UMass Amherst | College of Information & Computer Sciences

Electrical and Computer Engineering Department

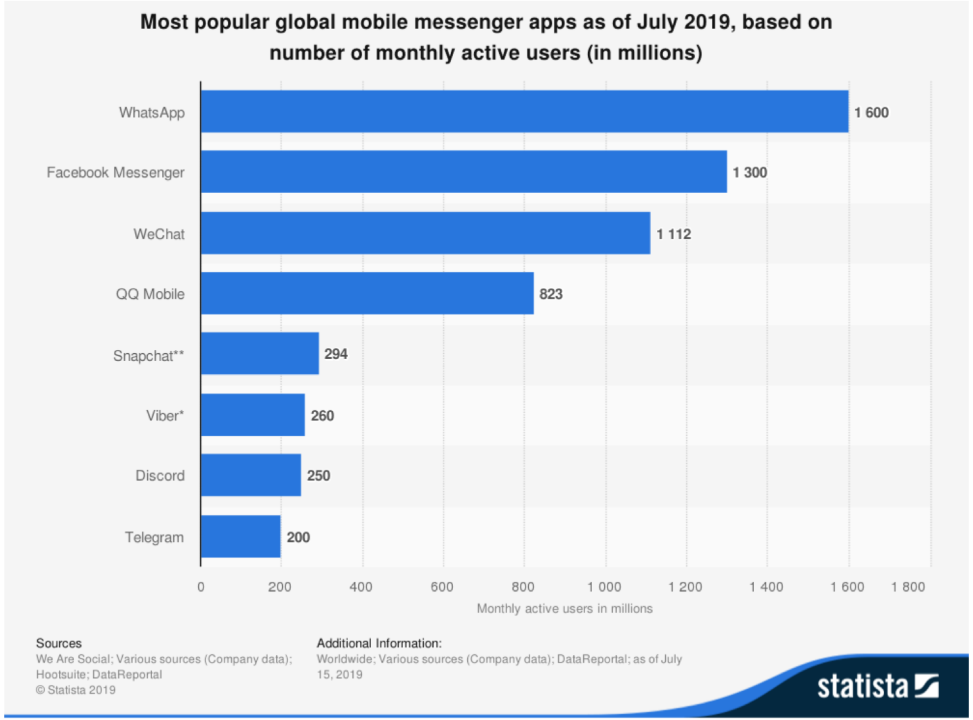
Practical Traffic Analysis Attacks on Secure Messaging Applications

Alireza Bahramali, Ramin Soltani, Amir Houmansadr, Dennis Goeckel, Don Towsley

University of Massachusetts Amherst

Instant Messaging is Popular!

- Over 2 billion people use Instant Messaging (IM) applications
- Used to exchange various types of messages

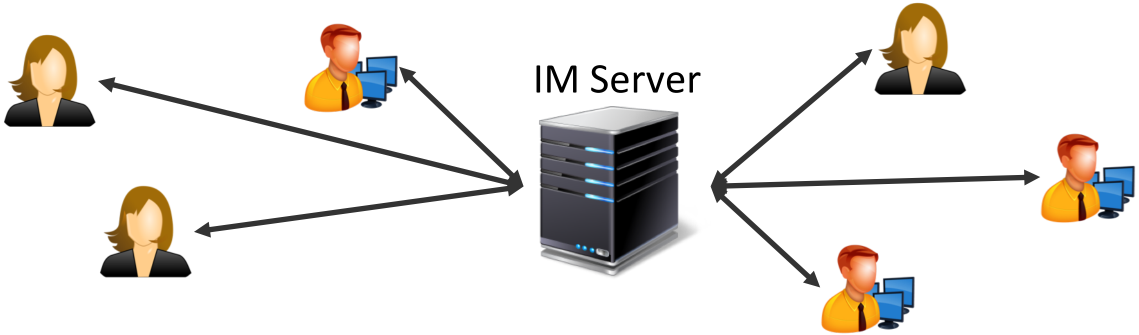

Most popular global mobile messenger apps as of July 2019, based on number of monthly active users (in millions)

Sources
We Are Social; Various sources (Company data); Hootsuite; DataReportal
© Statista 2019

Additional Information:
Worldwide; Various sources (Company data); DataReportal; as of July 15, 2019

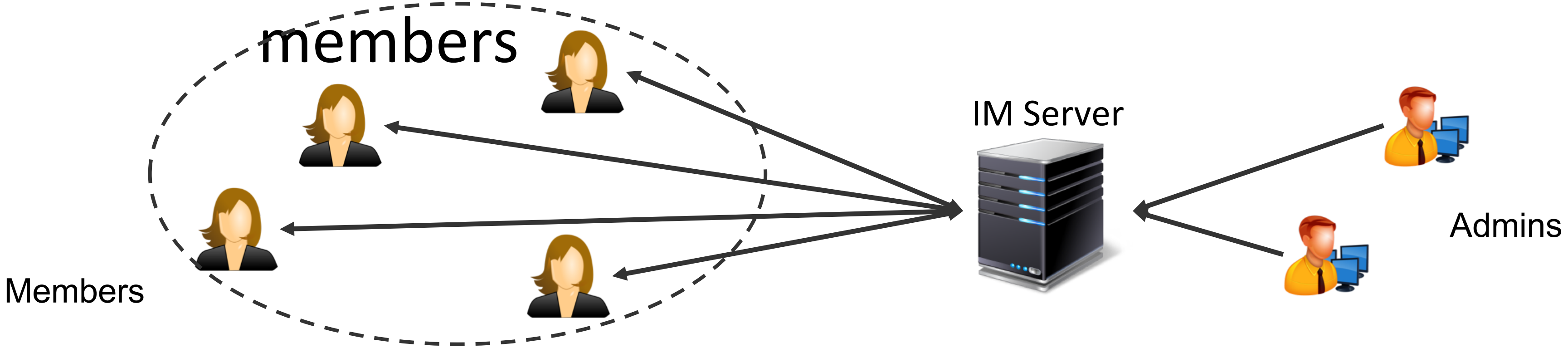
Typical IM Providers

- A variety of IM services: Telegram, WhatsApp, Signal
- Most IMs have centralized structure
  - All the communications are relayed through IM provider servers



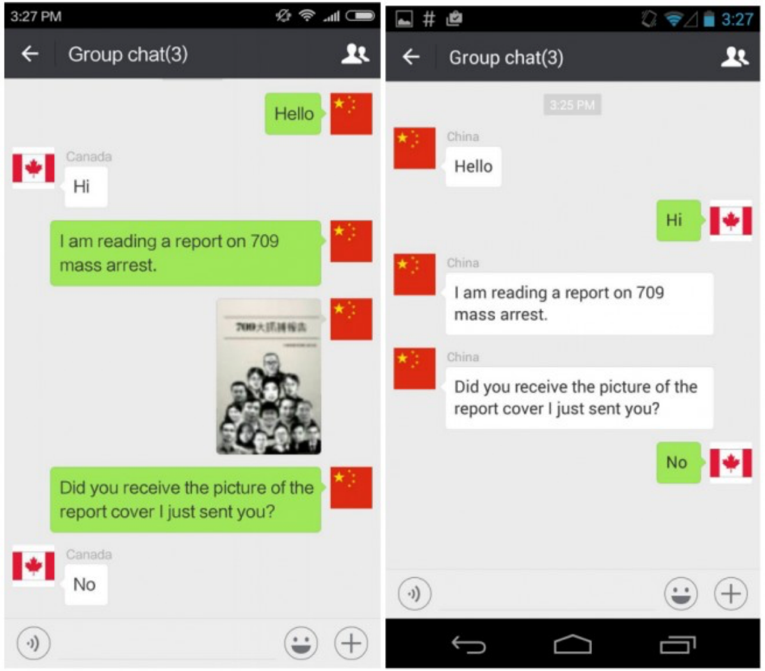
Typical IM Providers

- Various types of communication:
  - One-to-one communication
  - Group communication
  - Channel communication: admins and members



IM Communications are Sensitive

- Extensively used to exchange politically and socially sensitive contents
- Therefore, IM services are attractive targets for government and corporation surveillance



3:27 PM

Group chat(3)

Hello

Canada

Hi

I am reading a report on 709 mass arrest.

Did you receive the picture of the report cover I just sent you?

Canada

No

3:27

Group chat(3)

3:25 PM

China

Hello

Hi

China

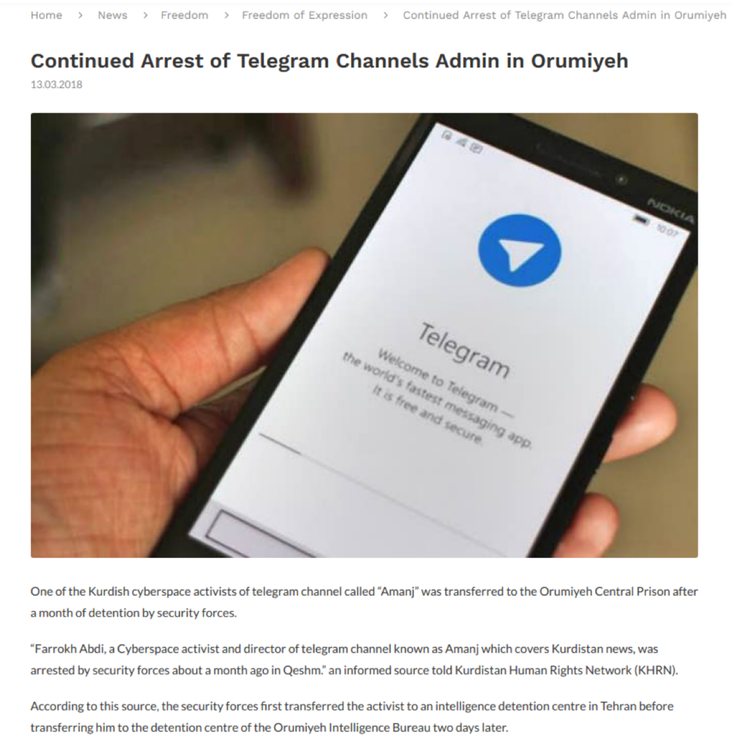
I am reading a report on 709 mass arrest.

China

Did you receive the picture of the report cover I just sent you?

No

Examples



Home › News › Freedom › Freedom of Expression › Continued Arrest of Telegram Channels Admin in Orumiyeh

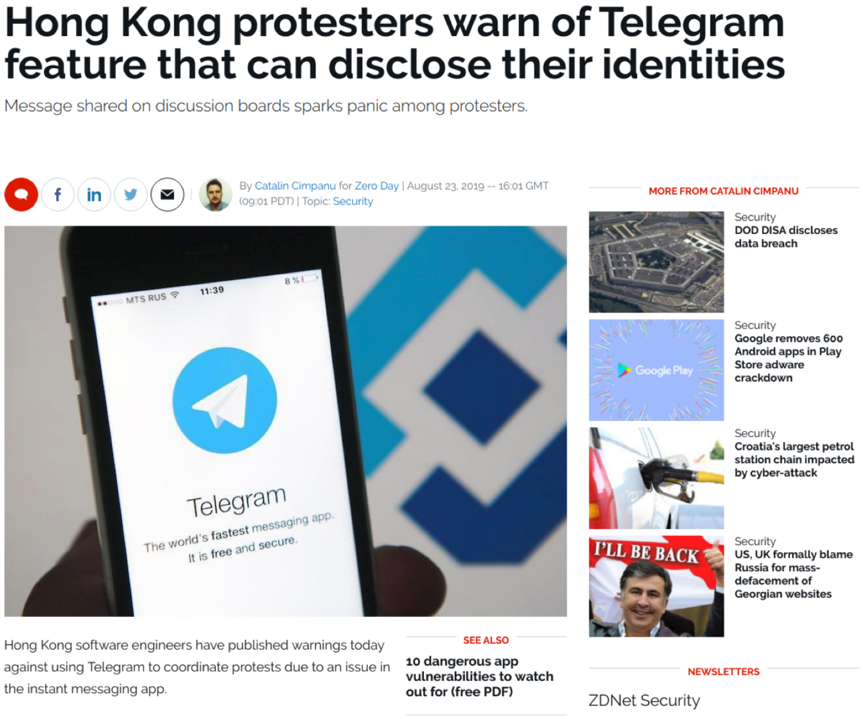
Continued Arrest of Telegram Channels Admin in Orumiyeh

13.03.2018

One of the Kurdish cyberspace activists of telegram channel called "Amanj" was transferred to the Orumiyeh Central Prison after a month of detention by security forces.

"Farrokh Abdi, a Cyberspace activist and director of telegram channel known as Amanj which covers Kurdistan news, was arrested by security forces about a month ago in Qeshm." an informed source told Kurdistan Human Rights Network (KHRN).

According to this source, the security forces first transferred the activist to an intelligence detention centre in Tehran before transferring him to the detention centre of the Orumiyeh Intelligence Bureau two days later.



Hong Kong protesters warn of Telegram feature that can disclose their identities

Message shared on discussion boards sparks panic among protesters.

By Catalin Cimpanu for Zero Day | August 23, 2019 -- 16:01 GMT (09:01 PDT) | Topic: Security

Hong Kong software engineers have published warnings today against using Telegram to coordinate protests due to an issue in the instant messaging app.

SEE ALSO

10 dangerous app vulnerabilities to watch out for (free PDF)

MORE FROM CATALIN CIMPANU

Security
DOD DISA discloses data breach

Security
Google removes 600 Android apps in Play Store adware crackdown

Security
Croatia's largest petrol station chain impacted by cyber-attack

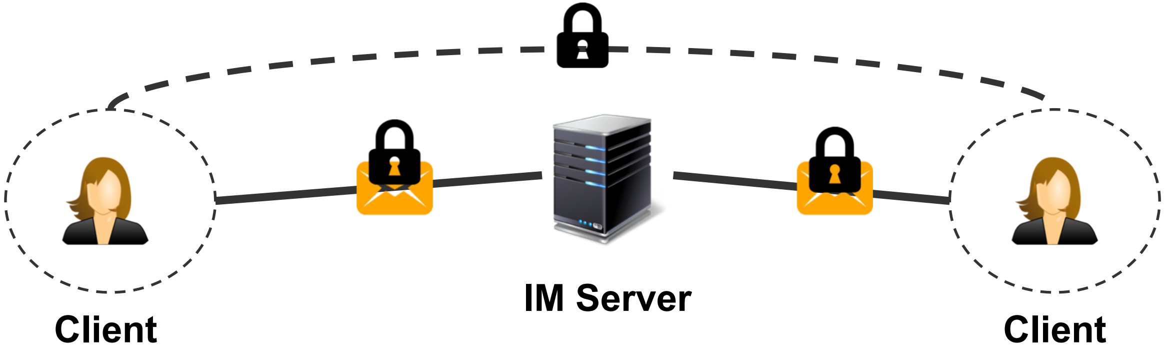
Security
US, UK formally blame Russia for mass-defacement of Georgian websites

NEWSLETTERS

ZDNet Security

How Confidential Are IMs?

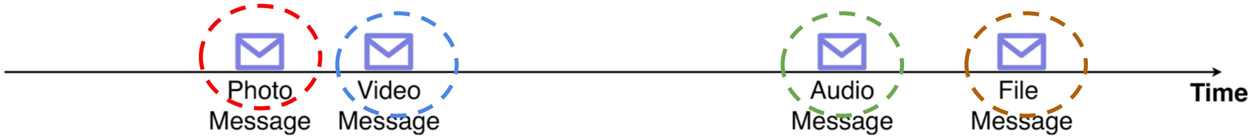
The good news: content is protected by Encryption, End-to-Middle or End-to-End



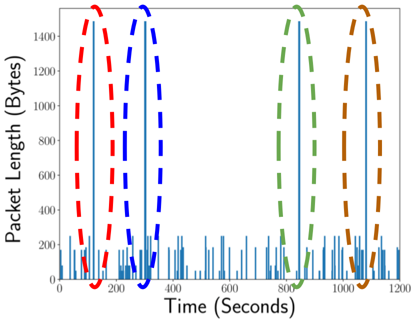
The bad news: traffic patterns leak information

How Patterns Leak?

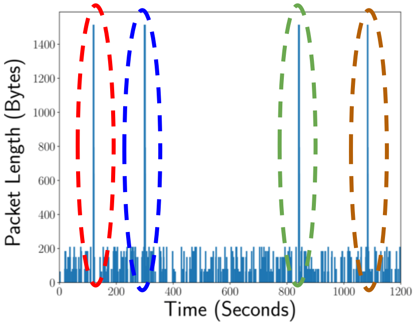
Sequence of Messages in the Channel



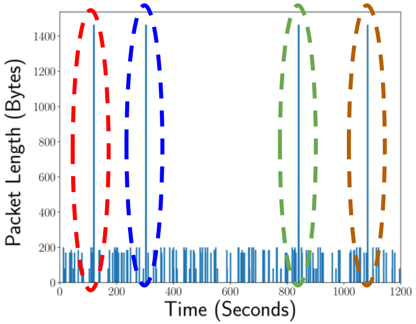
Admin



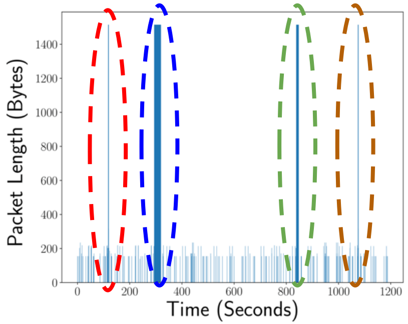
Member1



Member 2



Member 3



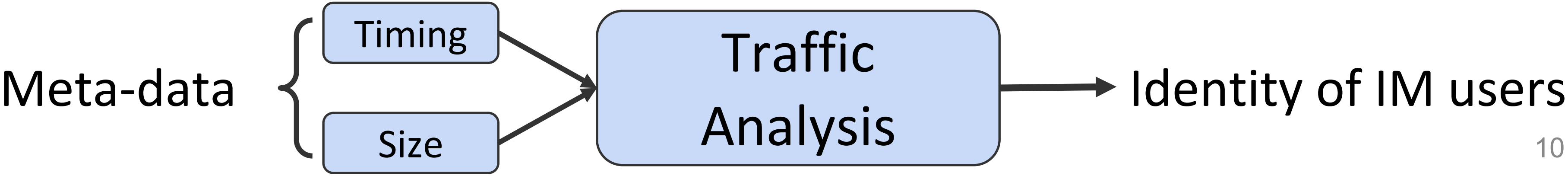
Objective of this study: investigate the threat of traffic analysis to popular IM services

- This is a fundamental vulnerability!
  - Major IM services do not obfuscate traffic patterns because it’s expensive

Our Attack

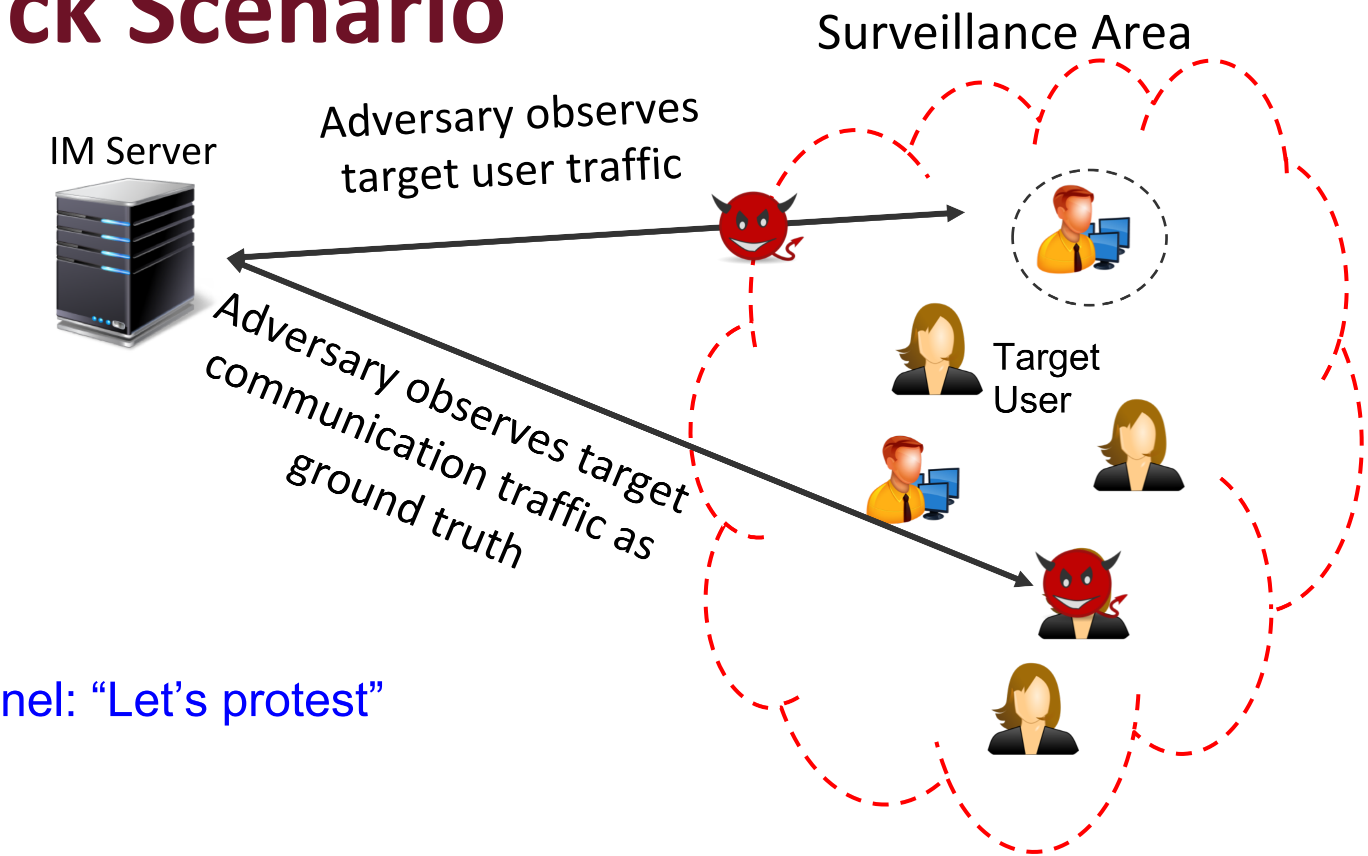
Adversary {
- A surveillance organization
- No need to cooperate with IM server

Goal → Identify participants of a target IM communication



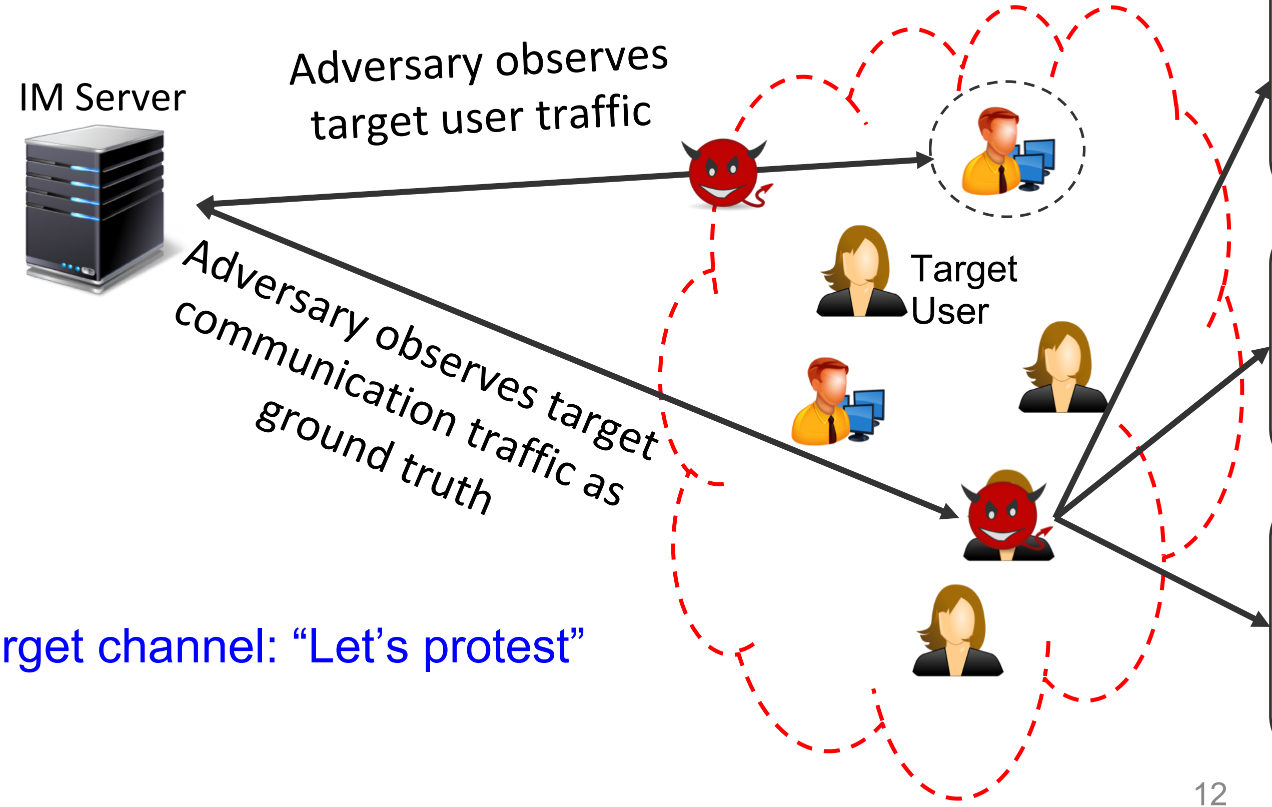
Meta-data { Timing, Size → Traffic Analysis → Identity of IM users

Attack Scenario



Target channel: “Let’s protest”

Adversary Ground Truth


IM Server
Adversary observes target user traffic
Adversary observes target communication traffic as ground truth
Target User

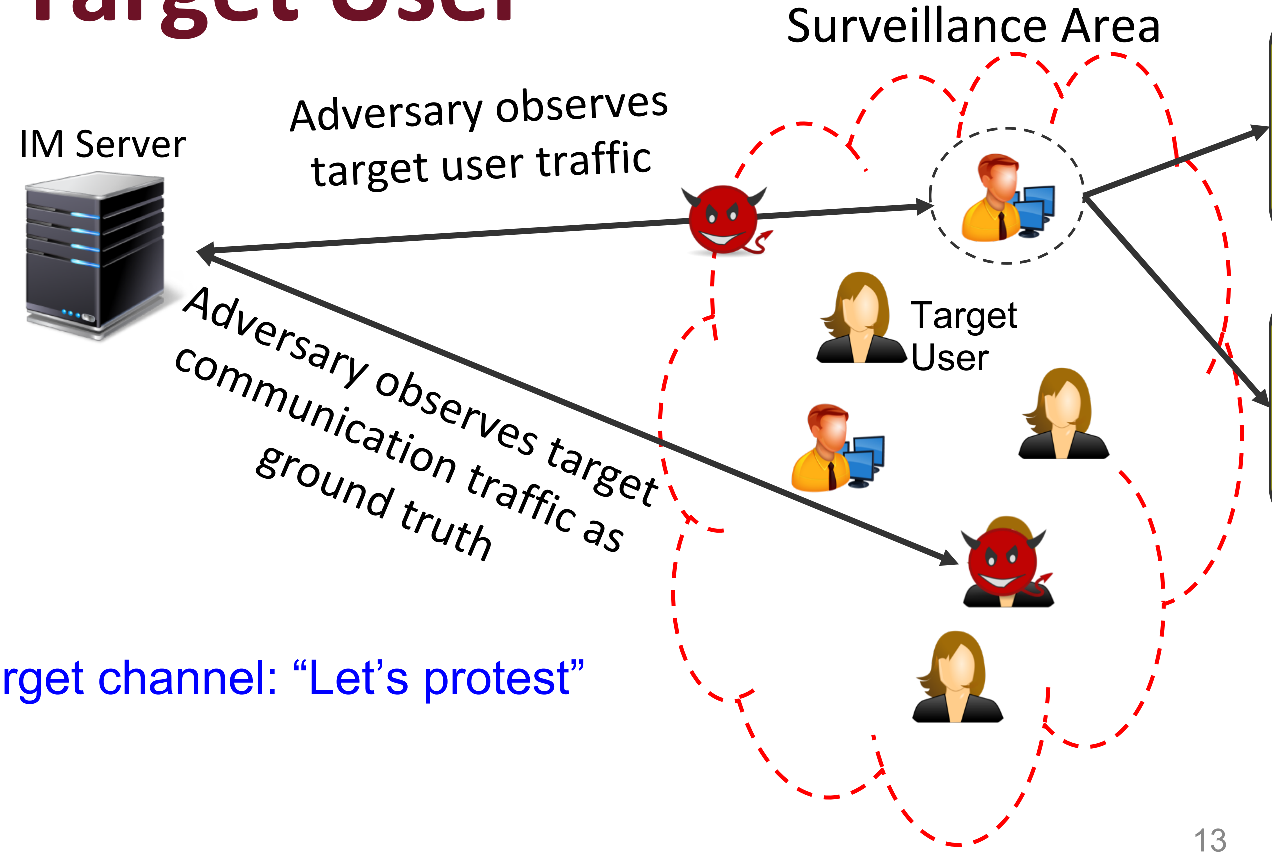
Adversary joins the target channel as a member.

Adversary joins the target channel as an admin.

Adversary wiretaps an identified member/admin.

Target channel: “Let’s protest”

Target User


Surveillance Area
IM Server
Adversary observes target user traffic
Adversary observes target communication traffic as ground truth
Target User

Target user is the admin of the target communication

Target user is the member of the target communication

Target channel: "Let's protest"

Outline

- Modeling IM traffic: We established a statistical model for regular IM communications
- Design attack algorithms: We use hypothesis testing to design attack algorithms
- Experiments: We perform experiments on Telegram, WhatsApp, and Signal
- Countermeasures: We design and implement an open-source countermeasure system called IMProxy

Outline

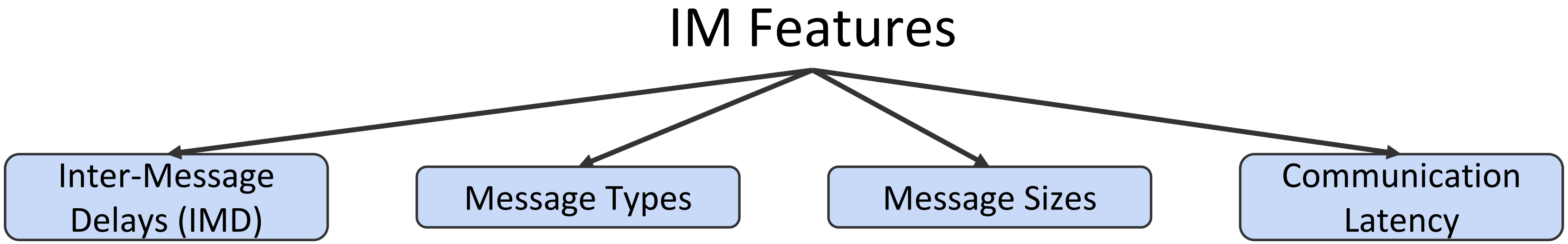
- Modeling IM traffic: We established a **statistical model** for regular IM communications.
- Design attack algorithms: We use hypothesis testing to design attack algorithms
- Experiments: We perform experiments on Telegram, WhatsApp, and Signal
- Countermeasures: We design and implement an open-source countermeasure system called **IMProxy**

Modeling IM Traffic

- Deriving theoretical bounds on our traffic analysis algorithms.
- Generating synthetic IM communication.
- Dataset: Traffic patterns of 1000 Telegram channels, each for 24 hours.

UMass Amherst | College of Information & Computer Sciences

Modeling IM Traffic



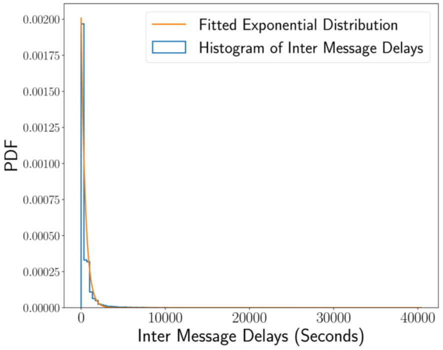
IM Features

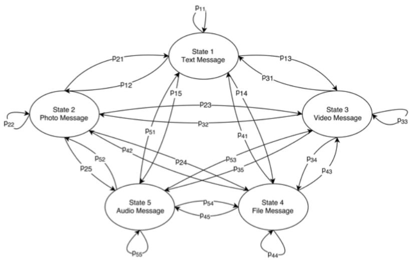
Inter-Message Delays (IMD)

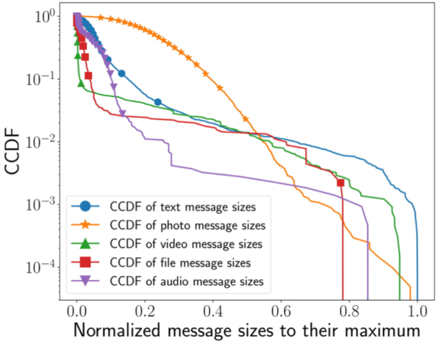
Message Types

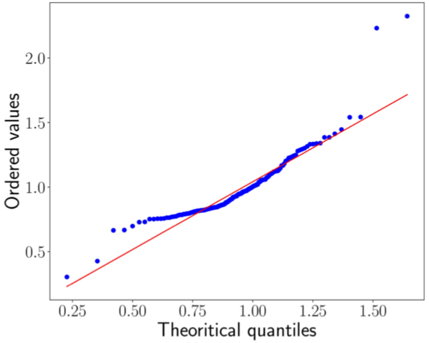
Message Sizes

Communication Latency









Outline

- Modeling IM traffic: We established a **statistical model** for regular IM communications
- Design attack algorithms: We use hypothesis testing to design attack algorithms
- Experiments: We perform experiments on Telegram, WhatsApp, and Signal
- Countermeasures: We design and implement an open-source countermeasure system called **IMProxy**

Attack Algorithms

Event-Based Algorithm

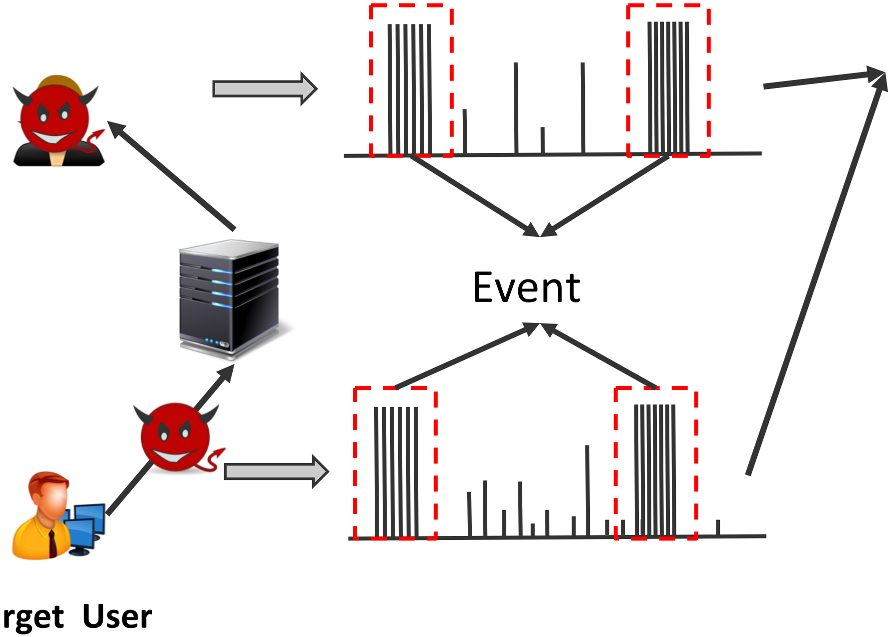
Shape-based Algorithm

Attack Algorithms: Event-Based

1- Event Extraction

2- Correlation Function

3- Comparing to a Threshold



If two events are close enough:

MATCH!

$$\frac{\text{number of matches}}{\text{number of events}} > \eta$$

UMassAmherst | College of Information & Computer Sciences

Hypothesis Testing

$$\begin{cases} H_0 : t_i^{(C)} = t_i^{(*)} + d_i^{(*)}, s_i^{(C)} = s_i^{(*)}, 1 \le i \le n \\ H_1 : t_i^{(C)} = t_i^{(U)} + d_i^{(U)}, s_i^{(C)} = s_i^{(U)}, 1 \le i \le n \end{cases}$$

$$\begin{aligned} \mathbb{P}_{\mathrm{FP}} = \mathbb{P}(k \ge \eta n \mid H_0) &= \mathbb{P}(n - k \le n - \eta n \mid H_0), \\ &= F(n - \eta n; n, 1 - p_0), \\ &\le \left(\frac{1-\eta}{p_0}\right)^{-n+n\eta\eta} \left(\frac{\eta}{1-p_0}\right)^{-n\eta} \end{aligned}$$

$$\begin{aligned} \mathbb{P}_{\mathrm{FN}} = \mathbb{P}\left(k \le \eta n | H_1\right) &= F(\eta n; n, p_1) \\ &\le \left(\frac{\eta}{p_1}\right)^{-n\eta} \left(\frac{1-\eta}{1-p_1}\right)^{\eta n - n} \end{aligned}$$

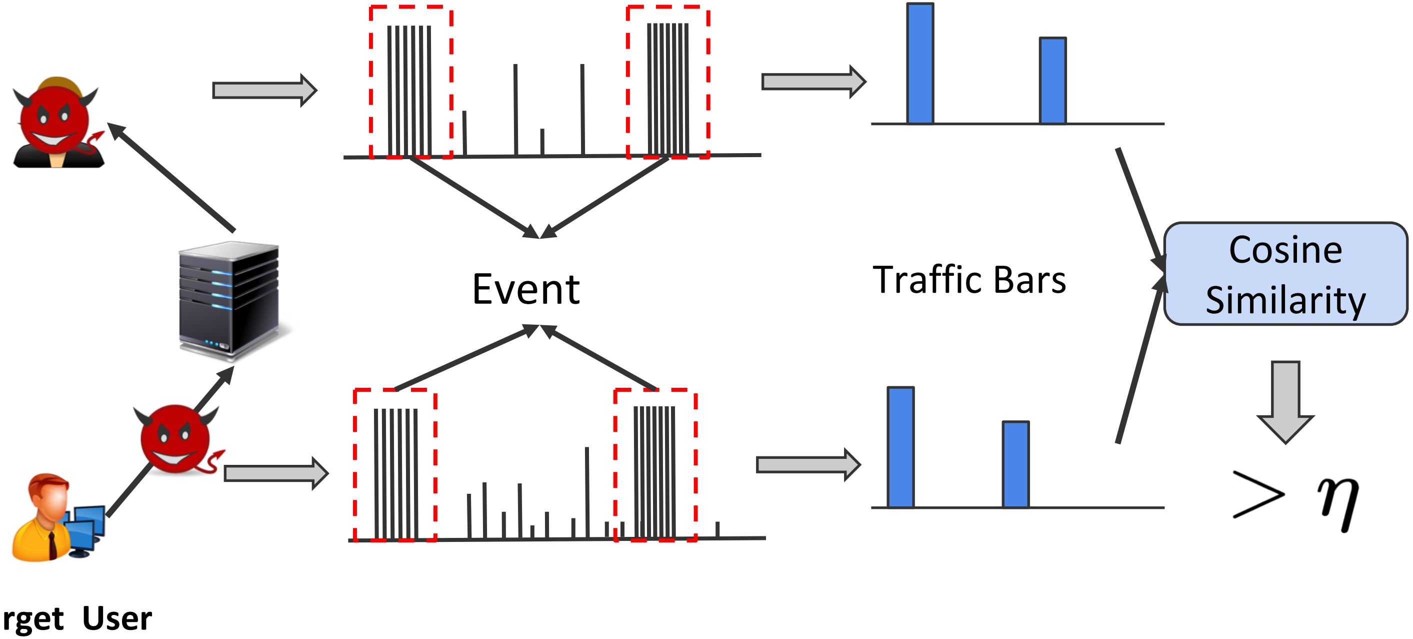
Attack Algorithms: Shape-Based

1- Event Extraction

2- Traffic Normalization

3- Correlation Function

4- Comparing to a Threshold



Outline

- Modeling IM traffic: We established a **statistical model** for regular IM communications
- Design attack algorithms: We use hypothesis testing to design attack algorithms
- Experiments: We perform experiments on Telegram, WhatsApp, and Signal
- Countermeasures: We design and implement an open-source countermeasure system called **IMProxy**

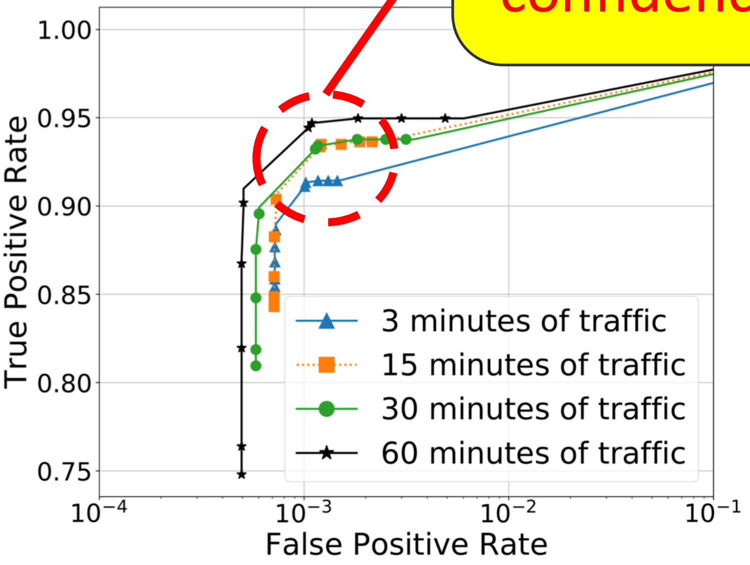
Experimental Setup

- We perform experiments extensively on Telegram, WhatsApp, and Signal
- We use patterns of 500 channels.
- Scenarios
  - Identifying Admin of a Telegram channel
  - Wiretapping an identified user (one-to-one)

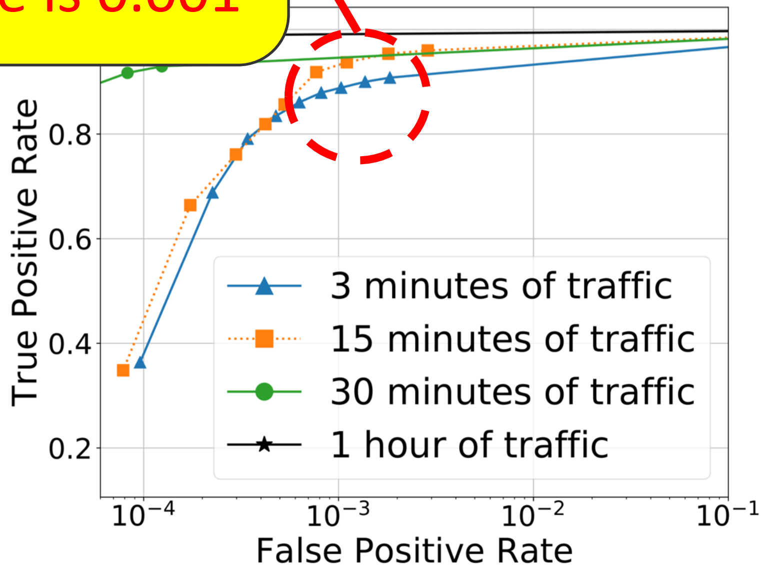
Attacks’ Performance

Even with 15 minutes of traffic both algorithms have 94% confidence while FP rate is 0.001

Event-based a



based algorithm



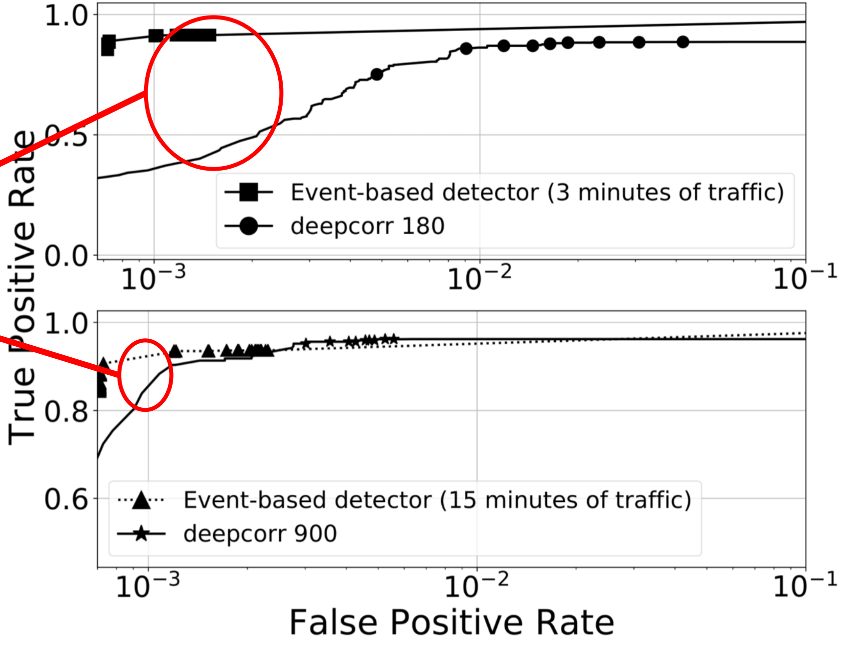
Why Not Deep Learning?

We compared our work with DeepCorr

We perform better than DeepCorr for smaller false positive rates!!?

1- IM flows are sparse.

2- IM flows are less noisy.



Outline

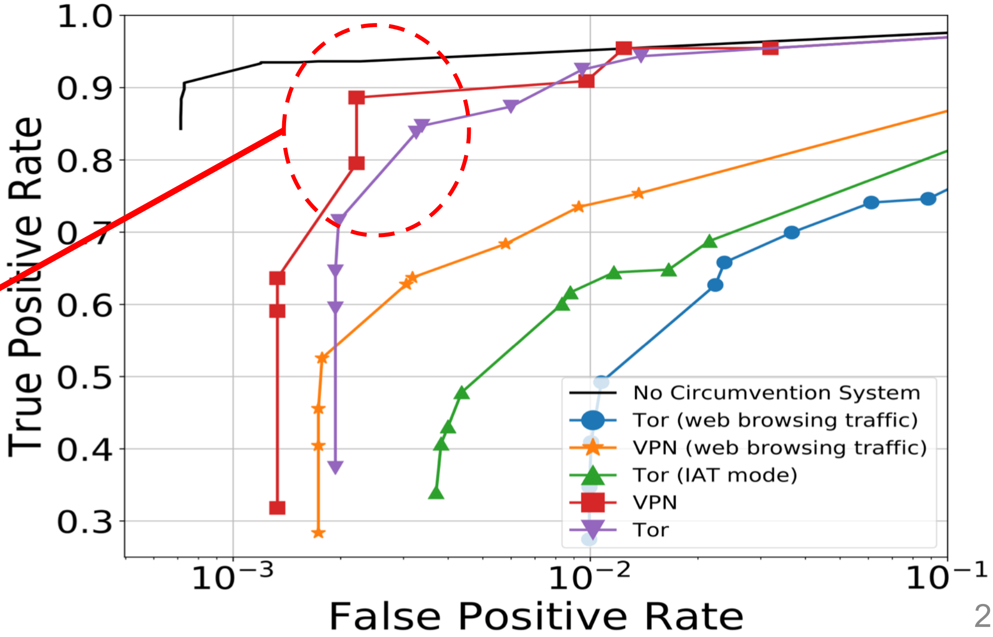
- Modeling IM traffic: We established a **statistical model** for regular IM communications
- Design attack algorithms: We use hypothesis testing to design attack algorithms
- Experiments: We perform experiments on Telegram, WhatsApp, and Signal
- Countermeasures: We design and implement an open-source countermeasure system called **IMProxy**

How to defend?

1- Using circumvention systems: Tor, VPN

They are not effective without any background traffic.

Event-based detector



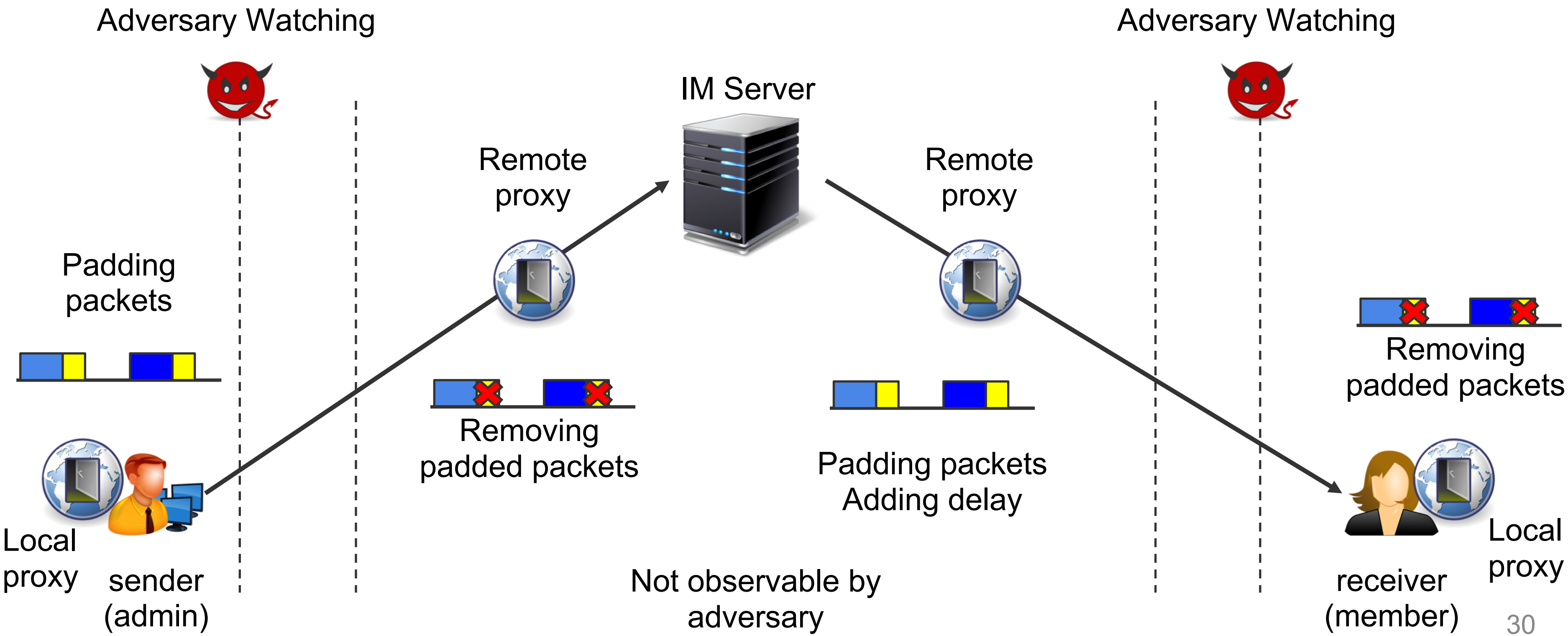
IMProxy

- A proxy-based obfuscation system
- No IM cooperation required
- Can be applied to any IM service just by proxy the IM traffic through it

- Algorithms:
  - Adding delay
  - Adding dummy packets

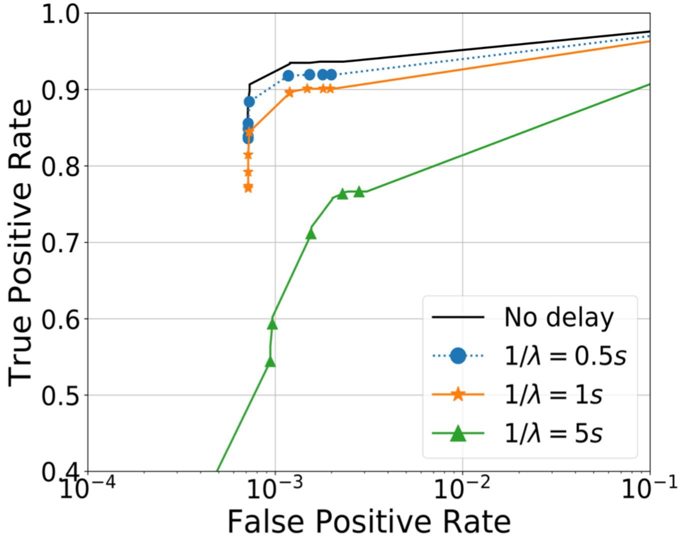
- Main components:
  - Local proxy
  - Remote proxy

How It Works?

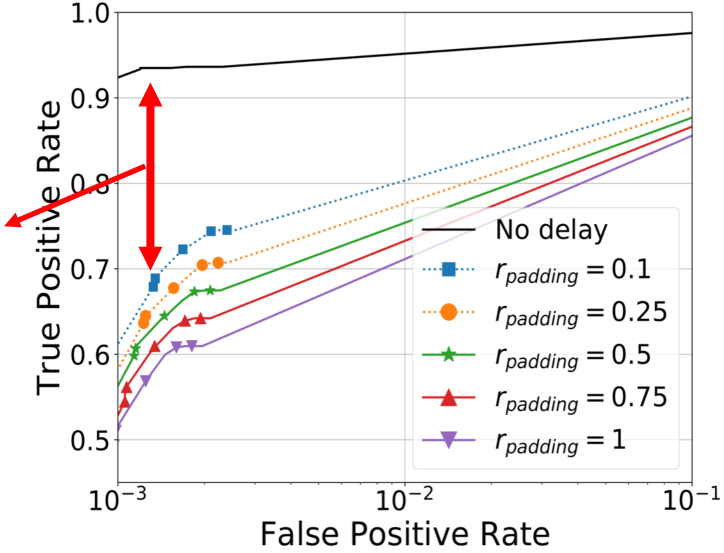

Adversary Watching
Adversary Watching
IM Server
Remote proxy
Remote proxy
Padding packets
Removing padded packets
Padding packets Adding delay
Removing padded packets
Local proxy
sender (admin)
Not observable by adversary
receiver (member)
Local proxy

Evaluating IMProxy

- Latency: A Laplacian distribution with parameter λ
- Adding dummy packets based on a Uniform Distribution
- SOCKS5 proxy
- Event-based attack



With 10% bandwidth overhead, we have 30% decrease in confidence

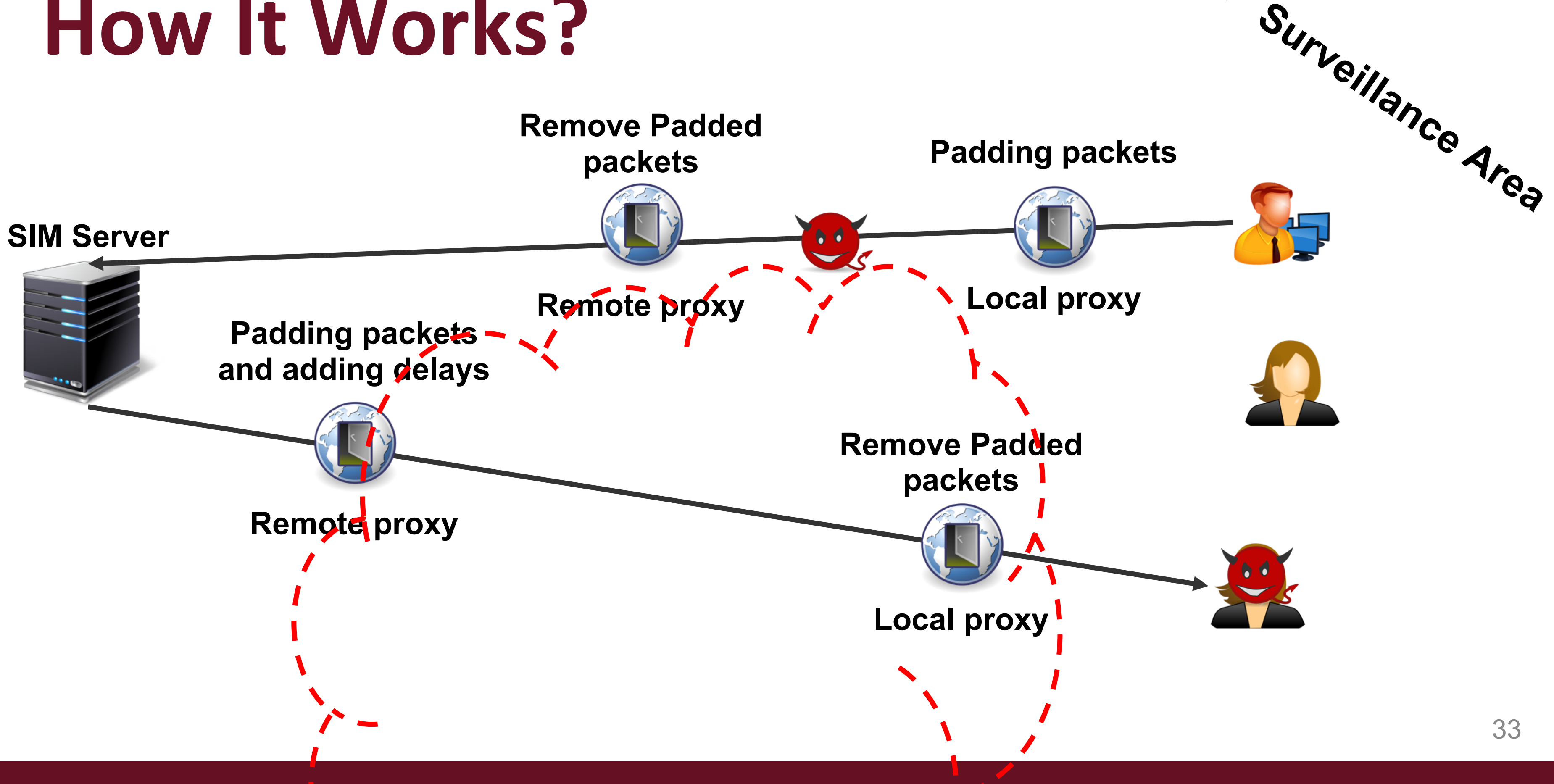


Conclusions

- We show that despite the use of encryption, popular IM applications leak sensitive information about their client’s activities.
- The reason is that IMs do not use any obfuscation algorithms because it is expensive
- We hope that our results warn IM providers to take proper measures

Thanks to NSF DARPA

How It Works?


Surveillance Area
Remove Padded packets
Padding packets
SIM Server
Remote proxy
Local proxy
Padding packets and adding delays
Remove Padded packets
Remote proxy
Local proxy

A Fundamental Vulnerability

We show that despite the use of encryption, popular IM applications leak sensitive information about their client's activities.

Why?

Obfuscation of traffic is expensive for IM operators.

How?

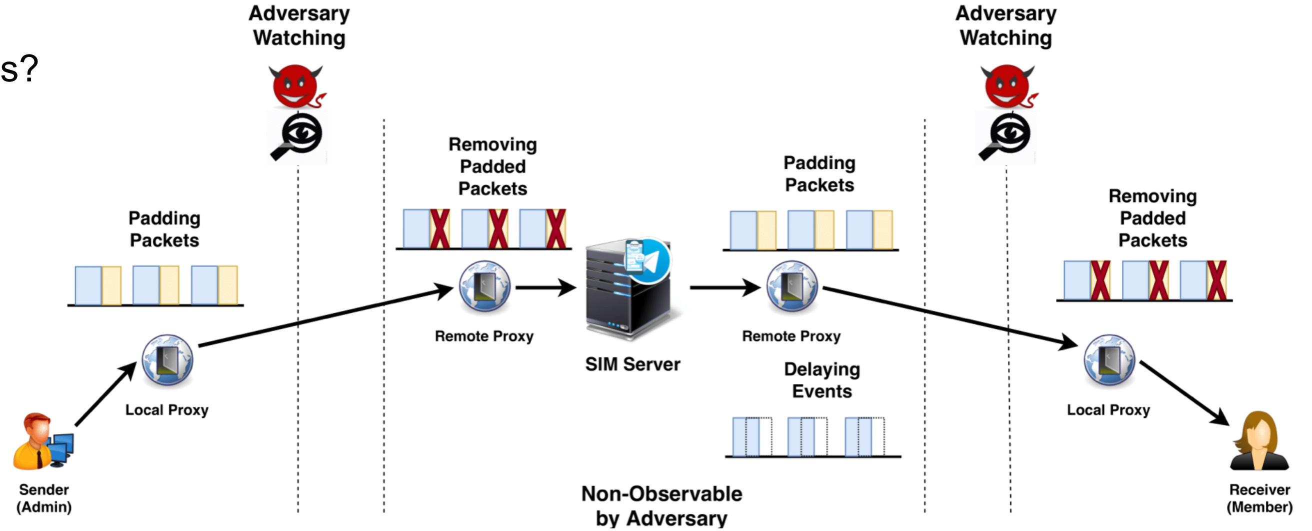
Merely watching encrypted IM traffic. (Traffic Analysis)

How to defend?

2- Using IMProxy

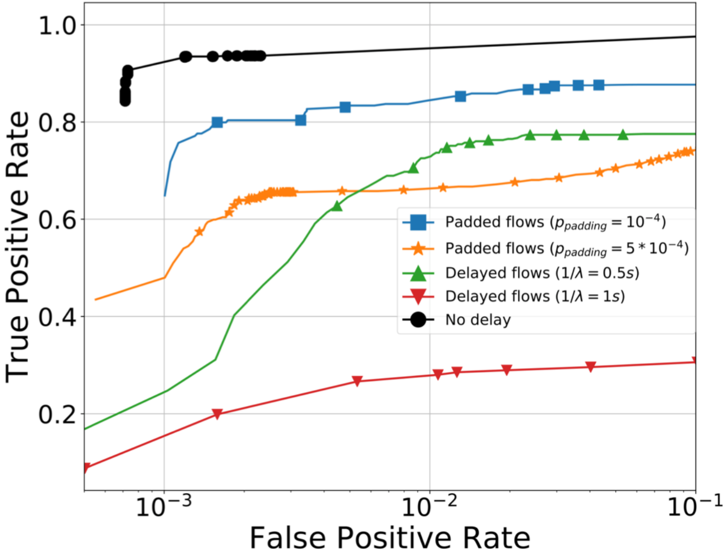
IMProxy: A proxy-based obfuscation system
- Obfuscate timings by adding delays
- Obfuscate sizes by adding dummy traffic

How it works?

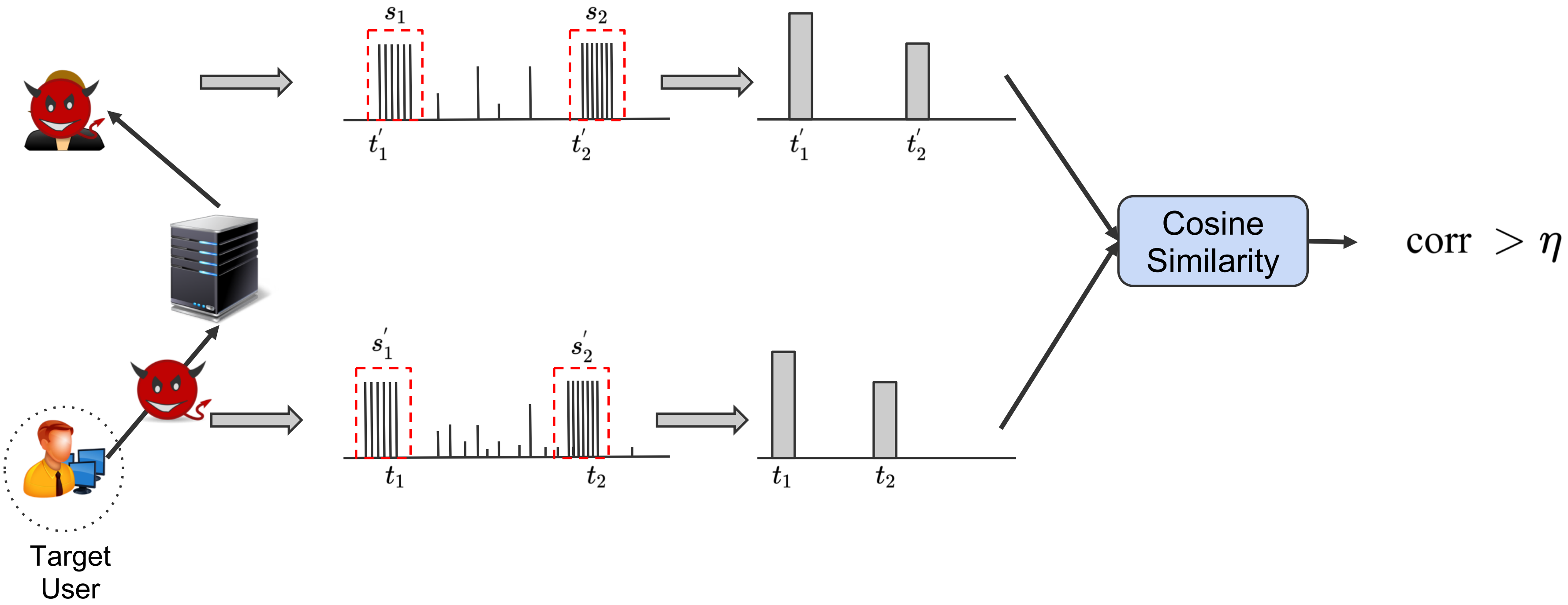


Evaluating IMProxy

- Evaluating against IMProxy aware adversary
- Adversary trains a classifier on traffic flows



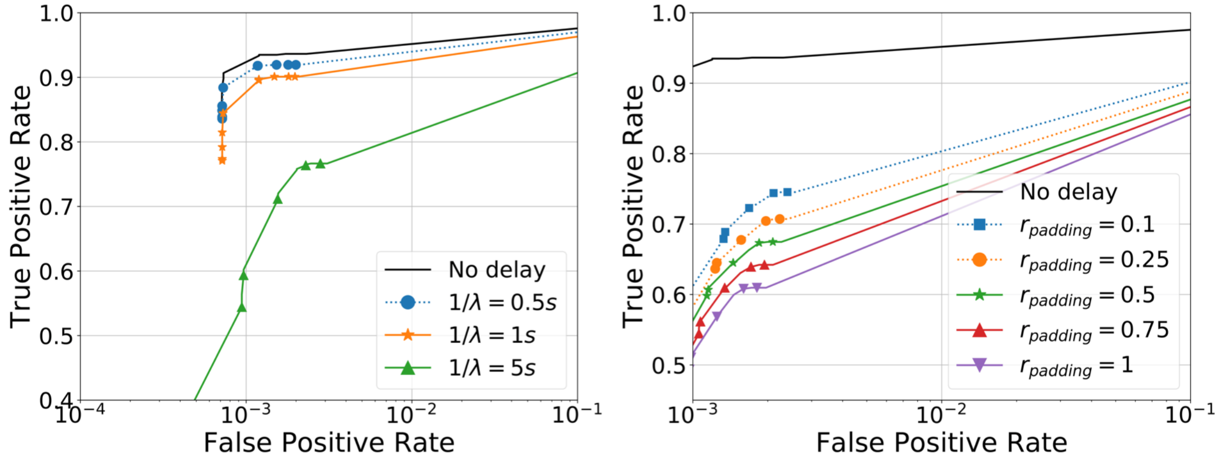
Attack Algorithms: Shape-Based



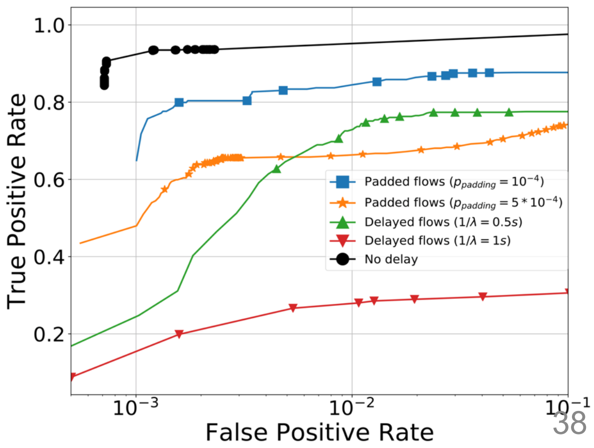
Evaluating IMProxy

- **Latency: A laplacian distribution with parameter λ**
- **Adding dummy packets based a Uniform Distribution**
- **SOCKS5 proxy**

Oblivious adversary



IMProxy-aware adversary

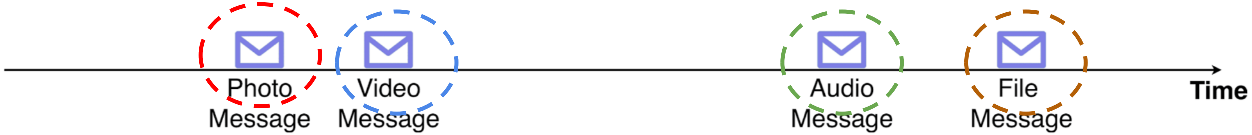


Generalizing to other IMs

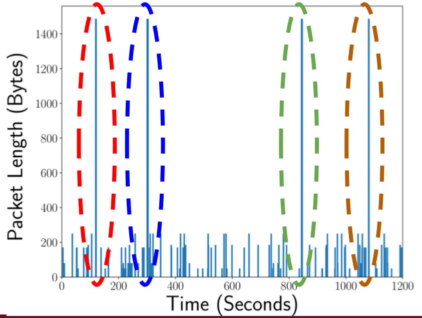
Messages in IMs have the same shape of traffic

They appear as bursts of packets

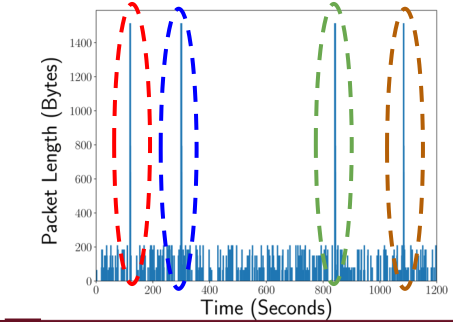
Sequence of Messages in the Channel



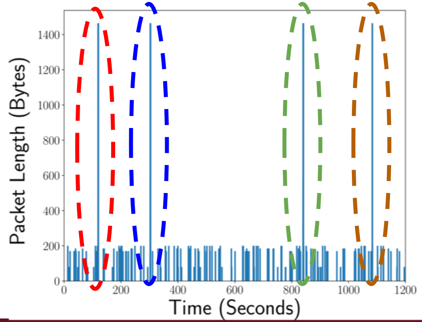
Viber



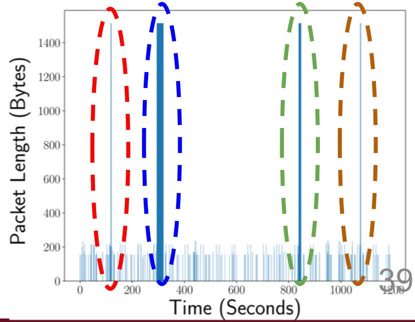
Signal



WhatsApp



Telegram



Telegram

- 200 million monthly active users.
- Most users are in countries with strict media regulations.
- It has the concept of channels.
- Telegram consumes 60! percent of Iran’s Internet bandwidth!

Iran

Russia