Implementation of MKD-WebServer Rating Application for Analysis of Web performance through SSL

Veereshkumar M Kolli1, Vinaykumar M Kolli2, Vaishakh B3

Dept. of Telecommunication Engg. 1, Dept. of Computer Science & Engg. 2&3 R.V.College of Engineering-Bangalore- 560 059, ¹veerbhadra@rvce.edu.in, ²vmkolli@yahoo.com, ³vaishakh.bargurreddy@gmail.com

Article Info

Article history:

Received Jan 19th, 2013 Revised Jan 21st, 2013 Accepted Jan, 201

Keyword:

SSL TLS Security Handshake Server Rating Cipher and Encryption

ABSTRACT (10 PT)

In recent years, protocols have been developed to ensure secure communications over the Internet, e.g., the secure sockets layer (SSL) and secure electronic transaction (SET). SSL is a deceptively simple technology. It is easy to deploy. SSL provides the necessary security, users must put more effort into properly configuring their servers. Deployment of these protocols incurs additional resource requirements at the client and server. This may have a negative impact on system performance. An practical model is developed to study the performance of a web server based on SSL. In our model, the details of the server certification are represented explicitly. Input parameters to this model are obtained by measuring an existing SSL implementation. Analysed the performance & security through characteristics of SSL.

Copyright © 2013 Institute of Advanced Engineering and Science. All rights reserved.

Corresponding Author:

Veereshkumar M Kolli, Departement of Telecommunication Engineering, R V College of Engineering, RV Vidyaniketan Post, Mysore Road, Bangalore-560098. Email: veerbhadra@rvce.edu.in

1. INTRODUCTION

The Internet and its underlying infrastructure is the most pervasive IT system ever built, accordingly, more and more applications are required for Web services. Thus, preserving the privacy and integrity of these messages in service-oriented architectures becomes a challenging part of business integration, and secure message exchange a requirement for the proliferation of Web services. Hence Secure Sockets Layer became a de facto security standard for the web services.

The Secure Sockets Layer, also known as SSL, was first created by Netscape Communications as the first version of SSL was SSLv2[9]. SSL is the most used security protocol for authentication on the Web, SSL secures data exchange between a client and a server by encrypting it. The SSL makes use of cryptographic encryption of data sent to and from your website. SSL provides a protected TCP channel that can be used by higher order protocols. In this way the SSL keeps malicious outsiders from decrypting the sensitive information. Your customers feel secure because they know that their information has been transmitted over the Internet with all precautions taken. You can recognize a Secure Sockets Layer by its web address prefix, "https."

31

2. RESEARCH METHOD

2.1. Background :

Secure communication between two systems (a client and a server for instance) can be achieved if the following three aspects are guaranteed:

(a) Privacy : to ensure that the data exchanged cannot be viewed by a anonymous user.

(b) Integrity : to ensure that the data are not modified along the way transferred and

(c) Authentication : to ensure that the end systems are indeed the systems that they say they are. SSL protocol succeeds the above three goals of communication though its main objectives as End Point Authentication, Message Integrity, Confidentiality.

To use "https", you are required to have an SSL certificate. The certificate is actually special data identifying your server and informing Internet browsers how to encrypt the data that is sent to it. When you use an SSL certificate, you ensure your eCommerce customers that they are downloading data from your site only. Your SSL certificate is only valid with your website's domain name. Your SSL certificate also guarantees your Internet shoppers that the information that they send via the Internet is secure, because only your server knows how to decode it.

Some web hosting servers include SSL certificates with their hosting packages. Some web hosts require you to buy your SSL certificate separately, a cost of almost \$75 to \$200 per year.

2.2. Methodology :

In this section, we discuss the methodology we use for evaluating the Web Server Performance using SSL.

- a) Calculate the cipher strength
- b) Within SSL processing, study the SSL Handshake and related major components in each phase.
- c) Analyze the crypto operations in the SSL processing in terms of their architectural characteristics like number of rounds, key length, block or stream cipher, key exchange support etc.,

To achieve these three major goals, we employed the analytics to compare the real time values of the server parameters with the range of the possible values for different security levels, thereby giving a rate out of 100 to that parameter.

The SSL Handshake process can be better explained by the following diagram[9].



Figure 1.SSL Handshake Process

2.3. Algorithm :

In step 1: We first look at the certificate of the server to verify that it is valid and trusted. The server fails this step is always assigned a "0" Score.

In Step 2: We inspect server configuration in 6 categories:

- i) Protocol Support
- ii) Key Exchange Support
- iii) Cipher Support
- iv) Validity of the Certificate
- v) Digital Signature Support
- vi) Renegotiation support
- vii) Length of the Security Chain

The parameters considered for the judging the security of web server are the signature algorithm employed (v) such as SHA-1 with MD5 RSA encryption. Not before and not after dates of certificates denoting validity of the SSL certification (iv), the type of public key used (i), issuer name, length of the public key, support of secure renegotiation (which is only available in some of the banking websites), the encryption algorithm used (number of the rounds, size of the key, is it a Block Cipher or Stream Cipher etc.,).

In Step 3: The final score, a number between 0 and 100 is a combination of scores achieved in individual categories. A 0 Score in any category lowers the total score depending on its weightage in the total score. Because small differences between configuration are some times less important, we use weightage and letter grading for the rating of Server.

The following tables shows the Grading Strategy for the given scores :

Numerical Cumulative Score	Grade assigned
Score >=80	А
Score >=65	В
Score >=50	С
Score >=35	D
Score >=20	Е
Score < 20	F
Score < 20	F

Table 1.Scoring Method for Web Server Rating

In Step 4 : According to the user requirement the analystical results along with ratings are displayed in different data analytical forms such as Data list, Pie Chart, Bar Charts etc,.

3. RESULTS AND ANALYSIS

We developed a web application, aligning with the goals of this research paper and algorithm described.

Versite visite 4 Centring Started Versite Versite 4 Centring Started Versite Versite 4 Versite Ve	C Restances de la destance de la	C localhost/M					
Model Veliete* HWNAV HWNAV HWNAV HWNAV HWNAV HWNAV HWNAV HWNAV HWNAV HWNAV HWNAV <th>Monte Vinted + Cetting Started</th> <th></th> <th>IKDCNPMKD/stdwelcome.php</th> <th></th> <th></th> <th>🗇 🛪 😋 🛃 🛪 Google</th> <th></th>	Monte Vinted + Cetting Started		IKDCNPMKD/stdwelcome.php			🗇 🛪 😋 🛃 🛪 Google	
		Most Visited	 Getting Started 				0 8
HWNY HWNY HWNY HWNY HWNY Station: Bring Sint HWNY HWNY HWNY <td>HINAY HAVE A LOOK AT Sisk. Annue A look A annue Sisk. Annue A look A annue</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	HINAY HAVE A LOOK AT Sisk. Annue A look A annue						
HAVE A LOUK AT	HAVE A LOCK AT			HI VINAY			
SSL Soor Hang die SSL Soor H			HAVE A LOOK AT		LogOut		
 Site Linear Balang data Site Site Site Site Site Site Site Site	 Sol. Lis Descriptions find a factor in the Dataset Sol. Lis Descriptions find find find Sol descriptions find find find find find find find find			Enter Web		Click bece to View Ratinos	
 SS. TLI Designerer later later later. Stater and SS. Some family State and SS. Some family State and S	 Status Datagenerii Bers Bastes Steres SS, Leere Bars Steres SS, Le		SSL Server Rating Gide	Address			
 Immed SAL Science Hanny Sitt Ansatz And SAL Later BLOCROLL Major and Mathin Mathin Mathin Mathin Mathin Mathin <li< td=""><td> Instruct SLA General Statute Instruct SLA General St</td><td></td><td>SSL /TLS Deployment Best Practices</td><td></td><td></td><td></td><td></td></li<>	 Instruct SLA General Statute Instruct SLA General St		SSL /TLS Deployment Best Practices				
* Will soop and Lake I Museum 2014 * Museum 2014 * Museum 2015 * Organized III. Museum 2015 * Museum 2015 *	Not which we have a solutions • With we have a solutions • Management Media • Manageme		Internet SSI Server Survey				
 Instant to Loss Instant to L	 INSTANT DECISION OF A DECISION OF A		· MAN and as 600 Long		TASK PROGRESS:		
BLOROLL 0% · Angelander Moll · Angelander Moll · Angelander Moll · Angelander Molla Prefix · Openeet Mit Matt Termologyna Que	BLORROLL 0% · Sustained Mide · Sustain		· Will page on SSL Layer				
LOURINE Conserver, fasting Applications - Medilla Frienda: Conserver, fasting Applications - Medilla Frienda	DUDVIKL 06 · Manual III Mile · Memories of TCS Tech Bans Bengares Bages, 502 · Operated III Mile Technologues Quit · Operated IIII		RIDCROLL				
Augustation Madel	 Adaptions Model Adaptions Mo		DEDUNOLE		0%		
 Maximum Madia Maximum Andali <l< td=""><td>Maximum Made Maximum Made Material Materia</td><td></td><td></td><td></td><td></td><td>ß</td><td></td></l<>	Maximum Made Material Materia					ß	
 Memores <	Subtraction Dial Subt		 Vinaykumar, M.Kolli 				
NENORES • American II TO The American Strategy • Agenered III Mile Transforgens Quet • Agenered III Mile Tra	MEMORES		<u>Vaishakh B N</u>			Click here to View previous ratings	
MEMORES	MEMORES * Brannenge ut TCS Toch Rives Rives Rights 2002 • Departed Rive Application - Health Friefrax • Departed Rives Application - Health Friefrax • Departed Rive						
 brane-size at TCS Tabli these Bargeane Brane-Size Connecting. Connecting.	Baseness of TICS both these Bargeare Baseness Baseness Bas		MEMORIES		back		
• Burne-score TSS Tech Agene Relegatestion • Burne-score TSS Tech Agene Relegatestion • Organisestion							
Biggin 2022 • Organized III: Mile Tennologene Quit State Medicance Reality Applications - Medilla Fineface • Ononettings. • Ononettings.	Biggin, 2012 • Organised link Mite Thereodogene, Qatz SSS. ModeServer Rating Applications - Modella Firefor: • Connections • Connections • Connections • Connections • Connections • Connections • Connections • SSS. Mode Rating Calab • SSS. Mo		Runner-ups of TCS Tech Bytes Bangalore				
Deparend III: Mile: Tamodinyous Que	Consection Mile Transforgen Que		Region 2012				
			· Openand Bit Min TestarCounty C.				
	COnvecting		 Schoolsen and sear transpolation data 				
Most Viside Minimum Sign Stated Minimum Sign Sta	Certified Stated Certified S	Conneccing	/MKDCNPMKD/stdwelcome.php			o • 📢 🗶 📖	
HVINAY HAVE A LOOK AT + WINAY HAVE A LOOK AT + Sisk denser filtering Clist - Sisk denser f	HVRAY HWE ALDOK AT HVRAY HWE ALDOK AT HVRAY HVRAY HVR	a Most Visite	d 👻 🗌 Getting Started				0.0
HVNAY HWVE A LOOK AT HVNAY HWVE A LOOK AT HVNAY HWVE A LOOK AT HVNAY HWVE average and Sal Assee Saleman HVNAY HWVE average and Sal Loop HVNAY HVNAY HVNAY HVNAY HVNAY HVNAY HVNAY HVNAY HVNAY HVNAY HVNA	HUNAY HAVE A LOOK AT UNIT OF A CONSTRUCTION OF	-					
H WNAY HAVE A LOOK AT H WNAY - Leacher States and the second s	HVRAV HVE A LOCK AT HVRAV HVE A LOCK AT HVRAV HVRAV HVRA						
HAVE A LOOK AT • Landon HAVE A LOOK AT • Standard Control of the star value fraction of the star value	HAVE A LOOK AT			HIVINAV			
State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State			HAVE A LOOK AT		LogOut		
State Constraining Constra	Statusen Entron Gibb Annum Statusen Stat			Enter	umu essele com		
SIX_CITS_Demonstrate their finances instruct SIX_Annex_Storey thinks append SIX_Liber: ELOGROLL 50% vinancestrate VINUE			SSL Server Rating Gide	Address			
Internal SSL Batter Source Mark and SSL Later BLOGROLL SOV Market SSL Mark Market SSL Market SSL Market SSL Market SSL Mark	Internet Sites. Barrow Saveray States and an Sites Later States and an Sites Later Software States Softwa		SSL /TLS Deployment Best Practices				
MINLange an SQL Layer Log TASK PROGRESS BLOGROLL S0% Minutered Minute	MEMORES MEMORES MEMORES MEMORES Memory		Internet SSL Server Survey				
BLOGROUL 50%	BLOGROLL 50%			Þ	TASK PROGRESS:		
BLOGROLL 50%	BLOGROLL 50%		Whi page on SSL Layer				
Mohammer Witch	Yotophania M Assi Satabab 1,13 Gita bare to View previous ratings MENORES back		 Whit page on SSL Layer 				
Moniformatic M Koff	Straduurus Missie Sudatusti Ji Si MEMORES Model Mark Memory		Will page on SSL Layer BLOGROLL		50%		
	2 · Santanti I. N. Citak New B View provides addres. MEMORES basis		Whill page on SSL Layer BLOGROLL		50%		
Velichath B.N Click here to View previous ratings	MEMORES Lines		With page on SSL Layer BLOGROLL Vitageoree M Kelli		50%		
	MEMORIES		Whit page on SSL Layer BLOGROLL Vionatures M Hotel Vionatures M Hotel Vionatures M Hotel		50%	Click here to View provious ratings	
23190131			With spage an SSL Lawer ELOGROLL Without Minist Ministration II IN MEMORIFS		50%	Click here to View provious ratings	
MEMORIES			White sample are SOL Larver BLOGROLL Vitransformer Ministe Vitransformer Ministe MemoRies		50%	Click here to View provided ratings	
Visitadh R N Click here to View previous ratings			Whit page on SSL Layer				
			White pages an SQL Layer BLOGROLL Vitraguarmer M.Kold Vitraguarmer M.Kold		50%	Click here to View provious satings	
MEMORIES			With super an SOL Layer BLOGROLL Statustance M Rold Machine R N Memories		50%	Click here to View provious ratings	
MEMORIES	Burner syn of TCS Tesh Botes Baropatore		 With same an 50k Lawr BLOGROLL Wonshame M Kells Wonshame J. 3: MEMORIES 		50%	Click here to View previous strings	
	Burner-ups of TCS Tech Bytes Bargatore Walting for forsiblet		White page on SSR. Layer BLOGROLL Wineykonner M Kotel Waterparter B. N		50%	Click here to View provious ratings	
MEMORIES Invest • Remercipant TCS Tech Barrel Barguitane wakiting for locathoost.	The managine assessments.	waiting fer locality	With same as 50k Laws ELOGROLL Vionstanse M Kell Vionstanse M Kell MEMORES Benne sage at 10% Torch Amerikangusee est		50%	. Cisk here to View provision natings	
MEMORES Bank waiting for locations	THRUTY INFORMATION	Waiting for locali	 With upper an 55% Lawr BLOGROLL Wondorme M Motil Method nu M Method nu M Method nu M Name upper d TCS Tech Intern Biogetime notice. 		50%	Clisk here to View providue ratings.	
MEMORIES Book waiting for localhost		Waiting for local#	With support SOL Layer BLOGROLL Vonstance Minute Vonstance Minute Memores Beners spin of TCS Treet. Bases Biopatore est.		50%	. Oli A here to View previous schirgs.	
MEMORIES Back * Back differences on all COL Texth Reven Bacquitere weakting for locationst		Walting for local	With super an SOL Layer BLOGROLL Montenance M molt Montenance M molt Montenance M molt Memorals Memorals Managements M		50%	. Click here to View previous entropy.	
MEMORES Back * Banksey of ICS Into them Bacyular valing for localbox. SSL WebServer Racting Application - Mozilla Firefex.	10 SSL Webserver Rating Application - Mozilla Firefox	Waiting for localb	Yith sugar an SOL Layer ELOGROLL Yonahamar M.Kata Sachard B.2 Memores Banner seg of TC3 Tech Dates Broyakow est. Elog Application - Modilla Firefox		50% bea	[Cità here to Vere provoquentitoja,] [Cità here to Vere provoquentitoja,] ■ 5-17 § 12] ← Mon Jan 14 o 23 PM	4 1 vijaylaze
MEMORES BARK Mailing for localbox SSIL WebServer Raining Application - Mosilia Frefex. Mon.an 14 625 FM 1 vijeplax	KD SSL WebServer Rating Application - Motilla Firefox MCD SSL WebServer Rating Application - Motilla Firefox MCD SSL WebServer Rating Application - Motilla Firefox	Waiting for local?	Vitili support SOL Layer BLOGROLL Vitili support SOL Layer Vitili support SOL Layer Vitili support SOL Layer MemoRes MemoRes		50%	Citik bereta Wewpressuscialings. Citik bereta Wewpressuscialings. ■ 147 \$ tyl 4+ Mon Jan 14 628 PM	4 1 vijaylass
MEMORES	KD SSL WebServer Rating Application - Mozilla Firefox MIO SSL WebServer Application - Mozilla Firefox MI	Waiting for local?	With super an SAL Layer BLOGROLL Manhammer Mindl Manhammer Mindl Manhammer Mindl Manhammer Mindl Manhammer San at 102 Tech Anton Bargatom atter Application - Manhammer Manhamme	.00m	50% (Main)	Citik bere in View previous statings 2 ■ 5-57 \$ t_al <+ Mon.Jan 14 c.25 PM • € 3 • Congle	4 L vijaylaxa
MEMORES Meximp for localhost. SSL WebServer Rating Application - Mozilla Firefex. Meximp Structure Rating Application - Mozilla Firefex. M	KO SSL Webserver Rating Application - Mozilla Firefox CO SSL Web	Waiting for local SSL WebServer Ra MCK SSL WebS Calaboxt Mont Solutions	With sample and SAL Later BLOGROLL Vionatume Al Kalal Vionatume Al Kalal Memore Sala Memore Sala Control Andre S	.00	50% bea	$\begin{tabular}{lllllllllllllllllllllllllllllllllll$	4 1 vijaylax
MEMORES	CO SSL WebServer Rating Application - Mozilla Firefex Control Contro Control Control Control Control Control Control Control Control	Weiting for localit SLL WebSover R R MKD SSL WebS C B Localitoxt	Vitili support SOL Layer BLOGROLL Vongenerer Minute Vongenerer Minute Vongenerer Minute MemoRes Benerer son of TCS Treft Mens Bregatere sot Benerer Mating Age	.com	50% box	Citik bere its Weer previous ratings. 2 ■ Exit \$ val • € • € • €	4 L vijaylaxa
MEMORES	CD SSL WebServer Rating Application - Mosilia Firefox CD SSL WebServer Rating Application - Mosilia Firefox () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the server google.com () @ Inclaims 2 Model and a constraint of the serv	Waiting for local SSL WebServer R R WKD SSL web/ KD SSL web/ MKD SSL w	With support = SOL Layer BLOGROLL Vitashama Aladi Wandows Biol Manage and TCS Tech Anna Bargeton Memorals Manage and TCS Tech Anna Bargeton setting Application - Modella Pirefax enery Fating Appl Debool/PireCip Vicashing Appl Laddress-www.google Getting Started	.com	50%	Citik bere to View previous satings; 2 ■ 5x17 \$ tail << Mon Jan 14 628 Pre	4 1 vijaylazz
MEMORES Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memores Memor	KD SSL WebServer Rating Application - Mozilla Firefox MMD SSL WebServer Rating Application - Mozilla Firefox MMD SSL WebServer Rating Application - Mozilla Firefox MMD SSL WebServer Rating Application - Wood Rating Applications - Wood	Waiting for local SSL WebServer Ra MKD SSL WebS () Dealbox () Dealbox () MKD Visite	With support 50L Laper BLOGROLL Worksmine Mixed Worksmine Mixed Worksmine Mixed Memores age of TCE Tech. Being Bargetore memore fracting Age. worksmine age of TCE Tech. Being Bargetore monocommonly support address-waves google d Contains Started HAVE ALLOCK AT	.com RATING OF WEB3 Processing		Citik hereb View predestratings 2 ■ Citif & t _{al} ← Mon Jan 14 620 Ph 	4 1 vijaydaar 0 0 -
MEMORES Memory	KD SSL WebServer Rating Application - Mosilia Firefox KD SSL WebServer Rating Application - Mosilia Firefox MID SSL WebServer Rating Applic	Weiting for local SSL WebServer Ra SSL WebServer Ra SSL WebServer Ra Most Visite	Vitil support SUL Layer BLOGROLL Vitil support SUL Layer V	com RATING OF WEB: Presenting	SON bea Bea Bea Beaging con 40 vocations in beach sumport con 40 vocations in beach sumport con 40 vocations in beach	Citik bereits Vier previous stringen 2 ■ 1:47 \$ val • € 34 • Coople	4 1 vijeylazz 0 0 m
MEMORES	CD 55L WebServer Rating Application - Mozilla Firefex CD 55L WebServer Rating Application - Mozilla Firefex CD 55L WebServer Rating Ap_ @ MRD 55L WebServer Ap_ @ MRD 55L WebServer Ap_ @ MRD 55L WebServer Ap_ manual application Ap	Waiting for local SSL WebServer R R WKD SSL WebFree R Most Visite	With support SUL Layer BLOGROLL Visuations Mindl With Support SUL Memoral SUL	com RATING OF WEB Processing Processing	50%	Citik bere to View previous cotings; ■ 1547 \$ val << Mon Jan 14 626 PM ■ 1547 \$ val << Mon Jan 14 626 PM	4 1 vijaylaan O 🖂
MEMORES	CO SSL WebServer Bating Application - Mosilia Frefex. CO SSL WebServer Bating Application - Mosilia Frefex. CO SSL WebServer Rating Ap CO SSL WebServer Ap CO SSL Web	Waiting for local SSL WebServer R R MRD SSL WebS Composition of the second seco		.com RATING OF WEE: Processing Processing	50% bed	Citik bere is View previous satings ■ 5-57 \$ t _u] (+ Mon Jan 14 o 25 PM • Couple	4 1 vijeytaar 0 🖂 i
MEMORES Memory	KD 55L Webserver Rating Application - Mostlla Firefrax KD 55L Webserver Rating Appli	Waiting for local SSL WebServer Ar WED SSL WebS C MED SSL WEBSC C MED SSL WEBSC SSL WEBSC C MED SSL WEBSC SSL WESSL WEBSC SSL WEBSC SSL WESSL WEBSC SSL WESSL WE		.com <u>RATING OF WEB</u> Processing	50%	Cità bertis Viergowousseitings. 2 ■ bt7 \$ tal 4+ Mon.Jan 14 623.Ph • € 8 • Coogle	i ⊥vijejazi (O ⊡
MEMORES	NO 55L WebServer Rating Application - Mozilla Firefox NO 55L Web	Waiting for local SL WebServer & Ra WRD SSL WebSite Control of the state MRD SSL WebSite MRD SSL WebSite	With support SUL Layer BLOGROLL Monitoria Mandi Watersame Mandi Watersame Mandi Watersame Mandi MedioRES MedioRES MedioRES MedioRES Mandia Application - Medilla Filerfox anner Maning Appl MedioRES MedioRES Getting Started MedioRES Support Support Support Support MedioRES MedioRES Support Support MedioRES Support Support MedioRES Support Support	com RATING OF WEB Processing	SON	Citik here ta View previous catilitys. 2 ■ 1:47 \$ xdl ← Mon Jan 14 623 Pho • € \$ 30 Coogle	4 1 vijajaza 0 0 0

Not After : Sep 30 23:59:59 2013

sha1WithRSAEncryption issuer=/C=ZA/O=Thawte Con-

Protocol : TLSv1.1 Cipher : ECDHE-RSA-RC4-SHA

1024 bR

4

back

where is google.com

Following are some of the snapshots of our project :

BLOGROLL

Yinaykumar M Ko

Verstrakti B.N
 MEMORIES

Bunner

Region 2012



4. CONCLUSION

Given that there is no single correct configuration for every possible use of SSL, we aim merely to give some reasonable advice in terms of rating that works for majority of users. Individual needs may vary but as a rule of thumb higher the value of website, stricter the configuration should be. The rating will generate awareness and enable both users and corporate sector releasing websites regarding the ssl configurations required for a secure and smart website.

The goal of this Implemented project is to measure the *effective security* of SSL. After some experimentation with an assessment of substantially all public SSL sites (about 150 most popular of them), based on Alexa's list of most popular sites in the world. Working with a smaller list is more manageable and allows us to conduct the surveys more often. It also allows us to conduct more thorough analysis to look for application-layer issues that may subvert SSL security. In addition, focusing on popular sites – we believe – gives us more relevant results and also excludes abandoned sites.

Having worked with several data sets, each drawing from a different list of sites, we have come to understand that what we are presenting in our surveys is not a measurement, but a reasonable approximation of the state of SSL. More important than the results from any one round of tests is how the measurements change over time. The adoption of a single selection methodology and a switch to monthly testing should give us an indicator of where we're heading, which is what we believe matters.

REFERENCES

- [1] K. Kant, R. Iyer, and P. Mohapatra. Architectural impact of secure socket layer on internet servers. In International conference on computer design (ICCD), page 7, 2000.
- [2] R. Mraz. An architecture for a high volume ssl internet server. In Proceedings of Seventeenth Annual Computer Security Applications Conference, page 7, Dec. 2001.
- [3] OpenSSL, http://www.openssl.org/
- [4] Xiaodong Lin, Johnny W. Wong, and Weidong Kou, Performance Analysis of Secure Web Server Based on SSL, International journal paper, page no. 249-261.
- [5] C. Michael Chernick, Charles Edington III, Matthew J. Fanto, Rob Rosenthal, NIST-US department of Commerce, a special publication on "Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations", pg.No.800-52.
- [6] Eric Rescorla, "SSL and TLS Designing and Building Secure Systems" Addison Wesley 3rd Printing_ Aug 2001.
- [7] Vicen c Beltran, Jordi Guitart, David Carrera, Jordi Torres, Eduard Ayguad'e and Jesus Labarta, Performance Impact of Using SSL on Dynamic Web Applications, XV JORNADAS DE PARALELISMO—ALMERIA, SEPTIEMBRE 2004.
- [8] SSL Server Rating Guide, 21 July 2009, SSL Labs (www.ssllabs.com).
- [9] Wikipedia.org [on SSL and TLS]

BIBLIOGRAPHY OF AUTHORS (10 PT)

Veereshkumar M Kolli. Department of Telecommunication Engineering, R V College of Engineering, Bangalore-560059 9844103324
Vinaykumar M Kolli Department of Computer Science and Engineering, R V College of Engineering, Bangalore-560059 9164616461
Vaishakh B N Department of Computer Science and Engineering, R V College of Engineering, Bangalore-560059 9035872670