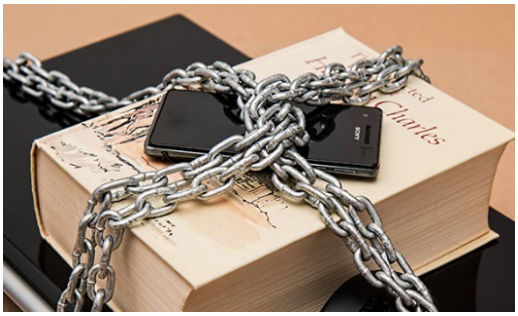

Security Lancaster | Lancaster University

**Institute Seminar**

***Automated Attack Discovery in TCP Congestion Control Using a Model-guided Approach***

*Professor Cristina Nita-Rotaru*
Northeastern University

Date: Jan 29th, 2021
Time: 14:00-15:00
Teams Link: Join Seminar (We'd appreciate if you could optionally register to join our mailing list)

Abstract:
One of the most important goals of TCP is to ensure fairness and prevent congestion collapse by implementing congestion control. Various attacks against TCP congestion control have been reported over the years, most of which have been discovered through manual analysis.

In this talk, we present an automated method that combines the generality of implementation-agnostic fuzzing with the precision of runtime analysis to find attacks against implementations of TCP congestion control. It uses a model-guided approach to generate abstract attack strategies, by leveraging a state machine model of TCP congestion control to find vulnerable state machine paths that an attacker could exploit to increase or decrease the throughput of a connection to his advantage. These abstract strategies are then mapped to concrete attack strategies, which consist of sequences of actions such as injection or modification of acknowledgements and a logical time for injection. We design and implement a virtualized platform, TCPwn, that consists of a a proxy-based attack injector and a TCP congestion control state tracker that uses only network traffic to create and inject these concrete attack strategies. We use TCP New Reno as the guiding abstract model and evaluated 5 TCP implementations from 4 Linux distributions and Windows 8.1. Overall, we found 11 classes of attacks, of which 8 are new.

We also applied a similar technique to BBR, a recent congestion control algorithm proposed by Google that builds a model of the network path consisting of its bottleneck bandwidth and RTT to govern its sending rate rather than packet loss (like CUBIC and many other popular congestion control algorithms). We found 5 classes of attacks causing BBR to send faster, slower or stall. We also found that BBR is immune to acknowledgment burst, division and duplication attacks that were previously shown to be effective against loss-based congestion control such as TCP New Reno.

Biography:
Cristina Nita-Rotaru is a Professor of Computer Science in the Khoury College of Computer Sciences at Northeastern University (since 2015) where she leads the Network and Distributed Systems Security Laboratory (NDS2). Prior to joining Northeastern she was a faculty in the Department of Computer Science at Purdue University (2003 - 2015). She served as Associate Dean of Faculty at Northeastern University (2017 - 2020) and as an Assistant Director for CERIAS at Purdue University (2011 - 2013). Her research lies at the intersection of security, distributed systems, and computer networks. The overarching goal of her work is designing and building secure and resilient distributed systems and network protocols, with assurance that their deployed implementations provide their security, resilience, and performance goals. Her work received several best paper awards in IEEE SafeThings 2019, NDSS 2018, ISSRE 2017, DSN 2015 as well as two IETF/IRTF Applied Networking Research Prize in 2018 and 2016. She is a recipient of the NSF Career Award in 2006.

Cristina Nita-Rotaru has served on the Technical Program Committee of numerous conferences in security, networking and distributed systems (IEEE S&P, USENIX Security, ACM CCS, NDSS, ACM Wisec, IEEE ICDCS, IEEE/IFIP DSN, ACM SIGCOMM, ACM CoNEXT, WWW, PODC, USENIX ATC, EuroSys, ACM SoCC). She has published over 100 articles in peer-reviewed conferences and journals. She was a member of the steering committee of ACM Wisec and is a member of the steering committee of IEEE/IFIP DSN. She was an Associate Editor for Elsevier Computer Communications (2008 - 2011), IEEE Transactions on Computers (2011 - 2014), ACM Transactions on Information Systems Security (2009 - 2013), Computer Networks (2012 - 2014), IEEE Transactions on Mobile Computing (2011 - 2016), and IEEE Transactions on Dependable and Secure Systems (2013 - 2017).

**Please contact Jennifer for any Teams connectivity issues: j.mcculloch@lancaster.ac.uk**