Identifying and Reducing Private DNS Updates

CAIDA/WIDE Workshop

Speaker: Hao Shang

Date: March. 17th, 2006

Outline

- Motivation
- Background of RFC1918 updates
- Magnitude of RFC1918 updates
- Identification of OSes producing the RFC1918 updates
- Methods to avoid/reduce RFC1918 updates
- Summary

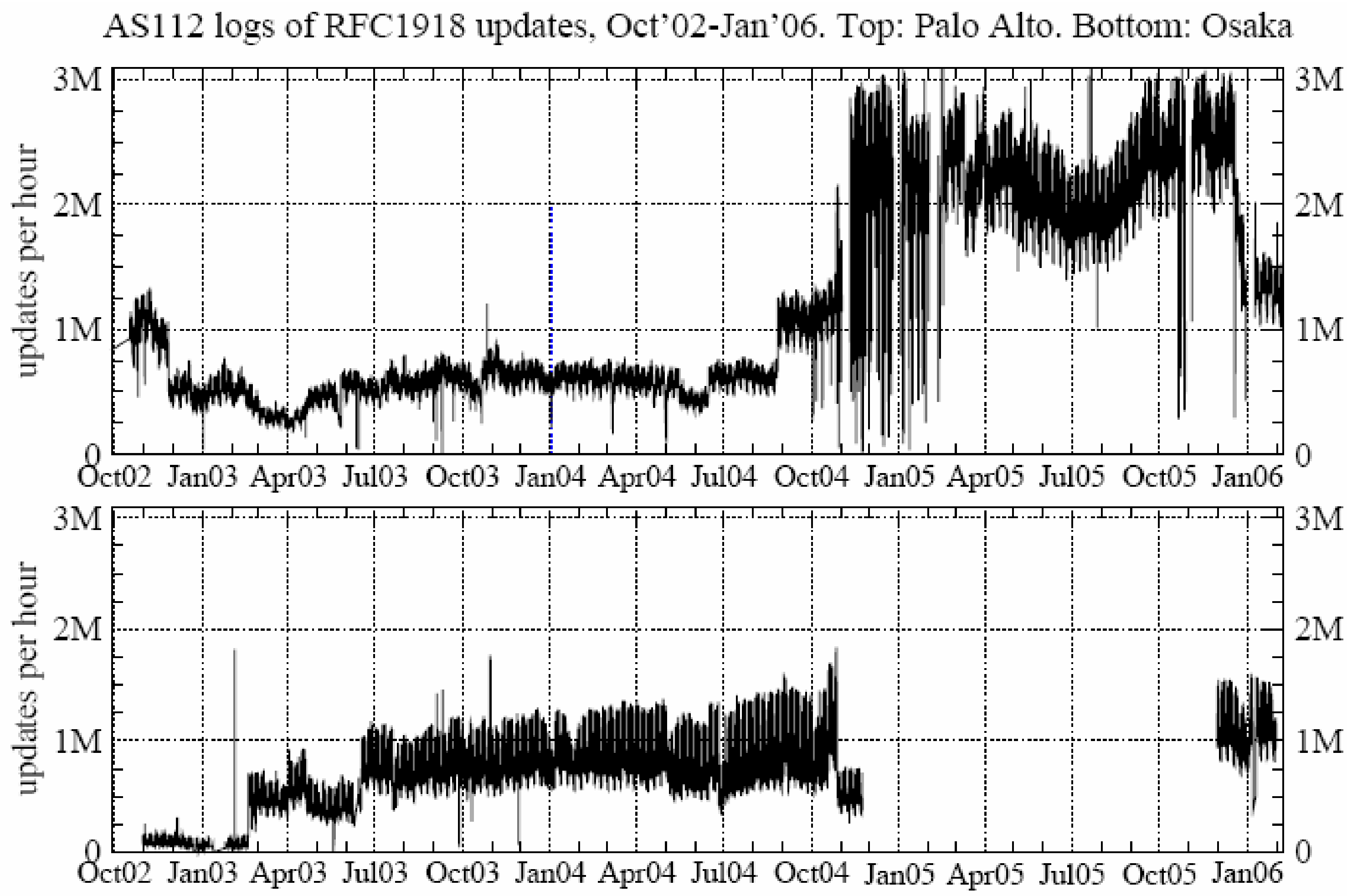
Motivation

- CAIDA's previous work reveals that lots of DNS updates for private (RFC1918) addresses hit AS112 servers
- Harms caused by these updates
  - Waste of bandwidth: up to 15Mbps in one link
  - Require creation and maintenance of AS112 servers
  - Risks to user's privacy and security
- Purpose of this study
  - Quantify, identify, and reduce RFC1918 updates

Background

- RFC1918
  - Allocates 3 blocks of private IP space
- RFC2131(DHCP)
  - Assigns IP addresses dynamically
  - Makes it hard to keep IP↔Name mappings current
- RFC2136(DDNS)
  - Allows dynamic updates of IP↔Name mappings at DNS servers
  - Consolidated with secure features (RFC2930, 3645)
- Problem?
  - Configuration inconsistency between DNS and DHCP server/client causes leaking of RFC1918 updates to public
  - Countermeasure: AS112 project

Magnitude of RFC1918 updates – General View (UDP Updates)



Magnitude of RFC1918 Updates – Observations

- Large amount of UDP updates at the level of millions/hour
  - Inbound packets are about 10 times more if also include TCP
- High diversity of IP sources
  - RFC1918 updates is a global phenomenon
- Abrupt jumps/drops at the number of updates are caused by route changes rather than OS evolution:
  - Proportional changes of unique IP addresses, prefixes, and ASes
  - Changes happened in seconds

Identification of OSes of RFC1918 Updates – Signature Techniques

- Application-level:
  - TCP TKEY message: query name, algorithm, key, RR location
  - UDP update: RR counts, location, types, TTL
  - Able to distinguish different flavors of Windows
- Transport-level:
  - Using a well-know software p0f
  - TCP SYN packet: window size, flags, options
  - Windows and non-windows split only
- Network-level:
  - TCP and UDP: TTL
  - Windows and non-windows split only

Identification of OSes of RFC1918 Updates – Data and Results

- Data description:

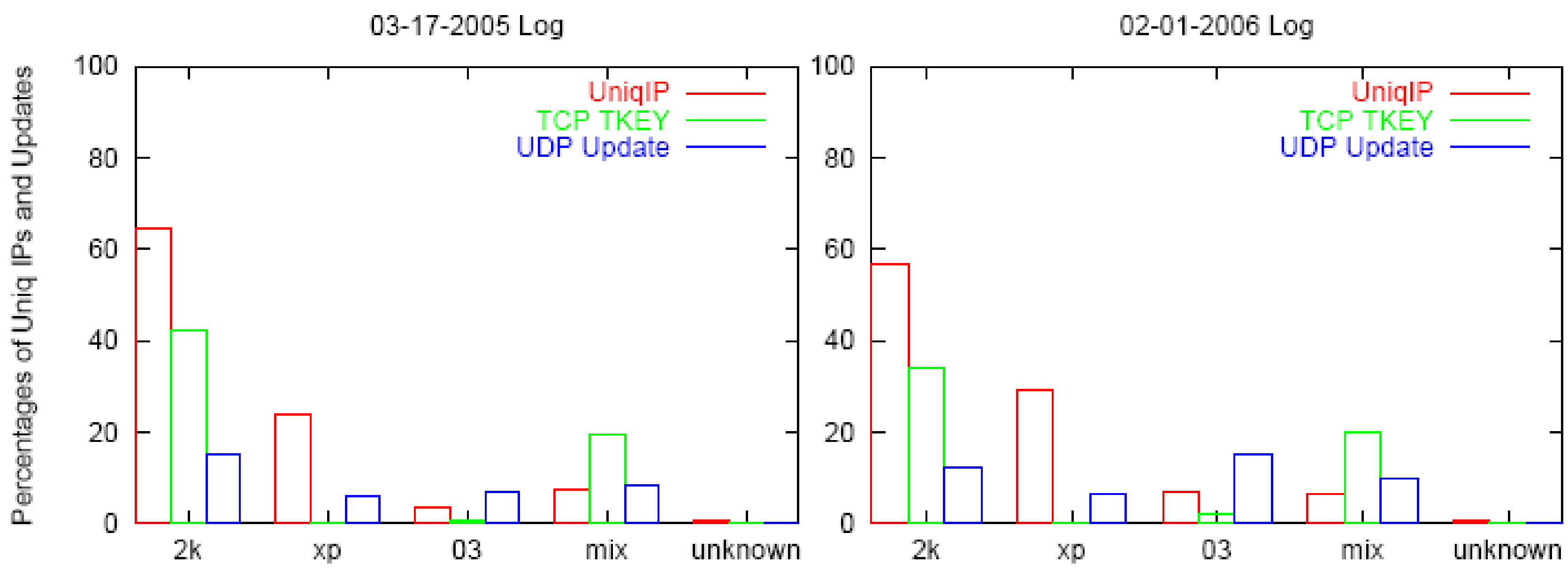
Date	Packets	TCP%	UDP%	SrcIPs	Prefixes	ASes
03-17-05	1.65M	89.5%	10.5%	69133	11954	2685
02-01-06	0.81M	86.7%	13.3%	37823	6314	1357

- RFC1918 Updates from Windows systems
  - This table is for 03-17-2005. Results for 02-01-2006 are the same or slightly higher.
  - *90% Internet generic traffic at a tire-1 link between San Francisco to Seattle is from Windows*

	TCP	**UDP**	**Total**
Application-level	98.6%	96.8%	98.4%
Transport-level	98.5%		
Network-level			> 97.6%

Identification of OSes of RFC1918 Updates – More Results

- Breakup unique IP addresses by different Windows Systems
- In total, 99.5% IP addresses in the logs having at least one Windows machine at or behind it



◆Mix: IPs showing more than one type of Windows signatures

Methods to Avoid/Reduce RFC1918 updates

- User efforts
  - Manually disable dynamic DNS updates
  - Require end users' awareness of this problem
- Vendor efforts
  - Turn off default dynamic DNS updates, or send RFC1918 update more conservatively
- Administrator efforts
  - Enterprise: configure DNS server and DNS updating clients consistently
  - ISP: configure DNS server to point itself as SOA for both forward and inverse RFC1918 blocks

Summary

- Leaking of RFC1918 updates is a global problem and costly in resource
- Windows systems account for over 97% of total RFC1918 updates
- Over 99% of unique source IP addresses in the traffic traces each has at least one Windows machine at or behind it
- Cautions can be taken to avoid/reduce RFC1918 updates

Questions/Comments

Thank You!