

TokDoc – The	
Token Doctor	

Tammo Krueger

Outline

Introduction

TokDoc

Anomaly

Detectors

Healing Action

Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work

TokDoc - The Token Doctor

Tammo Krueger

26.03.2010 25th Symposium On Applied Computing



TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Actior

Setup Process

Evaluation Ensemble of Learners Comparison to Other Detectors

Conclusion and Further Work

1 Introduction

2 TokDoc

- Walkthrough
- Anomaly Detectors
- Healing Actions
- Setup Process
- 3 Evaluation
 - Ensemble of Learners
 - Comparison to Other Detectors
 - Runtime
- 4 Conclusion and Further Work



Web Application Firewall (WAF) - Overview



- Evaluation
- Ensemble of Learners Comparison to Other Detectors Runtime
- Conclusion and Further Work

- We focus on reverse proxy setup
- Web Application Firewall monitors web applications
- Negative security model: set of fixed signatures/rules
- Positive security model: fixed allowed traffic
- reacts in real time to suspicious activities by
 - blocking the traffic
 - replacing parts of the request



TokDoc - Teach WAFs New Tricks



Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work Tune up existing WAF techniques with machine learning:

- use syntactical structure for local per-token model building
- decide on this token-base,
 - which detector is suitable
 - which action is applicable
- learn these assignments automatically from collected data
- no additional attack dataset needed



TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc

Walkthrough

Anomaly Detectors Healing Actions Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work

1 Introduction

2 TokDoc

Walkthrough

- Anomaly Detectors
- Healing Actions
- Setup Process
- 8 Evaluation
 - Ensemble of Learners
 - Comparison to Other Detectors
 - Runtime
- 4 Conclusion and Further Work



TokDoc – Walkthrough 1/4

TokDoc – The Token Doctor

Tammo Krueger

Outline

Introduction

TokDoc

Walkthrough

Anomaly Detectors Healing Actions Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detector Runtime

Conclusion and Further Work GET /index.php?cat=%2527+UNION+SELECT+user_pass+FROM+wp_users/* HTTP/1.1 Host: www.foobar.com User-Agent: Mozilla/4.0 Accept: */*



GET /index.php?cat=27 HTTP/1.1 Host: www.foobar.com User-Agent: Mozilla/4.0 Accept: */*



TokDoc – Walkthrough 2/4

TokDoc – The Token Doctor GET /index.php?cat=%2527+UNION+SELECT+user pass+FROM+wp users/* HTTP/1.1 Host: www.foobar.com Tammo User-Agent: Mozilla/4.0 Krueger Accept: */* **Reverse Proxy** HTTP Parser Mangle Walkthrough path: /index.php? cat: %27+UNION+SEL... host: www.foobar.com Action Detector user-agent: Mozilla... accept: */* Runtime Configuration and Further GET /index.php?cat=27 HTTP/1.1 Host: www.foobar.com User-Agent: Mozilla/4.0 Accept: */*



TokDoc – Walkthrough 3/4

TokDoc – The Token Doctor GET /index.php?cat=%2527+UNION+SELECT+user pass+FROM+wp users/* HTTP/1.1 Host: www.foobar.com Tammo User-Agent: Mozilla/4.0 Krueger Accept: */* **Reverse Proxy** HTTP Parser Mangle Walkthrough • • path: /index.php? cat: %27+IINTON+SEL host: www.foobar.com Detector Action user-agent: Mozilla... accept: */* Runtime Configuration and Further GET /index.php?cat=27 HTTP/1.1 Host: www.foobar.com User-Agent: Mozilla/4.0 Accept: */*



TokDoc – Walkthrough 4/4

TokDoc – The Token Doctor GET /index.php?cat=%2527+UNION+SELECT+user pass+FROM+wp users/* HTTP/1.1 Host: www.foobar.com Tammo User-Agent: Mozilla/4.0 Krueger Accept: */* **Reverse Proxy** HTTP Parser Mangle Walkthrough Ŧ path: /index.php? cat: %27+IINTON+SEL host: www.foobar.com Detector Action user-agent: Mozilla... accept: */* Runtime Configuration and Further GET /index.php?cat=27 HTTP/1.1 Host: www.foobar.com User-Agent: Mozilla/4.0 Accept: */*



TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc

Walkthrough

Anomaly Detectors

Healing Actions Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work 1 Introduction

2 TokDoc

Walkthroug

Anomaly Detectors

- Healing Actions
- Setup Process
- **Evaluation**
 - Ensemble of Learners
 - Comparison to Other Detectors
 - Runtime
- 4 Conclusion and Further Work



TokDoc – Anomaly Detectors NCAD

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthroug

Anomaly Detectors

Healing Actions Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work N-gram Centroid Anomaly Detector (NCAD)

Foundation n-gram vector space **Model** Distance $d(\mu, x)$ of new x to mean μ of data **Decision** Based on FP-tuned threshold t_a :

$$ext{score}_{ ext{NCAD}}(x) = egin{cases} ext{normal}, & ext{if } d(\mu, x) \leq t_a \ ext{anomaly}, & ext{otherwise}. \end{cases}$$

PRO Good general model, capable of learning "normal" behaviorCON Fails for multimodal data distribution



TokDoc – Anomaly Detectors MCAD

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc

Anomaly

Detectors Healing Actio

Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work Markov Chain Anomaly Detector (MCAD)

Foundation Markov Chain based on byte transitions (256 states with 256 transitions each)

Model Probablity P(x | C) of new x in Markov Chain C **Decision** Based on FP-tuned threshold p_a :

 $score_{MCAD}(x) = \begin{cases} normal, & \text{if } P(x \mid C) \ge p_a \\ anomaly, & \text{otherwise.} \end{cases}$

PRO Can cope with multimodal data distribution**CON** Not as tight as NCAD due to length dependence



TokDoc – Anomaly Detectors LAD

TokDoc - The Token Doctor

> Tammo Krueger

Anomaly

Detectors

Runtime

and Further

Length Anomaly Detector (LAD)								
Foundation	Robust estimati	obust estimation via bootstrap						
Model	Confidence inte seen data	Confidence interval around length quantile L_eta of seen data						
Decision	Estimate variablity σ of length quantile and decide for new data point x:							
	$score_{LAD}(x) = -$	{normal, anomaly,	$\begin{array}{l} \text{if } len(x) \leq L_{\beta} + c\sigma \\ \text{otherwise.} \end{array}$					
PRO	Works even for scarce data situations							
CON	No "deep" data	inspection, ju	st using length					



TokDoc – Anomaly Detectors LIST

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthroug

Anomaly Detectors

Healing Actions Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work List Anomaly Detector (LIST)

Foundation Lists Model Unique list *L* of seen values

Decision For new data point *x*:

$$\mathsf{score}_{\mathsf{LIST}}(x) = egin{cases} \mathsf{normal}, & \mathsf{if} \ x \in L \ \mathsf{anomaly}, & \mathsf{otherwise}. \end{cases}$$

PRO Fast and simpleCON We need to see all values beforehand (no "generalization" possible)



TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors

Healing Actions

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work 1 Introduction

2 TokDoc

- Walkthroug
- Anomaly Detectors
- Healing Actions
- Setup Process
- Evaluation
 - Ensemble of Learners
 - Comparison to Other Detectors
 - Runtime
- 4 Conclusion and Further Work



TokDoc – Healing Actions

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors

Healing Actions

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work

1 Dropping of tokens:

- remove anomalous token from request
- default action for LAD detector.

2 Preventive encoding:

- encode the anomalous value using HTML entities
- manual assignment.

3 Replacement with most frequent value:

- replace anomalous value with the most frequent normal value
- Default action for LIST detector.

4 Replacement with nearest value.

- replace anomalous value with its nearest-neighbor from the training set
- Default action for both MCAD and NCAD



TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Action Setup Process

Setup Flocess

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work 1 Introduction

2 TokDoc

- Walkthroug
- Anomaly Detectors
- Healing Actions
- Setup Process
- Evaluation
 - Ensemble of Learners
 - Comparison to Other Detectors
 - Runtime
- 4 Conclusion and Further Work



TokDoc – Setup Process





TokDoc – Setup Console



Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Activ

Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detector Runtime

Conclusion and Further Work

		TokDoc (TI	he token doctor)		
▼ VAL_board	^	1000			
NCAD		1600			
MCAD		1200			
LAD		1200			
▼ VAL c	=	800			
NCAD		600			
MCAD		400			
LAD		200			<mark>-</mark>
▼ VAL cat		0			-
NCAD		-200	-3000 -2500 -20	00 -1500 -1000 -500	
MCAD			A - 4 m -		•
LAD			🕂 🔍 🖾 🖷		
▼ VAL_category_name		dist.	value		
NCAD		-3286.221862	999 UNION SELECT null,	CONCAT(666,CHAR(58),user_pass	CHAR(5
MCAD		-2578.877358	%27 UNION SELECT CO	NCAT(666,CHAR(58),user_pass,CH	AR(58),6
LAD		-66.511160	http://www.agrippine.net	/titip/idfx1.txt?	
▼ VAL_catslist		-5.407787			
NCAD		-4.898445	35		
MCAD		-4.898445	30		
LAD		-4.675302	32		
▼ VAL_charset		-4.492980	36		
NCAD		-4.485209	19		
MCAD		-4.452276	20		
LAD		-4.351678	17		
✓ VAL_closedpostboxesnonce		4 220000	24	·	[
NCAD		re	s. threshold:	-3286.2218618758392950	
MCAD		cu	r. threshold:	-3286.2218618758392950	
LAD		•	set	data	



TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Action Setup Process

Evaluation

Ensemble of Learners

Comparison to Other Detectors Runtime

Conclusion and Further Work 1 Introduction

TokDoc

- Walkthrough
- Anomaly Detectors
- Healing Actions
- Setup Process

3 Evaluation

Ensemble of Learners

- Comparison to Other Detectors Runtime
- 4 Conclusion and Further Work



Evaluation – Ensemble of Learners

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Actio

Evaluation

Ensemble of Learners

Comparison to Other Detector Runtime

Conclusion and Further Work **Question:** Do we really need 4 different detectors? **Setup:** Use just one type of detector and compare to TokDoc performance (FP = false-positive rate. TP = attacks found in normal traffic. FN = false-negative rate):

Dataset	Detector	FP	ТР	FN
	TokDoc	0.00002	0	0.00000
EIDCTOO	TD _{LAD}	0.00000	0	0.02247
FIK3100	TD _{MCAD}	0.00001	0	0.00000
	TD _{NCAD}	0.00002	0	0.22472
	TokDoc	0.00003	212	0.04124
PLOCO0	TD _{LAD}	0.00001	68	0.15464
BLUGU9	TD _{MCAD}	0.00009	186	0.04124
	TD _{NCAD}	0.00003	0	0.22680



TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Action Setup Process

Evaluation

Ensemble of Learners

Comparison to Other Detectors

Conclusion and Further Work 1 Introduction

TokDoc

- Walkthrough
- Anomaly Detectors
- Healing Actions
- Setup Process

3 Evaluation

Ensemble of Learners

- Comparison to Other Detectors
- Runtime
- 4 Conclusion and Further Work



Evaluation - Comparison to Other Detectors

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Action Setup Process

Evaluation

Ensemble of Learners

Comparison to Other Detectors

Runtime

Conclusion and Further Work **Question:** Do we really need TokDoc at all? **Setup:** Compare TokDoc performance to other anomaly-based detectors (FP_{TD} = false-positive rate of detector when calibrated to the true-positive rate of TokDoc. FN_{TD} = rate of missed regular attacks when detector is calibrated to the false-positive rate of TokDoc):

Dataset	Detector	FP _{TD}	FN TD	
	TokDoc	0.00002	0.00000	
FIRST08	Markov Chain	0.02005	0.80899	
	Anagram	0.00004	0.16854	
	TokDoc	0.00003	0.04124	
BLOG09	Markov Chain	0.16698	0.18557	
	Anagram	1.00000	0.39175	

Answer: YES!



TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Action Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors

Runtime

Conclusion and Further Work 1 Introduction

TokDoc

- Walkthrough
- Anomaly Detectors
- Healing Actions
- Setup Process

3 Evaluation

- Ensemble of Learners
- Comparison to Other Detectors
- Runtime

4 Conclusion and Further Work



Evaluation – Runtime

TokDoc – The Token Doctor

Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Action Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detector

Runtime

Conclusion and Further Work **Question:** Is TokDoc ready for deployment? **Setup:** Measure median runtime in miliseconds per request and compare to other proxies:

	Proxy				
Dataset	Squid	ModSec.	twisted	TokDoc	
FIRST08	1.387	1.536	2.552	2.768	
BLOG09	1.500	1.694	2.430	2.902	

Answer: YES!



Conclusion and Further Work

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Action Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work Protocol-aware reverse proxy TokDoc:

- fine-grained decisions at token level
- automatic setup procedure, which determines suitable model for each token

intelligent mangling strategies for anomalous tokens
 Future work:

- Integration of TokDoc into Squid or the ModSecurity platform
- Incorporation of a feedback loop
- Integration of session-awareness and "long term memory"
 Test in the wild...



FokDoc – The	
Token Doctor	

Tammo Krueger

Outline

Introduction

TokDoc

Walkthroug

Anomaly

Delectors

Heating Actions

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work Questions? Comments? Thanks for your attention!



TokDoc – Anomaly Detectors NCAD

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Actio

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work Given the set of all possible n-grams over byte sequences $S = \{0, ..., 255\}^n$, we define the embedding function ϕ for a token value x as follows:

$$\begin{split} \phi(x) &= (\phi_s(x))_{s \in S} \in \mathbb{R}^{|S|} \quad \text{with} \quad \phi_s(x) = s \sqsubseteq x \\ \mu &= \frac{1}{N} \sum_{i=1}^N \phi(x_i) \\ d(x,z) &= \|\phi(x) - \phi(z)\|_2 = \sqrt{\sum_{s \in S} |\phi_s(x) - \phi_s(z)|^2} \\ \text{score}_{\text{NCAD}}(x) &= \begin{cases} \text{normal}, & \text{if } d(\mu, x) \le t_a \\ \text{anomaly}, & \text{otherwise.} \end{cases} \end{split}$$



TokDoc – Anomaly Detectors MCAD

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Action Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work Having learned the transition probabilities, we can estimate the probability of a token value x of length n based on the learned Markov chain C:

$$P(x \mid C) = P(X_1 = x[1]) \prod_{i=1}^{n} P(X_{i+1} = x[i+1] \mid X_i = x[i]$$

score_{MCAD}(x) =
$$\begin{cases} \text{normal}, & \text{if } P(x \mid C) \ge p_a \\ \text{anomaly}, & \text{otherwise.} \end{cases}$$



TokDoc – Anomaly Detectors LAD

TokDoc – The Token Doctor

> Tammo Krueger

Outline

Introduction

TokDoc Walkthrough Anomaly Detectors Healing Action Setup Process

Evaluation

Ensemble of Learners Comparison to Other Detectors Runtime

Conclusion and Further Work Given a predefined significance level α_{LAD} we estimate the $1 - \alpha_{LAD}$ quantile of the length distribution of the train and validation data L, namely $\hat{L}_{1-\alpha_{LAD}}$. Now we construct a confidence interval for $L_{1-\alpha_{LAD}}$ by first calculating the bootstrap estimate of the standard error of $\hat{L}_{1-\alpha_{LAD}}$, namely $\hat{\sigma}$, and determining the parameter c, so that the following interval has probability coverage of $1 - \alpha_{LAD}$:

$$\begin{array}{ll} & (\hat{L}_{1-\alpha_{\mathsf{LAD}}} - c\hat{\sigma}, \hat{L}_{1-\alpha_{\mathsf{LAD}}} + c\hat{\sigma}) \\ \text{score}_{\mathsf{LAD}}(x) & = & \begin{cases} \operatorname{normal}, & \text{if } \mathsf{len}(x) \leq \hat{L}_{1-\alpha_{\mathsf{LAD}}} + c\hat{\sigma} \\ \text{anomaly}, & \text{otherwise.} \end{cases} \end{array}$$



TokDoc - Setup Process





TokDoc – Setup Process

TokDoc – The Token Doctor			Dete	ctors FIR	ST08		
Tammo Krueger	Category	LIST	LAD	MCAD	NCAD	Σ	
Outline	Header	14	14	5	10	43	
Introduction	Parameter	9	3	4		16	
TokDoc	Path	_		1		1	
Walkthrough Anomaly Detectors	Σ	23	17	10	10	60	
Setup Process							
Evaluation Ensemble of		Detectors BLOG09					
Learners Comparison to Other Detectors	Category	LIST	LAD	MCAD	NCAD	Σ	
Runtime	Header	22	77	15	17	131	
Conclusion and Further	Parameter	14	166	28	7	215	
Work	Path		_	1	—	1	
	Σ	36	243	44	24	347	