Network Forensics:
Network OS Fingerprinting
Prefix Hijacking Analysis

Scott Hand

September 30th, 2011
<table>
<thead>
<tr>
<th>1</th>
<th>Network Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introduction</td>
</tr>
<tr>
<td></td>
<td>OS Fingerprinting</td>
</tr>
<tr>
<td>2</td>
<td>Prefix Hijacking Theory</td>
</tr>
<tr>
<td></td>
<td>BGP Background</td>
</tr>
<tr>
<td></td>
<td>Prefix Hijacking Basics</td>
</tr>
<tr>
<td></td>
<td>Hijacking Analysis</td>
</tr>
<tr>
<td></td>
<td>Interception Analysis</td>
</tr>
<tr>
<td>3</td>
<td>Prefix Hijacking Forensics</td>
</tr>
<tr>
<td></td>
<td>Internet Vulnerability Assessment</td>
</tr>
<tr>
<td></td>
<td>Internet Traffic Interception</td>
</tr>
<tr>
<td></td>
<td>Detecting Ongoing Interception</td>
</tr>
<tr>
<td></td>
<td>Detecting Ongoing Hijacking with OS Fingerprinting</td>
</tr>
<tr>
<td>4</td>
<td>Concluding Remarks</td>
</tr>
</tbody>
</table>
Outline

1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
Introduction

What is network forensics?
Introduction

1. What is network forensics?
2. What areas will we focus on today?
Outline

1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
OS Fingerprinting Basics

What is it?
OS fingerprinting aims to gather information about a target host to eventually determine the operating system that the machine is running.

Why?
Penetration testing is one of the most common motivations for determining a host’s OS. Once the OS is known, testers can take a make more focused and directed attempt at penetrating the system.
Some OS Fingerprinting Techniques

Direct Banner Grabbing

Basic, easy form of OS fingerprinting, but often efficient and reliable. One simply connects to the host via `telnet` or `http` and looks for any printed messages detailing the system’s operating system.
Some OS Fingerprinting Techniques

Direct Banner Grabbing
Basic, easy form of OS fingerprinting, but often efficient and reliable. One simply connects to the host via `telnet` or `http` and looks for any printed messages detailing the system’s operating system.

Indirect Banner Grabbing
Information is leaked about a system from sources such as received emails (in the header information or virus scanner tagging) or the `sysit` command in FTP that reveals a family of operating systems. Other examples include examining programs such as `ls` and `grep`. 
TCP Fingerprinting

Each operating system reacts differently to normal and special crafted TCP packets. In particular, the flags header field contains six flags (URG, ACK, PSH, RST, SYN, FIN) that can be used to differentiate operating system behavior.
Some OS Fingerprinting Techniques

TCP Fingerprinting
Each operating system reacts differently to normal and special crafted TCP packets. In particular, the flags header field contains six flags (URG, ACK, PSH, RST, SYN, FIN) that can be used to differentiate operating system behavior.

ICMP Fingerprinting
A similar approach can be taken using ICMP packets. The relevant field to vary is the Type field, a one byte field at the beginning of the header.
Automated Fingerprinting Tools - nmap

1. First sends an ICMP ping request then connects to port 80 to see if the target is responding.
2. A port scan is performed, identifying at least one open and one closed port.
3. nmap sends several crafted packets and records the replies.
   1. A packet is sent with only the SYN flag set.
   2. A packet is sent with no flags set. This is often called the null scan.
   3. A packet is sent with URG, PSH, SYN, and FIN set. This is often called the "christmas tree" packet.
4. nmap compares replies against an OS detection fingerprint file.
Automated Fingerprinting Tools - Xprobe2

- A GNU tool that utilizes ICMP packets rather than TCP packets.
- Utilizes modules to easily adopt new probes.
- A configuration file contains lists of operating systems along with replies to expect for the different type flag settings.
- Basically just your average ping sweeper.
Outline

1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
Basic Information

Other Names
- IP Hijacking
- BGP Hijacking
- Route Hijacking

Target and Scope
- Targets Application Layer protocol BGP (Border Gateway Protocol)
- Deals with service providers and large private networks
- Can black hole or intercept large amounts of internet traffic
Internet is a connected set of Autonomous Systems (AS)

AS Types
- Backbone Providers
- Regional Providers
- Customers

BGP aims to decentralize Internet by connecting ASes
Border Gateway Protocol

Problems

- We must find loop-free paths to destination
- This means traveling through ASes with their own set of policies

The way BGP handles these...

- Have designated border routers
- Advertise a possible route to destination to other routers
- Cache answers given by other routers and use those for future questions
Some Observations on BGP

Strengths

- Decentralized
- Doesn’t care about network topology
- Distributed and efficient

Exploitable?

YES.

- Relies on border routers trusting one another.
- Some ideas:
  1. If ISP trusts me as a user, advertise whatever I want!
  2. If ISP filters EBGP traffic, man-in-the-middle attack their BGP TCP communications.
Outline

1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
     - Hijacking Analysis
     - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
What do we want to achieve?

So we are AS X, and AS Y sends a path query to destination $p$. We know the next step is the prefix owner, AS O. The legitimate response illustrated here is to tell AS Y to send traffic to AS O. What else can we tell AS Y?
Tell AS Y to that route is [X]. We can now grab all traffic send to AS O.

**Some Remarks on This Approach**

- Very easy to accomplish. Happens accidentally when an ISP’s border router has corrupted routing table.
- Not very sneaky.
Tell AS Y that route is [X,O]. Forward traffic to AS O.

Some Remarks on This Approach
- Difficult. We’ll cover some problems shortly.
- Can be maintained discreetly much longer.
Fraudulent Advertisements Specificity

1. Advertise an invalid route for an existing routable prefix. Already covered.

2. Advertise a more specific prefix and thus grab all the traffic to that prefix. Problem: Not interceptable because you can’t route it onto the prefix owner.

3. Advertise a less specific prefix and get traffic when the owner stops advertising. Problem: Not very efficient and still impossible to forward.

We will focus on the first method.
1 Network Forensics
   - Introduction
   - OS Fingerprinting

2 Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3 Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4 Concluding Remarks
To judge the viability of several types of hijacking attempts, the following assumptions are made regarding ISP routing:

**Back Propagation**

The route advertised by AS X will propagate back towards AS Y. Some ISP filtering methods could prevent this, as could some difficulties that we will address. This can be verified in practice by recursively examining each AS in the route between X and Y.

**Routing Preference**

The ISP makes the following preference when routing traffic: Customer > Peer > Provider.
Types of Routing Attacks

With these assumptions, we can divide possible attack attempts into the following groups:

1. Existing route is Customer Route
   1. Invalid route is Customer Route
   2. Invalid route is Peer Route
   3. Invalid route is Provider Route

2. Existing route is Peer Route
   1. Invalid route is Customer Route
   2. Invalid route is Peer Route
   3. Invalid route is Provider Route

3. Existing route is Provider Route
   1. Invalid route is Customer Route
   2. Invalid route is Peer Route
   3. Invalid route is Provider Route
Existing Customer Route

Will traffic be hijacked...

1. ...after change to invalid Customer Route? **Maybe**
Existing Customer Route

Will traffic be hijacked...

1. ...after change to invalid Customer Route? **Maybe**
   The router will use a number of factors, including path length, policies, and distance heuristics, to decide the path to take. Therefore, this will work on some routers and not on others.

2. ...after change to invalid Peer Route? **No**
Will traffic be hijacked...

1. ...after change to invalid Customer Route? **Maybe**
   The router will use a number of factors, including path length, policies, and distance heuristics, to decide the path to take. Therefore, this will work on some routers and not on others.

2. ...after change to invalid Peer Route? **No**

3. ...after change to invalid Provider Route? **No**
Existing Peer Route

Will traffic be hijacked...

1. ...after change to invalid Customer Route? Yes
Existing Peer Route

Will traffic be hijacked...

1. ...after change to invalid Customer Route? Yes
2. ...after change to invalid Peer Route? Maybe
Existing Peer Route

Will traffic be hijacked...

1. ...after change to invalid Customer Route? \textbf{Yes}
2. ...after change to invalid Peer Route? \textbf{Maybe}
3. ...after change to invalid Provider Route? \textbf{No}
Existing Provider Route

Will traffic be hijacked...

1. ...after change to invalid Customer Route? \textit{Yes}
Existing Provider Route

Will traffic be hijacked...

1. ...after change to invalid Customer Route? **Yes**
2. ...after change to invalid Peer Route? **Yes**
Existing Provider Route

Will traffic be hijacked...

1. ...after change to invalid Customer Route? Yes
2. ...after change to invalid Peer Route? Yes
3. ...after change to invalid Provider Route? Maybe
Outline

1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
Why the need for further analysis?

Interception carries some of its own problems.

**Goal**

Safety condition - None of the ASes along the route to prefix $p$ used by the hijacking AS should choose the invalid route advertised by it (if they do receive the invalid route) over their existing route to $p$. 
Illustrated Problem

How we want things to be:

A → B → C (p)

X → Y → Z
Illustrated Problem

How things are:

A \rightarrow B
B \rightarrow C (p)
C (p) \rightarrow Z
X \rightarrow Y \rightarrow Z
Some more assumptions

Routing Preference
Again, assume ISPs prefer customers to peers to providers when making routing decisions.

Valley-free Property
We can assume that once traffic makes a route towards a more highly preferred AS, it will never prefer a route to a less preferred AS tier. Example: Once in a peer AS, traffic will not take a provider route if possible.

Let’s examine some consequences of advertising an invalid path...
Advertising any invalid route will be safe.

**Reasoning**

It is safe to assume that all further routes are routes of strictly lower tiers by the Valley-free assumption, and as a result it is a safe assumption that the route will not jump back up to AS X.
Advertising any invalid route will not always be safe.

Reasoning

It is possible that every part of the route after X will be moving down to peer and then customer, but it is possible that the first edge could be to a higher tier AS (a provider). In this case, either the invalid or existing route could be preferred by the providers, peers, and clients on the route. This breaks the safety assumption.
Outline

1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
Outline

1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
How likely is this given existing network infrastructure?

First, we focus on hijacking by tier-1 ASes for the following reasons:

1. They have no providers. Therefore, interception is safe.
2. Many tier-1 ASes have publicly available policies.

**Approach**

Examine the 7 tier-1 ASes with routes in the Route-Views repository. Estimate how many of those routes would be vulnerable to a routing attack by another tier-1 AS. Focus on top 100 sites, as many belong to a very limited set of ASes.
Results

![Graph showing hijacking probability for Tier-1 ASes:]

Scary. This has happened before when Cogent (AS174) hijacked Google’s prefix.
Other tiers

Comments

This is also pretty scary. There are lowered chances of hijacking prefixes with increasingly smaller ASes, but even 5 to 20% of the most popular prefixes could be devastating.
Hands-on Experiment

History
There have been recorded instances of prefix hijacking, but none of the proposed interception. Can it be done?

Method
The authors (Ballani, Francis, Zhang) decided to do a proof of concept. How did they simulate this attack?
Method

1. Five geographically distinct sites were set.
Method

1. Five geographically distinct sites were set.
2. Router software peered with different ISPs from the different sites.
Method

1. Five geographically distinct sites were set
2. Router software peered with different ISPs from the different sites
3. They analyzed the network structure and came to the conclusion that traffic was a provider path and therefore safe.
Method

1. Five geographically distinct sites were set.
2. Router software peered with different ISPs from the different sites.
3. They analyzed the network structure and came to the conclusion that traffic was a provider path and therefore safe.
4. Traffic was analyzed by pointing a domain name to their target prefix. Queries to it give a percent of traffic received at the site.
Method

1. Five geographically distinct sites were set.
2. Router software peered with different ISPs from the different sites.
3. They analyzed the network structure and came to the conclusion that traffic was a provider path and therefore safe.
4. Traffic was analyzed by pointing a domain name to their target prefix. Queries to it give a percent of traffic received at the site.
Results

**Traffic hijacked**
This ranged between 66% and 97.4%.

**Traffic intercepted**
This ranged between 23.4% and 78.8%.

**Comments**
This was a successful proof of concept and about what was expected from a low level AS. Methods described could be used by ISPs to intercept traffic. Not so good.
1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
**Attempt**

- The authors attempted to detect if any interception was currently being done.
- The method was complicated and did forensics on past routing tables by using the archived routing tables for simulated IP traceroutes.
- The results were inconclusive and neither detecting nor ruled out ongoing interception.
Outline

1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
The Need for Fast Detection

- While detecting interception was shown to be difficult by the previous attempt, it is still important to focus at detecting more general forms of hijacking.
- As insidious as interception is, black holing traffic is also extremely dangerous and needs to be dealt with as soon as possible.
Observations We Can Make

- Paths to a prefix might differ, but should all reach the same host.
- In the event of a hijacking pretending to be the source, we should look for inconsistency.
- Is this possible?
Observations We Can Make

- Paths to a prefix might differ, but should all reach the same host.
- In the event of a hijacking pretending to be the source, we should look for inconsistency.
- Is this possible? Yes. We showed previously that no hijacking method is perfect, especially not at the lower level tiers available to most attackers.
Outline

1. Network Forensics
   - Introduction
   - OS Fingerprinting

2. Prefix Hijacking Theory
   - BGP Background
   - Prefix Hijacking Basics
   - Hijacking Analysis
   - Interception Analysis

3. Prefix Hijacking Forensics
   - Internet Vulnerability Assessment
   - Internet Traffic Interception
   - Detecting Ongoing Interception
   - Detecting Ongoing Hijacking with OS Fingerprinting

4. Concluding Remarks
Any questions?
Ballani, Hitesh and Francis, Paul and Zhang, Xinyang

*A study of prefix hijacking and interception in the internet.*

Hu, Xin and Mao, Z. Morley

*Accurate Real-time Identification of IP Prefix Hijacking.*

Nostromo

*Techniques in OS-Fingerprinting*