

Research Statement

Alper T. Mizrak
University of California, San Diego
January 2007

1 Introduction

As distributed computing becomes ubiquitous, reliability, security, and fault-tolerance requirements have become more important for modern distributed systems. All applications are increasingly based on networks, yet the Internet is not a safe place. Unsecured hosts can expect to be compromised within minutes of connecting to the Internet and even well-protected hosts may be crippled with denial-of-service attacks. However, while such threats to host systems are widely understood, it is less well appreciated that the network infrastructure itself is subject to constant attack as well.

I have been interested in a simply stated, yet increasingly important network security problem: *how to detect the existence of compromised routers in a routing system and remove them from the routing fabric.*

Throughout my Ph.D. track, I have studied different aspects of this problem combining science and engineering. In collaboration with my advisors, I have specified the problem of detecting routers with incorrect packet forwarding behavior on the abstract level, provided a general framework for the protocols addressing this problem, explored the design space of protocols that implement such a detector, developed various such protocols, implemented and evaluated prototype systems, which are inexpensive enough for practical implementation at scale.

2 Research

I have motivated the problem of detecting routers with incorrect packet forwarding behavior and presented a general framework for the protocols addressing this problem in a position paper [FuDiCo 2004] and a brief announcement [PODC 2004]:

Network routers occupy a unique role in modern distributed systems. By manipulating, diverting, or dropping packets arriving at a compromised router, an attacker can trivially mount denial-of-service, surveillance, or man-in-the-middle attacks on end host systems. Consequently, Internet routers have become a choice target for would-be attackers and thousands have been subverted to these ends. Such attacks are not simply theoretically feasible, but are practiced today. Attackers have repeatedly demonstrated their ability to compromise routers, either by exploiting weak passwords or latent software vulnerabilities, and standard built-in commands are sufficient to drop or delay packets without requiring any modification to the router's code base. Moreover, several widely published documents provide a standard cookbook for transparently "tunneling" packets from a compromised router through an arbitrary third-party host and back again – effectively amplifying the attacker's abilities to including arbitrary packet sniffing, injection or modification. Such attacks can be extremely difficult to detect manually, and it can be even harder to isolate which particular router or group of routers has been compromised.

The problem of detecting and removing compromised routers can be thought of as an instance of anomalous behavior-based intrusion detection: a compromised router can potentially be identified

by correct routers when it deviates from exhibiting expected behavior. This overall approach can be broken into three distinct subproblems:

1. Traffic validation. Traffic information is the basis of detecting anomalous behavior: given traffic entering a part of the network, and an expected behavior for the routers in the network (i.e., a known routing configuration), anomalous behavior is detected when the monitored traffic leaving one part of the network differs significantly from what is expected. However, implementing such validation practically can be quite tricky and requires tradeoffs between the overhead of monitoring, communication, and accuracy.
2. Distributed detection. It is impossible for a single router to establish that its neighbor is anomalous. Thus, detection requires synchronizing a collection of traffic information and distributing the results so anomalous behavior can be detected by *sets* of correct routers.
3. Response. Once a router, or set of routers, is thought to be faulty, the forwarding tables of correct routers must be changed to avoid using those compromised nodes. In addition, over longer time scales an appropriate alert must be raised so human forensic experts can respond appropriately.

The initial results are presented in [TR 2004]. I have specified the problem on the abstract level and developed a formal specification for such a detector with properties similar to those used for traditional failure detectors. Furthermore, I have explored the design space of protocols that implement such a detector and developed two concrete protocols that differ in accuracy, completeness, and overhead - one of which is likely inexpensive enough for practical implementation at scale.

The main results are published as a regular paper [DSN 2005]. For different threats, I have explored a range of appropriate and efficient traffic validation functions and examined how those can be used to build an anomalous behavior detector for compromised routers. Finally, I have implemented a prototype system, **Fatih**, that is inexpensive enough for practical implementation at scale and can automatically isolate network paths demonstrating anomalous behavior. This work is an important step in being able to tolerate attacks on key network infrastructure components. This paper was recognized with the **William C. Carter Award** [Carter 2005].

The manuscript [IEEE TDSC 2006] is a significantly extended version of [DSN 2005]. I have developed a new distributed detection protocol that has theoretical interest (it is optimal) and derived proofs of correctness of the distributed detection protocols. A detailed description of the prototype system and a thorough evaluation are given with insights into the results of experimentation with it.

Finally, in the paper [DSN 2007 submitted], which is under review, I have designed, developed and implemented a new compromised router detection protocol that dynamically infers the precise number of congestive packet losses that will occur. Unfortunately, it is quite challenging to attribute a missing packet to a malicious action because normal network congestion can produce the same effect. Modern networks routinely drop packets when the load temporarily exceeds a router's buffering capacity. Previous detection protocols have tried to address this problem using a user-defined threshold: too many dropped packets implies malicious intent. However this heuristic is fundamentally unsound; setting this threshold is, at best, an art and will necessarily create unnecessary false positives or mask highly-focused attacks. Once the congestion ambiguity is removed, subsequent packet losses can be safely attributed to malicious actions. This protocol

is the first to automatically predict congestion in a systematic manner and is necessary for making any such network fault detection practical.

3 Conclusion and Future Directions

Over the course of my Ph.D. study, I have studied different aspects of this problem and gained general research expertise as an independent researcher: I have been trained, first, to identify, abstract, specify and formalize a problem; second, to develop protocols implementing various specifications; and then to build up a complete system including distributed computing, kernel programming, network routing protocols, traffic shaping. Furthermore, I am experienced in testing and evaluating the distributed systems using network simulators(ns2) and network emulation testbeds(Emulab, Deterlab).

In the future, I believe that computer systems will be more distributed and networked, and so reliability, security, and fault-tolerance requirements will become more vital. I expect that the know-how and expertise that I have gained over the course of my dissertation research will help me in studying these aspects of the distributed systems further and applying these ideas to other applications and systems.

References

- [FuDiCo 2004] Alper Tugay Mizrak, Keith Marzullo, and Stefan Savage. Fault-tolerant forwarding in the face of malicious routers. Workshop on the Future Directions in Distributed Computing, 2004.
- [PODC 2004] Alper Tugay Mizrak, Keith Marzullo, and Stefan Savage. Brief announcement: Detecting malicious routers. In Proceedings of the twenty-third annual ACM symposium on Principles of Distributed Computing, page 369. ACM Press, 2004.
- [TR 2004] Alper Tugay Mizrak, Keith Marzullo, and Stefan Savage. Detecting malicious routers. Technical Report CS2004-0789, UCSD, May 2004.
- [DSN 2005] Alper Tugay Mizrak, Yu-Chung Cheng, Keith Marzullo, and Stefan Savage. Fatih: Detecting and isolating malicious routers. In DSN 05: Proceedings of the 2005 International Conference on Dependable Systems and Networks, pages 538-547, Washington, DC, USA, 2005. IEEE Computer Society.
- [Carter 2005] W.C. Carter Award. In DSN 05: Proceedings of the 2005 International Conference on Dependable Systems and Networks, page xxiii, Washington, DC, USA, 2005. IEEE Computer Society.
- [IEEE TDSC 2006] Alper Tugay Mizrak, Yu-Chung Cheng, Keith Marzullo, and Stefan Savage. Detecting and isolating malicious routers. IEEE Transactions on Dependable and Secure Computing, 3(3):230-244, Jul-Sep 2006.
- [DSN 2007 submitted] Alper Tugay Mizrak, Keith Marzullo, and Stefan Savage. Detecting malicious packet losses. International Conference on Dependable Systems and Networks, 2007.