



Kerckhoffs' Principle for Intrusion Detection



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

Agenda

2

- Introduction
- Kerckhoffs' principle
- Base system
 - Test results
- Adding key
 - Test results
- Mimicry attack detection example
- Conclusion

Introduction

3

- **Intrusion detection system (IDS)**
 - Detective security mechanism
 - Host or network based
 - Signature or anomaly detection
- **Network IDS with anomaly detection**
 - New detection method – new attacks
 - Arms race

Kerckhoffs' principle

4

- Design of a system should not require secrecy, and compromise of the system should not inconvenience the correspondents. (Kerckhoffs, 1883)
- The enemy knows the system being used (Shannon, 1949)
- Open design principle for security mechanisms (Saltzer and Schroeder, 1975)
- Opposite of “security through obscurity”

Base system

5

- Packet payload (HTTP) divided into words
- Delimiters
CR LF TAB SPACE , . : / \ & ? = () [] " ; < >
- Learning words
- Detection – Payload anomaly score
$$\text{Score (\%)} = \text{New words} / \text{Total words}$$

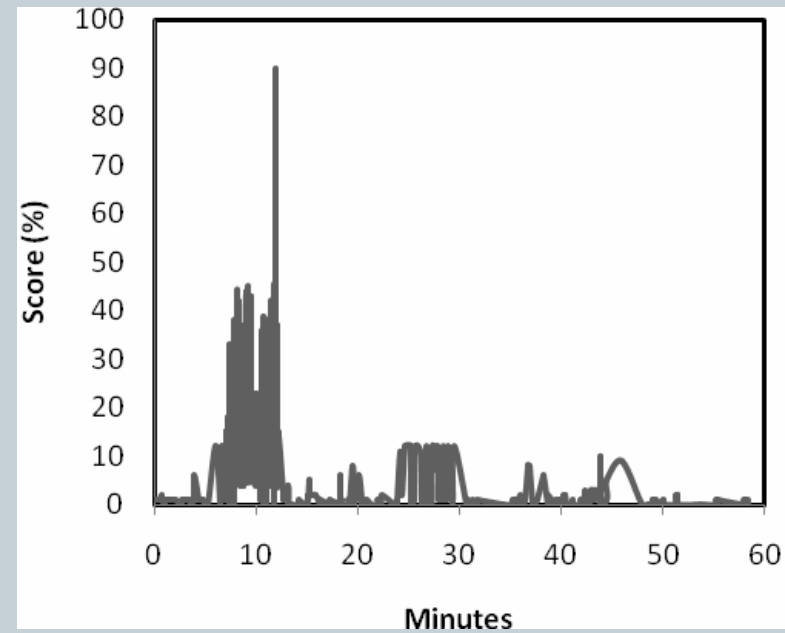
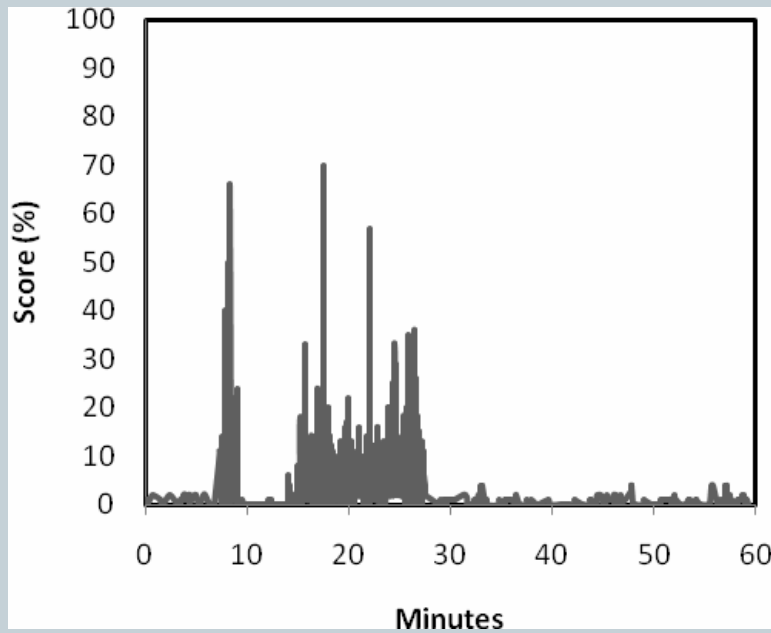
Tests

6

- **Real university department traffic**
 - Cleaned using Snort and manual inspection (for learning)
- **Current attacks (HTTP)**
 - Metasploit generated – 15 combinations of
 - ✦ 7 vulnerabilities
 - ✦ 8 attack payloads

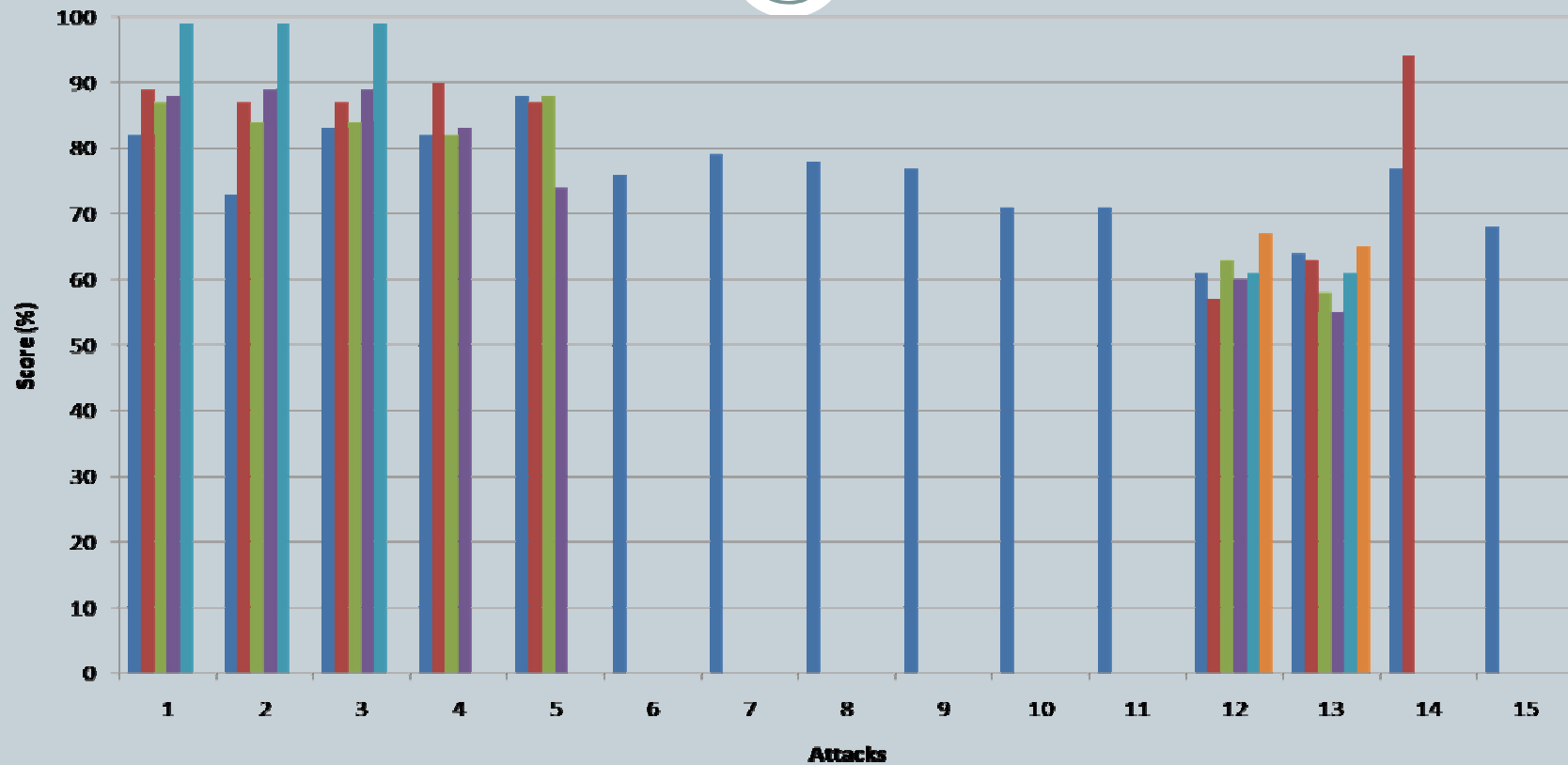
Results for Nessus and Nikto scans

7



Base system detection scores

8



Normal traffic: < 10 packets/day with score >20

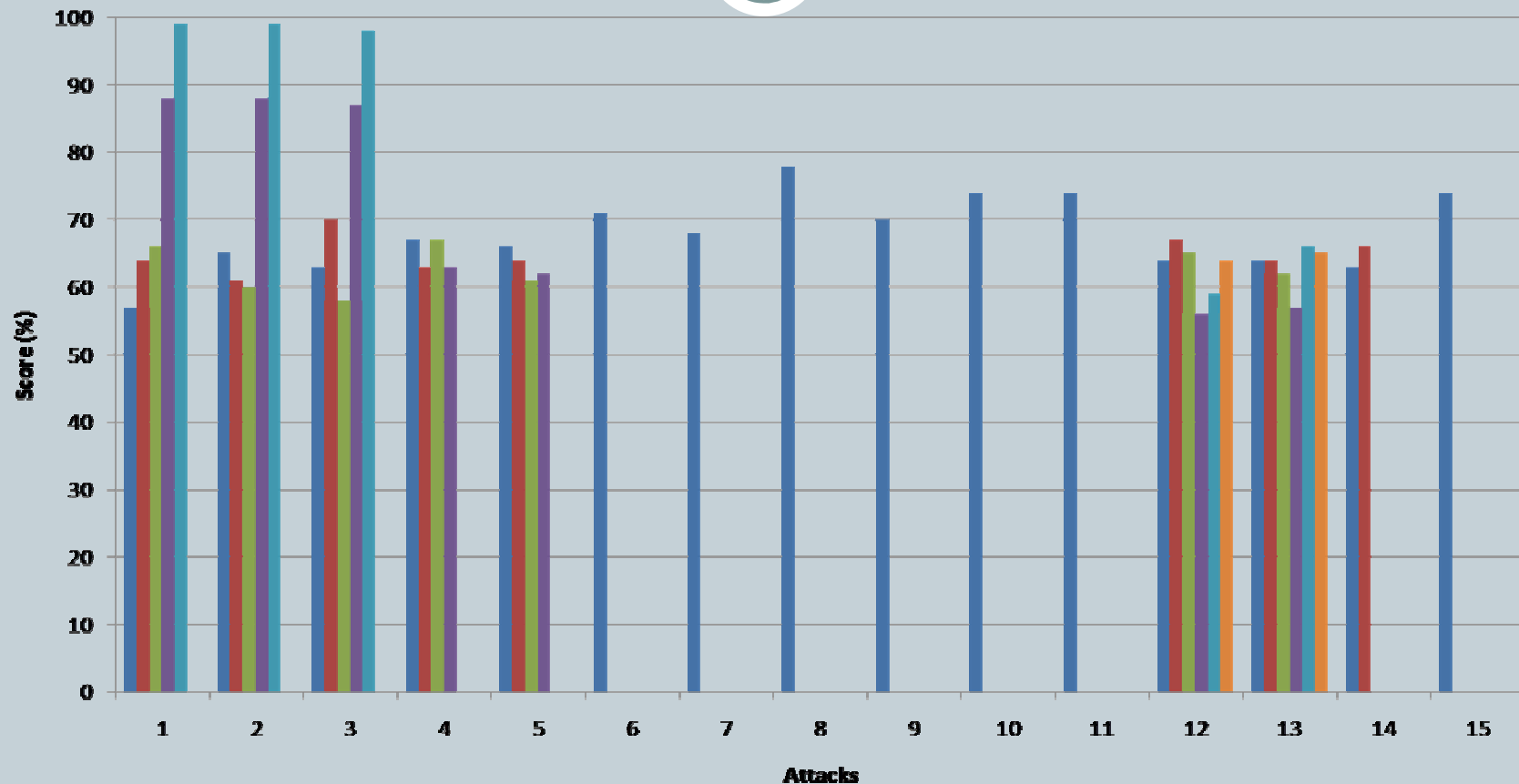
Adding key

9

- Different set of delimiters → different set of normal words → different model
- Set of delimiters = key
- Different test with different sets
 - 20 delimiters
{15, 19, 20, 30, 35, 37, 38, 41, 47, 56, 58, 63, 68, 69, 90, 97, 107, 109, 114, 122}
 - 15 delimiters
{ 9,20,34,36,53,60,63,64,66,69,71,97,103,111,116}

Set of 15 delimiters detection scores

11



Normal traffic: < 10 packets/day with score > 20

Mimicry attack detection example

12

- Original attack (Apache mod_rewrite vuln.)

GET

**/1/ldap://2QeT9jN5nS4QA9/HTiYB1T8LhY9Az9DTR9
%3feG%3fu%3fHT%3fk%3f%90+ encoded.payload**

- Modified attack (Apache mod_rewrite vuln.)

GET

**/1/ldap://GET.GET.GET.GET/GET.GET.GET.GET.G
ET.GET.GET.GET.%3f.HTTP.%3f.HTTP.%3f.GET.GE
T.GET.%3f.HTTP.%3f%90+ encoded.payload**

Mimicry attack detection scores

13

Base system		2 nd set of delimiters		3 rd set of delimiters	
Original attack	Modified attack	Original attack	Modified attack	Original attack	Modified attack
76	50	59	62	71	78
79	46	55	63	68	74
78	59	67	68	78	81
77	45	60	68	70	84

Base system – modified attack 35% lower score

Keyed system – modified attack \geq score

Conclusion

14

- New IDS design approach
- An example of idea implementation
- Should work with other application protocols
- Key maintenance issues

- Question ?

sasa.mrdovic@etf.unsa.ba