ARES 2019
International Conference on Availability, Reliability and Security
University of Kent, Canterbury, UK

Automated Cyber Threat Sensing and Responding

Integrating Threat Intelligence into Security-Policy-Controlled Systems

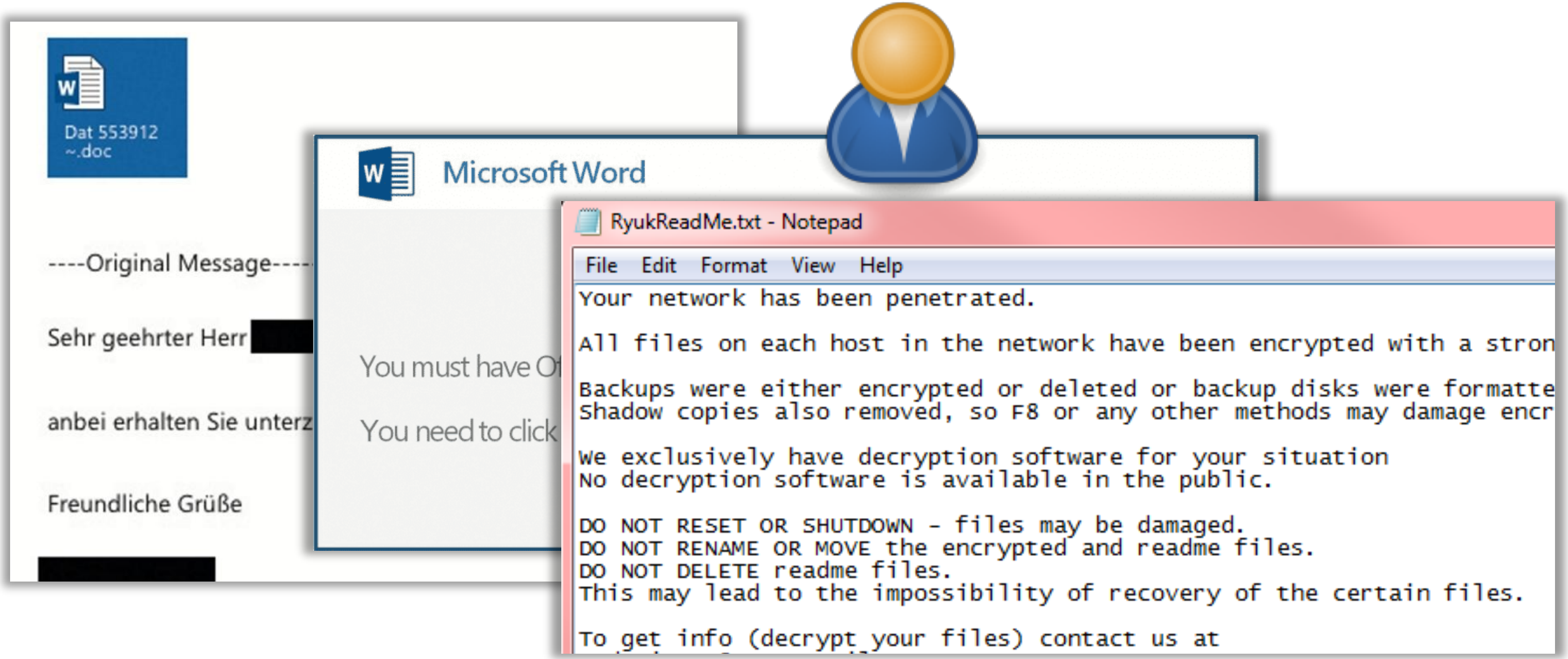
Peter Amthor • Daniel Fischer • Winfried E. Kühnhauser • Dirk Stelzer
Technische Universität Ilmenau, Germany

CyberTIM 2019
2nd International Workshop on Cyber Threat Intelligence Management

2019-08-28

Problem Statement

A Typical Cyber Security Incident



----Original Message----

Sehr geehrter Herr [redacted]

anbei erhalten Sie unterz

Freundliche Grüße

[redacted]

You must have O

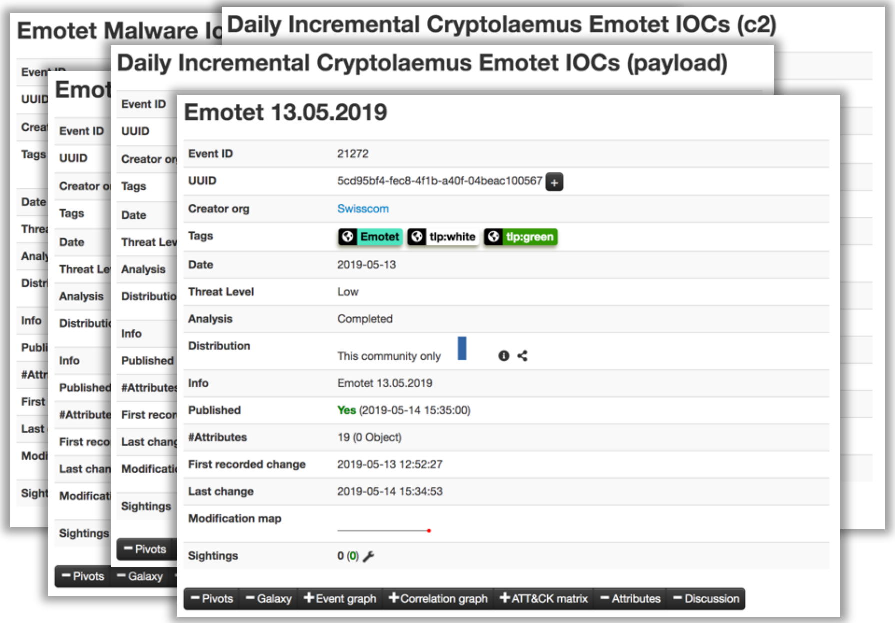
You need to click

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a stron

Backups were either encrypted or deleted or backup disks were formatte
Shadow copies also removed, so F8 or any other methods may damage encr

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
```

Problem Statement

State-of-the-Art Technology

Threat Intelligence Sharing



Emotet Malware Ic

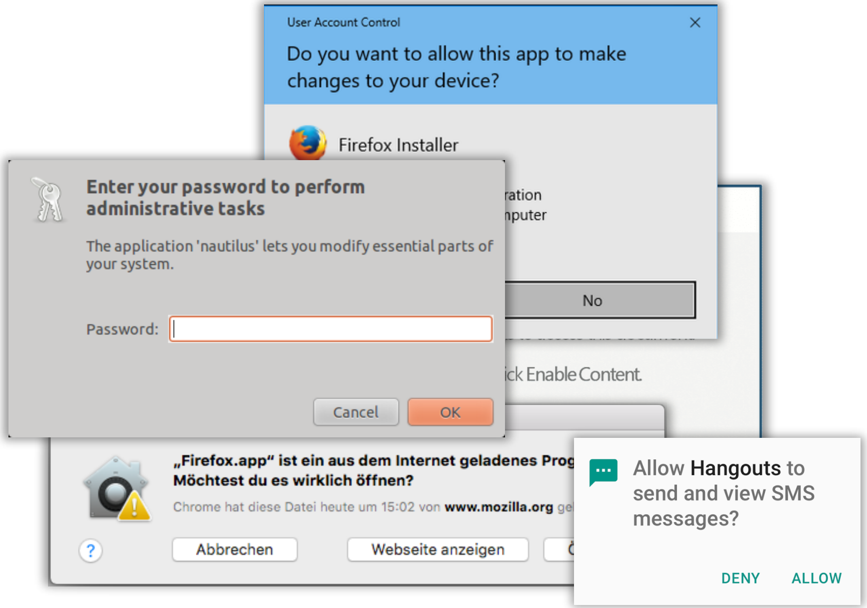
Daily Incremental Cryptolaemus Emotet IOCs (c2)

Daily Incremental Cryptolaemus Emotet IOCs (payload)

Emotet 13.05.2019

Event ID	21272
UUID	5cd95bf4-fec8-4f1b-a40f-04beac100567 +
Creator org	Swisscom
Tags	Emotet tlp:white tlp:green
Date	2019-05-13
Threat Level	Low
Analysis	Completed
Distribution	This community only
Info	Emotet 13.05.2019
Published	Yes (2019-05-14 15:35:00)
#Attributes	19 (0 Object)
First recorded change	2019-05-13 12:52:27
Last change	2019-05-14 15:34:53
Modification map	
Sightings	0 (0)

Automated Security Policies



User Account Control

Do you want to allow this app to make changes to your device?

Firefox Installer

ration

nputer

Enter your password to perform administrative tasks

The application 'nautilus' lets you modify essential parts of your system.

Password:

ick Enable Content.

„Firefox.app“ ist ein aus dem Internet geladenes Prog

Möchtest du es wirklich öffnen?

Chrome hat diese Datei heute um 15:02 von **www.mozilla.org** ge

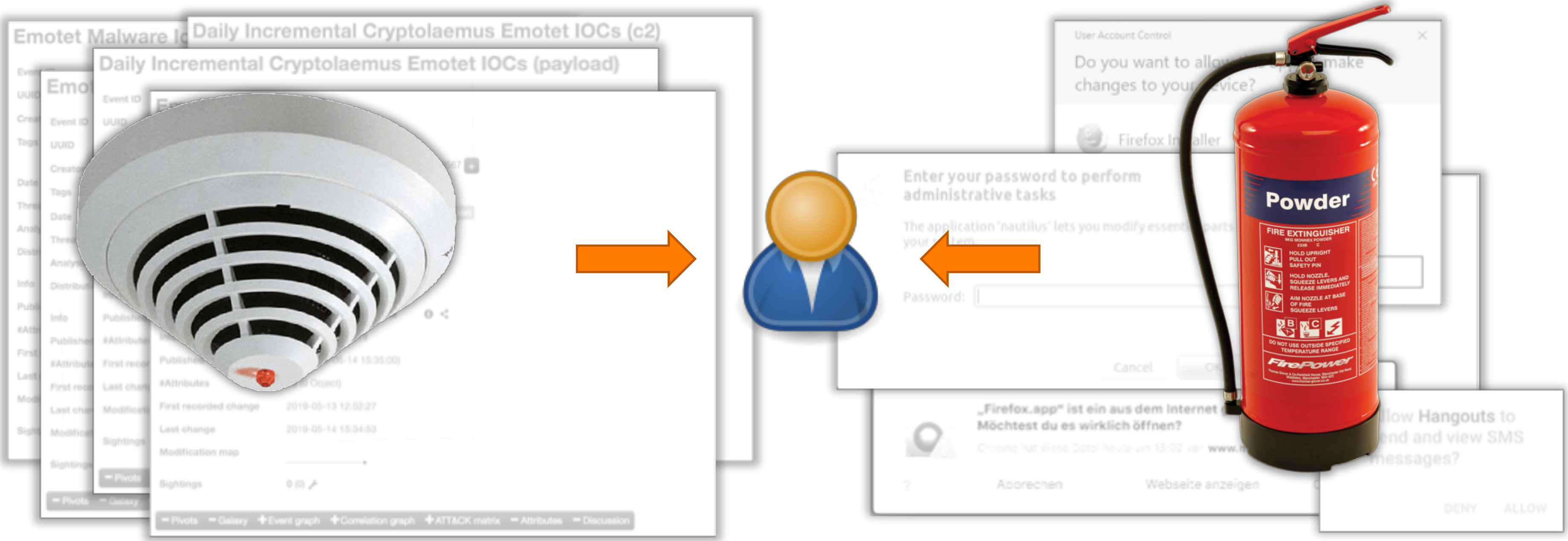
Allow **Hangouts** to send and view SMS messages?

Problem Statement

What We Have

Threat Intelligence Sharing

Automated Security Policies



Daily Incremental Cryptolaemus Emotet IOCs (c2)

Daily Incremental Cryptolaemus Emotet IOCs (payload)

User Account Control

Do you want to allow this app to make changes to your device?

Enter your password to perform administrative tasks

„Firefox.app" ist ein aus dem Internet geladenes Programm. Möchtest du es wirklich öffnen?

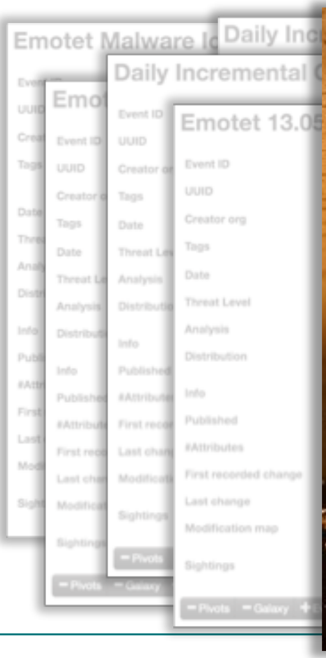
Allow Hangouts to send and view SMS messages?

Problem Statement

What We Actually Want

Threat Intelligence Sharing

Automated Security Policies



Emotet Malware Id

Daily Inc

Emo

Daily Incremental

Emotet 13.05

Event ID

UUID

Creator org

Tags

Date

Threat Level

Analysis

Distribution

Info

Published

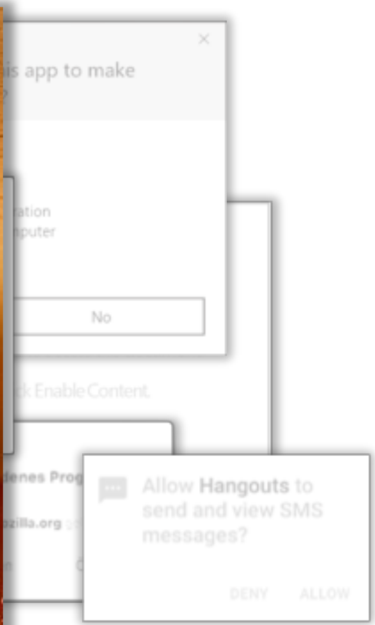
#Attributes

First recorded change

Last change

Modification map

Sightings



is app to make

ation

nputer

k Enable Content

enes Prog

zilla.org

Allow Hangouts to send and view SMS messages?

Problem Analysis

Part 1: The Merits of Threat Intelligence Sharing

- Scope here: Technical TI
  - widely used in practice
  - supported by standards: *IODEF, STIX, TAXII, …*
  - supported by tools: Threat Intelligence Sharing Platforms (*TISPs*)

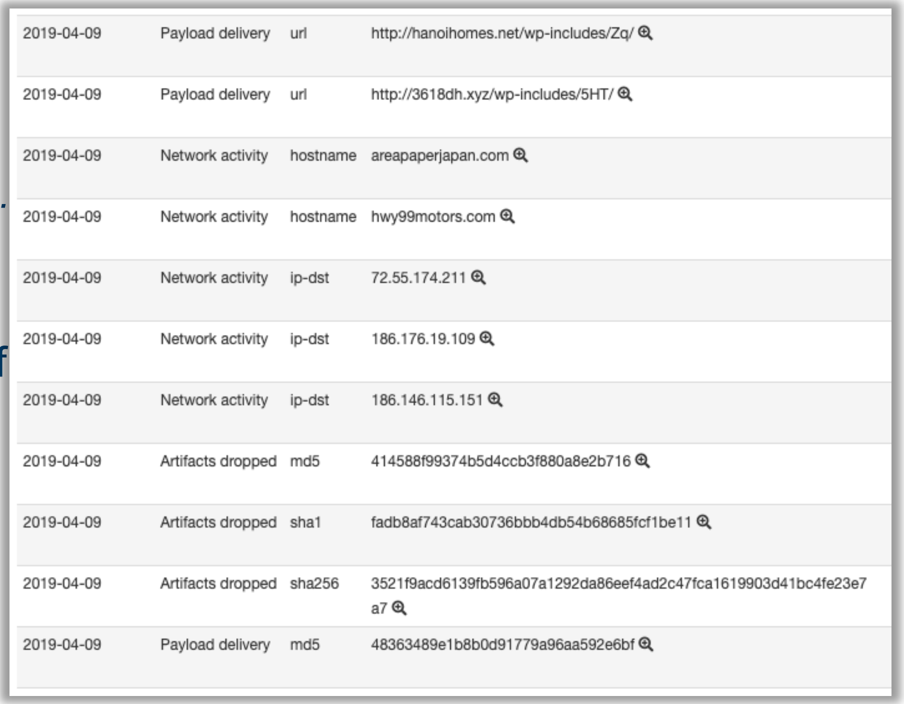
- Goal: disseminate information about a specific attack and attacker (*IoC*):
  - attack type
  - URLs, IP addresses, eMail addresses
  - payload hash sums
  - malware binaries
  - …

Problem Analysis

Part 1: The Merits of Threat Intelligence Sharing

- Scope here: Technical TI
  - widely used in practice
  - supported by standards: *IODEF, STIX, TAXII, ..*
  - supported by tools: Threat Intelligence Sharing

- Goal: disseminate information about a specif
  - attack type
  - URLs, IP addresses, eMail addresses
  - payload hash sums
  - malware binaries
  - …



2019-04-09	Payload delivery	url	http://hanoihomes.net/wp-includes/Zq/
2019-04-09	Payload delivery	url	http://3618dh.xyz/wp-includes/5HT/
2019-04-09	Network activity	hostname	areapaperjapan.com
2019-04-09	Network activity	hostname	hwy99motors.com
2019-04-09	Network activity	ip-dst	72.55.174.211
2019-04-09	Network activity	ip-dst	186.176.19.109
2019-04-09	Network activity	ip-dst	186.146.115.151
2019-04-09	Artifacts dropped	md5	414588f99374b5d4ccb3f880a8e2b716
2019-04-09	Artifacts dropped	sha1	fadb8af743cab30736bbb4db54b68685fcf1be11
2019-04-09	Artifacts dropped	sha256	3521f9acd6139fb596a07a1292da86eef4ad2c47fca1619903d41bc4fe23e7a7
2019-04-09	Payload delivery	md5	48363489e1b8b0d91779a96aa592e6bf

Problem Analysis

Part 1: The Merits of Threat Intelligence Sharing

- What we achieve using TISPs: **Cyber Threat Sensing**

- **Speed**

Fast Threat Information Sharing

Time for Human Response?

- **Cost**

Cost-efficient Threat Detection

Expertise for Threat Handling?

- **Quality**

More Reliable Threat Recognition

Confidence in Correct Actions?

Problem Analysis

Part 2: The Merits of Automated Security Policies

- Scope here: Security-Policy Controlled Systems (*SPCSs*)
  - *policy:* mandatory rules controlling security-critical operations
  - … in application software (*DBIS, ERP, WFMS, …*)
  - … in operating systems and middleware
  - studied here: access control (*AC*) policies

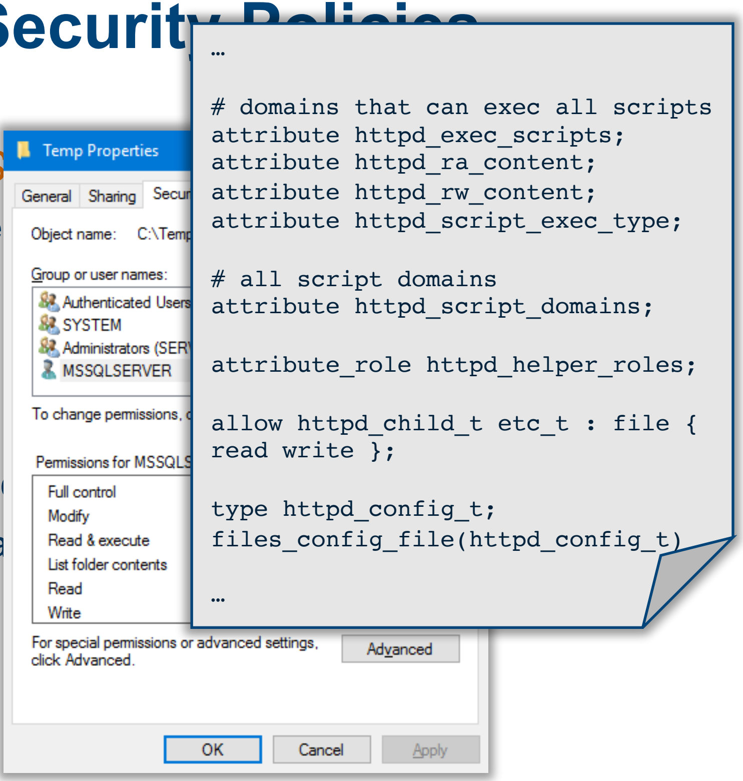
- Goal: automatically protect security-critical resources
  - SPCS engineering: based on formal methods → domain experts
  - SPCS maintenance: policy configuration and update
  - threat-related knowledge: pre-packed by design

Problem Analysis

Part 2: The Merits of Automated Security Policies

- Scope here: Security-Policy Controlled Systems (S
  - *policy:* mandatory rules controlling security-critical ope
  - … in application software (*DBIS, ERP, WFMS, …*)
  - … in operating systems and middleware
  - studied here: access control (*AC*) policies

- Goal: automatically protect security-critical resourc
  - SPCS engineering: based on formal methods → doma
  - SPCS maintenance: policy configuration and update
  - threat-related knowledge: pre-packed by design



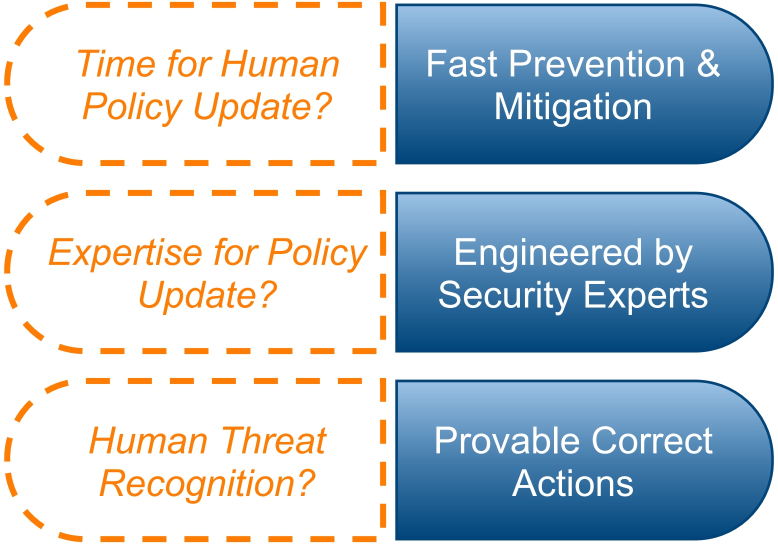
```
…

# domains that can exec all scripts
attribute httpd_exec_scripts;
attribute httpd_ra_content;
attribute httpd_rw_content;
attribute httpd_script_exec_type;

# all script domains
attribute httpd_script_domains;

attribute_role httpd_helper_roles;

allow httpd_child_t etc_t : file {
read write };

type httpd_config_t;
files_config_file(httpd_config_t)

…
```

Problem Analysis

Part 2: The Merits of Automated Security Policies

- What we achieve using security policies: **Cyber Threat Responding**

- **Speed**
- **Cost**
- **Quality**



Time for Human Policy Update?

Fast Prevention & Mitigation

Expertise for Policy Update?

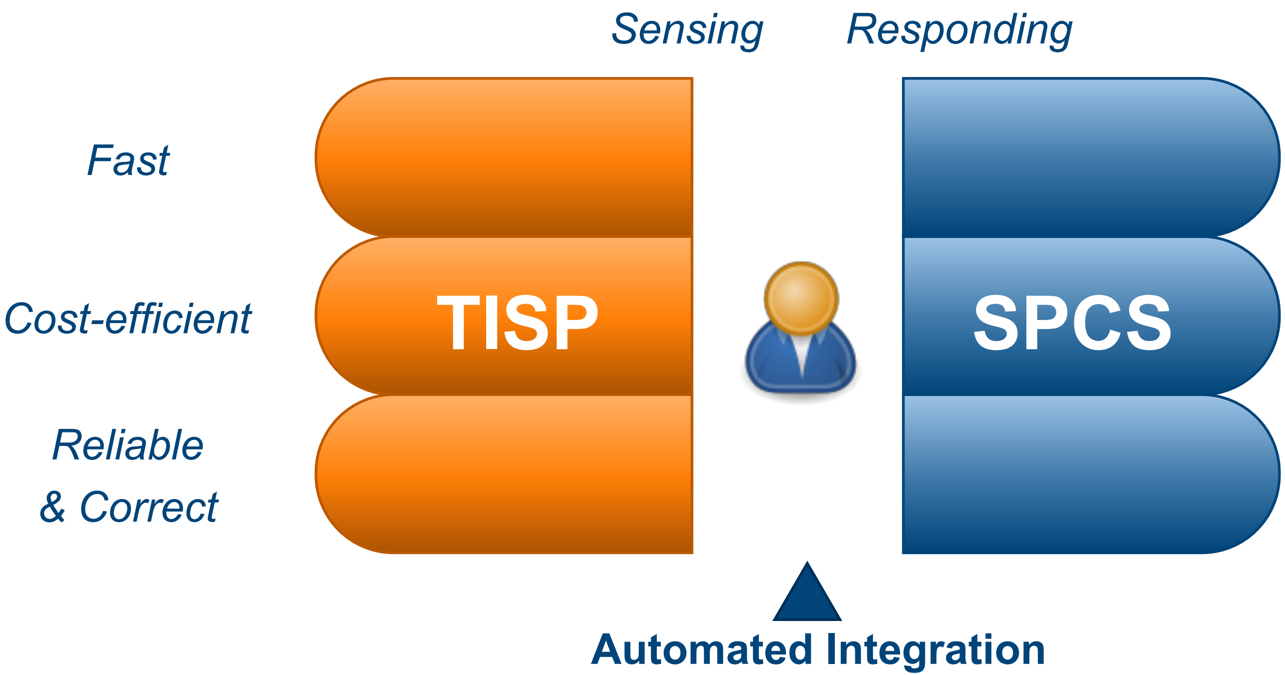
Engineered by Security Experts

Human Threat Recognition?

Provable Correct Actions

Problem Analysis

Consequence



Integration Concept

Design Questions

(1) Which strategies to implement in a threat-responsive SPCS?

(2) Which functional architecture is required to integrate such systems with TISPs?

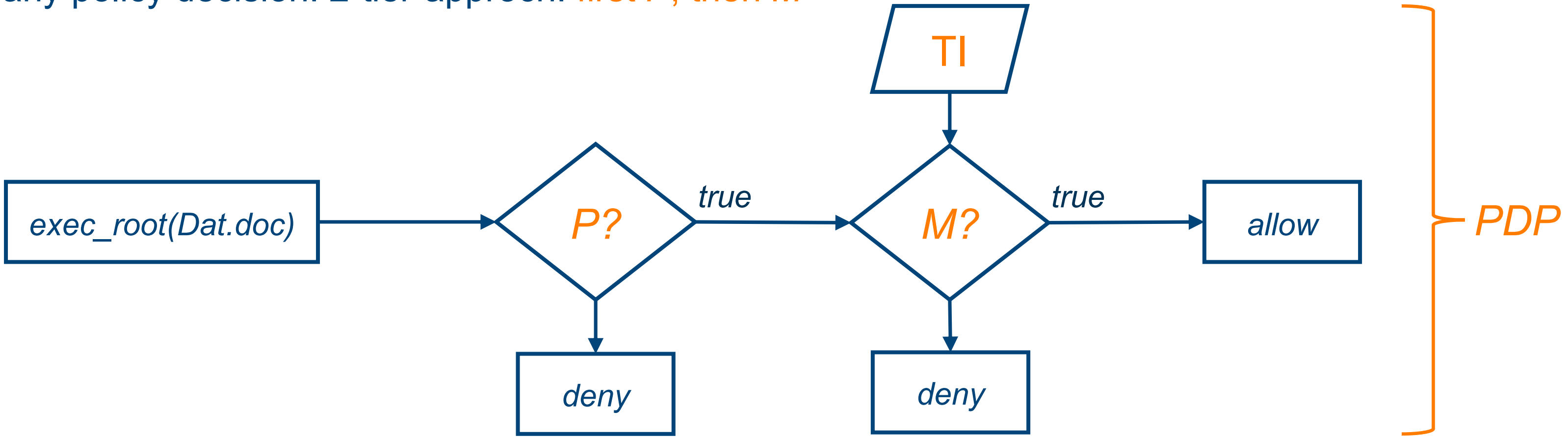
(3) How should TI knowledge be represented and exchanged between TISPs and SPCSs?

Integration Concept

Some Basic Answers (1)

(1) Which strategies to implement in a threat-responsive SPCS?

- compliance with any access control policy *P*
- TI response: risk evaluation metrics *M*
- any policy decision: 2-tier-approch: first *P*, then *M*

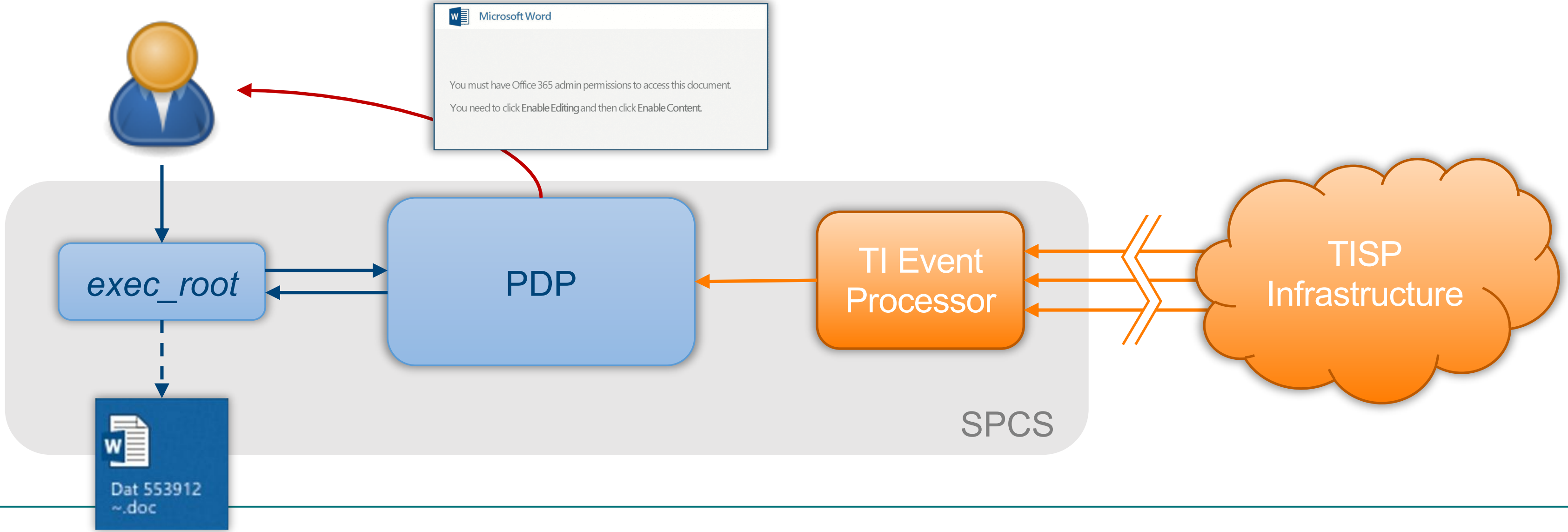


Integration Concept

Some Basic Answers (2)

(2) Which functional architecture is required to integrate such systems with TISPs?

(3) How should TI knowledge be represented and exchanged between TISPs and SPCSs?



Microsoft Word

You must have Office 365 admin permissions to access this document.

You need to click Enable Editing and then click Enable Content.

What’s Next

Ongoing & Future Work

- Question 3: Ontologies to represent relevant technical TI
  - starting points: *IODEF, STIX, TAXII*
  - primary goal: automated PDP interpretation
- Security policy design paradigms
  - TI ontology interface, TI-responsive rules
  - reliable and tamperproof enforcement

Prototype

- **Future Work:** strategic, operational, tactical TI
  - increasing relevance in practice
  - enables more sophisticated automatic response strategies

Conclusion

- Problem: Increasing threats, increasing TI sharing efforts
- Idea: Composition of state-of-the-art technology
  - Threat Intelligence Sharing Platform (TISPs)
  - Security-Policy-Controlled Systems (SPCSs)
- Goal: Automated integration, improving
  - speed
  - cost-effectiveness
  - quality

  } of threat response
- Next: evaluation of feasibility (prototype), practical impact

Peter Amthor • Daniel Fischer • Winfried E. Kühnhauser • Dirk Stelzer
(peter.amthor@tu-ilmenau.de)