

# Vivek Ramachandran

## Accolades:

---

- Received **international recognition as a Security Researcher** in 2007 for the discovery of the Caffe Latte Attack – was featured on CBS5, BBC, Computer World, Mac World, IT World, Network World, The Register etc
- Made it to the **India Top 10 list of the Microsoft Security Shootout 2006**, a web application security competition (over 50,000 participants)
- Received a **Team Achievement Award in Cisco Systems** for my contribution to a worldwide release

## In the Media:

---

- Featured in the **CBS5 6PM News, USA** – demonstrated wireless vulnerabilities in a coffee shop
- Was quoted / name mentioned on **BBC online, Computer World, Info World, Computer World, Mac World, The Register** etc in relation to the discovery of a wireless vulnerability called the Caffe Latte Attack.

## Talks and Presentations in Conferences:

---

- **The Caffe Latte Attack**, Toorcon 9, San Diego, USA
- **WEP Cloaking Exposed**, Defcon 15, Las Vegas, USA
- **E-Commerce Web Application Security**, 8<sup>th</sup> International Conference on Information Security, India
- **Network Security: Mitigating Hackers**, Cisco Systems, India
- **Network Security Basics Workshop**, IIT Guwahati, India

## Research Publications:

---

- **Detecting ARP Spoofing: An Active Technique**, Vivek Ramachandran, Sukumar Nandi, LNCS Publication, Proceedings of the 1<sup>st</sup> International Conference on Information Security Systems
- **Bleeding Edge Distributed Denial of Service (DDoS) Attack Mitigation Techniques for ISPs**, Vivek Ramachandran, Sukumar Nandi, Proceedings of 8<sup>th</sup> International Conference on Information Technology
- **Mapping the Internet: Record Route Revisited**, Vivek Ramachandran, Sukumar Nandi, submission under progress

## Patents:

---

- **Detecting ARP Spoofing using an Active Injection Technique**, Vivek Ramachandran, Sukumar Nandi, Filing in progress

## Expertise:

---

### Domains:

- **Wired Networking and Security** : L2, TCP/IP, Routing, Firewalls, IDS, IPS etc
- **Wireless Networking and Security** : 802.11, 802.1x, Radius, WEP, WPA/WPA2
- **Web Application Security** : web server / application / database security
- **Embedded Systems / System programming** : Unix and Linux based systems

### Programming:

- **Languages:** C, C++, C#, Assembly, Perl, ASP.NET, ActionScript, Bash Scripting, Javascript, Adobe Flex
- **Platforms:** Linux, Unix, Windows, .NET

### Education:

---

- Bachelor of Technology (**B.Tech**) in Electronics and Communication from the **Indian Institute of Technology, Guwahati (IIT-G)**
- Class X / XII from St. Lawrence High School, Kolkata India

*Bachelor Degree Project: Vulnerabilities in the TCP/IP Protocol Suite and Design of an Anomaly based Intrusion Detection (awarded 10/10)*

### Work Experience:

---

#### 1. Member of Research and Development Group, AirTight Networks, Pune, India ( Mar 2007 – Present ):

- Discovered the “**Caffe Latte Attack**”, a wireless vulnerability existing on laptops still using WEP and demonstrated the same at Toorcon 9
- Researched on the “**WEP Cloaking**” technology and publicly demonstrated its security holes at Defcon 15
- Designed and developed a **Wireless Lan Monitoring tool** on top of Backtrack 2.0
- Developed a **Data Visualization tool** for wireless packet traces
- Developed a **Wireless Protocol Fuzzer** for finding device driver vulnerabilities
- Provided **inputs to the Marketing Team** in the form of internal Whitepapers, Product demo videos etc
- Trained the **Web Analytics** and **Web Marketing** teams in India and laid out a formal process for their work

#### 2. Security Evangelist, Self Employed, Gurgaon, India (Sept 2006 – Feb 2007):

- Offered to write penetration testing tools, security tools and utilities
- **Founded www.Security-Freak.net**, a free video training website to help security professionals. The website has served around 65,000+ visitors, had over 1 million page views and used 200GB of bandwidth till date.

- **Founded *www.MbaFreak.com***, a free website to help MBA test takers collaborate and learn
- Both the above websites were ***monetized with Google AdSense***

**3. Senior Developer, Guavus Networks, Gurgaon, India (Jan 2006 – Aug 2006):**

- Design of a ***data collection framework*** for the backbone for ISPs
- Implementation of the above for various versions of ***Netflow***
- Design and setup of the network infrastructure to support testing of the above

**4. Developer, Internet Switching Business Unit, Cisco Systems, Bangalore, India (Nov 2004 – Jan 2006):**

- Worked in the Layer 2 security team on ***802.1x and Port Security features*** for the Catalyst 6500 series of switches
- Developed ***Private VLAN (PVLAN)*** feature to be used with 802.1x in Cisco IOS
- Developed ***Radius Accounting*** feature to be used with 802.1x in IOS
- Developed ***Session Timeout*** feature to be used with 802.1x in IOS
- Developed ***Posture Token Display*** feature to be used with Network Admission Control (NAC) on Cisco IOS
- Added ***High Availability (HA)*** support for clearing dynamically learnt addresses for Port Security on the standby supervisor
- Minor enhancements and bug fixes in the 802.1x and Port Security modules

**5. Developer, Emerging Technologies and Services Group, Reliance Infocomm, Mumbai, India (June 2004 – Oct 2004):**

- Design and implementation of a ***network backed for the HTK toolkit***
- Design and implementation of a ***tool for Grapheme to Phoneme mapping*** for 10 different Indian languages and a ***web based VXML editor***

**6. Student Researcher, Institute of Internet Technologies and Applications, University of Applied Sciences, Switzerland (May 2003 – July 2003):**

- Study existing ***attacks on WLANs*** and build tools to practically verify the same
- Study ***effects of roaming on Authentication mechanisms*** in WLANs using Cisco LEAP and Radius Servers