UNIVERSITÄT PADERBORN

IT - Security Group — UPB

Website Fingerprinting Defense: Walkie Talkie — A Review

Ashwin Prasad Shivarpatna Venkatesh

UNIVERSITÄT PADERBORN

Overview

UNIVERSITÄT PADERBORN

Context

- Internet users want to protect their privacy

UNIVERSITÄT PADERBORN

Context

- Internet users want to protect their privacy
- **Technologies:** VPNs, Tor – ***Encrypt Traffic***

Context

- Internet users want to protect their privacy
- **Technologies:** VPNs, Tor – ***Encrypt Traffic***
- But, what about a local observer?

UNIVERSITÄT PADERBORN

Context

- Internet users want to protect their privacy
- **Technologies:** VPNs, Tor – ***Encrypt Traffic***
- But, what about a local observer?
  - Can see packet sequence

UNIVERSITÄT PADERBORN

Context

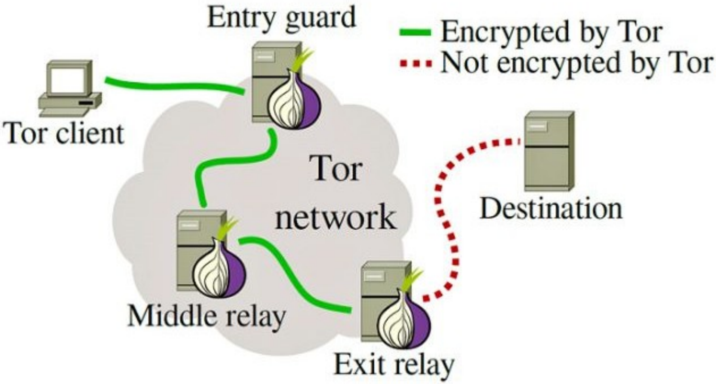
- Internet users want to protect their privacy
- **Technologies:** VPNs, Tor – ***Encrypt Traffic***
- But, what about a local observer?
  - Can see packet sequence
  - Find patterns to expose activity

UNIVERSITÄT PADERBORN

Context

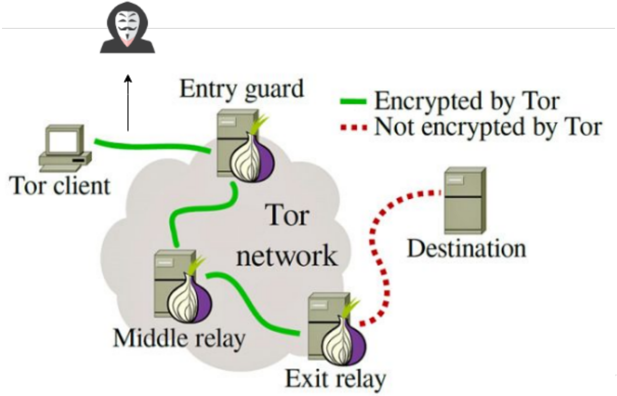
- Internet users want to protect their privacy
- **Technologies:** VPNs, Tor – ***Encrypt Traffic***
- But, what about a local observer?
  - Can see packet sequence
  - Find patterns to expose activity
  - ***Website Fingerprinting!***

Tor Network


Entry guard
Encrypted by Tor
Not encrypted by Tor
Tor client
Tor
network
Destination
Middle relay
Exit relay

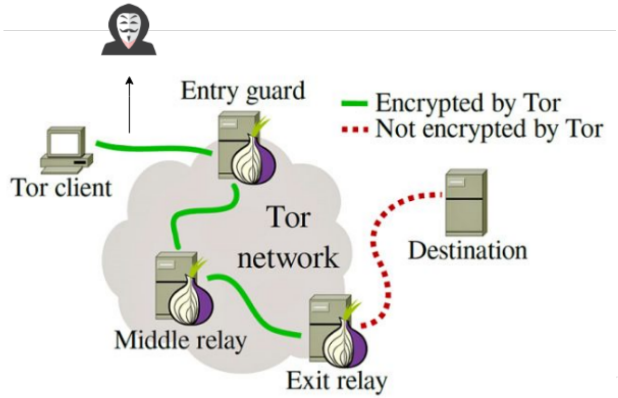
Attacker Model

- Local, Passive Attacker



Attacker Model

- Local, Passive Attacker
- ***ISP, Network administrator, Hacker...***



Exactly what features are used for website fingerprinting?

Exploitable Features

- Total transmission time, size

Exploitable Features

- Total transmission time, size
- Number of packets or ***cells***
  - **Cell** – Tor sends data in fixed-size (512-byte) packets

UNIVERSITÄT PADERBORN

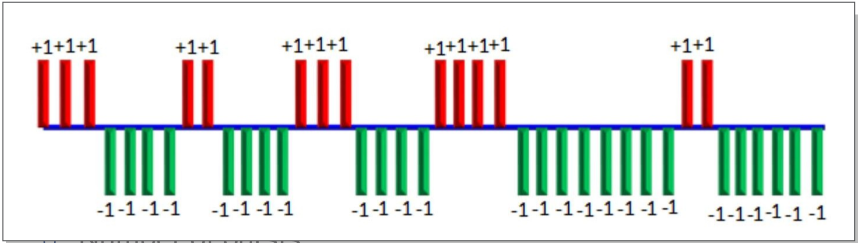
Exploitable Features

- Total transmission time, size
- Number of packets or ***cells***
  - **Cell** – Tor sends data in fixed-size (512-byte) packets
- Direction of cells
  - incoming and outgoing cells

Exploitable Features

- Total transmission time, size
- Number of packets or ***cells***
  - **Cell** – Tor sends data in fixed-size (512-byte) packets
- Direction of cells
  - incoming and outgoing cells
- Number of bursts
  - **Burst** – Number of cells in the same direction

Exploitable Features



- Number of bursts
  - **Burst** – Number of cells in the same direction

How does WF attacks work?

How does WF attacks work?

Machine learning — Classification of features

UNIVERSITÄT PADERBORN

Attacks

k-NN Classifier — [Wang et al.]

- Simple supervised learning algorithm

Attacks

k-NN Classifier — [Wang et al.]

- Simple supervised learning algorithm
- Training by learning distance between points
- Non-trivial distance function

UNIVERSITÄT PADERBORN

Attacks

k-NN Classifier — [Wang et al.]

- Simple supervised learning algorithm
- Training by learning distance between points
- Non-trivial distance function
- **Features:** Total size, time, packet ordering, bursts...

Attacks

k-NN Classifier — [Wang et al.]

- Simple supervised learning algorithm
- Training by learning distance between points
- Non-trivial distance function
- **Features:** Total size, time, packet ordering, bursts...

Deep Fingerprinting — [Sirinam et al.]

- Convolutional Neural Network

Attacks

k-NN Classifier — [Wang et al.]

- Simple supervised learning algorithm
- Training by learning distance between points
- Non-trivial distance function
- **Features:** Total size, time, packet ordering, bursts...

Deep Fingerprinting — [Sirinam et al.]

- Convolutional Neural Network
- Automatically detects important features
- **Hyperparameter Tuning:** adjusting trade-off

So, how to defend against WF attacks?

So, how to defend against WF attacks?

Traffic Manipulation — Mask unique features

Defense

- **Tamaraw** — [Cai et al.]
- **Supersequence** — [Wang et al.]
- **WTF-PAD** — [Juarez et al.]
- **...**

UNIVERSITÄT PADERBORN

Defense

- **Tamaraw** — [Cai et al.]
- **Supersequence** — [Wang et al.]
- **WTF-PAD** — [Juarez et al.]
- **...**

Walkie-Talkie — [Wang and Goldberg]

- Universal, provable, light weight WF defense

Defense

- **Tamaraw** — [Cai et al.]
- **Supersequence** — [Wang et al.]
- **WTF-PAD** — [Juarez et al.]
- **...**

Walkie-Talkie — [Wang and Goldberg]

- Universal, provable, light weight WF defense
- Half-duplex communication

Defense

- **Tamaraw** — [Cai et al.]
- **Supersequence** — [Wang et al.]
- **WTF-PAD** — [Juarez et al.]
- **...**

Walkie-Talkie — [Wang and Goldberg]

- Universal, provable, light weight WF defense
- Half-duplex communication
- Burst molding

Defense

- **Tamaraw** — [Cai et al.]
- **Supersequence** — [Wang et al.]
- **WTF-PAD** — [Juarez et al.]
- **...**

Walkie-Talkie — [Wang and Goldberg]

- Universal, provable, light weight WF defense
- Half-duplex communication
- Burst molding
- 50% max attacker accuracy

Full Duplex Communication

1. Request google.com $-- >$

Full Duplex Communication

1. Request google.com $-->$
2. $<--$ Start receiving google.com

Full Duplex Communication

1. Request google.com $-- >$
2. $< --$ Start receiving google.com
3. Browser notices google.com has logo.jpg

Full Duplex Communication

1. Request google.com $-- >$
2. $< --$ Start receiving google.com
3. Browser notices google.com has logo.jpg
4. Request logo.jpg $-- >$

Full Duplex Communication

1. Request google.com $-- >$
2. $< --$ Start receiving google.com
3. Browser notices google.com has logo.jpg
4. Request logo.jpg $-- >$
5. Browser notices google.com has icon.png

UNIVERSITÄT PADERBORN

Full Duplex Communication

1. Request google.com $-- >$
2. $< --$ Start receiving google.com
3. Browser notices google.com has logo.jpg
4. Request logo.jpg $-- >$
5. Browser notices google.com has icon.png
6. Request icon.png $-- >$

Full Duplex Communication

1. Request google.com $-- >$
2. $< --$ Start receiving google.com
3. Browser notices google.com has logo.jpg
4. Request logo.jpg $-- >$
5. Browser notices google.com has icon.png
6. Request icon.png $-- >$
7. ...

Full Duplex Communication

1. Request google.com $-->$
2. $<--$ Start receiving google.com
3. Browser notices google.com has logo.jpg
4. Request logo.jpg $-->$
5. Browser notices google.com has icon.png
6. Request icon.png $-->$
7. ...

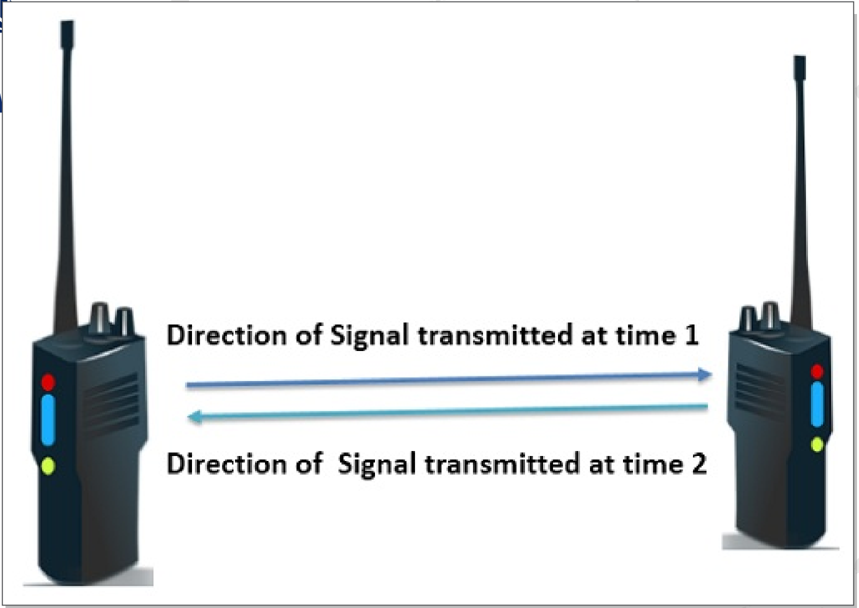
UNIVERSITÄT PADERBORN

Full Duplex Communication

1. Request google.com $-- >$
2. $< --$ Start receiving google.com
3. Browser notices google.com has logo.jpg
4. Request logo.jpg $-- >$
5. Browser notices google.com has icon.png
6. Request icon.png $-- >$
7. ...

Notice that 4, 6 happens while other requests are still not finished

W


Direction of Signal transmitted at time 1
Direction of Signal transmitted at time 2

W-T — Half Duplex Communication

1. Request google.com $-- >$

UNIVERSITÄT PADERBORN

W-T — Half Duplex Communication

1. Request google.com $-->$
2. $<--$ Finish receiving google.com

UNIVERSITÄT PADERBORN

W-T — Half Duplex Communication

1. Request google.com $-- >$
2. $< --$ Finish receiving google.com
3. Browser notices google.com has logo.jpg, icon.png ...

W-T — Half Duplex Communication

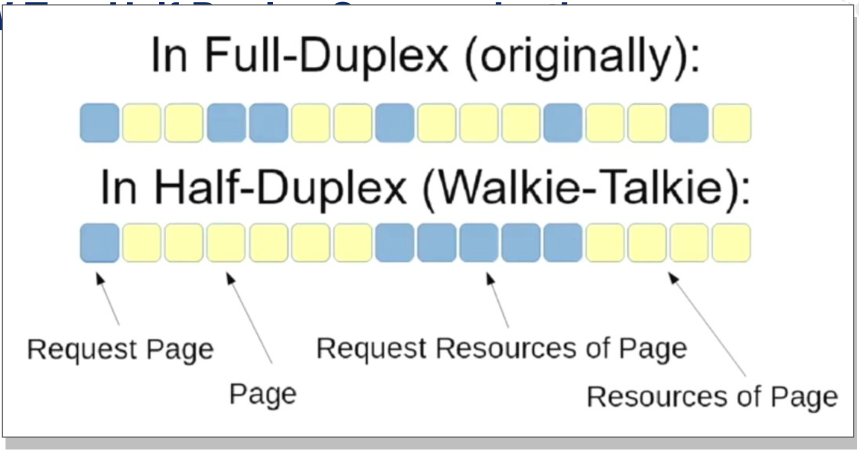
1. Request google.com $-->$
2. $<--$ Finish receiving google.com
3. Browser notices google.com has logo.jpg, icon.png ...
4. Request logo.jpg, icon.png $-->$

W-T — Half Duplex Communication

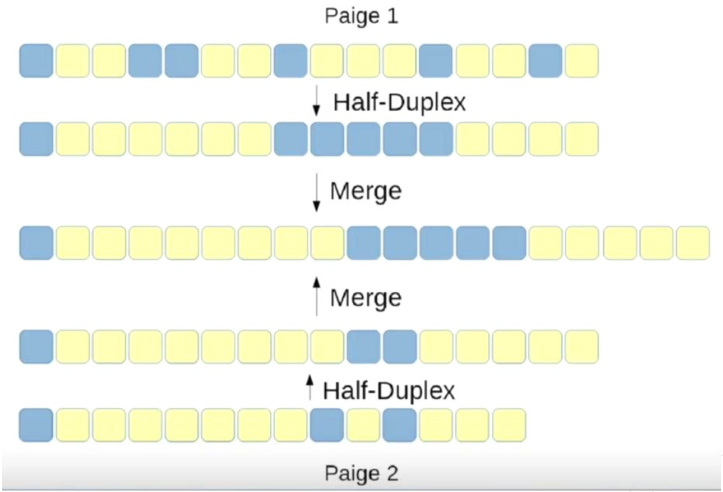
1. Request google.com $-->$
2. $<--$ Finish receiving google.com
3. Browser notices google.com has logo.jpg, icon.png ...
4. Request logo.jpg, icon.png $-->$
5. $<--$ Finish receiving logo.jpg, icon.png

W-T — Half Duplex Communication

1. Request google.com $-- >$
2. $< --$ Finish receiving google.com
3. Browser notices google.com has logo.jpg, icon.png ...
4. Request logo.jpg, icon.png $-- >$
5. $< --$ Finish receiving logo.jpg, icon.png
6. ...


In Full-Duplex (originally):
In Half-Duplex (Walkie-Talkie):
Request Page
Page
Request Resources of Page
Resources of Page

W-T — Burst Molding



W-T — Implementation

- Authors implement half-duplex on top of Tor Browser (Firefox)

W-T — Implementation

- Authors implement half-duplex on top of Tor Browser (Firefox)
- Client and Entry node/proxy together do **burst molding**

W-T — Implementation

- Authors implement half-duplex on top of Tor Browser (Firefox)
- Client and Entry node/proxy together do **burst molding**
- Burst sequences are to be known before hand

What is the Attacker Accuracy? Overhead?

Evaluation — W-T vs Attacks

Attack	Undefended	Defended
Jaccard [15]	0.01	0.01
Naive Bayes [15]	0.49	0.16
MNBayes [13]	0.03	0.02
SVM [23]	0.81	0.44
DLevenshtein [6]	0.94	0.19
OSAD [32]	0.97	0.25
FLevenshtein [32]	0.79	0.24
kNN [31]	0.95	0.28
CUMUL [22]	0.64	0.20
kFP [12]	0.86	0.41

[Walkie Talkie — Wang and Goldberg]

UNIVERSITÄT PADERBORN

Evaluation — W-T vs Deep Fingerprinting

Defenses	Overhead		Accuracy of WF attacks on defended datasets					
	Bandwidth	Latency	SDAE	DF	AWF	*k*-*NN*	CUMUL	*k*-*FP*
BuFLO	246%	137%	9.2%	12.6%	11.7%	10.4%	13.5%	13.1%
Tamaraw	328%	242%	11.8%	11.8%	12.9%	9.7%	16.8%	11.0%
WTF-PAD	64%	0%	36.9%	**90.7%**	60.8%	16.0%	60.3%	69.0%
Walkie-Talkie	31%	34%	23.1%	49.7%	45.8%	20.2%	38.4%	7.0%

DF - Deep Fingerprinting

[Deep Fingerprinting — Sirinam et al.]

UNIVERSITÄT PADERBORN

W-T — Evaluation vs Defenses

Defense	BWOH	TOH	kNN acc.
Adaptive [29]	193%	16%	0.67
Decoy [23]	100%	39%	0.25
BuFLO [8]	145%	180%	0.08
Supersequence [31]	222%	112%	0.05
Tamaraw [5]	103%	140%	0.05
WT (this work)	**31%**	**34%**	**0.28**

BWOH - Bandwidth Overhead, **TOH** - Time Overhead
[Walkie Talkie — Wang and Goldberg]

UNIVERSITÄT PADERBORN

Conclusion

- Website fingerprinting is still an **open problem** for users who are privacy concerned

Conclusion

- Website fingerprinting is still an **open problem** for users who are privacy concerned
- **Walkie-Talkie** is a low overhead solution that can defend against all WF attacks

UNIVERSITÄT PADERBORN

Conclusion

- Website fingerprinting is still an **open problem** for users who are privacy concerned
- **Walkie-Talkie** is a low overhead solution that can defend against all WF attacks
- Still unbroken by recent attacks

Conclusion

- Website fingerprinting is still an **open problem** for users who are privacy concerned
- **Walkie-Talkie** is a low overhead solution that can defend against all WF attacks
- Still unbroken by recent attacks
- Good candidate to be adopted by Tor