How vulnerable is your prefix? Assessing IP Prefix Hijackability

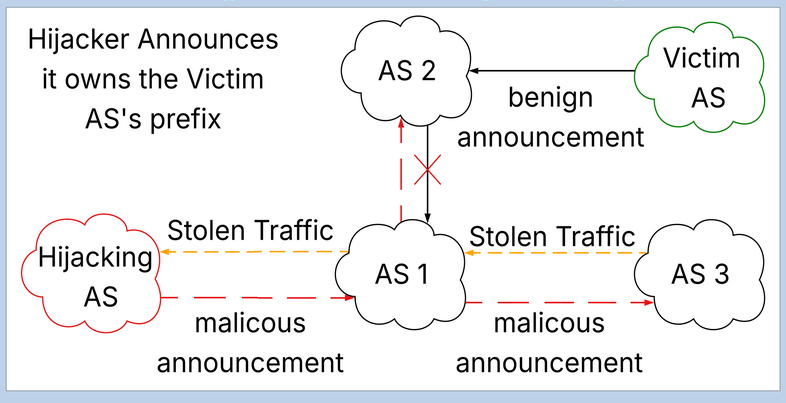
Nate Balmain & Jun Li (advisor)
Center for Cyber Security and Privacy

Chuck Fleming, Cisco

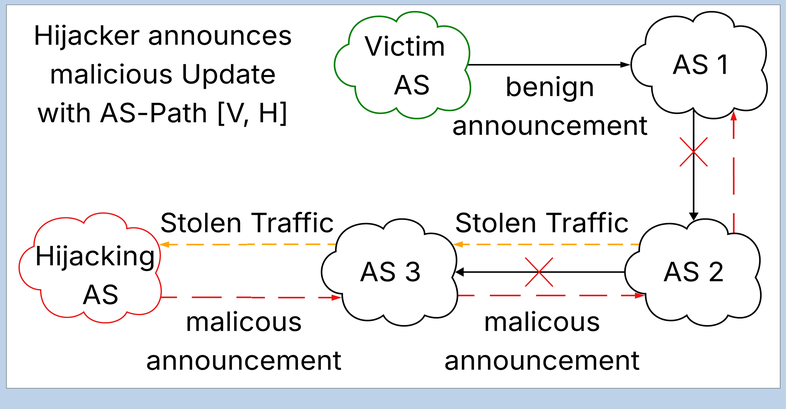
Introduction

- Autonomous Systems (ASes) on the Internet use Border Gateway Protocol (BGP) to exchange reachability information of IP address blocks, a.k.a. IP prefixes
- Malicious ASes can advertise an IP prefix that is not theirs (origin-based hijacking), or a path to a victim prefix that is short (path-based hijacking), causing IP prefix hijacking
- The Internet, as of today, is still vulnerable to IP prefix hijacking, which can lead to denial of Internet service or theft of information
- This research studies how likely an IP Prefix may be hijacked by an arbitrary hijacker

Origin-Based Hijacking



Path-Based Hijacking

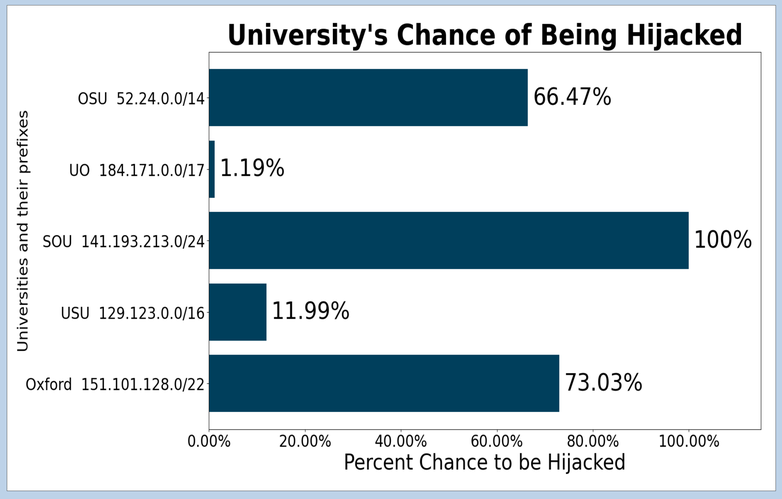


Methodology

- This study can investigate the hijackability of **any** IP prefix on the Internet

1. Select many BGP peers of RouteViews and RIPE Update Collectors as the observer to a BGP Hijack
2. Select a set of candidate hijackers for the target prefix from:
   - The vicinity of the victim prefix
   - The vicinity of each observer
   - A random point on the internet
3. For each observer and each hijacker inject fabricated hijacking updates into the observer that could occur if an AS turns malicious
4. Check how often the observer will adopt hijacking updates instead of benign updates

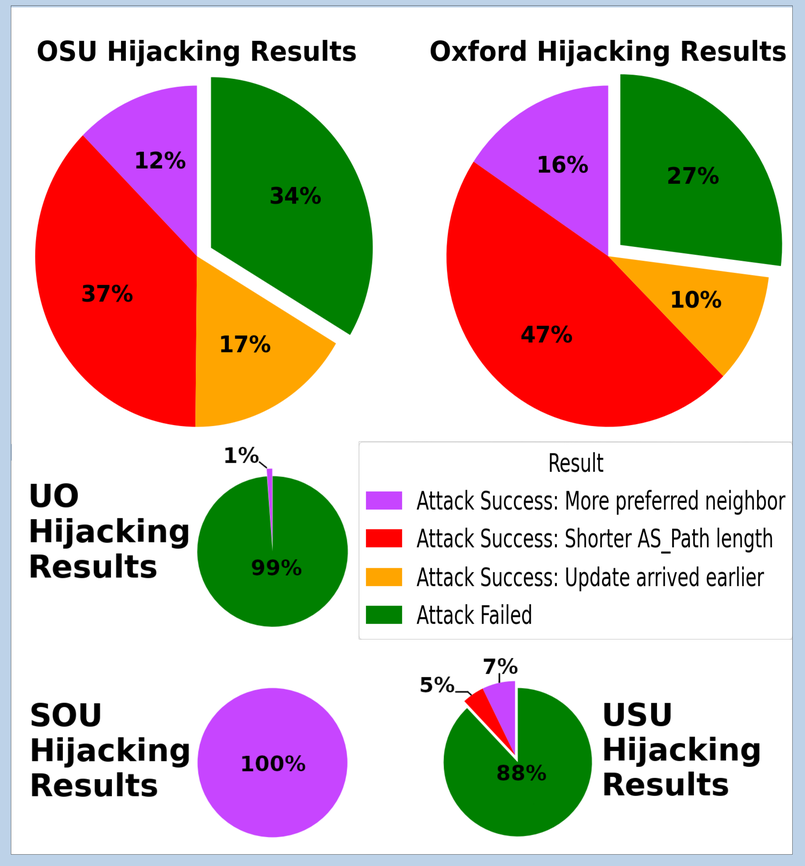
Results



From the perspective of 5 observing ASes

Analysis

- The observer always hears the hijacker's announcement from its most preferred neighboring AS
- Hijacks using a more preferred neighbor AS will **always succeed**
- UO remained relatively safe mostly due to hearing benign announcements
  - along a shorter AS Path or,
  - from the most preferred neighboring AS



Acknowledgments

This research was sponsored in part by Cisco