Denial of Sleep Attacks in Wireless Sensor Networks

Micah Thornton Ryan Sligh Bobby Santoski

Computer Science & Engineering, Southern Methodist University, USA,
mathornton@smu.edu

CSE 4344: Networks and Distributed Systems
Dallas, Texas
April 26, 2014

Reports of DDoS attacks are rampant

Figures/DDoS?.jpeg


Figures/SlushDDoS.jpeg


Figures/goxddos.jpeg


Figures/SatoshiDDoS.jpeg


Figures/ExchangesHit.jpeg


Figures/BitcoinAttacked.jpeg

Motivation

- DDoS attacks are perhaps the most common scourge to afflict Bitcoin participants
- No one has systematically tracked DDoS on Bitcoin
- Thus it is hard to assess their impact on the Bitcoin ecosystem
- We measure DDoS reports to identify their real prevalence and impact

Outline of today's talk

Outline

Data sources

Source	Data Collected	Description
Bitcointalk.org		Forum posts containing "DDoS"
Bitcoincharts.org		Currency exchange information
Blockchain.info/pools (Internet Archive)		Pool's historical hashrates
Bitcoin.it/wiki/Trade		List of services and pools


Figures/Portugese.png

Figures/DOSgames.png

Figures/btctalkdossidos.png

From posts to attacks

- Google API searched on Bitcointalk.org found **2940 pages** mentioning "DDoS"
- Pages were pared down to **1355 distinct threads (first page only)**
- Rule based classifier flagged **362 posts** as likely attacks
  - Whitelist: "unreachable", "offline", "on-line", "down", "flooding", "attack", "ddos", "unavailable", "blocking" and "connect"
  - Blacklist: "anti-ddos" or "vote"
  - Flagged posts contain at least one word in the whitelist and none in the blacklist
- Manual inspection of posts yields **200 attacks**
- De-duplication yields **142 distinct attack reports**

Outline

Mapping attacks to Bitcoin services

- Examined **1 240 services** including **32 mining pools**
- **142 distinct DDoS attacks** reported
- **46 specific services** were targeted:

Reported DDoS over time and by category

Identifying the use of anti-DDoS mechanisms

- Anti-DDoS mechanisms include content distribution networks (CDNs) and clever firewalls
- Anti-DDoS services identifed: **Amazon, Cloudflare, Incapsula**
- Resolved the IP addresses of Bitcoin services and compared with known CDN IP ranges
- Found **178 services** that used Anti-DDoS countermeasures out of a total **1190 services**

DDoS attacks and countermeasures by service category

Category	#	Suffer DDoS %	Suffer DDoS Sig.?	Use Anti-DDoS %	Use Anti-DDoS Sig.?
Average		*7.3*		*19.9*	
Currency exchanges	119	**10.9**	+	**36.1**	+
Financial	26	**15.4**	+	26.9	
Pool	41	**28.6**	+	**34.1**	+
Bitcoin eWallets	17	**26.8**	+	35.3	
Bitcoin payment systems	11	9.1		18.2	
Material/physical products	295	**0.7**	−	**10.5**	−
Internet & mobile services	225	1.8		16.9	
Online products	185	3.8		14.6	
Professional services	137	0		10.2	
Travel/tourism/leisure	78	0		10.3	
Commerce & community	71	1.4		12.7	
Getting started	31	0		12.9	

Do DDoSed firms buy anti-DDoS protection?

- Does suffering a DDoS attack make a service more likely to purchase DDoS countermeasures?

	Use Anti-DDoS		No Anti-DDoS	
	#	%	#	%
Suffered DDoS	25	54%	21	46%
No DDoS	178	15%	1 012	85%

Do DDoSed firms buy anti-DDoS protection?

- Does suffering a DDoS attack make a service more likely to purchase DDoS countermeasures? Yes!

	Use Anti-DDoS		No Anti-DDoS	
	#	%	#	%
Suffered DDoS	25	54%	21	46%
No DDoS	178	15%	1 012	85%

DDoS attacks on mining pools

- Does the size of a mining pool affect its tendency to be DDoSed?
- Captured 22 historical records of hashrate shares of mining pools
- A pool is "big" if it has at least a 5% share of the hash rate during 2 or more observations

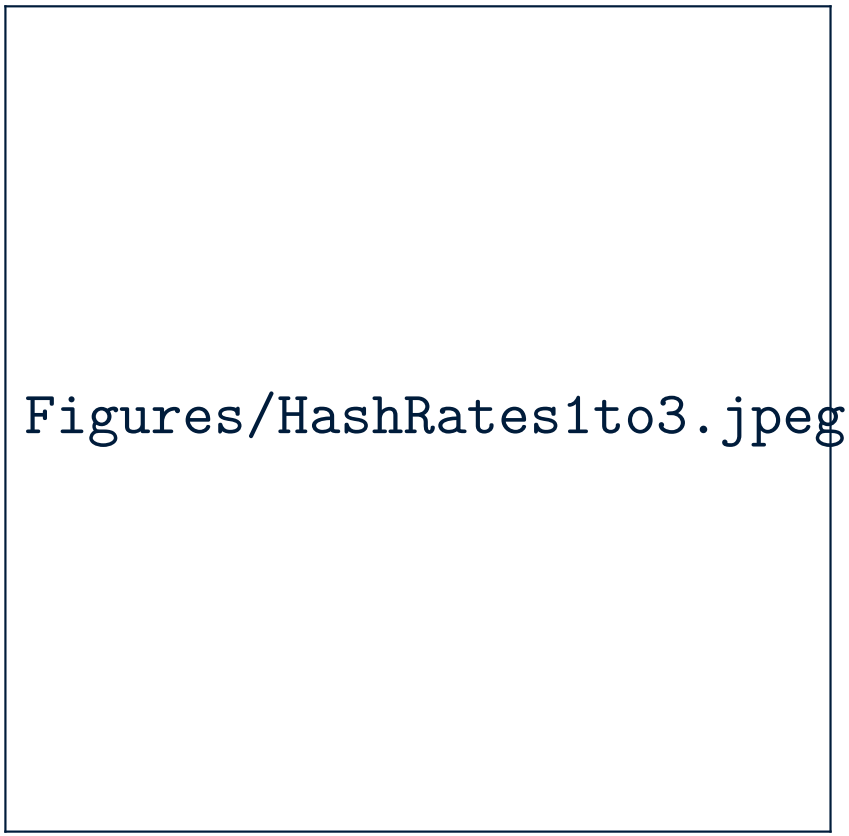
	Small Pools		Big Pools	
	#	%	#	%
Suffered DDoS	7	17.1%	5	62.5%
No DDoS	34	82.9%	3	37.5%

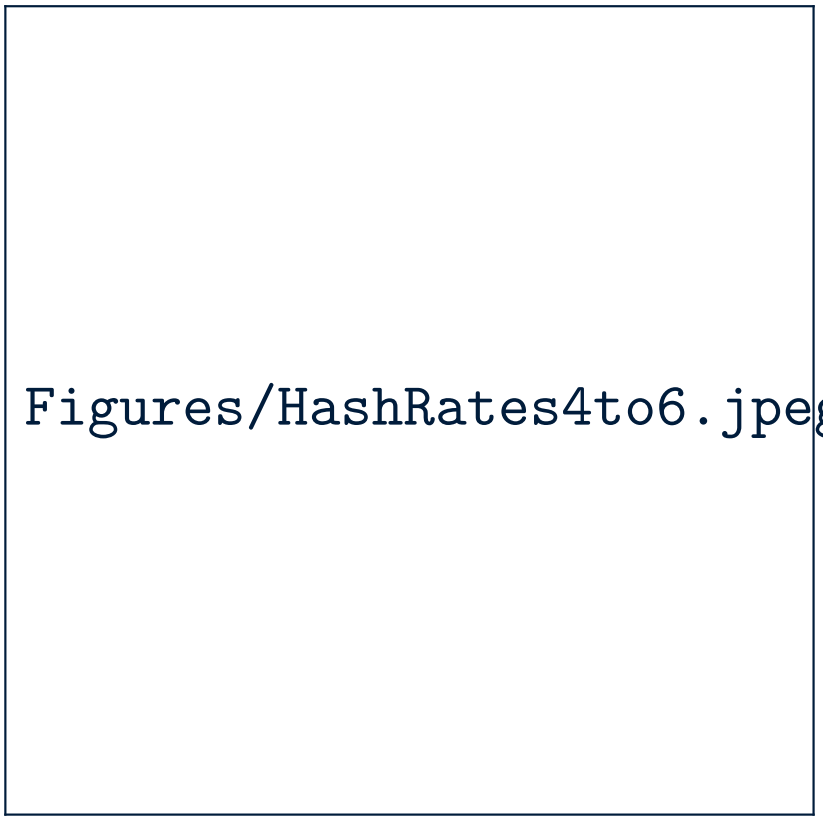
DDoS attacks on mining pools

- Does the size of a mining pool affect its tendency to be DDoSed? Yes!
- Captured 22 historical records of hashrate shares of mining pools
- A pool is "big" if it has at least a 5% share of the hash rate during 2 or more observations

	Small Pools		Big Pools	
	#	%	#	%
Suffered DDoS	7	17.1%	5	62.5%
No DDoS	34	82.9%	3	37.5%

Historical hash-rate-based market shares





Historical hash-rate-based market shares

Figures/AllPoolsDistributionSplit.pdf

- Pools sometime unfazed by DDoS attacks
  - BTC Guild increased its market share after an attack in mid-2012
  - But its share decreased after an attack in mid-2013
- DDoS attacks sometimes target multiple pools at once
  - Deepbit, BTC Guild, and Eclipse targeted at the same time as seen mid-2012
- We can reject the notion that DDoS attacks always trigger decline in market share
- DDoS attacks often precede shake ups in pool marketshare

DDoS effects on trade volume and price (Mt. Gox)

Figures/GoxDDoSData.jpeg

DDoS effects on trade volume and price (Mt. Gox)

- **29 total attacks** reported on Mt. Gox
- We compare transaction volume 1 week prior to DDoS and 1 week after DDoS

Δ **Transaction Vol.**	**# of Attacks**	**% Attacks**	**% Change**
Increase	12	41.4%	68.1%
Decrease	17	58.6%	31.9%

- Fall in transaction volume more common than rise after DDoS
- When increases in transaction volume do occur, the magnitude of change is greater than for decreases

Change in transaction volume at Mt. Gox following DDoS

Outline

Takeaways

- 7% of all known operators have been subject to DDoS attacks
- Currency exchanges, mining pools, gambling operators, eWallets, and financial services are more likely to be attacked
- Services that are attacked are more than 3 times as likely to buy anti-DDoS services
- Large mining pools more likely to be DDoSed than small pools

Future work

- Get a more accurate, network-based measure of Bitcoin DDoS
- Explore the relationship between DDoS and other currencies (e.g., Litecoin)
- Measure other anti-DDoS services
- Study impact of other factors on DDoS attacks (e.g., mining pool structure)

Questions?