foreseeti

Mapping Cyber Threat Intelligence to Probabilistic Attack Graphs

Presenter: Andreas Gylling

mekstedt@kth.se

andreas.gylling@foreseeti.com

zafzal@kth.se

per.eliasson@foreseeti.com

KTH VETENSKAP OCH KONST

RICS

SOCCRATES

This work has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement no. 833481 as well as the Swedish Civil Contingencies Agency through the research centre Resilient Information and Control Systems (RICS)

Agenda

Introduction

About the project

Method

Design & Implementation

Results

& Discussions

Conclusion

What's next?

Introduction

- Problem:
  - Growing Threats, limited resources
- Related Solutions:
  - ADGs (Attack-defense graphs)
  - CTI being made more accessible (E.g. by ACT)
  - Limited work on connection between ADGs/CTI
  - No work takes real time CTI information to create an attacker profile to enhance ADGs

- Question: *How can Cyber Threat Intelligence be used to enrich probabilistic attack graphs in real time, so that they represent a specific Threat Actor's common attack vectors?*
- Assess ICT systems' security:
  - W.r.t Specific Threat Actors - CTI
  - Visual Presentation – ADG
  - Proactive measures
    - Response & Actions

EU H2020

Background
Concepts

CTI

MITRE | ATT&CK®

Agenda

Introduction

About the project

Method

Design & Implementation

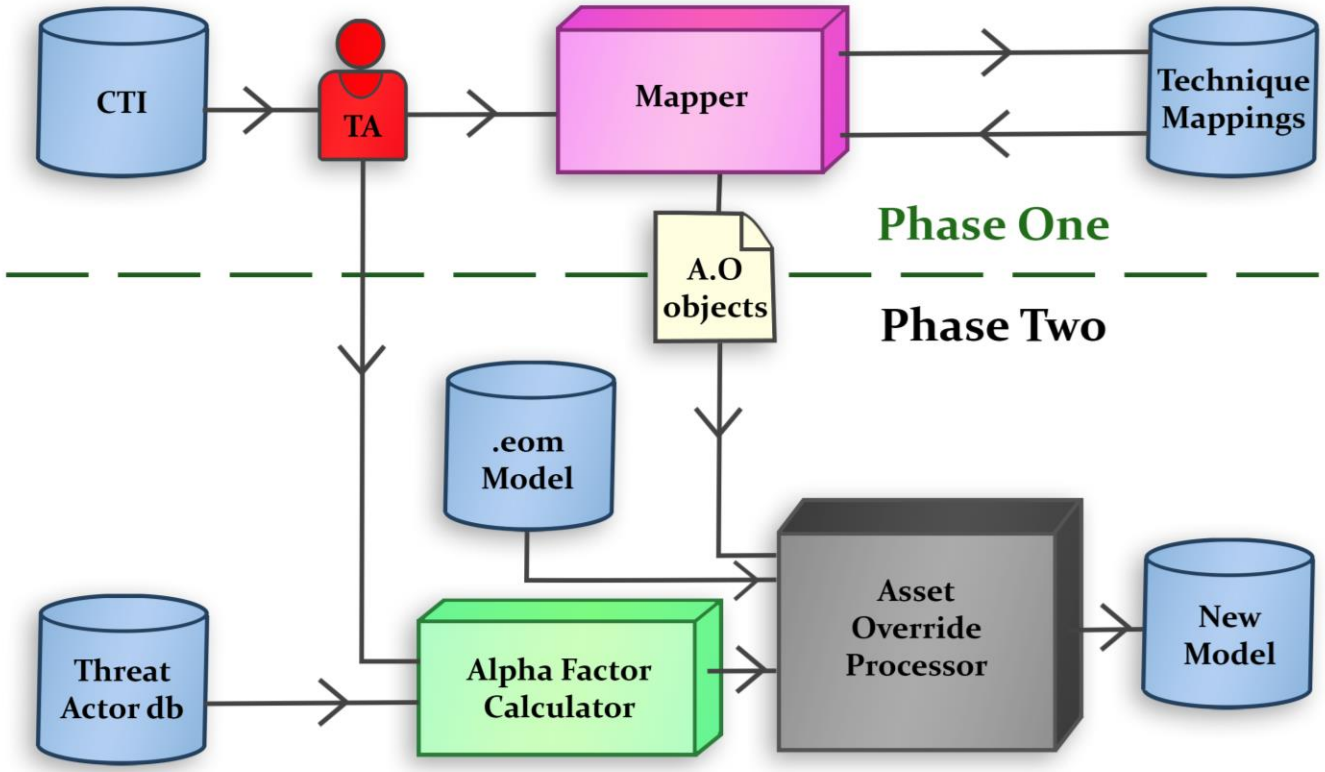
Results

& Discussions

Conclusion

What's next?

Design



- Threat Actor (TA)
- Scope of TA's abilities
- Overall Skill
- Model

Mapping Procedure

Technique

1. Identify Assets
2. Identifying Attack Steps
3. Isolation
4. Platform Specific
5. Defenses

DEP	ASLR	TTC
0	0	exponential(default*α)
1	0	exponential(default*α)
0	1	exponential(default*α)
1	1	exponential(default*α)

6. Scaling

securiLang

```
<Asset>: {
    "Tag": {
      "Type": [<Platform>, <Platform>, ...],
      "connectedTo": [                                  Optional
        <Type>,
        ...
      ]
    }
    AttackSteps: {
      <attackStep> : {
        <Distribution> : {
          <parameters>
        },"Defenses": {
          <Defense>: 0/1/<probability>,
          ...
        },"Alpha" : {
          "Affects" : true/false
        },"Epsilon": {                                  Optional
            "Action" : <Operator>
            "Value":  <Numerical>
        }
      }, ...
    }
}
```

Techniques Mapping

Initial Access	Execution	Defence Evasion	Credential Access	Lateral Movement
Drive-by Compromise	Command-Line Interface	Indicator Removal on Host	Input Capture	Remote File Copy
		File Deletion		
		Modify Registry		
		Software Packing		

securiLang

Alpha Factor – Overall Skill

Sophistication Properties

Code/Tools Developed	Copied	0
	Modified	1
	In-house	2
If In-house development: Actively maintained code	False	0
	True	1
Uses complex Components	False	0
	True	1
Familiar with Victims	False	0
	True	1
Heavy Reconnaissance Effort	False	0
	True	1
Familiar with Victim's Systems	False	0
	True	1
Consistent Operator Practices	False	0
	True	1
Operational Tempo	Low	0
	Medium	1
	High	2
Resource Level	Individual, Club, Contest	0
	Team	1
	Organization	2
	Government	3
Zero Day Capable	False	0
	True	0

$$\delta = \sum(\text{Sophistication Properties})$$

$$\alpha = alpha(\delta) = \begin{cases} 0.9, & \text{if } 6 \leq \delta < 7 \\ 0.8, & \text{if } 7 \leq \delta < 9 \\ 0.7, & \text{if } 9 \leq \delta < 11 \\ 0.6, & \text{if } 11 \leq \delta < 13 \\ 0.5, & \text{if } 13 \leq \delta \\ 1.0, & \text{otherwise} \end{cases}$$

$\alpha = 0.5$

Agenda

Introduction

About the project

Method

Design & Implementation

Results &

Discussions

Conclusion

What's next?

Model

- Smart grid use cases
- Describes a real world scenario
  - connected systems and suppliers
- Manual Tagging in securiCAD
  - WebBrowsers / WebServers
  - Linux / macOS / Windows

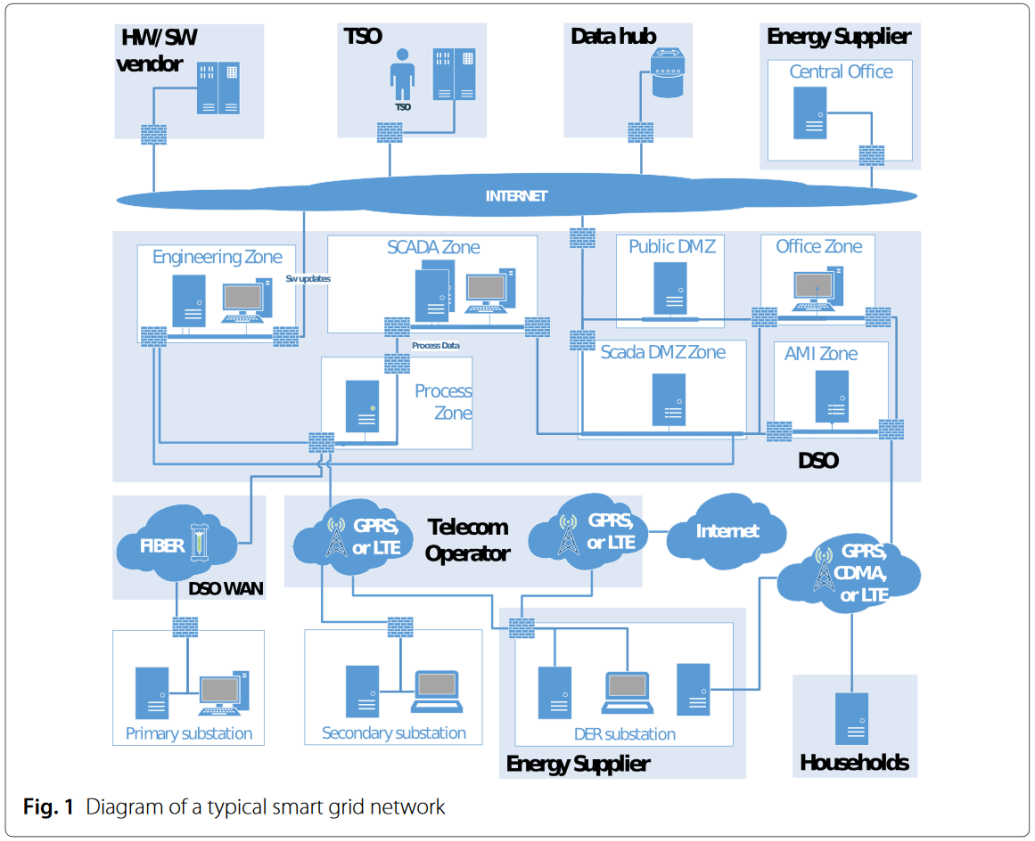
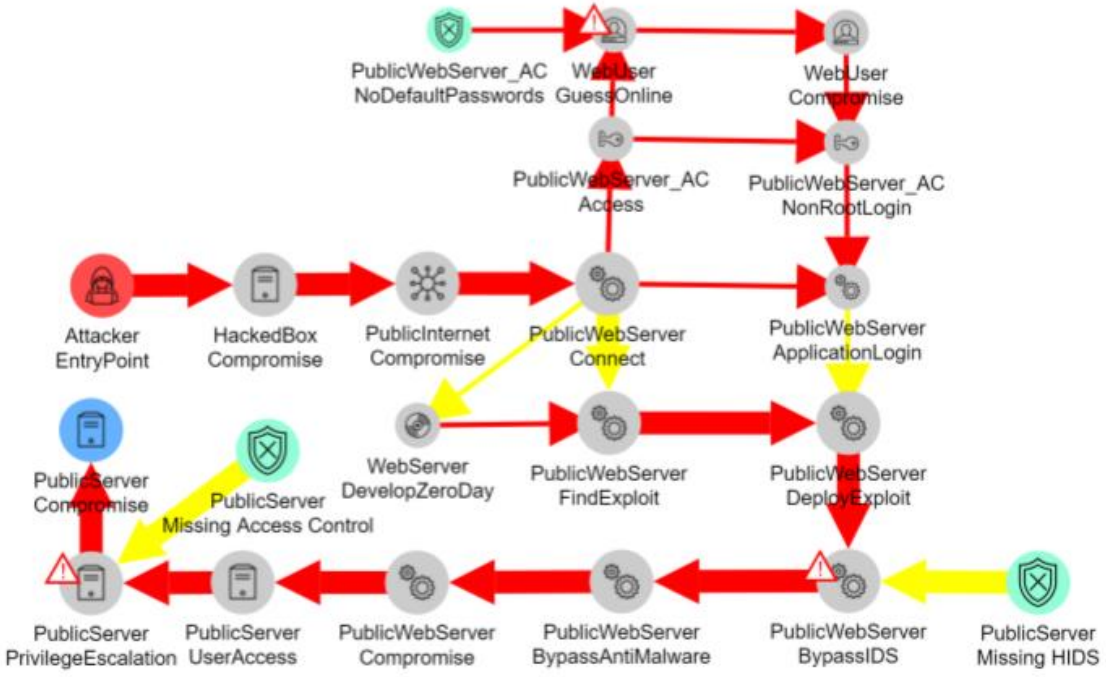
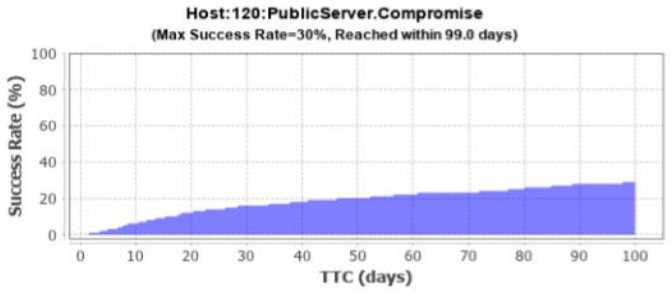


Fig. 1 Diagram of a typical smart grid network

Source: https://community.securicad.com/scada-reference-architecture/

Standard Pentester



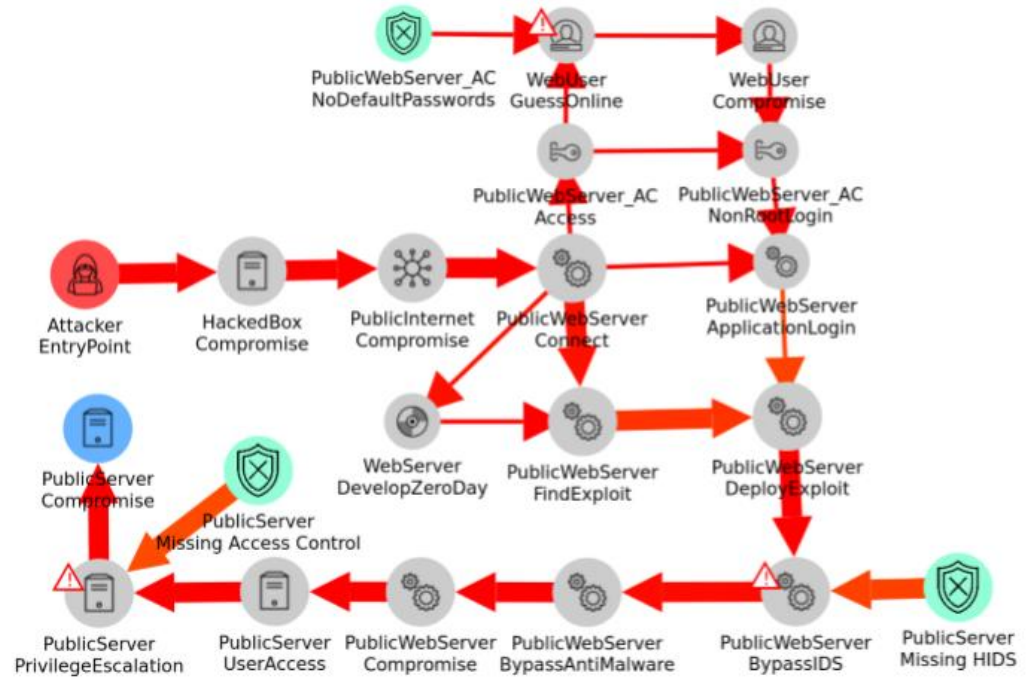


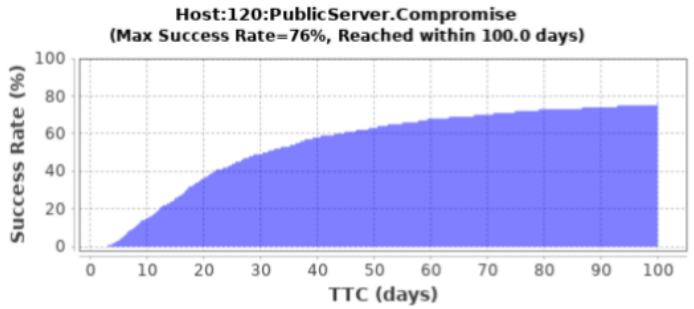
TTC (Days)	Success Rate (%)
10	7
20	13
50	21

Success Rate (%)	TTC (Days)
5	8
50	100
95	100

Figure 5.3: Standard TTC for Compromising a Public WebServer

APT38 Attacker Profile

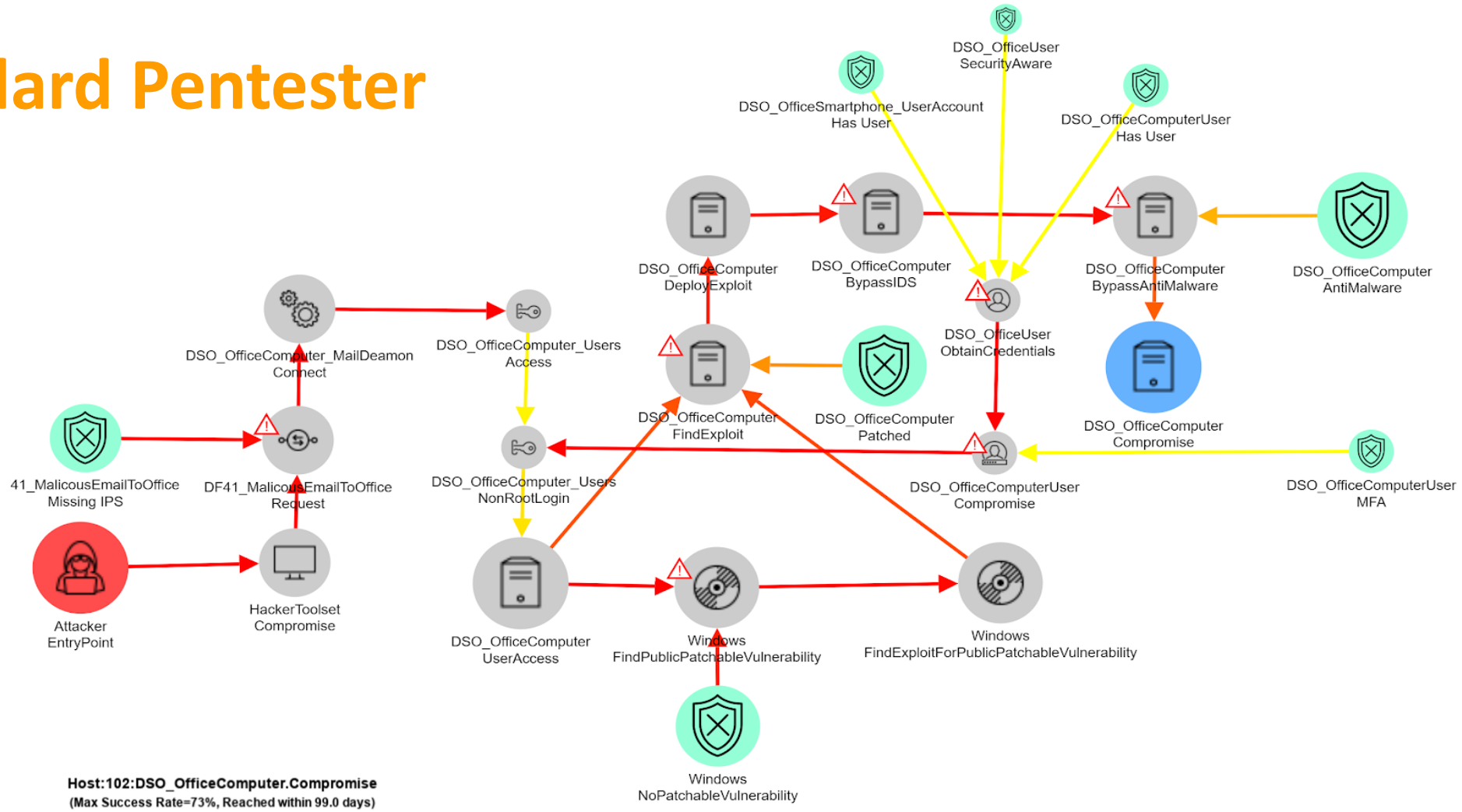


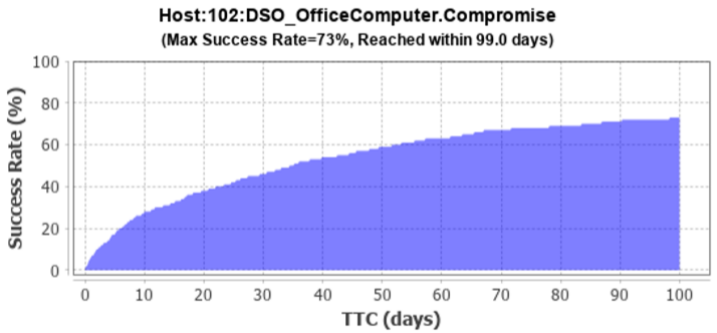


TTC (Days)	Success Rate (%)
10	16
20	37
50	64

Success Rate (%)	TTC (Days)
5	6
50	31
95	100

Standard Pentester

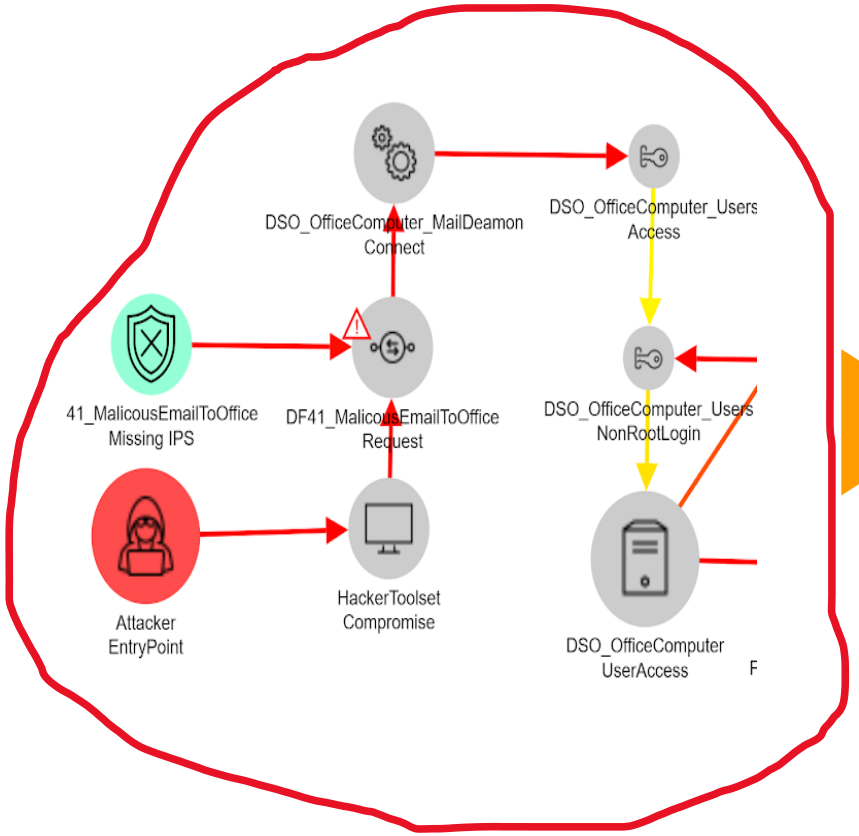


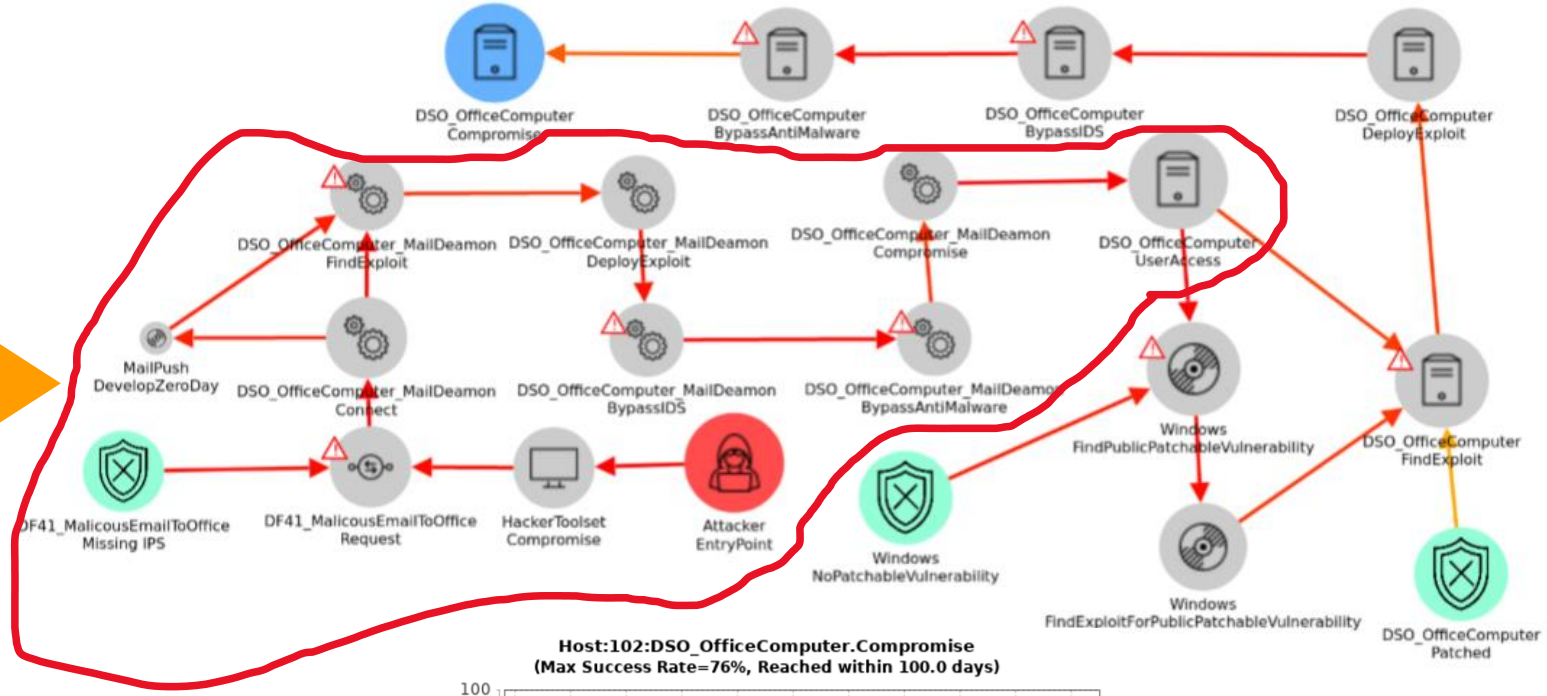


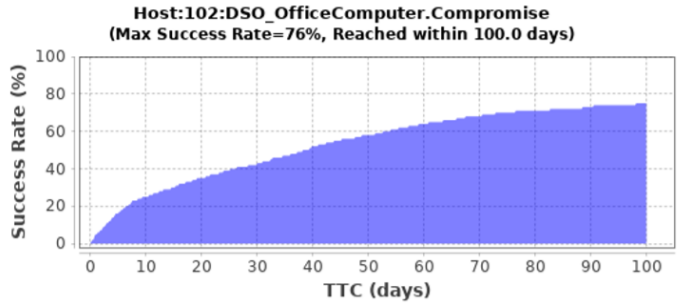
TTC (Days)	Success Rate (%)
10	28
20	35
50	60

Success Rate (%)	TTC (Days)
5	1
50	35
95	100

APT38 Attacker Profile



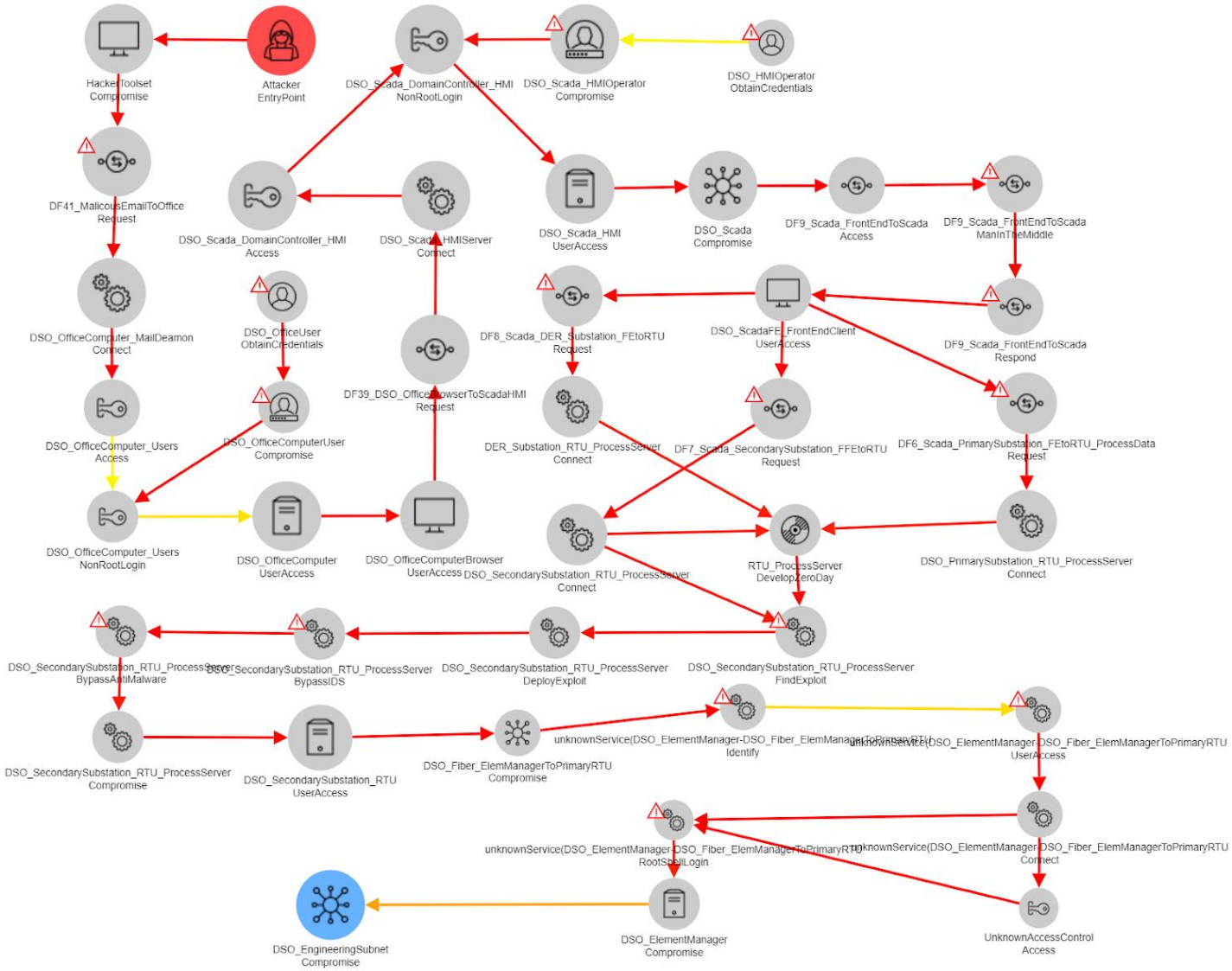


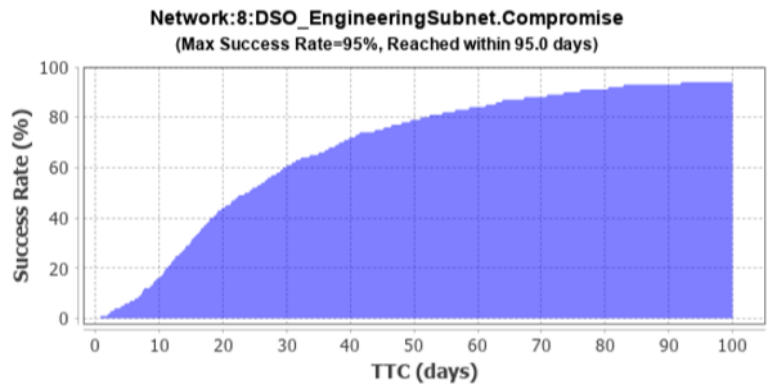


TTC (Days)	Success Rate (%)
10	26
20	36
50	59

Success Rate (%)	TTC (Days)
5	1
50	39
95	100

Standard Pentester

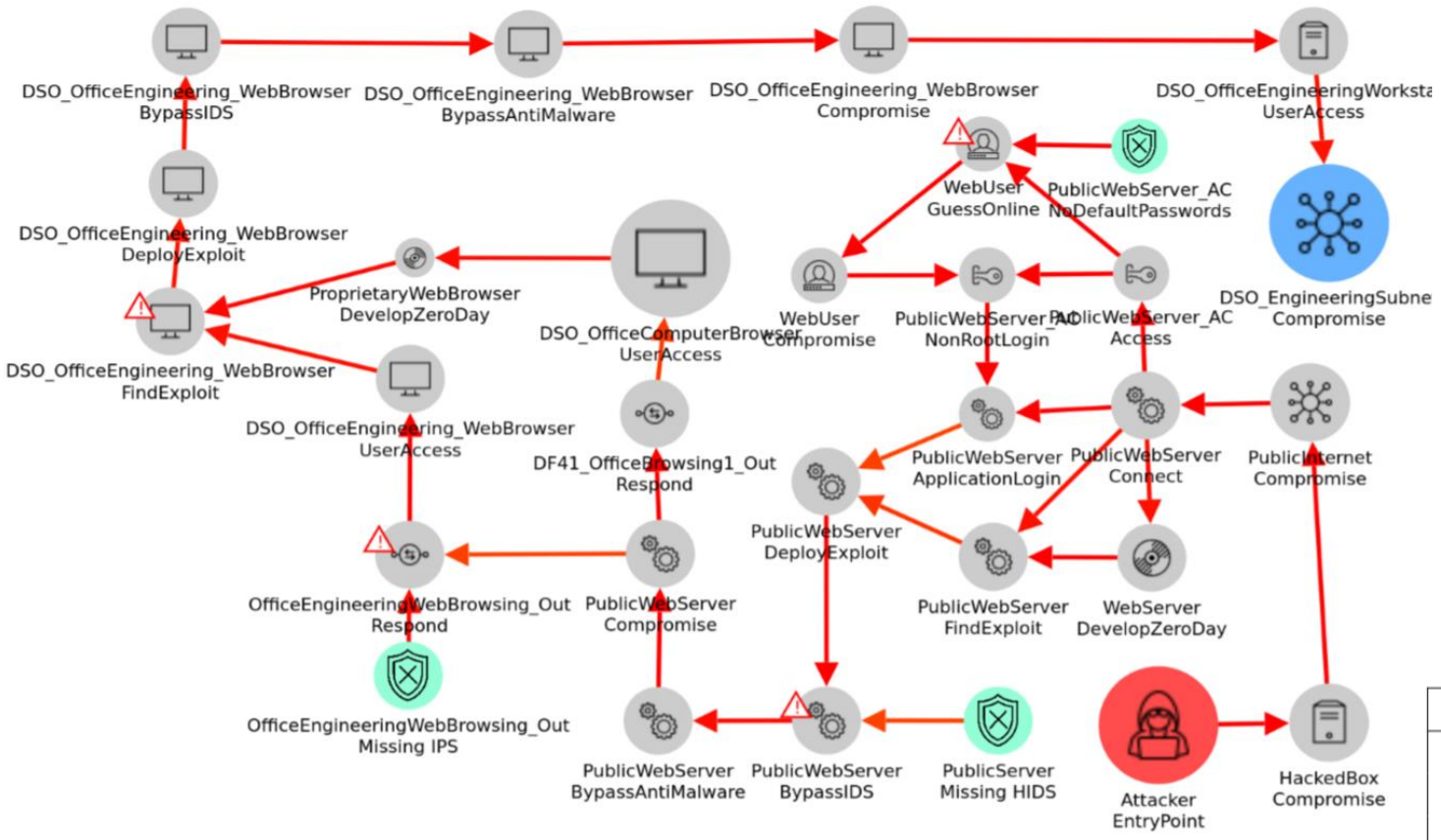


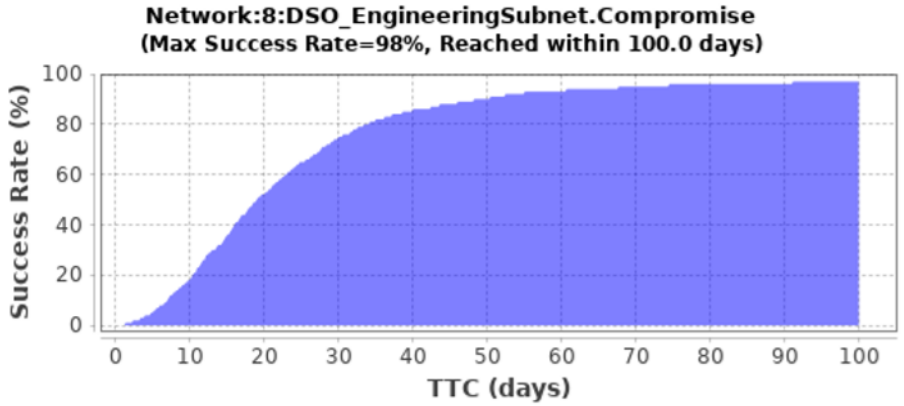


TTC (Days)	Success Rate (%)
10	17
20	45
50	80

Success Rate (%)	TTC (Days)
5	4
50	24
95	100

APT38





TTC (Days)	Success Rate (%)
10	19
20	53
50	91

Success Rate (%)	TTC (Days)
5	5
50	19
95	69

Agenda

Introduction

About the project

Method

Design & Implementation

Results &

Discussions

Conclusion

What's next?

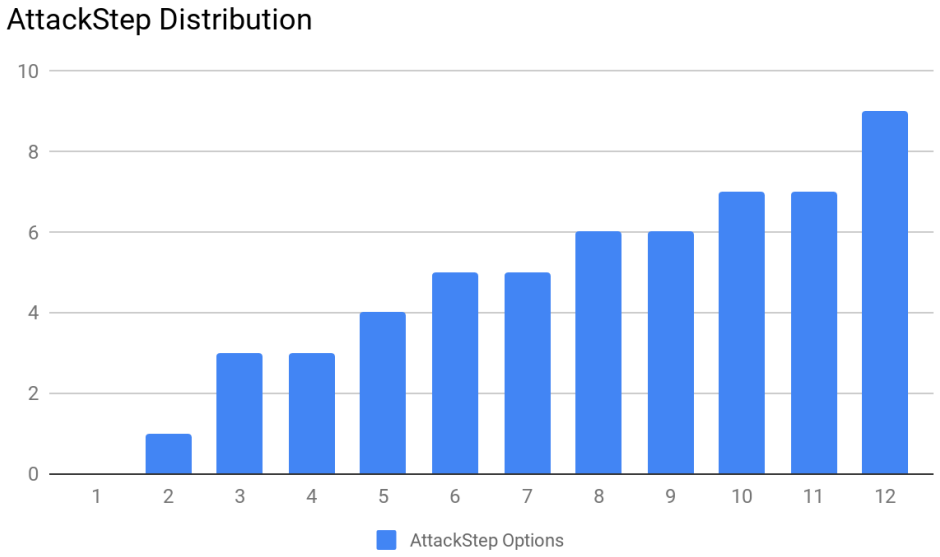
Limitations

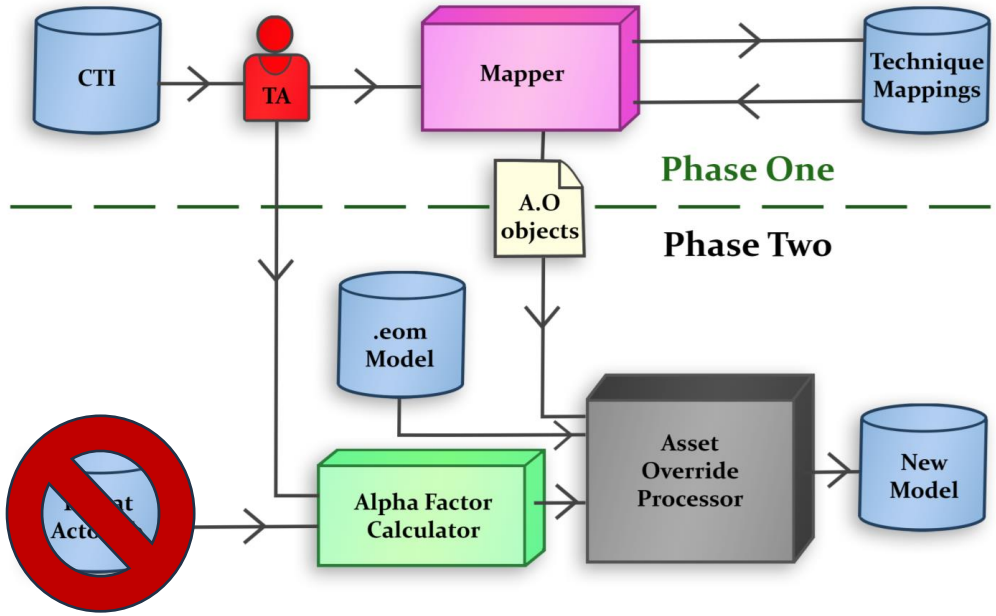
Code/Tools Developed	Copied	0
	Modified	1
	In-house	2
If In-house development: Actively maintained code	False	0
	True	1
Uses complex Components	False	0
	True	1
Familiar with Victims	False	0
	True	1
Heavy Reconnaissance Effort	False	0
	True	1
Familiar with Victim's Systems	False	0
	True	1
Consistent Operator Practices	False	0
	True	1
Operational Tempo	Low	0
	Medium	1
	High	2
Resource Level	Individual, Club, Contest	0
	Team	1
	Organization	2
	Government	3
Zero Day Capable	False	0
	True	0

- Sophistication Property Weights
  - Discrete assignment
- Multiple Options for attack steps
  - No added benefit
- Shortest path calculation
  - Attacker's TTPs not always present

Future Work

- Several Attack Step Options
  - Attack Step Distribution
- Full technique coverage
  - Test more TAs
- Usability
  - Automatic Tagging
  - Direct access to TA α-properties

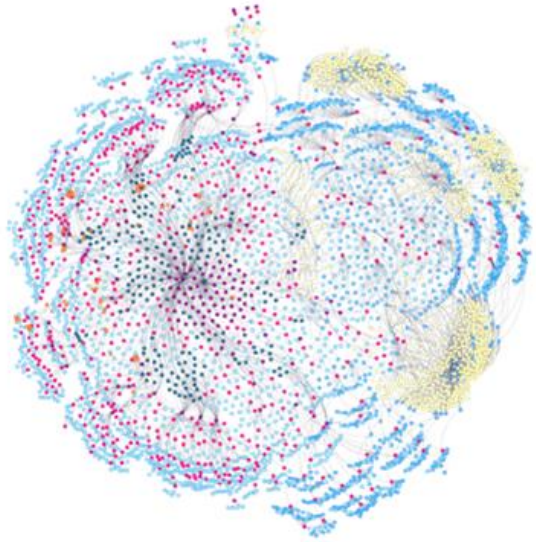




Conclusion

How can Cyber Threat Intelligence be used to enrich probabilistic attack graphs in real time, so that they represent a specific Threat Actor's common attack vectors?

- Identify CTI-objects that:
  - Represents scope of abilities
    - Accurately Map Techniques
  - Overall Skill
    - Sophistication Properties
- Model Tagging
- Attacker Profile similar to APT38's TTPs



foreseeti

Thanks for listening!

Questions ?

mekstedt@kth.se

zafzal@kth.se

andreas.gylling@foreseeti.com

per.eliasson@foreseeti.com

KTH VETENSKAP OCH KONST

RICS

SOCCRATES

This work has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement no. 833481 as well as the Swedish Civil Contingencies Agency through the research centre Resilient Information and Control Systems (RIC