

PRITHVI BISHT

2 East 8th St, Apt 2112, Chicago, Illinois 60605
 ☎ 312-810-1812 ✉ pbisht@cs.uic.edu
 WWW: www.cs.uic.edu/~pbisht

EDUCATION

Doctor of Philosophy, CS	University of Illinois at Chicago Aug 2006 - Jun 2011	GPA: 4.0/4.0 Advisor: Prof. V.N. Venkatakrisnan
Master of Technology, CS	Indian Institute of Technology, Kanpur 2000 - 2002	CPA: 7.71/10.0 Advisor: Prof. Rajat Moona
Bachelor of Engineering, CS	G.B. Pant Engineering College 1996 - 2000	Percentage: 80% (honors)

DOCTORAL DISSERTATION

LEARNING INTENDED BEHAVIOR TO DETECT AND PREVENT ATTACKS ON WEB APPLICATIONS: The key observation of this work is that the source code of a web application contains a wealth of information about its intended behavior. Typically, attacks manifest by tricking applications to yield an unintended behavior. This thesis has devised novel techniques that generate models of *intended behavior* through program analysis and then use them to prevent / eliminate attacks (*enforce conformance to the model*) or to find concrete attacks (*invalidate the model*).

RESEARCH INTERESTS

I am interested in most aspects of Computer Security, specifically in Language-based security solutions i.e., prevent / eliminate / detect vulnerabilities through program analysis and retrofitting. My ongoing work is exploring techniques to learn specifications of safe program behavior by applying a mix of static and dynamic analysis techniques on the source code and the output of web applications. These specifications will then be employed to find vulnerabilities or to safeguard the application by either selectively re-writing its output or its source code.

PUBLICATIONS

REFEREED JOURNAL ARTICLES

1. **CANDID: Dynamic Candidate Evaluations for Automatic Prevention of SQL Injection Attacks.** Prithvi Bisht, P. Madhusudan and V.N. Venkatakrisnan. *ACM Trans. Inf. Syst. Secur.*, Volume 13, Number 2, 2010, New York, NY, USA.

REFEREED CONFERENCE PAPERS

2. **WAPTEC: Whitebox Analysis of Web Applications for Parameter Tampering Exploit Construction.** Prithvi Bisht, Timothy Hinrichs, Nazari Skrupsky, and V.N. Venkatakrisnan. In *CCS'11: Proceedings of the 18th ACM Conference on Computer and Communications Security*, Chicago, Illinois, USA, 2011, **Acceptance Rate = 60 / 429, 14%**.
3. **NoTamper: Automatic Blackbox Detection of Parameter Tampering Opportunities in Web Applications.** Prithvi Bisht, Timothy Hinrichs, Nazari Skrupsky, Radoslaw Bobrowicz and V.N. Venkatakrisnan. In *CCS'10: Proceedings of the 17th ACM Conference on Computer and Communications Security*, Chicago, Illinois, USA, 2010, **Acceptance Rate = 55 / 320, 17%**.
4. **TAPS: Automatically Preparing Safe SQL Queries (Poster Paper).** Prithvi Bisht, A. Prasad Sistla and V.N. Venkatakrisnan. In *CCS'10: Proceedings of the 17th ACM Conference on Computer and Communications Security*, Chicago, Illinois, USA, 2010, **Acceptance Rate = 44 / 69, 64%**.
5. **Automatically Preparing Safe SQL Queries.** Prithvi Bisht, A. Prasad Sistla and V.N. Venkatakrisnan. In *FC'10: Proceedings of the 14th International Conference on Financial Cryptography and Data Security*, Tenerife, Canary Islands, Spain, 2010, **Acceptance Rate = 19 / 130, 14.6%**.
6. **Strengthening XSRF Defenses for Legacy Web Applications Using White-box Analysis and Transformation.** Michelle Zhou, Prithvi Bisht and V.N. Venkatakrisnan. In *ICISS'10: Proceedings of*

the 6th International Conference on Information Systems Security, Gandhinagar, Gujarat, India, 2010, **Acceptance Rate = 14 / 51, 27%**.

7. **XSS-GUARD: Precise Dynamic Prevention of Cross-site Scripting Attacks.** Prithvi Bisht and V.N. Venkatakrisnan. In *DIMVA'08: Proceedings of the 5th Conference on Detection of Intrusions & Malware, and Vulnerability Assessment*, Paris, France, 2008, **Acceptance Rate = 13 / 42, 31%**.
8. **CANDID: Preventing SQL Injection Attacks using Dynamic Candidate Evaluations.** Sruthi Bandhakavi, Prithvi Bisht, P. Madhusudan and V.N. Venkatakrisnan. In *CCS'07: Proceedings of the 14th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, 2007, **Acceptance Rate = 55 / 302, 18%**.

REFEREED WORKSHOP PAPERS

9. **Analysis of Hypertext Isolation Techniques for Cross-site Scripting Prevention.** Mike Ter Louw, Prithvi Bisht and V.N. Venkatakrisnan. In *2nd Workshop in Web 2.0 Security and Privacy*, Oakland, CA, USA, **Acceptance Rate = 14 / 45, 31%**.

INVITED PAPERS

10. **WebAppArmor: A Framework for Preventing Web-based Attacks.** V.N. Venkatakrisnan, Prithvi Bisht, Mike Ter Louw, Michelle Zhou, Kalpana Gondi and K. T. Ganesh. In *ICISS'10: Proceedings of the 6th International Conference on Information Systems Security*, Gandhinagar, Gujarat, India, 2010.

BOOK CHAPTERS

11. **Formal Methods in Web Application Security.** Prithvi Bisht and V.N. Venkatakrisnan. In *Encyclopedia of Cryptography and Security*, 2nd Ed., Springer, 2011. (Editors: Henk C.A. van Tilborg and Sushil Jajodia).

RESEARCH HIGHLIGHTS

NO-TAMPER [1] proposed a penetration-testing technique to find parameter tampering opportunities in web applications. It employed symbolic evaluation to learn constraints checked by the client-side code (application's intentions). Ideally, the server-side code should re-validate these constraints as the client-side environment is untrusted. NO-TAMPER then generated hostile inputs that systematically invalidated constraints (intentions) being checked at the client-side. It successfully revealed serious problems in several open source and commercial applications (online banking / shopping) that could amount to financial losses. *This work showcased that there is a significant gap in the validation that should happen and that does happen in web applications and that by invalidating models of the intended behavior it is possible to find security vulnerabilities in web applications.*

I have also explored *monitor based run time prevention* as well as *static analysis based security-by-construction* techniques. The former typically introduces a reference monitor to forbid anomalous behavior at runtime. CANDID [6,7] mitigated SQL injection attacks with a runtime monitor that learned structures of intended SQL queries in a novel fashion. A runtime query that had different structure than the corresponding intended query, was disallowed thus preventing SQL injection attacks. XSS-GUARD [5] extended this idea and mitigated Cross-site scripting attacks by removing injected scripts at the server-side. Recently, TAPS [2,3] proposed a *static analysis based security-by-construction* technique to statically learn the intended query structures in programs and transform the source code to generate PREPARE statements instead of vulnerable SQL queries. TAPS employed static analysis to “eliminate” vulnerabilities whereas its traditional use has been limited to “detection” of vulnerabilities. *CANDID and XSS-GUARD highlighted effectiveness of attack mitigation through automated model extraction and runtime enforcement. TAPS refined the enforcement and provided evidence that effective mitigation can be achieved through security-by-construction without requiring runtime monitors.*

XPROTECT [4] offered a principled approach to strengthen preventive solutions for Cross-site Request Forgery (XSRF) attacks. It employed secret token based defense to transform the web application code. Typically, web applications protect sensitive operations by checking authenticated status of the web request. XPROTECT programmatically identified and augmented these checks to validate secret token thus protecting sensitive operations against XSRF attacks. Further, it employed a novel client-side secret attachment technique to prevent leaks of the secret token. *XPROTECT further corroborated the idea of enforcing models of intended behavior.*

PRESENTATIONS

- Web Application Security: Trends and Mitigation through Source Code Analysis.
 - ◆ Dasient, Sunnyvale, USA, Mar 2011
 - ◆ AT&T Security Research Center, New York, USA, Feb 2011
 - ◆ SRI International, Computer Science Lab Seminar, Menlo Park, USA, Dec 2010
- NOTAMPER: Automatic Blackbox Detection of Parameter Tampering Opportunities in Web Applications
 - ◆ Poster presentation, Computer Security Awareness Week (CSAW), NY, USA, Oct 2010
 - ◆ Paper presentation, CCS Conference, Chicago, USA, Oct 2010
 - ◆ Rump session presentation, Usenix Security Symposium, Washington, USA, Aug 2010
- TAPS: Automatically Preparing Safe SQL Queries
 - ◆ Paper presentation, FC Conference, Tenerife, Spain, Jan 2010
 - ◆ Poster presentation, CCS Conference, Chicago, USA, Oct 2010
- XSS-GUARD: Precise Dynamic Prevention of Cross-site Scripting Attacks. Paper presentation, DIMVA Conference, Paris, France, Jul 2008
- CANDID: Preventing SQL Code Injection Attacks
 - ◆ Work-in-progress presentation, Usenix Security Symposium, Boston, Aug 2007
 - ◆ Poster presentation, Midwest Security Workshop, Chicago, Oct 2007

ADDITIONAL RESEARCH PROJECTS

- Automated Discovery of Zero-day Attacks through Binary Program Analysis (with Phillip Porras and Vinod Yegneswaran - SRI International Lab, V.N. Venkatakrishnan - UIC)
- Reduction of Data Lifetime (with Kalpana Gondi, Praveen Venkatachari, A. Prasad Sistla and V.N. Venkatakrishnan - UIC)

PROFESSIONAL EXPERIENCE

- Postdoctoral Researcher** Jul, 2011 – Present
University of Illinois at Chicago, Department of Computer Science, Chicago, IL, USA
- Study of security issues in Web applications.
- Doctoral Intern** May, 2010 – Aug, 2010
SRI International, Computer Science Lab, Menlo Park, CA, USA
- Analyzed malicious Flash applications and prepared a categorized knowledge base.
 - Studied existing literature on security analysis of binary applications.
 - Proposed a novel scheme to find and prevent Zero-day attacks in binary applications.
- Research Assistant** Jan, 2007 – Jul, 2011
University of Illinois at Chicago, Department of Computer Science, Chicago, IL, USA
- Studied security issues in Web applications.
 - Proposed solutions for mitigation of top security threats including SQL-injection, Cross-site scripting and Cross-site request forgery.
 - Proposed novel ways of finding high impact vulnerabilities in commercial web applications (online banking / shopping).
 - Published research papers in top tier security conferences and participated in preparation of grant proposals to NSF.
 - Peer reviewed academic conference papers and journal articles.
 - Prototyped and evaluated several research ideas.
- Teaching Assistant** Aug, 2006 – Dec, 2006
University of Illinois at Chicago, Department of Computer Science, Chicago, IL, USA
- Mentored tutorial sessions for undergraduate class “Introduction to Programming”.
 - Designed problems for weekly assignments and graded submissions.
 - Graded assignments for graduate class “Introduction to Algorithms”.

Senior Software Developer

Jul, 2003 – Jul, 2006

Intel Corporation, Bangalore, India

- Designed and developed software for concept platforms of Intel.
- Proposed novel ideas that showcased hardware strength.
- Prototyped and prepared demos for higher management to get seed money for projects.
- Interfaced with Bluetooth stack vendors (Toshiba Japan, IVT China) as the sole technical contact.
- Published patentable ideas at <http://www.ip.com>.

Senior Software Developer

Mar, 2002 – Jul, 2003

Novell Inc., Bangalore, India

- Developed software to provide location independent secure access to the corporate information.

Research Student

Jul, 2000 – Feb, 2002

Indian Institute of Technology Kanpur, Department of Computer Science, Kanpur, India

- Developed an architecture-independent disassembler.
- Studied hands-on security (buffer overflows, trojan horses, packet sniffers).

PROFESSIONAL ACTIVITIES

- Peer-reviewed research articles for:
 - ♦ IEEE Security & Privacy (Oakland): 2010, 2011
 - ♦ Network & Distributed Systems Security (NDSS): 2011
 - ♦ ACM Computer & Communications Security (CCS): 2009
 - ♦ Recent Advances in Intrusion Detection (RAID): 2008, 2010
 - ♦ Annual Computer Security Applications Conference (ACSAC): 2008, 2009, 2010, 2011
 - ♦ Computer Security Foundations Symposium (CSFW): 2009
 - ♦ Journal of Computer Security (JCS): 2009
 - ♦ Journal of Software Practice and Experience (JSPE): 2008
 - ♦ IET Information Security Journal: 2011
 - ♦ Web 2.0 Security and Privacy (W2SP): 2011

TECHNICAL REPORTS AND PATENTS

PATENTS

1. **Automatically Generating Safe SQL Queries** [Submitted to US Patent Office].

TECHNICAL REPORTS

2. **Designing secure SDKs.** [Published at www.ip.com].
3. **A Bluetooth based WiFi Access Point Management** [Published at www.ip.com].

HONORS AND DISTINCTIONS

- NOTAMPER project is among the 10 finalists in NYU-Polytechnic Computer Security Awareness Week competition 2010 (open to all students in the Continental USA).
- Research work featured in news
 - ♦ Oct 2010: <http://www.prnewswire.com/news-releases/105433278.html>
 - ♦ Oct 2010: <http://www.cs.uic.edu/Main/NewsItem?audience=public&ind=395>
 - ♦ Oct 2009: <http://www.uic.edu/htbin/cgiwrap/bin/uicnews/articledetail.cgi?id=13593>
- Student travel grants
 - ♦ 19th Usenix Security Symposium, Washington, 2010.
 - ♦ 18th Usenix Security Symposium, Montreal, 2009.
 - ♦ 16th Usenix Security Symposium, Boston, 2007.
- All India Rank 52, Graduate Aptitude Test of Engineering, India, 2000 (99.06 percentile).

SECURITY RELEVANT COURSEWORK AT UIC

Advanced Web and Electronic Voting Security Codes & Cryptography	Formal Methods in Concurrent and Distributed Systems Computer Systems Security	Secure Computer Systems Network and Distributed Systems Security
--	--	--

SKILLS

Research: Problem identification, theoretical analysis, solution development and concept prototyping. Author academic literature and research proposals. Collaboration. Knowledge extraction and critical review of academic literature.

Software Engineering: Conception, design, implementation, optimization, debugging, documentation, support and growth of small to large, long-term software development projects

Computer Languages: C, C++, HTML, L^AT_EX, Java, JavaScript, Perl, Shell script, PHP, SQL

Operating Systems: DOS, Linux (Gentoo/Ubuntu), UNIX, Windows (98/ME/2000/XP)