Alert-driven Attack Graph Generation using S-PDFA

Azqa Nadeem

PhD candidate

Cyber Analytics Lab

Cyber Analytics Lab

TU Delft

19 January 2021

CyberVSR

RIT

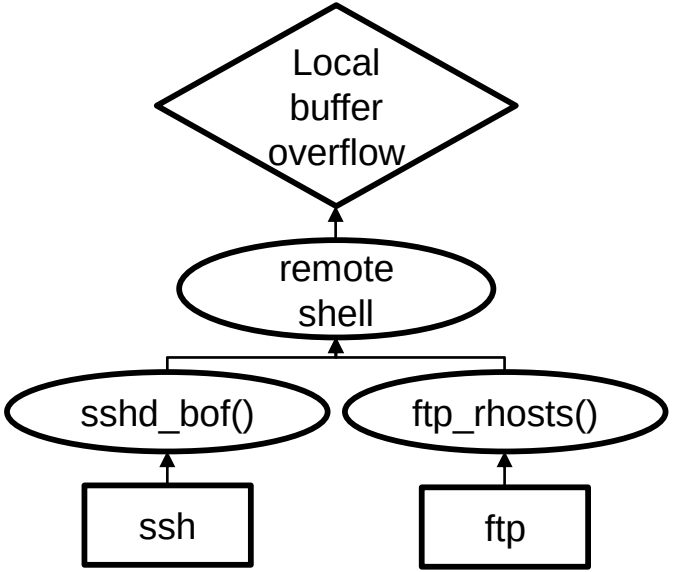
Motivation

- Security analysts handle > 1M intrusion alerts/day*

- Alert correlation groups related alerts
  - But how did the attack happen?

- Attack graphs for strategy depiction
  - Expert knowledge + known vulnerabilities
  - *… from intrusion alerts?*

    + Realistic attack graphs
    + Find paths missed by typical AGs

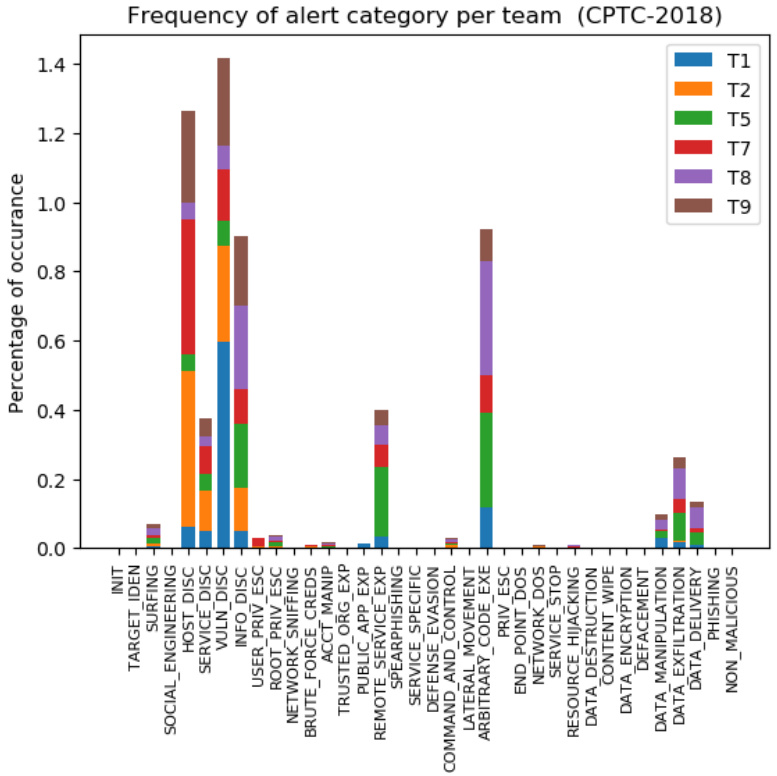


TU Delft

* https://www.imperva.com/blog/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/
https://www.researchgate.net/publication/220202986_Measuring_Security_Risk_of_Networks_Using_Attack_Graphs

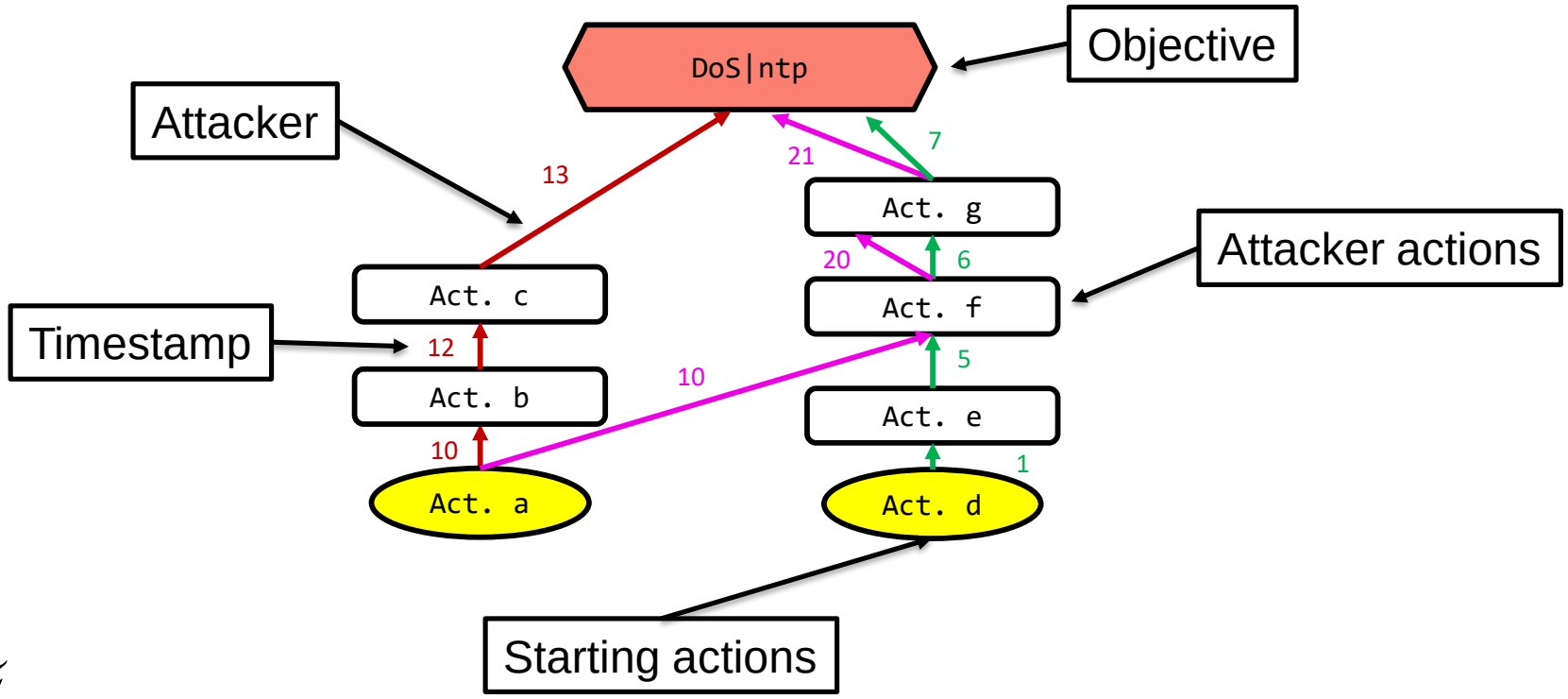
Threat model and Dataset

- Dataset: Penetration testing competition[1]
- Distributed multi-stage attacks
  - Various attackers
  - Various victims
  - Various attack stages
- Moskal's Attack-Intent framework[2]
  - Alert signature → Attack stage



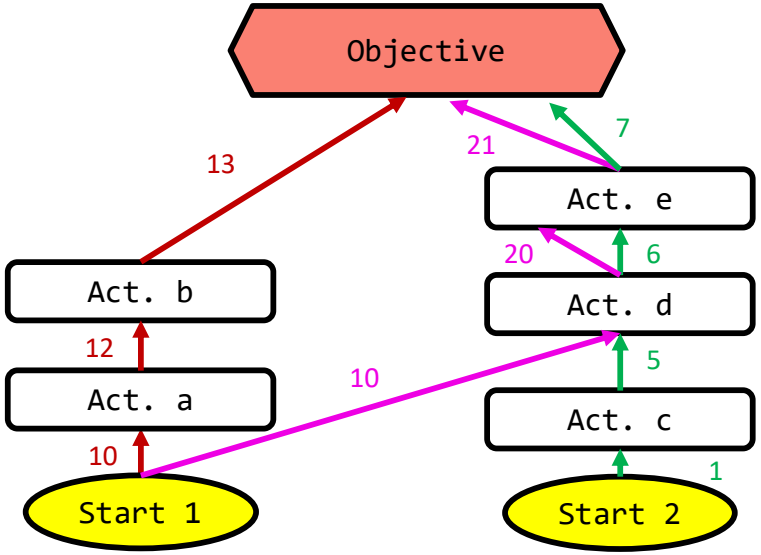
1. *CPTC dataset: https://www.nationalcptc.org/*
2. *S. Moskal and S. J. Yang, "Framework to describe intentions of a cyber attack action," arXiv preprint arXiv:2002.07838, 2020.*

Anatomy of an Alert-driven Attack Graph

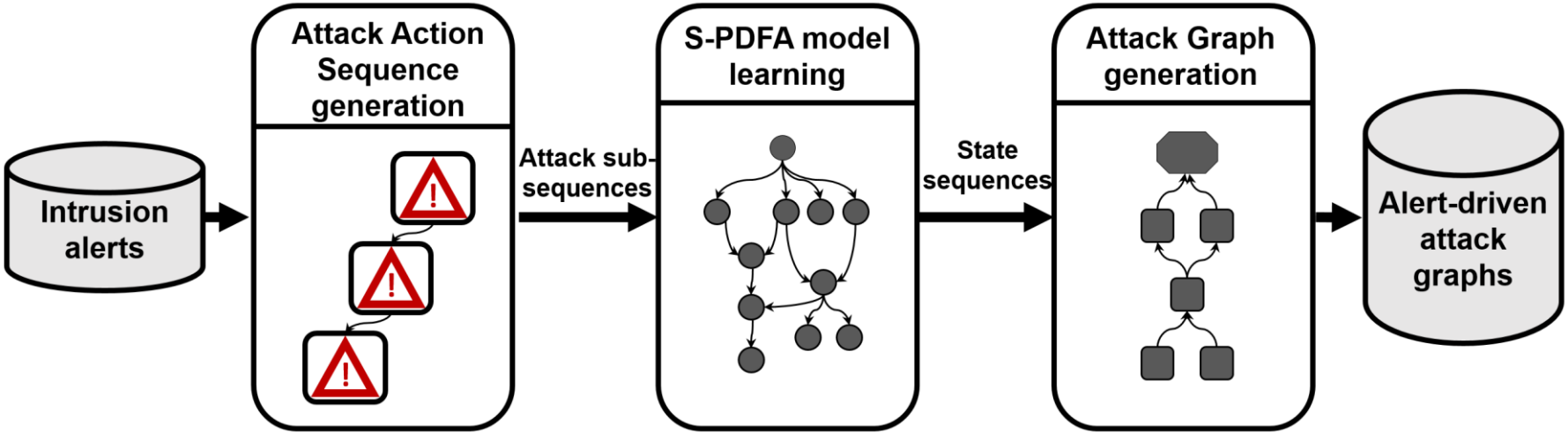


Anatomy of an Alert-driven Attack Graph

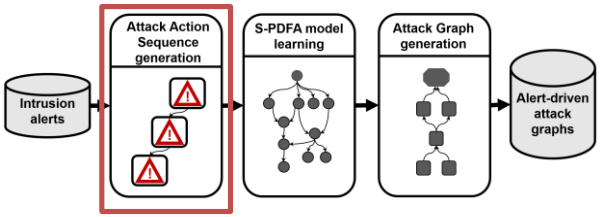
- But first… Challenges
  1. Alert type imbalance
  2. Alert → Action mapping
  3. Context of actions
  4. Comparing strategies



Methodology



Alerts → Actions




```
{   '_sourcetype': 'suricata:alert',
    'alert': {   'category': 'Attempted Information Leak',
                 'severity': 2,
                 'signature': 'ET POLICY Python-urllib\\/ '
                              'Suspicious User Agent'},
    'dest_ip': '169.254.169.254',
    'dest_port': 80,
    'src_ip': '10.0.0.20',
    'src_port': 56952,
    'timestamp': '2018-11-03T13:51:58.205548+0000'}}
```

IDS alerts

Alert Sequences

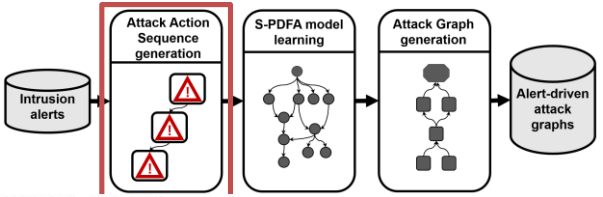
A ↔ X 

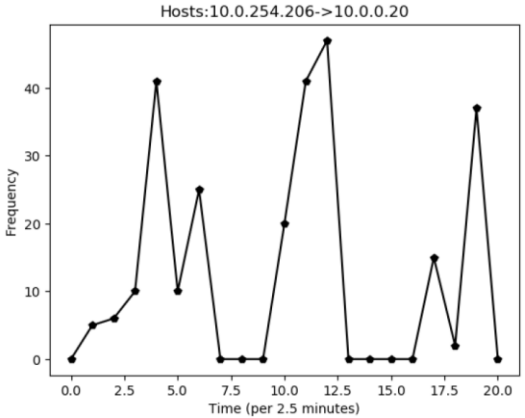
A ↔ Z 

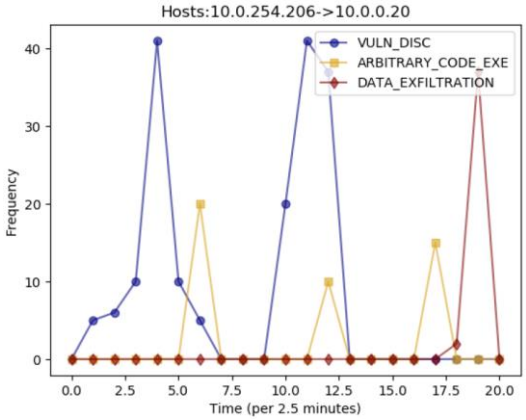
B ↔ X 

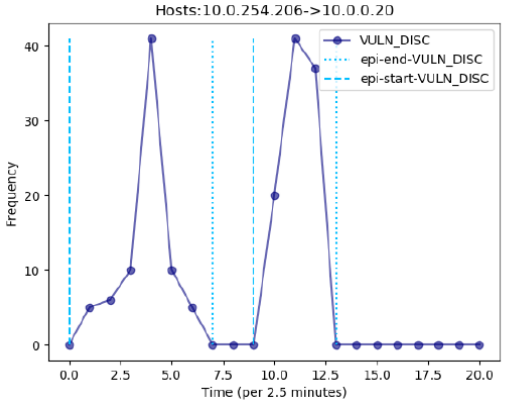
Alert-driven attack graphs using S-PDFA. Azqa Nadeem, Sicco Verwer, Stephen Moskal, Shanchieh Jay Yang. In IEEE Transactions on Dependable and Secure Computing, 2021. (Submitted)

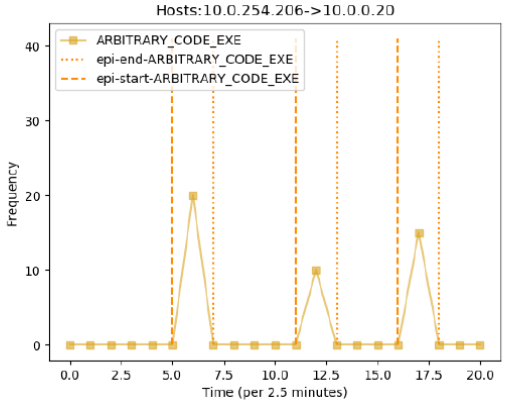
Action extraction

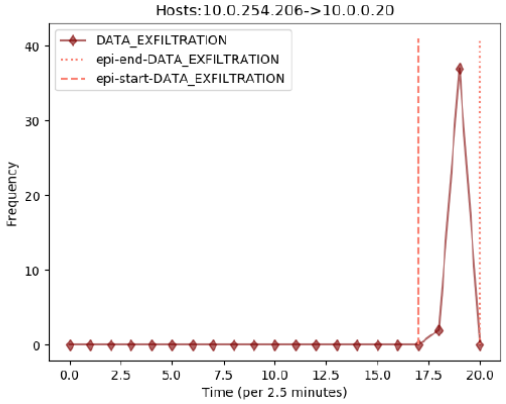




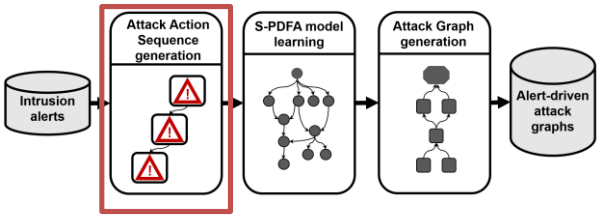








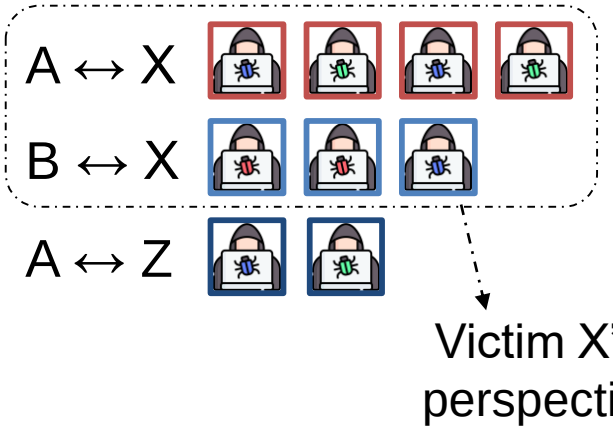
Action sequences



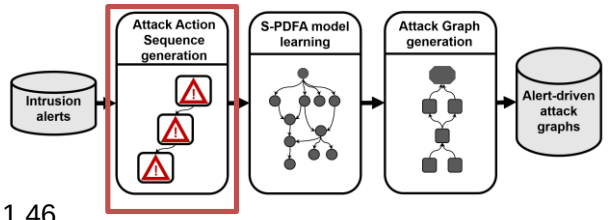
- $Action = \left\langle \begin{matrix} start\ time, \\ end\ time, \\ attack\ stage, \\ targeted\ service \end{matrix} \right\rangle$

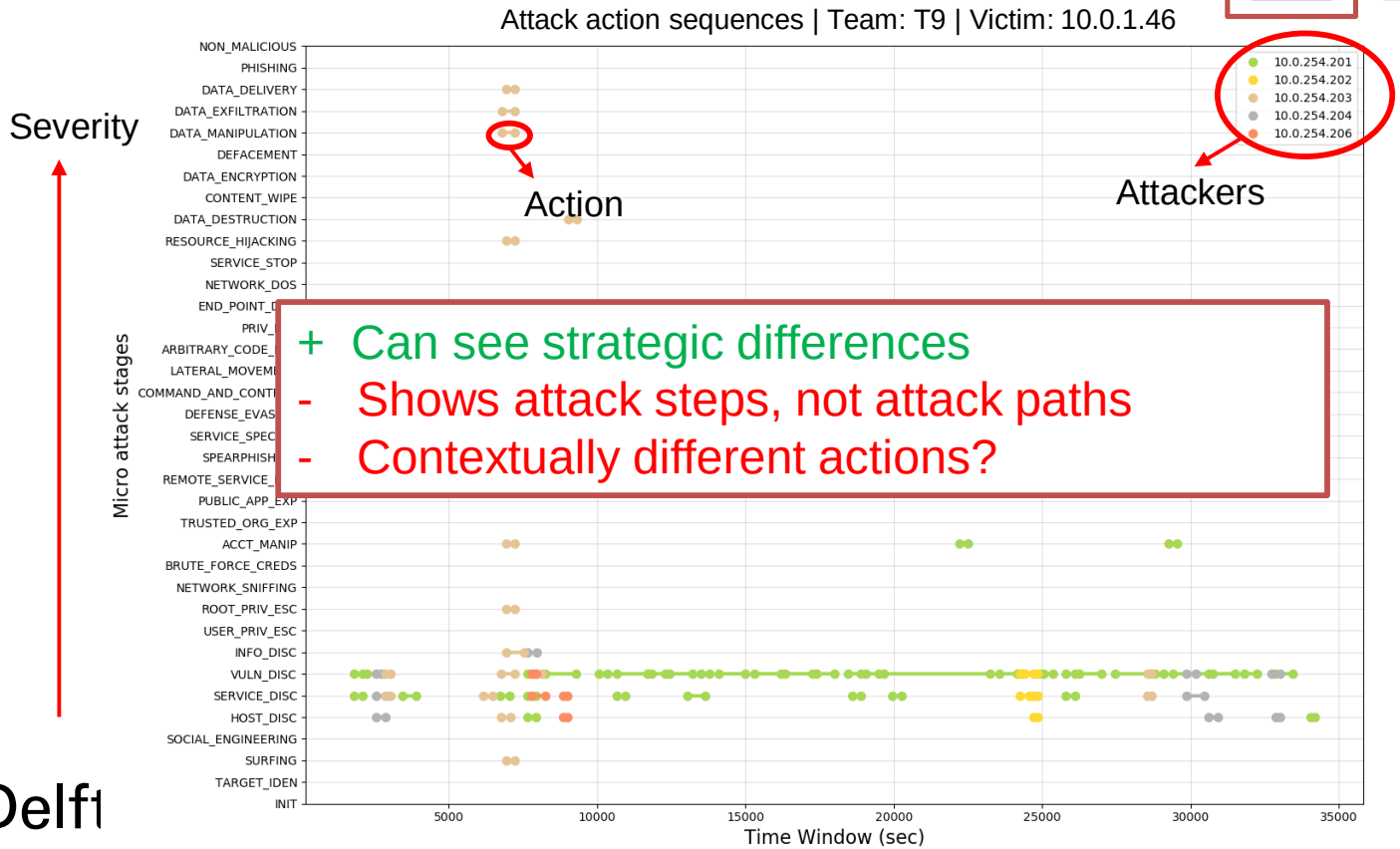
sorted by *start time*

Action Sequences



Action sequences (Vic view)



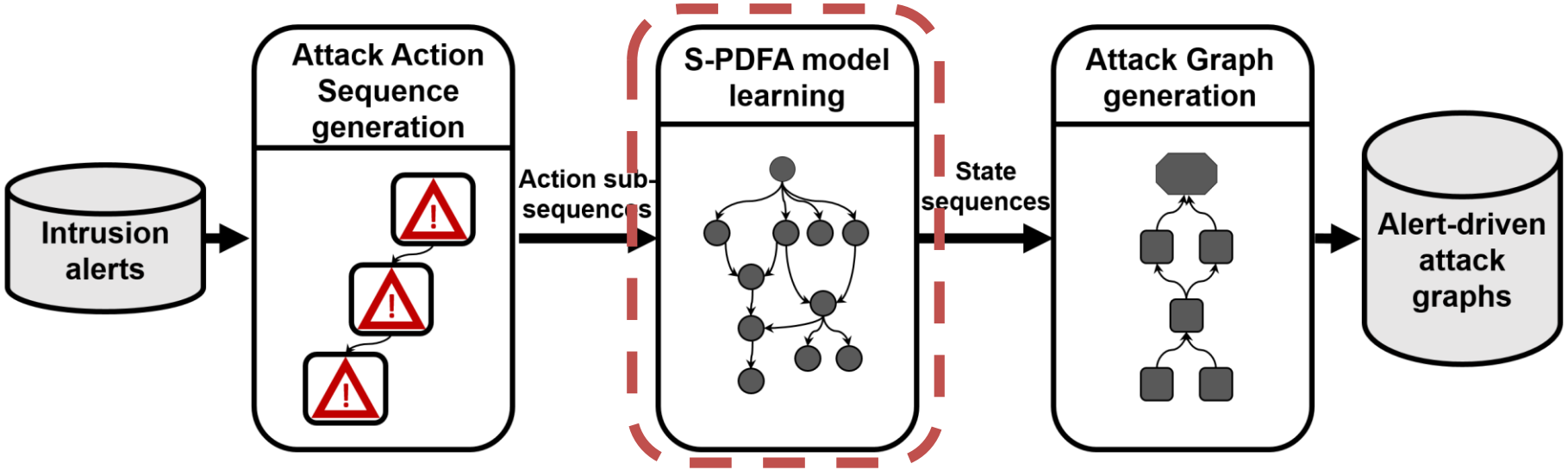


\+ Can see strategic differences

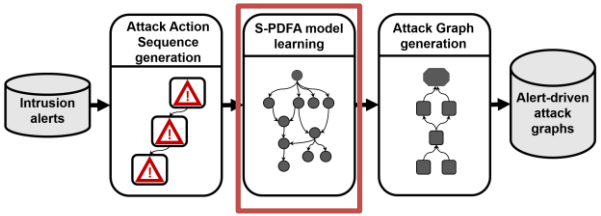
\- Shows attack steps, not attack paths

\- Contextually different actions?

Methodology



Break into sub-sequences

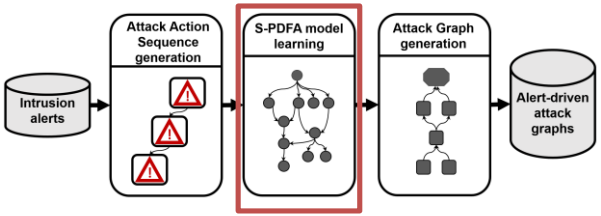


Action sequence: $attacker_i \rightarrow victim_j$

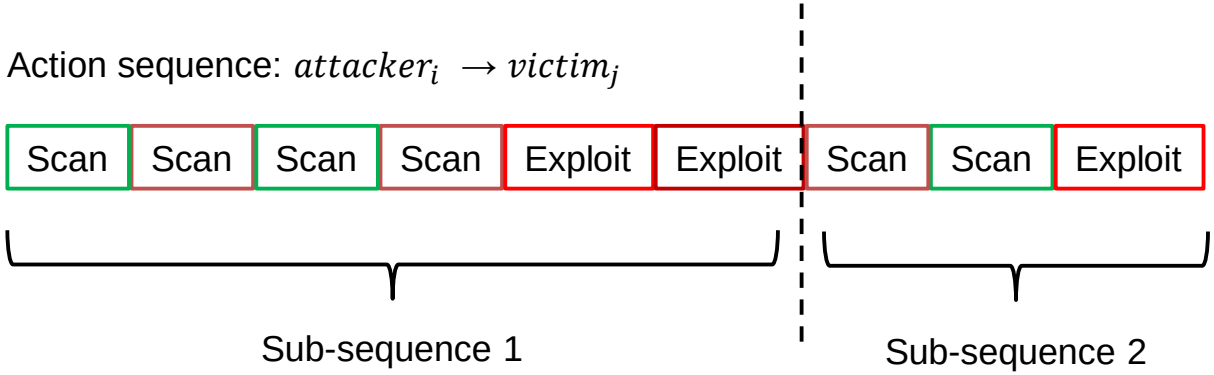
Scan	Scan	Scan	Scan	Exploit	Exploit	Scan	Scan	Exploit

TU Delft

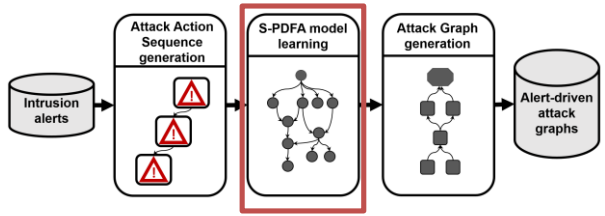
Break into sub-sequences



Action sequence: $attacker_i \rightarrow victim_j$



Suffix Tree



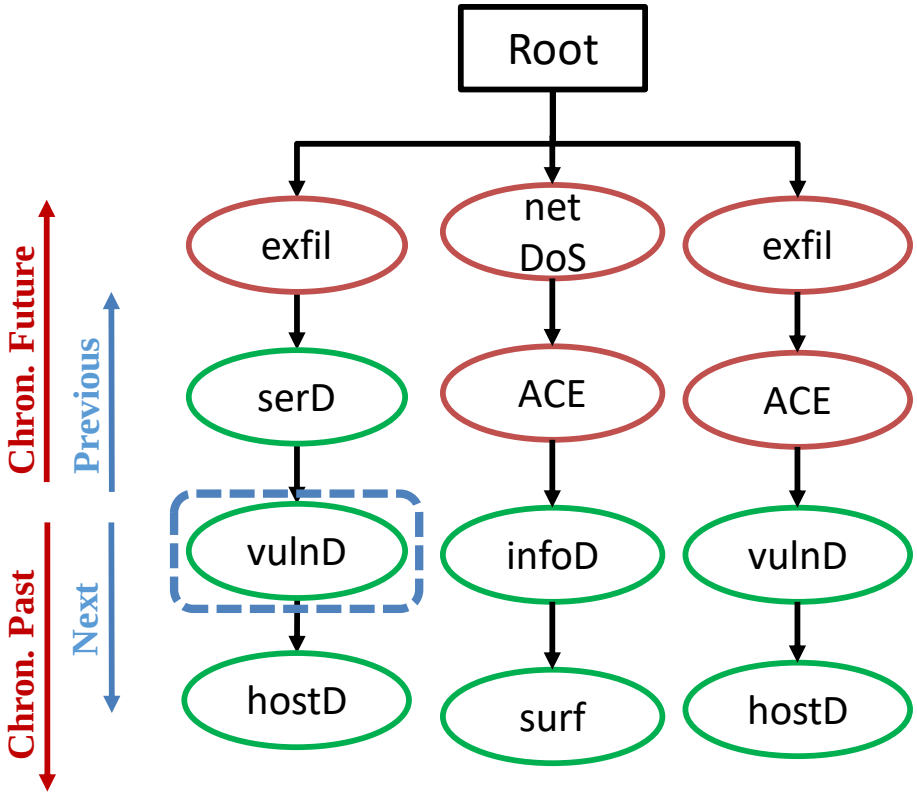
HostD | VulnD | ServD | Exfil

Surf | InfoD | ACExec | DoS

HostD | VulnD | ACExec | Exfil

…

… all sub-sequences!

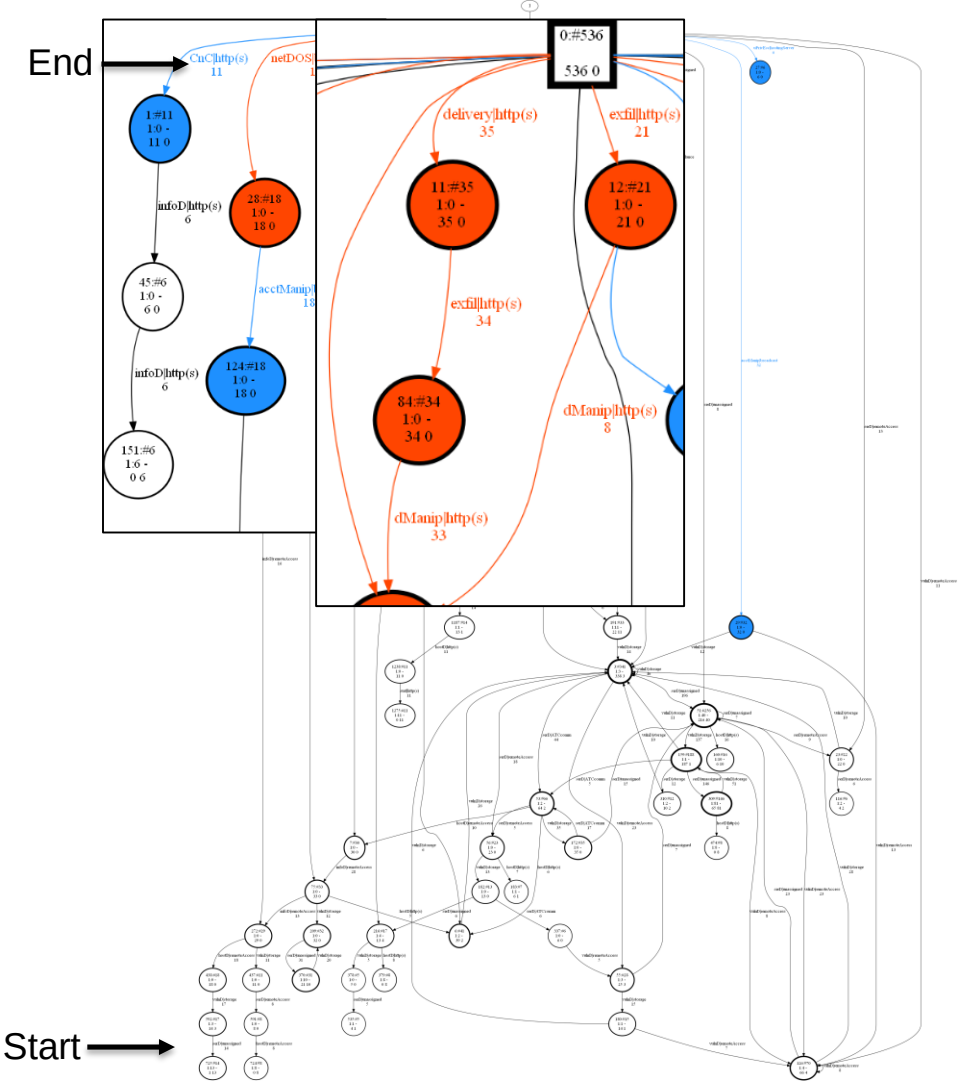


TU Delft

S-PDFA

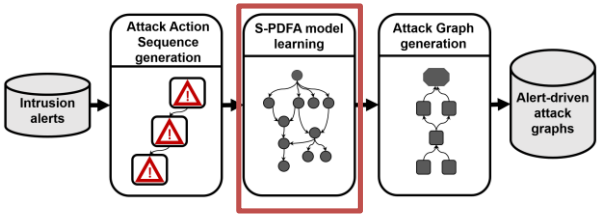
- *Suffix-based Probabilistic Deterministic Finite Automata*

- State colors
  - Severe | Medium | Low

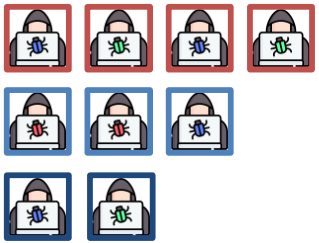


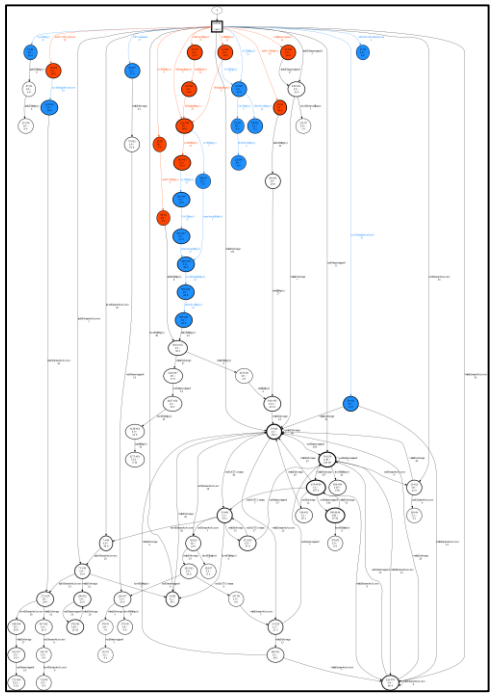
TU Delft

Encoding action sequences

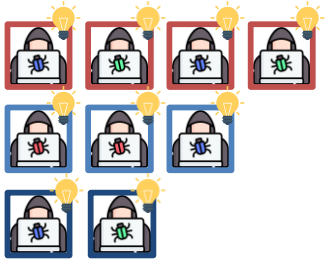


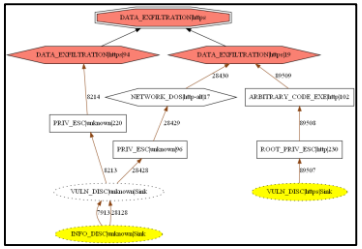
Action sequences





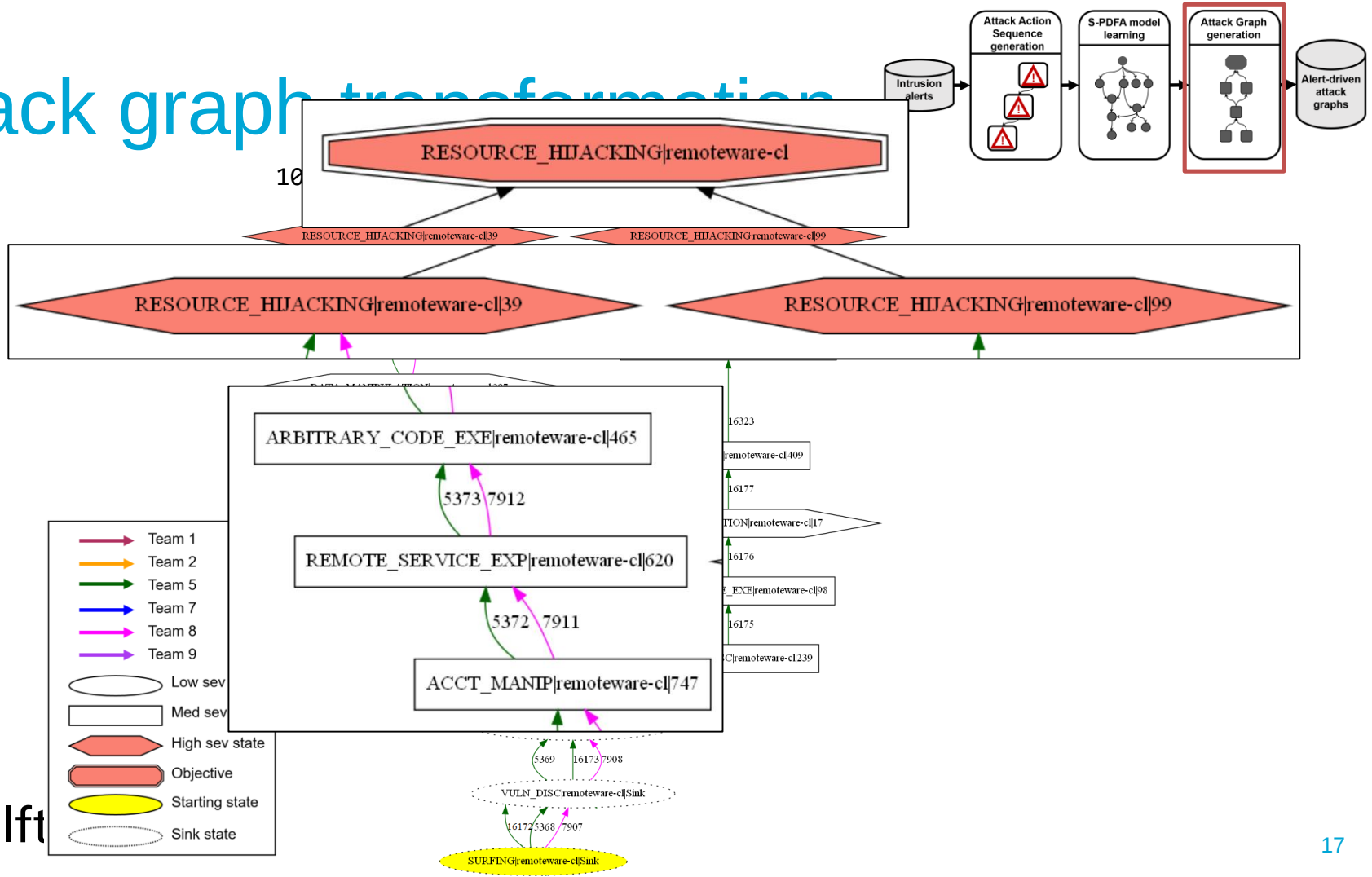
State sequences





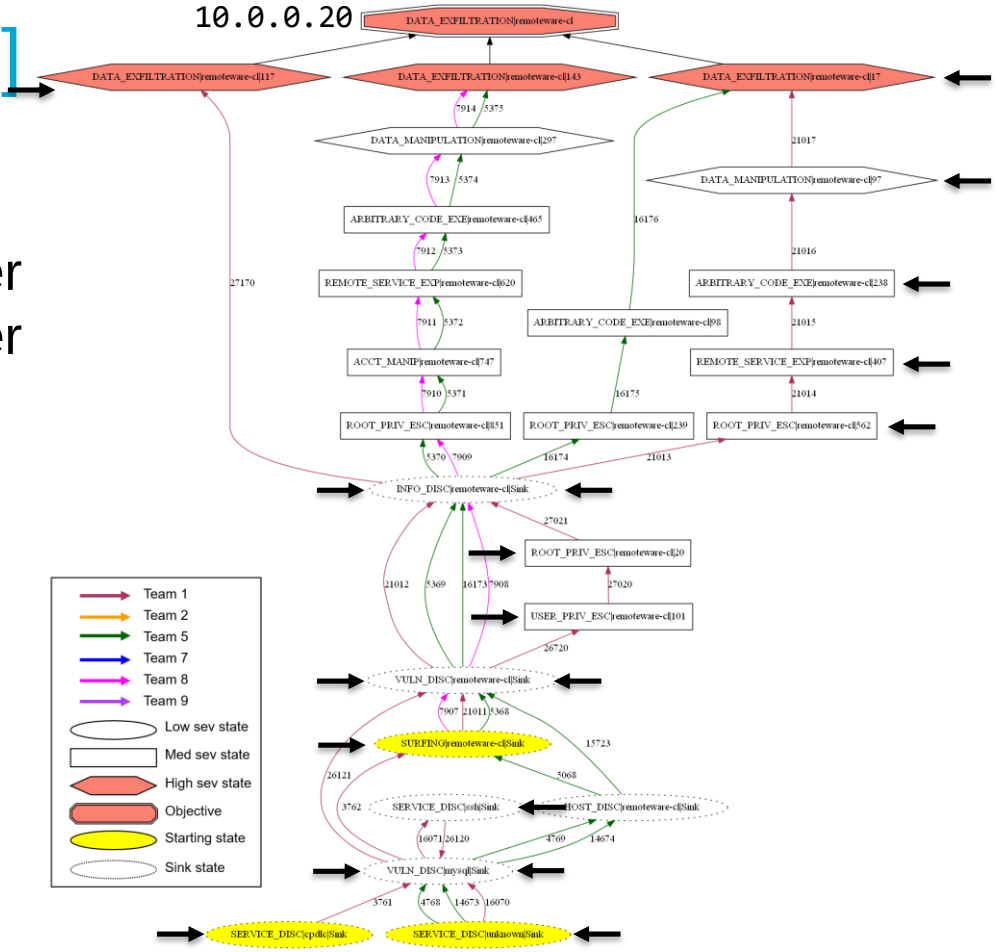
TU Delft

Attack graph transformation



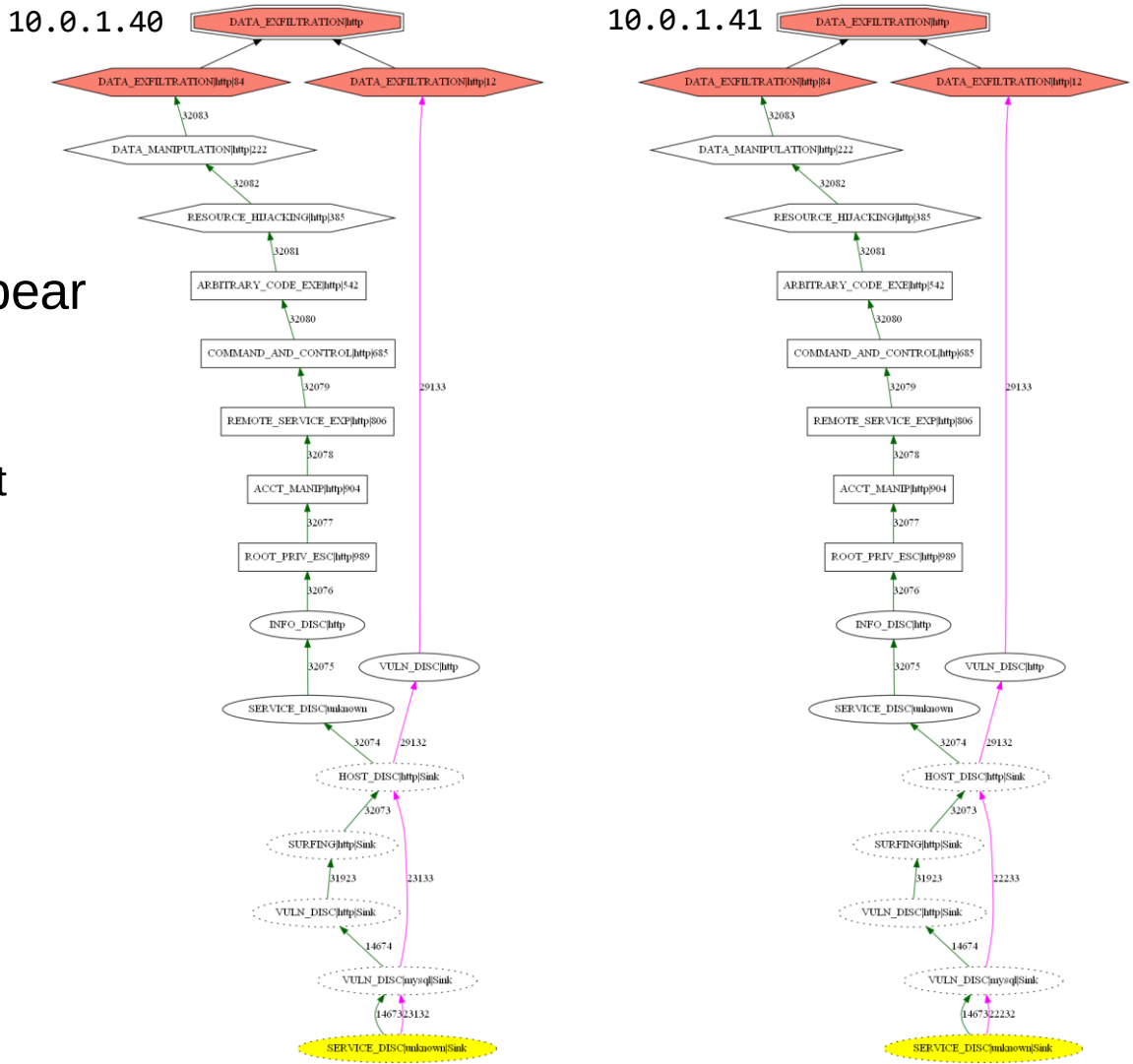
Insights [1/3]

- Attackers follow shorter paths after discovering longer ones



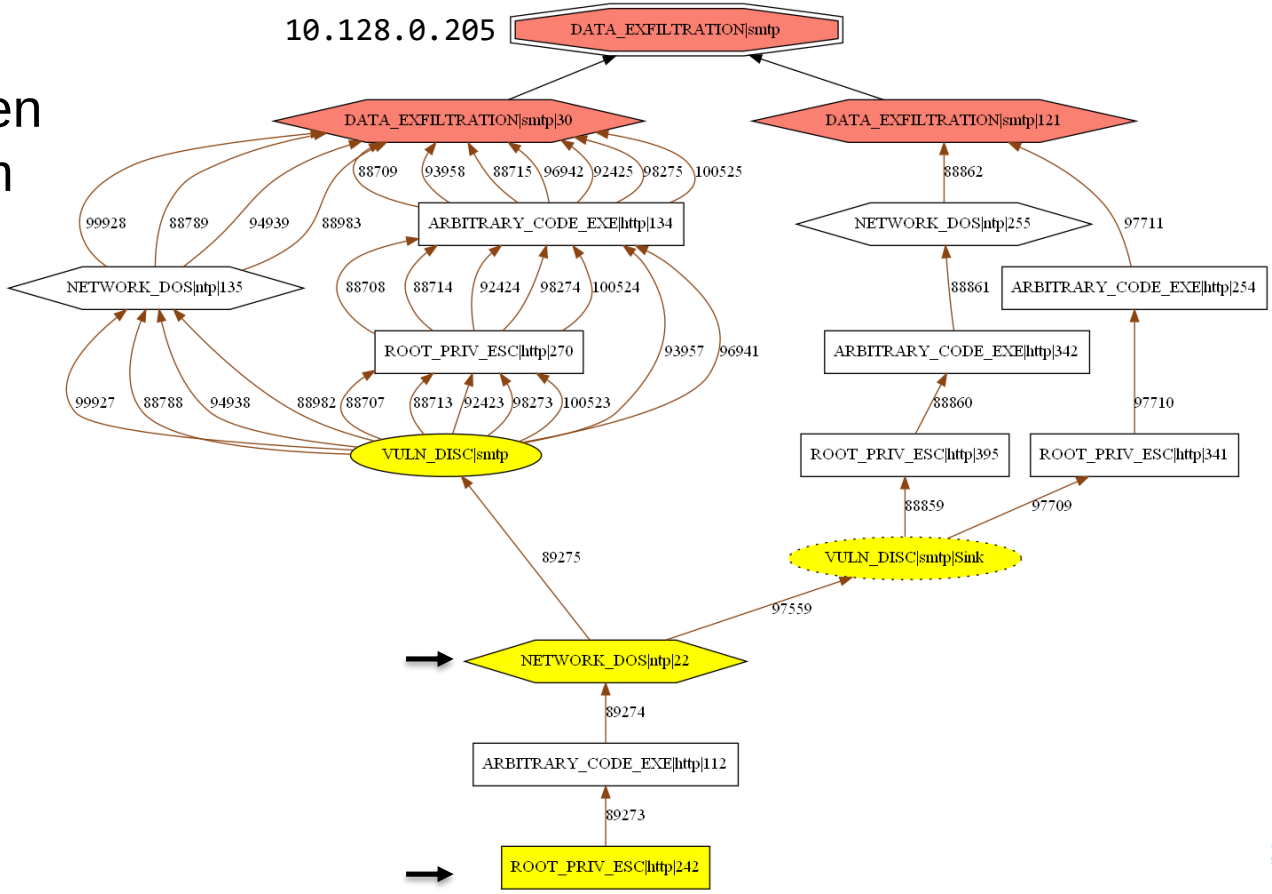
Insights [2/3]

- Parallel attacks appear as identical AGs
  - Targeted in parallel
  - Targeted in different ways



Insights [3/3]

- Paths in alert-driven AGs can start from severe states



Challenges + Future work

- Abstract attacker action mapping
- Enriching manual AGs

- Modelling collaborating attackers
- AG evasion resilience

Conclusion

- Attack forensic analysis is labor intensive & difficult
- Existing AG generation → expert knowledge + known vulnerabilities

- S-PDFA
  - highlights infrequent actions,
  - identifies contextually different actions
    (based on identical future and similar past)

- Attack graphs
  - show duplicate/near identical strategies,
  - capture attackers' behavior dynamics

- Alert-driven AGs can provide actionable intelligence

TU Delft

Thank you!
Questions?

- S-PDFA
  - highlights infrequent actions,
  - identifies contextually different actions
  - *(based on identical future and similar past)*
- Attack graphs
  - show duplicate/near identical strategies,
  - capture attackers' behavior dynamics
- Alert-driven AGs can provide actionable intelligence

azqa.nadeem@tudelft.nl

https://cyber-analytics.nl/

TU Delft