Assessing the Feasibility of Machine Learning to Detect Network Covert Channels

Name: Diogo Barradas

PhD Stage: Planner

Advisors: Prof. Luís Rodrigues & Prof. Nuno Santos

Research Area: Privacy-Enhancing Technologies

What's All This About?

- **What's the Problem?**
  - Current unobservability assessments of covert channels are flawed

What's All This About?

- **What's the Problem?**
  - Current unobservability assessments of covert channels are flawed
- **Why Should We Care?**
  - Inaccurate unobservability assessments can place human lives in jeopardy

What's All This About?

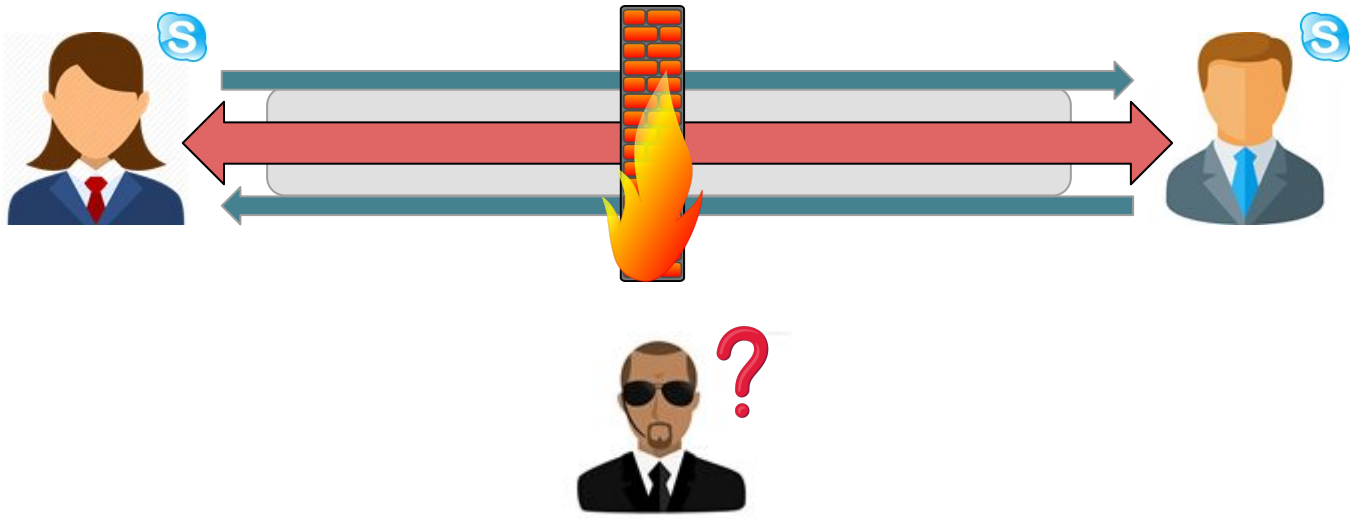
- **What's the Problem?**
  - Current unobservability assessments of covert channels are flawed
- **Why Should We Care?**
  - Inaccurate unobservability assessments can place human lives in jeopardy
- **What Are You Going To Do About It?**
  - Develop a robust framework for the unobservability assessment of covert channels

What's All This About?

- **What's the Problem?**
  - Current unobservability assessments of covert channels are flawed
- **Why Should We Care?**
  - Inaccurate unobservability assessments can place human lives in jeopardy
- **What Are You Going To Do About It?**
  - Develop a robust framework for the unobservability assessment of covert channels
- **Then What?**
  - Foster the design of new tools to circumvent repressive network control

Multiple Tools Generate Covert Channels in the Internet

- Recent approaches tunnel data through encrypted protocols
  - e.g. Skype



Covert Channels through Multimedia Protocol Tunneling

Facet

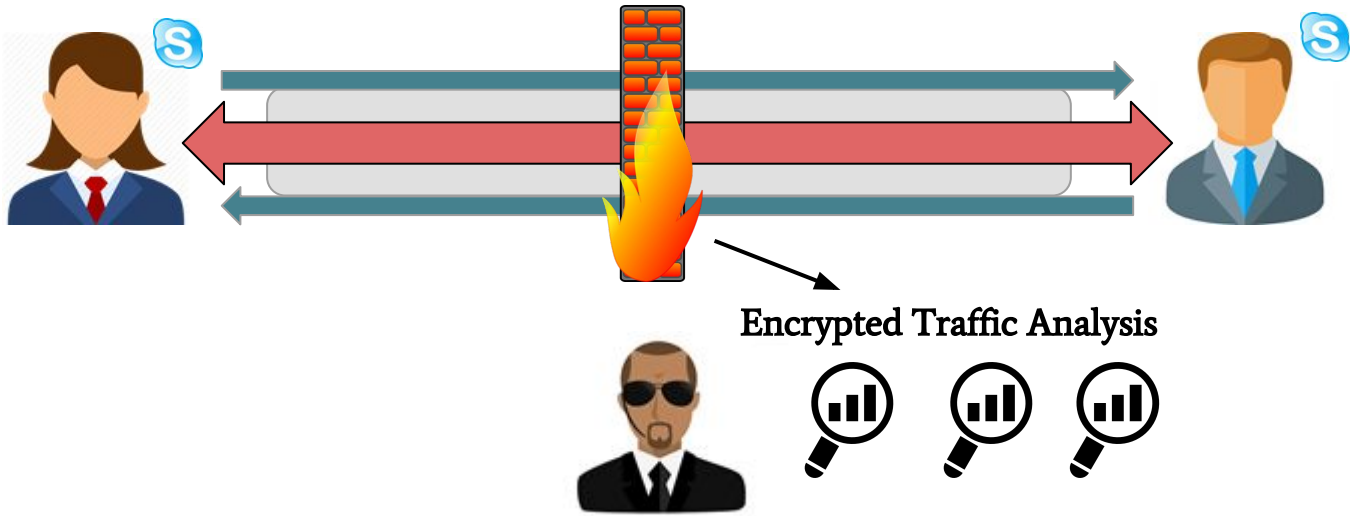
Unidirectional (A/V)
Video Transmission

DeltaShaper

Bidirectional (V)
Arbitrary Data Transmission

Adversaries can Learn from Encrypted Traffic

- Traffic analysis can detect unusual patterns in (**encrypted**) network flows
- Covert data must be carefully modulated to evade detection
  - Security => ***Unobservability***



Existing Unobservability Claims are Questionable

- ***Ad hoc* covert channel evaluation**
  - Similarity-based classifiers only
  - Unobservability measured against independently built classifiers
- **Lack of theoretical reasoning in covert channel design**
  - Covert data embedding is guided through black-box experimentation

Research Questions

- Are state-of-the-art covert channels observable?
- Can we better assess the unobservability of current tools?
- Can we accurately characterize covert data carrier protocols?
- Is it possible to provide theoretical bounds to unobservability?

Research Questions

- Are state-of-the-art covert channels observable?
- Can we better assess the unobservability of current tools?
- Can we accurately characterize covert data carrier protocols?
- Is it possible to provide theoretical bounds to unobservability?

Similarity-Based Detection

- **Unobservability claims are dependent on the classifier**
- **Similarity-based classifiers cannot accurately detect covert traffic**
  - **ROC AUC:**

System / Classifier	Chi-Square	Earth Mover's Distance
Facet	**0.83**	0.58
DeltaShaper	**0.74**	0.57

Similarity-Based Detection

- **Unobservability claims are dependent on the classifier**
- **Similarity-based classifiers cannot accurately detect covert traffic**
  - **ROC AUC:**

System / Classifier	Chi-Square	Earth Mover's Distance
Facet	0.83	0.58
DeltaShaper	0.74	0.57

Decision Tree-Based Detection

- **Largely undermine previous unobservability claims**
  - **Facet:** ROC AUC = **0.99** (vs **0.83**)
  - **DeltaShaper:** ROC AUC = **0.95** (vs **0.74**)

- **Provide us insight on useful features for identifying covert channels**

Takeaways

- Ensuring unobservability is **desirable** for covert channels
- Past unobservability assessments are **flawed**
- Goal: build a **rigorous** framework for the assessment of unobservability

https://web.ist.utl.pt/diogo.barradas

Thank You!