Tempest:
Temporal Dynamics in Anonymity Systems

Ryan Wails — *U.S. Naval Research Laboratory*
Yixin Sun — *Princeton University*
Aaron Johnson — *U.S. Naval Research Laboratory*
Mung Chiang — *Princeton University*
Prateek Mittal — *Princeton University*

PETS '18 25 July 2018

Introduction

Motivation

- Tor (USENIX 2004)
- DeNASA (PETS 2016)
- Counter-RAPTOR (S&P 2017)
- TAPS (NDSS 2017)
- LAP (S&P 2012)
- HORNET (CCS 2015)
- Dovetail (PETS 2014)
- PHI (PETS 2017)

Prior work:
static security analyses

Our Contribution: Three Temporal Dynamics

Our Contribution: Three Temporal Dynamics

1. **Client Mobility**: Clients move over time

Our Contribution: Three Temporal Dynamics

1. **Client Mobility**: Clients move over time
2. **User Behavior**: Users make many connections over time

Our Contribution: Three Temporal Dynamics

1. **Client Mobility**: Clients move over time
2. **User Behavior**: Users make many connections over time
3. **Routing Changes**: Internet routes change over time

Temporal Dynamics & Anonymity Systems

		Client Mobility	User Behavior	Routing Changes
Tor	Tor DeNASA Counter-RAPTOR TAPS			

Legend: Vulnerability ✗ Resistance ✓

Temporal Dynamics & Anonymity Systems

		Client Mobility	User Behavior	Routing Changes
Tor	Tor DeNASA Counter-RAPTOR TAPS			
Net-Layer	HORNET LAP Dovetail PHI			

Legend: Vulnerability ✗ Resistance ✓

Temporal Dynamics & Anonymity Systems

		Client Mobility	User Behavior	Routing Changes
Tor	Tor		Known ✗	Known ✗
	DeNASA			
	Counter-RAPTOR			Known ✓
	TAPS		Known ✓	
Net-Layer	HORNET			
	LAP			
	Dovetail			
	PHI			

Legend: Vulnerability ✗ Resistance ✓

Temporal Dynamics & Anonymity Systems

		Client Mobility	User Behavior	Routing Changes
Tor	Tor	Novel ✗	Known ✗	Known ✗
	DeNASA	Novel ✗	Novel ✗	
	Counter-RAPTOR	Novel ✗	Novel ✓	Known ✓
	TAPS		Known ✓	Novel ✗
Net-Layer	HORNET	Novel ✗		Novel ✗
	LAP	Novel ✗		Novel ✗
	Dovetail		Novel ✗	
	PHI		Novel ✗	

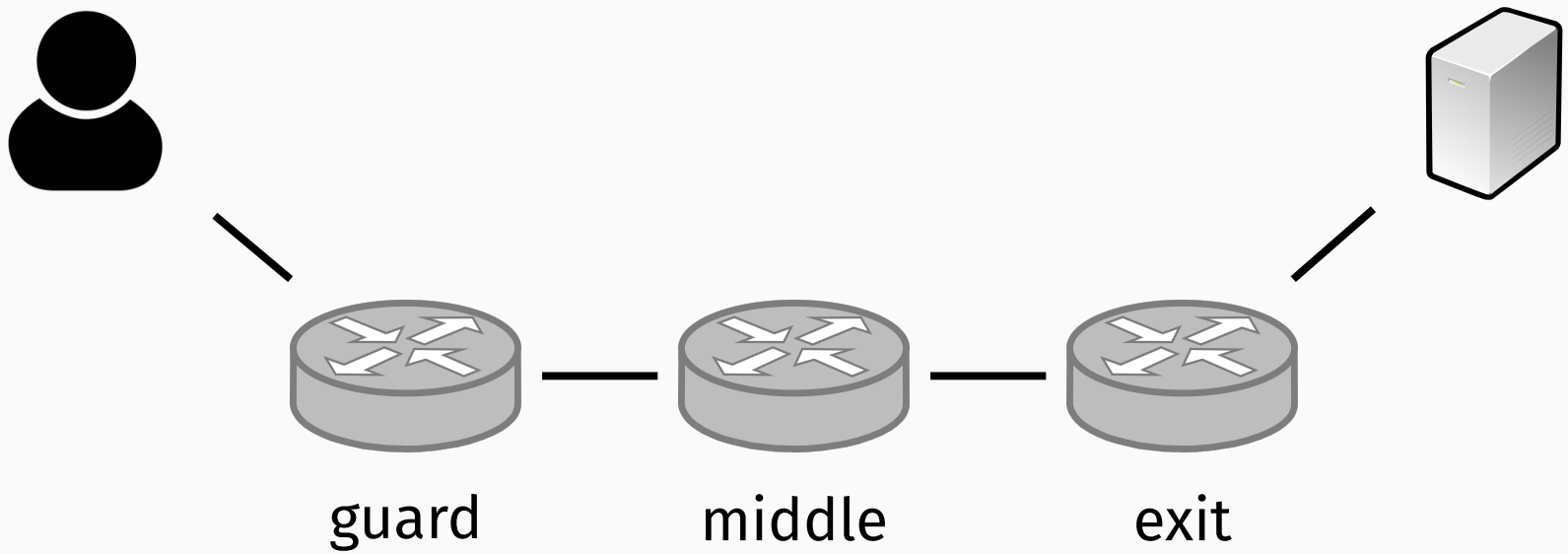
Legend: Vulnerability ✗ Resistance ✓

Outline

1. **Client Mobility & Tor**
2. **User Behavior & DeNASA**

Brief Tor Background

Tor Background



1. Clients use only one guard for a few months
2. Relays are selected with probability prop. to bandwidth

Client Mobility & Tor

Client Mobility Example

Ryan as an example...

Client Mobility Example

Connected to Tor from

1) Home

Which networks (ASes) saw my ingress Tor traffic?

Client Mobility Example

Connected to Tor from

1) Home

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb Comcast Telia

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop 3) Mobile Hotspot

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb Comcast Telia

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop 3) Mobile Hotspot

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb Comcast Telia AT&T

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop 3) Mobile Hotspot 4) Airport

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb Comcast Telia AT&T

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop 3) Mobile Hotspot 4) Airport

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb Comcast Telia AT&T Zayo

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop 3) Mobile Hotspot 4) Airport
5) Hotel

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb Comcast Telia AT&T Zayo

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop 3) Mobile Hotspot 4) Airport 5) Hotel

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb Comcast Telia AT&T Zayo TelefonicaEspaña Telxius

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop 3) Mobile Hotspot 4) Airport
5) Hotel 6) CCCB

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb Comcast Telia AT&T Zayo TelefonicaEspaña Telxius

Client Mobility Example

Connected to Tor from

1) Home 2) Coffee Shop 3) Mobile Hotspot 4) Airport
5) Hotel 6) CCCB

Which networks (ASes) saw my ingress Tor traffic?

Verizon Tata LeaseWeb Comcast Telia AT&T Zayo
TelefonicaEspaña Telxius OrangeEspaña

Client Mobility Example

During travel from United States to Spain:

- Connected to Tor from **6 different locations**
- Exposed my traffic to additional **7 ASes (3.3× increase)**

Adversary Model

- Adversary compromises a single AS
- Passive
- Goal: observe client-guard traffic

Mobility Analysis

1. How mobile are some clients?
2. Does mobility weaken system security?

Mobility Datasets

1. Foursquare (F)

- 270,000 users
- 18 months (Apr 2012 – Sep 2013)

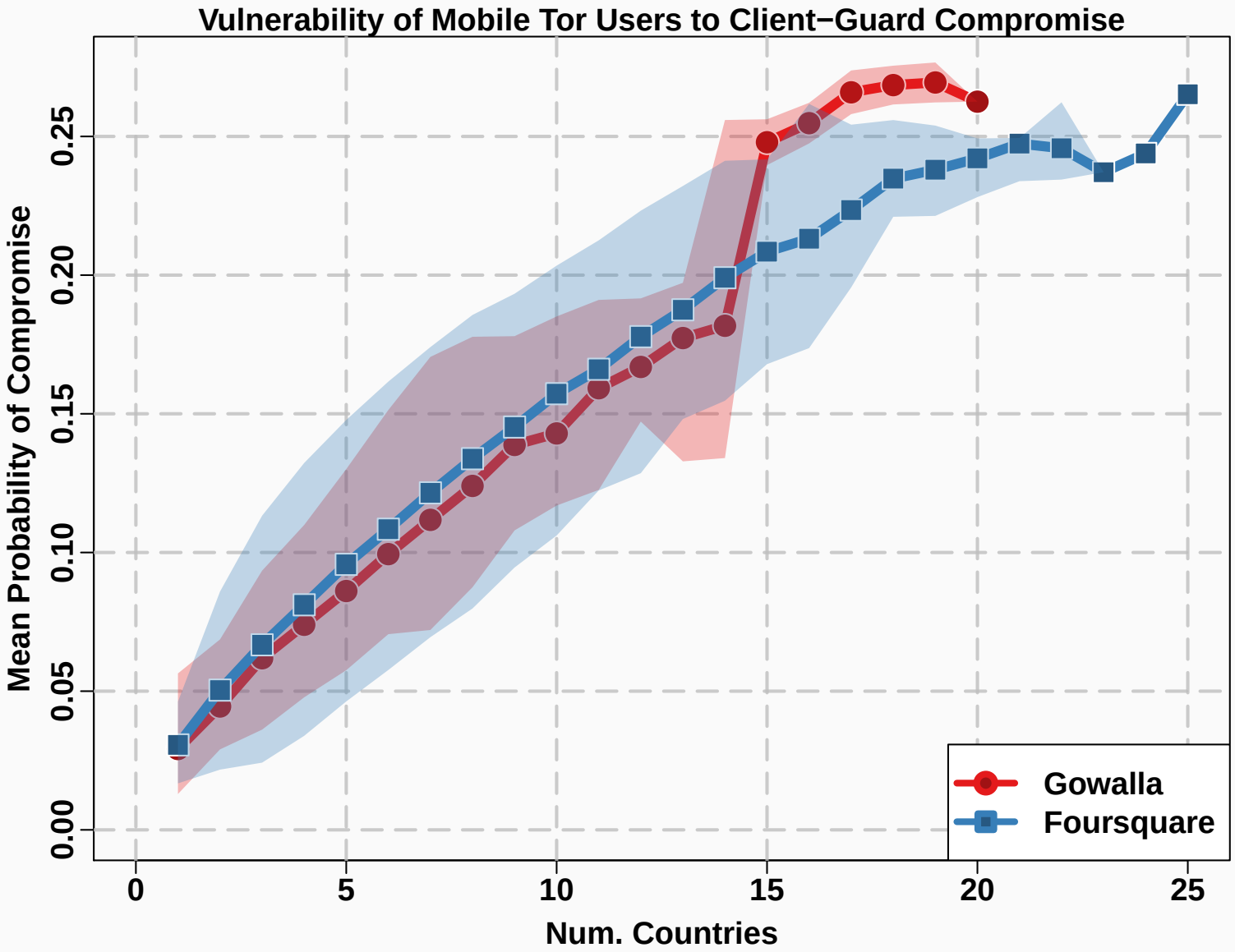
2. Gowalla (G)

- 100,000 users
- 20 months (Feb 2009 – Oct 2010)

# Countries		**2**	**3**	**4**	**5**	**6**	**$\geq$ 7**
Users	F	40145	13179	5649	2708	1490	2574
Users	G	17884	4557	1694	705	305	299
Q_1 Days	F	48	120	195	228	248	245
Q_1 Days	G	7	31	56	77	103	125

Mobility & Tor

- Assume each user connects from most popular Tor AS in each country.
- Compute average probability that largest 50 ASes compromise client-guard path.



Points denote median user, shade shows range

Takeaways

1. Many clients are mobile!
2. Mobility can reduce system security.

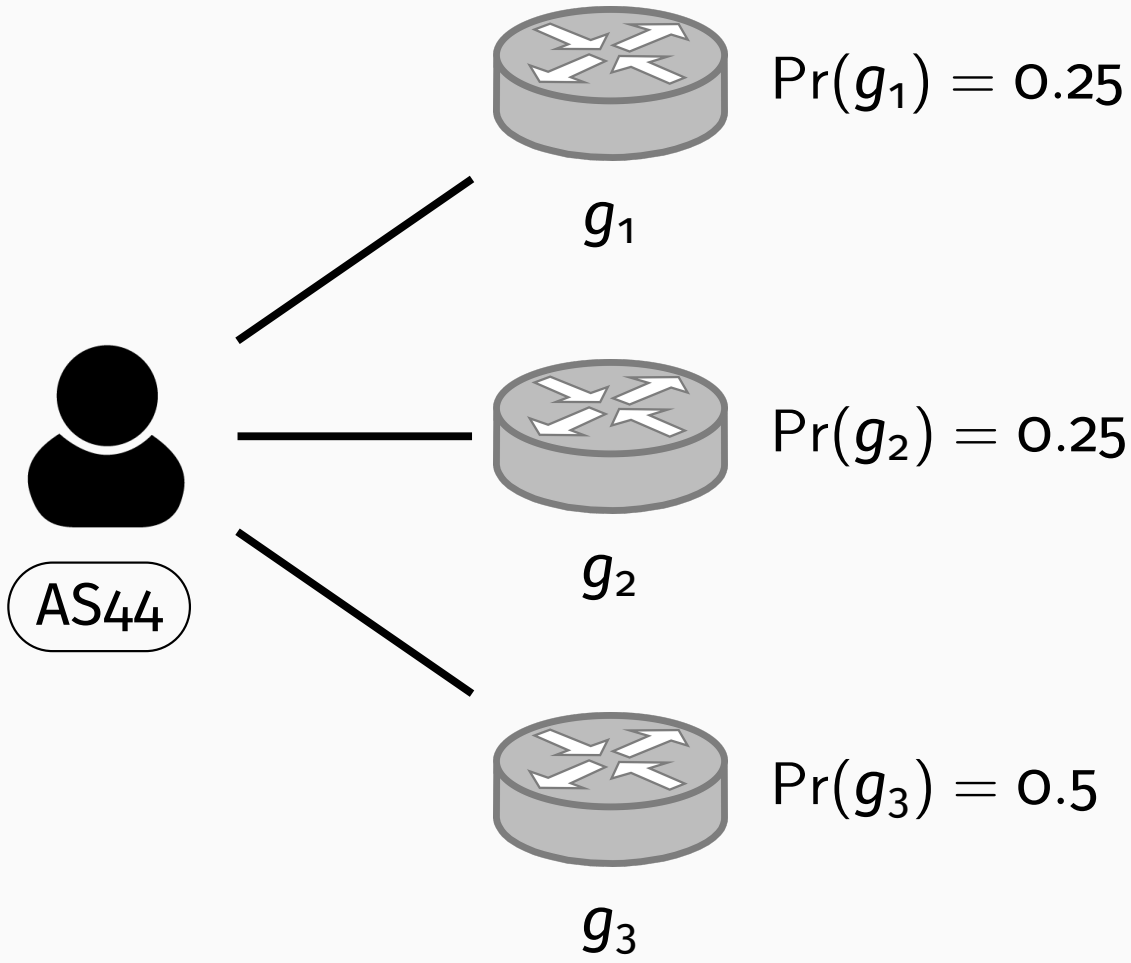
User Behavior & DeNASA (PETS 2016)

DeNASA

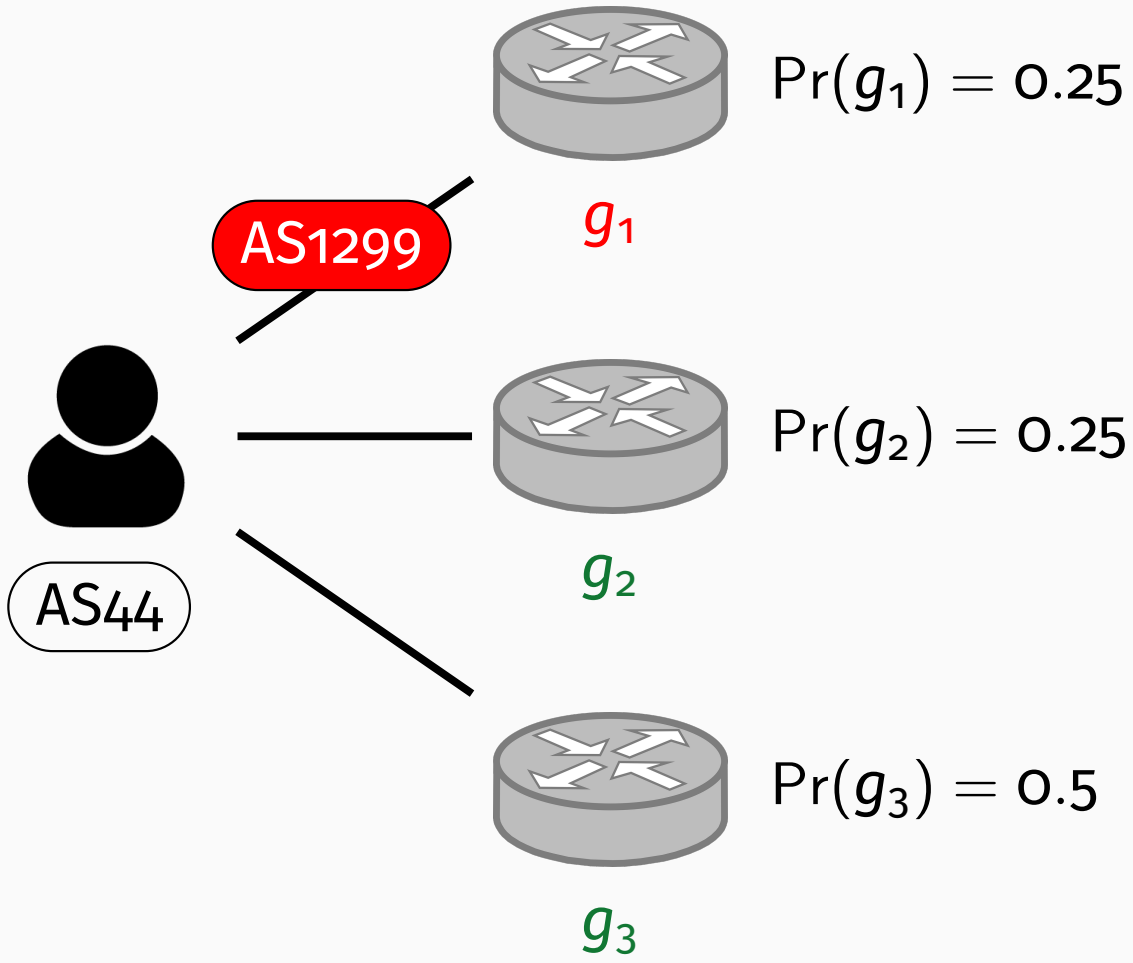
The DeNASA “g-select” algorithm:

Do not select guards where *suspects* AS1299 (Telia) or AS3356 (Level 3) are on the client-guard link.

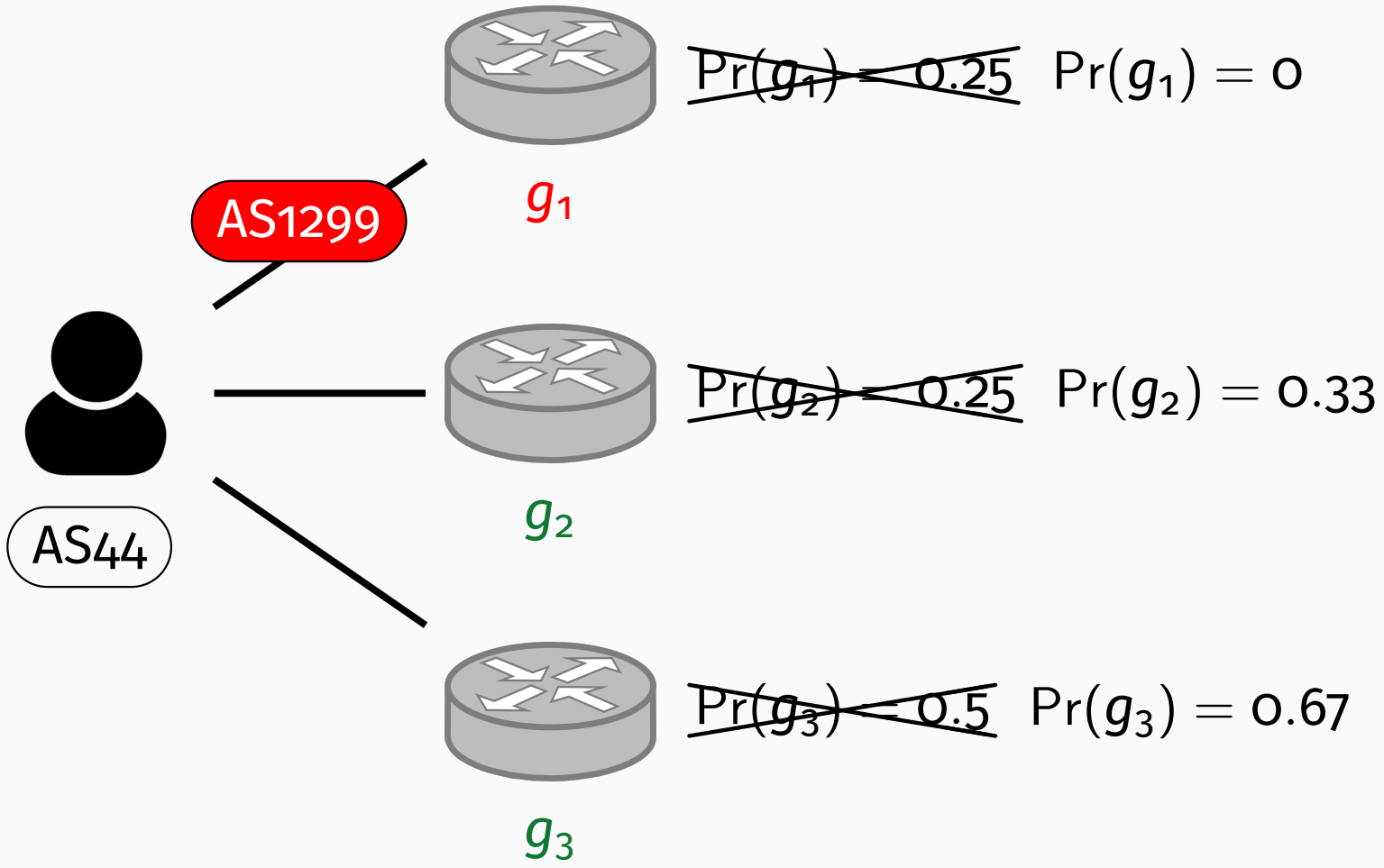
DeNASA Example



DeNASA Example



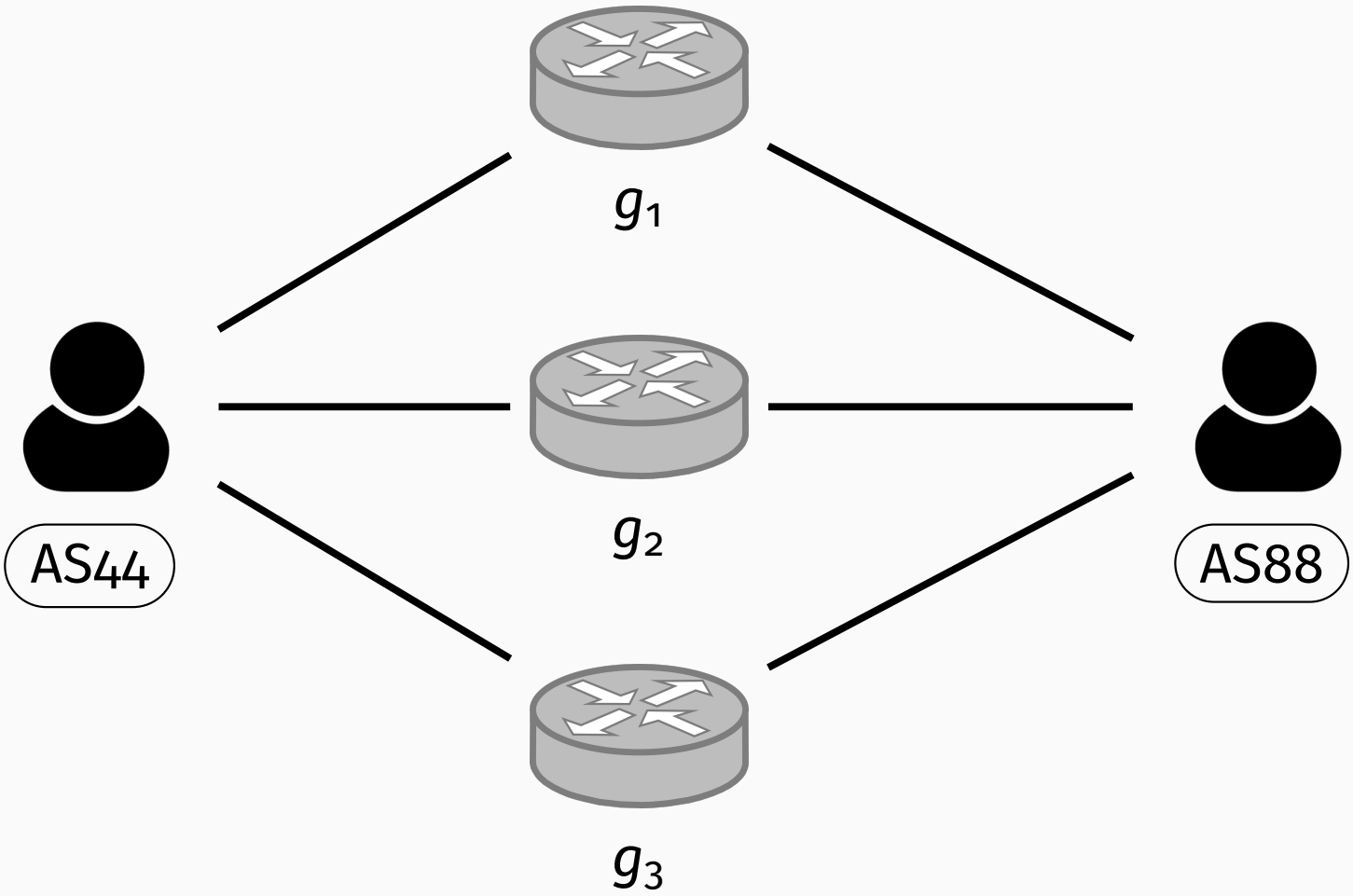
DeNASA Example



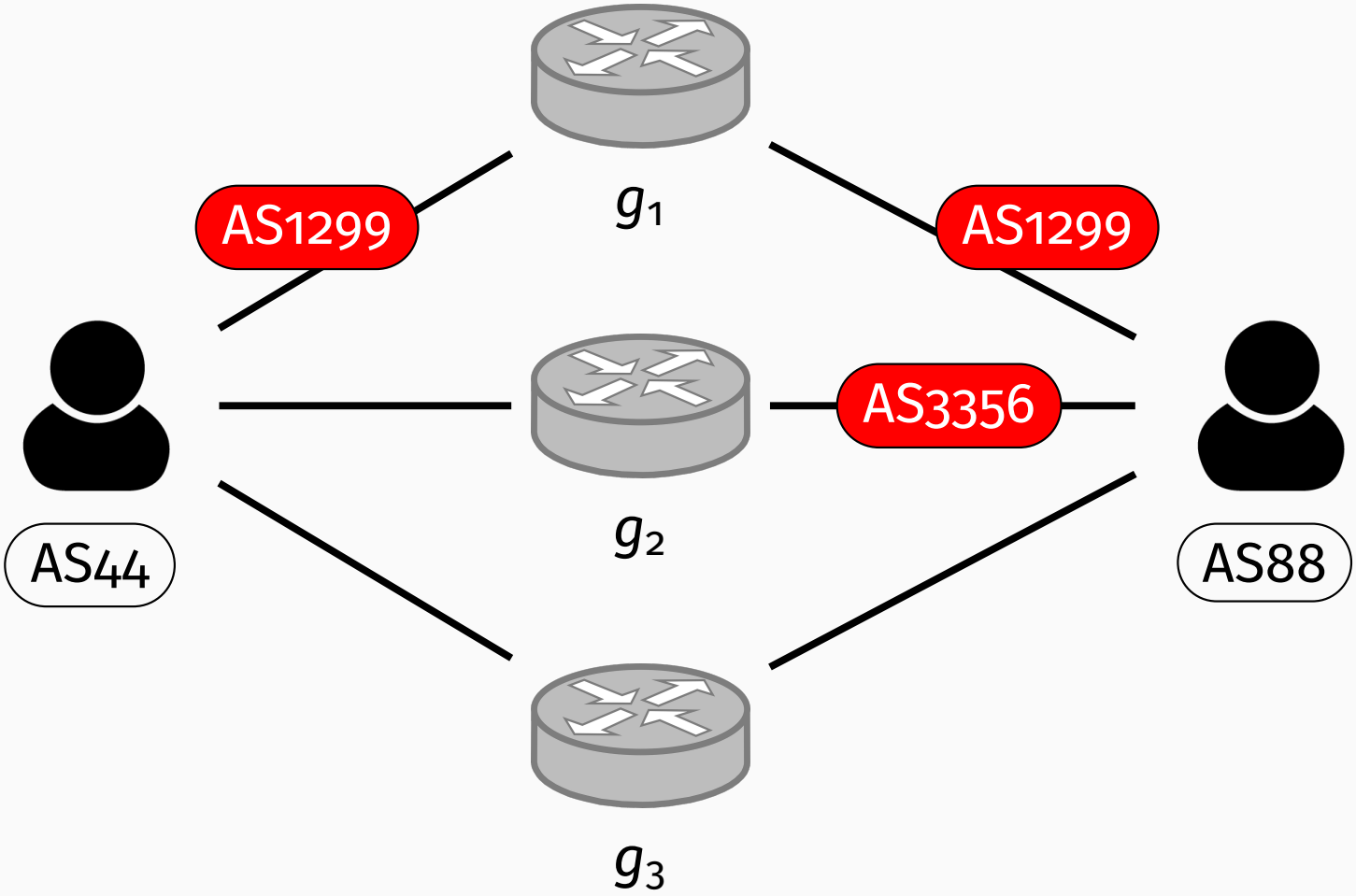
DeNASA Example

g-select leaks location information!

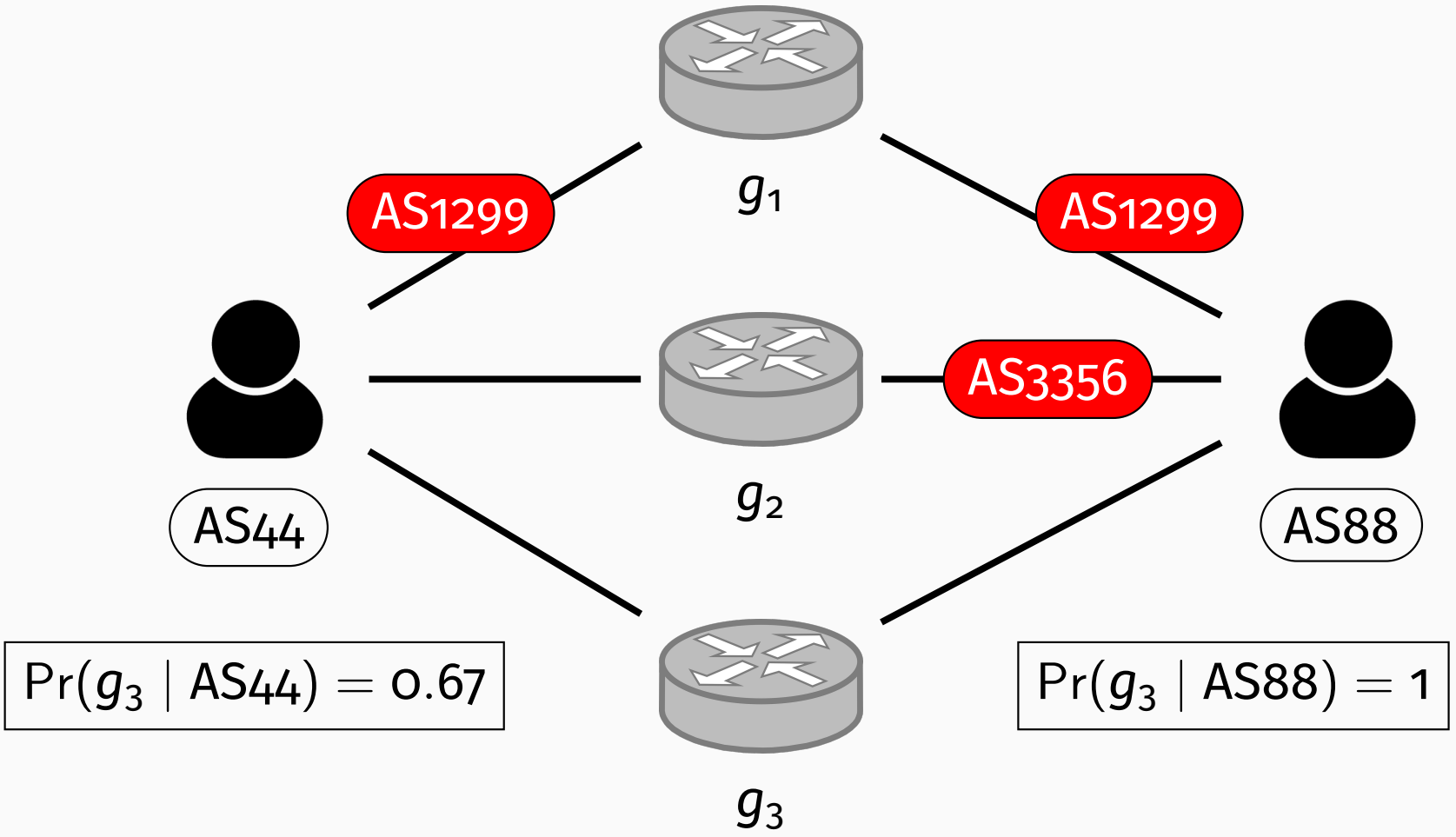
DeNASA Example



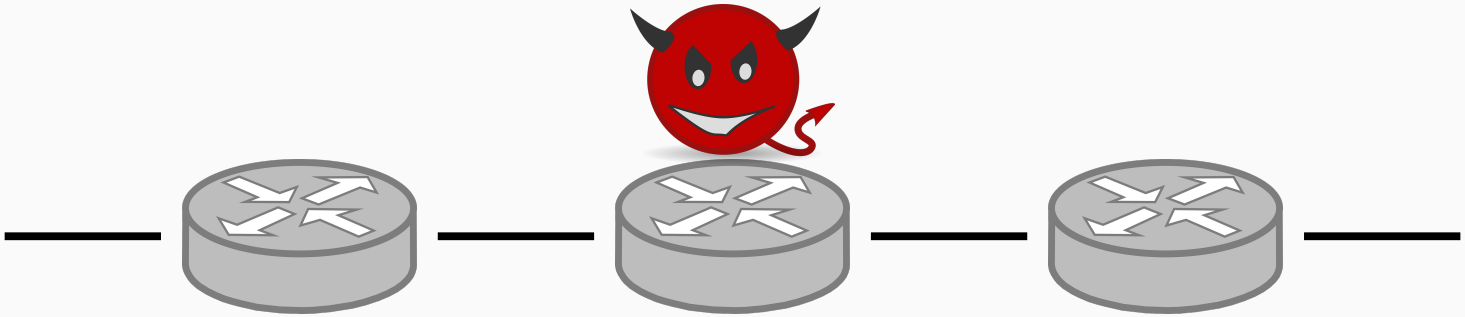
DeNASA Example



DeNASA Example



DeNASA Example



$$\boxed{\Pr(\text{AS44} \mid g_3) = 0.4}$$

$$\boxed{\Pr(\text{AS88} \mid g_3) = 0.6}$$

Our Tempest Attack

Leak worsens over time!

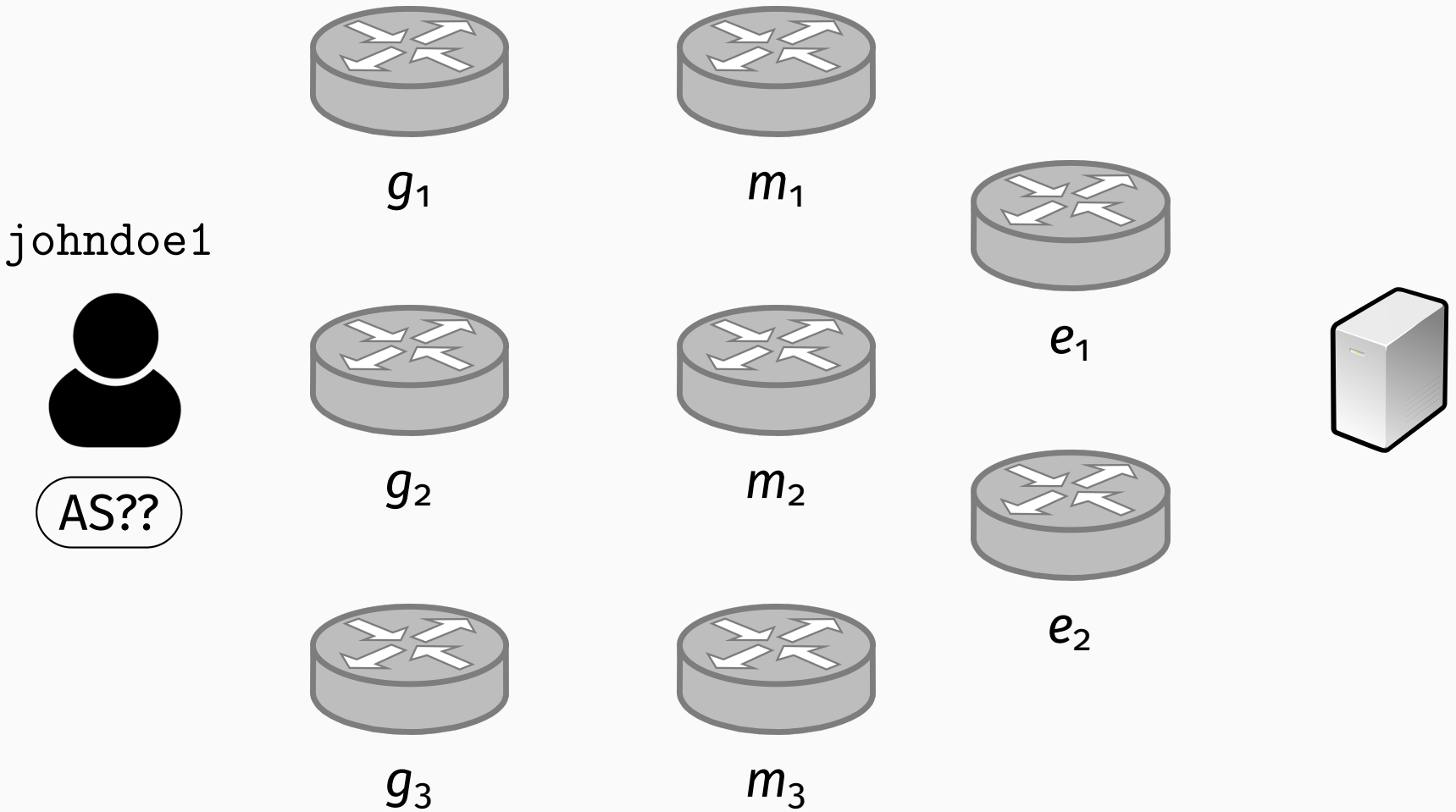
$$\Pr(\text{AS88} \mid G_1 \wedge G_2 \wedge \cdots \wedge G_N) \gg \Pr(\text{AS44} \mid G_1 \wedge G_2 \wedge \cdots \wedge G_N)$$

How can the adversary learn a client's guard history?

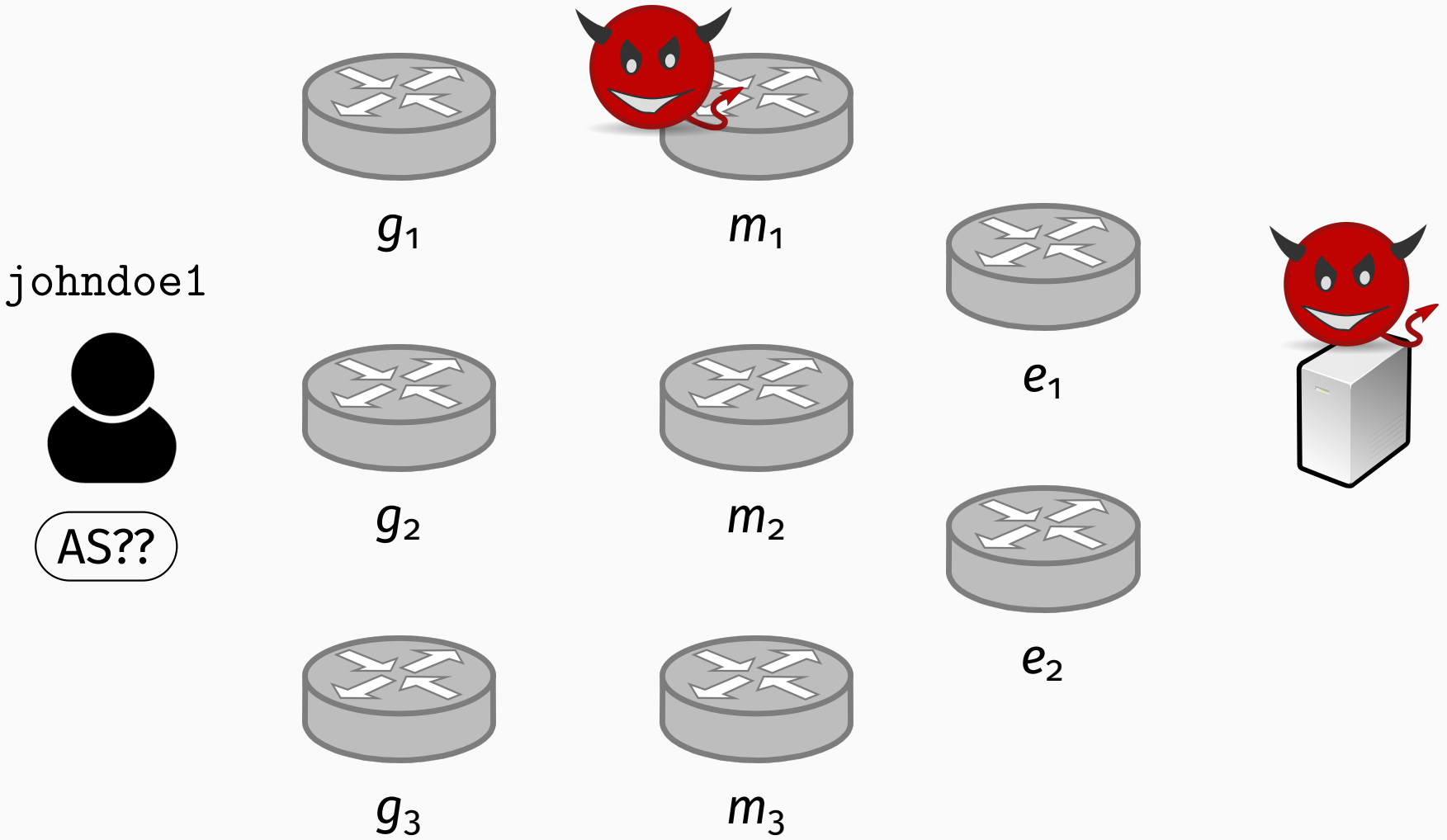
Adversary Model

- Adversary runs a destination and some relays
- Passive
- Goal: learn client AS

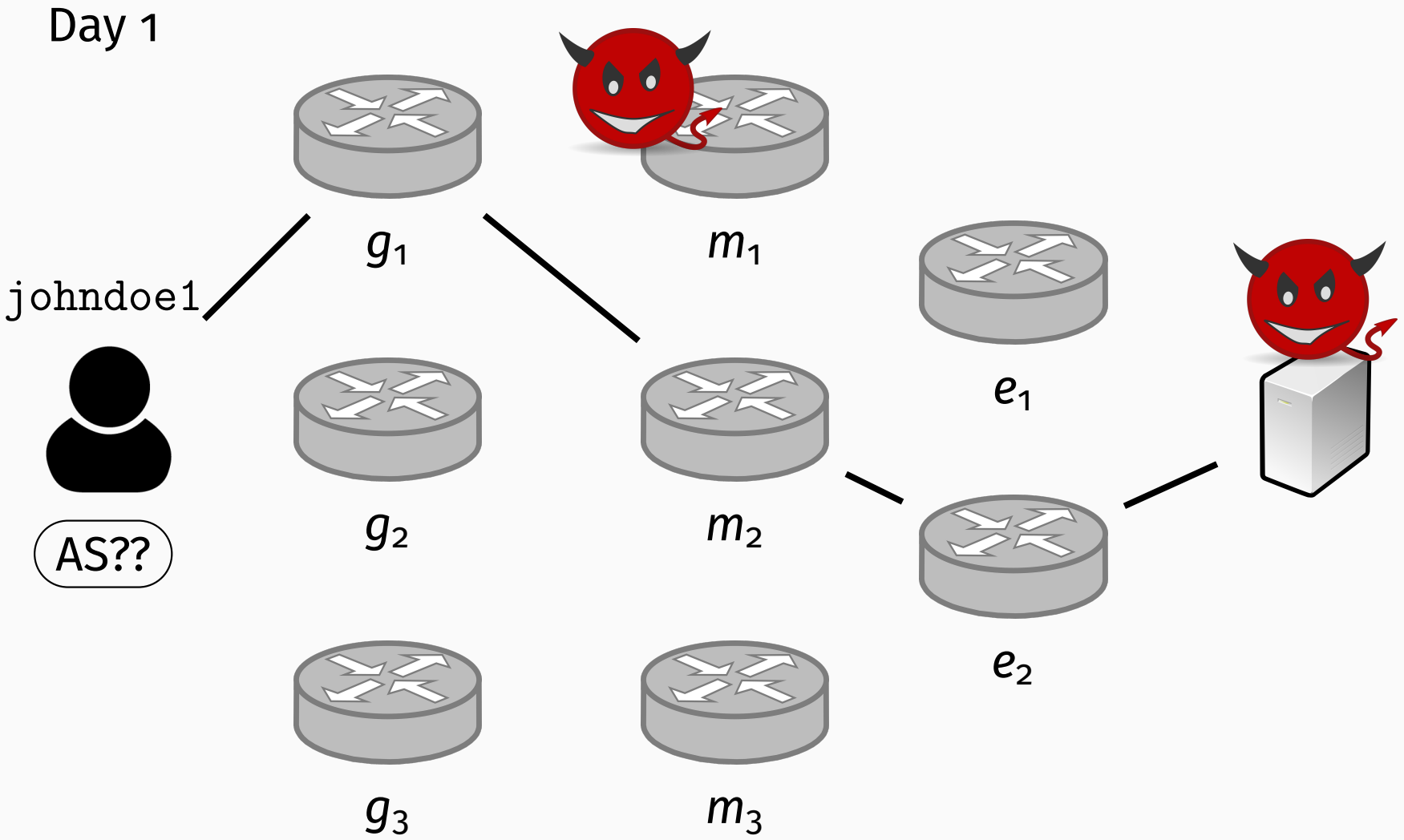
Discovering guards over time



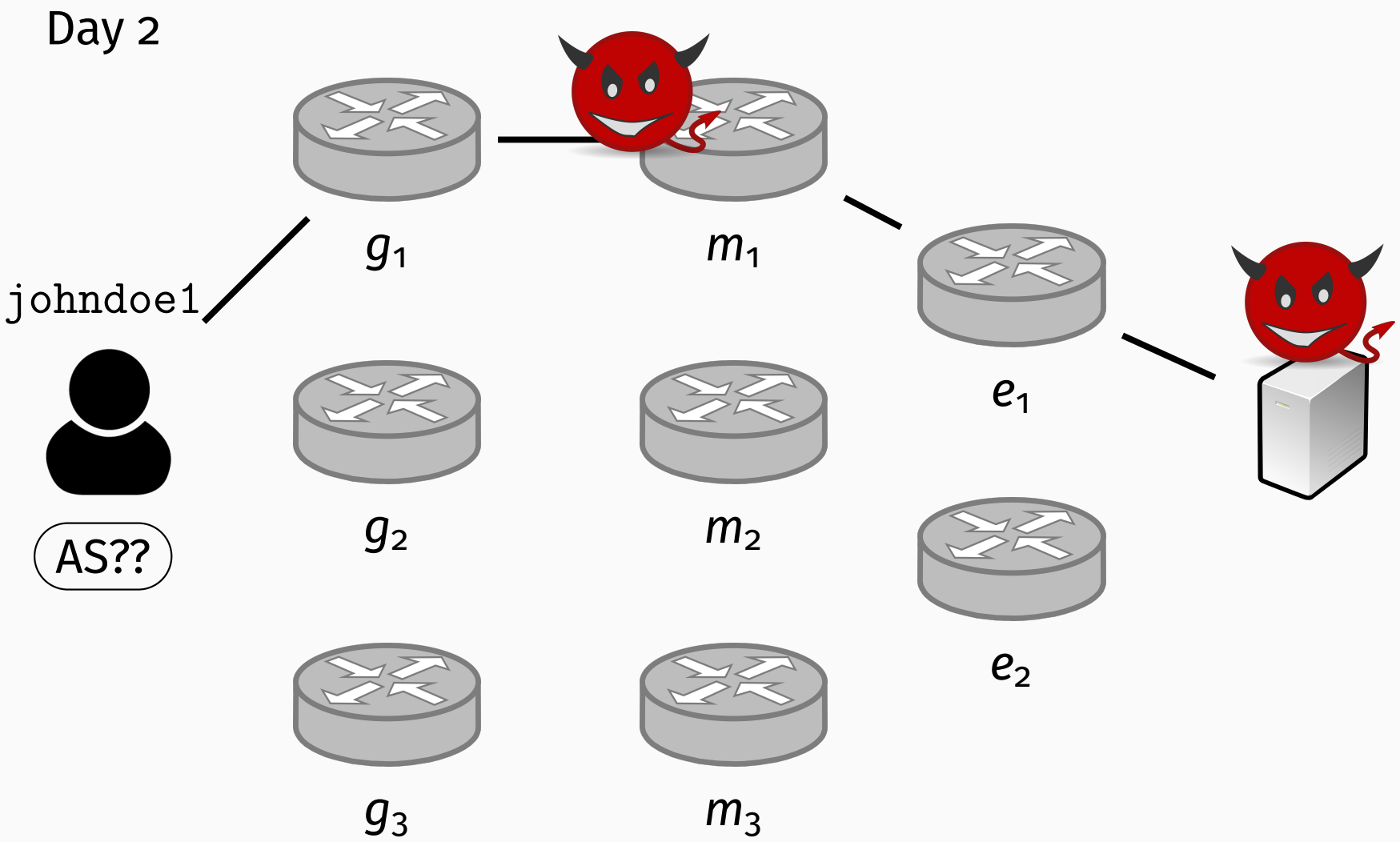
Discovering guards over time



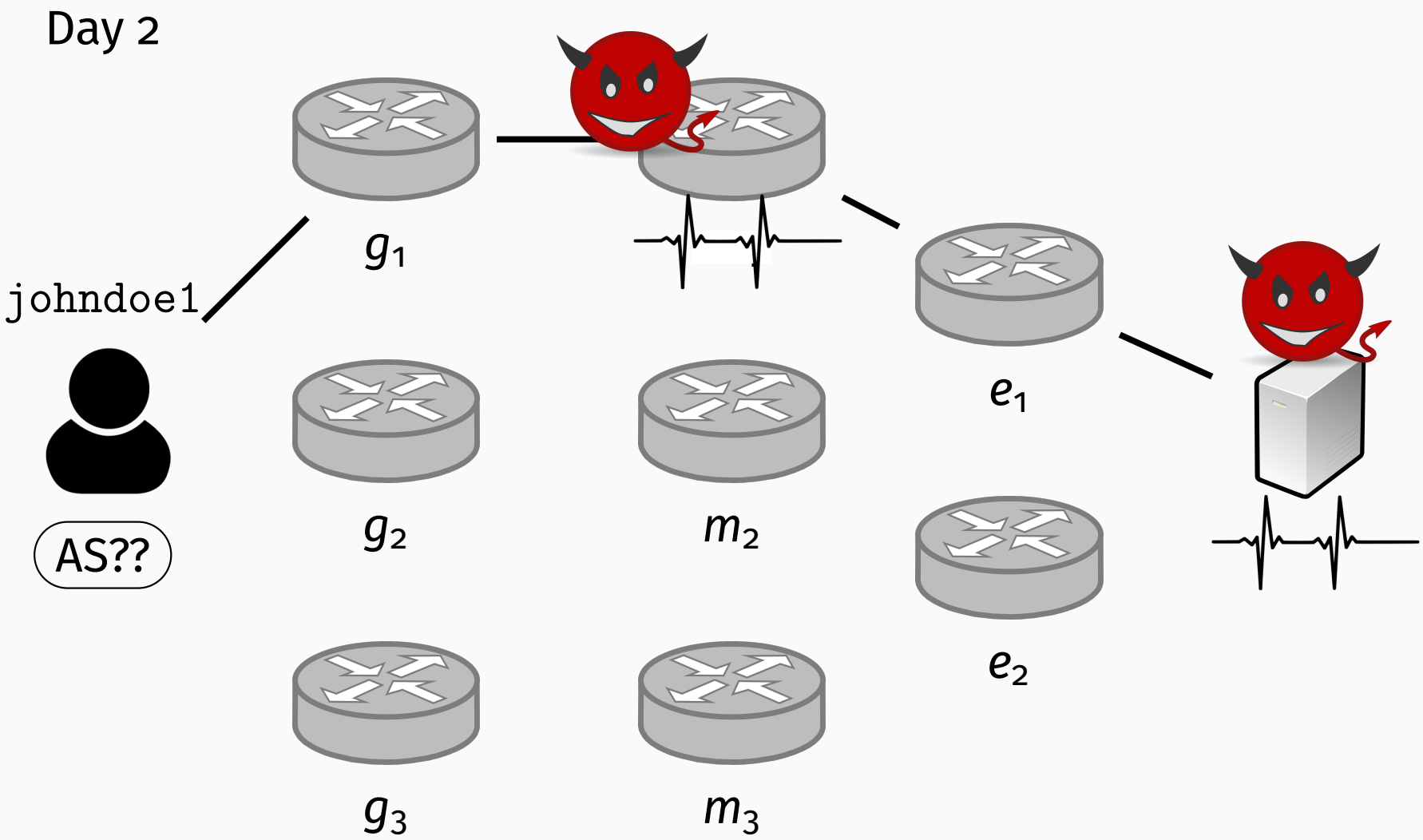
Discovering guards over time



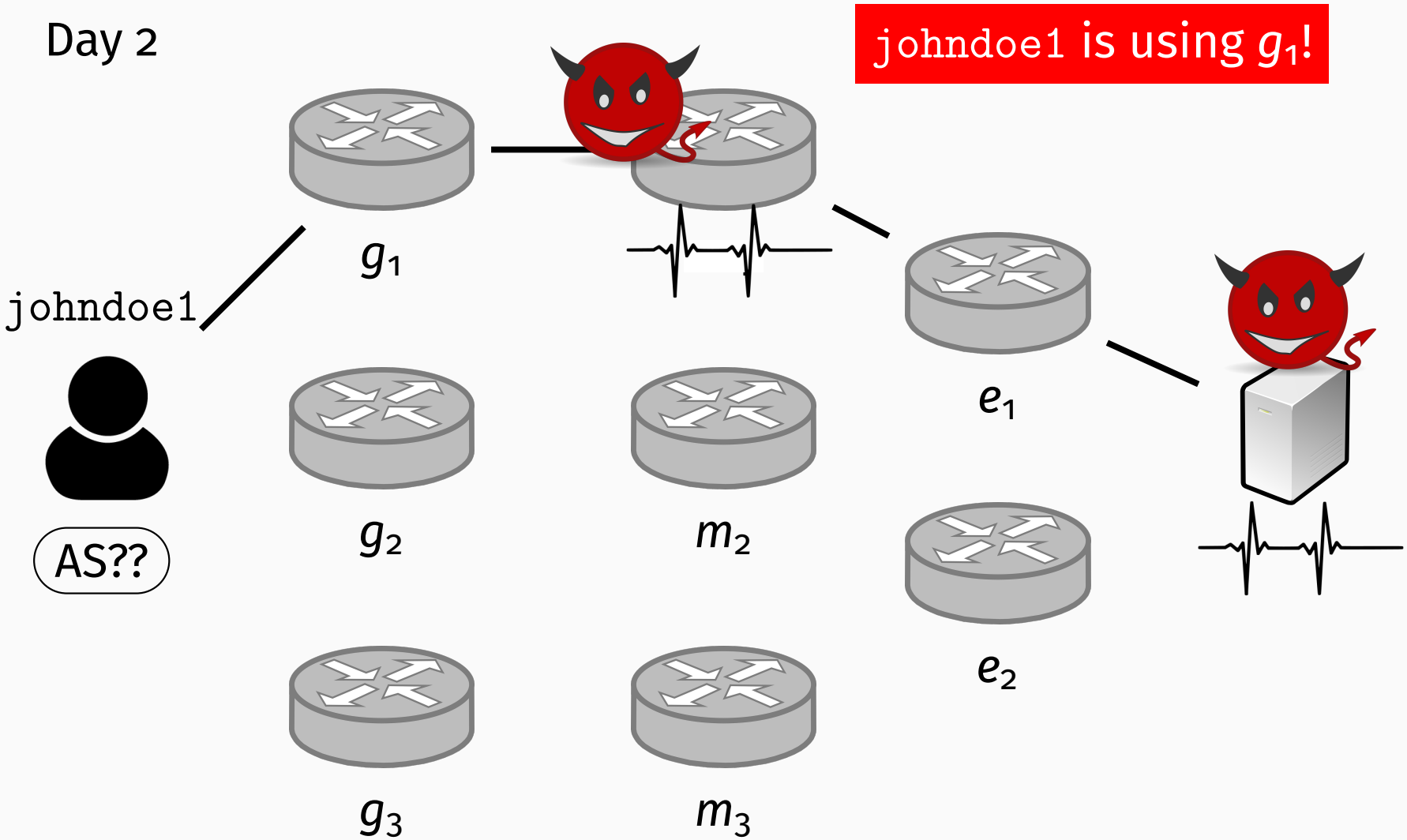
Discovering guards over time



Discovering guards over time



Discovering guards over time

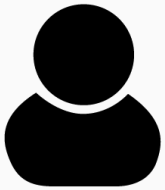


Discovering guards over time

Day 3

m_1

`johndoe1`



AS??

g_2

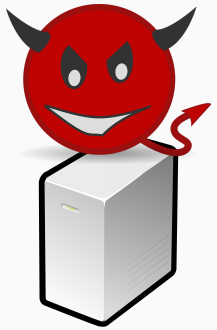
m_2

e_1

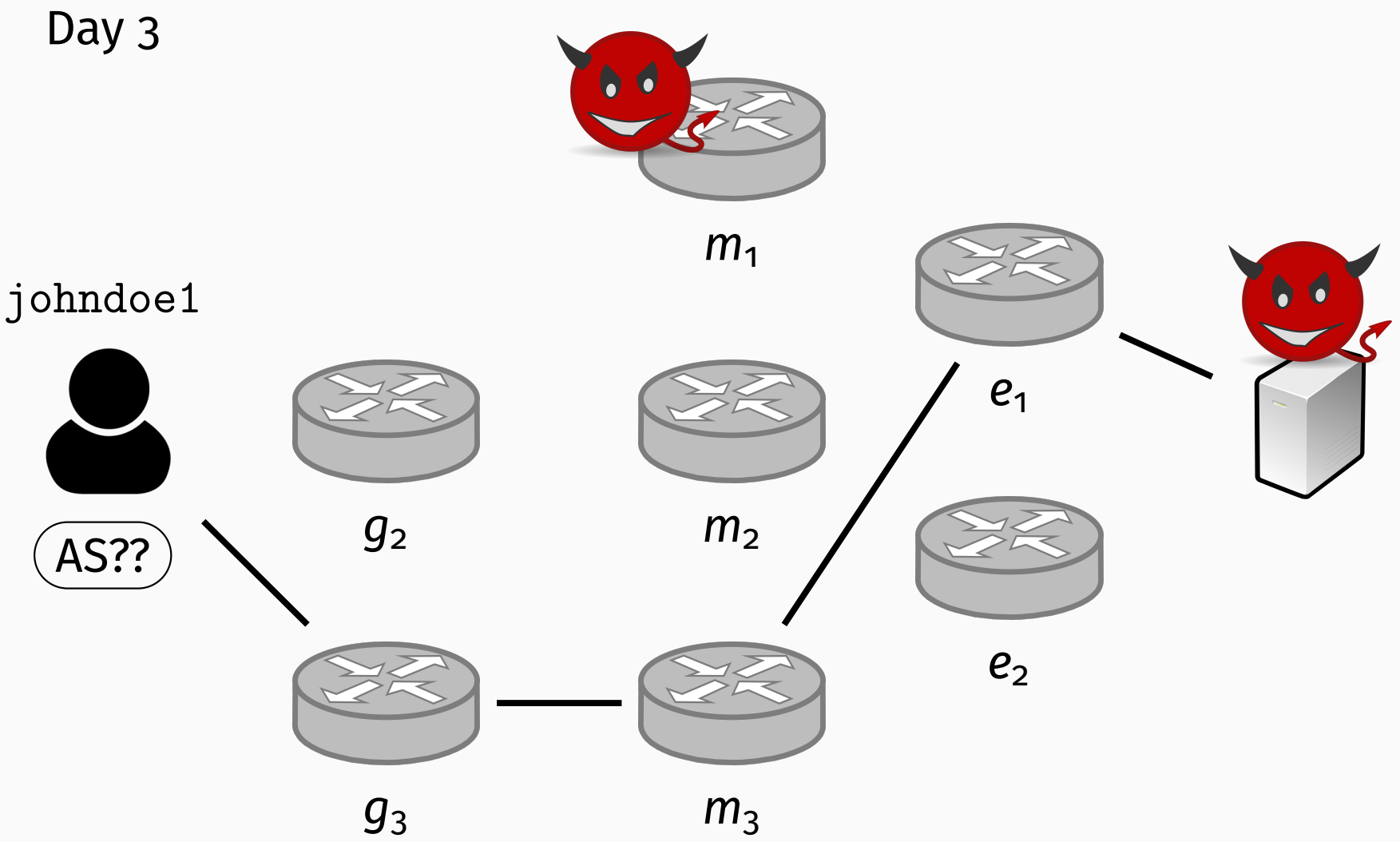
e_2

g_3

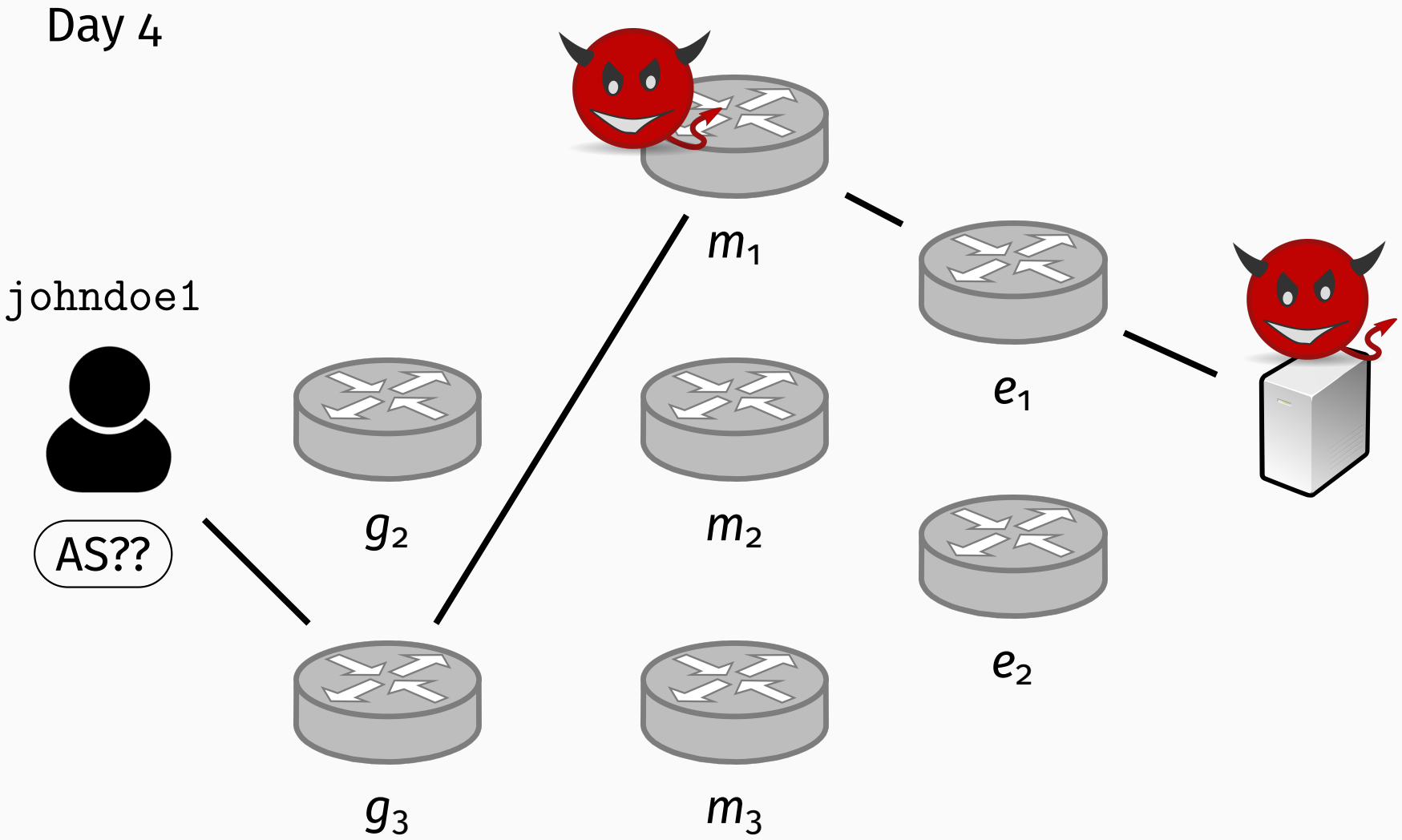
m_3



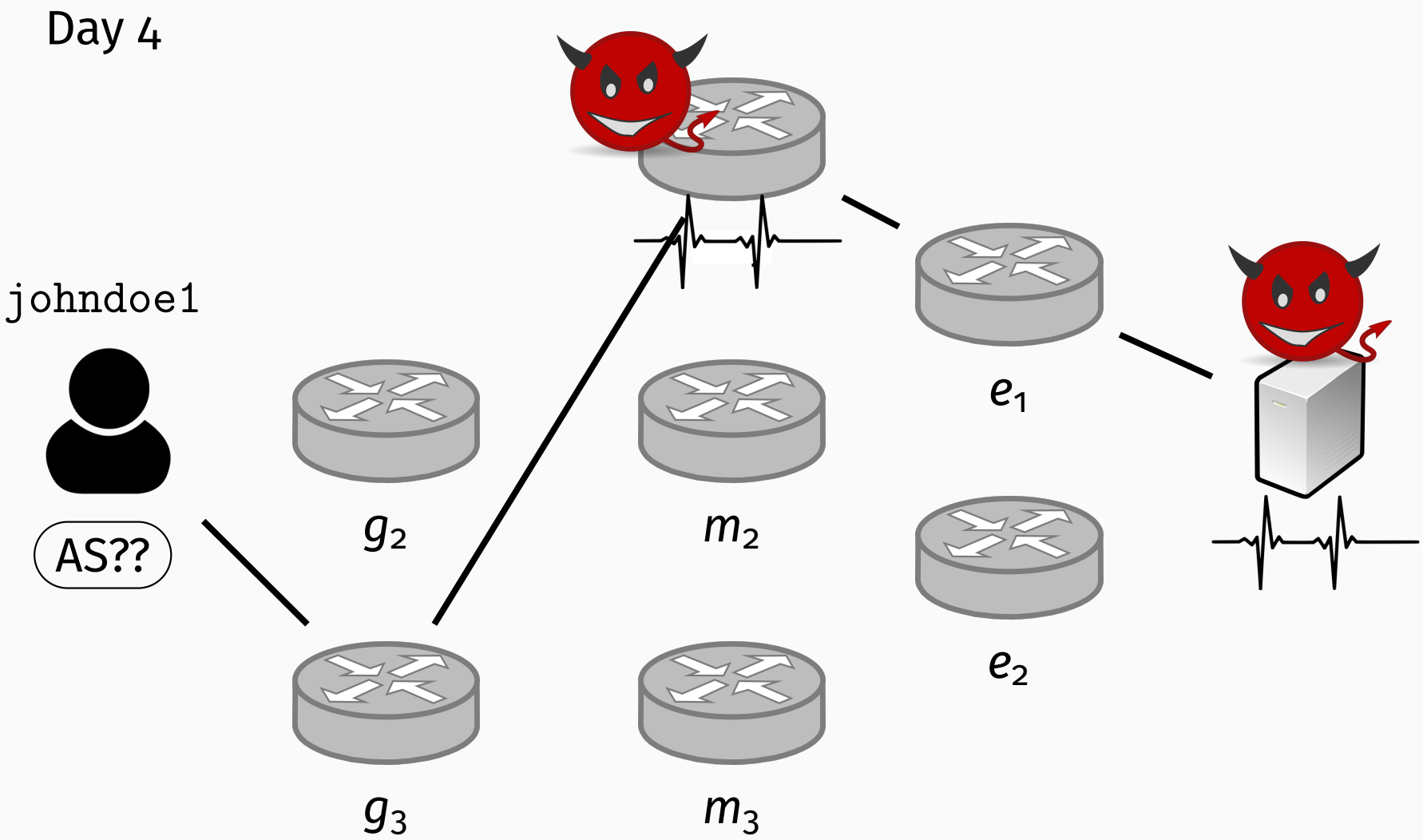
Discovering guards over time



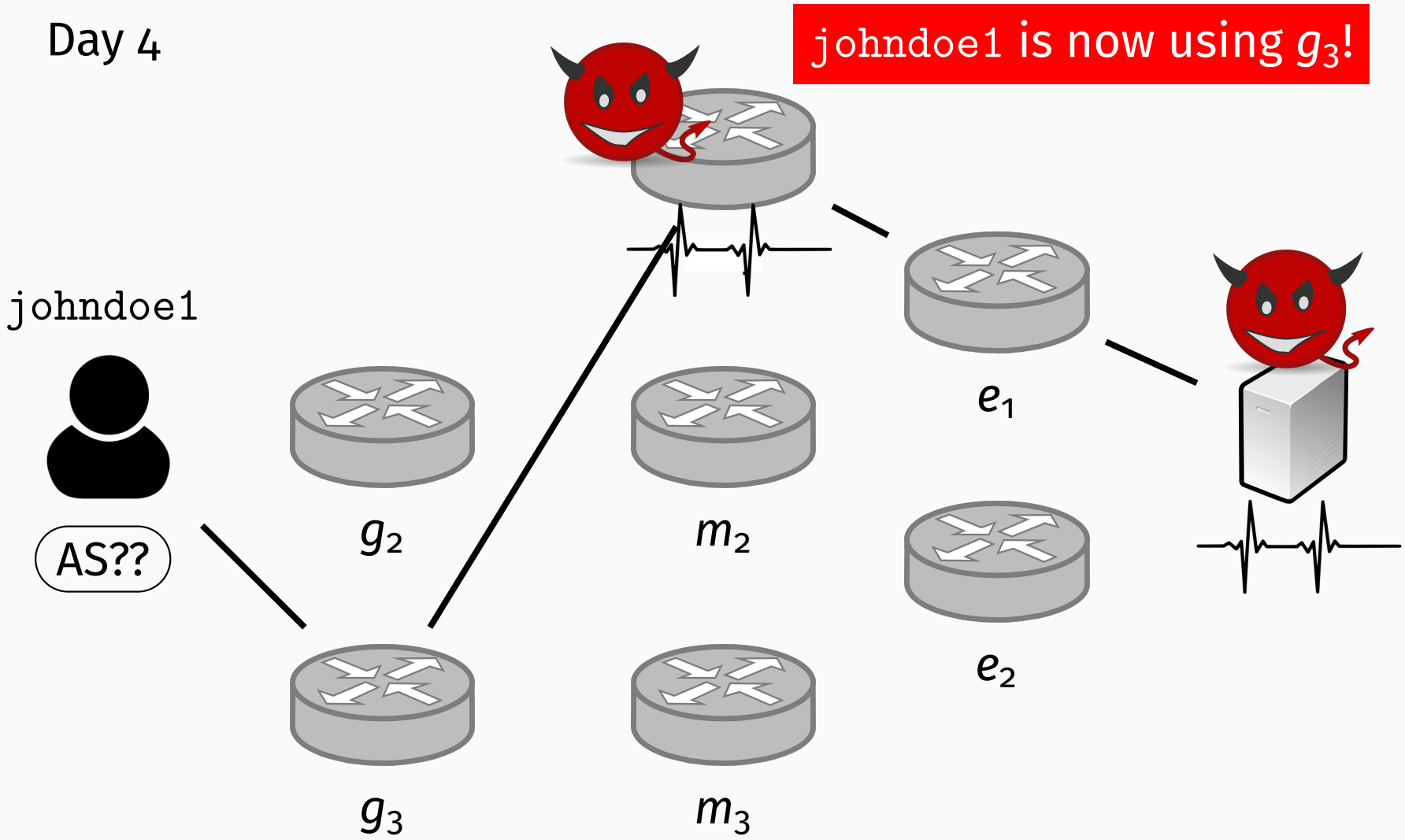
Discovering guards over time



Discovering guards over time



Discovering guards over time



Our Tempest Attack

Note:

1. Many other known guard discovery attacks.
2. Other ways to link client connections.

Our Tempest Attack

Adversary then computes posterior location distribution:

$\Pr(\text{AS1} \mid g_1 \wedge g_3)$

$\Pr(\text{AS2} \mid g_1 \wedge g_3)$

...

$\Pr(\text{AS60000} \mid g_1 \wedge g_3)$

Attack Evaluation

1. Adversary starts with uniform prior over $\sim$ 60K ASes

Attack Evaluation

1. Adversary starts with uniform prior over $\sim$ 60K ASes
2. Identified 10 “leaky” client locations

Attack Evaluation

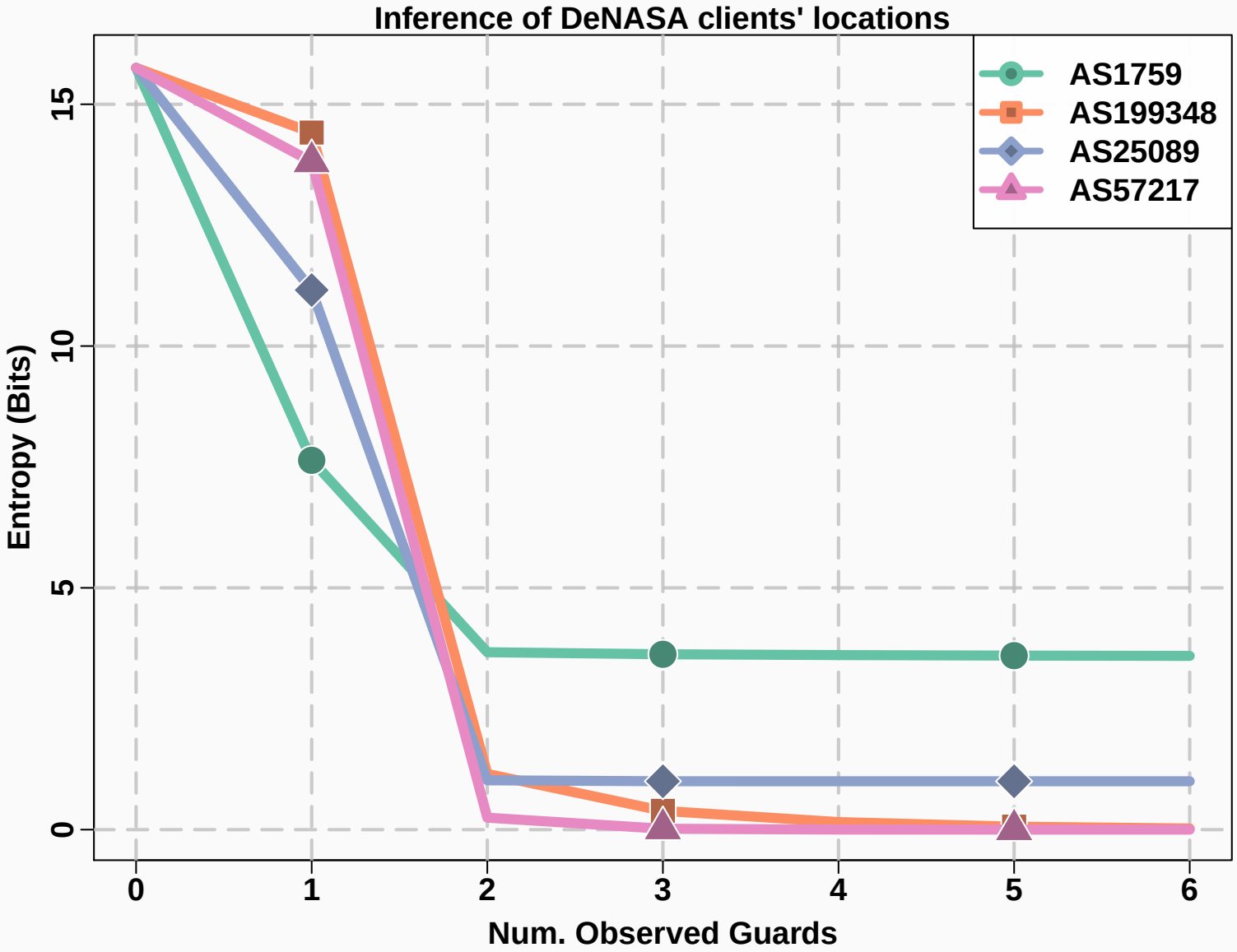
1. Adversary starts with uniform prior over $\sim$ 60K ASes
2. Identified 10 “leaky” client locations
3. Simulated a client making up to 6 guard selections

Attack Evaluation

1. Adversary starts with uniform prior over $\sim$ 60K ASes
2. Identified 10 “leaky” client locations
3. Simulated a client making up to 6 guard selections
4. Collected 100 samples for each location

Attack Evaluation

1. Adversary starts with uniform prior over $\sim$ 60K ASes
2. Identified 10 “leaky” client locations
3. Simulated a client making up to 6 guard selections
4. Collected 100 samples for each location
5. Computed average posterior entropy after adversary makes x guard observations



Points show average entropy after *x* guard observations

Takeaways

1. Small leaks can quickly become significant.
2. Important to consider the worst-case.

Conclusion

Temporal Dynamics & Anonymity Systems

		Client Mobility	User Behavior	Routing Changes
Tor	Tor	Novel ✗	Known ✗	Known ✗
	DeNASA	Novel ✗	Novel ✗	
	Counter-RAPTOR	Novel ✗	Novel ✓	Known ✓
	TAPS		Known ✓	Novel ✗
Net-Layer	HORNET	Novel ✗		Novel ✗
	LAP	Novel ✗		Novel ✗
	Dovetail		Novel ✗	
	PHI		Novel ✗	

Legend: Vulnerability ✗ Resistance ✓

Future Work

1. Explicitly accounting for temporal dynamics
2. Considering the long-lived adversary
3. Capturing time in evaluations and formalization

Thank you!