Secure message passing on networks with insecure nodes

Sebastian M. Krause and Vinko Zlatic
Ruder Boskovic Institute, Zagreb, Croatia

Michael M. Danziger
Department of Physics, Bar Ilan University, Ramat Gan, Israel

It is often necessary to transmit a message across a network when parts of the network are not secure. Here, we consider the case of a network partitioned into sets of nodes with the assumption that no single subset can be trusted. As such, the message needs to be divided and transmitted on multiple paths so that no subset sees the entire message. This problem arises, for instance, in a p2p network running different unpatched software versions and when considering AS-level listeners in the entry and exit to the Tor network.

We present a general analysis of this problem on random graphs including analytic solutions for Erdős-Rényiand scale-free networks and numerical simulations confirming our calculations and further numerical tests on real-world networks including the internet, partitioned by AS.

Surprisingly, we find that increased software heterogeneity may actually improve security.

Secure and anonymous communication over networks, in particular the internet, has become a central question facing the global community. In light of widespread state-surveillance, large-scale cybercrime and superbugs like "Heartbleed," one can no longer assume that an entire communications network is secure.

However, the network insecurity may be disjoint. For instance, on a p2p network, there may be different versions of the software running at the same time. In such a case, though there may be unpatched or even undiscovered bugs affecting a given version, it is unlikely that all of the versions will be compromised by the same group at the same time. In such a case, a sensible strategy for secure communication may be to divide the message and transmit it along different paths so that *no single version* receives the entire message.

This problem also arises when attempting to safeguard anonymity with the Tor network [1]. Recent work has shown that if the same autonomous system (AS) controls a router on the path from the source to the entry node of the Tor network and also a router on the path from the exit node to the destination, the identity of source and destination can be deduced from a statistical analysis of the traffic pattern and the anonymity of the Tor network is broken [2]. Since a relatively small number of AS's control the entire internet, this scenario is a serious concern [3].

Here we examine this problem on general network topologies several partitioning rules. We do not consider here the implementation details of such a communication strategy but rather show under what circumstances it would be possible in principle. We begin with a formal definition of the problem and its relationship to percolation theory and then proceed to demonstrate a number of key properties on random graphs and sample measurements on real-world networks, including the AS-level internet.

To analyze this problem, we consider a network for which each node is assigned exactly one color. A pair of nodes is securely connectable iff there exist a set of paths connecting the nodes such that no color appears on all of the paths. To calculate this property we begin by examining color-avoiding connected components. For every color c, the color avoiding component is defined as all nodes which can be reached when the c-colored nodes are removed.

[1] R. Dingledine, N. Mathewson, and P. Syverson, in *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, SSYM'04 (USENIX Association, Berkeley, CA, USA, 2004) pp. 21–21.

[2] S. Murdoch and P. Zieliski, in *Privacy Enhancing Technologies*, Lecture Notes in Computer Science, Vol. 4776, edited by N. Borisov and P. Golle (Springer Berlin Heidelberg, 2007) pp. 167–183.

[3] M. Edman and P. Syverson, in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09 (ACM, New York, NY, USA, 2009) pp. 380–389.