KIDS – Keyed Intrusion Detection System

SAŠA MRDOVIĆ, BRANISLAVA DRAŽENOVIĆ
UNIVERSITY OF SARAJEVO
FACULTY OF ELECTRICAL ENGINEERING
BOSNIA AND HERZEGOVINA

Agenda

- Introduction
- Related work
- Proposed detection method
  - Key introduction
- Testing
- Conclusion

Introduction

- Intrusion detection systems
  - Evolution and improvement ☺
- => Attack improvement
  - => undetected ☹
- Anomaly based NIDS
  - Detection method known
    - packet elements used to build model of normal
  - Mimicry attack
    - mimics normal packets – in used elements

Related Work

- PAYL [Wang04,05]
  - Model - single payload bytes frequencies
- Anagram [Wang06]
  - Model - fixed length payload byte sequences (n-grams)
  - Simple (fast) anomaly score calculation
    - new n-gram/all n-gram in packet payload
- Language model …[Riecko7]
  - Payload divided into words
    - byte sequence between delimiters
  - Comparable accuracy to n-grams
  - Smaller computational load

Proposed Detection Method

- Words based
- Word transitions, also
- Resistant to some attacks in training data
- Prevents mimicry
  - Introduce key
    - Kerckhoffs' principle [Kerckhoffs, 1883]
    - Shannon's maxim [Shannon, 1949]
    - Open design principle [Saltzer and Schroeder, 1975]

Set of Delimiters - Key

- Set of “normal” words depends on selection of delimiters
- Selected set of delimiters determines model of normal packet payload
- The same model creation method and different delimiters set => different model
- Set of delimiters – Key
  - Method – public
  - Set of delimiters - secret

Learning

- Normal, attack free, payloads - partitioned into words.
- Model of normal packet:
  - Word frequency distribution
  - Word transition frequency distribution
- Training phase
  - Appearance of any word is counted and stored
  - Appearance of any pair of words is counted and stored.

Detection

- Word based score
  - k – number of words in payload
  - $n(w_i)$ - number of appearances of the word w_i in learned model
  - Tolerant to some attacks in training data

$$S_w = \frac{\sum_{i=1}^{k} \frac{1}{n(w_i)}}{k}$$

- Transition based score
  - m – number of word transitions in a payload
  - $n(t_i)$ - number of times transition t_i occurred during training

$$S_t = \frac{\sum_{i=1}^{m} \frac{1}{n(t_i)}}{m}$$

- Total score $S = S_w * S_t$

Testing

- Used HTTP traffic and attacks
- Real university department traffic
  - Cleaned using Snort and manual inspection
- Metasploit for attacks

Initial Set of Delimiters

- From [Rieck07]

  CR LF TAB SPACE , . : / \ & ? = ( ) [ ] " ; < >

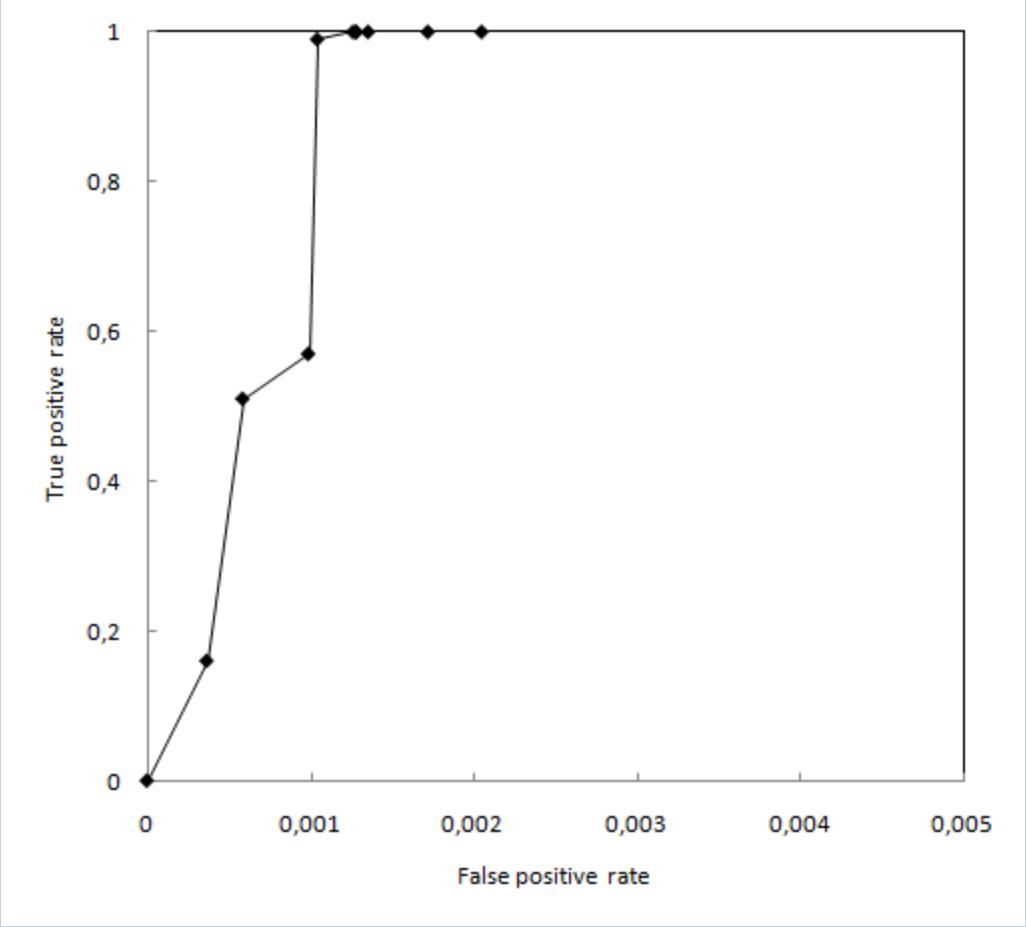
- Number of learned words
  - Levels after 96 hours of traffic
  - Around 33000
- Number of transitions
  - 33000 x 33000 matrix
  - Too much
  - Some words are very rare
  - Use only words that appear more than 10 times
  - 80 times smaller matrix

Test attacks (part)

No.	Vulnerability / payload	CVE
1	**Apache Chunked-Encoding** / meterpreter-reverse_tcp	2002-0393
2	**Apache Chunked-Encoding** / shell-reverse_http	2002-0394
3	**Apache mod_jk overflow** / adduser	2007-0775
4	**Apache mod_rewrite** / shell-bind_tcp	2006-3748
5	**Apache mod_rewrite** /vncinject-reverse_tcp	2006-3749
6	**IIS 5.0 IDQ Path Overflow** / shell-reverse_http	2001-0501
7	**IIS 5.0 IDQ Path Overflow** / shell-reverse_tcp	2001-0502
8	**IIS ISAPI w3who.dll** / exec	2004-1135
9	**IIS ISAPI w3who.dll** / shell-reverse_tcp	2004-1136
10	**Oracle 9i XDB HTTP PASS** / shell-reverse_tcp	2003-0728
11	**Xitami If_Mod_Since** / shell-reverse_tcp	2007-5068

Attacks with related vulnerability and used payload

ROC curve


1
0,8
0,6
0,4
0,2
0
True positive rate
0
0,001
0,002
0,003
0,004
0,005
False positive rate

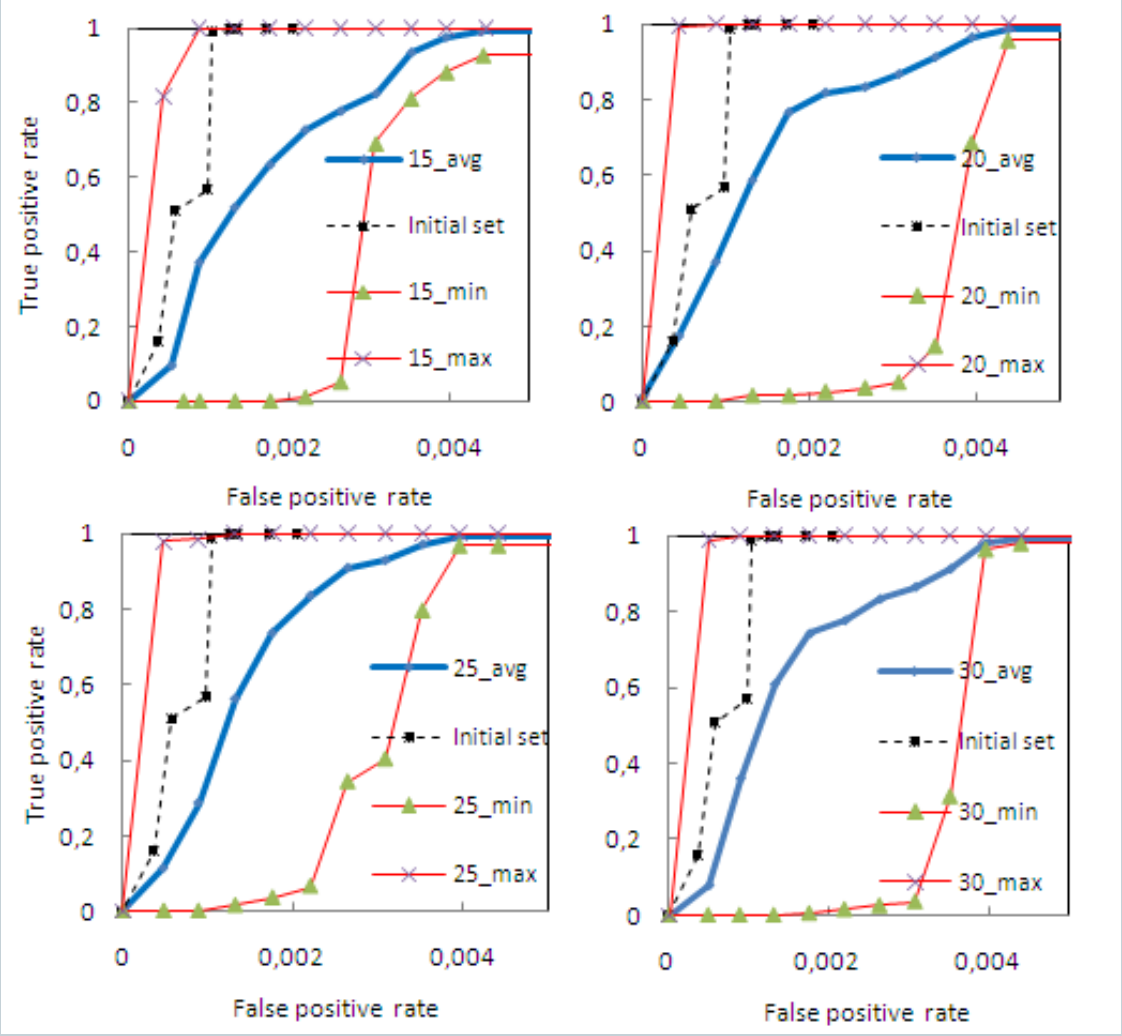
Arbitrary Set of Delimiters

- Different sets of delimiters
- Different number of delimiters in set
  - 15, 20, 25, 30
- 30 different sets of each size
- Total of 120
- Random choice of delimiters
  - Function “rand” to generate number 0 - 255

Results

- Number of learned words
  - Levels after 96 hours of traffic (again)
  - 40000 – 50000 (20 to 50% increase)
- Number of transitions
  - Again, some words are very rare
  - Use only words that appear more than 10 times
  - Matrix of managable size

ROC curves


True positive rate
False positive rate
15_avg
Initial set
15_min
15_max
20_avg
Initial set
20_min
20_max
25_avg
Initial set
25_min
25_max
30_avg
Initial set
30_min
30_max
0
0,2
0,4
0,6
0,8
1
0,002
0,004

Conclusion

- Implementation of open design principle
- Now HTTP – others should work too
  - Protocol independent
- Key selection should be further tested
- Keyed IDS is the main idea
  - There might be better implementations

Questions

?

sasa.mrdovic@etf.unsa.ba