Sanjay Rawat

Contact Information

Verimag
Centre Equation
2, ave, de Vignate
38610 GIERES (France)

Mobile: +33 06 64549739
E-mail: sanjayr@ymail.com
Home-Page: http://www-verimag.imag.fr/~rawat/

Objective

Placement in a research position that allows for research in topics related to *program analysis*, leading to better code quality (for example, security program analysis, application security) with a focus on *security vulnerability code analysis* including static and dynamic analysis techniques.

Research Interests

Static and Dynamic Security code analysis (using techniques dataflow analysis, abstract interpretation, value-set analysis for pointer analysis, equational reasoning etc.), Binary analysis, smart fuzzing, machine learning for security, evolutionary algorithms for security testing (fuzzing), intrusion detection systems, network security, application security.

Education

University of Hyderabad, Hyderabad, India

Ph.D., Department of Computer & Information Sciences and Institute for Development & Research in Banking Technology (IDRBT) July 2001 - December 2005 (submitted in June 2005)

- Thesis Topic: *Efficient Data Mining Algorithms for Intrusion Detection*
- Adviser: Prof. Arun K. Pujari and Dr. V. P. Gulati
- Area of Study: Intrusion Detection Systems using Data Mining & Machine Learning Techniques
- Affiliation: Institute for Development and Research in Banking Technology, Hyderabad, india

Dr. B R Ambedkar University, (formerly Agra University) Agra, India

M.Phil., Mathematic Dept., Institute of Basic Sciences, July, 1997 June, 1998

- Thesis Topic: *Some Secret Sharing Schemes*
- Adviser: Professor sunder Lal
- Area of Study: Cryptography
- Marks aggregation: 87.0%

M.Sc., Agra College, Agra July, 1995 May, 1997

- Marks aggregation: 74.75
- Area of Study: Mathematics

B.Sc., Agra College, Agra July, 1992 May, 1995

- Marks aggregation: 70.85
- Area of Study: Mathematics, Physics, Chemistry

Academic Appointments

Postdoctoral Fellow December 2009 to present

Verimag, Joseph Fourier University (University of Grenoble), Grenoble, France

- DIAMONDS (ITEA2 project) Development and Industrial Application of Multi-Domain Security Testing Technologies
  - DIAMONDS aims at developing efficient and automated security testing methods of industrial relevance for highly secure systems in multiple domains (incl. e.g. banking, transport or telecommunication).

  - DIAMONDS goal is based on the observation: *The security of a software-intensive system is directly related to the quality of its software. In particular, over 90% of software security incidents are caused by attackers exploiting known software defects.*
  - My focus is on smart fuzzing, based on static/dynamic analysis of binary executable of the application to find vulnerable patterns and taint analysis.
  - Techniques: Static code analysis (abstract interpretation and value-set analysis), dynamic code analysis, taint analysis, Control- and data-flow techniques, Smart Fuzzing, Evolutionary algorithms.
- VULCAIN- Vulnérabilités : caractérisation et inférences
  - Vulcain project aims at analyzing software vulnerabilities using white-box and black-box techniques. In particular, I am focusing on intelligent fuzzing to discover vulnerabilities in applications.
  - Techniques: Static code analysis, dynamic code analysis, taint analysis, Control- and data-flow techniques, Smart Fuzzing, Evolutionary algorithms.

Postdoctoral Fellow March 2007 to October 2007

Department of Information Engineering and Computer Science, University of Trento, Italy

- BIONETS and CASCADAS EU Projects.
  - Both of the projects aim at autonomic capabilities of the networks to provide robust systems using biologically-inspired concepts permeating the network and its services, blending them together, so that the network molds itself to the services it runs. In particular, I worked on biologically inspired computer networks with a focus on Intrusion Detection, based on Artificial Immune System.
  - Techniques: autonomic computing, artificial immune system based security.

Reseach Fellow Jan 2001 to June 2005

IDRBT- Institute for Development & Research in Banking Technology

- Worked on security architecture of INFINET-INdian FInancial NETwork.
- While perusing PhD, I was also involved in internal security incidence analysis.
- Taught various topics in network security (e.g. firewalls, IDS) during workshops organized in IDRBT for banking professionals.

UGC Project Fellow July, 1999 to Dec 2000

Institute of Basic Sciences (Dr. B R Ambedkar University), Agra, India.

- I worked as Project Fellow in the UGC project on Cryptography.
- Taught cryptography to M.Phil. class as teaching assistant.

Industrial Experience

Infosys Technologies, Hyderabad, India.

Research Associate, SETLabs **Dec 2007 to Nov 2009**

- Involved in R&D activities to address innovative solutions pertaining to various domains like data mining and security.
- Focused on security code analysis using white-box and black-box techniques.

Intoto (I) Pvt. Ltd. (now FreeScale), Hyderabad, India

Security Research Engineer **June 2005 to Feb 2007**

- Analysis of computer attacks/vulnerabilities and form signatures for the Intoto IIPS, called IntruPro.
- Presenting results of the analysis and research in the form of Internet security advisories.
- Involved in suggesting new features and functionalities in the IIPS engine.

Teaching

- Code Optimization and Code Generation (Master course on Programming Languages and Compilers, MOSIG)- 2012.
- Cryptography and Number Theory (M.Phil course, 1999-2000).
- Network Security: Firewalls and Intrusion Detection (IDRBT, 2002 -2004)
- Networking lab (M.Tech, IDRBT, 2001-2002)

Projects

DIAMONDS Oct, 2011 to present

- DIAMONDS is a security testing project whose motivation is based on the observation by the Software Engineering Institute, US, 2009: The security of a software-intensive system is directly related to the quality of its software. In particular, over 90% of software security incidents are caused by attackers exploiting known software defects. DIAMONDS addresses this increasing need for systematic security testing methods by developing techniques and tools that can efficiently be used to secure networked applications in different domains. My focus is on software vulnerability detection and statically/dynamically testing them. In particular, I focus on analyzing binary executables of the application statically and dynamically to find tainted path and generating tests to trigger vulnerabilities. Static analysis is based on *Abstract Interpretation* and *Value-Set Analysis*. Input generation is based on *evolutionary algorithms*.

VULCAIN Dec, 2009 to Sept, 2011

- Vulcain project focuses on analysing software vulnerabilities statistically and dynamically. I work as postdoc fellow along with other faculty members. I proposed a framework for dynamic analysis of applications using evolutionary algorithms. This techniques is also known as *intelligent or smart fuzzing*. I made use of an existing technique called *taint dependency sequence* to get a *tainted path* and then produced inputs that executed the tainted path to trigger the vulnerability. The approach is able to learn and satisfy light constraints automatically. Another novel aspect of this work is the metric on *exploitability* of the discovered vulnerability. On-going work on this project is the analysis at binary (assembly) level and using more sophisticated techniques, e.g. program slicing, to analyze program statically and dynamically.

BIONETS and CASCADAS, University of Trento, Italy (March 2007 Oct 2007

- BIONETS and CASCADAS are EU funded projects. I worked there as Postdoc. My role was to research and propose security solutions, which included intrusion detection, privacy and authentication in WSN. As both of the projects were based on autonomic communication environment, it was a challenging task to understand and learn various malicious activities. Therefore, I focused on *autonomic intrusion detection system* to learn various attacks in autonomic way.

Revamping of IDRBT network and its connectivity with INFINET March, 2001- May, 2002

- Under this project, various network architectures have been studied and accordingly an optimal solution is proposed and implemented. The implementation part includes deployment of routers, firewalls, IDS and other devices. A *duel-homed architecture* is implemented for optimal link utilization.

U.G.C sponsored research project July, 1999- Dec 2000

- Under this project entitled *A study of some protocols related to secrecy, key exchange, authentication and identification using public key cryptosystems*, I worked as a Project Fellow. Various cryptographic schemes have been studied and improvements are suggested. New schemes for secret sharing have been proposed.

M.Phil. Dissertation June, 1998 Dec, 1998

- Entitled *Some Secret Sharing Schemes*, also popularly known as Threshold Schemes. A secret sharing scheme is a method of partitioning and distributing a secret among participants such that only the authorized sets of participants can recover the secret. In the dissertation, a geometrical construction of *pre-positioned secret sharing scheme* is proposed using finite geometries i.e. projective and affine geometries. The focus is on *how to change the value of the secret without changing the shares of the secret that are already distributed to the participants*.

Refereed Journal Conference Publications

1. Sanjay Rawat, Laurent Mounier and Marie-Laure Potet, *Static Taint Flow Analysis: Discovering Vulnerable Paths in Binary Executables*, Submitted to RAID 2013.
2. Fabien Duchene, Sanjay Rawat, Jean-Luc Richier, Roland Groz, *A hesitation step into the blackbox: Heuristic based Web-Application Reverse-engineering*, Accepted in: NoSuchCon (NSC), Paris, France May 2013
3. Fabien Duchene, Sanjay Rawat, Roland Groz and Jean-Luc Richier, *Kameleon-Fuzz: Fuzzing Intelligent de XSS Type-2 Filtrés selon Darwin*, Accepted in: Symposium sur la sécurité des technologies de l'information et des communications (SSTIC), Rennes Beaulieu Sud, France, 5-7 June 2013.
4. Gustavo Grieco, Laurent Mounier, Marie-Laure Potet and Sanjay Rawat,*A stack model for symbolic buffer overflow exploitability analysis*, Accepted in: International workshop on Constraints in Software Testing Verification and Analysis CSTVA'2013 (with ICST 2013).
5. Sanjay Rawat, Fabien Duchene, Roland Groz and Jean-Luc Richier, *Evolving Indigestible Codes: Fuzzing Interpreters with Genetic Programming*, Accepted in: IEEE Symposium on Computational Intelligence in Cyber Security (CICS 13), in association with IEEE SSCI 2013, 15 Mon -19 Fri April 2013, Singapore.
6. Sanjay Rawat and Laurent Mounier, *Finding Buffer Overflow Inducing Loops in Binary Executables*, In Proc. of The Sixth International Conference on Software Security and Reliability (SERE 2012), Washington DC, US, 2012. pp 177-186.
7. Fabien Duchene, Roland Groz, Sanjay Rawat and Jean-Luc Richier, *XSS Vulnerability Detection Using Model Inference Assisted Evolutionary Fuzzing*, In proc. of the Third International Workshop on Security Testing (SECTEST), in association with ICST 2012, Montreal, IEEE CS press, April 2012
8. Sanjay Rawat and Laurent Mounier, *Offset-Aware Mutation based Fuzzing for Buffer Overflow Vulnerabilities: Few Preliminary Results*, In proc. of The Second International Workshop on Security Testing (SECTEST) , in association with 4th ICSTW 2011, Berlin, IEEE CS press, March 2011, pp 531-533
9. Sanjay Rawat and Laurent Mounier, *An Evolutionary Computing Approach for Hunting Buffer Overflow Vulnerabilities: A case of aiming in dim light*, In the proc. of 6th EC2ND (European Conference on Computer Network Defense, Berlin, Oct 2010, IEEE CS, pp 37 - 45
10. Sanjay Rawat and Ashutosh Saxena, *Danger Theory Based SYN Flood Attack Detection in Autonomic Network*, Proc. Of the 2nd International Conference on Security of Information and Networks (SIN 2009), 6-10 October, Gazimagusa, North Cyprus 2009
11. Sanjay Rawat and Ashutosh Saxena, *Application Security Code Analysis: A Step towards Software Assurance*, International Journal of Information and Computer Security (IJICS), Vol. 3, No. 1, pp.86110, 2009.

12. Subrat Kumar Dash, Sanjay Rawat and Arun K. Pujari, *Use of Dimensionality Reduction for Intrusion Detection*, In Proc. of the Third International Conference on Information Systems Security (ICISS 2007), December 2007, LNCS 4812, Springer 2007, ISBN 978-3-540-77085-5

13. Subrat Kumar Dash, Sanjay Rawat and Arun K. Pujari, *LLE on System Calls for Host Based Intrusion Detection*, In: Proc. of the International Conference on Computational Intelligence and Security (CIS2006) November 3-6, 2006, Guangzhou, China, IEEE, 2006

14. Challa S. Sastry, Sanjay Rawat , Arun K. Pujari and V. P. Gulati, *Network Traffic Analysis using SVD and Multiscale Transforms*, Information Sciences. 177, 23 (Dec. 2007), 5275-5291. Elsevier Science Inc. New York, NY, USA

15. Subrat Kumar Dash, Sanjay Rawat, G. Vijaya Kumari and Arun K. Pujari, *Masquerade Detection Using IA Network*, In Proc. of First International Workshop on Applications of Constraint Satisfaction and Programming to Computer Security Problems, Sitges, Spain, 1st October 2005. pp 18-30.

16. Sanjay Rawat , Arun K. Pujari, V. P. Gulati and V. Rao Vemuri, *Intrusion Detection using Text Processing Techniques with a Binary-Weighted Cosine Metric*, Journal of Information Assurance & Security (JIAS), Volume 1, Issue 1, March 2006. pp 43-50.

17. Sanjay Rawat, Arun K. Pujari and V. P. Gulati, *A Fast Host-Based Intrusion Detection System Using Rough Set Theory*, Transactions on Rough Sets, Vol 4, Springer, LNCS# 3700. pp 144-161

18. Sanjay Rawat, V. P. Gulati and Arun K. Pujari, *Frequency And Ordering Based Similarity Measure For Host Based Intrusion Detection*, Journal of Information Management and Computer Security, 12(5). Emerald Press. 2004. pp. 411-421

19. Sanjay Rawat, Arun K. Pujari and V. P. Gulati, *On the Use of Singular Value Decomposition for a Fast Intrusion Detection System*, In: Proc. of the First International Workshop on Views On Designing Complex Architectures (VODCA 2004), Bertinoro, Italy, ENTCS, vol 142, Elsevier 2006. pp. 215-228

20. Sanjay Rawat and Challa S. Sastry, *Network Intrusion Detection System Using Wavelet Analysis*, In: Proc of the 7th International Conference on Information Technology (CIT 2004), Hyderbad, India. LNCS # 3356, Springer.

Contributed Book Chapters

1. Challa S. Sastry and Sanjay Rawat, *Application of Wavelets in Network Security*, Vemuri, V. and V. Sreeharirao, (Eds.), ***Enhancing Computer Security with Smart Technology***, CRC Press, 2006. pp 209-228

Other Publications

1. Sanjay Rawat, V. P. Gulati and Arun K. Pujari, *An Intrusion Detection Scheme Based on Frequency and Ordering*, In: Proc of the National Workshop on Cryptology 2003, Chennai, India. 2003

2. Sanjay Rawat and Sunder Lal, *A Pseudo Dynamic Threshold Scheme*, Journal of Natural & Physical Sciences, vol. 14(1-2), 2000. pp 97-104

3. Ashutosh Saxena and Sanjay Rawat, *Y2K38*, IDRBT Working Papaer 9, 2005.

Technical Report

1. Sanjay Rawat and Laurent Mounier, ***Value-Set-Analysis of Assembly (REIL) Programs (Technical Report)***, Verimag Technical Report, 2011. [*This report describes some technical details and methods that are basis for our recent work, like pointer analysis at binary level.*]

2. Sanjay Rawat, Dumitru Ceara, Laurent Mounier and Marie-Laure Potet, *Combining Static and Dynamic Analysis for Vulnerability Detection*, Verimag Lab, UJF, Grenoble, France. 2010.

3. Sanjay Rawat , Arun K. Pujari and V. P. Gulati, *Intrusion Detection Systems: A Survey on Algorithms and Methods*, 2005. AI Lab, CS Dept., University of Hyderabad.

Technical Presentations

1. *Return Oriented Programming : A Perspective*, SecurIMAG Technical Talk, Ensimag, INP Grenoble, Grenoble, France.

2. *An Improved kNN-Scheme for Intrusion Detection with a New Binary Weighted Cosine Metric*, In: One Day Tutorial on Intrusion Detection & Computer Security, Dept. Of Computer & Information Sciences, University of Hyderabad, Hyderabad, India.

3. *Some Protocols for Multisignatures*, In: 66th Annual conference of Indian Mathematical Society, Aurangabad, India. 2000

4. *A Dynamic Threshold Scheme*, In: 65th Annual conference of Indian Mathematical Society, Rewa, India. 1999

Summer Schools

- *SecNet 2005*, IIT Bombay, Feb 11 - 13, 2005
- *4th International School on Foundations of Security Analysis and Design*, Bertinoro University Residential Center, Italy. 6-11 September 2004
- *VLDV summer school on Frontiers of Database Technology*, IIT Delhi, India. 1- 4 June 2004.

Honors & Awards

- IDRBT (RBI, India) Research Fellowship for PhD
- M.Phil Topper (1998) class, IBS, Dr. B. R. Ambedkar University.
- Recipient of U.P. State Scholarship for Higher Education for the academic session 1996-97 during M.Sc.

Technical Skills

Computer Programming:

- C, Python, Jython, Perl, Unix shell scripting, MySQL, HTML, Matlab

Information/Internet Technology:

- Networking (Routing, UDP, TCP, ARP, FTP, HTTP, DNS, SMTP)
- Firewalls (Cisco PIX, MS ISA, LinkProof, eTrus)
- IDS (RealSecure, Snort, MS ISA, IntruPro)

Tools & Packages

- Code analyzers: OllyDbg, IDA Pro, BinNavi, Paimei, Fortify Code Analyzer.
- Network/vulnerability Analyzer: Ethereal, TCPDump, Metasploit, Nessus etc.

Operating Systems:

- Microsoft Windows family, Linux, and other UNIX variants

References Available to Contact

Dr. Laurent MOUNIER (e-mail: Laurent.Mounier@imag.fr; phone: +(33) 4 56 52 03 54)

- Professor, University of Grenoble, France, Verimag, Grenoble, France

◇ Verimag - Centre Equation 2, avenue de Vignate 38610 Gières - France

⋆ *Prof. Mounier is my postdoc advisor.*

Dr. Marie-Laure POTET (e-mail: Marie-Laure.Potet@imag.fr; phone: +(33) 4 56 52 04 28)

- Professor, Ensimag, Grenoble, France, Grenoble Institute of Technology, Grenoble, France,
  Verimag, Grenoble, France

◇ Verimag - Centre Equation 2, avenue de Vignate 38610 Gières - France

⋆ *Prof. Potet is my postdoc co-advisor.*

Dr. Arun K. Pujari (e-mail: akpcs@uohyd.ernet.in; arun.k.pujari@gmail.com; Ph (Off): +91-40-23134114)

- Professor, Dept. of Computer and Information Sciences
  University of Hyderabad

◇ AI Lab, University of Hyderabad, Central University P.O, Hyderabad - 500 046.INDIA.

⋆ *Prof. Pujari was my PhD advisor.*

Dr. Rao Vemuri (e-mail: rvemuri@ucdavis.edu; rvemuri@gmail.com; phone: +1-530 754-7209)

- Professor, Dept. of Computer Science, University of California, Davis, US

◇ 236 Walker Hall, Davis CA 95616

⋆ *Prof. Vemuri was in my thesis research committee and I worked with him on a large part of my thesis.*

Dr.V. P. Gulati (e-mail: vp.gulati@tcs.com; phone: +91 40 66673003)

- Vice President, Business Domain Academy, TCS Tata Consultancy Services, Hyderabad, India

◇ Plot No 1, Survey No. 64/2, Software Units Layout Serilingampally Mandal, Madhapur Hyderabad - 500034,Andhra Pradesh India

⋆ *Dr. Gulati was my PhD co-advisor. He was Professor and ex-diretor, IDRBT.*