Twitch Chat Fingerprinting

David Hasselquist, Linköping University & Sectra Communications, Sweden

Christian Vestlund, Sectra Communications, Sweden

Niklas Johansson, Sectra Communications, Sweden

Niklas Carlsson, Linköping University, Sweden

Proc. IFIP Network Traffic Measurement and Analysis
Conference (TMA), Enschede, The Netherlands, June 2022

LINKÖPING UNIVERSITY

WASP | WALLENBERG AI, AUTONOMOUS SYSTEMS AND SOFTWARE PROGRAM

SECTRA

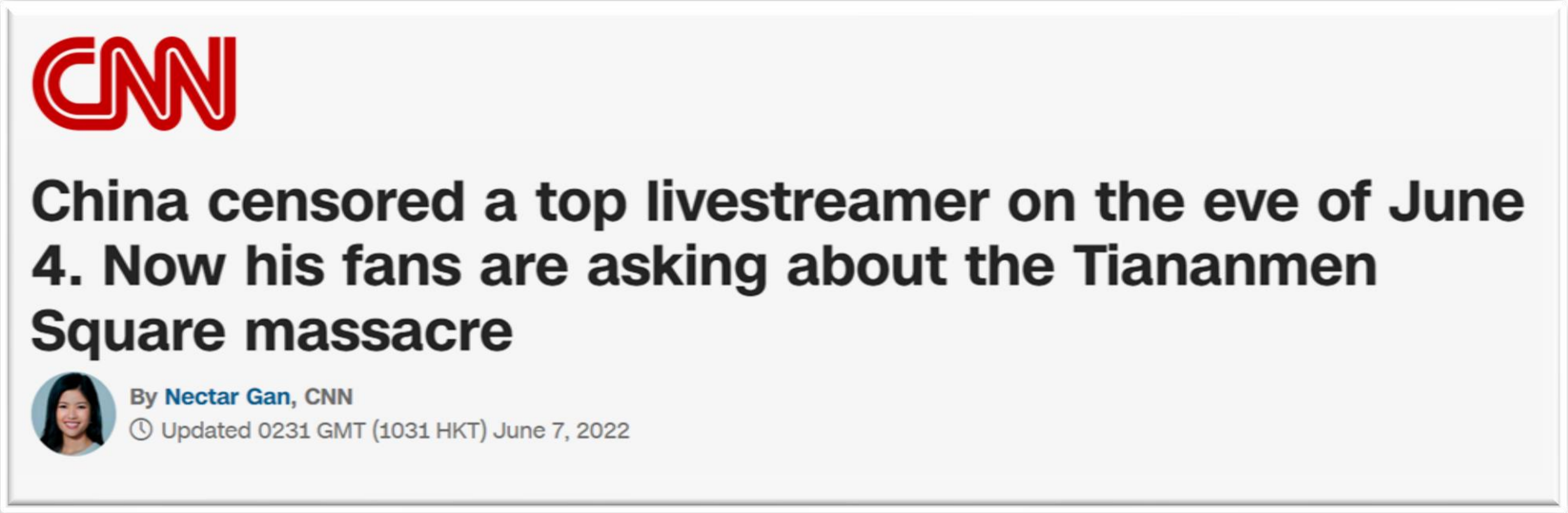
Motivation

- Live streaming accounts for major part of internet activity
- Live streaming provides first viewer advantage and interaction
- Users should be able to freely browse the internet
- The streaming content we choose can reveal much about us
- An adversary capable of determining our activity presents a privacy threat

Examples: governmental monitoring/censorship

- Mass surveillance to identify protesters or users with specific opinions

Examples: governmental monitoring/censorship



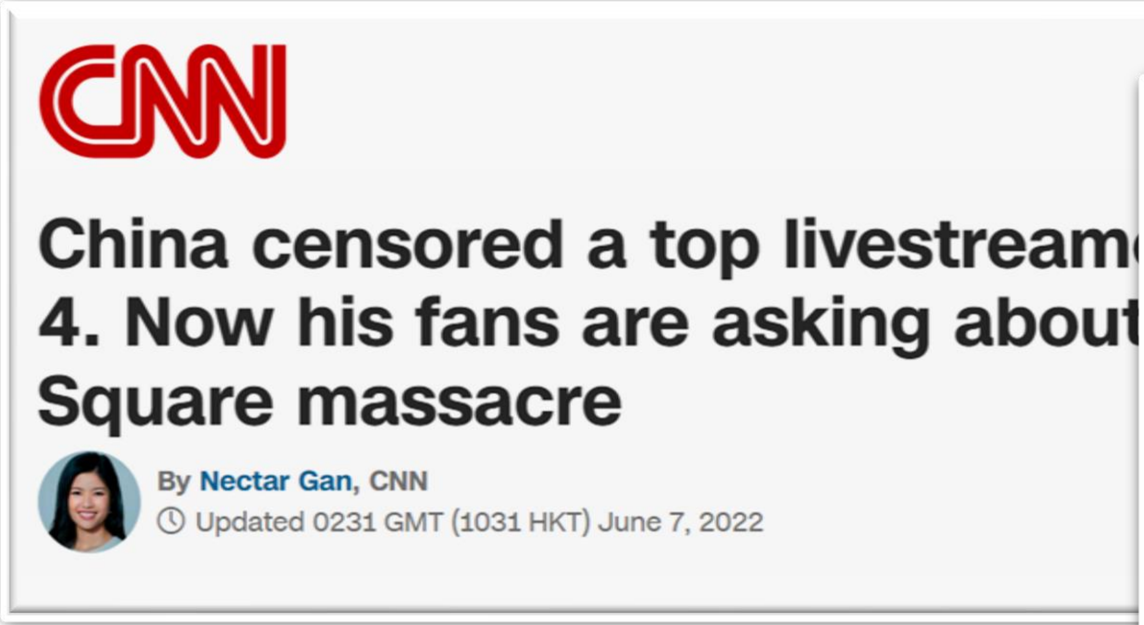
CNN

China censored a top livestreamer on the eve of June 4. Now his fans are asking about the Tiananmen Square massacre

By Nectar Gan, CNN

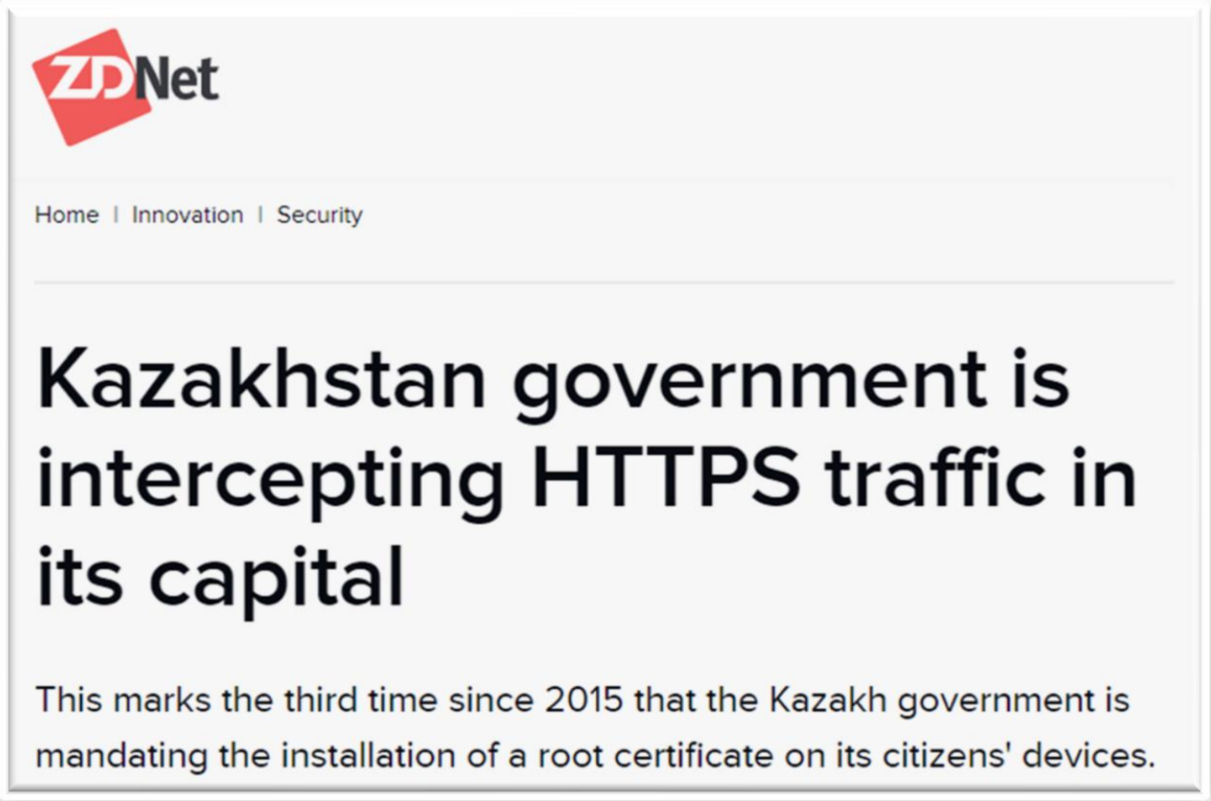
Updated 0231 GMT (1031 HKT) June 7, 2022

Examples: governmental monitoring/censorship



China censored a top livestream
4. Now his fans are asking about
Square massacre

By Nectar Gan, CNN
Updated 0231 GMT (1031 HKT) June 7, 2022



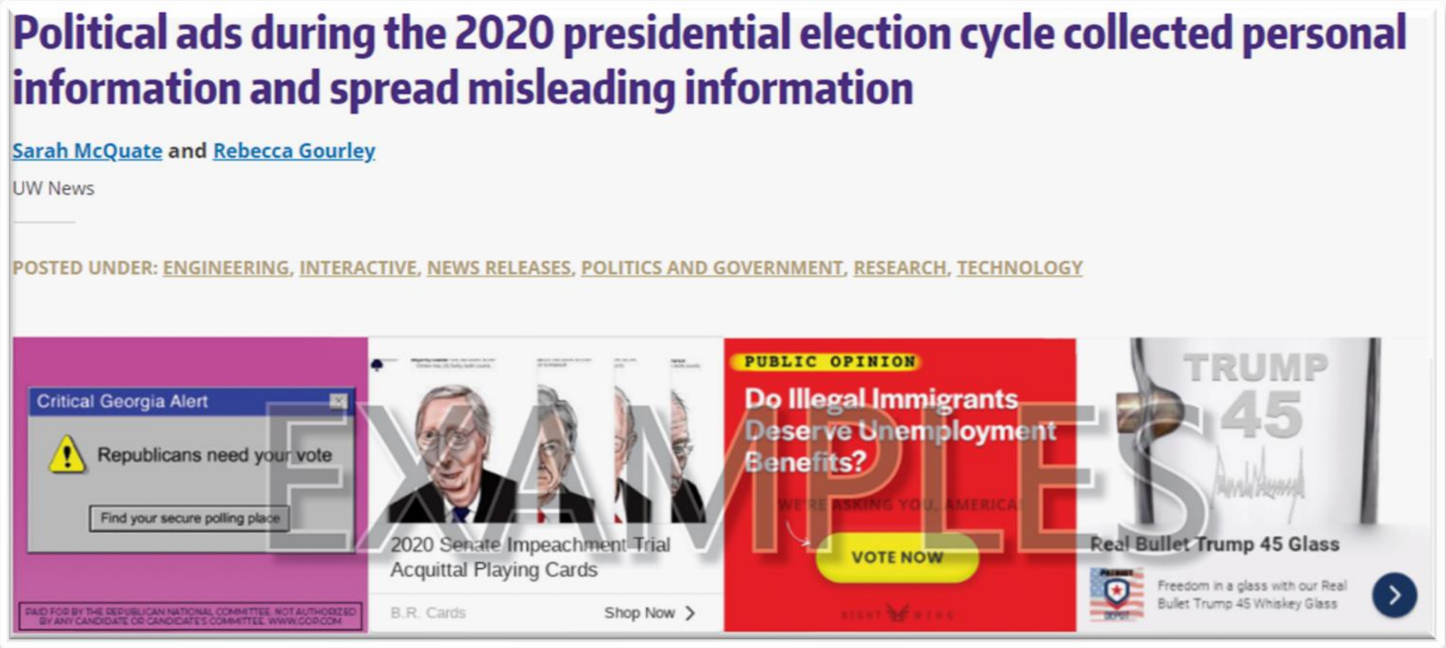
Kazakhstan government is intercepting HTTPS traffic in its capital

This marks the third time since 2015 that the Kazakh government is mandating the installation of a root certificate on its citizens' devices.

Examples: political misinformation

- Campaigns targeting users with particular interests or biases with advertisements or (mis)information

Examples: political misinformation



Political ads during the 2020 presidential election cycle collected personal information and spread misleading information

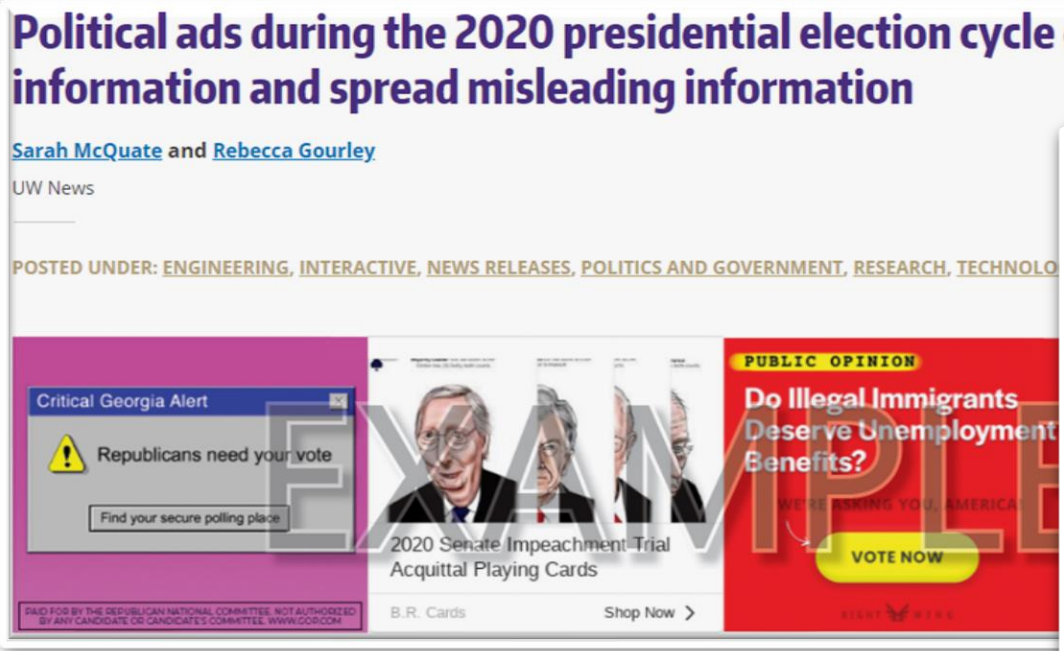
Sarah McQuate and Rebecca Gourley

UW News

POSTED UNDER: ENGINEERING, INTERACTIVE, NEWS RELEASES, POLITICS AND GOVERNMENT, RESEARCH, TECHNOLOGY

EXAMPLES
Critical Georgia Alert
Republicans need your vote
Find your secure polling place
PAID FOR BY THE REPUBLICAN NATIONAL COMMITTEE. NOT AUTHORIZED BY ANY CANDIDATE OR CANDIDATE'S COMMITTEE. WWW.GOP.COM
2020 Senate Impeachment Trial Acquittal Playing Cards
B.R. Cards
Shop Now
PUBLIC OPINION
Do Illegal Immigrants Deserve Unemployment Benefits?
WE'RE ASKING YOU, AMERICA!
VOTE NOW
RIGHT WING
TRUMP 45
Real Bullet Trump 45 Glass
Freedom in a glass with our Real Bullet Trump 45 Whiskey Glass

Examples: political misinformation



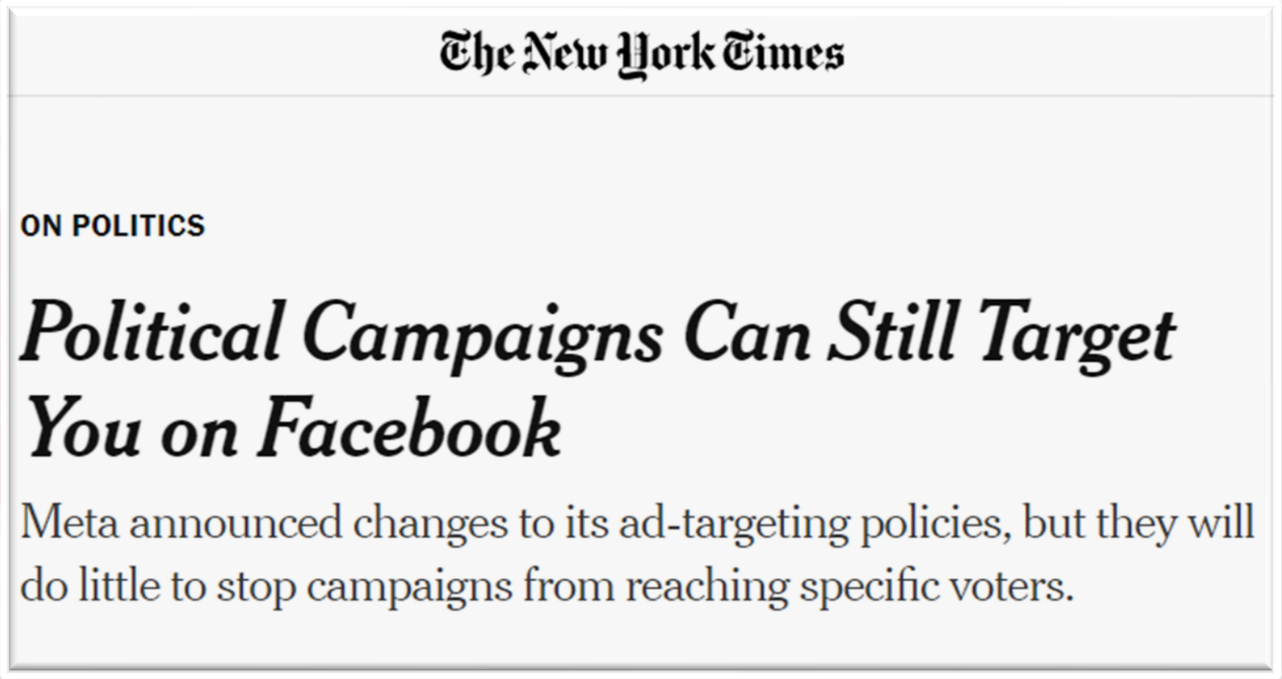
Political ads during the 2020 presidential election cycle collected personal information and spread misleading information

Sarah McQuate and Rebecca Gourley

UW News

POSTED UNDER: ENGINEERING, INTERACTIVE, NEWS RELEASES, POLITICS AND GOVERNMENT, RESEARCH, TECHNOLO

Critical Georgia Alert
Republicans need your vote
Find your secure polling place
PAID FOR BY THE REPUBLICAN NATIONAL COMMITTEE. NOT AUTHORIZED BY ANY CANDIDATE OR CANDIDATE'S COMMITTEE. WWW.GOP.COM
EXAMPLE
2020 Senate Impeachment Trial Acquittal Playing Cards
B.R. Cards
Shop Now
PUBLIC OPINION
Do Illegal Immigrants Deserve Unemployment Benefits?
WE'RE ASKING YOU, AMERICA
VOTE NOW



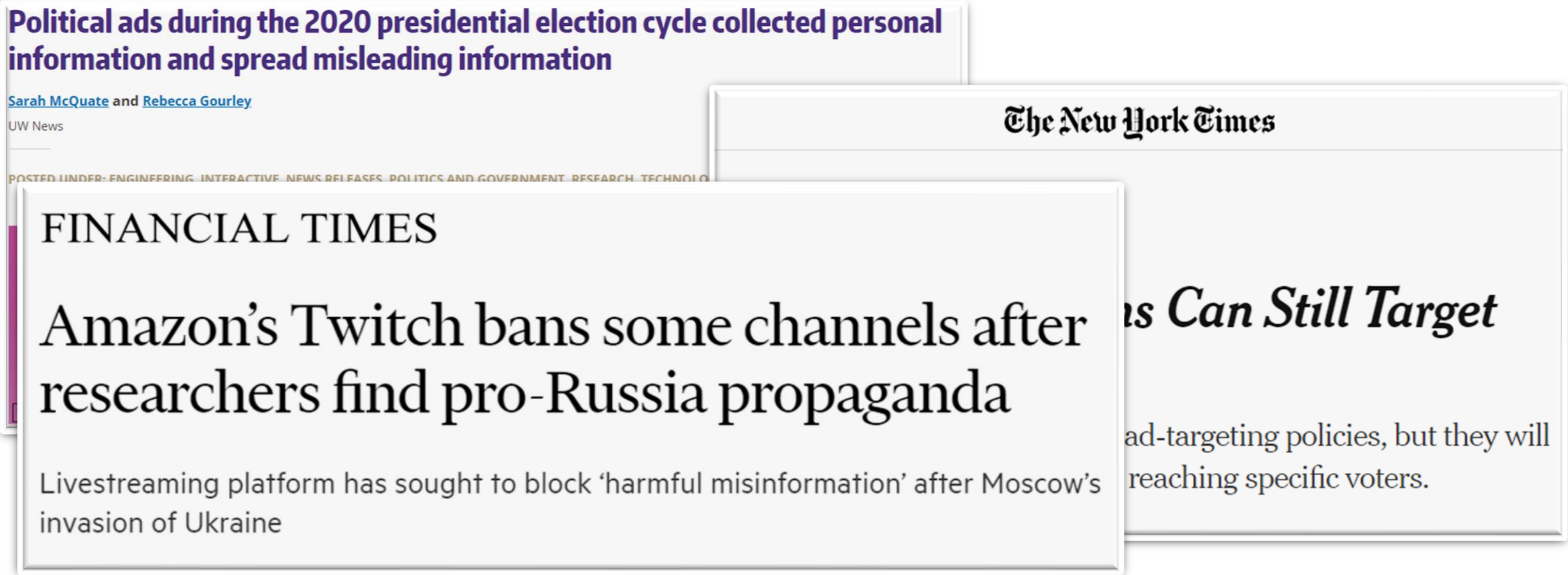
The New York Times

ON POLITICS

Political Campaigns Can Still Target You on Facebook

Meta announced changes to its ad-targeting policies, but they will do little to stop campaigns from reaching specific voters.

Examples: political misinformation



Political ads during the 2020 presidential election cycle collected personal information and spread misleading information

Sarah McQuate and Rebecca Gourley

UW News

POSTED UNDER: ENGINEERING, INTERACTIVE, NEWS RELEASES, POLITICS AND GOVERNMENT, RESEARCH, TECHNOLO

The New York Times

s Can Still Target

ad-targeting policies, but they will reaching specific voters.

FINANCIAL TIMES

Amazon's Twitch bans some channels after researchers find pro-Russia propaganda

Livestreaming platform has sought to block 'harmful misinformation' after Moscow's invasion of Ukraine

Contributions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)

Contributions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)

- High accuracy by passively eavesdropping for short time
  - Further increase by interacting with stream

Contributions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)
- High accuracy by passively eavesdropping for short time
  - Further increase by interacting with stream
- Demonstrate that naive use of HTTPS or VPN is not enough to protect users’ privacy
  - Packet sizes and their relative timing

Contributions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)
- High accuracy by passively eavesdropping for short time
  - Further increase by interacting with stream
- Demonstrate that naive use of HTTPS or VPN is not enough to protect users’ privacy
  - Packet sizes and their relative timing
- Large-scale evaluation of countermeasures
  - VPN, new client based timing countermeasure, packet padding

Contributions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)
- High accuracy by passively eavesdropping for short time
  - Further increase by interacting with stream
- Demonstrate that naive use of HTTPS or VPN is not enough to protect users' privacy
  - Packet sizes and their relative timing
- Large-scale evaluation of countermeasures
  - VPN, new client based timing countermeasure, packet padding
- Provide insights for websites and users to better protect their privacy

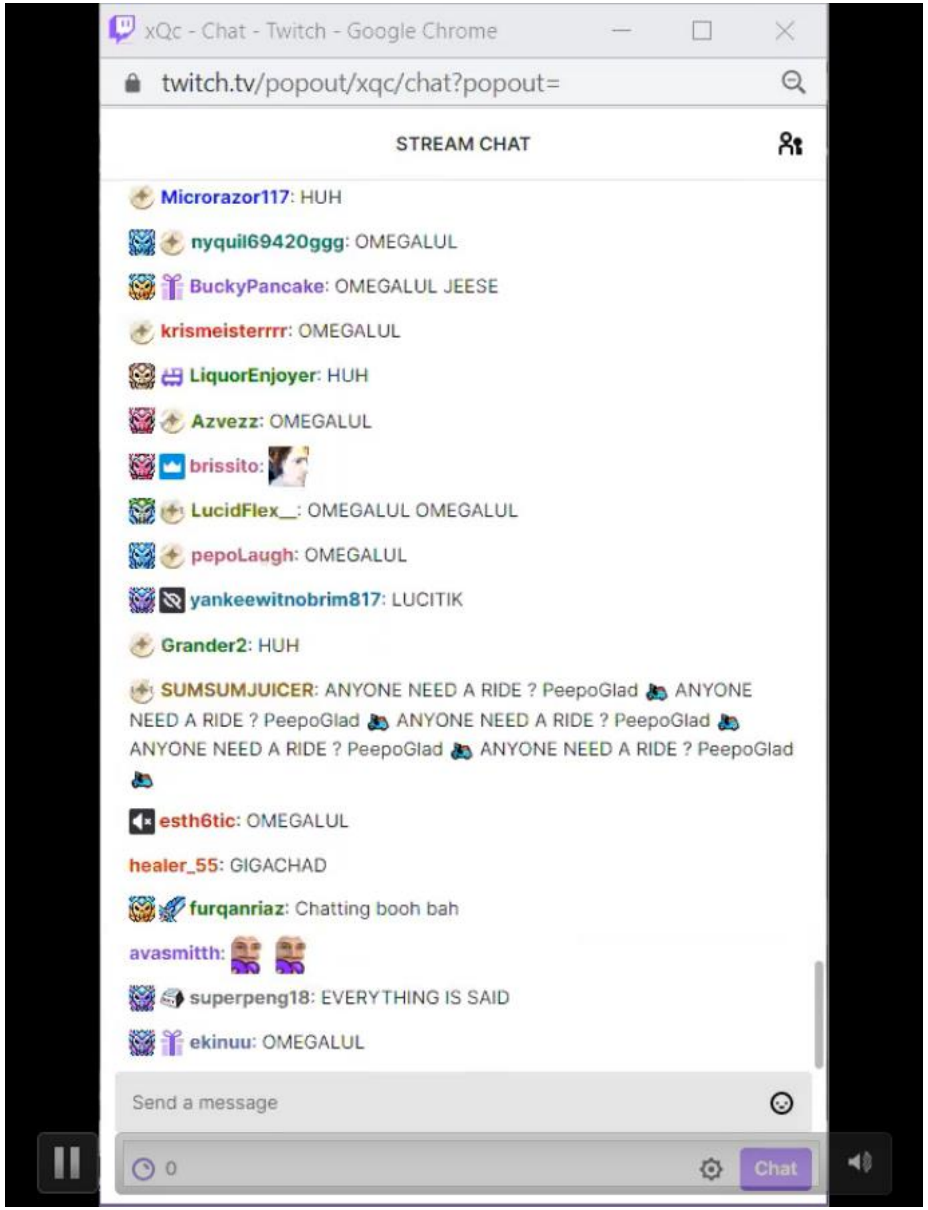
Fingerprinting

- Related work has identified on-demand video using Variable Bit Rate (VBR) encoding
- Twitch uses Constant Bit Rate (CBR) encoding by default
  - Video patterns does not leak information
- Encrypted chat messages as a side-channel
  - Allows interaction with stream

Twitch chat

Twitch chat

- » Distinguishable patterns between streams
  - » Packet size
  - » Packet timing (relative)
- » Two users watching the stream have similar network patterns
- » Users identifiable based on their encrypted network patterns



xQc - Chat - Twitch - Google Chrome

twitch.tv/popout/xqc/chat?popout=

Microrazor117: HUH

nyquil69420ggg: OMEGALUL

BuckyPancake: OMEGALUL JEESE

krismeisterrrr: OMEGALUL

LiquorEnjoyer: HUH

Azvezz: OMEGALUL

brissito:

LucidFlex_: OMEGALUL OMEGALUL

pepoLaugh: OMEGALUL

yankeewitnobrim817: LUCITIK

Grander2: HUH

SUMSUMJUICER: ANYONE NEED A RIDE ? PeepoGlad ANYONE NEED A RIDE ? PeepoGlad ANYONE NEED A RIDE ? PeepoGlad ANYONE NEED A RIDE ? PeepoGlad ANYONE NEED A RIDE ? PeepoGlad

esth6tic: OMEGALUL

healer_55: GIGACHAD

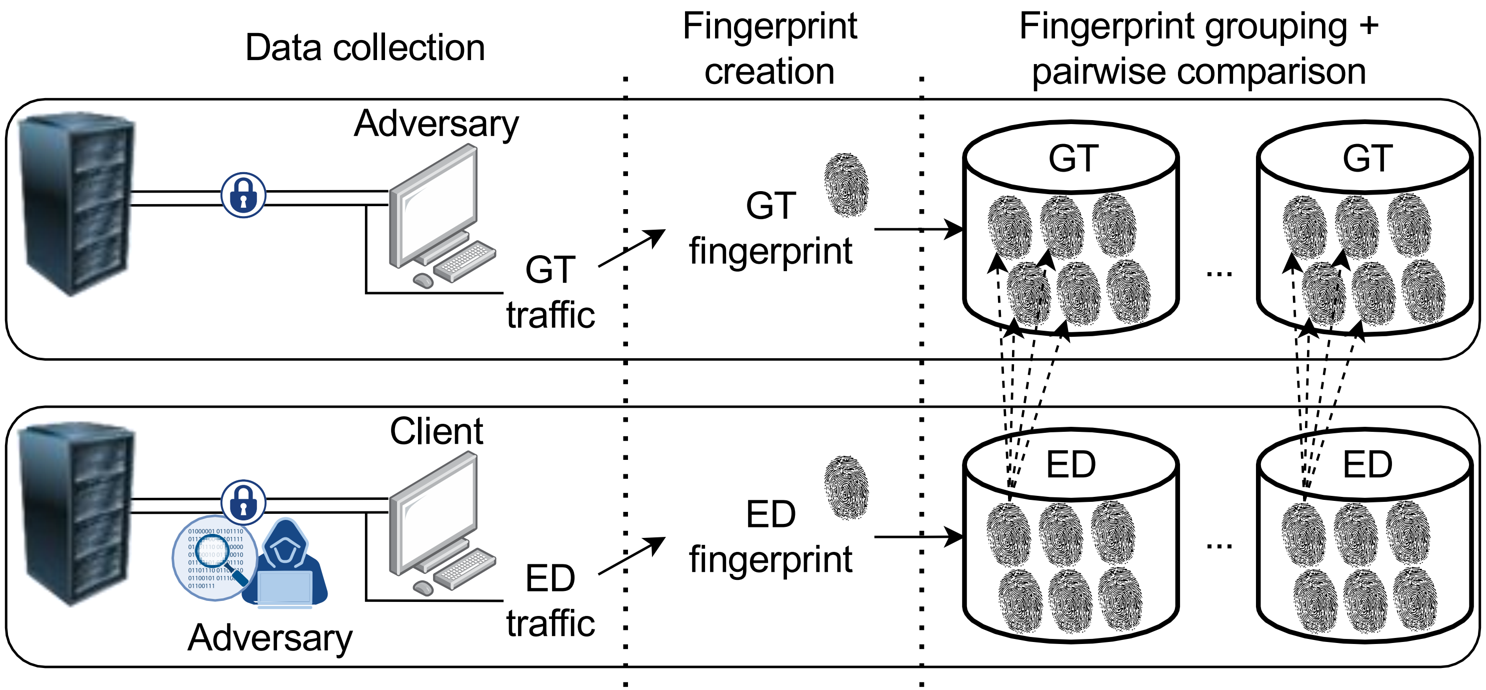
furqanriaz: Chatting booh bah

avasmitth:

superpeng18: EVERYTHING IS SAID

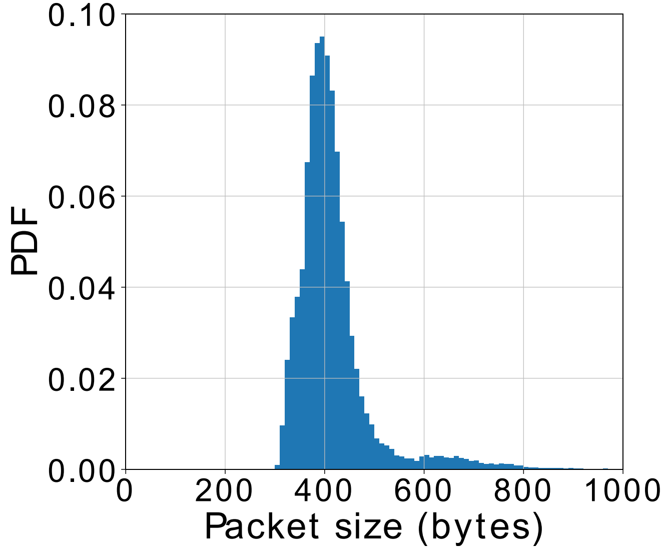
ekinuu: OMEGALUL

System overview



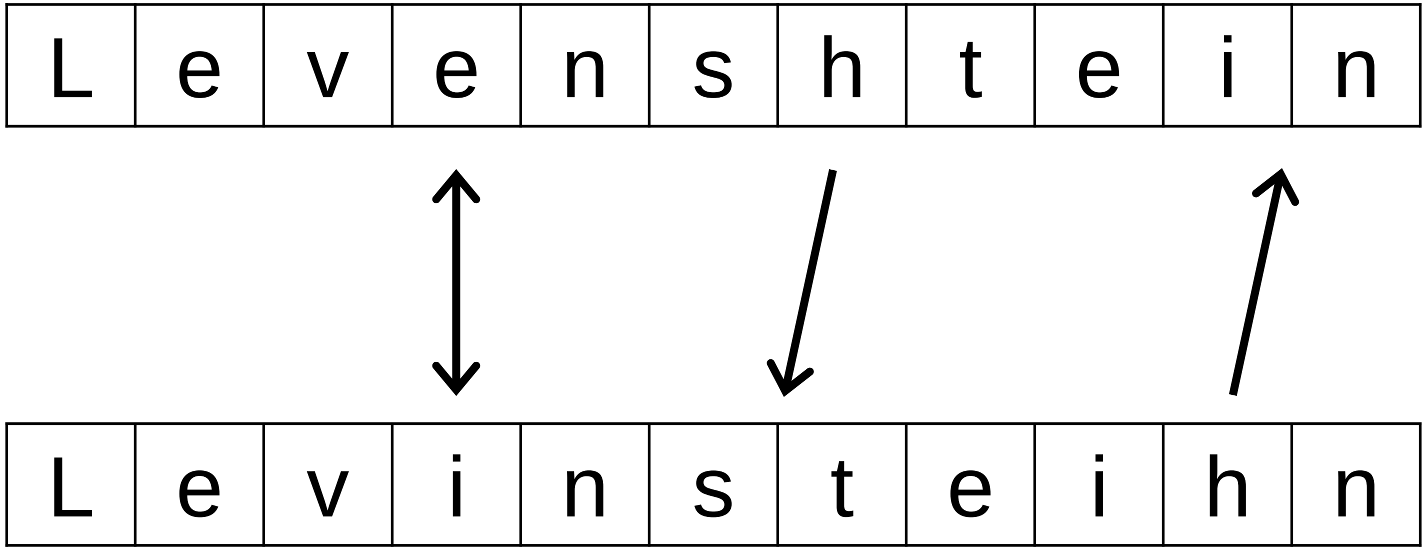
Data extraction: Twitch

- Video and chat data are delivered separately
- IP addresses for chat messages resolve to *ec2-[ip].us-west-2.compute.amazonaws.com*
- Internet Relay Chat and WebSocket Secure protocol with URL *irc-ws.chat.twitch.tv*
- Periodical resolve request URL
- Packet size distribution if IP addresses not available



Edit distance

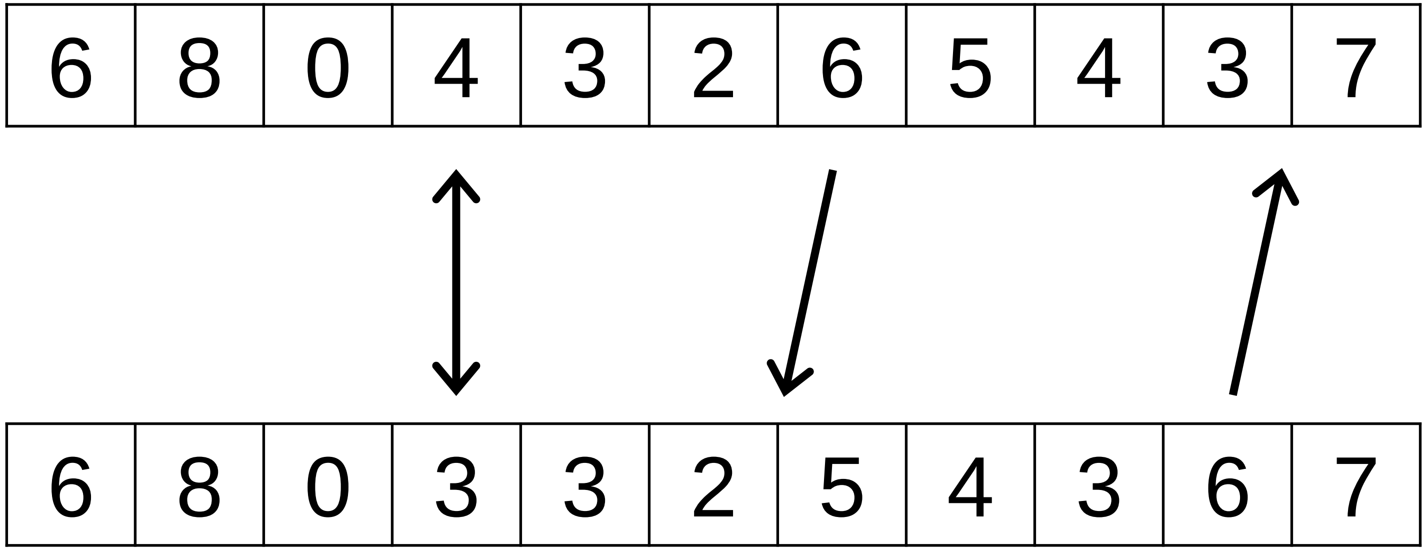
- 3 operations
  - Substitution
  - Insertion
  - Deletion



L	e	v	e	n	s	h	t	e	i	n
L	e	v	i	n	s	t	e	i	h	n

Edit distance

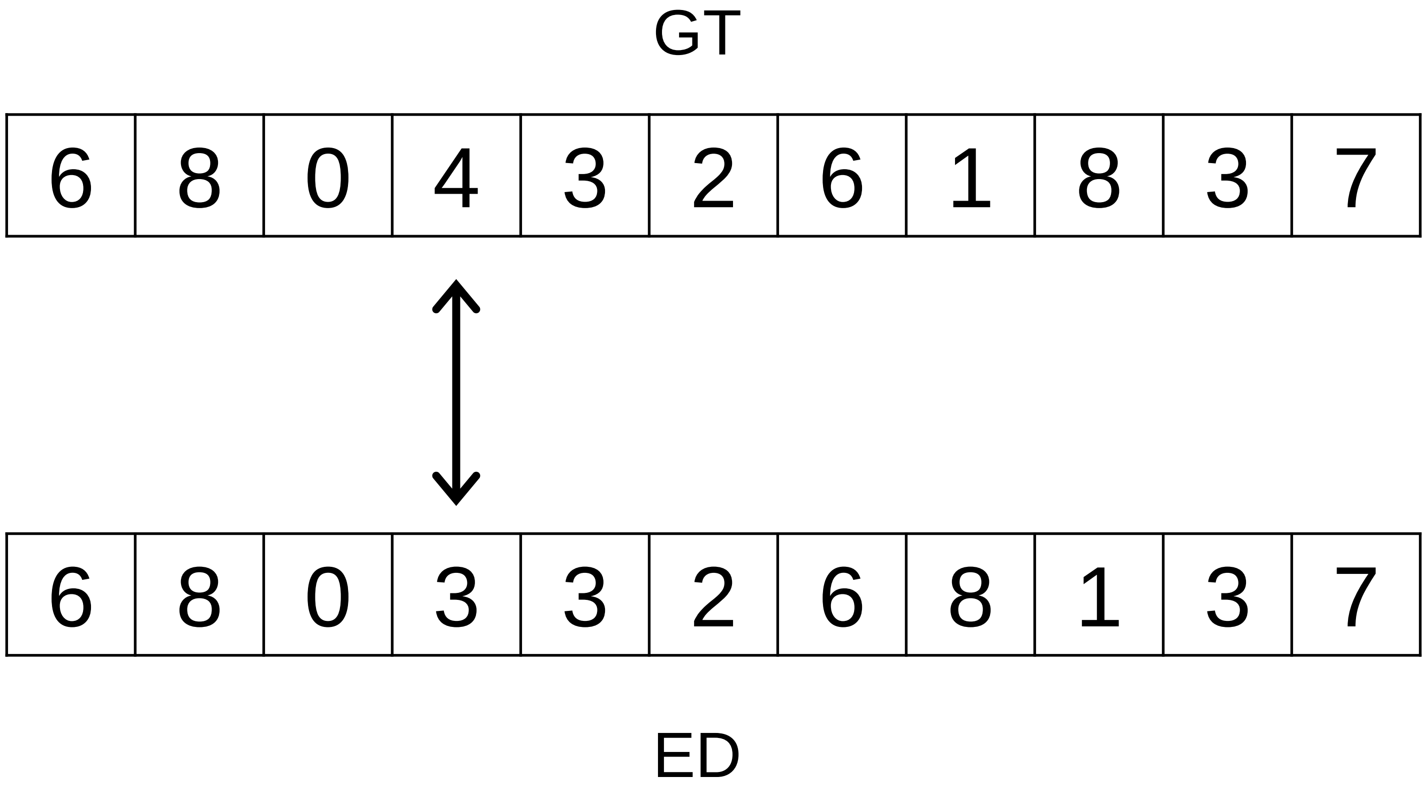
- 3 operations
  - Substitution
  - Insertion
  - Deletion



6	8	0	4	3	2	6	5	4	3	7
6	8	0	3	3	2	5	4	3	6	7

Edit distance

$$C_i = \frac{|\mathrm{GT}_i - \mathrm{ED}_i|}{\mathrm{GT}_i} = 0.25$$



GT

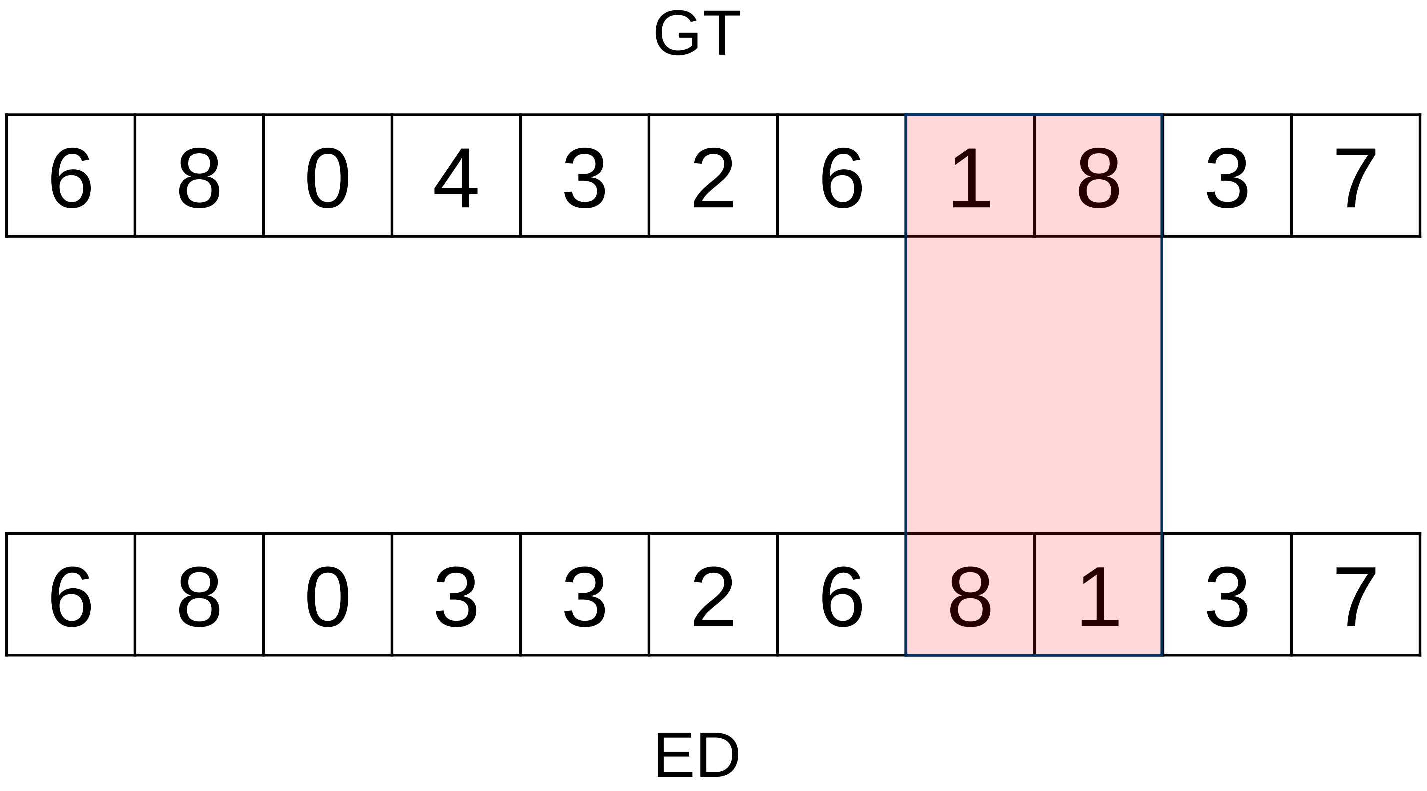
6	8	0	4	3	2	6	1	8	3	7

6	8	0	3	3	2	6	8	1	3	7

ED

Edit distance

$$C_i = \frac{|\mathrm{GT}_i - \mathrm{ED}_i|}{\mathrm{GT}_i} = 0.25$$



GT

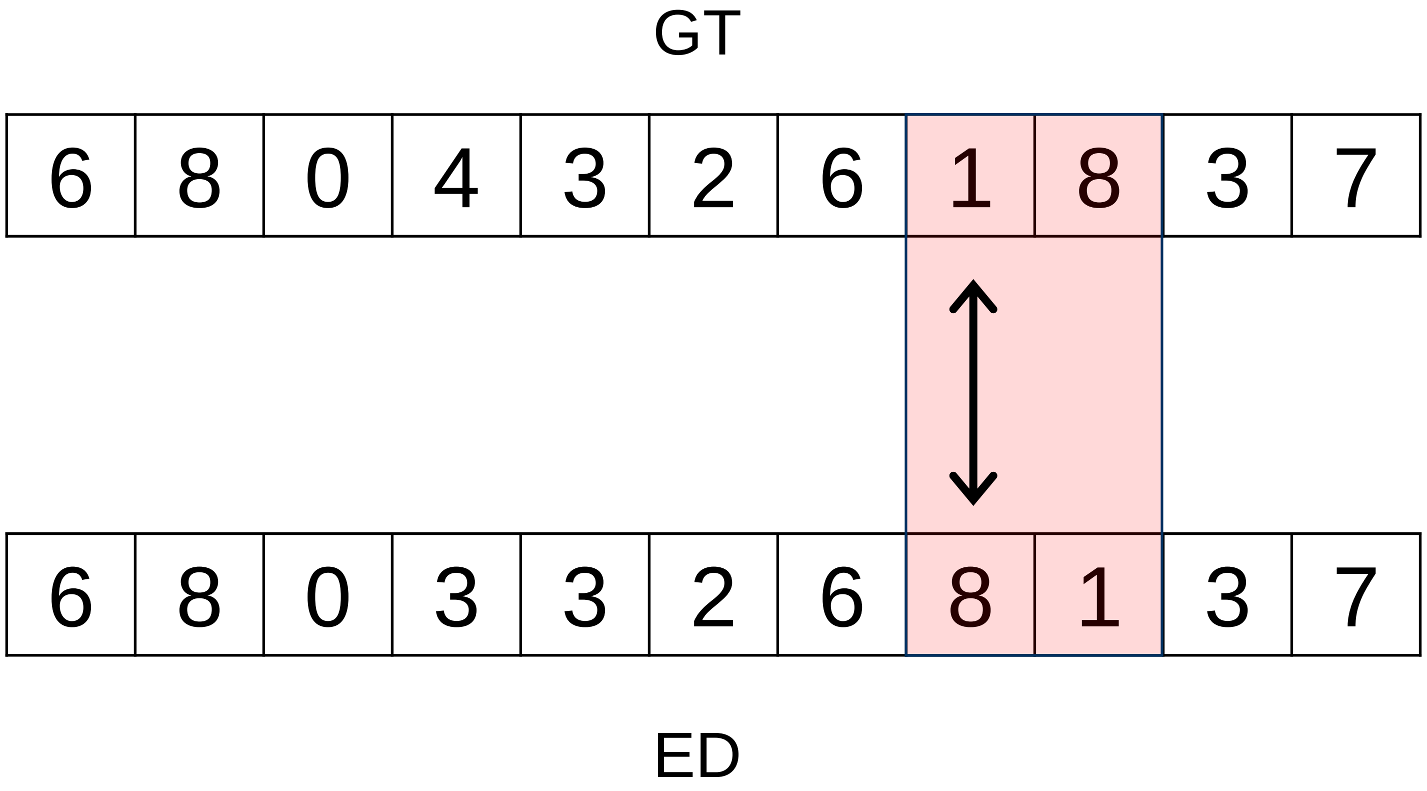
6	8	0	4	3	2	6	1	8	3	7
6	8	0	3	3	2	6	8	1	3	7

ED

Edit distance

$$C_i = \frac{|\mathrm{GT}_i - \mathrm{ED}_i|}{\mathrm{GT}_i} = 0.25$$

$$C_i = \text{min(left, mid, right)}$$

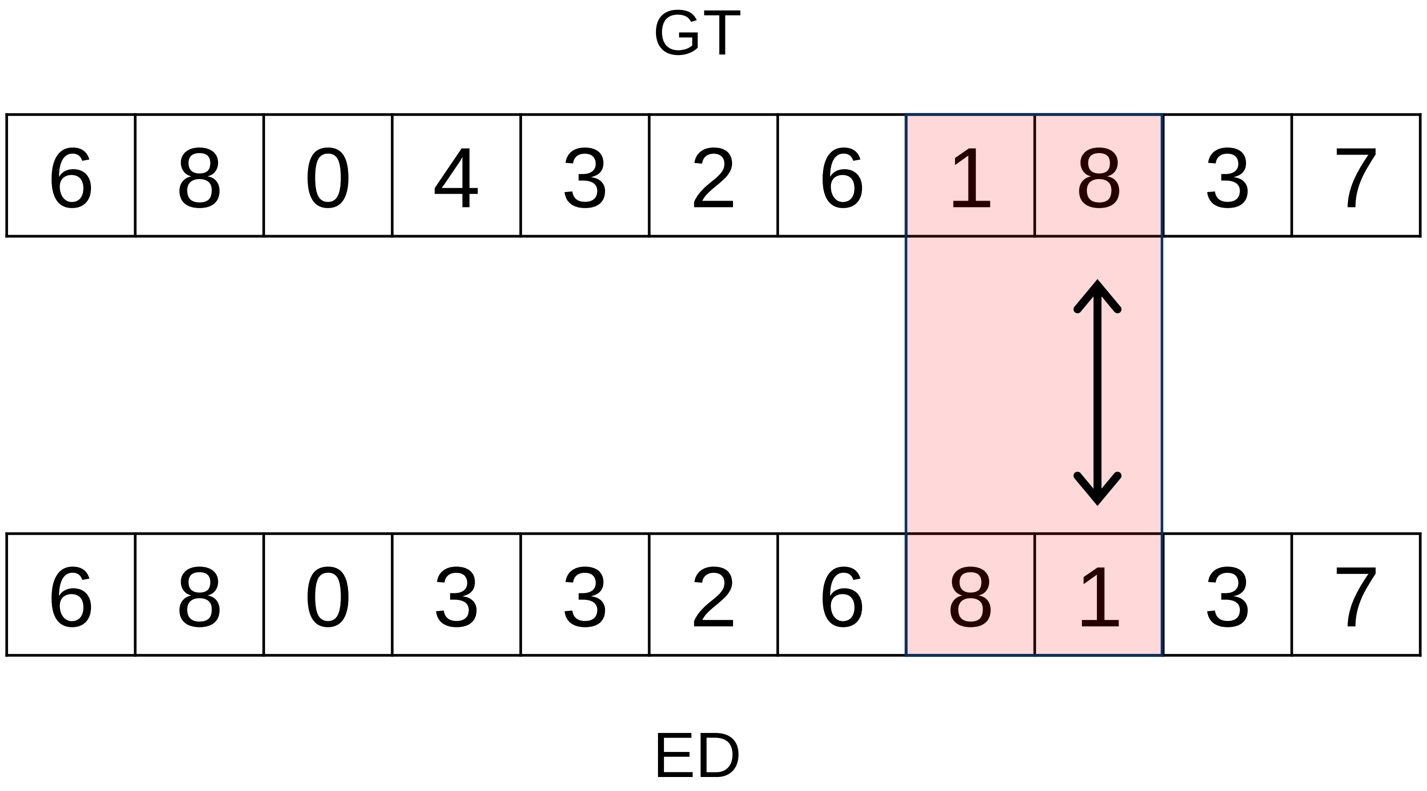


GT	6	8	0	4	3	2	6	1	8	3	7
ED	6	8	0	3	3	2	6	8	1	3	7

Edit distance

$$C_i = \frac{|\mathrm{GT}_i - \mathrm{ED}_i|}{\mathrm{GT}_i} = 0.25$$

$$C_i = \text{min(left, mid, right)}$$



GT

6	8	0	4	3	2	6	1	8	3	7
6	8	0	3	3	2	6	8	1	3	7

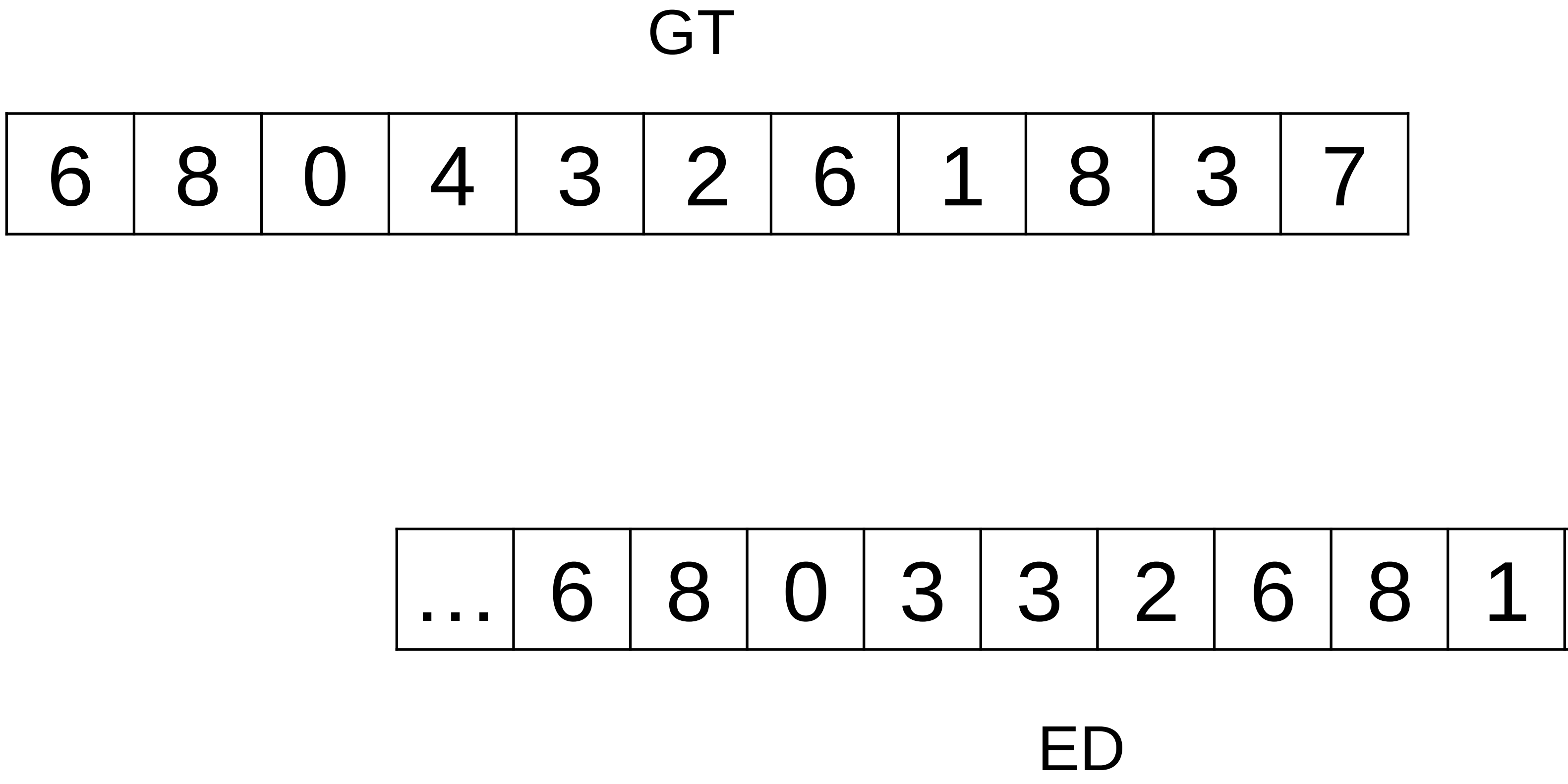
ED

Edit distance

$$C_i = \frac{|\mathrm{GT}_i - \mathrm{ED}_i|}{\mathrm{GT}_i} = 0.25$$

$$C_i = \text{min(left, mid, right)}$$

Offset up to 10 seconds



GT

6	8	0	4	3	2	6	1	8	3	7

…	6	8	0	3	3	2	6	8	1

ED

Fingerprint comparison

- Each ED compared to all GT
  - $d = \{d_1, d_2, \dots, d_{1000}\}$

- Relative classifier
  - $d_2/d_1 > \mu$

- Absolute classifier
  - $d_1 < \lambda$

Fingerprint comparison

- Each ED compared to all GT
  - $d = \{d_1, d_2, \dots, d_{1000}\}$

- Relative classifier
  - $d_2/d_1 > \mu$

- Absolute classifier
  - $d_1 < \lambda$

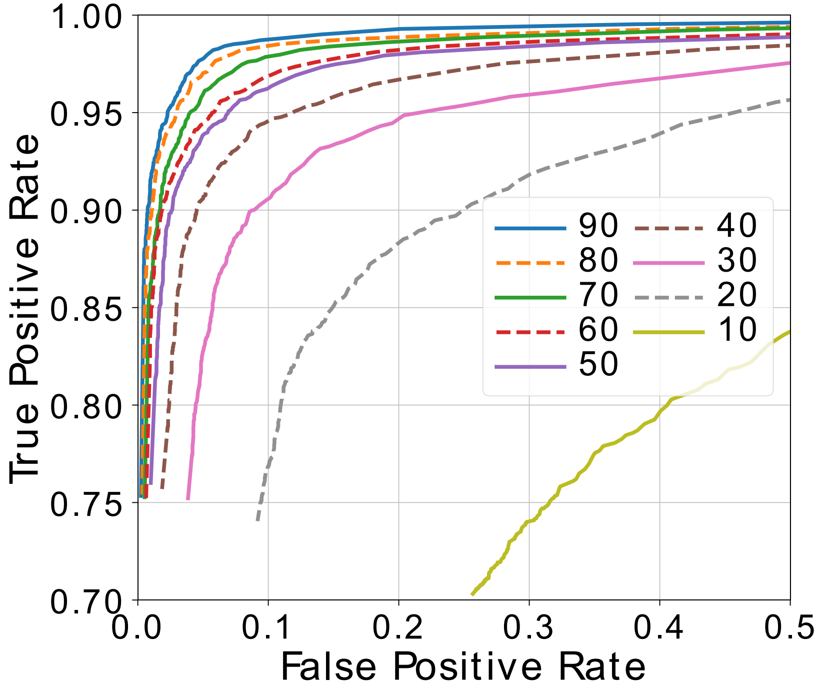
Example:

$d = \{20, 180, 185, \dots\}$ $\mu = 2.00$ $\lambda = 10$

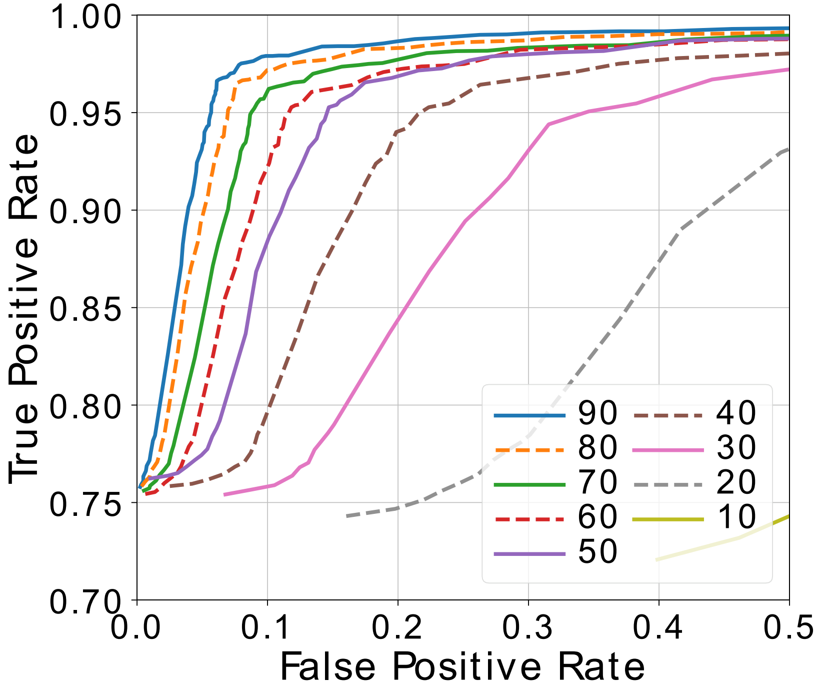
Relative: $\frac{180}{20} > 2.00$

Absolute: $20 \nless 2.00$

Example results: attack duration



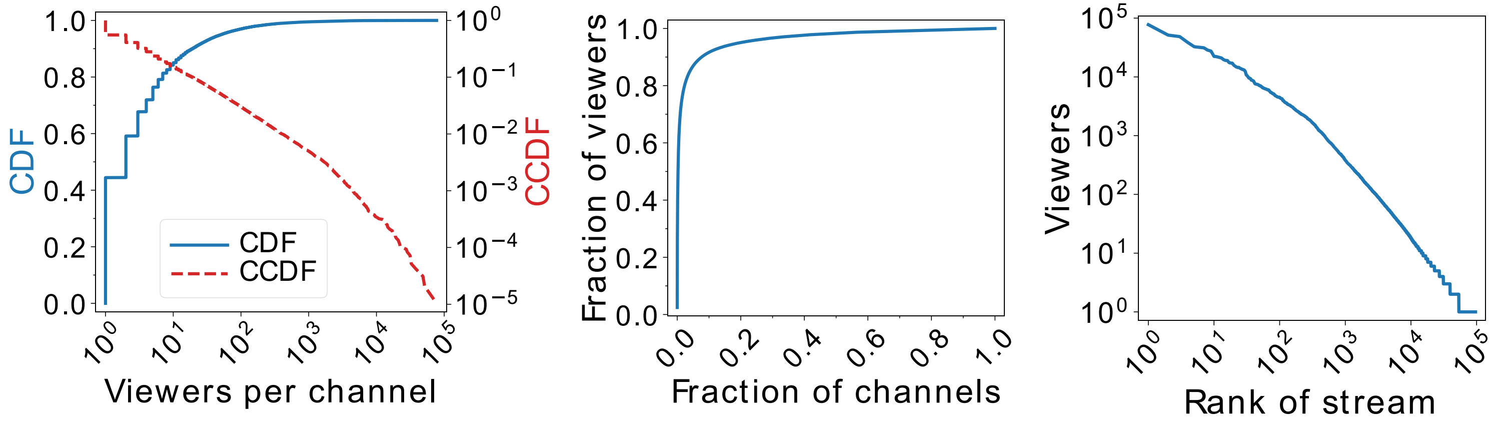
- Relative classifier
- Diminishing improvements
- F1-score 0.966 for 90 seconds

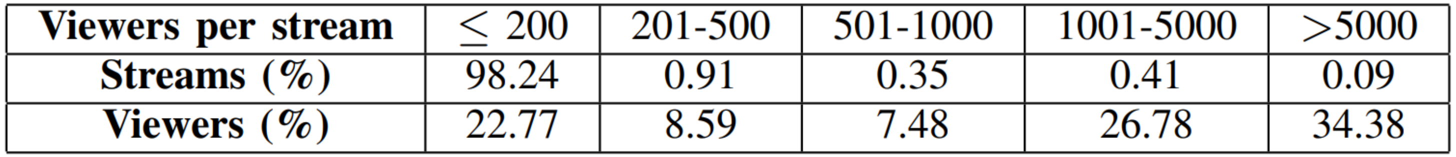


- Absolute classifier
- F1-score 0.953 for 90 seconds

Stream popularity: Twitch

- Viewer distribution is heavy tailed
  - Pareto principle

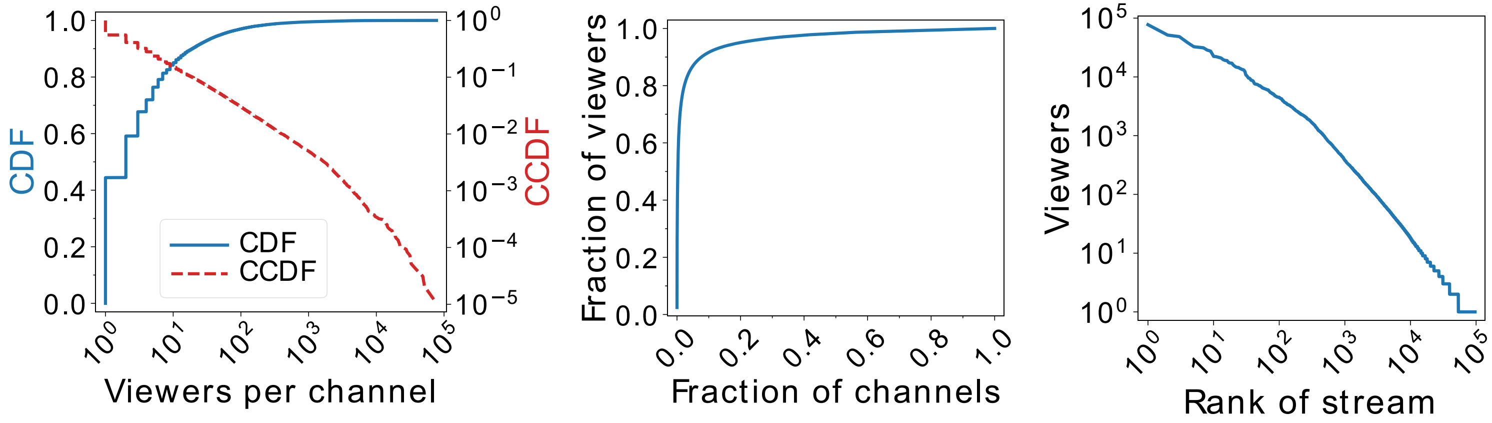




Viewers per stream	$\leq$ 200	201-500	501-1000	1001-5000	>5000
Streams (%)	98.24	0.91	0.35	0.41	0.09
Viewers (%)	22.77	8.59	7.48	26.78	34.38

Stream popularity: Twitch

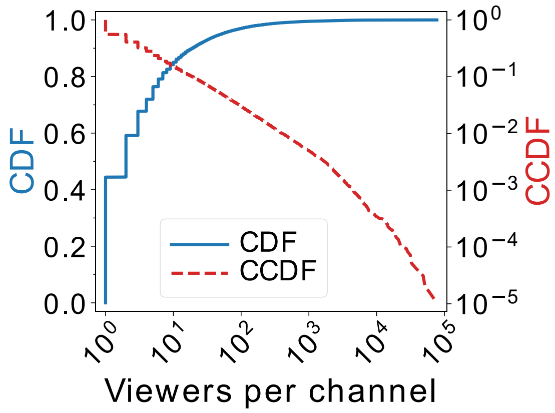
- Viewer distribution is heavy tailed
  - Pareto principle
  - 98% of channels have less than 200 viewers and 23% of viewers

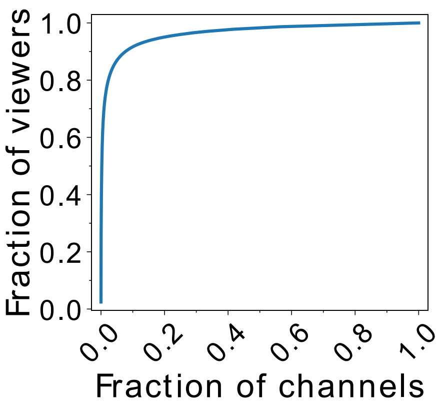


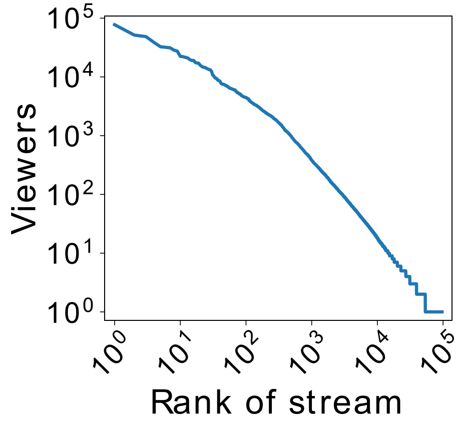
Viewers per stream	≤ 200	201-500	501-1000	1001-5000	>5000
Streams (%)	98.24	0.91	0.35	0.41	0.09
Viewers (%)	22.77	8.59	7.48	26.78	34.38

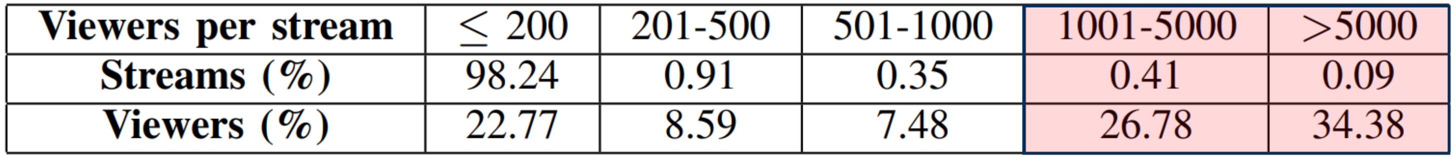
Stream popularity: Twitch

- Viewer distribution is heavy tailed
  - Pareto principle
  - 98% of channels have less than 200 viewers and 23% of viewers
  - 0.5% of channels have more than 1000 viewers and 61% of all viewers





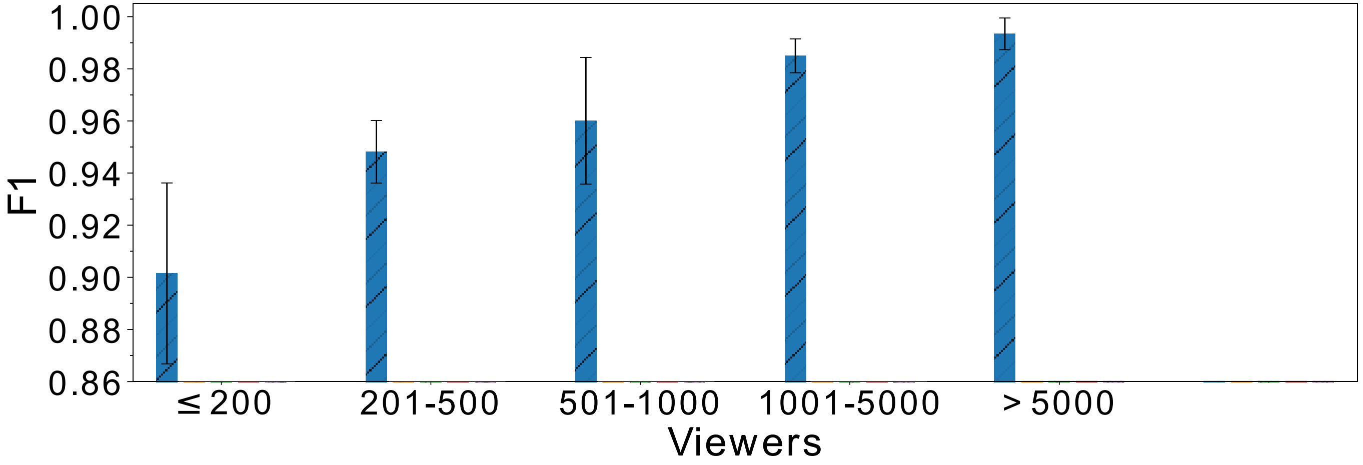




Viewers per stream	$\leq$ 200	201-500	501-1000	1001-5000	>5000
Streams (%)	98.24	0.91	0.35	0.41	0.09
Viewers (%)	22.77	8.59	7.48	26.78	34.38

Example results

- Accuracy much lower for less popular streams

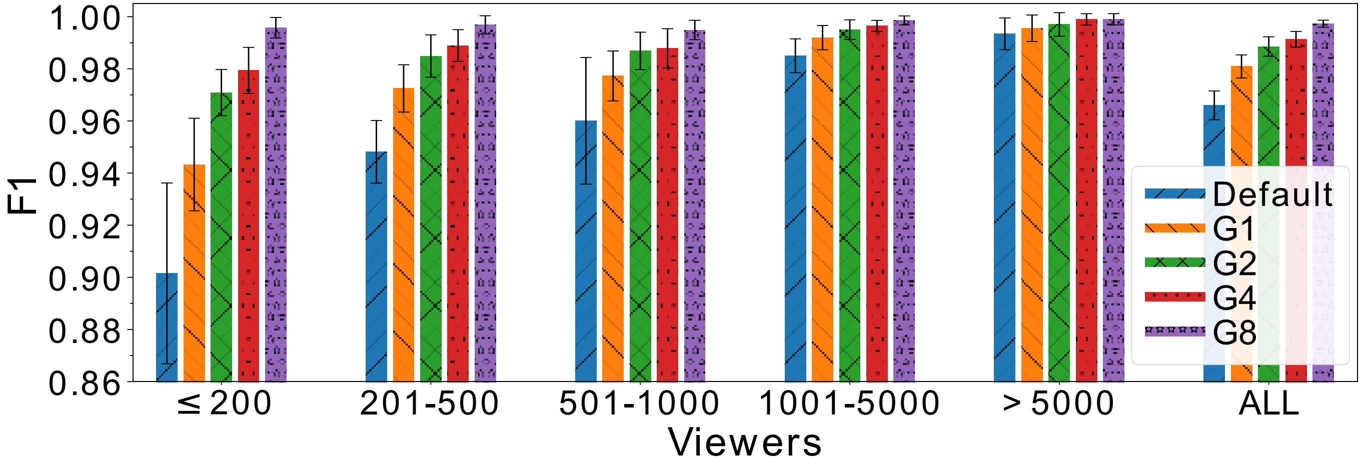


Example results

- Accuracy much lower for less popular streams

- Accuracy can be increased by interacting with the stream

- F1-score improves from 0.90 to 0.97 by inserting two additional chat messages



Countermeasures

- Five countermeasures
  - Campus-based off-the-shelf VPN
  - OpenVPN
  - Client timing
  - OpenVPN + padding
  - OpenVPN + padding + client timing

Countermeasure: client timing

- TCP Zero Window packets
  - Modification of TCP receive window

- Two random parameters
  - Silent/zero period t_z
  - Normal period t_n

- Burst of packets at start of t_n

- Larger silent period decreases accuracy at the cost of data freshness and traffic bursts

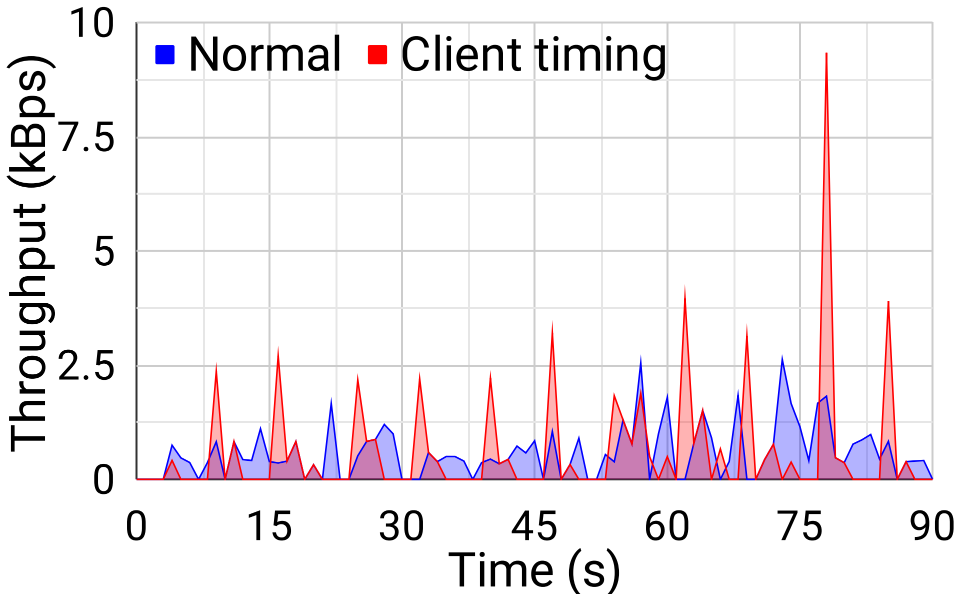
Countermeasure: client timing

- TCP Zero Window packets
  - Modification of TCP receive window

- Two random parameters
  - Silent/zero period t_z
  - Normal period t_n

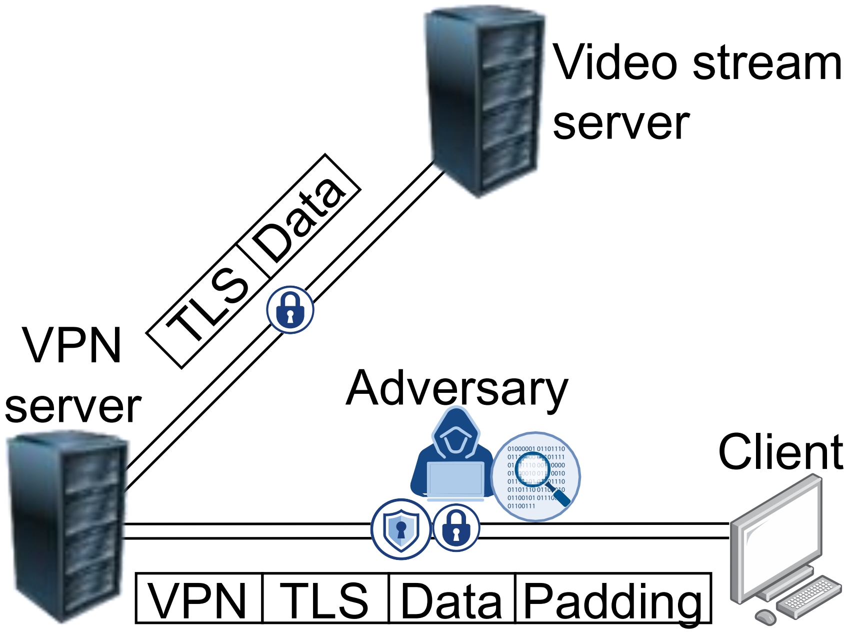
- Burst of packets at start of t_n

- Larger silent period decreases accuracy at the cost of data freshness and traffic bursts



$t_z = 5 \quad t_n = 2$

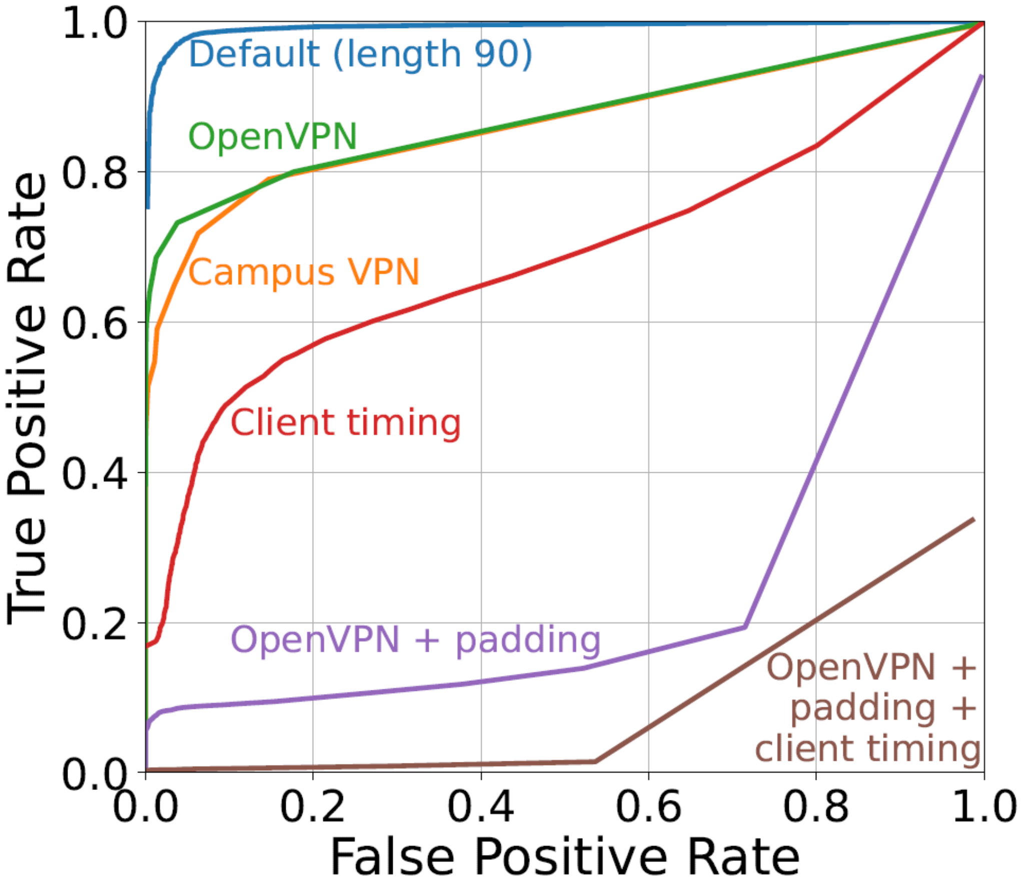
Countermeasure: padding



Countermeasure: results

- Best F1-scores
  - Default: 0.966
  - OpenVPN: 0.826
  - Campus VPN: 0.810
  - Client timing (5, 2): 0.637
  - OpenVPN + padding: 0.152

- Best protection achieved using a combination of countermeasures



Conclusions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)

Conclusions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)

- High accuracy by passively eavesdropping for short time
  - Further increase by interacting with stream

Conclusions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)

- High accuracy by passively eavesdropping for short time
  - Further increase by interacting with stream

- Demonstrate that naive use of HTTPS or VPN is not enough to protect users’ privacy
  - Packet sizes and their relative timing

Conclusions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)

- High accuracy by passively eavesdropping for short time
  - Further increase by interacting with stream

- Demonstrate that naive use of HTTPS or VPN is not enough to protect users’ privacy
  - Packet sizes and their relative timing

- Large-scale evaluation of countermeasures
  - VPN, new client based timing countermeasure, packet padding

Conclusions

- First fingerprinting attack against Twitch
  - Identify viewers of live streams despite encryption using chat messages
  - 140,000 fingerprints (3,700 hours of labeled data)
- High accuracy by passively eavesdropping for short time
  - Further increase by interacting with stream
- Demonstrate that naive use of HTTPS or VPN is not enough to protect users’ privacy
  - Packet sizes and their relative timing
- Large-scale evaluation of countermeasures
  - VPN, new client based timing countermeasure, packet padding
- Provide insights for websites and users to better protect their privacy

Twitch Chat Fingerprinting

David Hasselquist
Christian Vestlund
Niklas Johansson
Niklas Carlsson

David Hasselquist (david.hasselquist@liu.se)