An Analysis of Location-Hiding Using Overlay Networks

Ju Wang (student)
Department of Computer Science and Engineering
University of California, San Diego
jwang@cs.ucsd.edu

Andrew A. Chien (faculty)
Department of Computer Science and Engineering
University of California, San Diego
achien@ucsd.edu

ABSTRACT

Overlay networks have been proposed as a means to achieve application location-hiding. In particular, overlay networks are used as proxies which mediate communication between applications and their users without revealing application IP addresses. The capability to communicate without revealing IP addresses is also known as location-hiding or application hiding, and its essence is indirect communication. This capability can support anonymous communication, protect applications and hosts from direct attacks, and supporting physical infrastructure from Denial-of-Service (DoS) attacks. For example, many researchers [1-4] exploit this location-hiding capability to protect Internet applications from DoS attacks on application's supporting physical infrastructure.

However, fundamental questions about such proxy networks remain unanswered, especially in the presence of intelligent attackers: Can proxy networks achieve location-hiding via indirection? If so, under what circumstances can they stably withstand attacks? How long will it take attackers to penetrate a proxy network and reveal application location?

To shed light on these questions, we develop a generic framework for proxy network approaches to location-hiding, which encompasses most of the proposed approaches. We also develop a stochastic model to characterize the dynamic behavior of the system — exploring in particular how attacks, defense mechanisms and correlated host vulnerabilities affect stability (the ability to resist an attack). Based on this framework and model, using theoretical analysis combined with simulation techniques, we analyze the behavior of proxy network systems and characterize when location hiding is feasible and when it is not.

We focus on classes of attacks that exploit the connection structure of the proxy networks, and use directed penetration in an attempt to reveal the application's hidden location. Such attacks focus on elements that are present in all proxy network approaches.

Our specific research contributions include:

- design of a generic framework and analytic model for proxy network approaches to location-hiding,
- based on the model, we characterize several fundamental properties of the proxy network-based location-hiding, showing that existing approaches employing static structure against host compromise attacks are infeasible,
- based on the model, proxy-network-based location-hiding can be successful if it includes proactive defenses employing proxy network reconfiguration and migration. The proxy network depth and reconfiguration rates are the critical factors for achieving the effectiveness.
- using simulation techniques, we explore cases where host vulnerabilities are correlated, showing that in many cases this distinction makes proxy-based location-hiding infeasible.
- finally, we show that with intelligent exploitation, only limited host (OS/software) diversity is needed to mitigate the negative impact of correlated vulnerabilities and location-hiding can be achieved.

These results provide both deeper understanding of the location-hiding problem and guidelines for proxy network design. The generic framework provides a foundation to understand proxy networks' capability of location-hiding, to formally analyze the behavior of such systems, to rigorously reason about how proxy networks should be designed, and serves as a foundation for future studies employing more complex and realistic models.

References

1. Adkins, D., et al., *Towards a More Functional and Secure Network Infrastructure*. 2003, Computer Science Division, UC Berkeley: Berkeley.
2. Adkins, D., et al. *Taming IP Packet Flooding Attacks*. in *HotNets-II*. 2003.
3. Andersen, D.G. *Mayday: Distributed Filtering for Internet Services*. in *4th Usenix Symposium on Internet Technologies and Systems*. 2003. Seattle, Washington.
4. Keromytis, A.D., V. Misra, and D. Rubenstein. *SOS: Secure Overlay Services*. in *ACM SIGCOMM'02*. 2002. Pittsburgh, PA: ACM.

Related publication and project information can be found at http://www.cs.ucsd.edu/~jwang/