Detecting malware even when it is encrypted

Machine Learning for network HTTPS analysis

František Střasák
strasfra@fel.cvut.cz
@FrenkyStrasak

Sebastian Garcia
sebastian.garcia@agents.fel.cvut.cz
@eldracote

František Střasák

- Student
- CTU FEE Prague, Artificial Intelligence
- strasfra@fel.cvut.cz
- @FrenkyStrasak
- https://github.com/frenky-strasak/HTTPSDetector

Photo

CZECH TECHNICAL UNIVERSITY IN PRAGUE

FACULTY OF ELECTRICAL ENGINEERING

Sebastian Garcia

- Researcher and lecturer
- CTU FEE Prague, Department of computer science
- Founder and head of Stratosphere IPS (https://stratosphereips.org)
- sebastian.garcia@agents.fel.cvut.cz
- @eldracote

CZECH TECHNICAL UNIVERSITY IN PRAGUE

FACULTY OF ELECTRICAL ENGINEERING

Introduction

- Over half of global web traffic is encrypted
    - https://transparencyreport.google.com/https/overview
    - https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web
    - https://letsencrypt.org/stats/

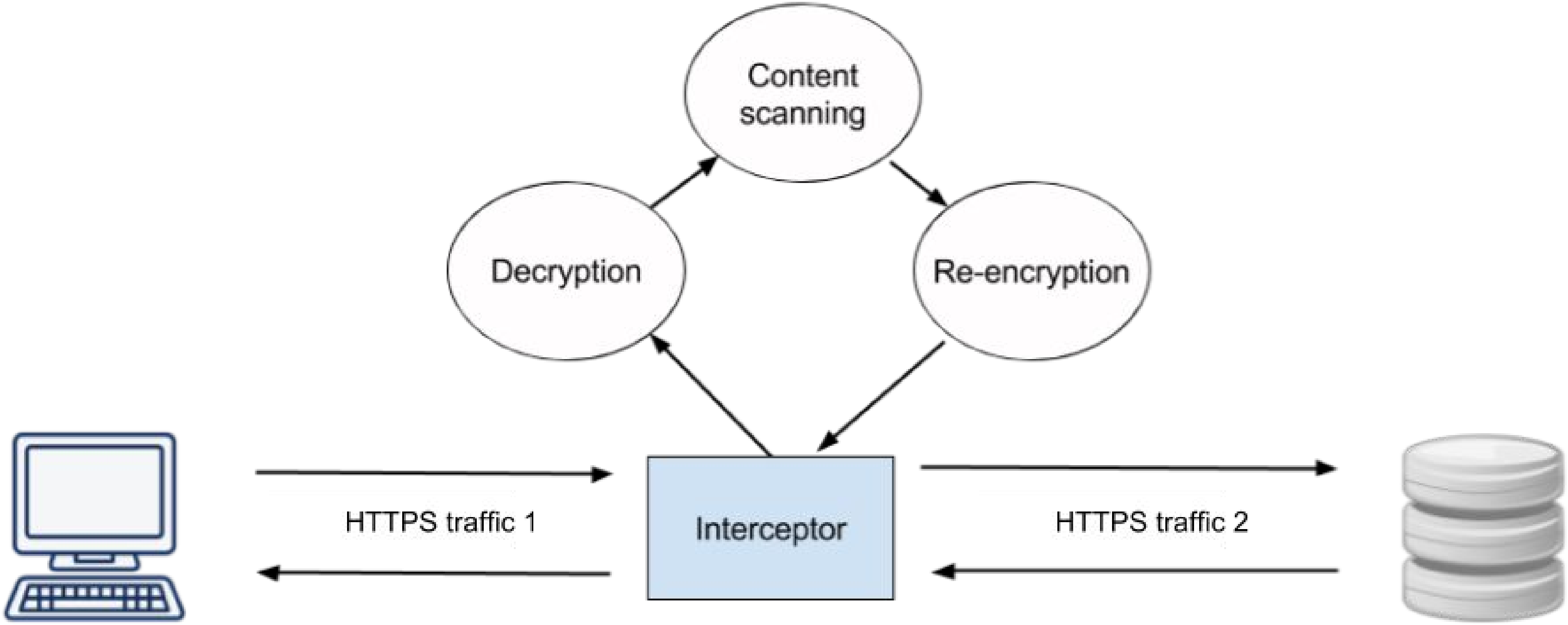
Introduction

- 10% - 40% of all malware traffic is encrypted
  - https://blogs.cisco.com/security/malwares-use-of-tls-and-encryption
  - https://blog.cyren.com/articles/over-one-third-of-malware-uses-https

Problem

- The encryption interferes with the efficacy of classical detection techniques

TLS inspection



TLS inspection

- Advantages
  - TLS inspection can use classical detection techniques
- Disadvantages
  - TLS inspection can be expensive
  - TLS inspection is computationally demanding (can be slow)
  - TLS inspection does not respect the original idea of HTTPS (privacy)

Without decryption

- Find and discover new features and methods to detect malware without decrypting the traffic

Without decryption

- Advantages
  - No SSL inspection
- Disadvantages
  - The need to discover new features and methods

Goal

- To detect the malware HTTPS traffic without decryption with high accuracy, low false positive rate and false negative rate

Goal

- True Positive (TP) - “we predicted **malware** and it is **malware**”
- True Negative (TN) - “we predicted **normal** and it is **normal**”
- False Positive (FP) - “we predicted **malware** and it is **normal**”
- False Negative (FN) - “we predicted **normal** and it is **malware**”

Accuracy = (TP + TN) / (TP + TN + FP + FN)

False Positive Rate = FP / (FP + TN)

False Negative Rate = FN / (FN + TP)

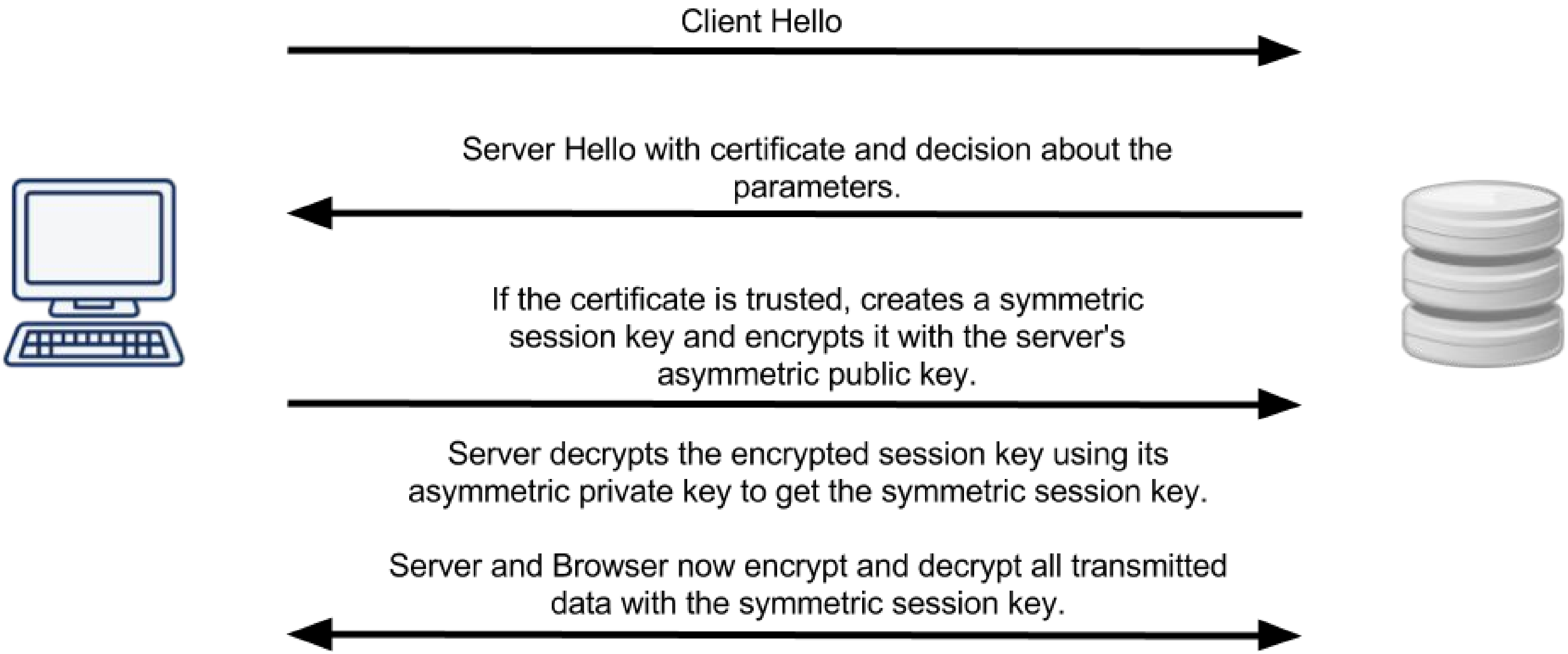
HTTPS

- HTTPS = HTTP + SSL/TLS
- Verifying that you are talking directly to the correct server
- Ensuring that only the server can read what you send and only you can read what it sends back

SSL/TLS handshake

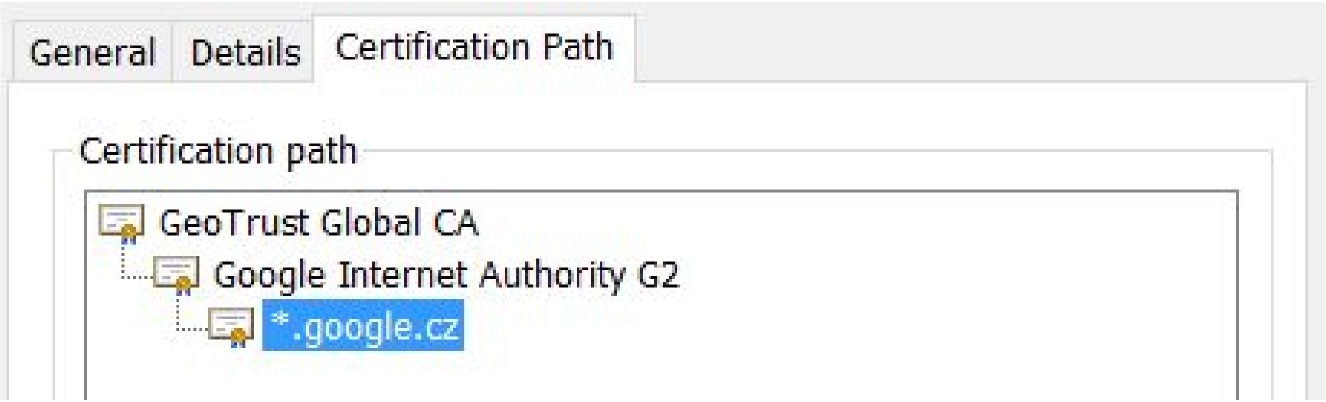
- Client and server Hello
- Certificate Exchange
- Key Exchange

SSL/TLS handshake



Certification path

- A root CA
- An intermediate CA

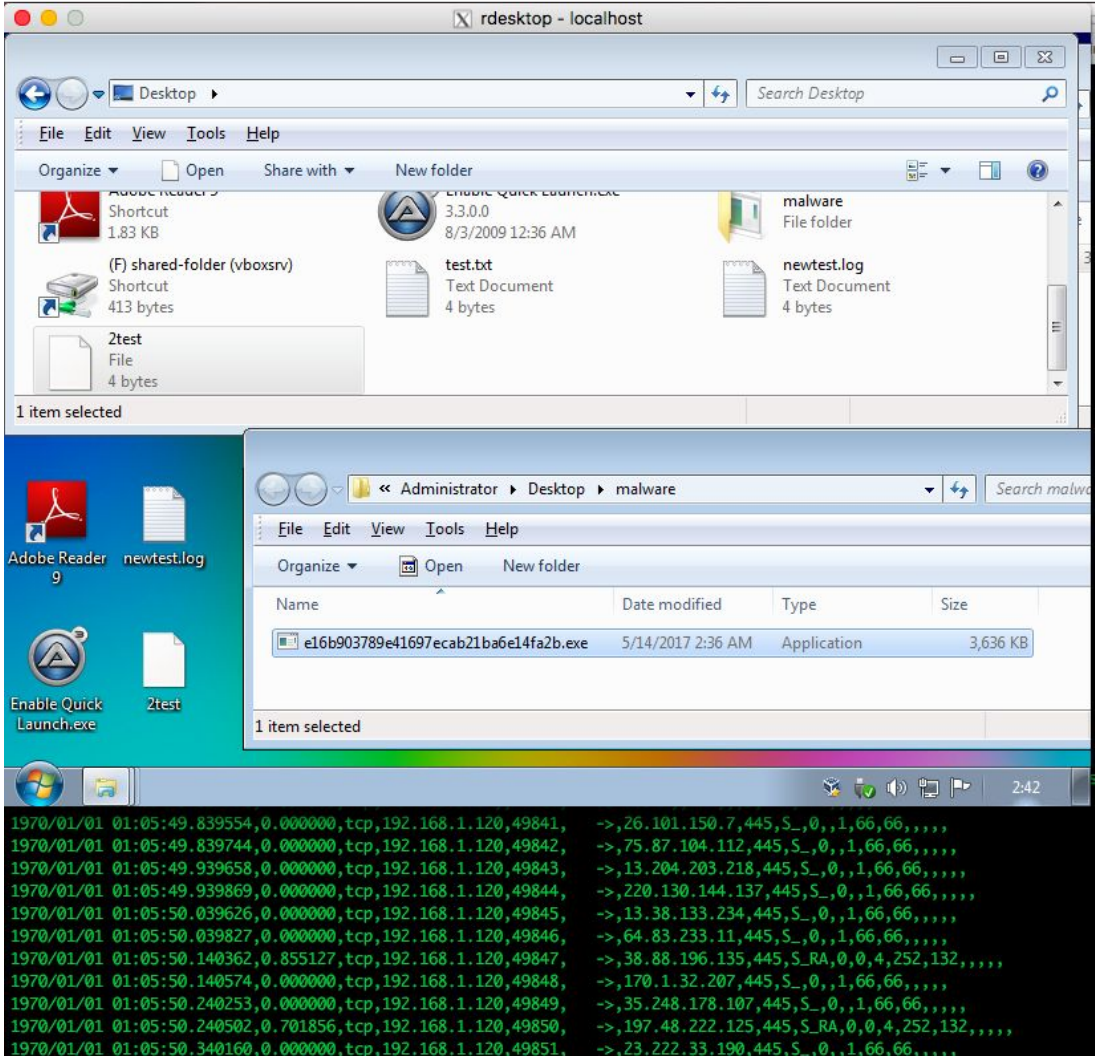


Privacy does not mean Security!

Dataset

Dataset

- Flows with HTTPS traffic
- Malware and Normal
- 4 sub dataset
- 163 malware and normal captures



Dataset

- CTU-13 dataset - public
  - Malware and Normal captures
  - An Empirical Comparison of Botnet Detection Methods research
  - http://mcfp.weebly.com/the-ctu-13-dataset-a-labeled-dataset-with-botnet-normal-and-background-traffic.html

- MCFP dataset - public
  - Malware and Normal captures
  - Malware Capture Facility Project
  - https://stratosphereips.org/category/dataset.html

Dataset

- Own normal dataset - public
  - Normal captures
  - 3 days of accessing to secure sites (Alexa 1000)
  - Google, Facebook, Twitter accounts
  - https://stratosphereips.org/category/dataset.html

- Normal CTU dataset - almost public
  - Normal captures
  - 22 known and trusted people from department of FEE CTU

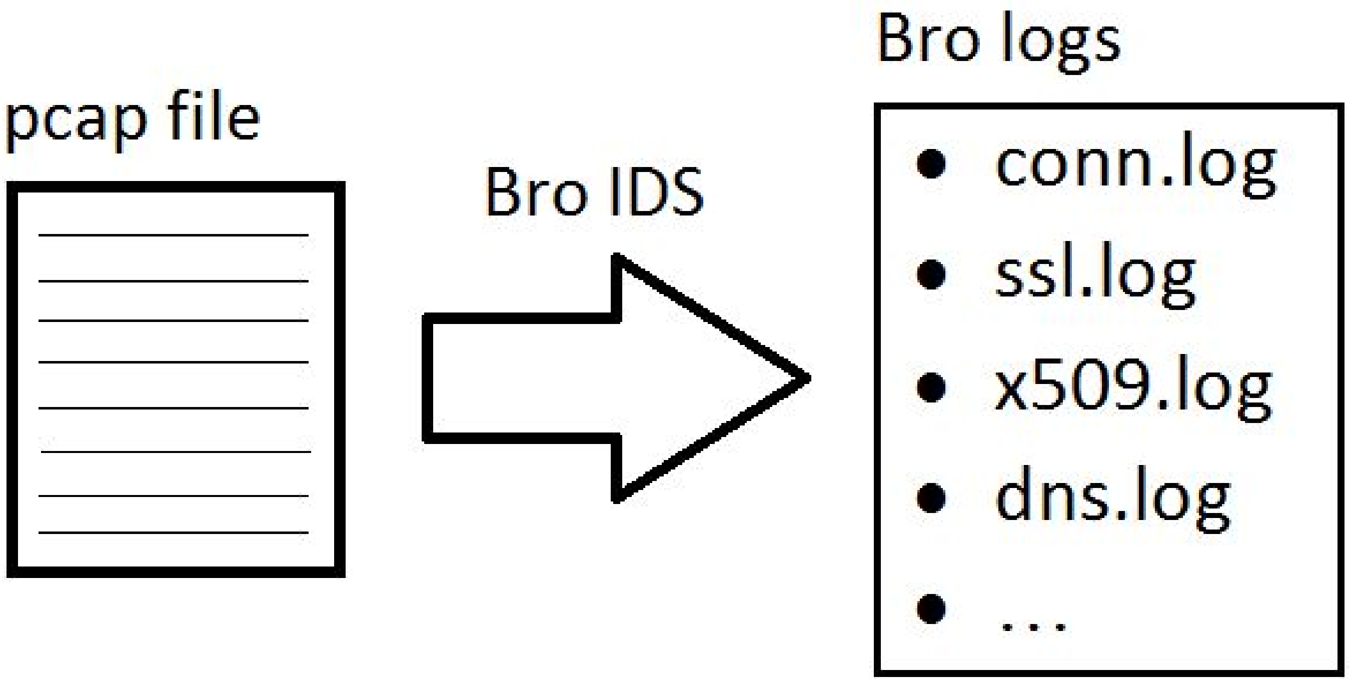
Dataset

- Size of log files in dataset (include background):
  - Normal: 331 GB
  - Malware: 44 GB
  - Total: 375 GB
- All SSL/TLS flows:
  - Normal: 1,357,112
  - Malware: 552,919
  - Total: 1,910,031
- All unique certificates:
  - Normal: 7,040
  - Malware: 1,579
  - Total: 8,619

Most of datasets are public!

Features and Methods

Bro logs



https://www.bro.org/

conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
  - Source and destination IP and Ports

conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
    - Source and destination IP and Ports
    - Number of packets
    - Number of bytes

conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
  - Source and destination IP and Ports
  - Number of packets
  - Number of bytes
  - Timestamp

conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
  - Source and destination IP and Ports
  - Number of packets
  - Number of bytes
  - Timestamp
  - State of connection

conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
  - Source and destination IP and Ports
  - Number of packets
  - Number of bytes
  - Timestamp
  - State of connection
  - Duration

ssl.log

- SSL/TLS handshake info
- Some of the available data:
    - Version of SSL/TLS
    - Ciphersuite

ssl.log

- SSL/TLS handshake info
- Some of the available data:
  - Version of SSL/TLS
  - Ciphersuite
  - Server name

ssl.log

- SSL/TLS handshake info
- Some of the available data:
  - Version of SSL/TLS
  - Ciphersuite
  - Server name
  - Certificate path

Certificate path

ssl.log

SSL records

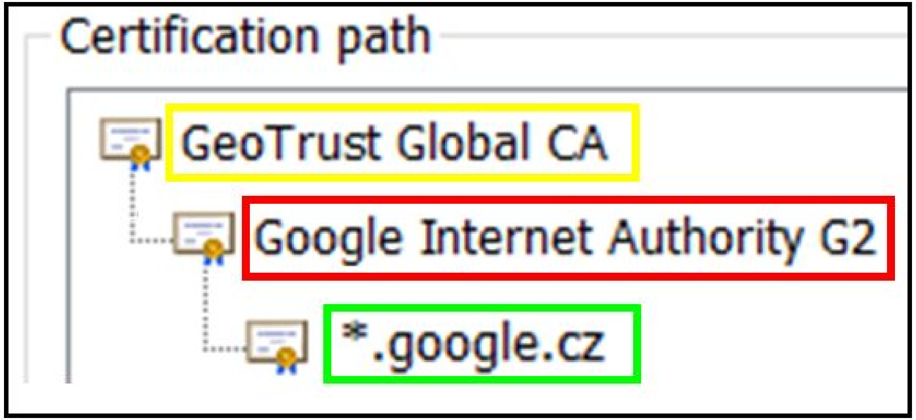
					Certificate path
3511.617809	Ctgc353XKjtCwYMPXd	10.0.2.109	443	TLSv10	FlseAT2YTTirnFNwwa,FtLQ4i1LMP06OKenK9,FzMJtN2WvGLBJQmAde
3652.492566	Cfb2BM3PUzkFjD4L22	10.0.2.109	443	TLSv10	fyqU32jvPwlbeg8Sd,FmYVTL3wUsvW6p0Ko8
3654.509631	CeZN8N3d5uxTGKh51g	10.0.2.109	443	TLSv10	-

x509.log

Certificate records

3504.673635	FlCtgE1o1S0RuoUafe	3	02FC2E
3511.621231	FlseAT2YTTirnFNwwa	3	0D335238E52B18BE
3511.736478	FtLQ4i1LMP06OKenK9	3	0676549500C6A380
3513.557920	FzMJtN2WvGLBJQmAde	3	7C653E7DFE20BF0E
3513.573938	F5v6ic30yxSRz40Fvf	3	49853ED8F7165597

Certificate path in Google Chrome



x509.log

- X.509 certificate info
- Some of the available data:
    - Serial number

x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name

x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
  - Validity of the certificate

x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
  - Validity of the certificate
  - Public key

x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
  - Validity of the certificate
  - Public key
  - Signature algorithm name

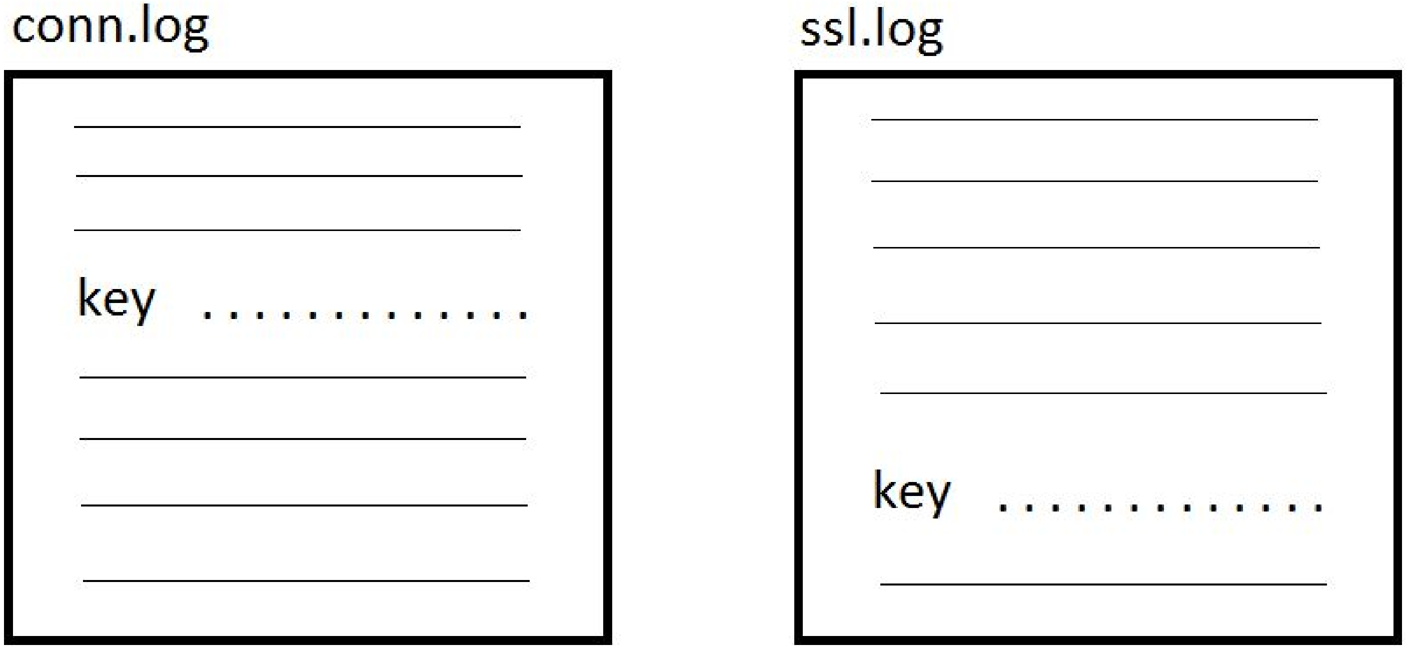
x509.log

- X.509 certificate info
- Some of the available data:
    - Serial number
    - Common name
    - Validity of the certificate
    - Public key
    - Signature algorithm name
    - Issuer

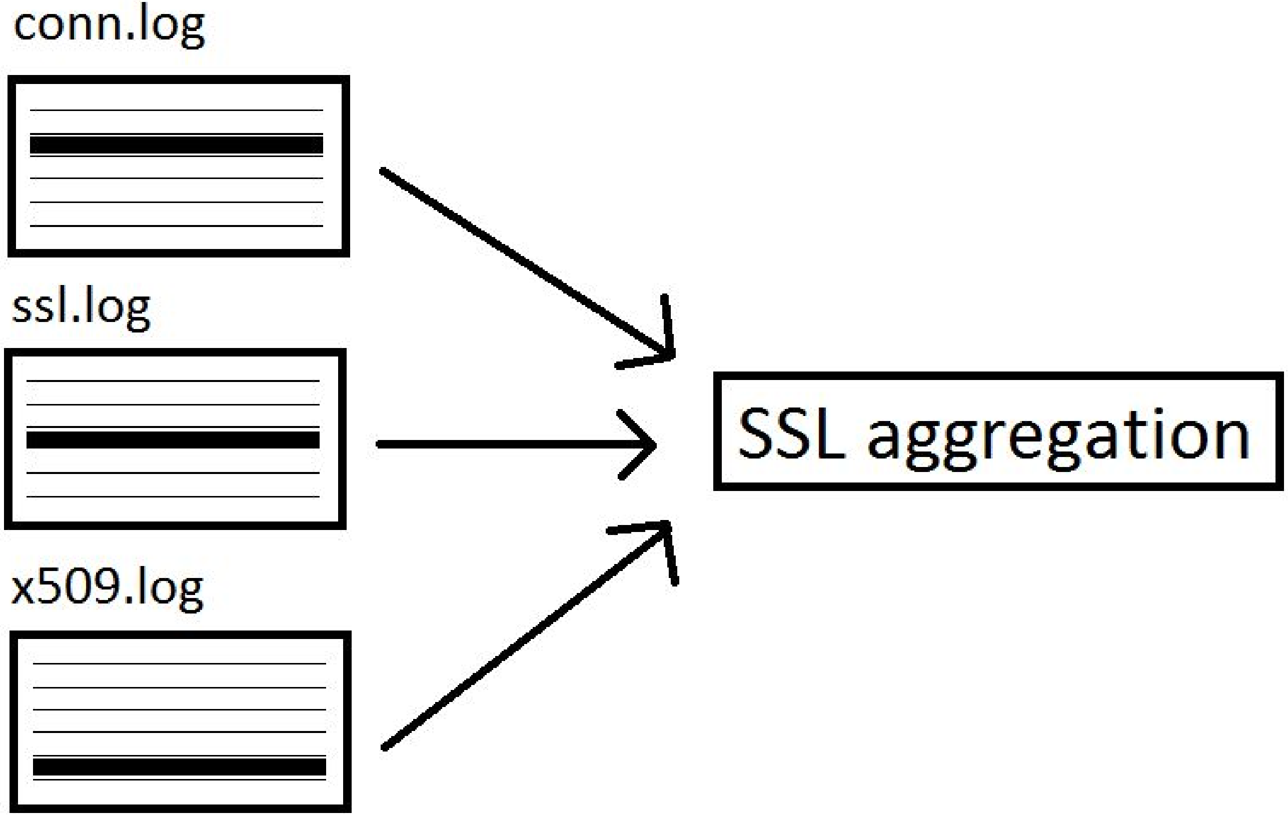
x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
  - Validity of the certificate
  - Public key
  - Signature algorithm name
  - Issuer
  - SAN DNS (Subject alternative name extension of the certificate)

Interconnection of logs



SSL aggregation



SSL aggregation

conn.log

131.728991	CgFZEv44vwsP9QlnR6	10.0.2.15	49163	104.108.46.209	80	tcp	http
128.944596	CK8hoP3M4XoQDJSxRi	10.0.2.15	49162	52.222.174.197	80	tcp	http
132.428808	Cjkwxu3NuUE41WTAB	10.0.2.15	49167	52.222.171.204	443	tcp	ssl
132.428083	C0wDNN17bO5uKwO7kf	10.0.2.15	49166	52.222.171.204	443	tcp	ssl
132.430278	CFQBuv4I7yFo9h3tP6	10.0.2.15	49169	52.222.171.204	443	tcp	ssl

ssl.log

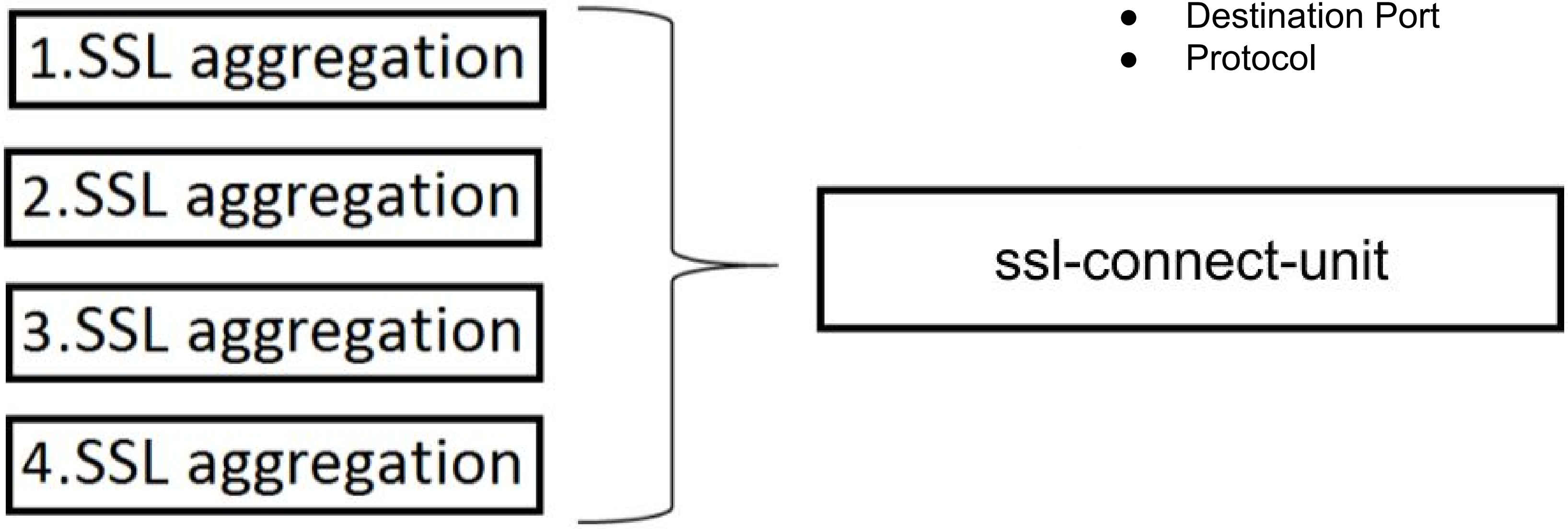
132.478442	Cjkwxu3NuUE41WTAB	10.0.2.15	443	TLSv12	FA8t03GcfncuIzHUd,FKbqgmdc7kcsRbYHi
132.481833	CFQBuv4I7yFo9h3tP6	10.0.2.15	443	TLSv12	FIbw2G14fJaazLLjoc,FKbqgmdc7kcsRbYHi
132.483473	CHPgsdopxgJIkZpxl	10.0.2.15	443	TLSv12	-
132.495937	CIPPIMsm5VQsGp4Si	10.0.2.15	443	TLSv12	-
132.494901	CAfZdW3MYCnWgYbuv9	10.0.2.15	443	TLSv12	FCA9ID2CxKqL6GqUgh,FRb04E41gABeDidrCi

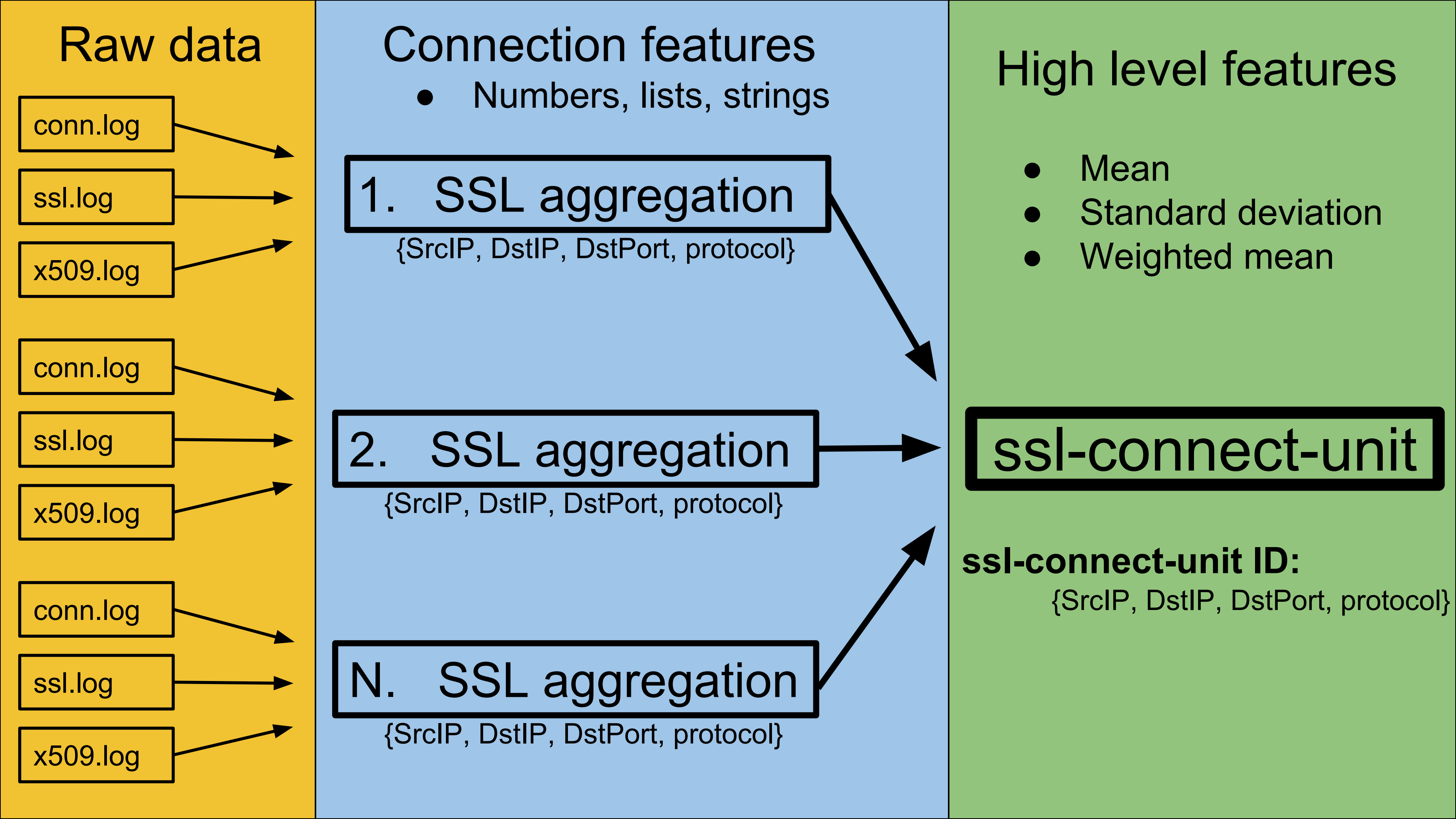
x509.log

132.527217	FmF1bg1sqhde52Xjyh	3	0CA9C64361BFC92A79B1DD9CFB9E48EC	CN=
132.527217	FzYrZo28CimnSKCR01	3	01FDA3EB6ECA75C888438B724BCFBC91	CN=
133.579209	FA8t03GcfncuIzHUd	3	5A000529CF2A5A6396D3FD74EC0001000529CF	
133.579209	FKbqgmdc7kcsRbYHi	3	0727AA47	CN=Microsoft IT SSL SHA2,OU
134.111336	FIbw2G14fJaazLLjoc	3	5A000529CF2A5A6396D3FD74EC0001000529CF	

ssl-connect-unit

ssl-connect-unit ID:
- Source IP
- Destination IP
- Destination Port
- Protocol

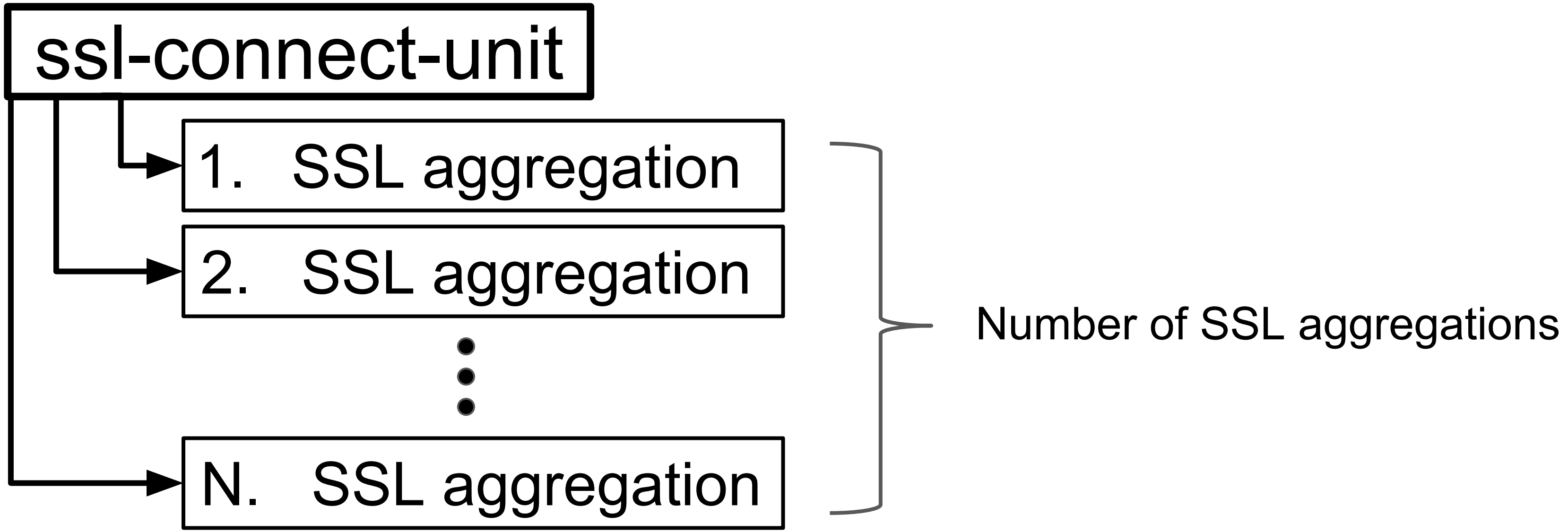



Raw data
conn.log
ssl.log
x509.log
conn.log
ssl.log
x509.log
conn.log
ssl.log
x509.log
Connection features
Numbers, lists, strings
1. SSL aggregation
{SrcIP, DstIP, DstPort, protocol}
2. SSL aggregation
{SrcIP, DstIP, DstPort, protocol}
N. SSL aggregation
{SrcIP, DstIP, DstPort, protocol}
High level features
Mean
Standard deviation
Weighted mean
ssl-connect-unit
ssl-connect-unit ID:
{SrcIP, DstIP, DstPort, protocol}

High level features

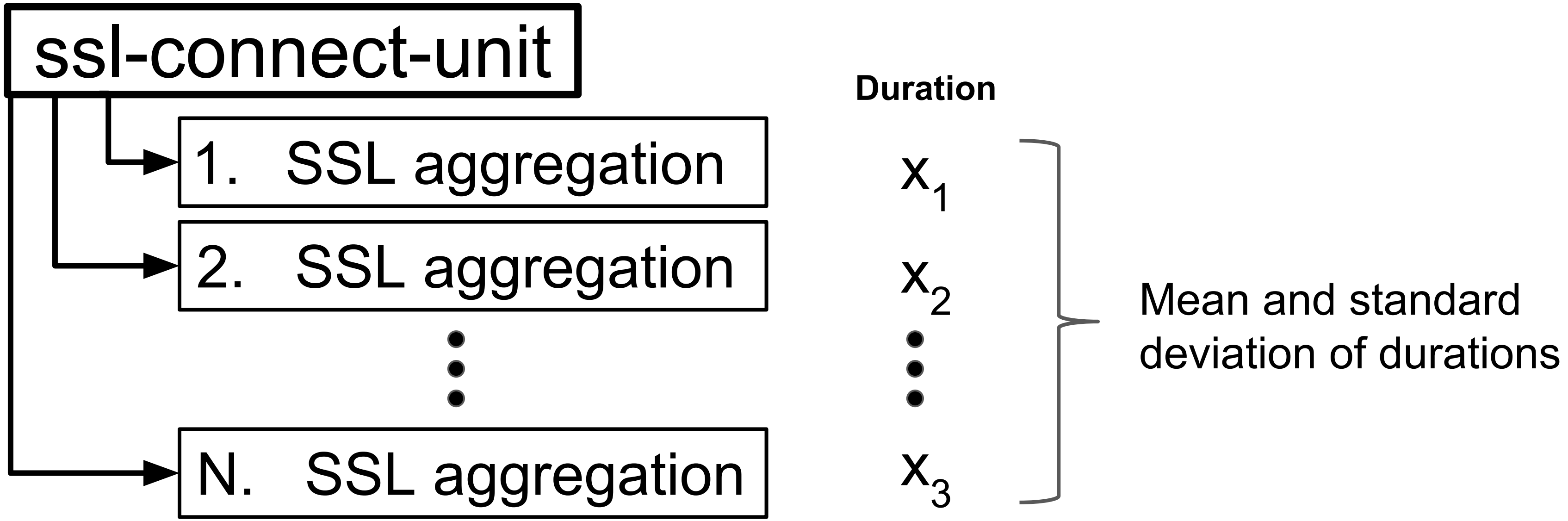
- 40 different features

1. Number of SSL aggregations



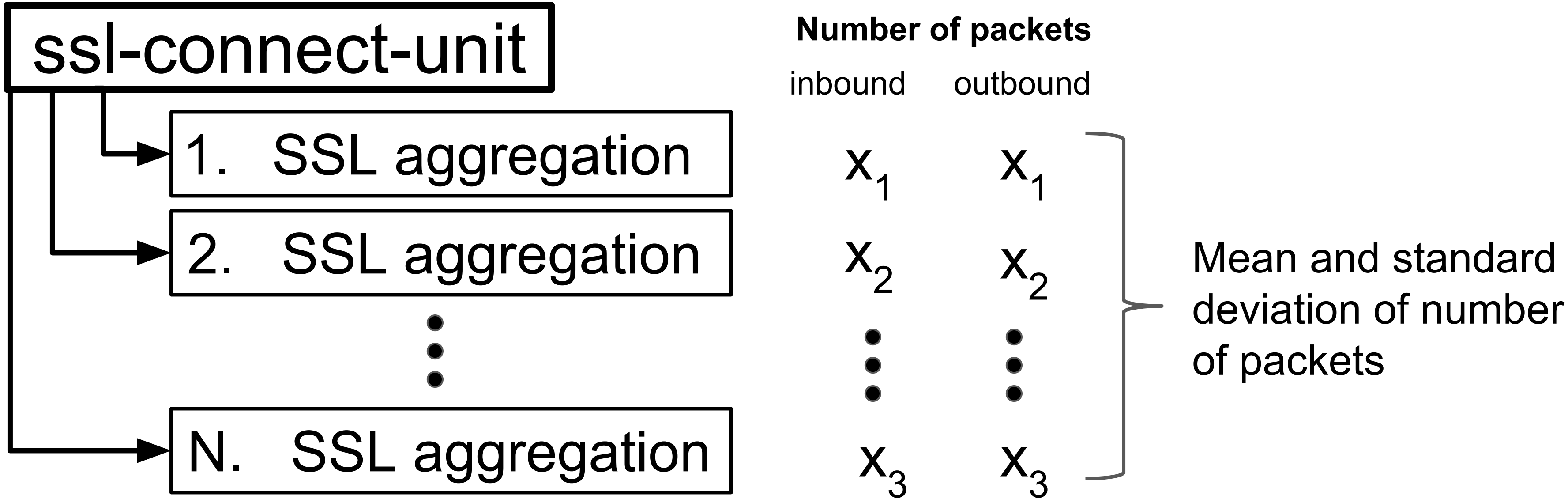
2. Mean of duration

3. Standard deviation of duration

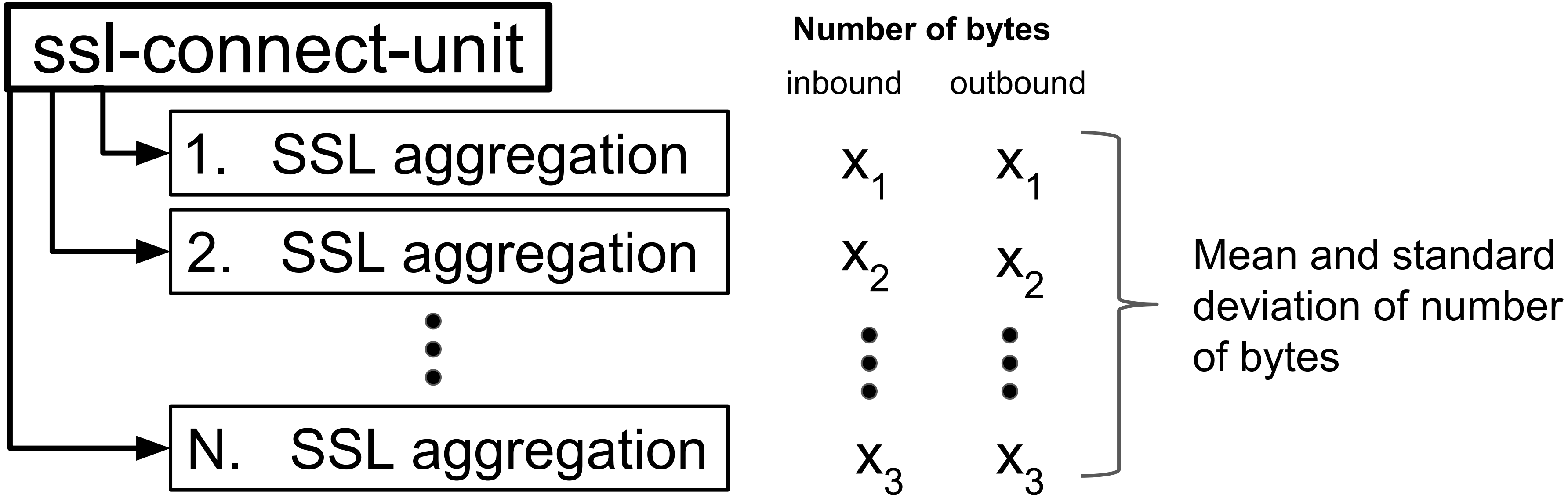


4. Mean of number of packets

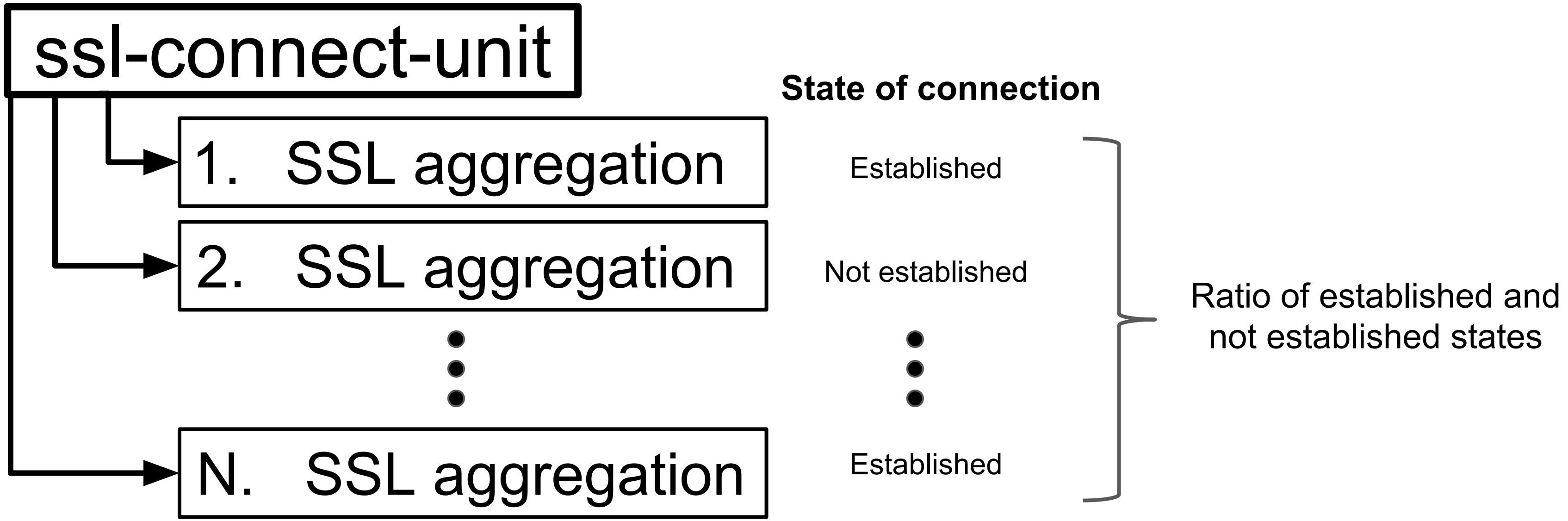
5. Standard deviation of number of packets



6. Mean of number of bytes
7. Standard deviation of number of bytes

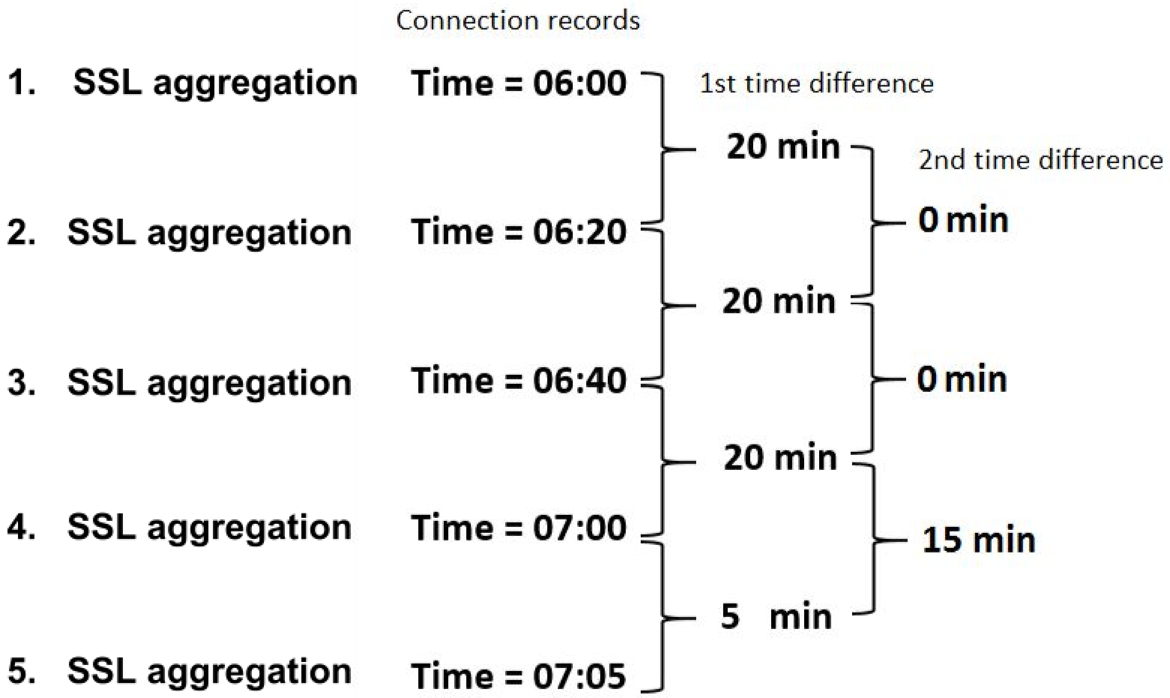


8. Ratio of established and not established states

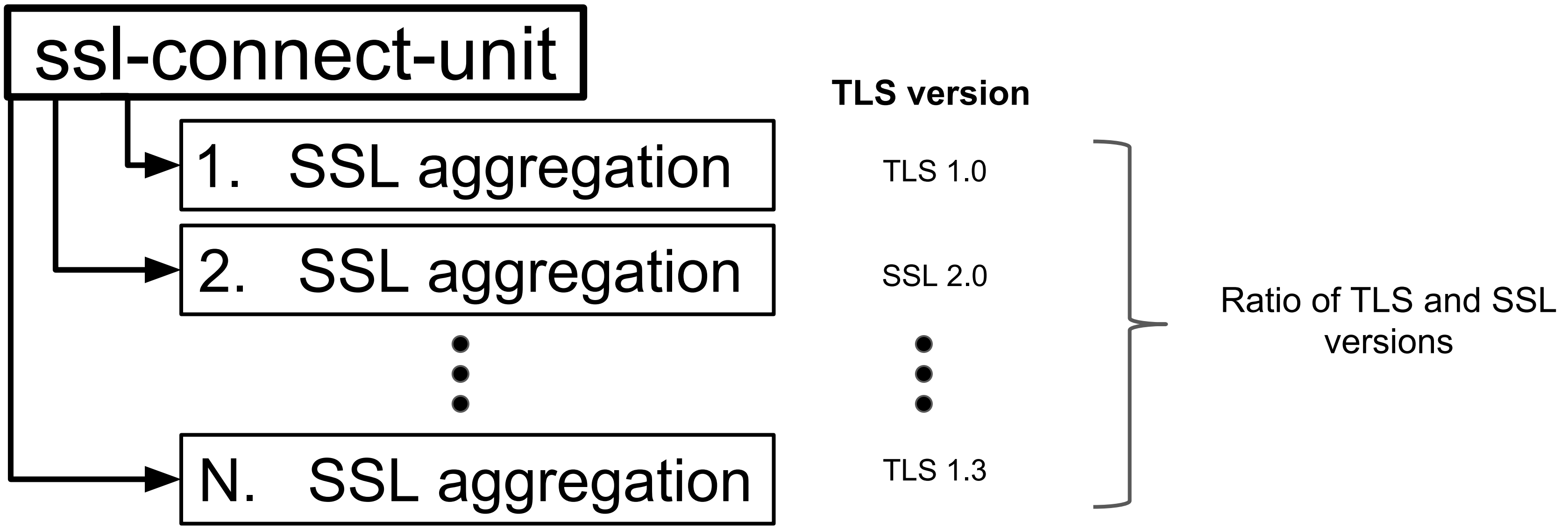


9. Mean of 2nd level time difference

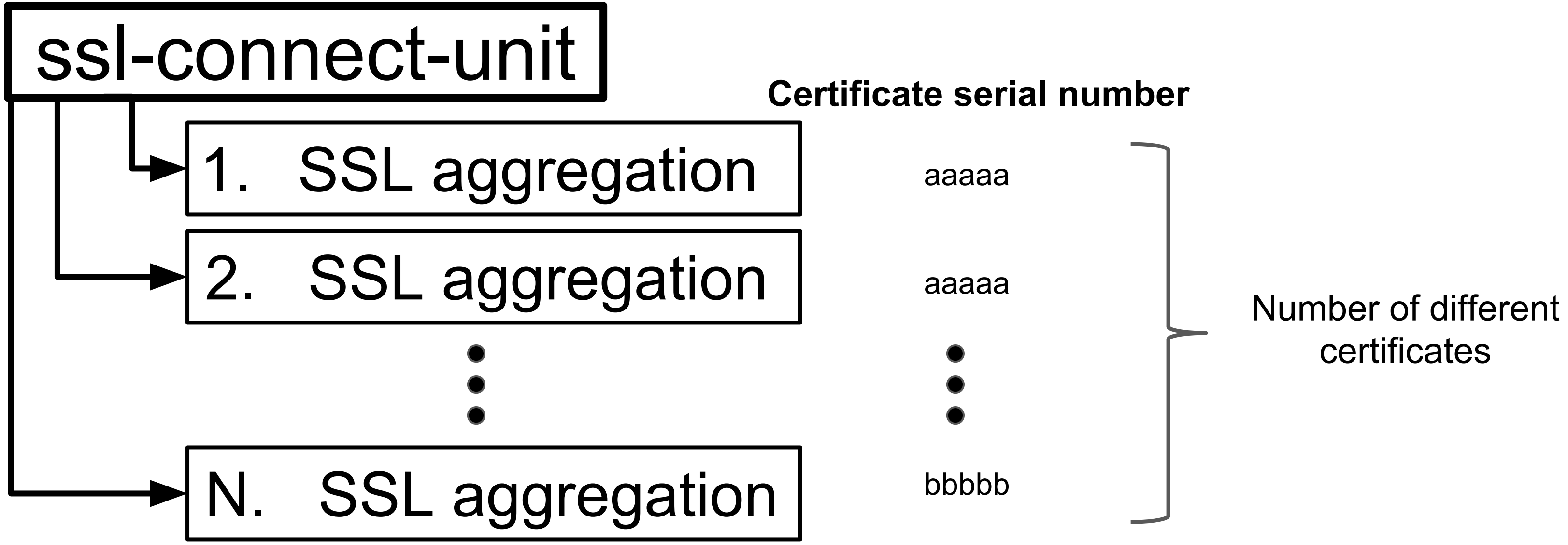
10. Standard deviation of 2nd level time difference



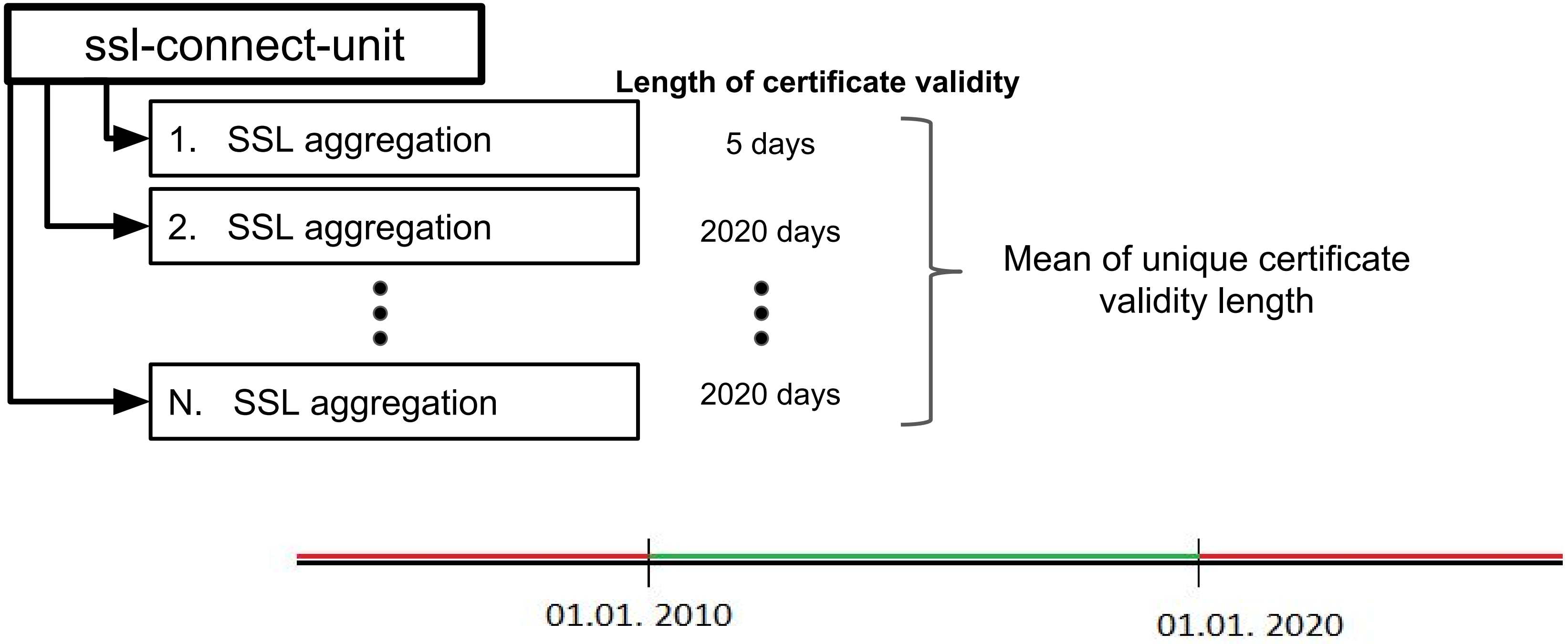
11. Ratio of TLS and SSL version



12. Number of different certificates

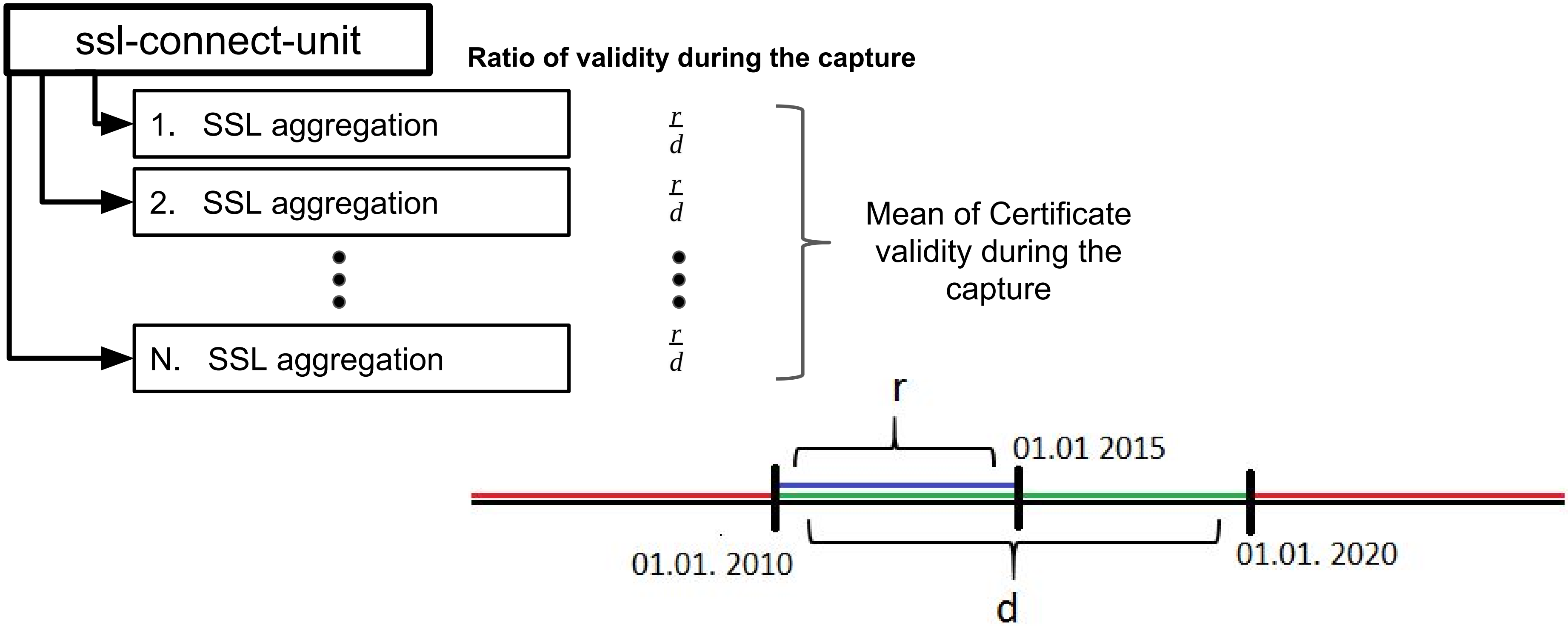


13. Mean of certificate validity length
14. Standard deviation of certificate validity length

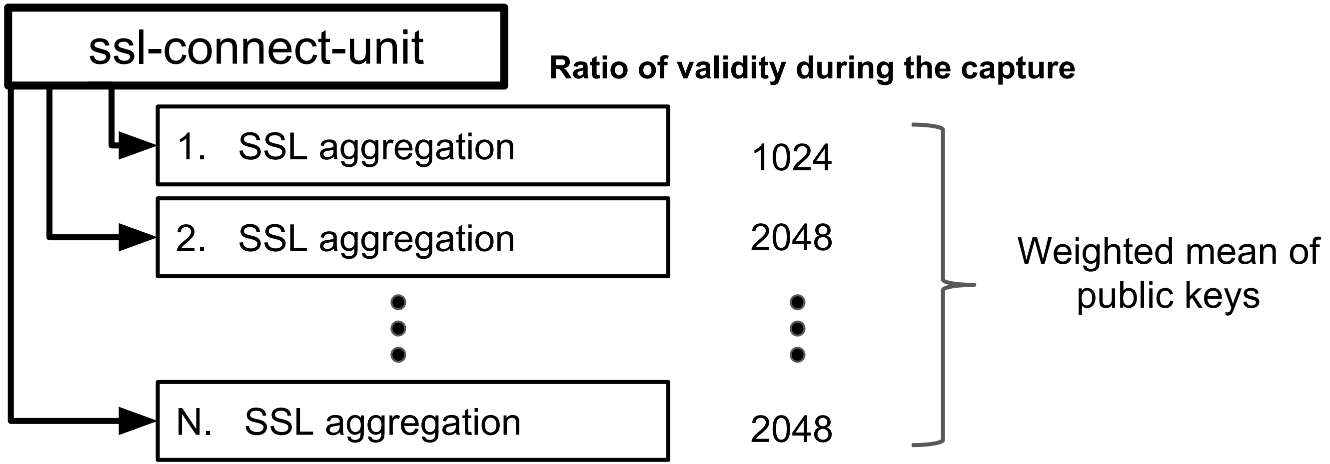


15. Mean of certificate validity during the capture

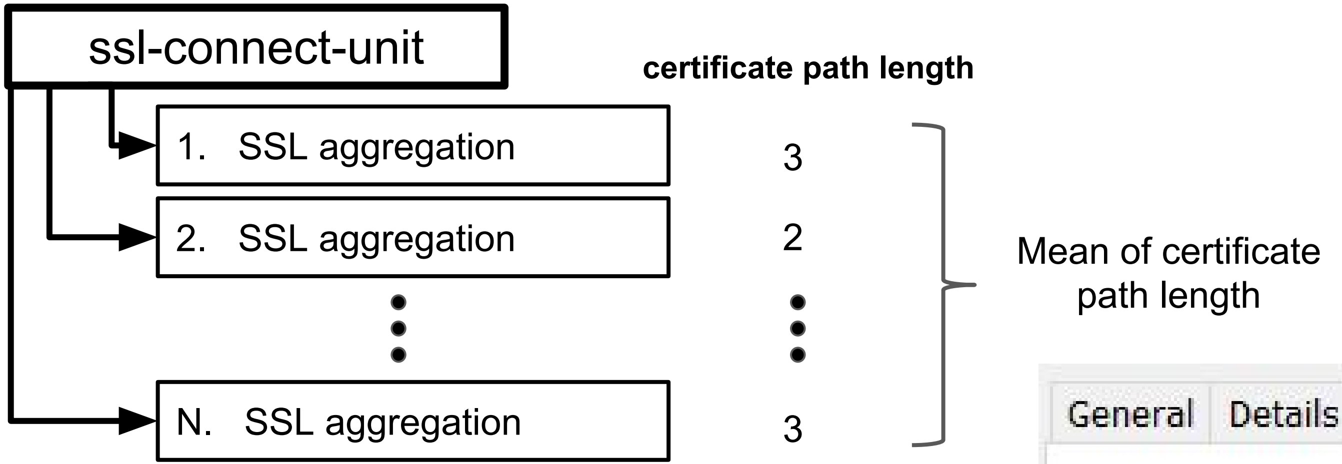
16. Standard deviation of certificate validity during the capture

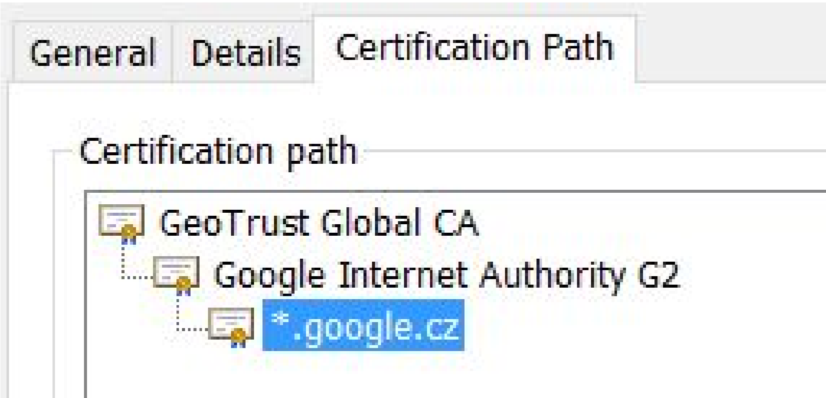


17. Weighted mean of public keys



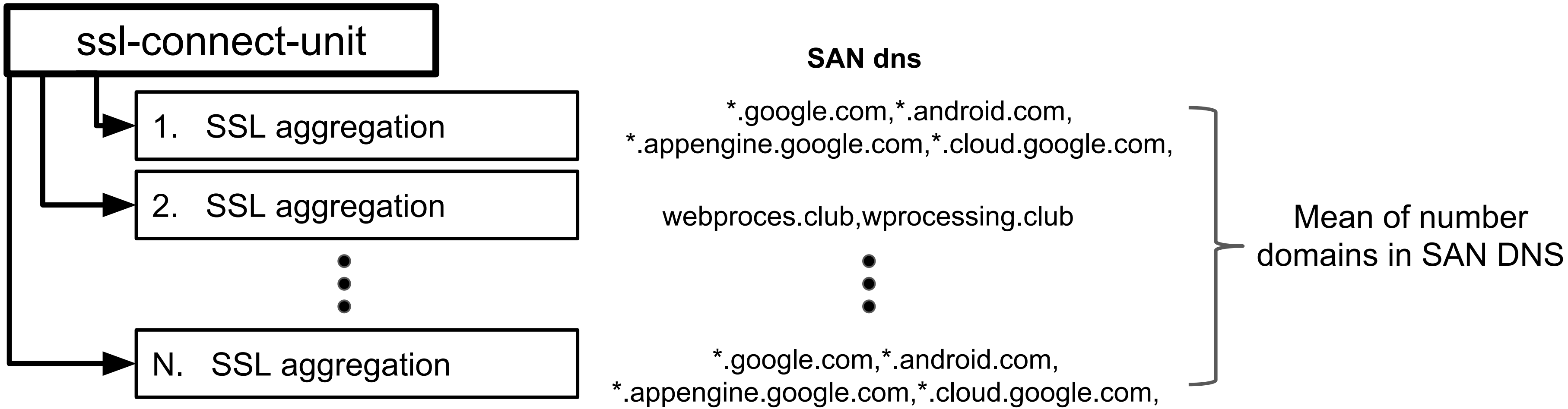
18. Mean of certificate path length
19. Standard deviation of certificate path length



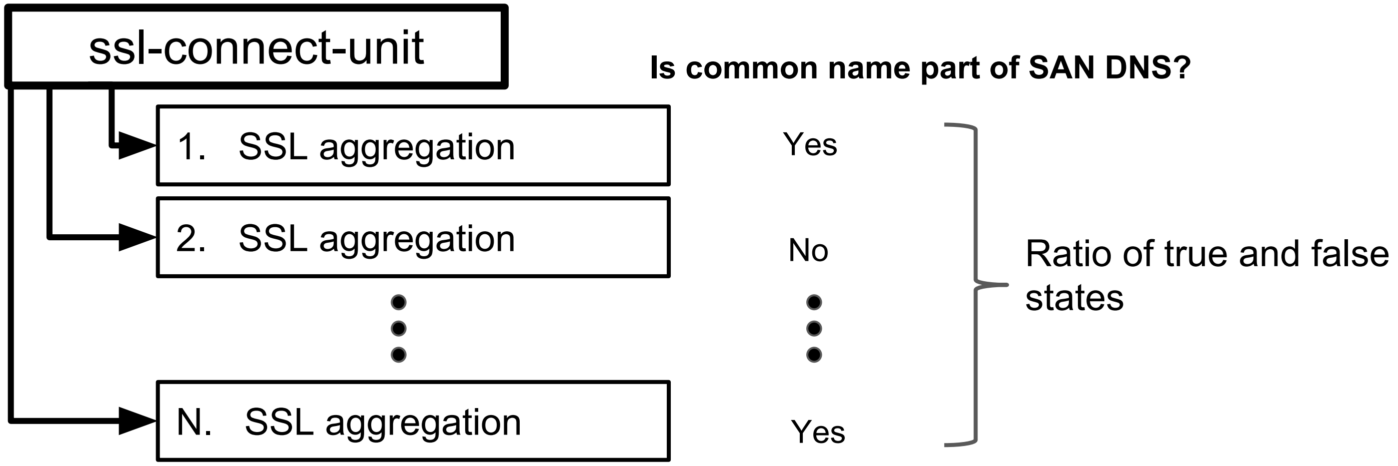


20. Mean of number of domains in SAN DNS

21. Standard deviation of number of domains in SAN DNS



22. Ratio of common name and SAN DNS



Data model

ssl-connect-unit	40 features					Label
{ 10.0.2.15, 54.201.174.90, 443, tcp }	f1	f2	f3	…	f40	Normal
{ 10.0.2.109, 173.194.122.30, 443, tcp }	f1	f2	f3	…	f40	Malware
⋮						

Normal dataset

- All ssl-connect-units:
  - Normal: 46,387
  - Malware: 8,313
- All SSL-aggregation:
  - Normal: 1,357,112
  - Malware: 552,919
- All unique certificates:
  - Normal: 7,040
  - Malware: 1,579

Machine learning algorithms

XGBoost

- Extreme Gradient Boosting
- Tree booster with logistic regression
- Parameters:
  - max depth — describe maximum depth of a tree
  - gamma — minimum loss reduction required to make a further partition on a leaf node of the tree.
  - min child weight — minimum sum of instance weight (hessian) needed in a child.

Random forest

- Random Forest Classifier model that is an estimator that fits a number of decision tree classifiers on various sub-samples

Neural Network

- MLP Classifier (Multi-layer Perceptron classifier)
- stochastic gradient descent with Adam (Adaptive Moment Estimation)

SVM

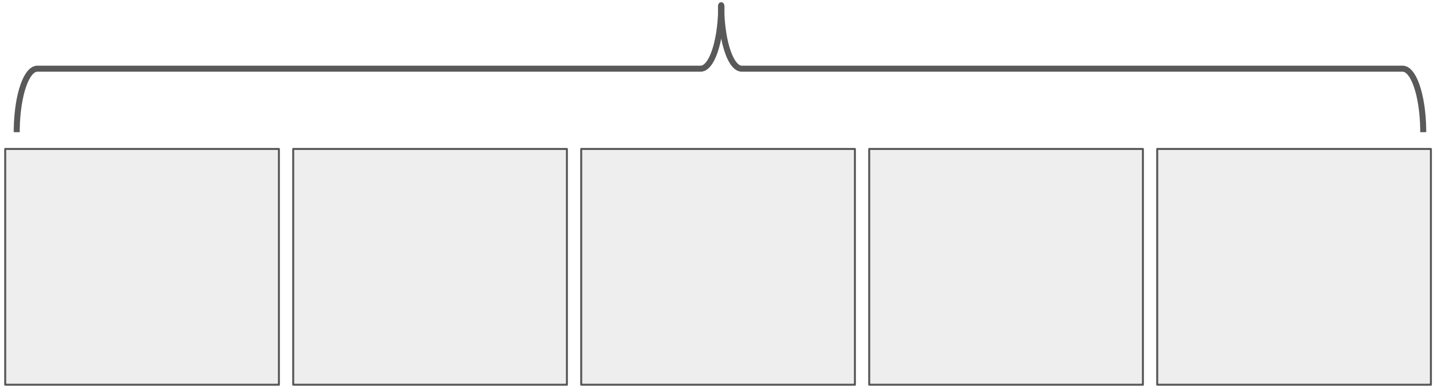
- Radial Basis Function (RBF) kernel
- perform a non-linear classification using the kernel trick, mapping inputs into high-dimensional feature spaces

Experiments

Experiments

1. Split dataset to N same subsets

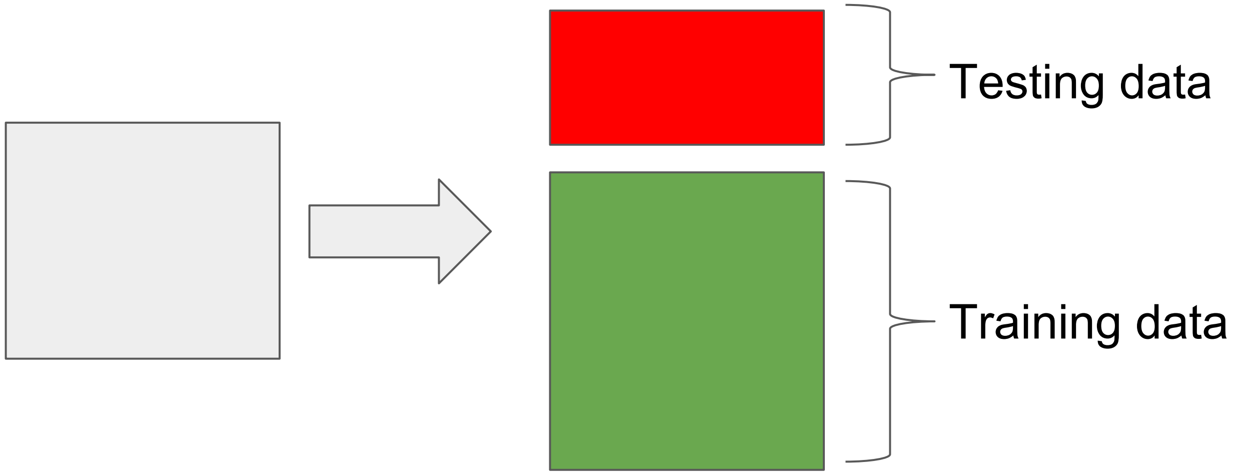
N subsets



- Each subset contains unique malware test data

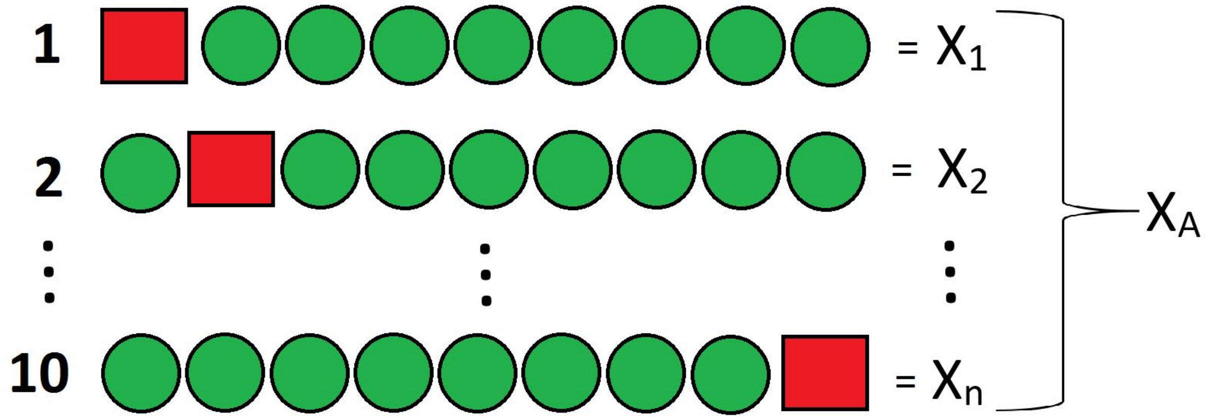
Experiments

1. Split dataset to N same subsets
2. For each subset:
    a. Split subset for training and testing data



Experiments

1. Split dataset to N same subsets
2. For each subset:
    a. Split subset for training and testing data
    b. Cross Validation on training data



Experiments

1. Split dataset to N same subsets
2. For each subset:
    a. Split subset for training and testing data
    b. Cross Validation on training data
    c. Train on all training data and test on test data

Experiments

1. Split dataset to N same subsets
2. For each subset:
   a. Split subset for training and testing data
   b. Cross validation on training data
   c. Train on all training data and test on testing data
3. Final result is an average of all results in subsets

Measures

Accuracy = (TP + TN) / (TP + TN + FP + FN)

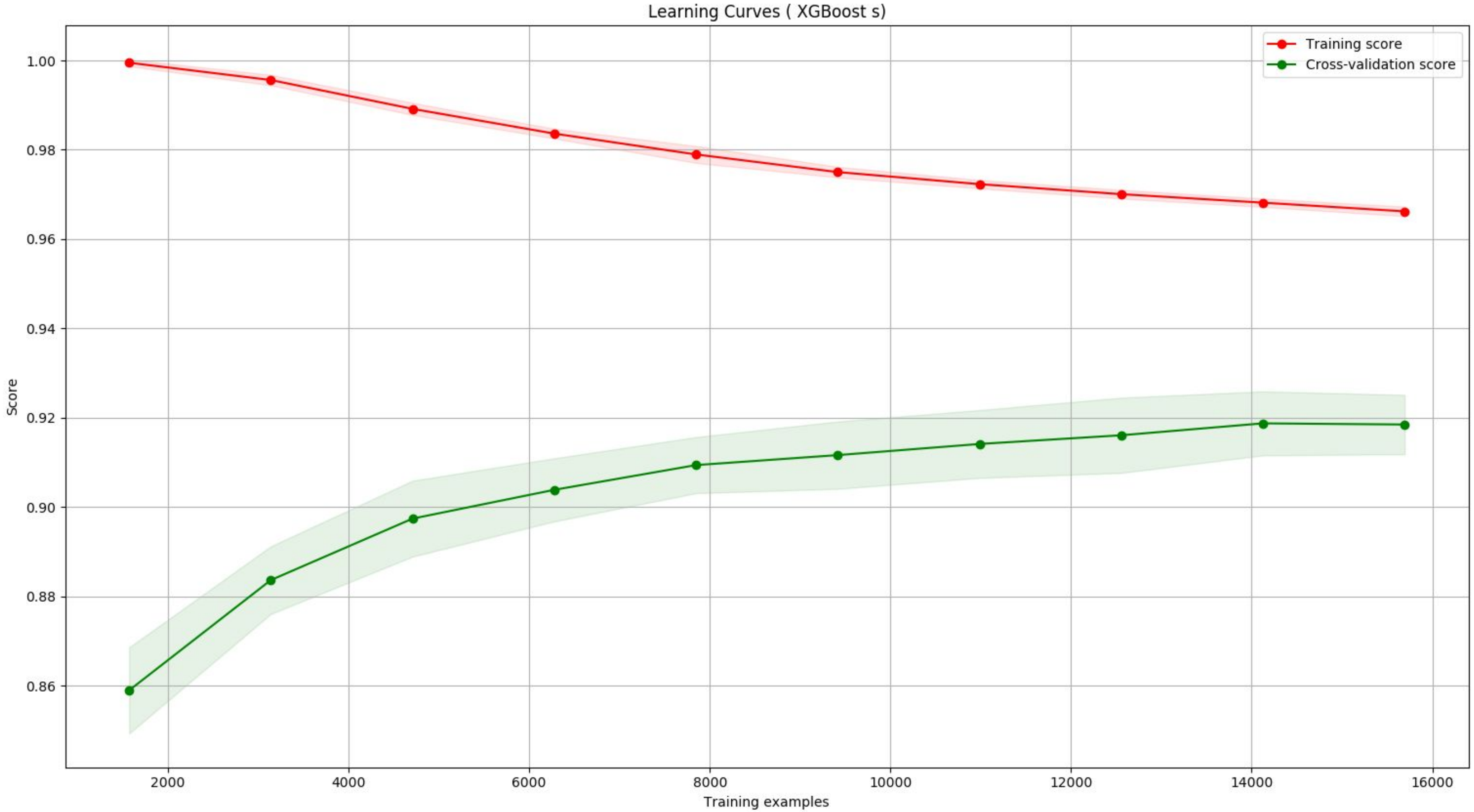
False Positive Rate = FP / (FP + TN)

False Negative Rate = FN / (FN + TP)

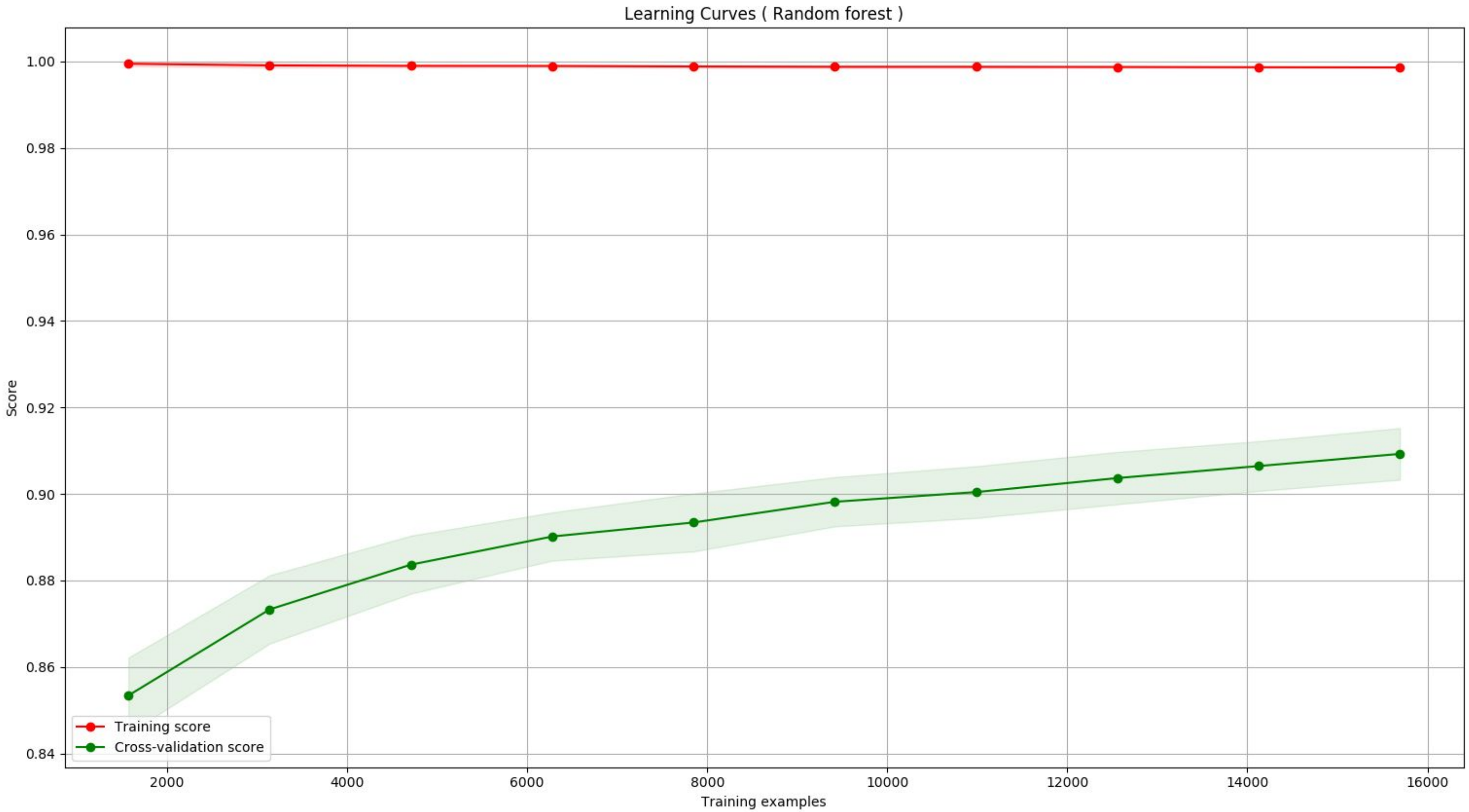
Sensitivity = TP / (TP + FN)

F1 score = 2TP / (2TP + FP + FN)

Learning curve - XGBoost



Learning curve - Random Forest



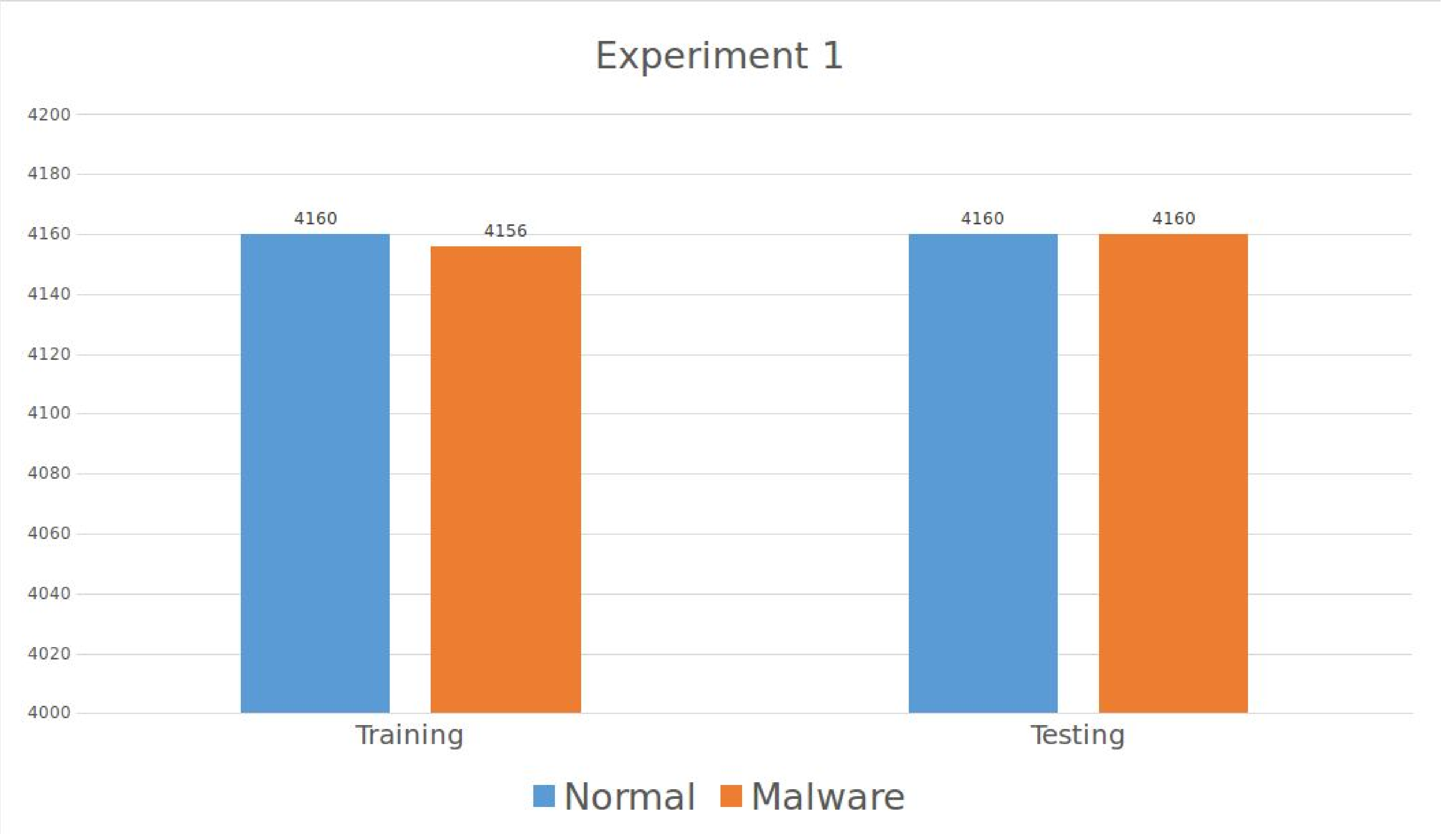
Experiment 1

Experiment 1

- Subset 1
  - Training
    - Normal: 4,160 ssl-connect-units
    - Malware: 4,156 ssl-connect-units
  - Testing
    - Normal: 4,160 ssl-connect-units
    - Malware: 4,160 ssl-connect-units
- Subset 2
  - Training
    - Normal: 4,160 ssl-connect-units
    - Malware: 4,156 ssl-connect-units
  - Testing
    - Normal: 4,160 ssl-connect-units
    - Malware: 4,160 ssl-connect-units

Experiment 1

- Training: 50% - 50%
    - Normal: 4,160 ssl-connect-units
    - Malware: 4,156 ssl-connect-units
- Testing: 50% - 50%
    - Normal: 4,160 ssl-connect-units
    - Malware: 4,160 ssl-connect-units


Experiment 1
4200
4180
4160
4140
4120
4100
4080
4060
4040
4020
4000
4160
4156
4160
4160
Training
Testing
Normal
Malware

Experiment 1

- XGBoost
  - Cross validation accuracy: 91.58%
  - Testing accuracy: 92.11%
  - False Positive Rate: 7.5%
  - False negative rate: 8.5%
  - Sensitivity: 91.48 %
  - F1 Score: 51.96 %

Experiment 1

- Random Forest
  - Cross validation accuracy: 90%
  - Testing accuracy: 90%
  - False Positive Rate: 8.3%
  - False negative rate: 11.7%
  - Sensitivity: 88.2%
  - F1 Score: 89.76%

Experiment 2

Experiment 2

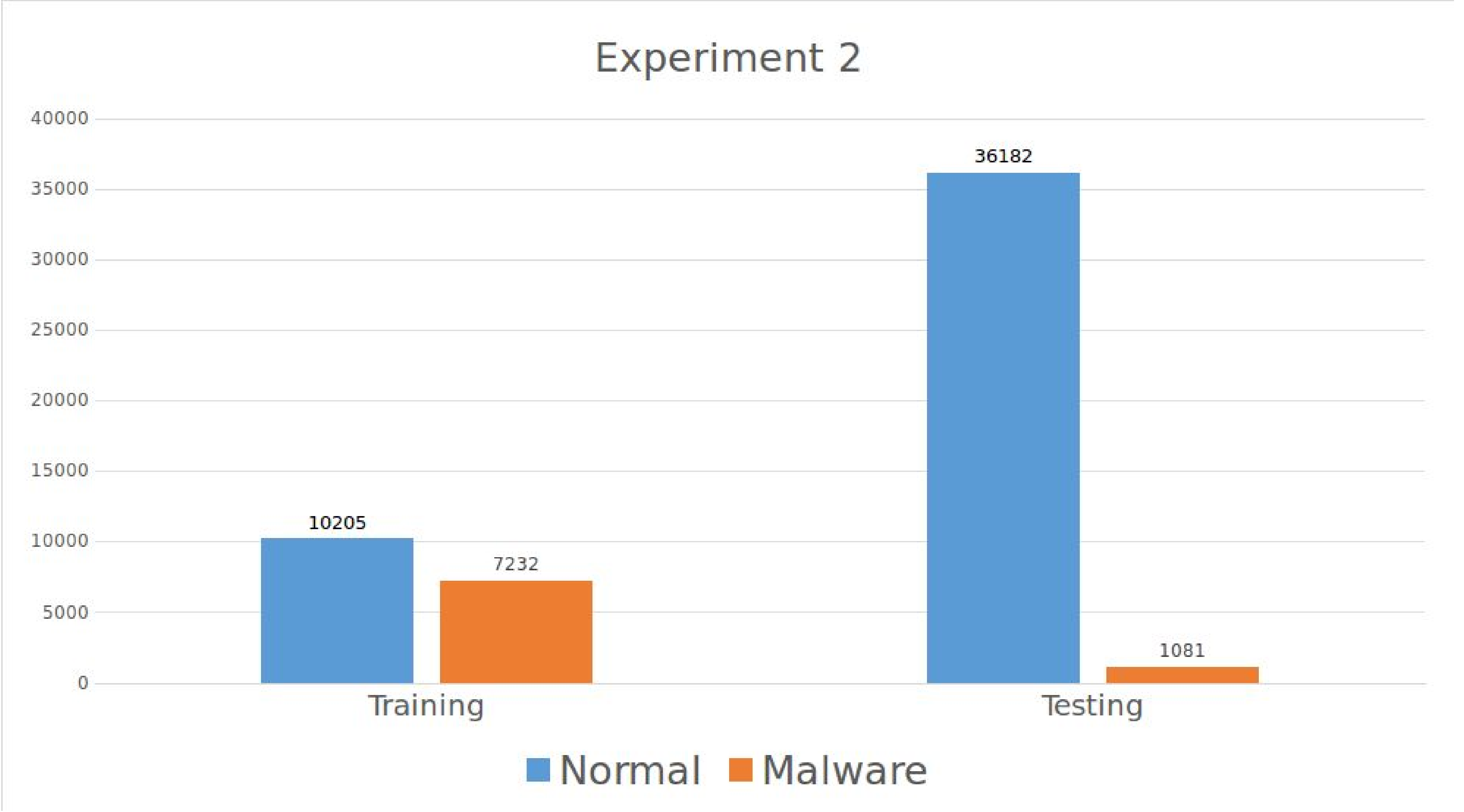
- Subset 1
  - Training
    - Malware: 7,232 ssl-connect-units
    - Normal: 10,205 ssl-connect-units
  - Testing
    - Malware: 1,081 ssl-connect-units
    - Normal: 36,182 ssl-connect-units
- Subset 2
  - Training
    - Malware: 7,232 ssl-connect-units
    - Normal: 10,205 ssl-connect-units
  - Testing
    - Malware: 1,081 ssl-connect-units
    - Normal: 36,182 ssl-connect-units
- Subset 3

  ⋮

- Subset 8
  - Training
    - Malware: 7,567 ssl-connect-units
    - Normal: 10,205 ssl-connect-units
  - Testing
    - Malware: 746 ssl-connect-units
    - Normal: 36,182 ssl-connect-units

Experiment 2

- Training: 40% - 60%
  - Malware: 7,232
  - Normal: 10,205
- Testing: 3% - 97%
  - Malware: 1,081
  - Normal: 36,182


Experiment 2
40000
35000
30000
25000
20000
15000
10000
5000
0
10205
7232
36182
1081
Training
Testing
Normal
Malware

Experiment 2

- XGBoost
    - Cross validation accuracy: 92.45%
    - Testing accuracy: 94.33%
    - False Positive Rate: 5.54%
    - False negative rate: 10.11%
    - Sensitivity: 89.89%
    - F1 Score: 46.96 %

Experiment 2

- Random Forest
  - Cross validation accuracy: 91.21%
  - Testing accuracy: 95.65%
  - False Positive Rate: 4.05%
  - False negative rate: 14.82%
  - Sensitivity: 85.18%
  - F1 Score: 52.24%

Feature importance

1. Certificate length of validity
2. Inbound and outbound packets
3. Validity of certificate during the capture
4. Duration
5. Number of domains in certificate
6. SSL/TLS version
7. Periodicity

Malware and Certificates

- Certificates used by Malware in Alexa 1000 ~ 50%
- Certificates used by Normal in Alexa 1000 ~ 30%

- Usage of certificate by Malware is almost correct

Did we achieve the goal?

Thanks for attention!

František Střasák
strasfra@fel.cvut.cz
@FrenkyStrasak

Sebastian Garcia
sebastian.garcia@agents.fel.cvut.cz
@eldracote