CYBER SECURITY COOPERATIVE RESEARCH CENTRE
QUT Queensland University of Technology
Quintessence Labs
CSIRO DATA 61

Cyber Security Research Centre Limited
ABN 11 605 454 144
ceo@cybersecuritycrc.org.au
02 6103 9922

CSCRC AND CSIRO DATA61 SEMINAR

THURSDAY MARCH 10TH

Anomaly Detection in Key-Management Activities Using Metadata: Case Study and Framework

Dr. Mir Ali Rezazadeh Baee (Theme 1.1: Resilient Systems)

INTRODUCTION

- Enterprise information systems produce massive volumes of data
- Information is transmitted over communications networks
- Cryptographic techniques is used to protect stored and transmitted enterprise data

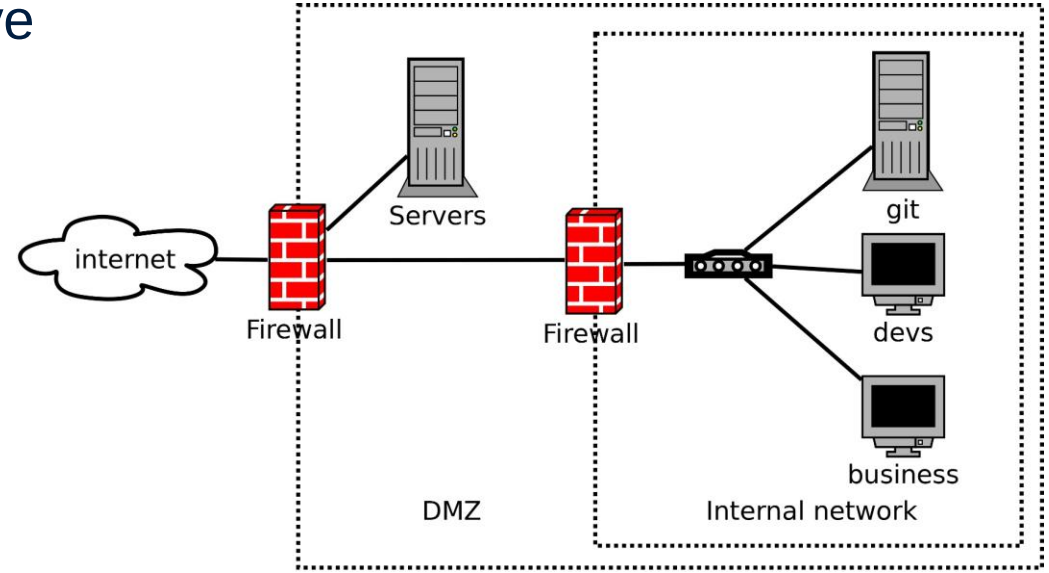

Figure 1. Enterprise network

RESEARCH MOTIVATION

- Applying cryptography requires the use of cryptographic keys
- A key management system is required to achieve organisational data protection objectives
- Enterprise Key-Management (EKM) server may be used for management of the keys

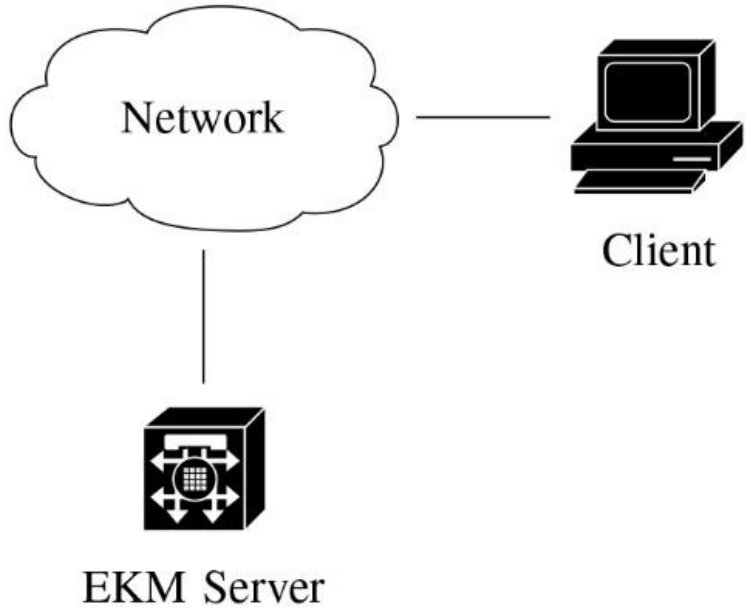

Figure 2. The EKMS network

RESEARCH MOTIVATION

- Various operations may be used
  e.g., create, activate, get, revoke, locate, destroy, modify attribute
- These activities provide additional data
- Analysis of the metadata may reveal information from which inferences about normal and abnormal activity may be made

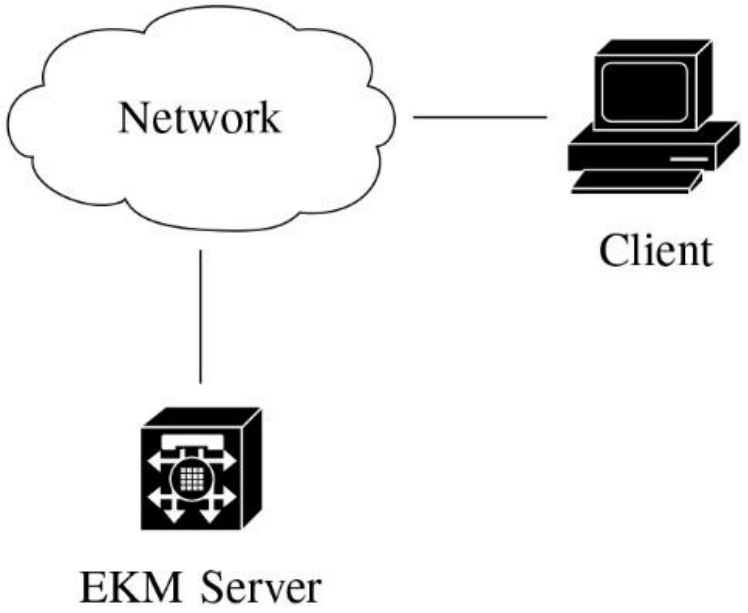

Figure 2. The EKMS network

RESEARCH MOTIVATION

The aim is to develop a framework that can be applied to the EKM metadata:

- for generating heuristics based on categories of behavior
- for use in detecting anomalous enterprise network activities (perhaps malicious)

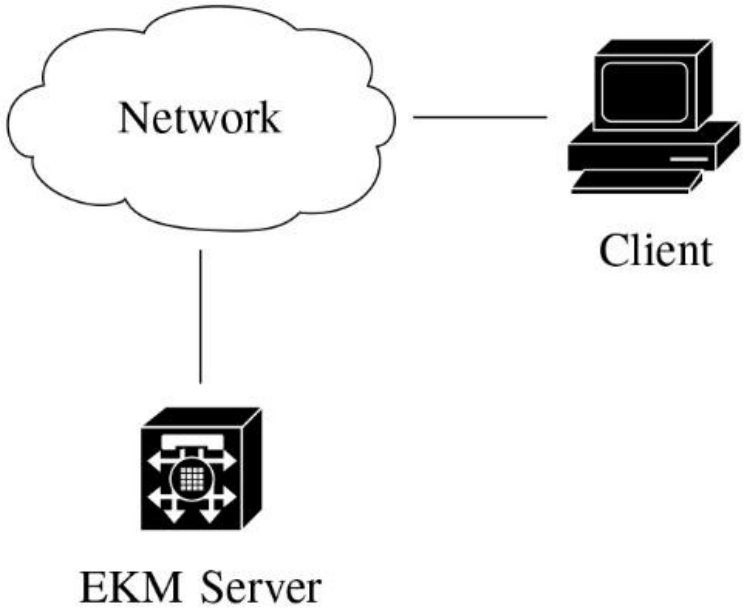

Figure 2. The EKMS network

RESEARCH CHALLENGE

- Defining adversary's aims and capabilities for a set of predefined scenarios
- Determining the specific EKM metadata characteristics to use for anomaly detection

Factors to consider include:

- time variant characteristics of the environment
- changes in user habits
- variations in workload across different periods and context dependent variables

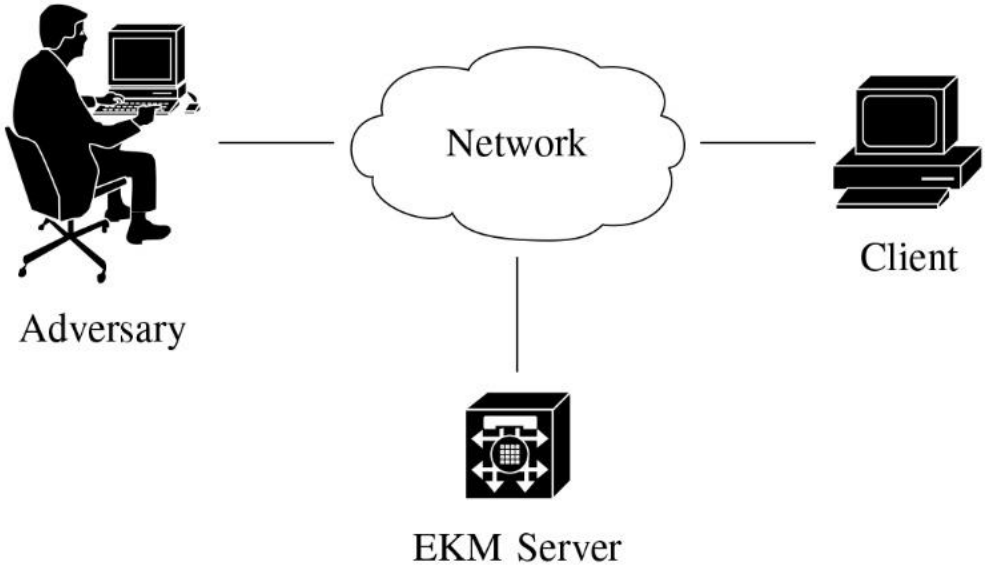

Figure 3. The adversarial model

RESEARCH BRIEF

This work involves:

- Hands-on use of an EKM system
- Simulations of various enterprise operations
- Generation of datasets for a variety of use conditions
- Analysis of the datasets to establish heuristics
- Application of statistical and deep learning based pattern recognition methods for anomaly detection
- Integration with existing anomaly detection using other network metadata

RESEARCH ARCHITECTURE

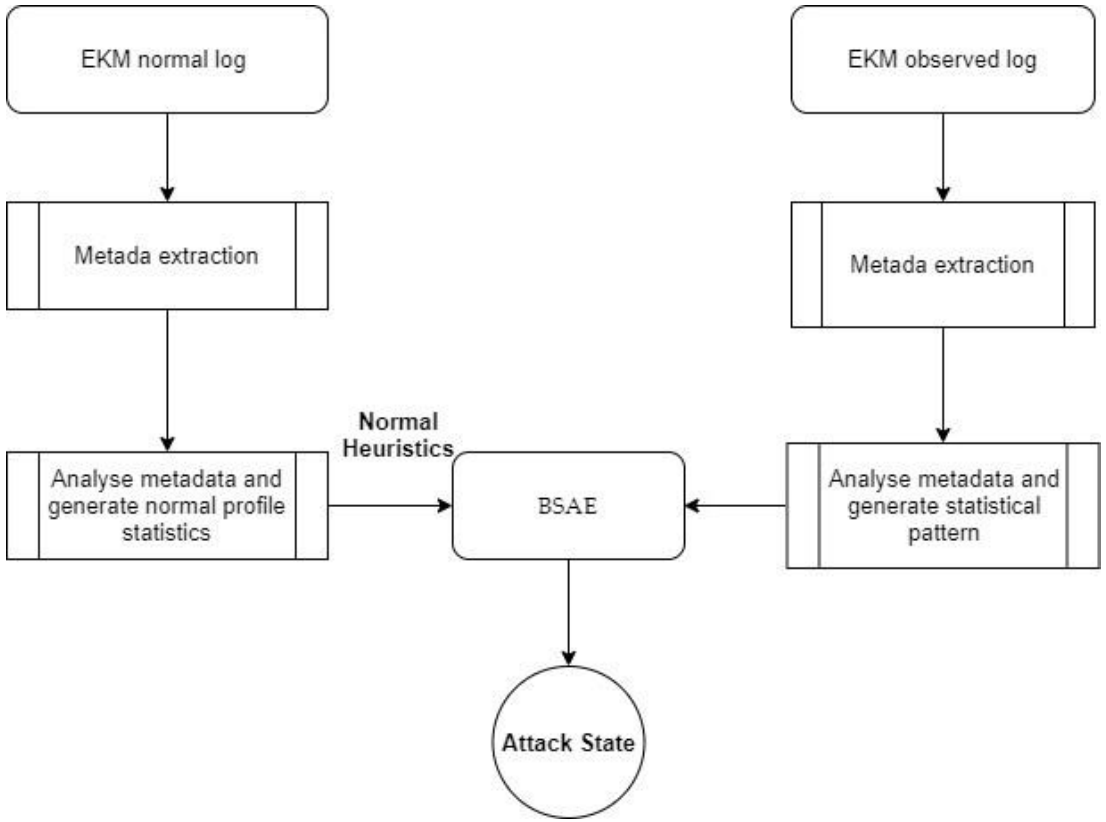

Figure 4. Detection based on EKMS log

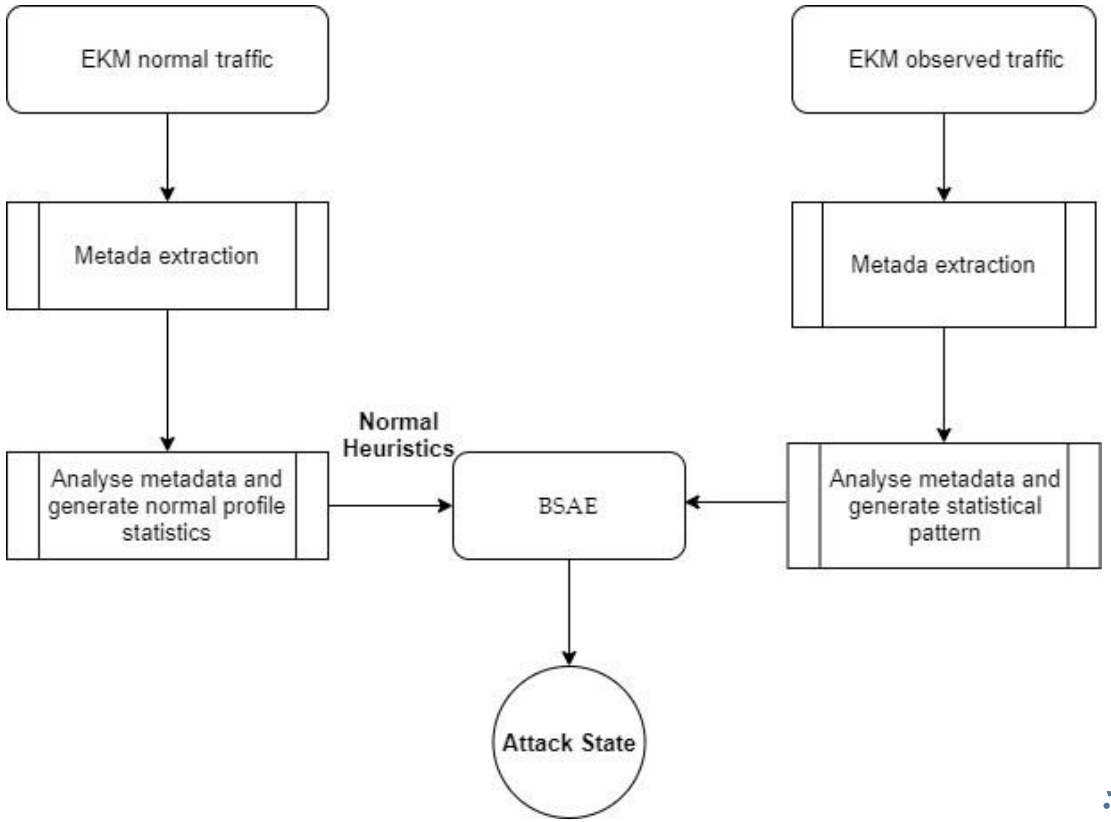

Figure 5. Detection based on EKMS traffic

RESEARCH CONTRIBUTION

To the best of our knowledge, this is the first work applying EKM metadata for enterprise network anomaly detection.

Our contribution is developing a framework that includes:

- A process to identify EKMS metadata associated with normal and abnormal behaviors
- A process to generate datasets of EKMS metadata for normal and abnormal enterprise activities
- Application of neural networks with specific parameters for automated anomaly detection

IMPLEMENTATION

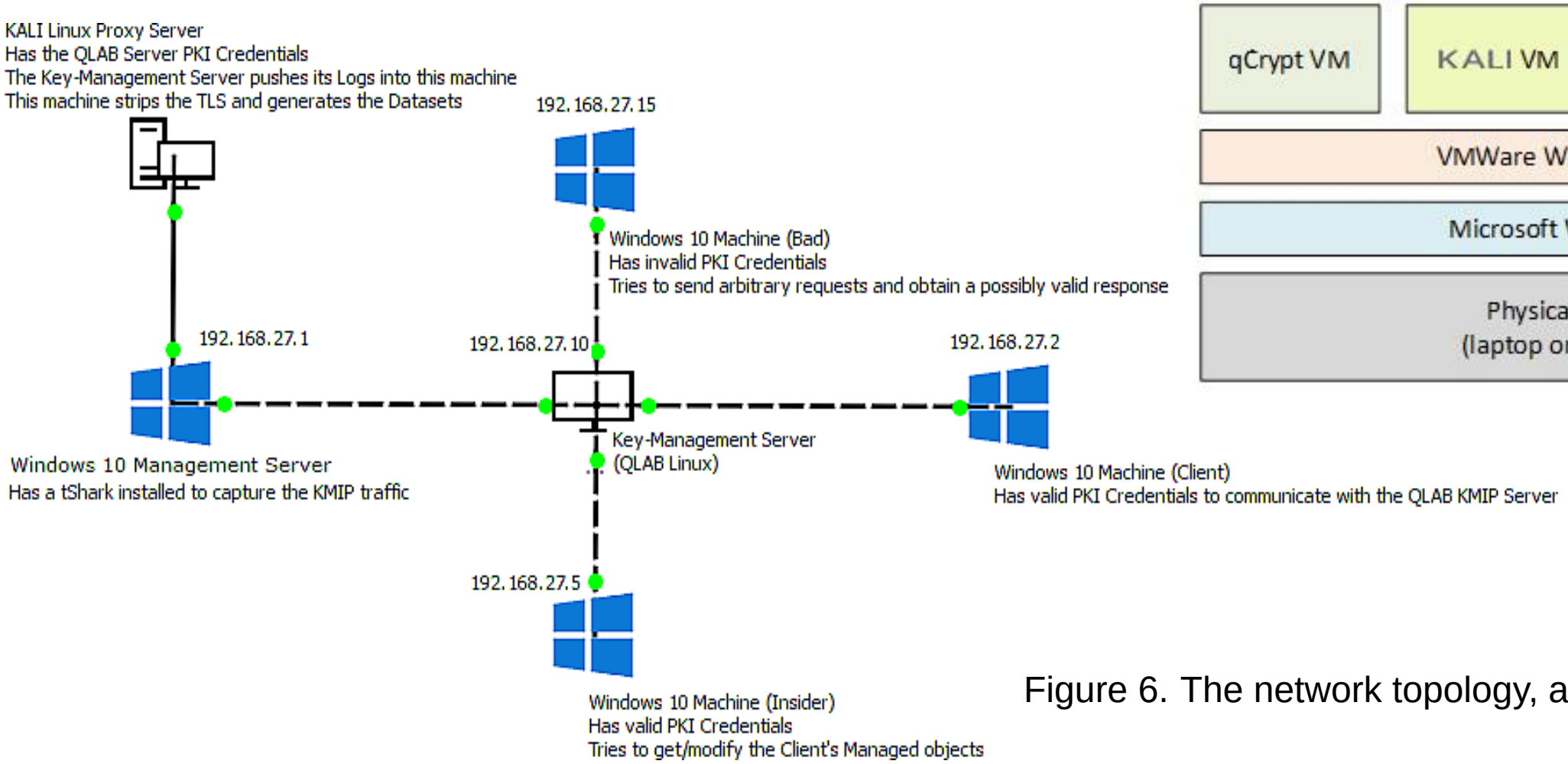

Figure 6. The network topology, actors, and nodes

RFC5424 [1] LOG-BASED METADATA

Awaiting connection
2021.09.05.01.19.36
New connection accepted from 192.168.27.2:55598
Connection server started
ciphers: AES128-SHA:AES128-SHA256:AES256-
checking ca
Initialising_SSL ctx
Supplied PIN null
Selected OS entropy source on port 10002
accepted connection from client (fd=7)
Subject = C=AU/ST=ACT/O=QuintessenceLabs
Subject = CN=QUT/C=AU/ST=QLD/L=Brisbane/O=QUT
Shared ciphers: AES256-SHA256
Current connection cipher AES256-SHA256
addr= 192.168.27.2, port=55598, cert_serial=46EE
issuer= C = AU, ST = ACT, O = QuintessenceLabs
Received **104 byte** message
Operation **Discover Versions succeeded**
Operation allowed by the action **policy**
Received **384 byte** message
operation= **Create**, addr=**192.168.27.2**, user=**client**
Operation allowed by **global rule**
Operation Create **succeeded**
Connection server stopped

Figure 7. The RFC5424 log-based metadata

RFC5424 [1] LOG-BASED DATASETS

2021.09.05.01.19.36,104,DiscoverVersions,192168272,client,policy,Success,320,Locate,192168272,client,owner,0,0,0,Success,Get,192168272,client,0,UIDexists,owner,0,Success,0

2021.09.05.01.19.37,104,DiscoverVersions,192168272,client,policy,Success,200,GetAttributes,192168272,client,0,UIDexists,owner,0,0,0,0,0,Success,0,0,0,0,0

2021.09.05.01.19.39,104,DiscoverVersions,192168272,client,policy,Success,224,AddAttribute,192168272,client,0,UIDexists,owner,0,0,0,0,0,Success,0,0,0,0,0

2021.09.04.01.40.07,104,DiscoverVersions,1921682722,client,policy,Success,200,GetAttributes,1921682722,client,0,UIDexists,owner,0,0,0,0,0,Success,0,0,0,0,0

2021.09.04.01.40.08,104,DiscoverVersions,192168272,leonie,policy,Success,224,AddAttribute,192168272,leonie,0,UIDexists,owner,0,0,0,0,0,Success,0,0,0,0,0

2021.09.04.01.40.08,104,DiscoverVersions,192168272,client,policy,Success,344,Locate,192168272,client,owner,0,0,0,Success,Revoke,192168272,client,0,UIDexists,owner,RevokefromActivetoDeactivated,0,Success

Figure 8. Sample datasets: training (top) and testing (bottom)

KMIP [2] TRAFFIC-BASED METADATA

REQUEST_MESSAGE:STRUCTURE(376):stru1
REQUEST_HEADER:STRUCTURE(56):stru2
PROTOCOL_VERSION:STRUCTURE(32):stru3
PROTOCOL_VERSION_MAJOR:INTEGER(4):1
PROTOCOL_VERSION_MINOR:INTEGER(4):4
BATCH_COUNT:INTEGER(4):1
REQUEST_BATCH_ITEM:STRUCTURE(304):stru2
OPERATION:ENUMERATION(4):CREATE
REQUEST_PAYLOAD:STRUCTURE(264):stru3
OBJECT_TYPE:ENUMERATION(4):SYMMETRIC_KEY
TEMPLATE_ATTRIBUTE:STRUCTURE(240):stru4
ATTRIBUTE:STRUCTURE(64):stru5
ATTRIBUTE_VALUE:STRUCTURE(40):stru6
ATTRIBUTE:STRUCTURE(48):stru6
ATTRIBUTE_VALUE:ENUMERATION(4):Cryptographic Algorithm
ATTRIBUTE:STRUCTURE(48):stru6
ATTRIBUTE_VALUE:INTEGER(4):12
ATTRIBUTE:STRUCTURE(48):stru6
ATTRIBUTE_VALUE:INTEGER(4):256

RESPONSE_MESSAGE:STRUCTURE(208):stru1
RESPONSE_HEADER:STRUCTURE(72):stru2
PROTOCOL_VERSION:STRUCTURE(32):stru3
PROTOCOL_VERSION_MAJOR:INTEGER(4):1
PROTOCOL_VERSION_MINOR:INTEGER(4):4
BATCH_COUNT:INTEGER(4):1
REQUEST_BATCH_ITEM:STRUCTURE(120):stru2
OPERATION:ENUMERATION(4):CREATE
RESULT_STATUS:ENUMERATION(4):SUCCESS
RESPONSE_PAYLOAD:STRUCTURE(64):stru3
OBJECT_TYPE:ENUMERATION(4):SYMMETRIC_KEY

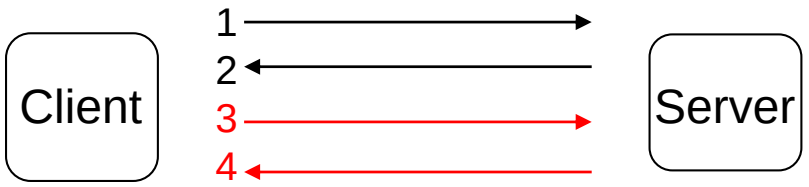

Figure 9. The KMIP traffic-based metadata

KMIP [2] TRAFFIC-BASED DATASETS

REQUESTMESSAGESTRUCTURE376stru1,STRUCTURE376stru1,STRUCTURE56stru2,STRUCTURE32stru3,INTEGER41,INTEGER44,INTEGER41,STRUCTURE304stru2,ENUMERATION4CREATE,STRUCTURE264stru3,ENUMERATION4SYMMETRICKEY,STRUCTURE240stru4,STRUCTURE64stru5,STRUCTURE40stru6,STRUCTURE48stru6,ENUMERATION4CryptographicAlgorithm,STRUCTURE48stru6,INTEGER412,STRUCTURE48stru6,INTEGER4256,0,0,0,0,0,0

RESPONSEMESSAGESTRUCTURE208stru1,STRUCTURE208stru1,STRUCTURE72stru2,STRUCTURE32stru3,INTEGER41,INTEGER44,INTEGER41,STRUCTURE120stru2,ENUMERATION4CREATE,ENUMERATION4SUCCESS,STRUCTURE64stru3,ENUMERATION4SYMMETRICKEY,0,0,0,0,0,0,0,0,0,0,0,0,0,0

REQUESTMESSAGESTRUCTURE312stru1,STRUCTURE312stru1,STRUCTURE88stru2,STRUCTURE32stru3,INTEGER41,INTEGER44,ENUMERATION4STOP,BOOLEAN8True,INTEGER42,STRUCTURE160stru2,ENUMERATION4LOCATE,STRUCTURE120stru3,STRUCTURE40stru4,ENUMERATION4ObjectType,STRUCTURE64stru4,STRUCTURE40stru5,STRUCTURE40stru5,ENUMERATION4ACTIVATE,STRUCTURE0stru6,0,0,0,0,0,0,0

RESPONSEMESSAGESTRUCTURE256stru1,STRUCTURE256stru1,STRUCTURE72stru2,STRUCTURE32stru3,INTEGER41,INTEGER44,INTEGER42,STRUCTURE56stru2,ENUMERATION4LOCATE,ENUMERATION4SUCCESS,STRUCTURE0stru3,STRUCTURE104stru3,ENUMERATION4ACTIVATE,ENUMERATION4OPERATIONFAILED,ENUMERATION4INVALIDMESSAGE,0,0,0,0,0,0,0,0,0,0,0

Figure 10. Sample datasets: training (top) and testing (bottom)

SUMMARY

- This research investigated EKM metadata, determined characteristics for extraction, and looked for possible patterns to detect anomaly.
- Demonstrated the possibility to detect anomalous activity within an organisation through events such as:
  - requests for key material of specific or unexpected sizes,
  - outside of normal time periods,
  - with unusual frequency,
  - or from abnormal locations.
- Additionally, this could be integrated with other enterprise information to sharpen detection capabilities.

CYBER SECURITY COOPERATIVE RESEARCH CENTRE
Queensland University of Technology
Quintessence Labs
CSIRO
DATA 61

Cyber Security Research Centre Limited
ABN 11 605 454 144
ceo@cybersecuritycrc.org.au
02 6103 9922

Thanks for your attention

Edith Cowan University
270 Joondalup Drive,
Joondalup WA 6027

cybersecuritycrc.org.au

REFERENCES

[1] The Syslog Protocol (https://datatracker.ietf.org/doc/html/rfc5424)

[2] Key Management Interoperability Protocol Specification (http://docs.oasis-open.org/kmip/spec/v1.4/kmip-spec-v1.4.html)