Argus: An Accurate and Agile System to Detecting IP Prefix Hijacking

Yang Xiang Zhiliang Wang
Xia Yin Jianping Wu
Tsinghua University, Beijing

FIST 2011 @ Vancouver
2011-10-17

Outline

- Introduction
  - Background - Prefix hijacking
  - Existing detection method
  - Our proposal
- Argus
  - Goals: Accurate, Real-time, Easy to deploy, …
  - Architecture
  - Hijacking identification
- Evaluations
  - Detection delay
  - Recent hijackings
- Conclusions

Outline

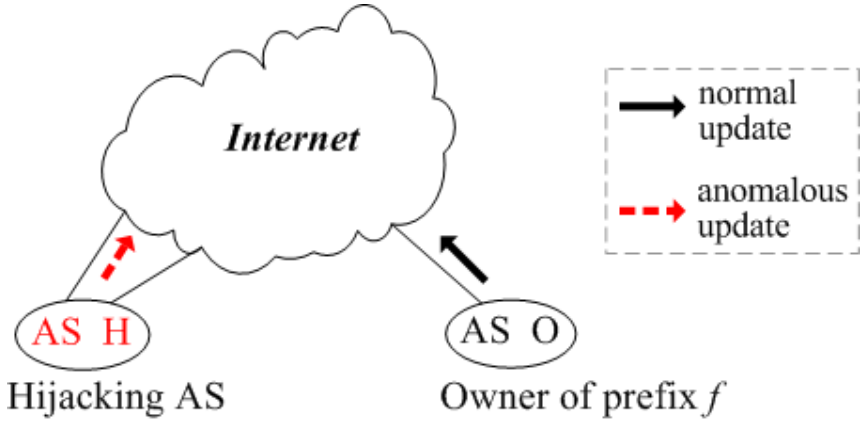
- ***Introduction***
  - ***Background - Prefix hijacking***
  - Existing detection method
  - Our proposal
- Argus
- Evaluations
- Conclusions

Inter-domain Routing

- BGP (Border Gateway Protocol)
  - *De facto* Inter-domain routing protocol
  - Update: prefix ***f***, AS path ***p*** = $<a_n, \ldots a_i, \ldots a_1, a_0>$
- BGP update message can **not** be verified
  - Mis-configuration or malicious attack can generate invalid BGP update

Prefix Hijacking

- AS **H** hijacked prefix ***f*** owned by AS **O**
- Two types
  - Mis-configuration
    - Black-hole: H simply drops the attracted traffic
  - Malicious attack
    - Black-hole
    - Imposture: H response to senders of the hijacked traffic
    - Interception: H finally forwards the traffic to O



We focus on Mis-config hijackings

- Malicious attack is rare
  - Internet connected by trustworthy ASes
  - AS neighbors (business partners) are build based on credit

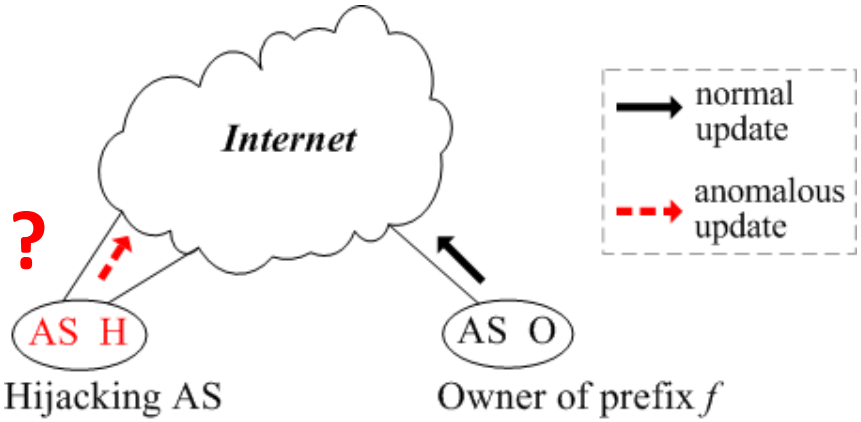
- **Mis-configuration occurs frequently**
  - 2010, China Tele. hijacked **10% of Internet** prefixes
  - 2008, Pakistan Tele. hijacked Youtube for **two hours**

Outline

- ***Background***
  - Background - Prefix hijacking
  - ***Existing detection methods***
  - ***Our proposal***
- Argus
- Evaluations
- Conclusions

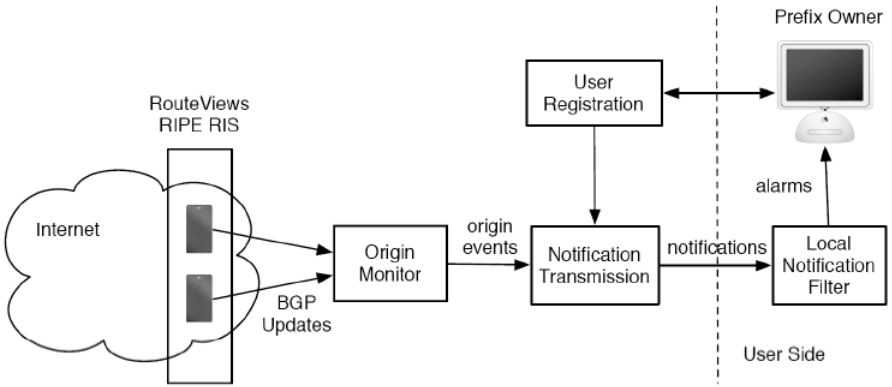
Challenge of Detection

- Distinguish from valid scenarios
  - MOAS (Multi-Origin AS)
    - Multi-homing
    - BGP Anycast
    - …
  - Valid AS Path



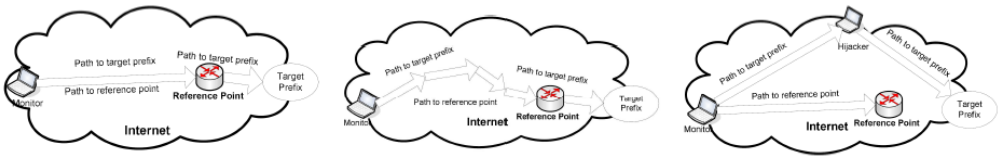
Existing Methods
Control-plane

- PHAS: Prefix Hijack Alert System
  - Report any announcement with a unusual <home-AS, prefix> mapping



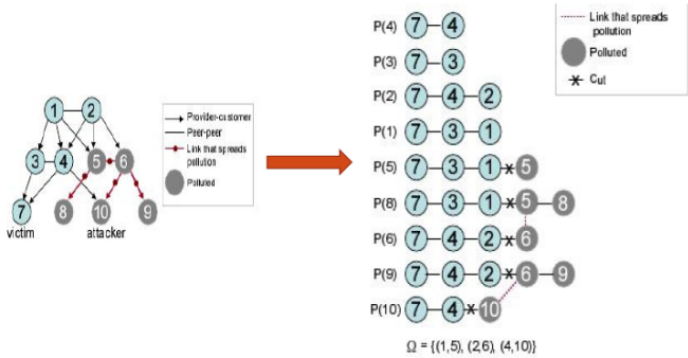
Existing Methods
Data-plane

- 1. Monitoring from several Vantage Points
  - Detect path disagreement between target and reference router
  - Accuracy is highly dependent on reference routers



(a) Original (b) Legitimate route change (c) Prefix hijacking

- 2. iSPY: Probe transit ASes from prefix owner



Existing methods - Comparison

- Control plane ***v.s.*** Data plane

Monitoring

+

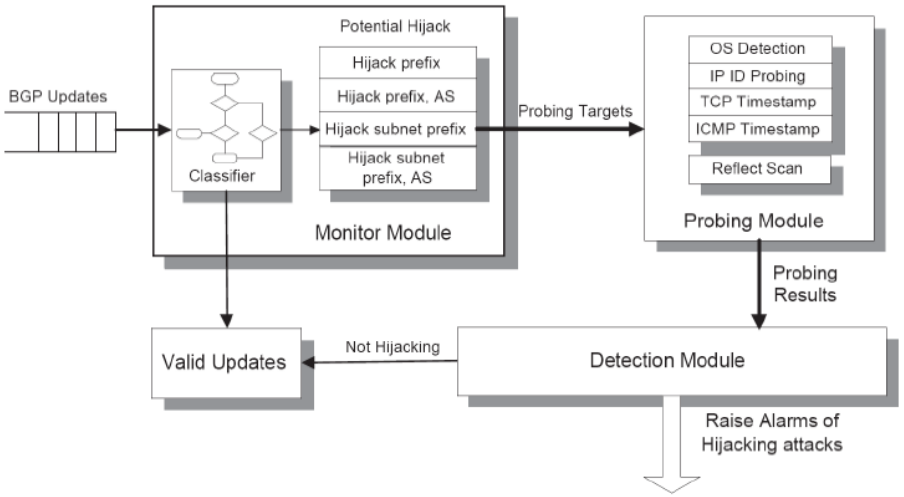
Detection

Methods	Pros	Cons
Control-plane	1. Realtime (live BGP feed) 2. Luxuriant information (victim and attacker)	1. Very low accuracy 2. Lots of alarms
Data-plane	1. High accuracy 2. Few alarms	1. Heavy-weight, not scalable 2. Lack of attacker's info. 3. Minutes of detection delay 4. Can't detect sub-prefix hijacking

- Control + Data plane methods

Existing Method
Control + Data plane

- Monitoring IP Prefix Announcements and Network Fingerprints.



- Cons.
  - Probing from arbitrary point is **inefficient**
  - **Minutes** of detection delay (complicated commands)
  - Complicated, **rely** heavily on external vantage point (advance permission, new software, …)

Our proposal

- State of the art: Control + Data plane
  - Control plane monitoring
  - (Only) Data plane detection
- Our proposal: Control **x** Data plane
  - Control plane monitoring
  - Control **x** Data plane detection
    - **Correlation** between two planes !

Outline

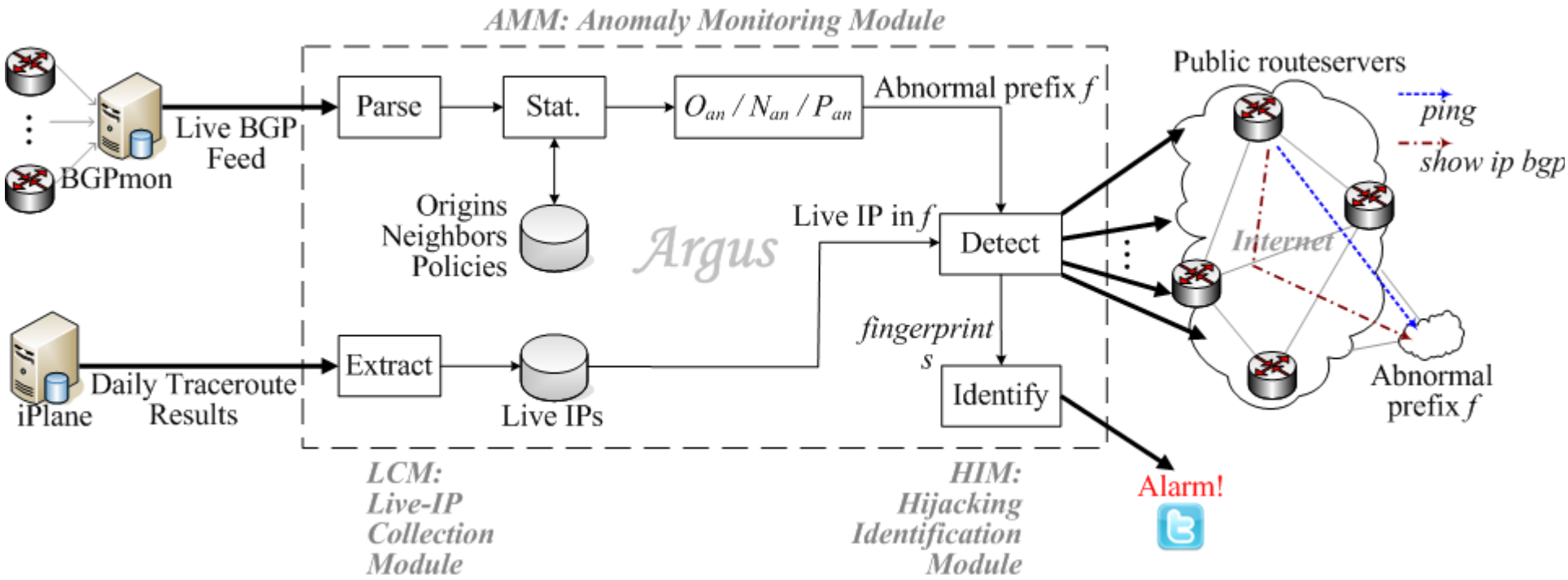
- Introduction
- ***Argus***
  - ***Goals: Accurate, Real-time, Easy to deploy, …***
  - ***Architecture***
  - ***Hijacking identification***
- Evaluations
- Conclusions

Design goals

Accurate	Low false positive rate **Correlation: Control x Data plane**
Real-time	Seconds of detection delay **Use simple & efficient commands**
Easy to deploy	Low dependence on external nodes **Use public interface/service**
Perceptive	Luxuriant information (attacker & victim, various kinds of hijacking) **Control-plane monitoring**
Scalable	Light-weight **Control-plane driving**

Architecture

- Key observation: probing from a polluted router will not receive response, ***vise versa***



-- *In Greek Myth,* ***Argus*** *is a primordial giant with one hundred eyes*

Correlation: Control **x** Data plane

Hijacking Identification

- Anomaly prefix: ***f*** Live IP: ***i***
- Keep on detecting for ***W*** seconds
- Control-plane routing information (***C_t***: $c_{t,1}$, … , $c_{t,N}$)
  - "$c_{t,j} = \begin{cases} 0 & \text{if } r_{t,j} \text{ contains the anomaly} \\ 1 & \text{if } r_{t,j} \text{ does not contain the anomaly} \end{cases}$ vers
- Data-plane probing result (***D_t***: $d_{t,1}$, …, $d_{t,N}$)
  - "$d_{t,j} = \begin{cases} 1 & \text{if the probe to } f \text{ get a reply} \\ 0 & \text{if the probe to } f \text{ does not get a reply} \end{cases}$

Control- and Data- plane correlation
Hijacking Identification

- Control-plane & data-plane correlation
  - Ideal state

Relationships of D_t and C_t		Possible Reasons
Unrelated	$d_{t,j} = 0$	Firewall, Not Alive
	$d_{t,j} = 1$	Multiple Origin AS
Negatively Correlated	$d_{t,j} = 1 - c_{t,j}$	Origin AS Changing
Positively Correlated	$d_{t,j} = c_{t,j}$	Prefix Hijacking

- **Fingerprint F_t**: correlation coefficient of D_t and C_t
  - Raise a alarm if $F_t > \mu$

$$F_t = \frac{\sum_{j=1}^{m}(c_{t,j} - E(C_t))(d_{t,j} - E(D_t))}{\sqrt{\sum_{j=1}^{m}(c_{t,j} - E(C_t))^2 \times \sum_{j=1}^{m}(d_{t,j} - E(D_t))^2}}$$

Outline

- Introduction
- Argus
- ***Evaluations***
  - ***Detection delay***
  - ***Recent hijackings***
- Conclusions

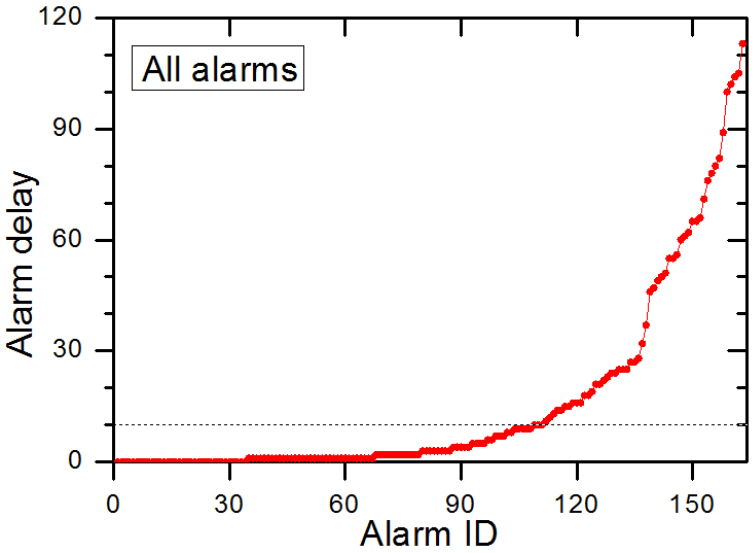
Argus is online

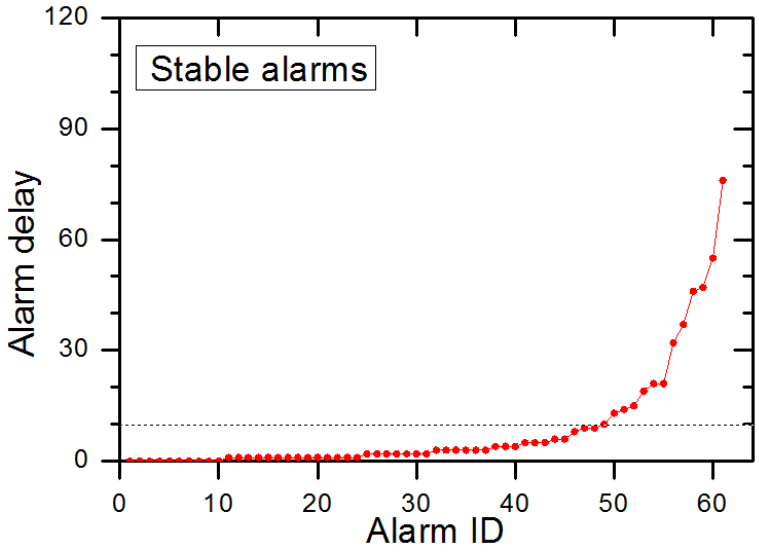
- goo.gl/x0YQc
- Parameters
  - Detection window W = 120 seconds
  - Alarm threshold μ = 0.6
- In the past 4 months:
  - Argus monitored **34659** anomalies,
  - finally figured out **61** possible hijackings.

---- less alarms, ***low false positive*** *rate*

Detection delay

- Most of alarms has a detection delay **less than 10 seconds**



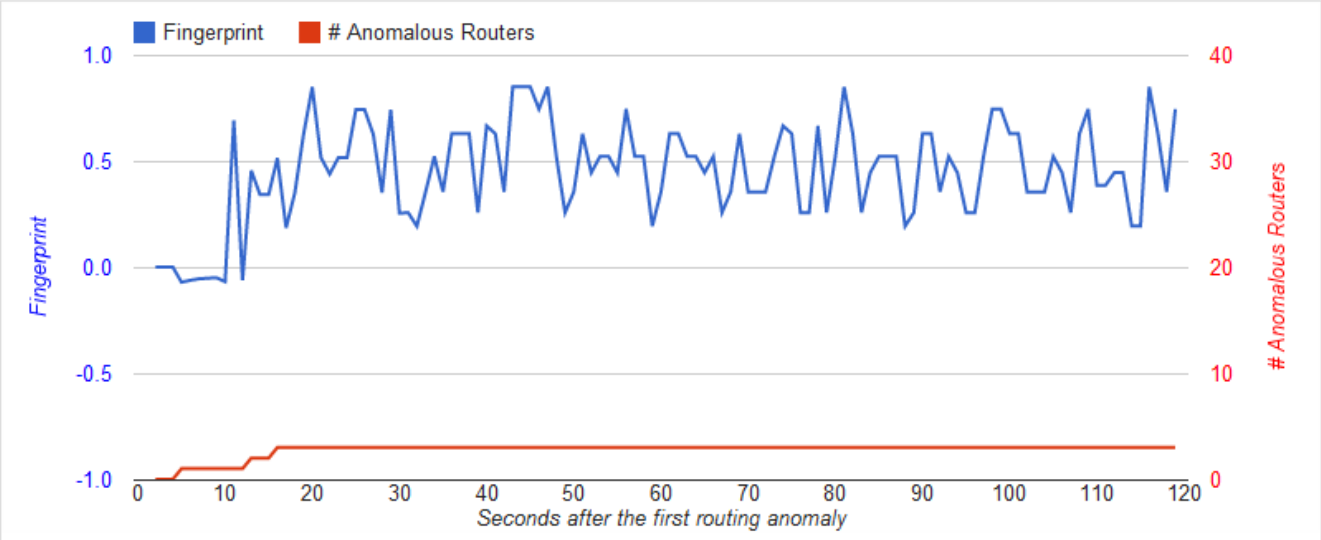


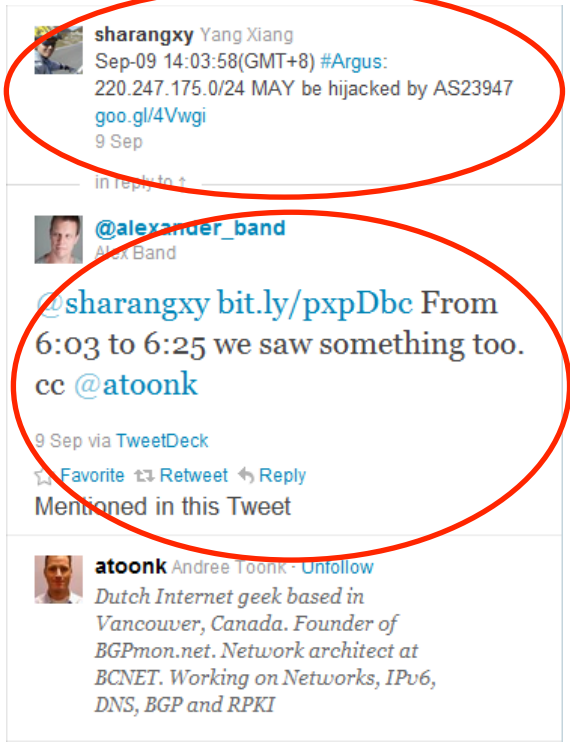
Case Study
Hijacking Alarm /1

Hijacking Alarm Information

Date (UTC)	Timestamp	IP Prefix	Anomalous Origin AS	Alarm Delay (s)	Alarm Lasts (s)	Avg Fing. [.6, 1]
11-09-09 06:03:58	1315548238	220.247.175.0/24	AS23947	9	38	0.70

Fingerprints and # anomalous routers along with time





- Original Home: AS38202 (PT. Mnet **Indonesia** Transit AS)
- Anomalous Home: AS23947 (Internet Service Provider PT.Mora Telematika **Indonesia**)

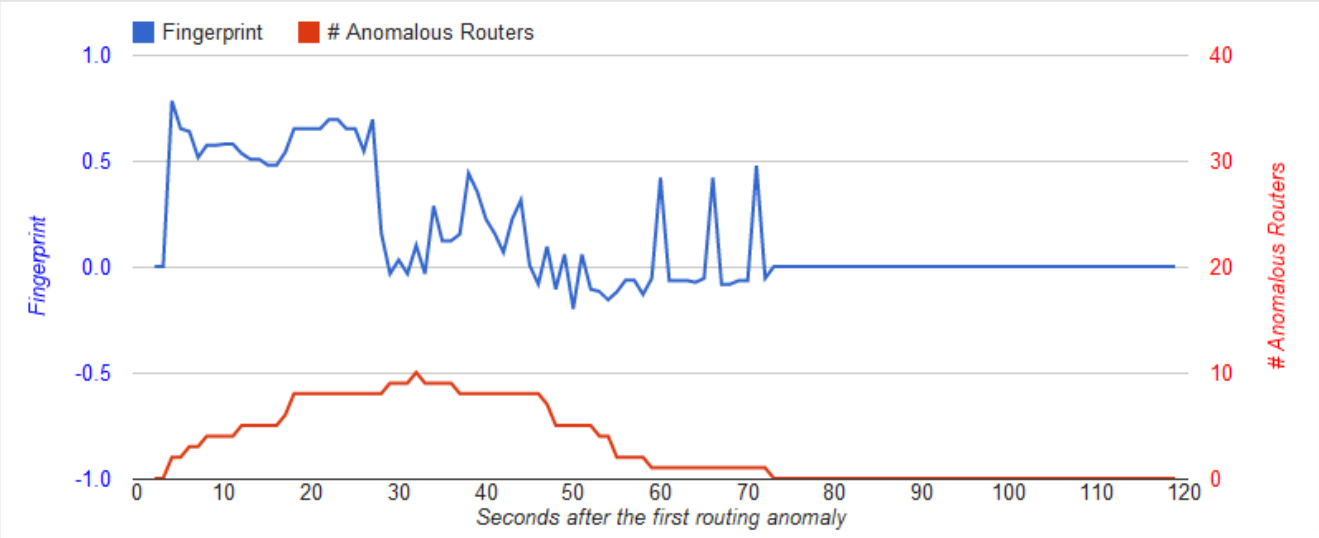
Case Study
Hijacking Alarm /2

Hijacking Alarm Information

Date (UTC)	Timestamp	IP Prefix	Anomalous Origin AS	Alarm Delay (s)	Alarm Lasts (s)	Avg Fing. [.6, 1]
11-06-28 09:00:55	1309251655	91.216.157.0/24	AS35638	2	12	0.67

Short-live hijacking
~ 30 seconds

Fingerprints and # anomalous routers along with time



- Original Home: AS51108 (ASESOFT DISTRIBUTION SRL, EU)
- Anomalous Home: AS35638 (2K Telecom SRL, EU)

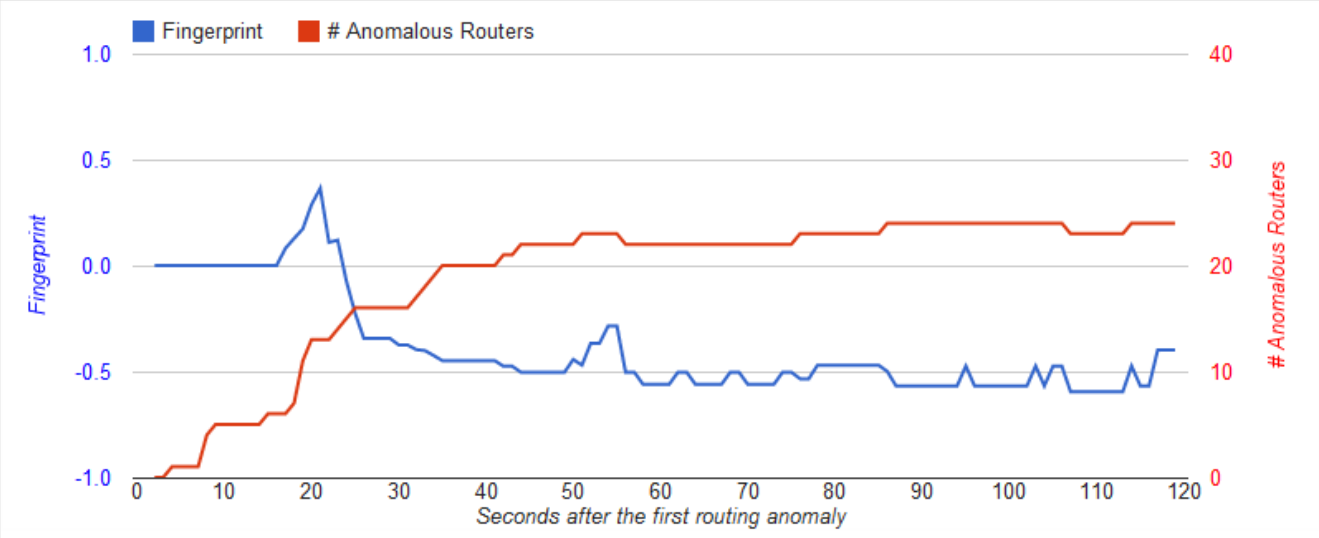
Case Study
Routing Anomaly /1

Routing Anomaly Information

Date (UTC)	Timestamp	IP Prefix	Anomalous Origin AS	Max Fing.	Min Fing.	Avg Fing. [-1, 1]
11-06-23 21:39:27	1308865167	192.203.206.0/24	AS18566	0.36	-0.59	-0.39

Multi-homing

Fingerprints and # anomalous routers along with time



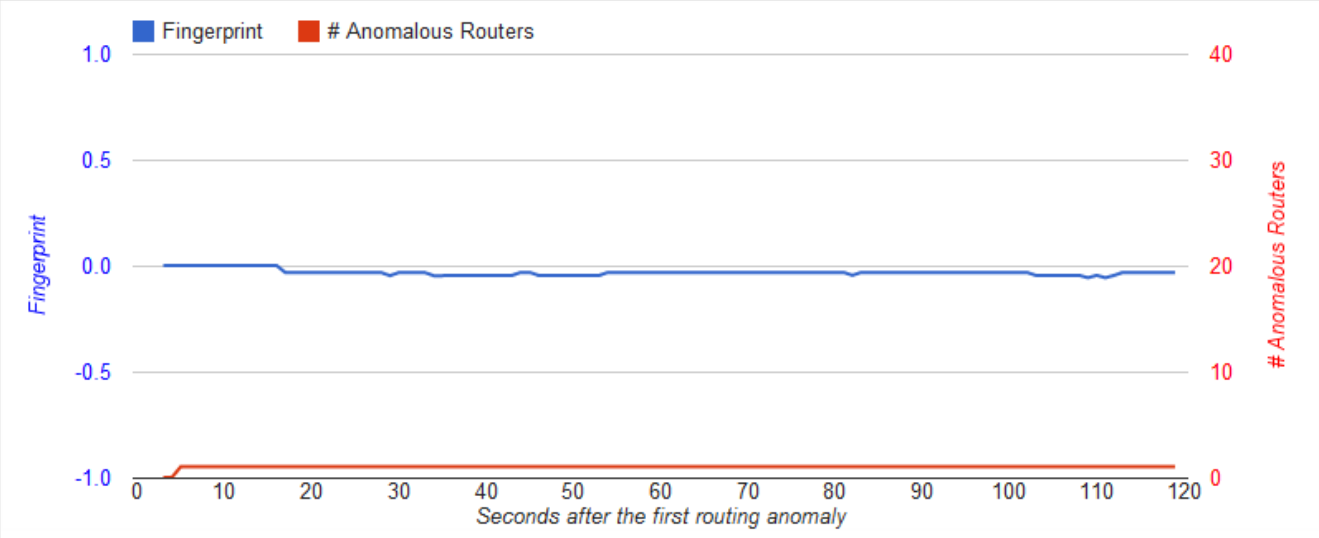
- Original Home: AS18530 (Wonderworks Inc.)
- Anomalous Home: AS18566 (Wonderworks Inc.)

Case Study
Routing Anomaly /2

Routing Anomaly Information

Date (UTC)	Timestamp	IP Prefix	Anomalous Origin AS	Max Fing.	Min Fing.	Avg Fing. [-1, 1]
11-08-03 14:19:07	1312381147	193.0.16.0/24	AS197000	0.00	-0.06	-0.03

Fingerprints and # anomalous routers along with time



BGP Anycast
(*Root-DNS server*)

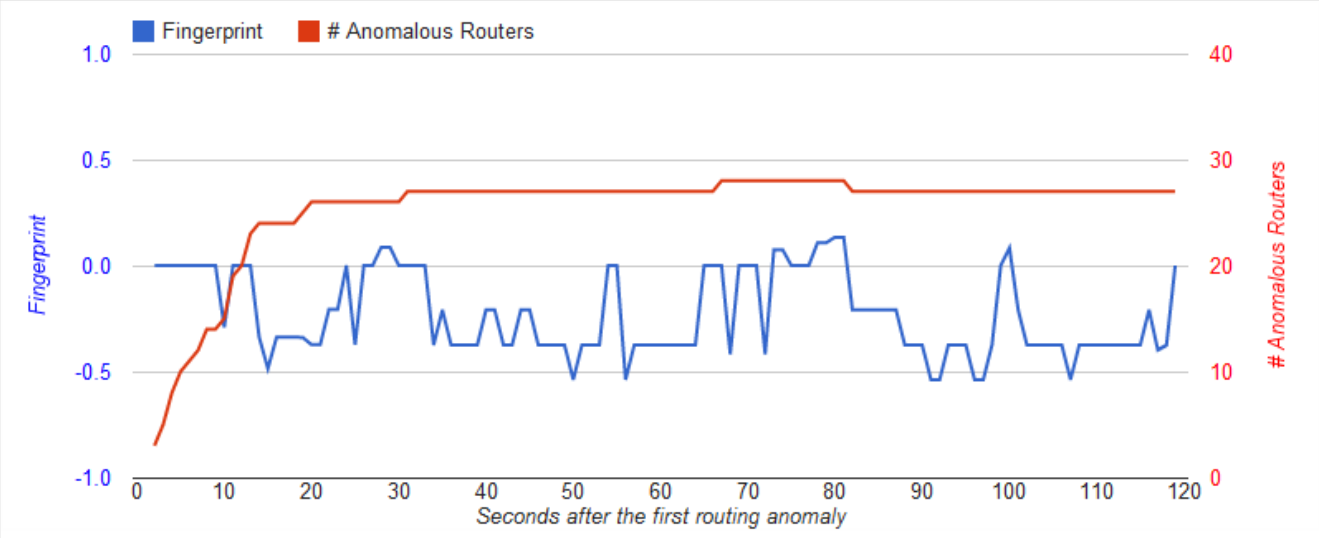
- Original Home: AS25152 (Support network for **k.root-servers.net**)
- Anomalous Home: AS197000 (Support network for **k.root-servers.net**)

Case Study
Routing Anomaly /3

Routing Anomaly Information

Date (UTC)	Timestamp	IP Prefix	Anomalous Origin AS	Max Fing.	Min Fing.	Avg Fing. [-1, 1]
11-08-23 02:07:58	1314065278	199.7.60.0/24	AS36630	0.13	-0.54	-0.23

Fingerprints and # anomalous routers along with time



BGP Anycast (*Veri-sign*)

- Original Home: AS36618 (VeriSign Global Registry Services)
- Anomalous Home: AS36630 (VeriSign Global Registry Services)

Outline

- Introduction
- Argus
- Evaluations
  - Detection delay
  - Recent hijackings
- ***Conclusions***

Review of design goals

Accurate	Control **x** Data plane correlation 61 alarms out of 34659 anomalies (low false positive)
Real-time	Simple & efficient commands ***ping***, ***show ip bgp*** (complete immediately)
Easy to deploy	Public interface/service directly use existing public route-servers
Perceptive	Control-plane monitoring
Scalable	Control-plane driving

Future works

- Accuracy
  - Looking glasses
- Ground truth
  - Evaluate the false positive/negative rate of Argus
  - Manual analysis, Simulation, Email confirmation, …

Thanks!
Q & A

- Introduction
  - Background - Prefix hijacking
  - Existing detection methods
  - Our proposal
- Argus
  - **Design goals: Accurate, Real-time, Easy to deploy, …**
  - Architecture
  - Hijacking identification
- Evaluations
  - Detection delay
  - Recent hijackings
- Conclusions

goo.gl/x0YQc

twitter.com/sharangxy