

Crowd-sourcing for Detection of Phishing

Disclosure Number

201303021

Technology Summary

This method would allow e-mail providers and organizations to use their own users to classify phishing messages. Though it is likely that some number of users will click on phishing messages, a large percentage of people will not. While unlikely that all of the users that did not click recognized a phishing attempt, it is likely that a significant portion did. In order to take advantage of this awareness, I propose that we provide a method to fingerprint incoming messages in such a way that, when a phishing attempt is reported, an information system can automatically find other similar messages sent to its users. This is crowdsourcing in that we suggest using human input to solve the problem of identifying phishing emails. While this method does not guarantee that users would not click on malicious links, it adds a much need layer of security to the process. This method is not a silver bullet, but it advances the state of the art.

Inventor

RICHARDSON, GREGORY D

Computational Sciences & Engineering Div

Licensing Contact

SIMS, DAVID L

UT-Battelle, LLC

Oak Ridge National Laboratory

Rm 124C, Bldg 4500N, MS: 6196

1 Bethel Valley Road

Oak Ridge, TN 37831

Office Phone: (865) 241-3808

E-mail: SIMSDL@ORNL.GOV

Note: The technology described above is an early stage opportunity. Licensing rights to this intellectual property may be limited or unavailable. Patent applications directed towards this invention may not have been filed with any patent office.