ASHOKKUMAR C

Current location: Yokohama, Japan
Homepage: http://cse.iitb.ac.in/~ashokkumar
LinkedIn: http://in.linkedin.com/in/ashokcse
Google Scholar: https://scholar.google.com/citations?user=d5M9SyoAAAAJ&hl=en

Nationality: Indian
Phone: +81 80-9513-7407
Email ID: ashokkumariitb@gmail.com

INDUSTRIAL EXPERIENCE

Assistant Researcher
Research & Development Group, Hitachi, Ltd. (Japan) Oct 2019 - Current
Working on projects dealing with automation of effective Vulnerability Management, using technologies and standards such as TAXII, STIX, NVD CVE, and CPE databases, JVN db, ISO7000 series.

ACADEMIC EXPERIENCE (TEACHING ASSISTANT)

CS101: Computer Programming and Utilization (Head TA) Jul - Dec 2016
Department of Computer Science and Engineering, IIT Bombay

CS213.2x: Implementation of Data Structures Sept - Nov, 2016
edx.org *and* ***IITBombayX.in***

CS213.3x: Algorithms Jul - Sep, 2016
edx.org *and* ***IITBombayX.in***

CS101: Computer Programming and Utilization (Coordinating TA) Jul - Dec 2013
Department of Computer Science and Engineering, IIT Bombay *Jan - May 2015*

CS 341: Computer Architecture Lab Jul - Dec 2014
Department of Computer Science and Engineering, IIT Bombay

PUBLICATIONS

- **Ashokkumar C** and Bholanath Roy and M. Bhargav Sri Venkatesh and Bernard Menezes, "*S-Box Implementation of AES is NOT side channel resistant*", Journal of Hardware and Systems Security (2019), Springer, pp 1-12, 05 December 2019
- **Ashokkumar C**, Bhargav Sri Venkatesh, Ravi Prakash Giri, Bholanath Roy, Bernard Menezes, "*An error-tolerant approach for efficient AES key retrieval in the presence of cache prefetching - Experiments, Results, Analysis*", SADHANA - Journal of the Indian Academy of Sciences, Springer, Volume 44, Issue 4, April 2019
- Jiji Angel, Rahul R., **Ashokkumar C** and Bernard Menezes, "*DSA Signing Key Recovery with noisy Side Channels and Variable Error Rates*", 18th International Conference on Cryptology in India (**IndoCrypt'17**), Chennai 2017.
- **Ashokkumar C** and M. Bhargav Sri Venkatesh and Ravi Prakash Giri and Bernard Menezes, "*Design, Implementation and Performance Analysis of Highly Efficient Algorithms for AES Key Retrieval in Access-driven Cache-based Side Channel Attacks*", Cryptology ePrint Archive: Report 2017/896
- **Ashokkumar C**, Ravi Prakash Giri, Bernard Menezes, "*Highly Efficient Algorithms for AES Key Retrieval in Cache Access Attacks*", IEEE European Symposium on Security and Privacy (**IEEE Euro S&P 2016**), Saarbrucken, Germany, March 21-24 2016
- Bholanath Roy, Ravi Prakash Giri, **Ashokkumar C**, Bernard Menezes: "*Design and Implementation of an Espionage Network for Cache-based Side Channel Attacks on AES*", International Conference on Security and Cryptography (**SECRYPT 2015**) Colmar, France, July 20-22, pp. 441-447

EDUCATION

Ph.D. in Compute Science and Engineering (Thesis under review) Jan 2013 - Present
Indian Institute of Technology Bombay *Mumbai, India*
Topic : Highly efficient algorithms for AES key retrieval in cache access attacks (Side channel Attacks on Cryptographic algorithms)

M.Tech. in Compute Science and Engineering Jul 2010 - Jun 2012
Defence Institute of Advanced Technology *Pune, India*
Overall GPA: 70.40%

B.E. in Compute Science and Engineering Jul 2005 - Jun 2009
Anna University Chennai *Salem, India*
Overall GPA: 73.04%

PH.D. RESEARCH

Side Channel Attacks on Advanced Encryption Standard (AES)
Under the supervision of Prof. Bernard Menezes and Prof. G. Sivakumar, IIT Bombay

Abstract: The software implementation of AES is an especially attractive target for cache-based side channel attacks on AES since it makes extensive use of cache-resident table look-ups. Modern processors employ hardware prefetching to reduce memory latency (cache lines are fetched in anticipation of their future use). This greatly complicates access-driven attacks since they are unable to distinguish between a line fetched on demand versus one prefetched and not subsequently used during a run of a victim running AES. Our multi-threaded spy code and key retrieval algorithms are designed to succeed even in the presence of prefetching albeit at the cost of requiring more blocks of ciphertext. We demonstrate through implementations on real machines corroborated by analytical models that, with probability 95%, we are able to recover the AES key using 25 blocks of ciphertext in the presence of prefetching and, stunningly, a mere 3-5 blocks with prefetching disabled. Moreover, our implementation is error-tolerant and also succeeds on the i3/i5/i7 processors which are equipped with highly aggressive prefetchers.

Wikipedia excerpt on our work: "In March 2016, Ashokkumar C., Ravi Prakash Giri and Bernard Menezes presented a very efficient side-channel attack on AES that can recover the complete 128-bit AES key . . . ",
`https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Side-channel_attacks`

OTHER RESEARCH PROJECTS

M.Tech Thesis:
Implementation of mini-cloud (IaaS) using OpenStack and Enhanced Mutual Authentication Scheme for cloud computing Jul 2011 - May 2012
under the guidance of Prof. Jaidhar C.D, DIAT(DU), Pune

A mini cloud (IaaS) has been implemented using OpenStack. It provides Infrastructure as a Service along with Storage as a Service (S3 like service). As a part of the thesis, the enhanced mutual authentication scheme was proposed. The scheme uses two way handshake between cloud server and user. It also withstands various known attacks.

A performance comparison of Local Storage VM vs Shared Storage VM Jan - May 2013
under the guidance of Prof. Umesh Bellur, IIT Bombay

The objective of this R&D project was to compare the IO performance of physical system, local storage VM and shared storage VM in detail. It was concluded that the local storage VM performs better than shared storage VM in most cases; though in random RW IO they perform at par.

FireBird VI based Fertilizer Feeding Robot Oct -Nov 2013
CS684: Embedded Systems Course Project, IIT Bombay

We designed and built an autonomous system on top of FireBird VI robot to find the plants in a greenhouse environment and feed a precise amount of solid fertilizer. We used off the shelf image processing algorithm to locate the plant stem and verify post-fertilization.

TALKS

System Security Tools: OSSEC and Metasploit 25^{th} May 2017
Tools for CyberSec 2017, Quality Improvement Programme (QIP)" IIT Bombay

Hosted Based Intrusion Detection using OSSEC and OSSIM 15^{th} Jul 2014
ISTE Main Workshop on Cyber Security, IIT Bombay *Yokohama, Japan*

Hosted Based Intrusion Detection using OSSEC and OSSIM 20^{th} May 2014
ISTE Coordinators Workshop on Cyber Security, IIT Bombay

Cloud Computing model - Infrastructure as a Service (IaaS) using OpenStack
Workshop on "Challenges in Cloud Computing", DIAT(DU), Pune *16^{th} Dec 2011*

ORGANIZING LAB SESSIONS

Tools for CyberSec 2017, QIP Workshop, IIT Bombay May 22-26, 2017
Information Security Research and Development Center ***(ISRDC, IIT Bombay)***
Key responsibility: to coordinat and conduct lab sessions on system security
(used OSSEC and Metasploit).

ISTE Main Workshop on Cyber Security July 10-20, 2014
Sponsored by the National Mission on Education through ICT (MHRD, Government of India)
Key responsibility: to create lab assignments on **Host Based Intrusion detection and prevention using OSSEC and OSSIM**

ISTE Coordinators Workshop on Cyber Security May 17-21, 2014
Sponsored by the National Mission on Education through ICT (MHRD, Government of India)
Key responsibility: to create lab assignments on **Host Based Intrusion detection and prevention using OSSEC and OSSIM**

POSITIONS OF RESPONSIBILITY

Manager (Web Team), ReSCon 2015 Mar 20 -21 , 2015
Led four-member group responsible for developing the website and coordination with organizers

AURAA (Ph.D.), IIT Bombay 2014 - 2015
Academic Unit Representative for Academic Affairs(AURAA)
Represented Department of Computer Science & Engineering in Institute Academic Council 2014-15

Member of Election Commission, Hostel 1, IIT Bombay 2016 - 2017
Responsible for online voting system and smooth conducting of election to elect members of "Hostel 1 Students council"

Computer Councilor, Students Council Hostel 1, IIT Bombay 2015 - 2016
Led three-member group responsible for Hostel 1 website, Computer room and networks."

Computer Secretary, Students Council Hostel 1, IIT Bombay 2015 - 2016
Responsible for Hostel 1 website, Computer room and networks."

LANGUAGE PROFICIENCY

English (Fluent), **Tamil** (Native), **Hindi** (Fluent)