Pankaj Kohli

pankaj208@gmail.com • +65 96744595 (*AU permanent resident*)

Professional Experience

- **V-Key** [Sept 2013 – present]
  Senior Security Researcher *Singapore*
  - Performed reverse engineering and penetration testing of Android and iOS apps
  - Researched anti-debugging, anti-runtime injection and code obfuscation techniques to protect Android and iOS apps from malware and runtime attacks
  - Developed and enhanced proprietary virtual processor, virtual OS, and toolchain
  - Performed vulnerability research on iOS platform
- **Citibank** [Sept 2012 – Aug 2013]
  Application Security Analyst *Singapore*
  - Performed web and mobile application penetration testing
  - Performed source code reviews
  - Performed application architecture reviews and threat modeling
  - Researched new threats and kept knowledge base updated
  - Liaised with development teams for timely resolution of outstanding security issues
- **D'Crypt** [Apr 2010 – Sept 2012]
  R&D Engineer (IT Security) *Singapore*
  - Developed static and dynamic analysis tools for vulnerability research
  - Performed Adobe Reader crash analysis
  - Led a small team of developers and oversaw the development process

Non-Professional Experience

- **Independent Security Researcher** [June 2009 – Mar 2010]
  Blog: http://www.pank4j.com *New Delhi, India*
  - Reported vulnerabilities and developed exploits for Windows and Linux applications
    - *CVE-2009-3711*: httpdx http.cpp h_handlepeer() function overflow **(exploit included in Metasploit Framework)**
    - *CVE-2009-3050*: HTMLDOC "html" File handling remote stack buffer overflow vulnerability
    - *CVE-2009-2484*: VLC media player "smb://" URI handling remote buffer overflow vulnerability
    - *CVE-2009-3663*: httpdx httpdx_src/http.c h_readrequest() function format string vulnerability
- **System Administrator** [June 2008 – May 2009]
  Center for Security, Theory & Algorithmic Research labs, IIIT *Hyderabad, India*
  - Voluntarily worked as a system administrator for the research labs.

Certifications

- Certified Information Systems Security Professional (**CISSP**)
  License 428854 (July 2014 – June 2017)

Skills / Knowledge

- Experience with automated and manual penetration testing of web and mobile applications
- Experience with reversing engineering of malware using disassemblers like IDA Pro, familiar with exploit writing
- Knowledge of OWASP Top 10, CWE Top 25 vulnerabilities
- Development: C, Assembly (x86 / ARM), shell scripting

Education

- **International Institute of Information Technology (IIIT)** Hyderabad, India
  Master of Science in Computer Science & Engineering *2009*
  - Thesis: Automatic detection of memory corruption attacks
- **Punjab Technical University** Jalandhar, India
  Bachelor of Technology in Computer Science & Engineering *2006*

Publications

- J. Gan, R. Kok, P. Kohli, Y. Ding, B. Mah, *"Using Virtual Machine Protections to Enhance Whitebox Cryptography,"* in Proceedings of 1st International Workshop on Software Protection (SPRO), Florence, Italy, May 2015.
- P. Kohli, *"Exploiting File Uploads for Fun and Profit,"* in Hakin9 magazine, Apr 2013.
- P. Kohli, *"Coarse-grained Dynamic Taint Analysis for Defeating Control and Non-control Data Attacks,"* published online at Computing Research Repository, 2009.
- P. Kohli, B. Bruhadeshwar, *"FormatShield: A Binary Rewriting Defense against Format String Attacks,"* in Proceedings of 13th Australasian Conference on Information Security and Privacy (ACISP), Wollongong, Australia, Jul 2008.
- V. S. Sathyanarayan, P. Kohli, B. Bruhadeshwar, *"Signature Generation and Detection of Malware Families,"* in Proceedings of 13th Australasian Conference on Information Security and Privacy (ACISP), Wollongong, Australia, Jul 2008.

Activities

- Program Committee Member, International Conference on Dependability (DEPEND), 2011.
- External Reviewer, International Conference on Distributed Computing and Networking (ICDCN), 2009.

Personal Profile

- Interests: Blogging
- Languages: English, Hindi
- Nationality: Indian