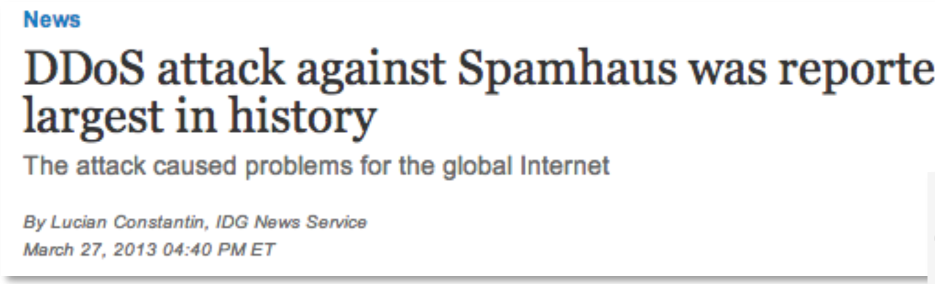
On the Mismanagement and Maliciousness of Networks

Jing Zhang[1], Zakir Durumeric[1], Michael Bailey[1],
Mingyan Liu[1], and Manish Karir[2]

[1] Computer Science and Engineering, University of Michigan

[2] Department of Homeland Security, Science and Technology Directorate,
Cyber Security Division

Motivation: DNS Amplification Attack

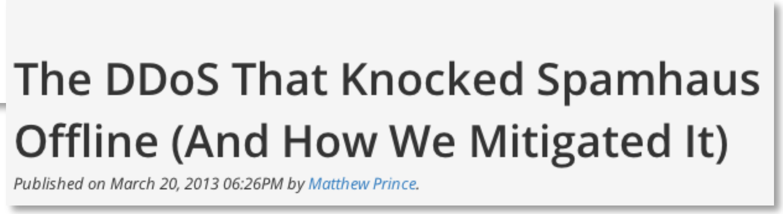


News

DDoS attack against Spamhaus was reportedly the largest in history

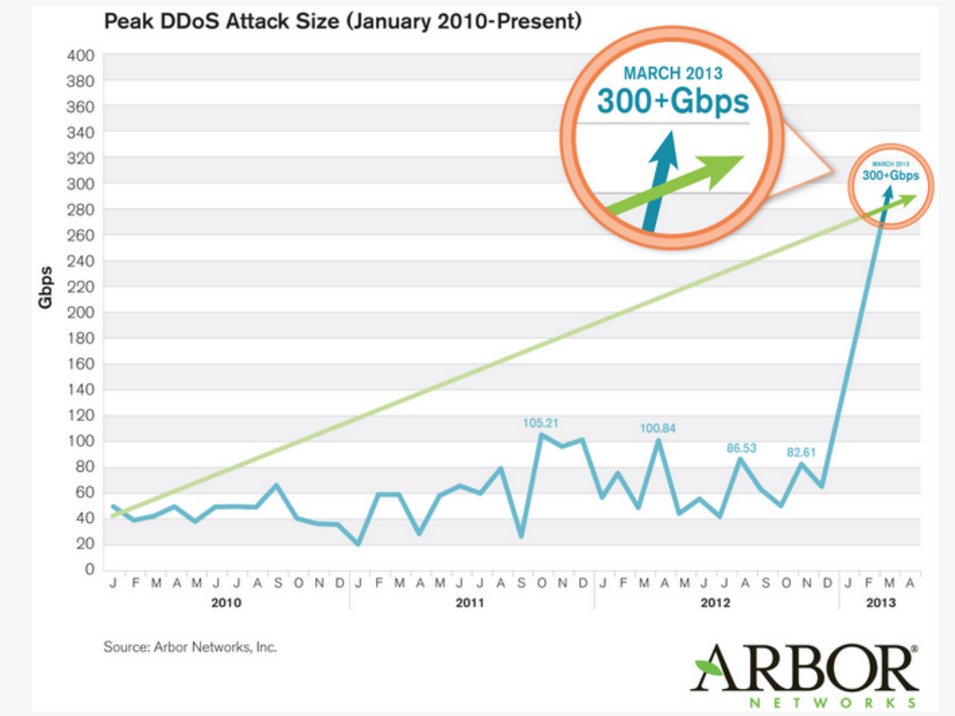
The attack caused problems for the global Internet

By Lucian Constantin, IDG News Service
March 27, 2013 04:40 PM ET



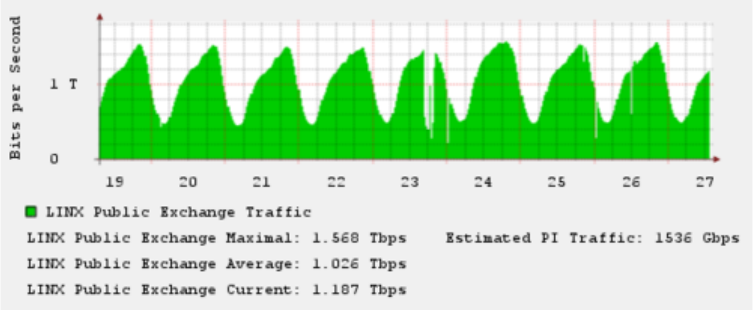
The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)

Published on March 20, 2013 06:26PM by Matthew Prince.



Source: Arbor Networks, Inc.

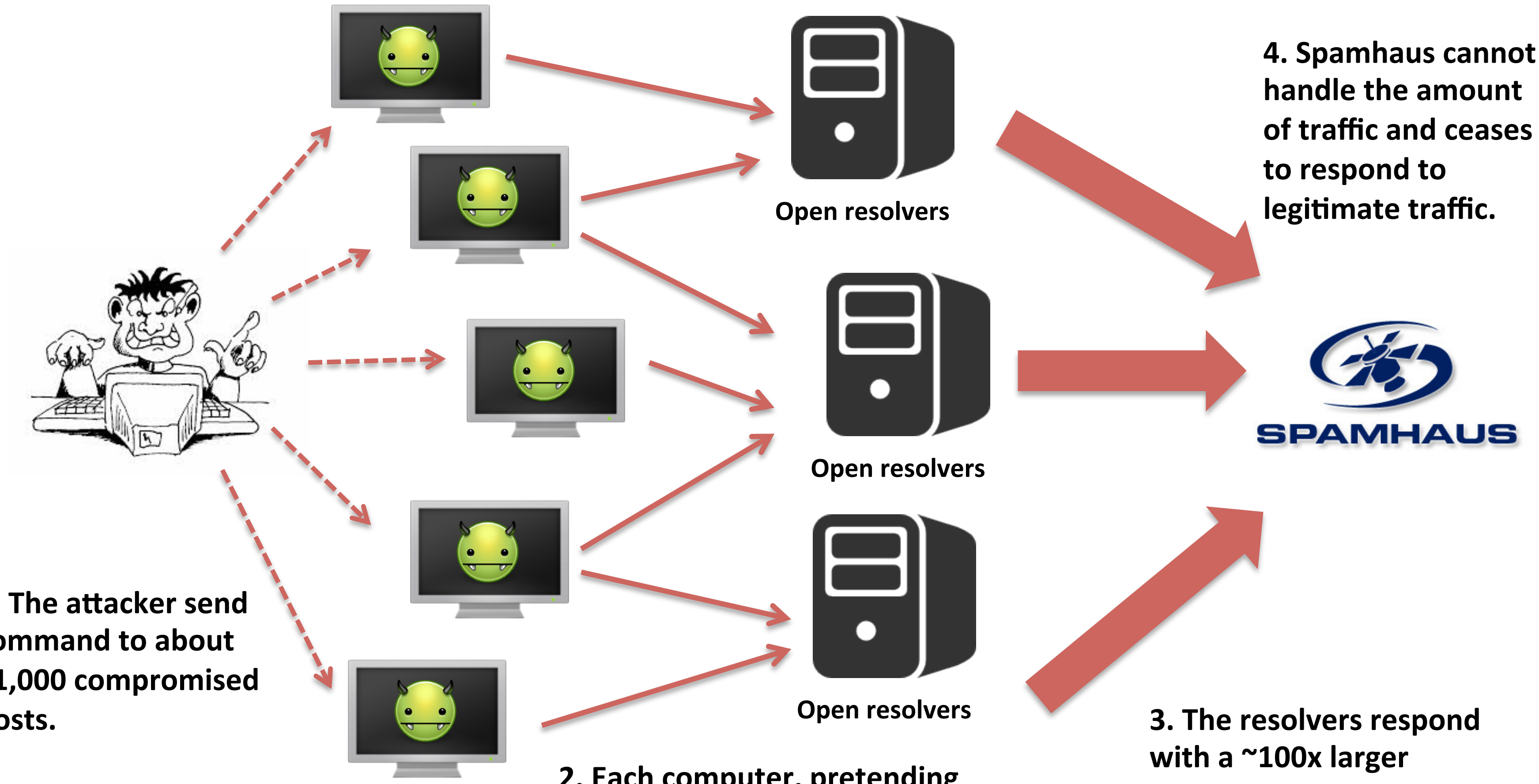
Internet Under Attack: World's Largest DDoS Attack Almost Broke The Internet



🟩 LINX Public Exchange Traffic

```
LINX Public Exchange Maximal: 1.568 Tbps     Estimated PI Traffic: 1536 Gbps
LINX Public Exchange Average: 1.026 Tbps
LINX Public Exchange Current: 1.187 Tbps
```

Motivation: DNS Amplification Attack



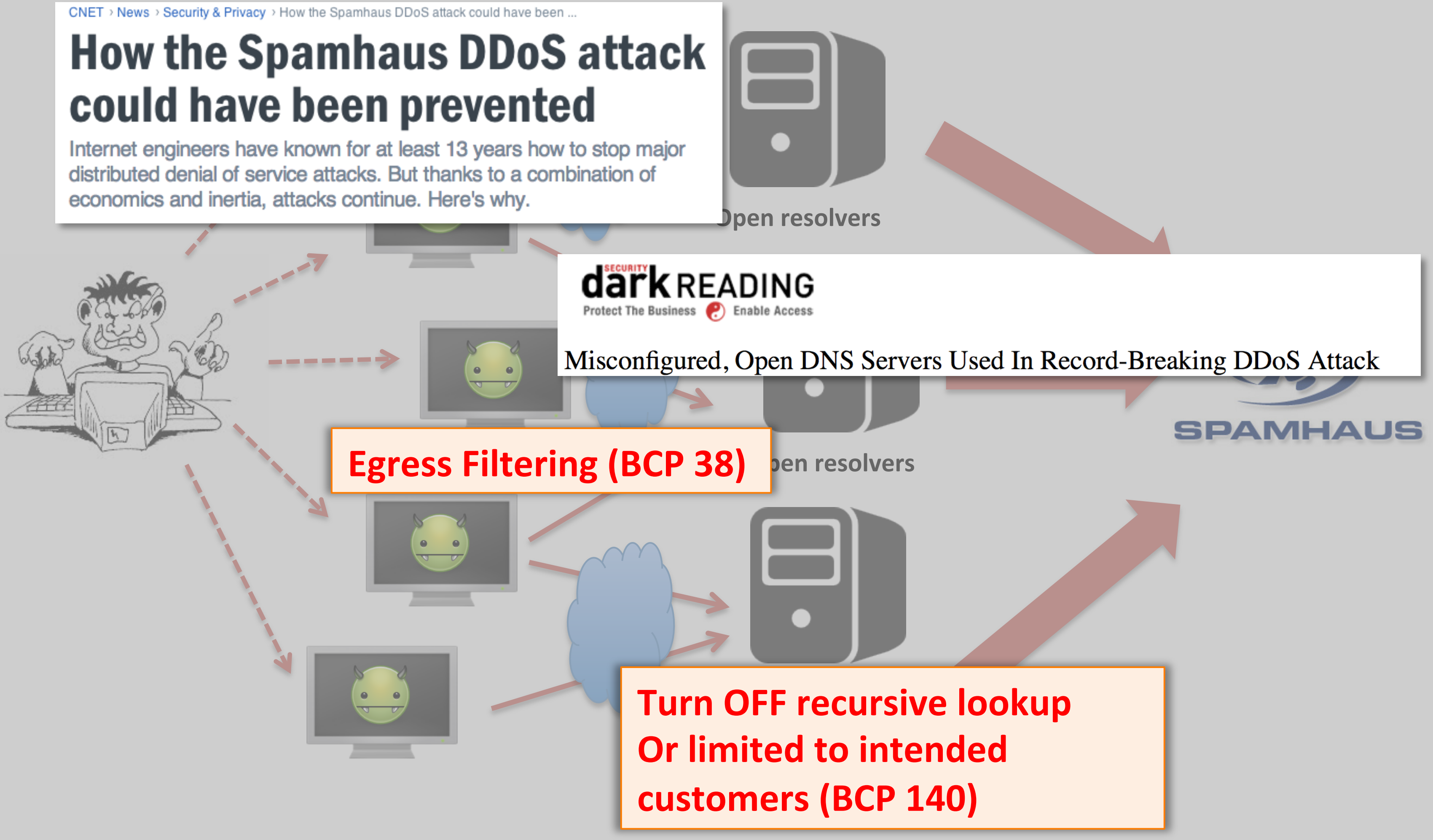
1. The attacker send command to about ~1,000 compromised hosts.

2. Each computer, pretending to be Spamhaus (spoofing source IP), send DNS request to resolvers.

3. The resolvers respond with a ~100x larger message to 'Spamhaus'.

4. Spamhaus cannot handle the amount of traffic and ceases to respond to legitimate traffic.

Motivation: DNS Amplification Attack



CNET › News › Security & Privacy › How the Spamhaus DDoS attack could have been ...

How the Spamhaus DDoS attack could have been prevented

Internet engineers have known for at least 13 years how to stop major distributed denial of service attacks. But thanks to a combination of economics and inertia, attacks continue. Here's why.

SECURITY dark READING
Protect The Business · Enable Access

Misconfigured, Open DNS Servers Used In Record-Breaking DDoS Attack

Egress Filtering (BCP 38)

Turn OFF recursive lookup Or limited to intended customers (BCP 140)

Mismanagement & Malicious Use

- Obvious causality between misconfigured open resolvers and DDoS attacks
  - Misconfigured -> Vulnerability -> Exploited -> Malicious sources

- Mismanagement and Malicious use in general
  - Are Mismanagement symptoms related?
    - E.g. Would networks with more open resolvers also have more untrusted HTTPS certificates?
  - Are mismanagement and malicious use of networks related?
    - E.g. Would networks with more open resolvers send more Spam?

Agenda

- Mismanagement of Networks
- Maliciousness of Networks
- Relationship
- Discussions & Future work

Agenda

- Mismanagement of Networks
- Maliciousness of Networks
- Relationship
- Discussions & Future work

Measuring Mismanagement

- What is Mismanagement?

  "Managing ineffectively, incompetently, carelessly, or wrongly. Mismanagement ranges from making poor decisions to breaking rules for personal gain." [1]

- How to measure Mismanagement?
  - Internal auditing and reviews
  - External observation
- Our Approach – Inferring from mismanagement symptoms
  - Well documented security practices
  - External observations
  - Broad coverage

[1] The American Heritage Dictionary of Business Terms.

Summary of Selected Symptoms

Symptom	Best security Practices	Function	Data Sources
Open recursive DNS resolver	BCP 140	Naming Infrastructure	Open Resolver Project [1]
DNS source port randomization	RFC 5452	Naming Infrastructure	Inferred from Verisign .com and .net TLD queries
Consistent A and PTR records	RFC 1912	Naming Infrastructure	rDNS lookup on all .com and .net A records
BGP misconfiguration	RFC 1918, RFC 6598	Routing Infrastructure	Inferred from routing updates collected by Route Views and RIPE
Lack of Egress Filtering	BCP 38	Transit	Spoofer Project [2]
Untrusted HTTPS Certificates	RFC 5246, RFC 2459	Web Application	Collected with Zmap network scanner
Open SMTP mail relays	RFC 2505	Mail Application	Collected with Zmap network scanner
Publicly Available Out-of-Band Management cards	Manufacturer's Guideline	Server	Collected with Zmap network scanner

[1] Open Resolver Project. http://openresolverproject.org/

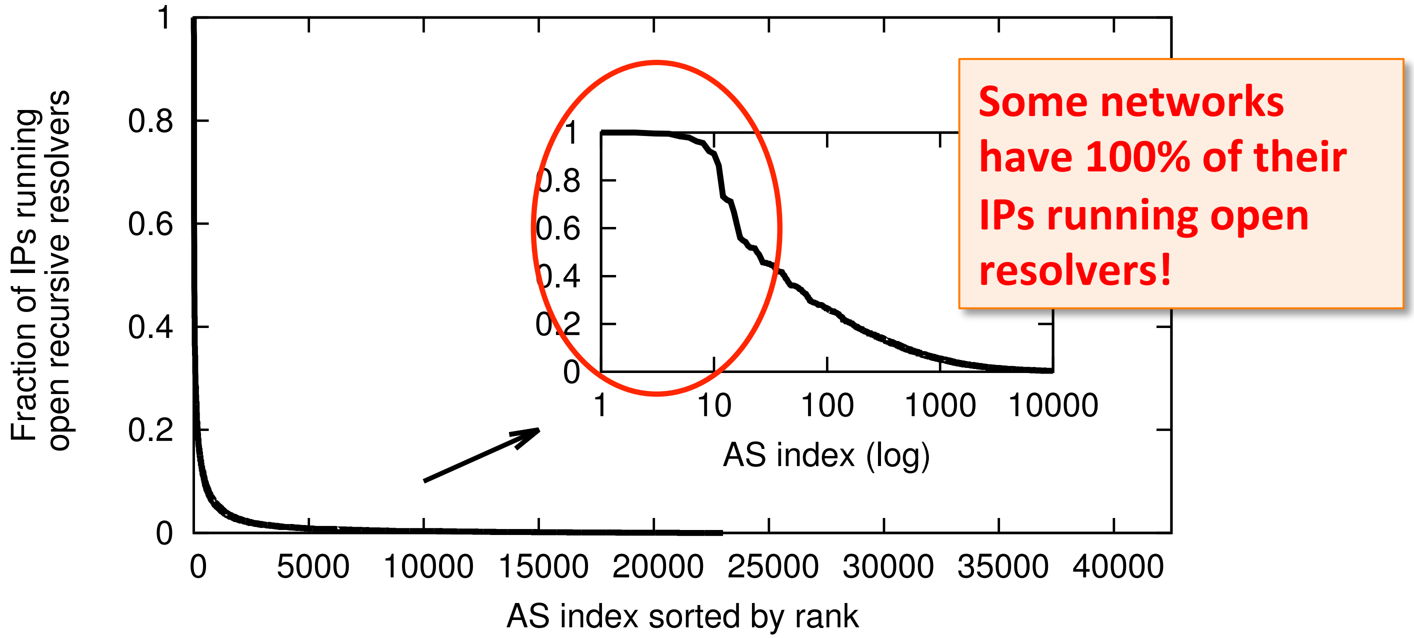
[2] Spoofer Project: State of IP Spoofing. http://spoofer.cmand.org/

Widespread Mismanaged Systems

Open recursive DNS resolver	*27 million* open recursive resolver
DNS source port randomization	*226,976 (4.8%)* DNS resolvers without using source port randomization
Consistent A and PTR records	*27.4 million (23.4%)* A records that do not have matching PTR records
BGP misconfiguration	*42.4 million (7.8%)* short-lived BGP routes
Lack of Egress Filtering	*35.6%* tested netblocks that have not implemented egress filtering
Untrusted HTTPS Certificates	*10.2 million (52%)* HTTPS servers using untrusted certificates
Open SMTP mail relays	*22,284 (2%)* SMTP servers that allow open mail relays
Publicly available IPMI cards	*98,274* public accessible IPMI cards

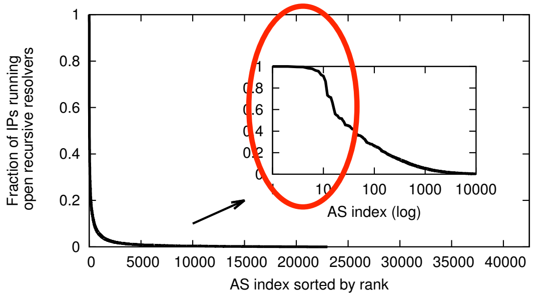
Abstracting Networks

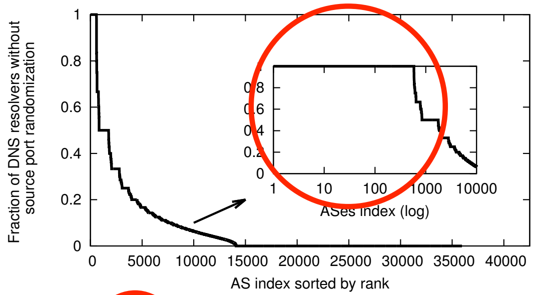
- Network-level mismanagement measures
  - *Aggregating* IP addresses into Autonomous Systems
  - *Normalized* mismanagement symptoms to enable fair comparison

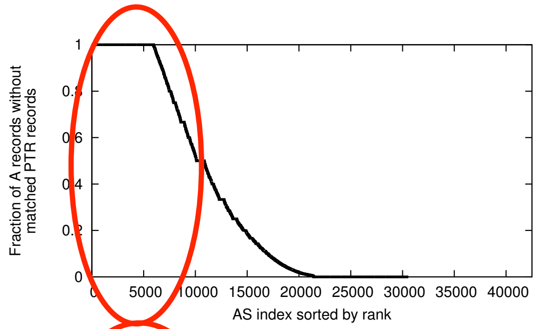


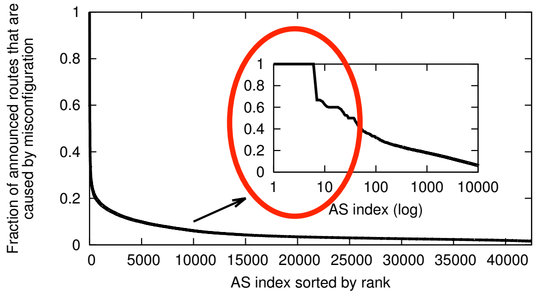
Some networks have 100% of their IPs running open resolvers!

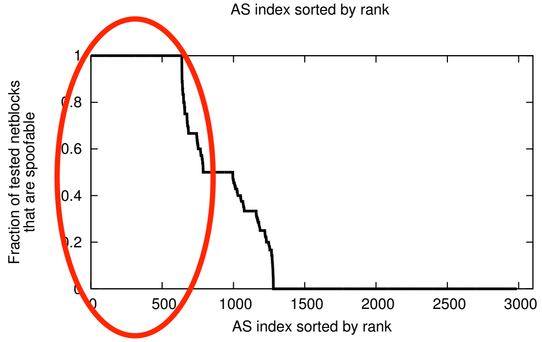
Mismanagement of Autonomous Systems

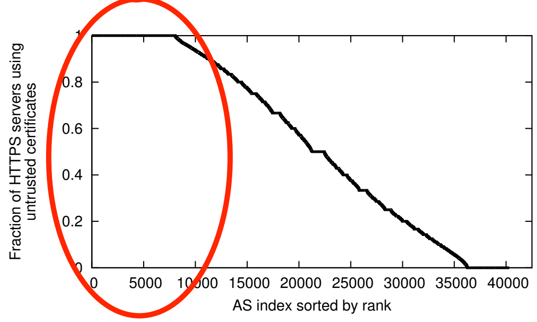


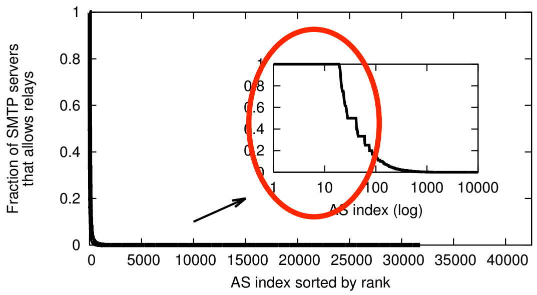


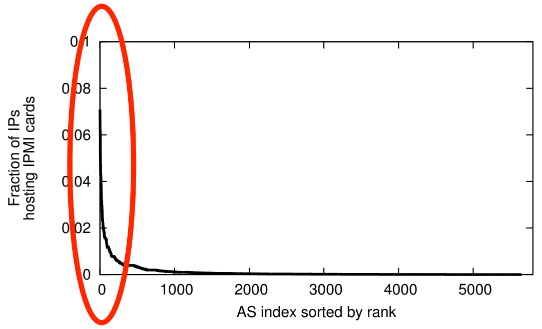












Some networks are disproportionally poorly-managed!

Are Mismanagement Symptoms Related?

YES!

	Open resolver	port rand.	PTR records	BGP misconfig.	Egress Filtering	HTTPS Cert.	SMTP relays
Open resolver	-						
port randomization	0.35	-					
PTR records	0.01	0.15	-				
BGP misconfig.	0.17	0.07	0.03	-			
Egress Filtering	0.09	0.04	0.01	0.04	-		
HTTPS Certificates	0.46	0.23	0.00	0.16	-0.01	-	
SMTP relays	0.14	0.16	0.10	0.02	0.14	0.06	-
IPMI cards	0.26	0.26	0.15	0.03	0.10	0.15	0.26

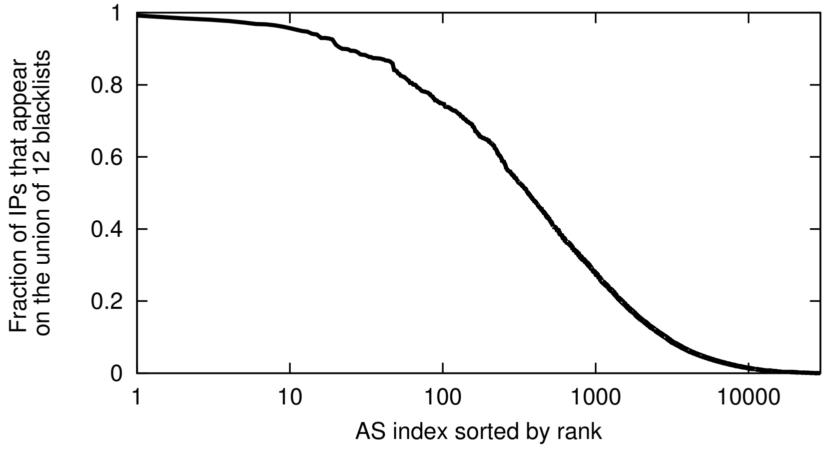
- Most of the symptoms are correlated
  - Statistically significant at 95% confidence level
  - Weak to moderate positive correlation

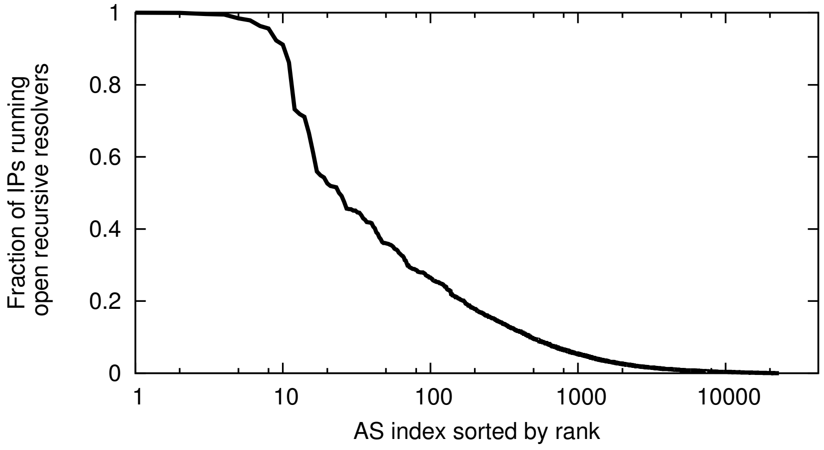
Agenda

- Mismanagement of Networks
  - Symptoms of mismanagement
  - Mismanagement of networks
- Maliciousness of Networks
- Relationship
- Discussions & Future work

Measuring the Malicious Use of ASes

- *Union* of 12 network reputation blacklists, covering spam, malware, phishing, and active scanning [1]
- *Aggregate* to Autonomous Systems
- *Normalize* by the number of announced IP





[1] J Zhang, A Chivukula, M Bailey, M Karir, M Liu. *Characterization of Blacklists and Tainted Network Traffic* (PAM'13)

Agenda

- Mismanagement of Networks
  - Symptoms of mismanagement
  - Mismanagement of networks
- Maliciousness of Networks
- Relationship
- Discussions & Future work

Are mismanagement and Malicious Use Related?

Metric	Coefficient	Interpretation
Open recursive DNS resolver	0.59	Strong Positive Correlation
DNS source port randomization	0.45	Moderate Positive Correlation
Consistent A and PTR records	0.20	Weak Positive Correlation
BGP misconfiguration	0.19	Weak Positive Correlation
Untrusted HTTPS Certificates	0.44	Moderate Positive Correlation
Open SMTP mail relays	0.23	Weak Positive Correlation
Mismanaged IPMI cards	0.22	Weak Positive Correlation
Egress Filtering	0.04	No Correlation

- Individual symptoms are positively correlated to the malicious use

Are mismanagement and Malicious Use Related?

YES!

Metric	Coefficient	Interpretation
Open recursive DNS resolver	0.59	Strong Positive Correlation
DNS source port randomization	0.45	Moderate Positive Correlation
Consistent A and PTR records	0.20	Weak Positive Correlation
BGP misconfiguration	0.19	Weak Positive Correlation
Untrusted HTTPS Certificates	0.44	Moderate Positive Correlation
Open SMTP mail relays	0.23	Weak Positive Correlation
Mismanaged IPMI cards	0.22	Weak Positive Correlation
Egress Filtering	0.04	No Correlation
Overall Mismanagement	***0.64***	***Strong Positive Correlation***

- Individual symptoms are positively correlated to the malicious use
- Overall Mismanagement are correlated to the malicious use
  - A rank calculated by linearly combining all the rank of individual symptoms

Causal Inference

- Correlation ≠ Causality
  - Latent variable can cause both factors
    - Country GDP are positively correlated
    - Business relationship are positively correlated
- Formal Causal Inference
  - Fast Causal Inference algorithm
  - Control variable: country GDP, country GDP per capita, # of peers, # of customers
  - Limitation: there might be other latent variables that affect the correctness of the inference result

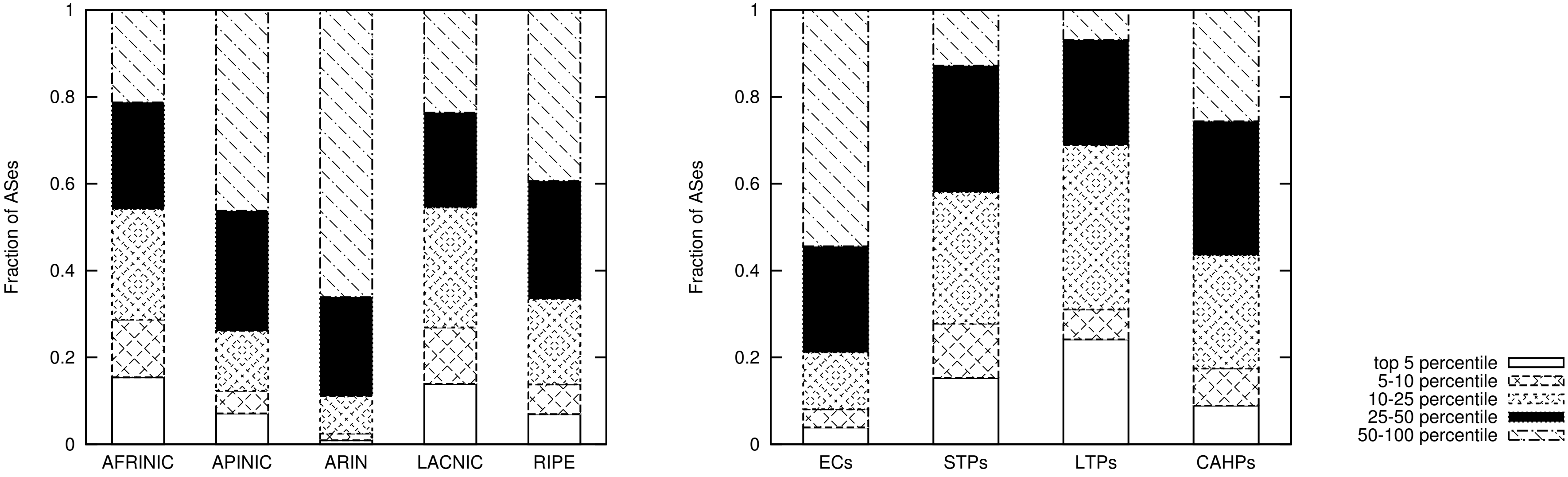
Mismanagement leads to maliciousness under the control of selected economic and social factors.

Agenda

- Mismanagement of Networks
  - Symptoms of mismanagement
  - Mismanagement of networks
- Maliciousness of Networks
- Relationship
- Discussions & Future work

Different Mismanagement Levels

- Break down by Geographic and Topology
  - AFRINIC > LACNIC > RIPE > APINIC > ARIN
  - LTPs > STPs > CAHPs > ECs
- Why different?

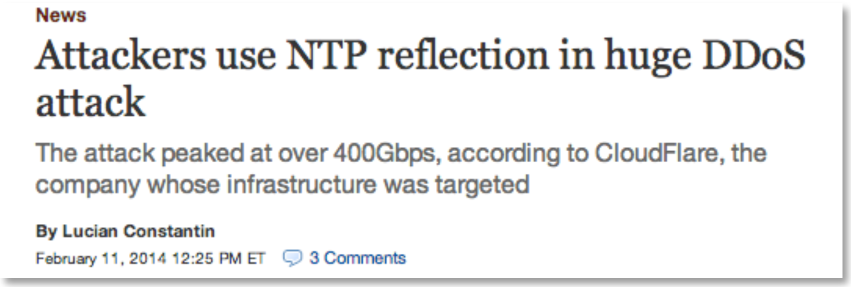


Proactive Reputation

- Regular active scans of the Internet for mismanagement
- Can the mismanagement be used to predict/prevent future attacks?

- ~380,000 open NTP servers [1]
- Moderate correlated to overall mismanagement, reputation and other mismanagement symptoms

	Correlation
Reputation	0.35 (p <0.01)
Overall Mismanagement	0.42 (p <0.01)



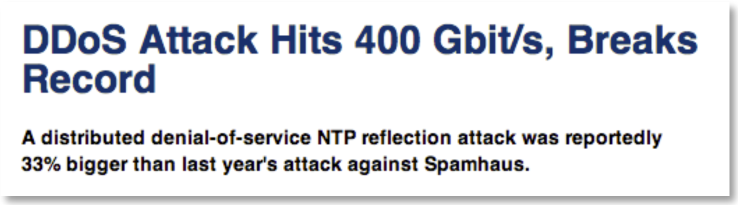
News

Attackers use NTP reflection in huge DDoS attack

The attack peaked at over 400Gbps, according to CloudFlare, the company whose infrastructure was targeted

By Lucian Constantin

February 11, 2014 12:25 PM ET 3 Comments



DDoS Attack Hits 400 Gbit/s, Breaks Record

A distributed denial-of-service NTP reflection attack was reportedly 33% bigger than last year's attack against Spamhaus.

[1] Open NTP Project. http://openntpproject.org/

Thanks!

Appendix

Level of Aggregation

- Impact of Aggregation
  - All the correlations are statistically significant at prefix-level
  - Very slightly differences in the strength of correlations

Metric	AS-level			Prefix-level		
	Coefficient	P-value	Interpretation	Coefficient	P-value	Interpretation
Open recursive DNS resolver	0.59	<0.01	Strong	0.54	<0.01	Strong
DNS source port randomization	0.45	<0.01	Moderate	0.24	<0.01	Weak
Untrusted HTTPS Certificates	0.44	<0.01	Moderate	0.39	<0.01	Moderate
Open SMTP mail relays	0.23	<0.01	Weak	0.15	<0.01	Weak
Mismanaged IPMI cards	0.22	<0.01	Weak	0.18	<0.01	Weak