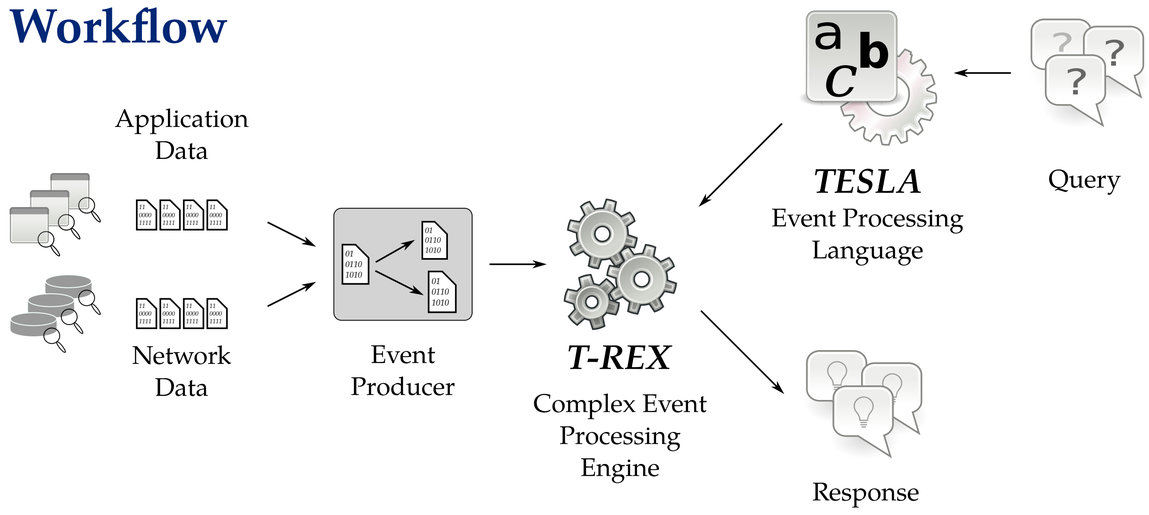
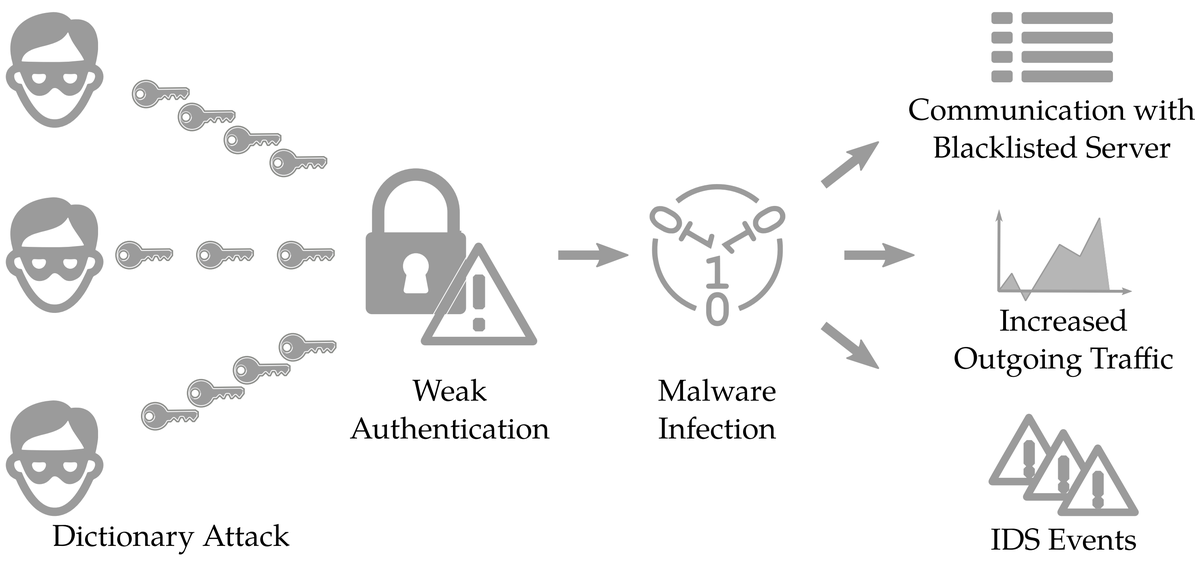
Abstract - *IT operation analytics (ITOA) is used for discovering complex patterns in data from IT systems. The analytics process still includes a significant portion of human interaction which makes the analysis costly and error-prone. Human operators need to formulate queries over the collected data to identify the complex patterns. The queries are usually multilevel, perplexing, and complicated to create. We demonstrate an application of the complex event processing principles in the ITOA domain. We adjust T-Rex complex event processing engine and modify TESLA event processing language to suit for ITOA tasks.*

Workflow



Use-case 1: Malware Infection

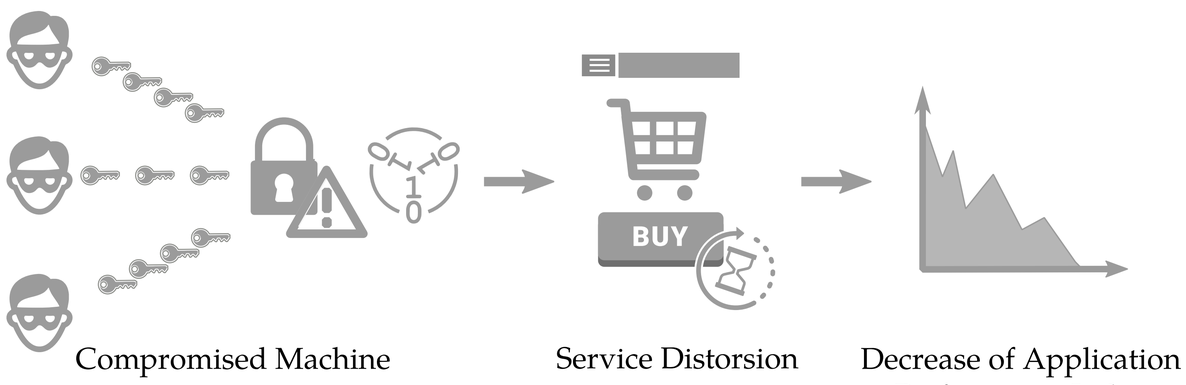


Define CompromisedMachine(ip: inet)

From DictionaryAttack(dst_ip => $target, dst_ip =~ "10.1.0.0/16")
and last 10 OutTrafficInc(src_ip = $target) within 7 day
from DictionaryAttack
and last 10 Blacklist(src_ip = $target) within 7 day
from DictionaryAttack and
each IDSEvent(src_ip = $target) within 7 day
from DictionaryAttack

Where ip := $target;

Use-case 2: Service Disruption

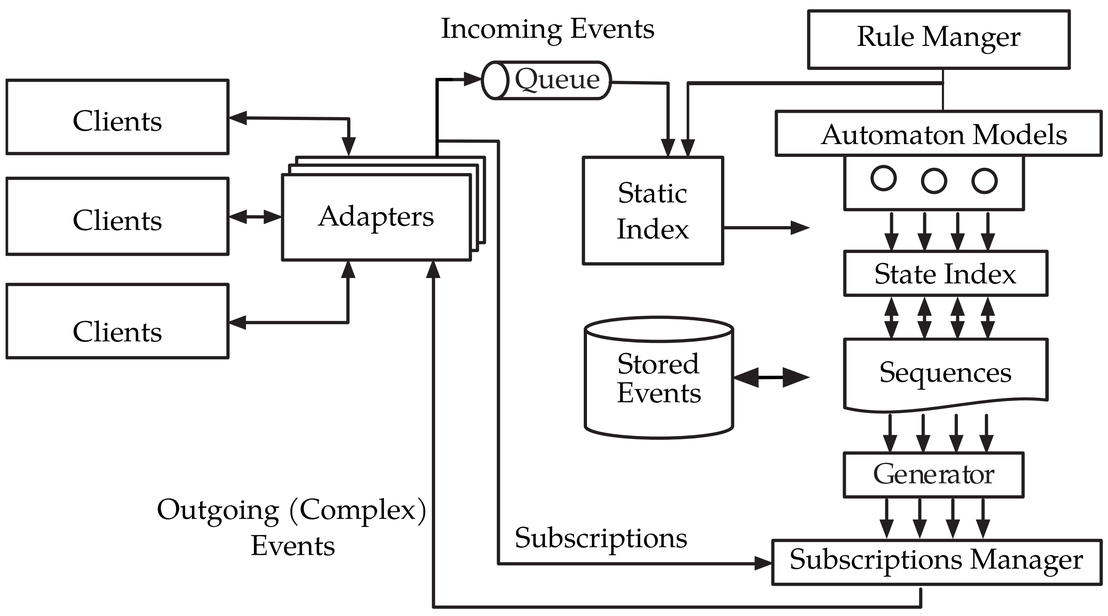


Define MalwareServiceDisruption(ip: inet, source: inet)

From APMIndexDecrease(ip => $target) and
CompromisedMachine($target in [OutTrafficInc.dst_ips,
IDSEvent.dst_ips])

Where ip := $target,
source := CompromisedMachine.ip;

T-REX Complex Event Processing Engine



TESLA Event Processing Language Additions

- Support for user defined types and operations
- Support for array operations
- Transformation of events to user-readable text
- Root-cause analysis and providing of audit trail
- Management of complex event definitions
- Verification of complex event definitions

https://csirt.muni.cz/ @csirtmu

This research was supported by the Technology Agency of the Czech Republic under No. TH02010185 "Research and Development of Advanced Analytics Tools for Security and Performance Analysis of Network Infrastructure, Applications and Services".

CSIRT-MU