Bringing a GAN to a Knife-fight: Adapting Malware Communication to Avoid Detection

Maria Rigaki, Sebastian Garcia
{maria.rigaki, sebastian.garcia}@fel.cvut.cz
Czech Technical University in Prague, Czech Republic
Stratosphere Lab

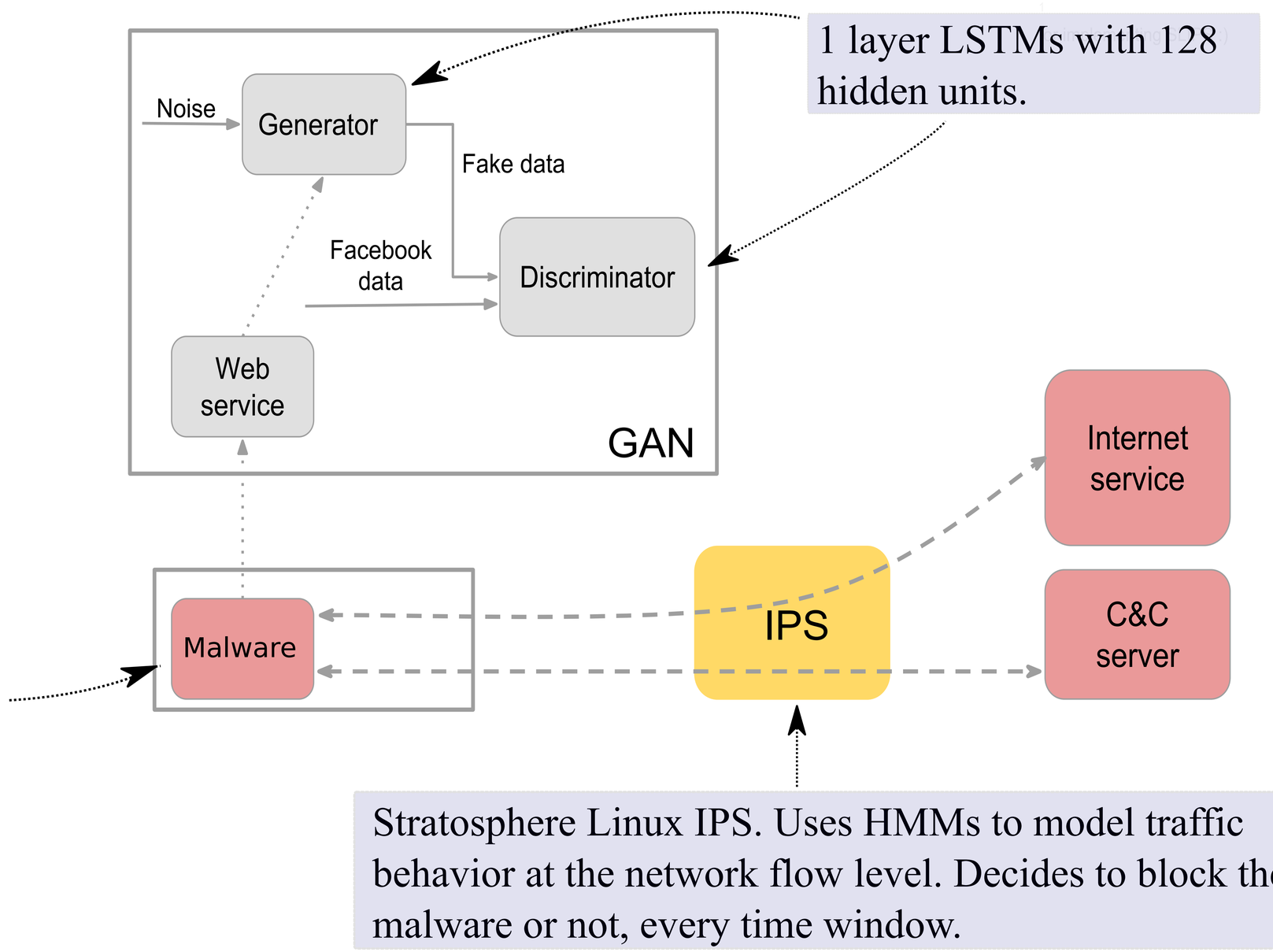
Abstract

- Use GANs to generate network traffic.
- Adapt malware C&C channel to mimic Facebook characteristics and avoid detection.
- Sense blocking actions and use it as feedback to adapt behavior and re-train the GAN.

Experiment Setup

Dataset

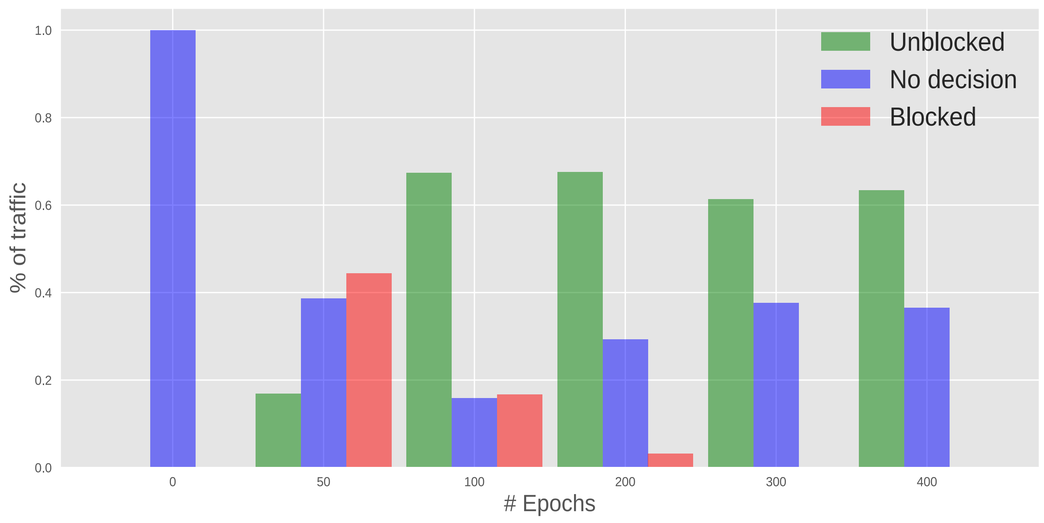
Network captures of two users chatting over Facebook messenger. Extracted features: the **duration** of the network flow, **total number of bytes** in the flow and **inter-flow** time.



Flu, an open source RAT, modified to adapt its network behavior in real time, based on input from the GAN.

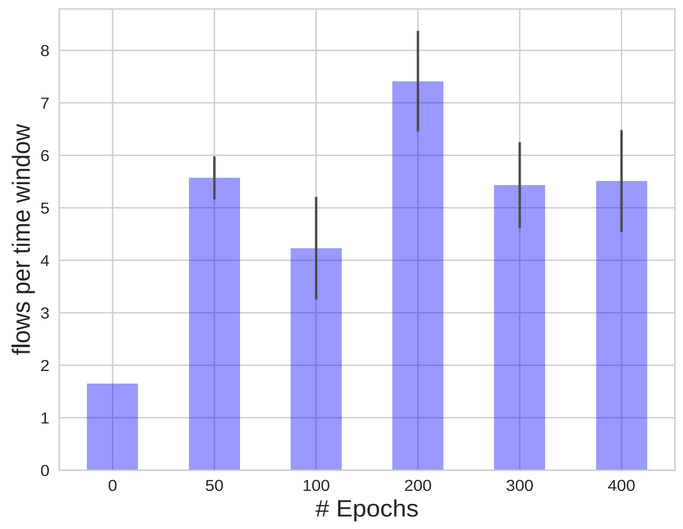
Stratosphere Linux IPS. Uses HMMs to model traffic behavior at the network flow level. Decides to block the malware or not, every time window.

Detection Performance



Detection results for each of the pre-trained models.

Efficiency



> 5 flows per time window!

Number of flows per time window for each pre-trained model.

Conclusions

- It is possible to use GANs for mimicking network traffic characteristics
- Areas of application: censorship circumvention, network traffic generation, red team tools.

Future Work

- Implementation improvements: HTTPS support, combined generator and malware, etc.
- Testing against different types detectors and with different types of traffic profiles.

Acknowledgements

The authors thank Ondrej Lukas for his implementation of the SLIPS system in the Turris Routers. This research was partially supported by the Czech TACR project no. TH02010990.