Identification of malicious Autonomous systems

Dominik Vít

Faculty of Nuclear Sciences and Physical Engineering
CTu Prague

June 18, 2018

Table of contents

Autonomous systems

- a collection of IP prefixes under the control of single administrative entity
- currently around 60 000 ASes
- a unique number assigned to each AS
  - AS 2852 CESNET2
- BGP= Border Gateway Protocol

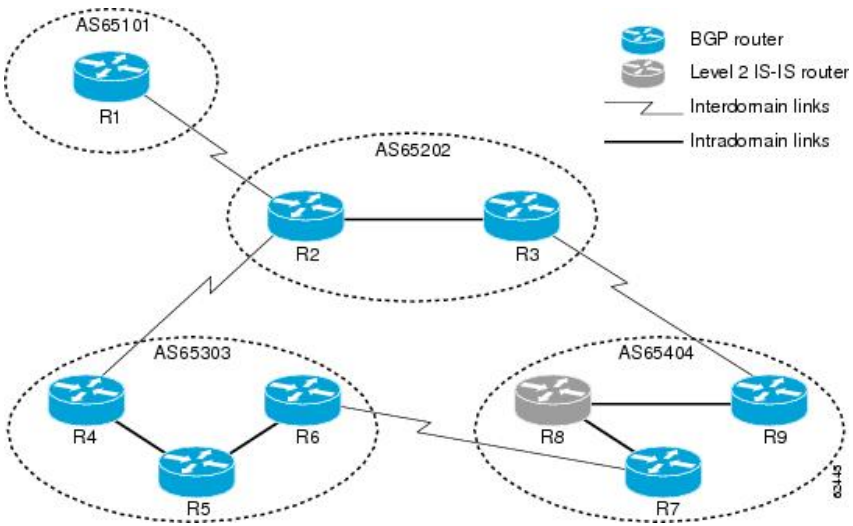

Figure: Diagram of ASes and BGP routers

Dataset

AS number	*company*	*flow*	*users*	*domains*	*upload*	*download*	*m. flow*	*m. upload*	*m. download*
AS15169 Google	333	3,7e9	2.3e6	5.2e6	1.5e13	1.9e14	5.2e3	2.5e6	3.2e7
AS30633 Leaseweb	320	1.5e7	5.3e5	4.3e4	1.8e10	2.4e11	5.3e4	5.4e7	1.5e6
AS60592 GRANSY	97	9.9e3	3.9e2	5.7e2	1e7	6.6e7	3.1e3	1.9e3	5.6e3

Time evolution

Why are we interested in evolution of ASes in time?

- Can they be considered static?
- If so, can we train a set of detectors on the training data?
- If they prove to be dynamic, can we determine how?

Measured traffic

Evolution of probability of malicious flows in the course of 10 months

- Significant fluctuation
- Often between zero and nonzero for a single AS
- 3 statistics:
  - Number of ASes with nonzero probability of malicious flows
  - Born rate - ASes that changed the probability from zero to nonzero
  - Churn rate - AS that fell to a zero probability in a given month

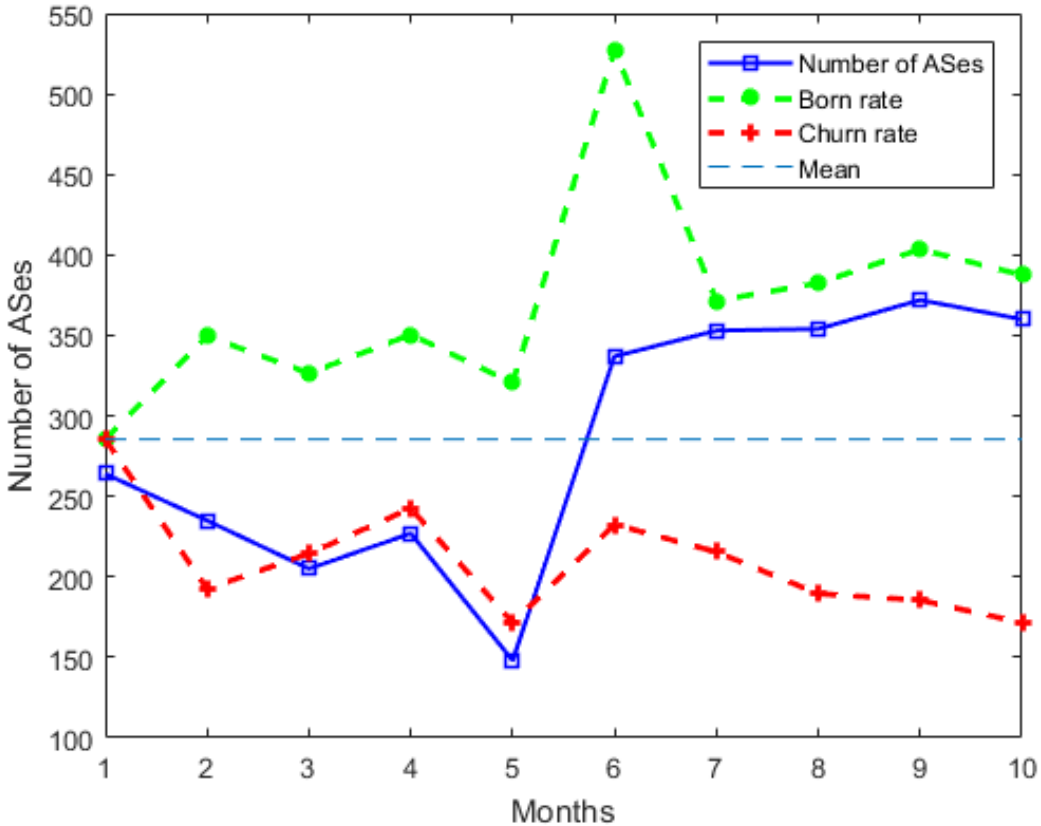

Figure: Evolution of the probability of malicious flows within 10 months

Markov chain

Is it possible to predict the state of an AS given the knowledge of a state in a previous time step?
Markov property:

$$Pr(s_{t+1}|s_t, s_{t-1}, \ldots, s_0) = Pr(s_{t+1}|s_t)$$

- Continuous state space
- Discretization by the order of magnitude
- Calculating the transition matrix
- Monte Carlo method simulations

Transition matrix

- Discretization of states
- Ratio of ASes passing from the state $S_{i,j}$ to $S_{k,l}$ and the total AS count
- Exploits the fact, that there is a large amount of data in a single month, but only a few observed months

	0	1e-08	1e-07	1e-06	1e-05	0.0001	0.001	0.01	0.1	1
0	0.49761	0.014354	0.057416	0.1244	0.11005	0.066986	0.052632	0.047847	0.028708	0
1e-08	0.33333	0.16667	0.16667	0.16667	0	0.16667	0	0	0	0
1e-07	0.42553	0.06383	0.21277	0.19149	0.10638	0	0	0	0	0
1e-06	0.36264	0	0.12088	0.2967	0.18681	0.032967	0	0	0	0
1e-05	0.38462	0	0.021978	0.16484	0.32967	0.076923	0.021978	0	0	0
0.0001	0.37662	0	0.025974	0.051948	0.1039	0.35065	0.090909	0	0	0
0.001	0.32203	0	0	0	0	0.18644	0.38983	0.10169	0	0
0.01	0.36364	0	0	0	0.030303	0	0.18182	0.27273	0.15152	0
0.1	0.44444	0	0	0	0	0	0	0.18519	0.37037	0
1	0.66667	0	0	0	0	0	0	0	0	0.33333

Table: Transition matrix

Training dataset

- Extending the training data from 3 to 9 months
- Validation on testing dataset using methods of Monte Carlo
- 1e5 of repetitions is sufficient as higher orders only improve accuracy incrementally
- Tolerance of $\pm$ 1 order
- Excluding ASes that probably were abuses (only 1 month of measured malicious traffic)

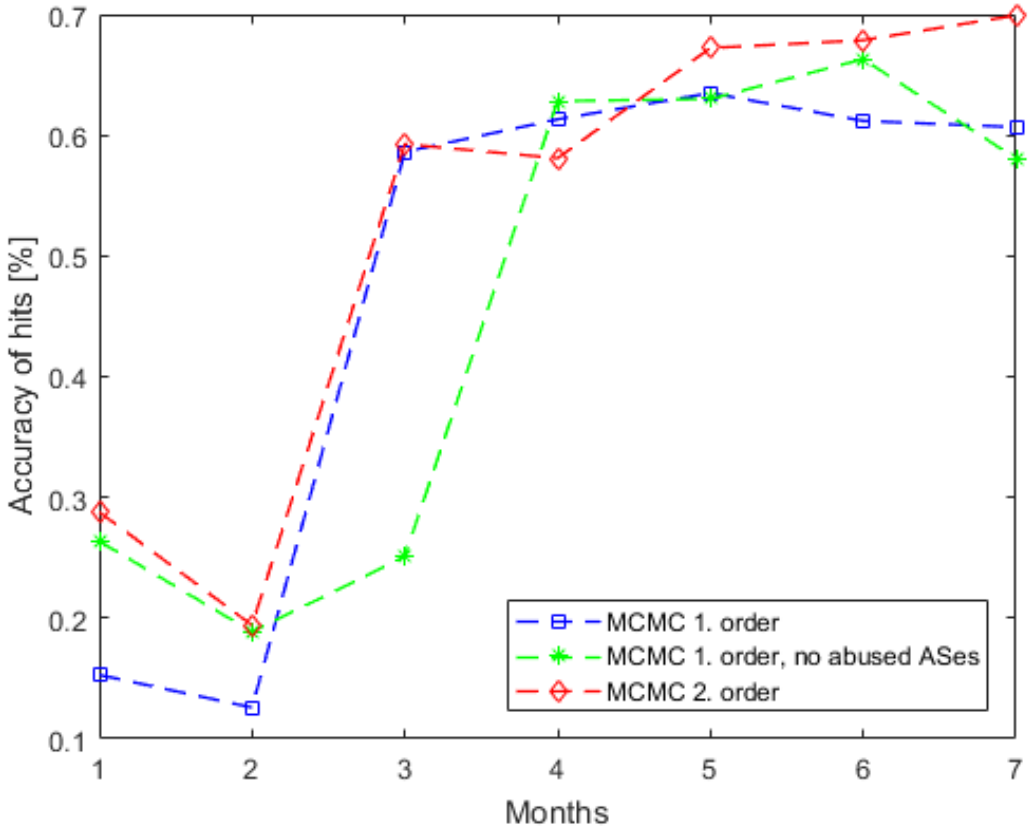

Figure: Prediction accuracy

MC of higher orders

Markov chain of 2. order follows the property:

$$Pr(s_{t+1}|s_t, s_{t-1}, \ldots, s_0) = Pr(s_{t+1}|s_t, s_{t-1}).$$

We predict the future state based on the knowledge of 2 previous states. Transition matrix expands from $10x10$ to $100x10$.

MCMC conclusion

- Exploiting Markov chains partially describes AS behavior.
- They are not accurate enough to be used as standalone detectors.
- We cannot prove stationarity of ASes states, but we can see a raise in robustness of detectors with larger dataset.

Characteristics of training data

Detectors

- For future application in malware connection detection
- Assign each AS an anomaly score
- In real time traffic the connection will be flagged as malicious based on the ASes it visited.

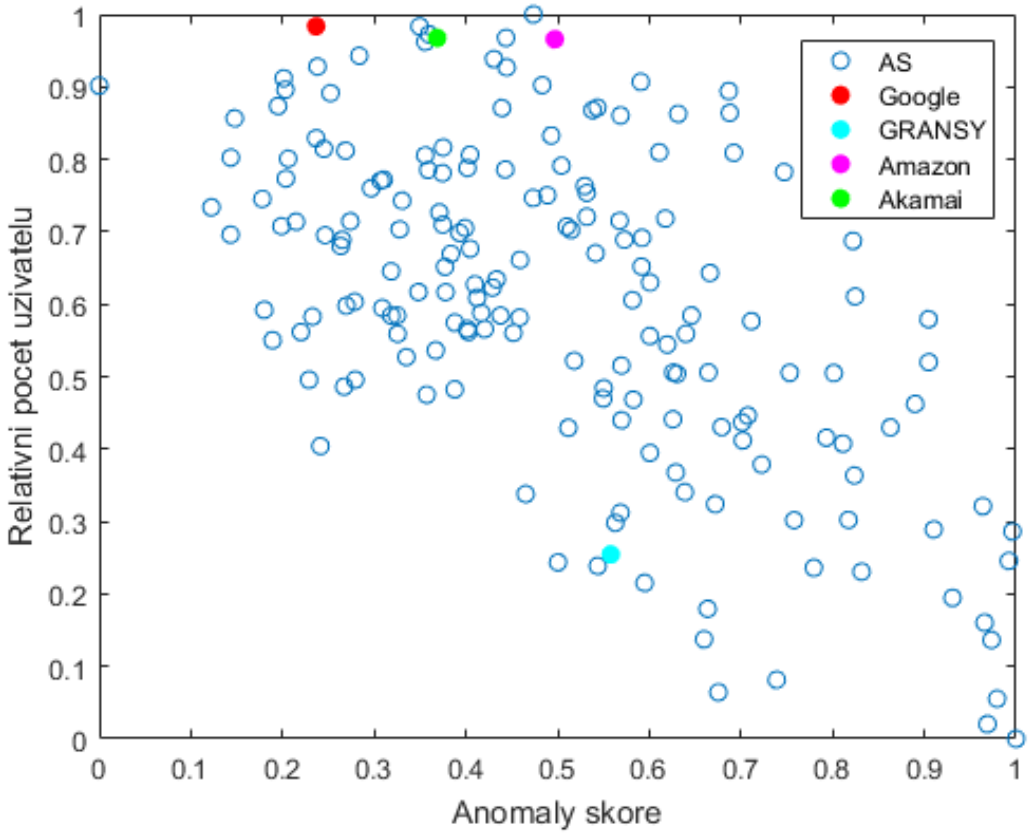

Figure: Relation of users and anomaly score

Elementary detectors

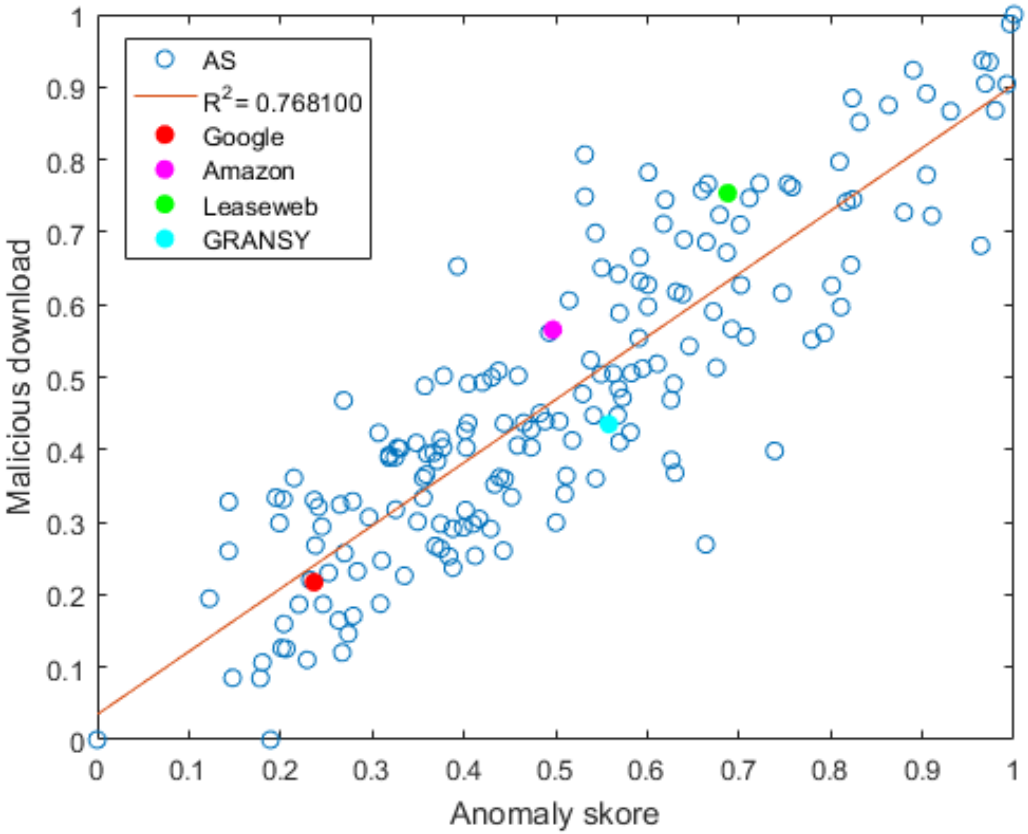

Figure: Relation of relative download and anomaly score

Evaluating elementary detectors

ROC... Receiver Operating Characteristic

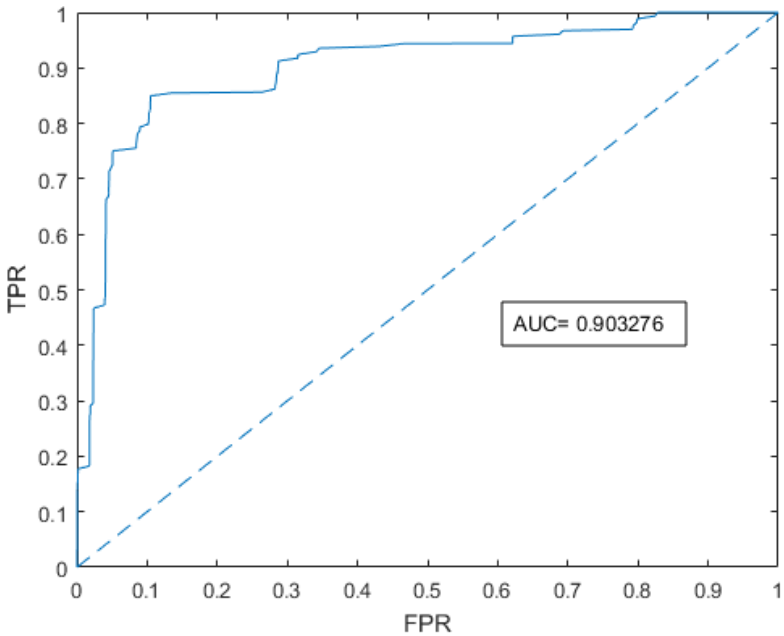

Figure: ROC for domains

AUC for each detector:

- companies AUC=0.88
- users AUC=0.90
- dommains AUC=0.90
- upload AUC=0.98
- download AUC=0.96

Agregated detectors

AUC for agregated detectors:

- average AUC=0.934
- Evangelista functionAUC=0.939
- weighted average AUC=0.945

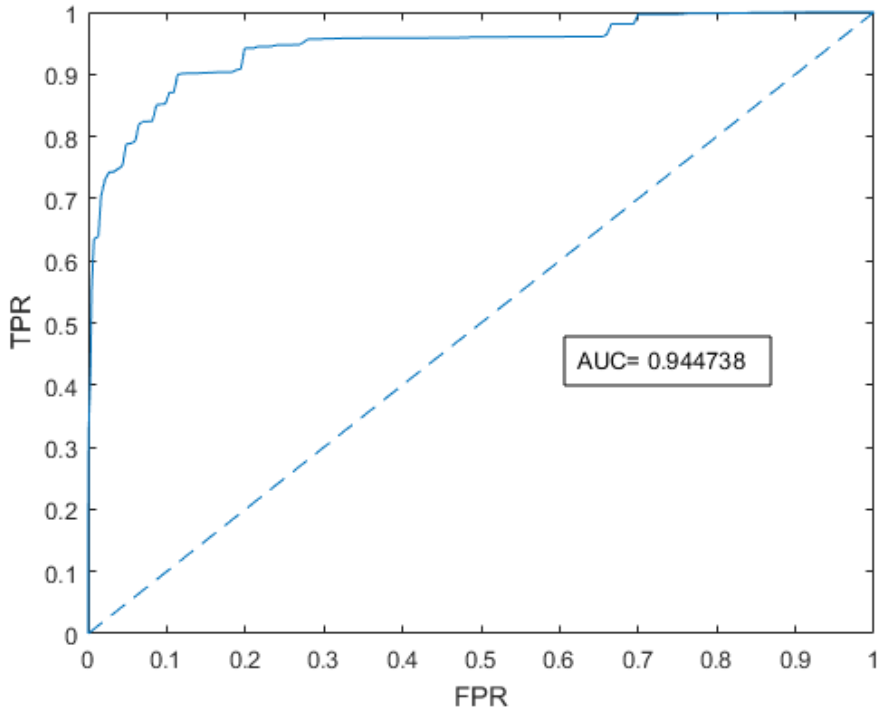

Figure: ROC for weighted average

Conclusion

- Using AS reputation has a positive effect on malware detection
- Due to the small dataset we cannot prove time stationarity of ASes
- Markov chains help understand their time evolution
- Detectors still exhibit high false positive rate

References

1. Antonakakis, Manos, et al. "Building a Dynamic Reputation System for DNS." USENIX security symposium. 2010.
2. PETERKA, Jiří. Přednáška na MFF UK: Počítačové sítě [online]. [cit. 2017-04-12]. Dostupné z: http://www.earchiv.cz/l226/index.php3
3. Receiver operating characteristic. In: Wikipedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2017-04-12]. Dostupné z: https://en.wikipedia.org/wiki/Receiver-operating-characteristic
4. Giorgio Giacinto and Fabio Roli. Intrusion detection in computer networks by multiple classifier systems. in *In Proc. of the 16th International Conference on Pattern Recognition (ICPR), Volume 2*, Pages 390-393. IEEE press, 2002.