

# VU Research Portal

## Keylogger Detection and Containment

Ortolani, S.

2013

### **document version**

Publisher's PDF, also known as Version of record

[Link to publication in VU Research Portal](#)

### **citation for published version (APA)**

Ortolani, S. (2013). *Keylogger Detection and Containment*. [PhD-Thesis - Research and graduation internal, Vrije Universiteit Amsterdam].

### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

### **Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

### **E-mail address:**

[vuresearchportal.ub@vu.nl](mailto:vuresearchportal.ub@vu.nl)



# Contents

- Acknowledgements** **vii**
- Contents** **ix**
- List of Figures** **xiii**
- List of Tables** **xv**
- Publications** **xvii**
  
- 1 Introduction** **1**
  - 1.1 The Problem . . . . . 2
  - 1.2 Goals . . . . . 5
  - 1.3 Contributions . . . . . 6
  - 1.4 Organization of the Thesis . . . . . 7
  
- 2 Background** **9**
  - 2.1 What Modern Keyloggers are . . . . . 9
    - 2.1.1 User-Space Keyloggers . . . . . 10
  - 2.2 Current Defenses . . . . . 15
    - 2.2.1 Signature Based . . . . . 16
    - 2.2.2 Behavior Based . . . . . 16
  
- 3 Unprivileged Detection of Keyloggers** **21**
  - 3.1 Introduction . . . . . 21
  - 3.2 Our Approach . . . . . 21
  - 3.3 Architecture . . . . . 23

3.3.1	Injector . . . . .	24
3.3.2	Monitor . . . . .	25
3.3.3	Pattern Translator . . . . .	25
3.3.4	Detector . . . . .	26
3.3.5	Pattern Generator . . . . .	29
3.4	Evaluation . . . . .	33
3.4.1	Performance . . . . .	33
3.4.2	Keylogger detection . . . . .	33
3.4.3	False negatives . . . . .	35
3.4.4	False positives . . . . .	39
3.5	Evasion and Countermeasures . . . . .	41
3.5.1	Aggressive Buffering . . . . .	42
3.5.2	Trigger-based Behavior . . . . .	42
3.5.3	Discrimination Attacks . . . . .	42
3.5.4	Decorrelation Attacks . . . . .	43
3.6	Related Work . . . . .	45
3.7	Conclusions . . . . .	47
<b>4</b>	<b>Unprivileged Toleration via Keystrokes Hiding</b>	<b>49</b>
4.1	Introduction . . . . .	49
4.2	Our Approach . . . . .	50
4.2.1	Architecture . . . . .	51
4.3	Keystroke Dynamics Model . . . . .	52
4.4	Privacy Model . . . . .	53
4.5	Evaluation . . . . .	55
4.5.1	Preliminaries . . . . .	56
4.5.2	Performance . . . . .	57
4.5.3	Effectiveness . . . . .	59
4.6	Conclusions . . . . .	60
<b>5</b>	<b>Privileged Detection of Keylogging Malware</b>	<b>63</b>
5.1	Introduction . . . . .	63
5.2	Background . . . . .	64
5.3	Our Approach . . . . .	65
5.3.1	Detector . . . . .	68
5.3.2	Injector . . . . .	68
5.3.3	Monitor . . . . .	69
5.4	Optimizing Detection Accuracy . . . . .	71
5.5	Evaluation . . . . .	74
5.5.1	Synthetic Evaluation . . . . .	74
5.5.2	Malware Detection . . . . .	76
5.5.3	False Positive Analysis . . . . .	79
5.5.4	Performance Analysis . . . . .	80

5.6	Discussion . . . . .	83
5.7	Related Work . . . . .	85
5.8	Conclusions . . . . .	86
<b>6</b>	<b>Privileged Detection of Keylogging Add-ons</b>	<b>87</b>
6.1	Introduction . . . . .	87
6.2	Our Approach . . . . .	88
6.3	Browser Memory Profiling . . . . .	90
6.4	The Model . . . . .	91
6.4.1	Support Vector Machine . . . . .	92
6.4.2	Feature Selection . . . . .	93
6.4.3	Feature Vector: Ideal Case . . . . .	95
6.4.4	Feature Vector: Real Case . . . . .	96
6.5	Application to Keylogging Extensions . . . . .	98
6.6	Evaluation . . . . .	99
6.6.1	False Negatives . . . . .	100
6.6.2	False Positives . . . . .	102
6.6.3	Performance . . . . .	102
6.7	Discussion . . . . .	105
6.8	Related Work . . . . .	105
6.9	Conclusions . . . . .	107
<b>7</b>	<b>Conclusions and Future Works</b>	<b>109</b>
	<b>References</b>	<b>113</b>
	<b>Summary</b>	<b>125</b>
	<b>Samenvatting</b>	<b>127</b>