Detection of DNS Tunnels Using Throughput Estimation

Michael Himbeault  
Dept. Electrical & Computer Engineering  
University of Manitoba  
umhimbea@ee.umanitoba.ca

In a world that runs on data, protection of that data and protection of the motion of that data is of the utmost importance. Covert communication channels attempt to circumvent established methods of control, such as firewalls and proxies, by utilizing non-standard means of getting messages between two endpoints. DNS (Domain Name System), the system that translates text-based resource names into resource records, is a very common and effective platform upon which covert channels are often built. This work proposes a novel new technique that estimates data transmission throughput over DNS in order to identify the existence of a DNS tunnel. The proposed technique is robust in the face of the obfuscation techniques that are able to hide tunnels from existing detection methods.

REFERENCES
INSTRUCTIONS

Here are instructions for the GradCon 2012 template (see previous)

Bookman Old Style  --  20 pts
Color:  R=148, G=54, B=52
Paragraph:  Left Justified

Mangal – 8 pts
(any sans-serif is OK)
Paragraph:  Right Justified

Times – 14pts
(OK to BOLD if you want)
Paragraph – Centered

Times – 11 or 12pts
Paragraph -- Centered

Times – 11 or 12pts

Times – 9, 10, or 11 pts
Paragraph:  Hanging paragraph also OK

Times – 9 pts

Calibri -- 9 pts
Paragraph:  Center Justified

Abstract Title

Your name
Dept. Electrical & Computer Engineering
University of Manitoba
Email

Body of Abstract

References

Advisor  --  at the bottom of the page in the footer

Proceedings of the 2012 Graduate Students Conference,
GRADCON 2012
Winnipeg, MB, Canada; October 12, 2012
©Copyright retained by author and collaborators