Assessing Vulnerabilities in Software Systems: A Quantitative Approach

Yashwant K Malaiya
BMAC Sept 17, 07

Colorado State University
Knowledge to Go Places

Presentation Outline

- Motivation and Background
- Vulnerability data and AML Vulnerability Discovery Model
  - Fitting HTTP Web servers' and Browsers' datasets
  - Measuring Prediction Capabilities
- Fitting categorized vulnerabilities
  - Categories
  - Severity Levels
  - Analyzing categorized vulnerabilities
- Conclusions and Future Work

2

Motivation

- Security maintenance management
  - Security patch scheduling
  - Estimating the number of vulnerabilities
- Growing risk caused by software vulnerabilities
  - Loss estimation
  - Ownership cost estimation

3

Research Objectives

- This research look into ways to estimate the number of potential vulnerabilities
- Providing users with:
  - Improving risk assessment
  - Comparison tools
  - Lay a foundation for stable metrics
- Providing developers with
  - Guidelines and tips for better development
  - Testing optimization tools
  - Improving software maintenance resource allocation

4

Definition and Background

Definition: vulnerability is "a defect which enables an attacker to bypass security measures" [Schultz et al. 1990]

Related work:

- " [Rescorla 2005] and [Ozment 2005] applied some SRGMs to vulnerabilities
- Anderson suggested a model based on thermodynamics analogy
- Arbach et al. proposed a model for incidents

5

Data Description

- Vulnerability Databases
  - National Institute of Standards and Technology's National Vulnerability Database, http://nvd.nist.gov
  - MITRE Corporation, http://www.mitre.org
- Defects Data
  - Vendors
  - Bugzilla, http://www.bugzilla.org
  - Independent Articles
- Market share
  - Google (until mid-2004)
  - Internet counters
- Software sizes
  - Vendors
  - Experts

6

Vulnerability Datasets

- Operating Systems
  - Windows and Red Hat Linux
- Web-servers
  - Microsoft IIS and Apache
- Web-browsers
  - Internet Explorer and Fire Fox

7

Vulnerability Discovery Models

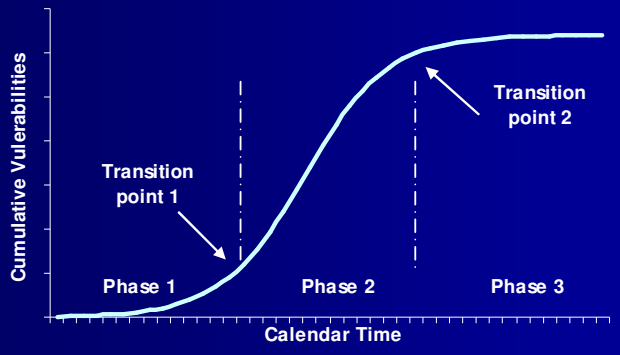
- Security and reliability analogy
- VDMs and SRGMs analogy
- Characterizing security
  - Number of potential vulnerabilities
  - Vulnerability discovery rate

8

The Logistic Model

- A time-based model

$$\Omega(t) = \frac{B}{BCe^{-ABt} + 1}$$



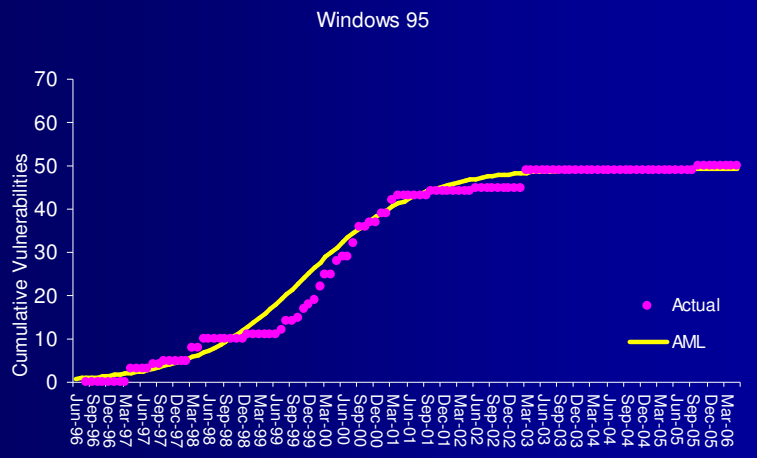
9

The Linear Model

- Approximation of the logistic model
- The learning phase may be very brief
- Significant number of vulnerabilities are still present and continue to be found
- The dataset is a superimposition of two or more consecutive S-shaped models $\Omega(t) = (S \times t) + k$

10

Validating The Logistic Model



11

Goodness of fit test-AML

System	A	B	C	DF	χ^2	$\chi^2_{critial}$ (5%)	P-value	Fit Result
Win 95	0.001652	49.5512	1.32092	132	45.748	159.8135	1	*Significant*
Win 98	0.000522	92.6789	0.10233	92	107.001	115.3898	0.135785	*Significant*
Win XP	0.000232	280.513	0.09994	59	54.6261	77.93052	0.637299	*Significant*
Win NT 4.0	0.000317	184.78	0.44439	140	267.173	168.613	0	Insignificant
Win 2000	0.0001096	391.984	0.0386	79	95.1500	100.7486	0.104079	*Significant*
R H Linux 6.2	0.000855	121.235	0.13973	75	36.19688	96.21667	0.999956	*Significant*
R H Linux 7.1	0.169437	166.735	0.29531	65	39.6227	84.82064	0.99456	*Significant*
Red Hat Fedora	0.002014	139.045	0.53497	31	31.81382	44.98534	0.425800	*Significant*
Solaris 7.0	0.000526	126.32	0.11076	95	107.701	118.7516	0.1759	*Significant*
Solaris 8.0	0.000961	99.815	0.26380	80	69.7045	101.8795	0.7877	*Significant*
Solaris 9.0	0.000528	114.25045	0.11979	52	34.964	69.83216	0.9665	*Significant*

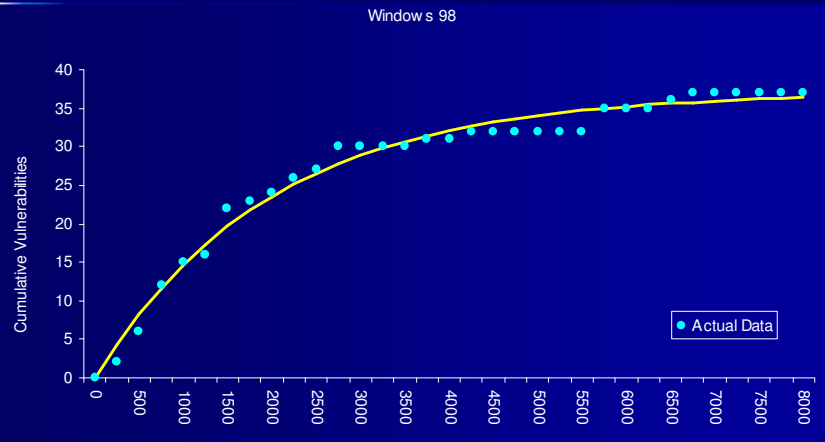
The Effort-Based Model

- Data needed: The total effort spent using the software system
  - Percentage of market share
  - Global internet population
  - Effort is calculated: $E = \sum_{i=0}^{n} (U_i \times P_i)$
- The effort is mapped to the vulnerability datasets by eliminating the time
- The effort/vulnerabilities data is fitted to the model:

$$\Omega(E) = B(1 - e^{-\lambda_{vu} E})$$

13

Validating The Effort-Based Model



14

Web Servers Datasets Overview

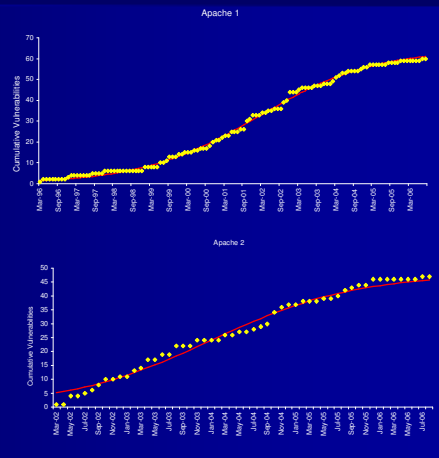
- Apache and IIS market share (90.6%)

	Apache		IIS		SJSWS (SunOne)	Zeus
First Release	1995		1995		2002	1995
Market Share	69.7%		20.92%		2.53%	0.78%
Version	**1.x**	**2.x**	**4.0**	**5.0**	Up to 6.1	Up to 4.3
Vulnerabilities	58	45	85	73	3	5

15

Web servers Datasets Goodness of Fit Test

Software Sys	Fit
Apache 1.x	*Significant*
Apache 2.x	*Significant*
IIS 4.x	*Significant*
IIS 5.x	*Significant*



16

Web Browsers Datasets Overview

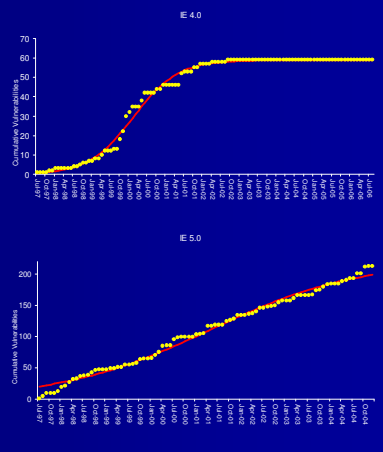
Web Browser	IE	Firefox	Mozilla	Safari	Other
Market Share	85.2%	9.6%	0.37%	3.06%	1.77%
Vulnerabilities	265	94	38	24	N/A
Release Date	Aug 95	Sep 02	Dec 98	Jan 03	N/A

Browser	Nov 2004	Apr 2005	Jan 2006	Jul 2006
IE	88.9%	86.63%	85.82%	83.05%
Firefox	4.58%	8.69%	11.23%	12.93%

17

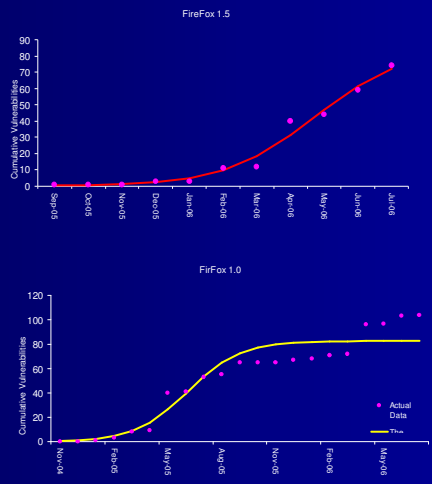
Web Browsers Datasets Goodness of Fit Test

Software Sys	Significant
IE 4.0	*Significant*
IE 5.0	*Significant*
IE 6.0	Insignificant
FFox1.0	Insignificant
FFox1.5	*Significant*



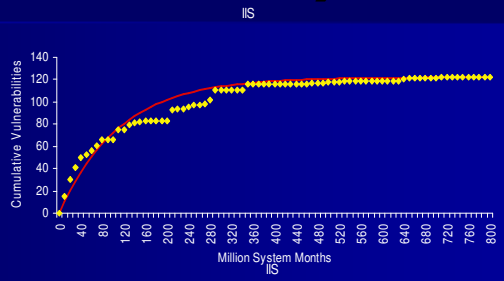
18

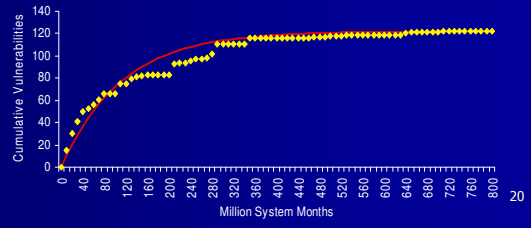
Web Browsers Datasets Goodness of Fit Test



Goodness of Fit Results (Effort-Based Model)

	Significance
Apache	*Significant*
IIS	*Significant*



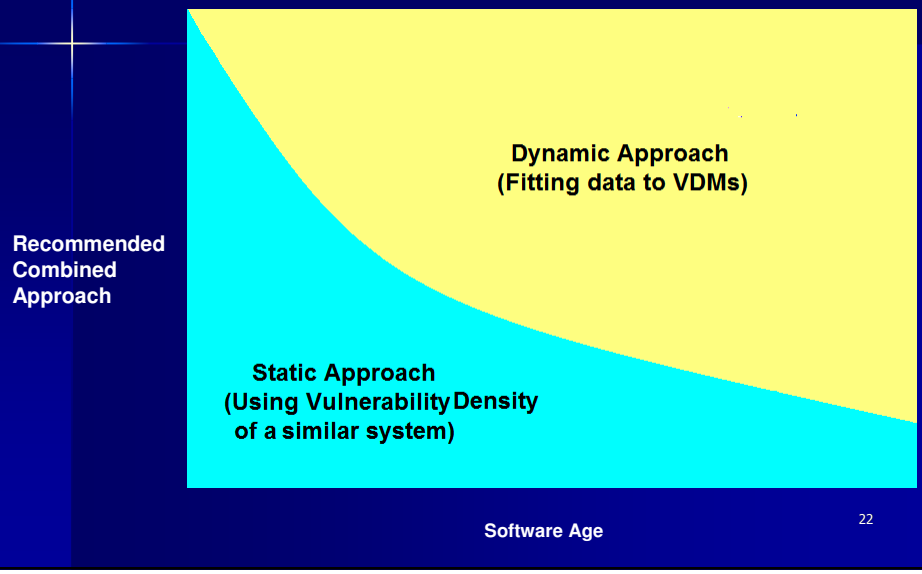


Goodness of Fit Results

- AML model fits the datasets
  - The superposition effect: Consecutive S-shaped models because of shared vulnerabilities
- Effort-based model fits the datasets

21

Prediction Approaches



22

Vulnerabilities Taxonomy

- Input Validation Error (IVE) (Boundary condition error (BCE), Buffer overflow (BOF)):
  - Include failure to verify the incorrect input and read/write involving an invalid memory address.
- Access Validation Error (AVE):
  - These vulnerabilities cause failure in enforcing the correct privilege for a user.
- Exceptional Condition Error Handling (ECHE):
  - May arise due to failures in responding to unexpected data or conditions.
- Environmental Error (EE):
  - Triggered by specific conditions of the computational environment.

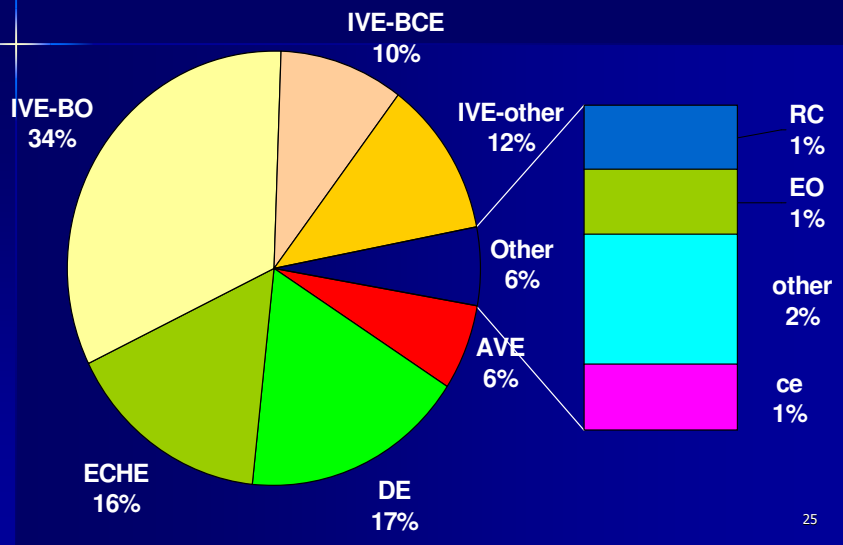
23

Vulnerabilities Taxonomy

- Configuration Error (CE):
  - These vulnerabilities result from improper system settings.
- Race Condition Error (RC):
  - These are caused by the improper serialization of the sequences of processes.
- Design Error (DE):
  - These are caused by improper design of the software structure.
- Others:
  - Includes vulnerabilities that do not belong to the types listed above, sometimes referred to as nonstandard.

24

Windows XP



25

Goodness of Fit Results

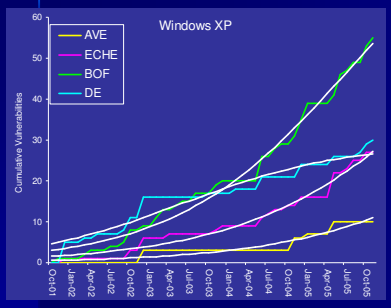
Windows 2000

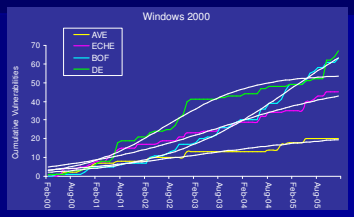
Vulnerability Type	Parameters			X^2		
	A	B	C	P-value	X^2	X^2 Critical
AVE	0.002121	23.181	0.279309	*1*	25.5528	92.81
ECHE	0.001026	51.954	0.189765	*0.99956*	38.63088	
BOF	0.000676	93.862	0.495049	*1*	19.62047	
DE	0.001791	54.358	0.343025	*0.99448*	45.14116	

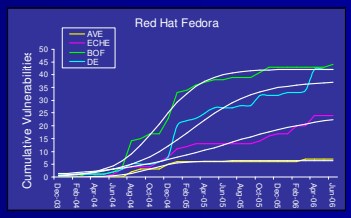
Windows XP

Vulnerability Type	Parameters			X^2		
	A	B	C	P-value	X^2	X^2 Critical
AVE	0.001035	63.595	2.0119	*1*	17.70871	67.50
ECHE	0.000700	92.864	0.674	*1*	12.10664	
BOF	0.000808	93.578	0.348	*1*	14.82454	
DE	0.002854	28.984	0.1958	*1*	13.08505	

OS: Vulnerability Categories







27

Severity Levels

- Common Vulnerabilities Scoring System: A 10 points system to measure the risk of the vulnerabilities
  - High (7-10)
  - Medium (4-6.99)
  - Low (1- 3.99)

28

Modeling Vulnerabilities by Severity

Apache

Vulnerability Severity Level	Parameters			X^2		
	A	B	C	P-value	X^2	$X^2_{Critical}$
High	.00156	27.00	1.00	1	42.1	144.3
Low	.00248	18.00	1.76	1	15.7	

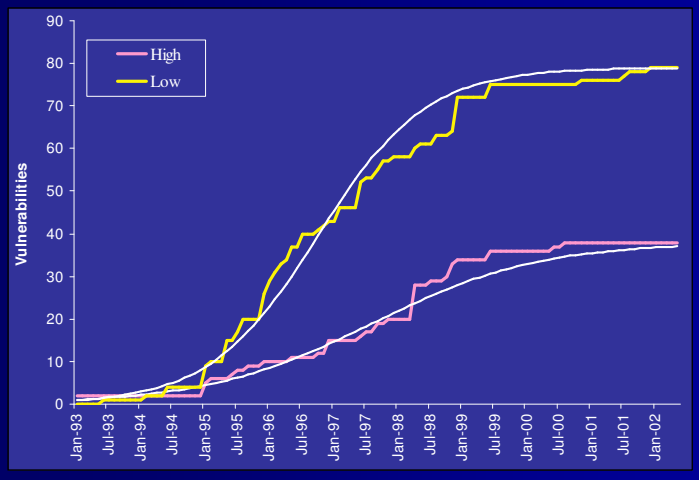
IIS

Vulnerability Severity Level	Parameters			X^2		
	A	B	C	P-value	X^2	$X^2_{Critical}$
High	.00176	38	.999	1	28.2	133.2
Low	.00127	77.9	1.21	.999	53.5	

29

Modeling Vulnerabilities by Severity

IIS



30

Categories vs. Severity level

Apache

	AVE	DE	ECHE	IVE BOF	IVE BCE	IVE other	RC	EE	CE	other	Total
High	3	5	3	7	1	10	0	3	2	1	35
Medium	0	1	1	3	0	0	1	0	0	0	6
Low	3	17	***12***	3	1	14	1	1	***12***	4	68
Total	6	23	16	13	2	24	2	4	14	5	109

Windows 2000

	AVE	DE	ECHE	IVE BOF	IVE BCE	IVE other	RC	EE	CE	other	Total
High	10	29	12	***52***	18	7	1	2	4	1	135
Medium	6	15	2	5	0	2	0	0	2	1	33
Low	6	26	***32***	9	3	16	1	2	3	1	100
Total	22	70	46	66	21	25	2	4	9	3	268

Results Summary

- Buffer overflow
  - Linked to high severity vulnerabilities
- Exceptional Control Handling Error
  - Linked to low severity vulnerabilities
- Input Validation errors
  - Vulnerabilities of this type other than Buffer overflow and boundary condition error has also shown to be linked to low severity vulnerabilities
- Design Error vulnerabilities
  - found to be a significant category of which a significant proportion is usually of high severity

32

Summary

- The AML was validated on systems, web servers and web browsers
- The Effort-based model was validated on web server's datasets
- The prediction capabilities were tested
- Several estimation approaches were suggested

33

Summary

- Constrained version of AML model was suggested
- Prediction capability is comparable to SRGMs
- Categorized vulnerabilities has been analyzed
- The AML was fitted to categorized data
- Some severity levels has shown strong relationship with some vulnerability categories

34

Future Work

- White Box analysis
  - Identifying vulnerable modules
  - Analyzing the impact of the code reuse
- Studying the impact of patches
  - what happens after a major patch is applied (e.g. SP1, SP2)?

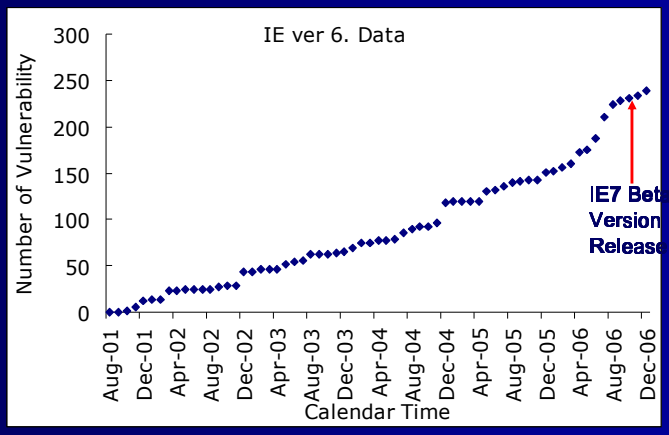
35

Future Work

- Evaluating the vulnerabilities economical impact
  - Incentives for vulnerabilities finders
- Real-time quantitative risk assessment using
  - Vulnerabilities and incidents
- Using Testing-oriented categorization of vulnerabilities

36

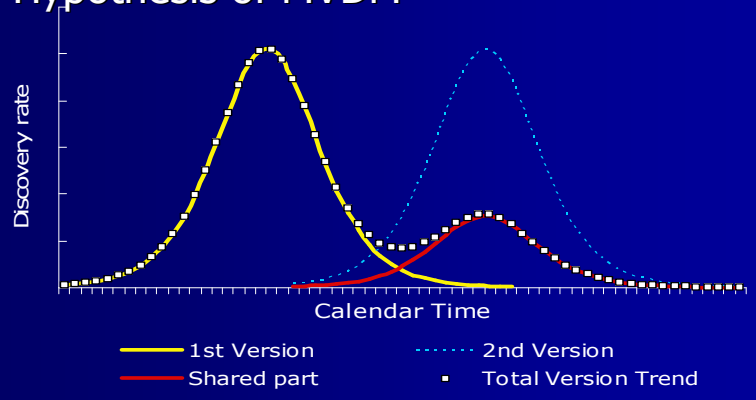
Beta test version effect



37

Multiple Vulnerability Discovery Model (MVDM)

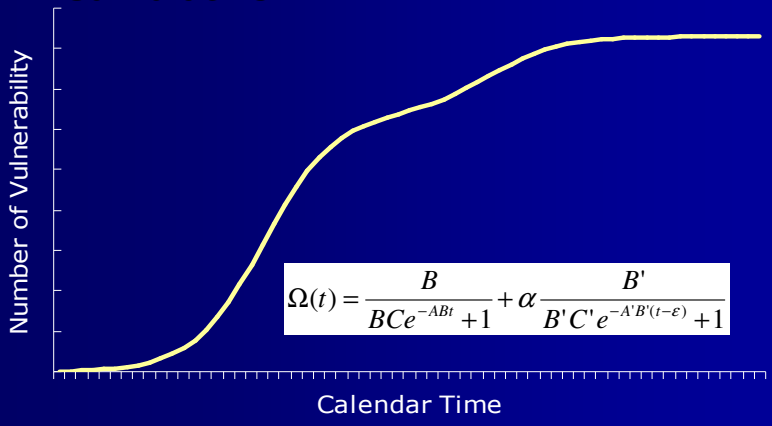
- Hypothesis of MVDM



38

Multiple Vulnerability Discovery Model (MVDM) – Cont.

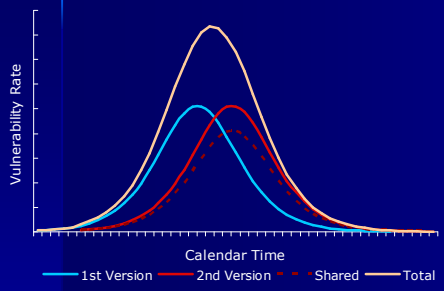
- Cumulative MVDM



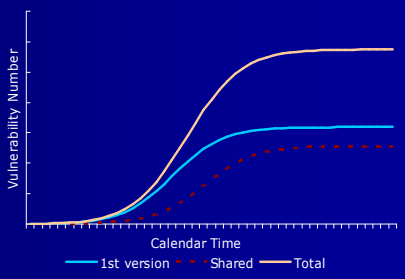
$$\Omega(t) = \frac{B}{BCe^{-ABt}+1} + \alpha\frac{B'}{B'C'e^{-A'B'(t-\varepsilon)}+1}$$

39

One-hump MVDM



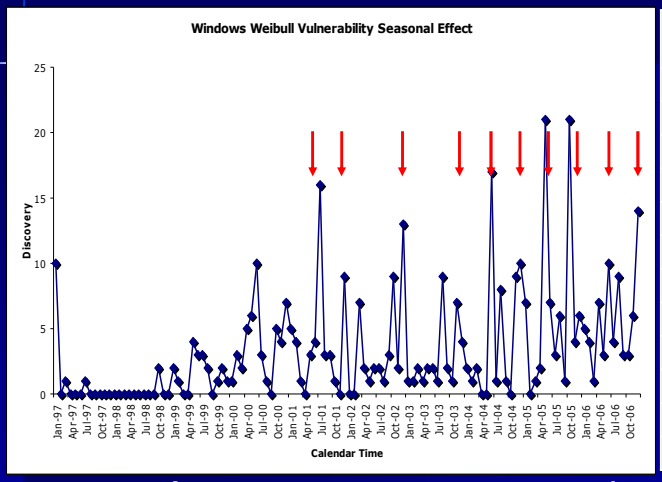
<One-Hump MVDM Rate>



<One-Hump MVDM>

40

Seasonality of Vulnerabilities



Month	Seasonal Effect
March	-1.213
April	-1.846
May	1.123
June	1.888
July	0.008
August	-0.017
September	-2.226
October	1.141
November	-0.260
December	2.068
January	-1.059
February	-2.122

- ARIMA (AutoRegressive Integrated Moving Average)

41

Recent Conference Papers

- W. S–W. , O. H. Alhazmi, and Yashwant K. Malaiya, *Assessing Vulnerabilities in Apache and IIS HTTP Servers*, Proc. of the 2nd IEEE International Symposium on Dependable Autonomic and Secure Computing Sept. 29-Oct. 1, 2006. pp.103-110.
- O. H. Alhazmi, W. S-W., and Yashwant K. Malaiya, *Security Vulnerability Categories in Major Software Systems*, Proc. of International Conference on Communication, Network and Information Security, Oct. 9-11, 2006. pp.138-143.
- J-Y. Kim, O. H. Alhazmi and Y. K. Malaiya, *Vulnerabilities in Browsers: Trends in Internet Explorer and Firefox*, Proc. of 17th IEEE International Symposium on Software Reliability Engineering, Nov. 7-10 2006.
- W. S-W., O. H. Alhazmi, and Y. K. Malaiya, *An Analysis of the Vulnerability Discovery Process in Web Browsers*, Proc. of the 10th International Conference on Software Engineering and Applications, Nov. 13-15, 2006

42