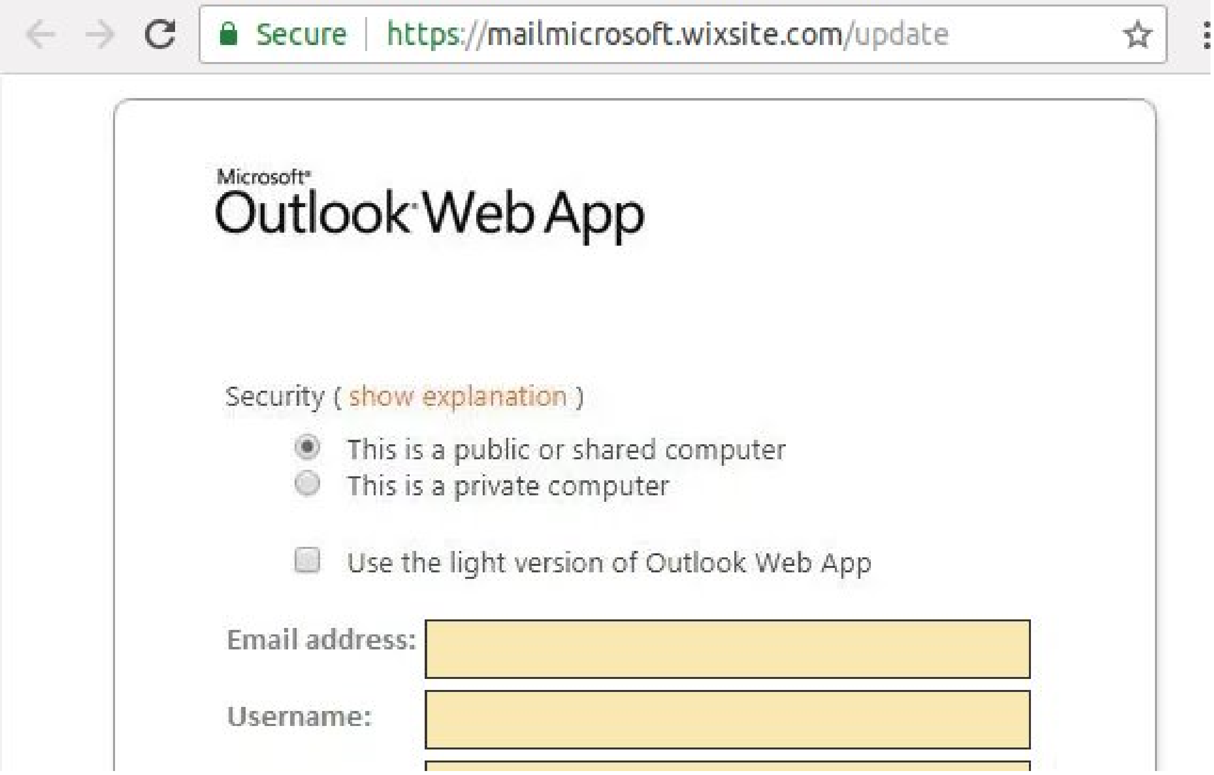
TechXplore

Using deep neural networks to hunt malicious TLS certificates

November 2 2018, by Ingrid Fadelli



Secure | https://mailmicrosoft.wixsite.com/update

Microsoft Outlook Web App

Security (show explanation)

● This is a public or shared computer
○ This is a private computer

□ Use the light version of Outlook Web App

Email address:

Username:

Example of phishing attacks using TLS. Credit: Torroledo, Camacho & Bahnsen

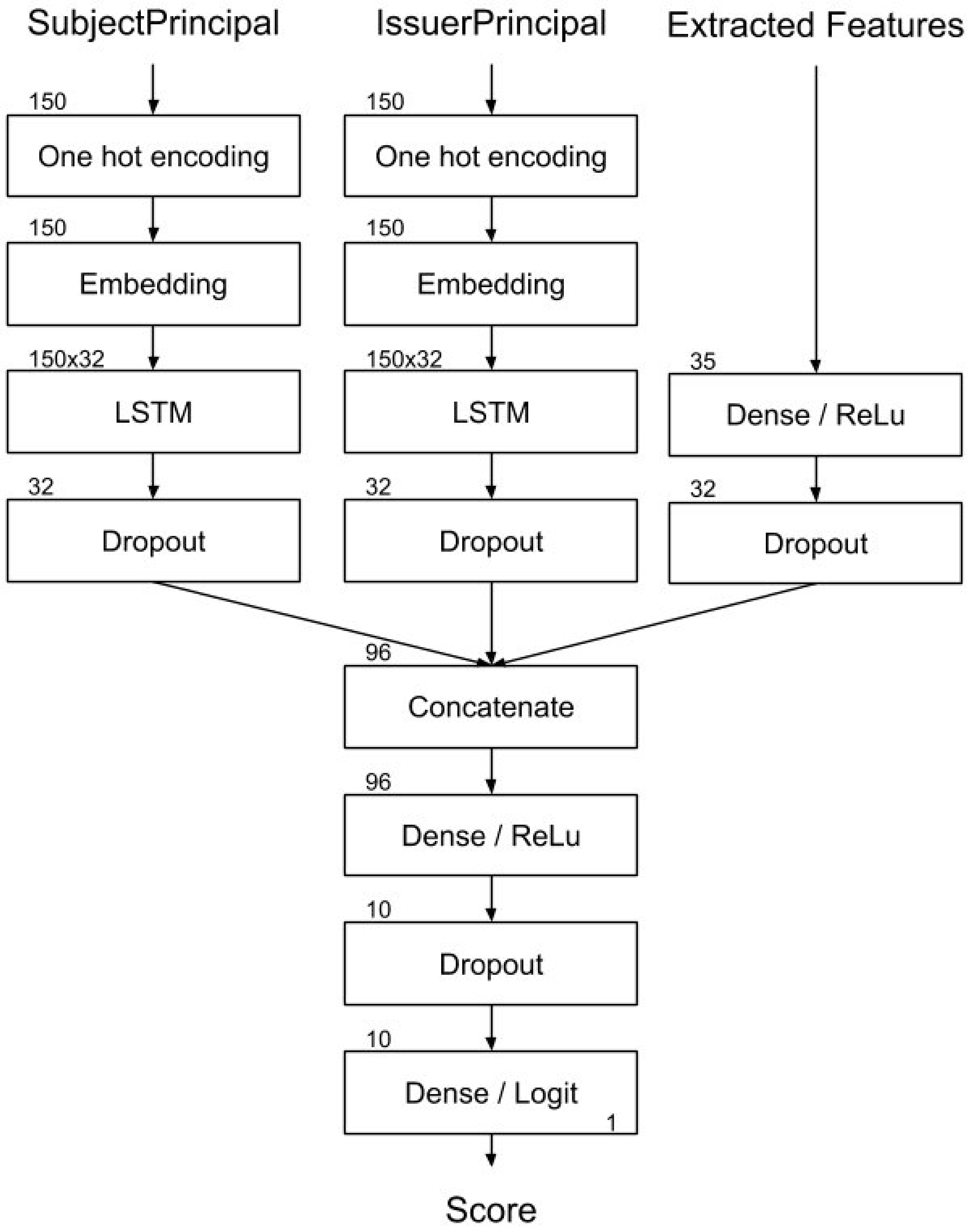
A team of researchers at Cyxtera Technologies has recently proposed a neural network-based method for identifying malicious use of web certificates. Their approach, outlined in a paper published in *ACM Digital Library*, uses the content of transport layer security (TLS) certificates to identify legitimate certificates, as well as malicious patterns used by attackers.

Encryption is an increasingly popular way of securing communications and exchanges of data online so that they cannot be intercepted and accessed by third parties. Despite its many advantages, encryption also allows cybercriminals to hide their messages and avoid detection when carrying out malware attacks.

Moreover, encryption can give online users a false sense of security, as many web browsers display a green lock symbol when the connection to a website is encrypted, even when these websites are actually executing phishing attacks. To address these challenges, researchers are exploring new ways of detecting and responding to malicious online traffic.

"We are seeing an increase in the sophistication of phishing attacks over the last 12 months," Alejandro Correa Bahnsen, one of the researchers who carried out the study, told TechXplore. "In particular, attackers started using web certificates to make end users believe that they are entering a secure website."

As there is currently no way to detect TLS certificates in the wild, the researchers developed a new method to identify the malicious use of web certificates, using deep neural networks. Essentially, their system uses the content of TLS certificates to successfully identify legitimate certificates and malicious ones.

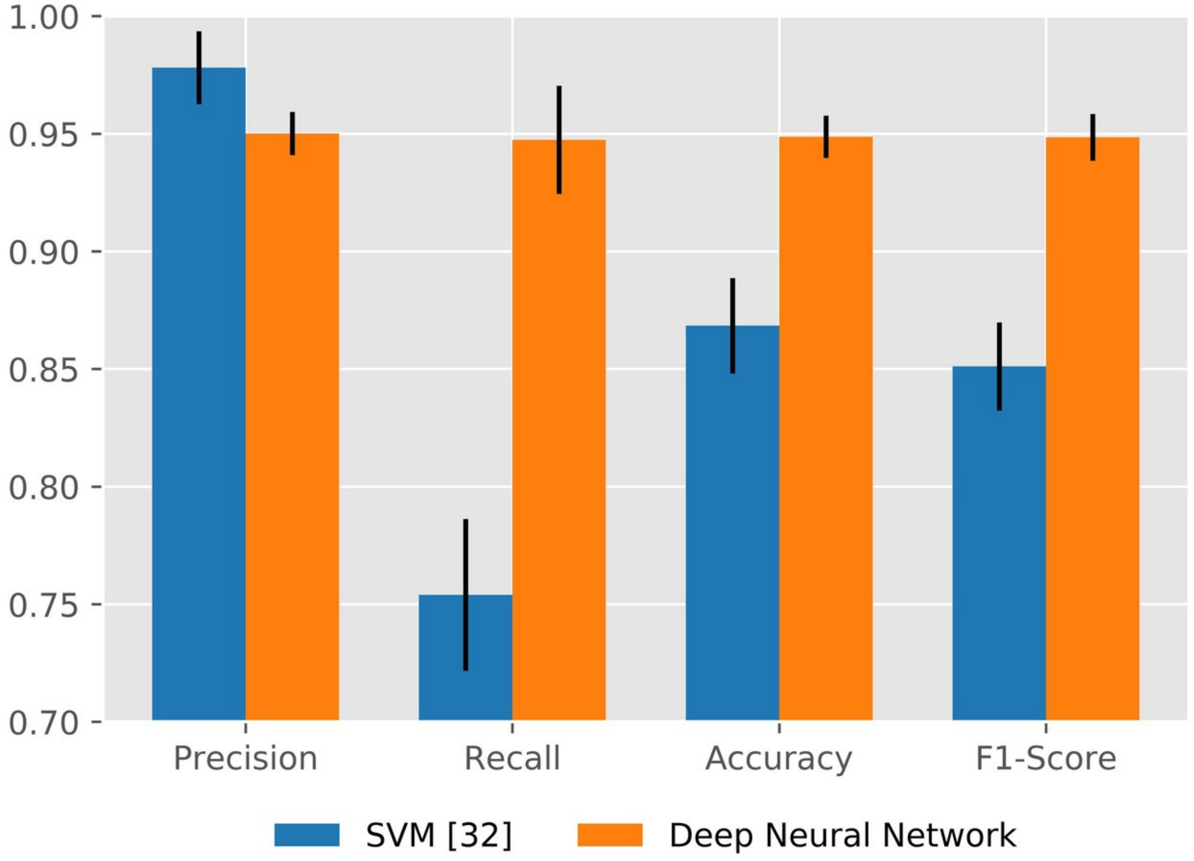


Neural network architecture to classify malicious certificates. Credit: Torroledo, Camacho & Bahnsen

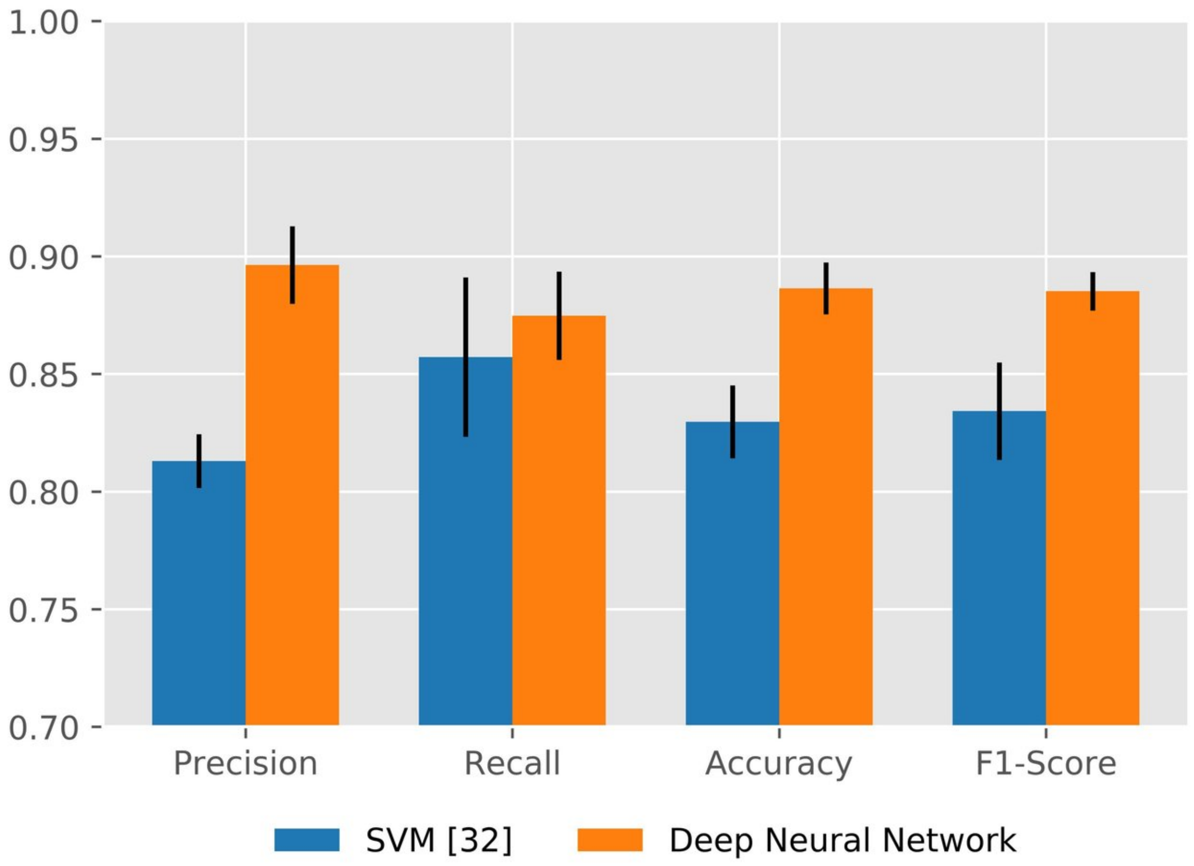
"The use of web certificates by attackers is increasing the efficiency of their attacks, but at the same time, it leaves more traces of their actions," Bahnsen said. "With these additional data points, we created a deep neural network to find hidden malicious patterns in web certificates and use them to predict the legitimacy of a web site."

Bahnsen and his colleagues evaluated their new method and compared it to an existing model, namely Splunk's support vector machines (SVM) algorithm. Their deep neural network used the text information contained in the certificate more effectively than SVM, identifying malware certificates with an accuracy of 94.87 percent (7 percent more than SVM) and phishing certificates with an accuracy of 88.64 percent (5 percent more than SVM).

"Using this methodology, we were able to detect previously undetected phishing web sites," Bahnsen said. "In fact, deep neural networks show the potential to mitigate new strategies deployed by attackers by being able to quickly uncover previously unseen malicious patterns."



Comparison of algorithms performance using support vector machines and deep neural networks for malware classifier. Credit: Torroledo, Camacho & Bahnsen



Comparison of algorithms performance using support vector machines and deep neural networks for phishing classifier. Credit: Torroledo, Camacho & Bahnsen

The study carried out by Bahnsen and his colleagues provides important insight into the potential of deep neural networks for the detection of malware and phishing certificates. In the future, their work could aid the development of more effective tools to safeguard users from the latest strategies employed by attackers.

"We are now going to share this research with the community via open source," Bahnsen said. "This should help researchers to develop the next generation of defenses and combat fraudulent activities."

More information: Ivan Torroledo et al. Hunting Malicious TLS Certificates with Deep Neural Networks, *Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security - AISec '18* (2018). DOI: 10.1145/3270101.3270105

Citation: Using deep neural networks to hunt malicious TLS certificates (2018, November 2) retrieved 20 March 2024 from https://techxplore.com/news/2018-10-deep-neural-networks-malicious-tls.html