

Enhancing Network Security: Host Trustworthiness Estimation



Tomáš Jirsík, Pavel Čeleda

`{jirsik|celeda}@ics.muni.cz`

Institute of Computer Science, Masaryk University

■ Goal

25,739%

■ Goal

114,3

25,739%

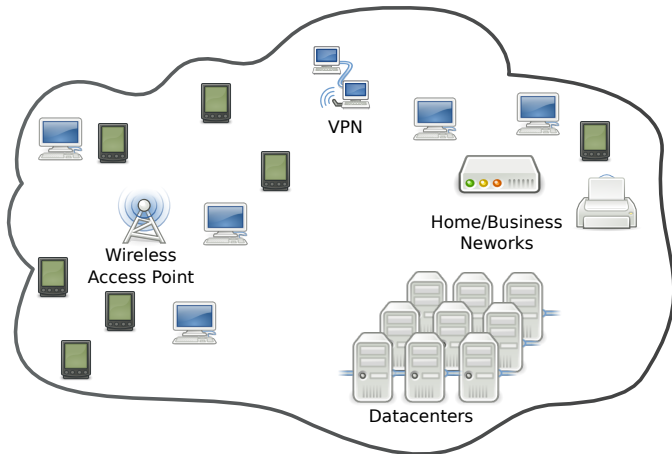
■ Goal

114,3

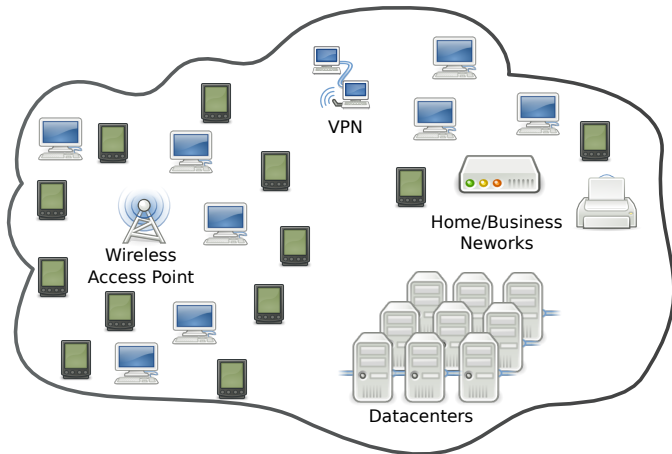
25,739%

33,4

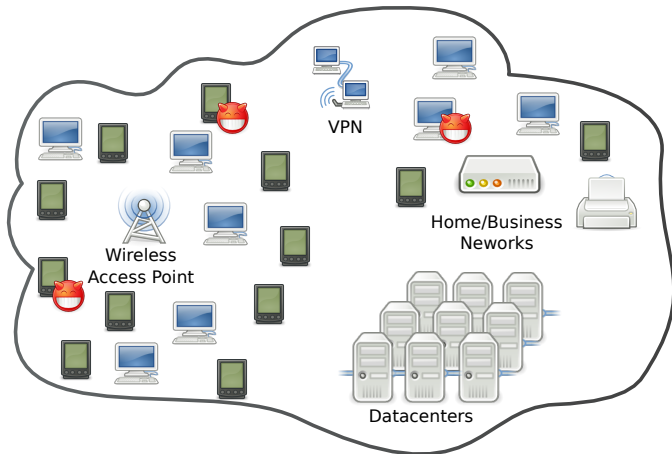
■ Why?



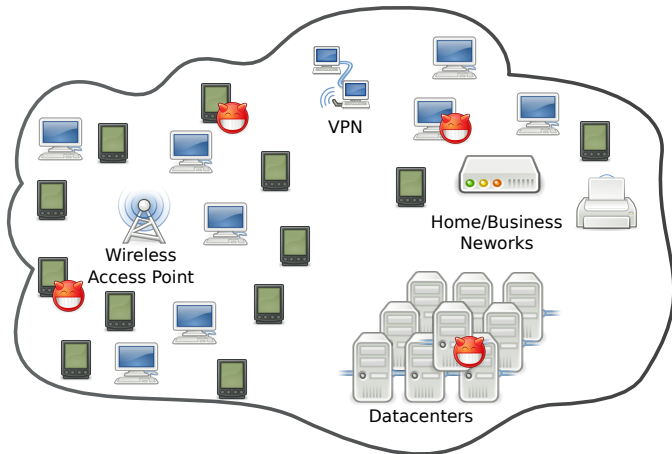
■ Why?



■ Why?

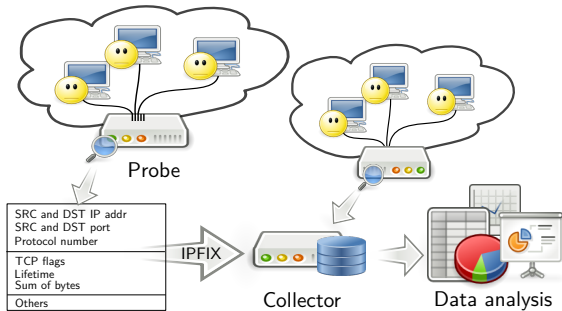


■ Why?



■ Data collection

- Target Customer
- DPI vs. Flow monitoring



Flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Packets	Bytes
09:41:21.763	0.101	TCP	172.16.96.48:15094	-> 209.85.135.147:80	.AP.SF	4	715
09:41:21.893	0.031	TCP	209.85.135.147:80	-> 172.16.96.48:15094	.AP.SF	4	1594

■ Steps to reach the goal

Goal: *estimate a host trustworthiness based only on flow information*

1. Develop tools for data storing and handling

■ Steps to reach the goal

Goal: *estimate a host trustworthiness based only on flow information*

1. Develop tools for data storing and handling
2. Host identification

■ Steps to reach the goal

Goal: *estimate a host trustworthiness based only on flow information*

1. Develop tools for data storing and handling
2. Host identification
 - **RQ1:** *Is it possible to unambiguously identify a host employing only flow information?*

■ Steps to reach the goal

Goal: *estimate a host trustworthiness based only on flow information*

1. Develop tools for data storing and handling
2. Host identification
 - *RQ1: Is it possible to unambiguously identify a host employing only flow information?*
3. Trustworthiness estimation

■ Steps to reach the goal

Goal: *estimate a host trustworthiness based only on flow information*

1. Develop tools for data storing and handling
2. Host identification
 - RQ1: *Is it possible to unambiguously identify a host employing only flow information?*
3. Trustworthiness estimation
 - RQ2 a): *How can the trustworthiness of a host be estimated?*

■ Steps to reach the goal

Goal: *estimate a host trustworthiness based only on flow information*

1. Develop tools for data storing and handling
2. Host identification
 - RQ1: *Is it possible to unambiguously identify a host employing only flow information?*
3. Trustworthiness estimation
 - RQ2 a): *How can the trustworthiness of a host be estimated?*
 - RQ2 b): *What features should be used for the estimation?*

■ Steps to reach the goal

Goal: *estimate a host trustworthiness based only on flow information*

1. Develop tools for data storing and handling
2. Host identification
 - RQ1: *Is it possible to unambiguously identify a host employing only flow information?*
3. Trustworthiness estimation
 - RQ2 a): *How can the trustworthiness of a host be estimated?*
 - RQ2 b): *What features should be used for the estimation?*
4. Models evaluation

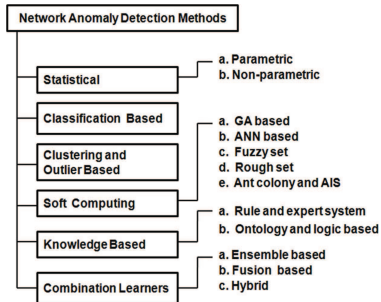
■ Steps to reach the goal

Goal: *estimate a host trustworthiness based only on flow information*

1. Develop tools for data storing and handling
2. Host identification
 - RQ1: *Is it possible to unambiguously identify a host employing only flow information?*
3. Trustworthiness estimation
 - RQ2 a): *How can the trustworthiness of a host be estimated?*
 - RQ2 b): *What features should be used for the estimation?*
4. Models evaluation
 - RQ3: *What methodology should be used to evaluate proposed models for host trustworthiness estimation?*

■ State-of-the-art

- Intrusion detection systems
- Anomaly/Misuse detection methods



- Host based intrusion detection using DPI - ADMIT

■ Proposed Approach

RQ1 - host identification

- host classification research, host specific features, next generation flows

RQ2 - trustworthiness estimation

- trustworthiness concept definition
- inspired by credit scoring
- scoring flow features, flow events

RQ3 - estimated model evaluation

- honeypots, KYPO - Cyber Exercise & Research Platform

■ Current State

Work done

- Getting familiar with research area
- Research problem and questionsa definition
- Flow extension - IPv6 tunnels, HTTP, DNS
- Host specific features - OS detection

Work in progress

- Host database implementation
- Formalization of flow and trustworthiness concept


■ Summary

114,3

25,739%

33,4

Thank you for your attention!

A decorative graphic at the bottom of the slide consists of several wavy, overlapping lines in shades of blue, grey, and red. Three small blue dots are connected by thin lines to the top of the wavy lines, resembling a stylized network or signal path.

Tomáš Jirsík, Pavel Čeleda
{jirsik|celeda}@ics.muni.cz