 'false positive' can also be used when legitimate anti-spyware applications are mistakenly evaluated as a threat. In addition to this, Professor Steve Grobman said wrong authentication errors can have catastrophic consequences. A good example of this was in a terrifying 23 minutes on September 26, 1983 - at the height of the Cold War's intense climax. A number of international warning centers, including the United States and the Soviet Union, issued high warnings about a lightning strike that shocked the world, but in the end it was just a mistake. true wrong. Specifically, the Soviet Union discovered five US nuclear missiles launched and headed for its territory, immediately instructed to put all armed forces in a state of war readiness. fight. But with the siren and flashing screen, Lieutenant Colonel Stanislav Petrov finally determined that the incident was just an incident from the computer system. Specifically, Petrov argues that the United States will not be able to start a world war by launching only 5 missiles. He ignored the instructions he had been trained and, intuitively, the Lieutenant Colonel correctly judged the situation, contributing to preventing a nuclear war.

'It turns out that the root cause of the incident is the rare association of sunlight on overhead clouds that creates missile-like effects. So we can see just how dangerous the confusion on computer systems is, can even trigger a nuclear war. What if at that time the Soviet Union made immediate response missiles? And the important thing is that we have to be aware of the real power of AI in solving problems, but that will also be a double-edged sword if it's in the hands of the bad guys that are full of online, 'said Steve Grobman. .



1. Supercomputers can completely detect cyber threats

Besides, Grobman also said that he himself believed that technology was essentially an inanimate tool, and it could be applied to both good and bad purposes. For example, a crime map with data on where the crime occurred and where the culprit could be used can help police break the sentence - or it can also be used by the criminal to evade police pursuit. In another example, an airplane was used to bomb civilians, resulting in 2 million casualties during World War II. When asked if he regretted the invention of an aircraft, Orville Wright said in 1948 that he saw it as using fire, which could cause great damage if a fire occurred, but still okay. Use for thousands of important purposes. And so is AI.

'Orville's insight shows us that in essence, technology is inherently irrelevant, it is really thought to be beneficial or harmful depending on the way people use it, and this is also what our industry, cyber security, is constantly fighting! '