Poonam and Prabhu Goel Faculty Chair Annual Report 2015-2016

Name of the Poonam and Prabhu Goel Chair Professor: Sandeep Kumar Shukla
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur
email: sandeeps@cse.iitk.ac.in
URL: http://www.cse.iitk.ac.in/users/sandeeps/

A. Contributions towards Academia and Research at IITK as a Faculty Chair

Teaching

(i) A new course "Cyber Security for Critical Infrastructure" was created and taught in the even semester of 2015. The course was at the post graduate level (CS631) -- however, the class had an even mix of post graduate and undergraduate students. Topics covered included -- SCADA (Supervisory Control and Data Acquisition) Security, SCADA infrastructure and cyber threat models to SCADA systems, power systems security, and use of machine learning techniques for anomaly detection in cyber physical system behavior to detect security breaches. Since a majority of students did not have sufficient machine learning background, almost 40% of the course was dedicated to machine learning. In the future offering, machine learning will be put in as a prerequisite. The enrollment in the course was 14 (7 undergraduates, and 7 post graduates).

(ii) Taught the course on "Computer Systems Security" which covered in details software vulnerability and exploits, real cyber attack exercises based on software vulnerabilities, systems security and threat models based on privilege escalation, and other system access control breaches, real attacks based on privilege escalation, web client security, web server security, cross site scripting based attacks, cross site request forgery based attacks, SQL and command injection attacks, internet protocol vulnerabilities, and exploits, and remediation etc. The course had 4 projects with sandboxed virtual machine provided, and students had a real hands on experience in finding vulnerabilities, creating exploits and attacking sandboxed servers, and finally a capture the flag tournament topped off the course. There were 101 students in the class with about 30% post graduate students, and 70% undergraduate students.

(iii) Chaired a departmental committee for reviewing the current departmental norms for Ph.D comprehensive examination, and based on extensive survey of current and past students, created new norms for PhD comprehensive examination in the department.

(iv) Organized a 4 day workshop at IIT Kanpur during February 8 to February 11, 2016 on "Side Channel Analysis and Cyber Security". The workshop had 4 days of tutorials on various aspects of side channel based cyber vulnerabilities, and remediation measures. The workshop was taught by Prof. Patrick Schaumont (Virginia Tech, USA), Prof. Ingrid Verbauwhede (University of Leuven, Belgium), Prof. Lejla Batina (Radboud University, The Netherlands), and Prof. Thomas Eisenbarth (Worcester Polytechnic University, USA). The workshop was attended by various government agencies, faculty and

students of various IITs, and other universities in India. More information about this workshop can be found at http://wosca.cse.iitk.ac.in/. The video of all the tutorials are also available at this site. Since side channel based attacks on cryptographic processes is a major concern in the US, Israel and Europe, it was very valuable to bring these experts in the field to India, and have Indian government scientists as well as faculty and students getting exposed to this field, and its importance in cyber security.

(v) I also invited two foreign experts to IIT Kanpur for periods of couple of days in one case, and a week in another. Prof. Johannes Kinder from Royal Holloway University in UK came and gave tutorial on symbolic analysis of software for vulnerability detection, and also interacted with graduate students in our group. Dr. Jean-Pierre Talpin from INRIA, France came for a week, interacted with the group on program synthesis from formal specifications. These invited researchers contributed not only in enhancing knowledge of the students, but also in inspiring the post graduate students.

(v) Admissions in Charge of PG Admissions: As admissions in charge of PG admissions, I have worked on improving the Ph.D, M.Tech and M.S admissions process by introducing programming test, multiple views on each student (written test, programming test, interview), and thereby increasing the number of Ph.D students admitted in the current year.

(vi) Currently supervising 1 post doctoral fellow, 3 PhD students, and 6 Masters thesis students. Also supervising a Project Engineer.

Research

(i) Worked on an interdisciplinary proposal to establish a cyber security center at IIT Kanpur. The proposed center will be headed by Prof. Sandeep K. Shukla, and Prof. Manindra Agrawal. Talks are ongoing with various governmental agencies including the NTRO (National Technology and Research Organization), DST (Department of Science and Technology), DEIT (Department of Electronics and Information Technology) for funding of the center. The center will involve 10 faculty members from Computer Science and 2 faculty members from Electrical Engineering, and the focus of the center will be on Cyber Security of Critical Infrastructure.

(ii) In the process of creating a SCADA lab in the CSE department of IIT Kanpur from the faculty initiation grant provided by the institute. A project engineer was hired for the SCADA Lab. The elaborate tendering process was carried out, and the order has been given. In about 2-3 months time (By August 2016) we should have a working prototype SCADA Lab with Schneider SCADA solutions, PLCs, SCADA network, and a prototype field instrumentation. Cyber Security vulnerabilities in SCADA systems, and various remediation techniques are main target of research in the SCADA Lab.

(iii) Received the Ramanujan Fellowship from the DST SERB (Science and Engineering Research Board). This is a fellowship given to faculty who just moved from a faculty position abroad to an Indian institute. The fellowship's salary component is not availed as it is only given to those who are not paid by the host institute. However, a 7 lacs INR per year for 5 years is being provided for research. This fund is being used to supplement the Initiation Grant from the institute towards building the SCADA lab.

(iv) US AFOSR (Air Force Office of Scientific Research) has agreed to fund our research on formal methods for detecting code-replacement attacks in SCADA systems, and remediation techniques by

behavioral signature derivation technique. The funding will come from their Asian office, and the funding will be for 1 year (amount: 51,000 US Dollars) starting from July 1st, 2016.

(iv) Working with Nivetti Systems which is a start up working on developing indigenous router and switches, on cyber security of their routers, and switches. Also working with their Claynet cyber range product which allows for a complete virtualized network construction, and using that to create honeypot and honeynet to obtain malware signatures, and use data analytics on such signatures. We are also working with Nivetti system in developing a fully indigenous version of an SSL implementation which will be then used in their networking products. The reason for developing an indigenous version is that the existing implementations (open source or not) might have vulnerabilities (such as Heartbleed), and/or trojans and backdoors. A joint proposal for funding under the government of India's UAY scheme has been submitted and expected to be funded soon. The funding amount is expected to be 1.3 crores, of which 25% will be funded by the company (Nivetti Systems).

(v) Working with a team of researchers in formal methods from IIT Kharagpur, and IIT Mumbai to develop a formal methods based methodology and framework for critical software industry sector in India such as nuclear industry, railways, and automotive industry. A proposal to the Government of India's IMPRINT scheme has been submitted on this topic. Our funding portion in this proposal is about 1.2 crores over 3 years.

(vi) Working with a team of researchers from IIT Kharagpur for an UK-India Renewable Energy Joint Research program, where we will work on the solar energy forecasting by using weather data, and analytics based on past weather data. This proposal seems to be in the process of being funded. Our funding is expected to be around 55 lacs over 4 years.

(vii) We also submitted another IMPRINT proposal on cyber security of critical infrastructure, and the funding requested is about 8 crores.

(viii) Other than these, working with IBM, TCS and few other companies to establish cooperative research relations between IIT Kanpur Cyber Security initiatives, and the cyber security researchers at these companies.

(ix) An Indo-French proposal has been submitted as well on the cyber security of automotive systems using formal methods, and the proposal is under consideration. Our funding part in this proposal is about 30 lacs over 3 years.

(x) An Indo-Japanese collaborative proposal on "Smart Society" to be demonstrated with multi-robot systems is being developed at the moment -- headed by Prof. Manindra Agrawal and his Japanese counterpart. Our contribution to this proposal on the cyber security issues in such systems.

(ix) Other than these funded research -- with the various research we are doing at this moment are:

a. VLSI Design of Crypto Hardware for various Cryptographic primitives (2 papers written so far) with post doctoral fellow Dr. Asan Basiri

b. Protocol reverse engineering for vulnerability detection in application level protocols (with PhD student Abhay Kumar)

c. Scheduling problems in automotive systems (with PhD student Prachi Joshi at Virginia Tech)

d. Android based apps development for intrusion detection in mobile phones (with UG student Devasish Yadav)

e. Malware analytics with Honey pots and Honey Nets (with 4 Masters thesis students)

f. Behavioral type for Safety during program synthesis from Synchronous Specifications (with Dr. Jean-Pierre Talpin, INRIA)

g. Cyber Attacks on Power System State estimation (with Prof. S. C Srivastava and his students in EE)

B. One paragraph on your accomplishment as a Faculty Chair

Academic Accomplishments during 2015-2016

- Two Journal papers (One IEEE Transactions on Smart Grid, another ACM Computing Surveys)
- Three Invited Conference Papers
- Five Peer Reviewed Conference/Workshop Papers
- One Invited Conference Tutorial
- Two Keynote talks at International Conferences
- Two Invited talks at Conferences (One International, One National)
- Three short courses at NTRO, and CDAC
- One Special Talk (KTalk series organized by Keonics in Bangalore)
- Three Invited Talks at three institutes

Other Accomplishments during 2015-2016

- Selected as a Ramanujan Fellow
- Continuing as the Editor-in-Chief of ACM Transactions on Embedded Computing
- Finished Term as a subject editor for ACM Computing Reviews
- Started as an Associate Editor for ACM Transactions on Cyber Physical Systems
- Served on Program committees of 6 International Conferences
- Serving as a Local arrangement chair of an International Conference in November 2016

C. Research Publications and Research Activities in Bulleted List form during 2015-16

Journal Papers (Peer Reviewed):

- John Narayan, **Sandeep K. Shukla**, and T. Charles Clancy. 2015. A Survey of Automatic Protocol Reverse Engineering Tools. *ACM Comput. Surv.* 48, 3, Article 40 (December 2015), 26 pages. DOI=http://dx.doi.org/10.1145/2840724

- S. C. Mueller; H. Georg; J. J. Nutaro; E. Widl; Y. Deng; P. Palensky; M. U. Awais; M. Chenine; M. Kuch; M. Stifter; H. Lin; **S. K. Shukla**; C. Wietfeld; C. Rehtanz; C. Dufour; X. Wang; V. Dinavahi; M. O. Faruque; W. Meng; S. Liu; A. Monti; M. Ni; A. Davoudi; A. Mehrizi-Sani, "Interfacing Power System and ICT Simulators: Challenges, State-of-the-Art, and Case Studies," in *IEEE Transactions on Smart Grid* , vol.PP, no.99, pp.1-1
doi: 10.1109/TSG.2016.2542824

Conference Papers (Peer Reviewed)

- J. P. Talpin, P. Jouvelot and **S. K. Shukla**, "Towards refinement types for time-dependent data-flow networks," *Formal Methods and Models for Codesign (MEMOCODE), 2015 ACM/IEEE International Conference on*, Austin, TX, 2015, pp. 36-41.
doi: 10.1109/MEMCOD.2015.7340465
- Dayal, Yi Deng, A. Tbaileh and **S. Shukla**, "VSCADA: A reconfigurable virtual SCADA test-bed for simulating power utility control center operations," *2015 IEEE Power & Energy Society General Meeting*, Denver, CO, 2015, pp. 1-5.
doi: 10.1109/PESGM.2015.7285822
- S. V. Chakraborty, **S. K. Shukla** and J. Thorp, "A framework for analyzing and optimizing renewable energy portfolios," *PowerTech, 2015 IEEE Eindhoven*, Eindhoven, 2015, pp. 1-6.
doi: 10.1109/PTC.2015.7232423
- Dayal, A. Tbaileh, Y. Deng and **S. Shukla**, "Distributed VSCADA: An integrated heterogeneous framework for power system utility security modeling and simulation," *Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2015 Workshop on*, Seattle, WA, 2015, pp. 1-6.
doi: 10.1109/MSCPES.2015.7115408
- Prachi Joshi, **Sandeep K. Shukla**, Jean Pierre Talpin Inria, and Huafeng Yu. 2015. Mapping functional behavior onto architectural model in a model driven embedded system design. In*Proceedings of the 30th Annual ACM Symposium on Applied Computing* (SAC '15). ACM, New York, NY, USA, 1624-1630. DOI=http://dx.doi.org/10.1145/2695664.2695934

Conference Papers (Invited Papers)

- Huafeng Yu, Prachi Joshi, Jean-Pierre Talpin, **Sandeep Shukla**, and Shinichi Shiraishi. 2015. The challenge of interoperability: model-based integration for automotive control software. In *Proceedings of the 52nd Annual Design Automation Conference* (DAC '15). ACM, New York, NY, USA, , Article 58 , 6 pages. DOI=http://dx.doi.org/10.1145/2744769.2747945
- Dayal, Avik, Deng, Yi and **Shukla, Sandeep K**, 2015, Design of Cyber Security for Critical Infrastructures: A Case for a Schizoid Design Approach. In *Proceedings of the Security, Privacy, and Applied Cryptography Engineering: 5th International Conference, SPACE 2015*, Jaipur, India, October 3-7, 2015. Pages: 41-54 DOI= http://dx.doi.org/10.1007/978-3-319-24126-5_3
- Asan Basiri and **Sandeep K. Shukla**, Hardware Optimizations for Crypto Implementations (Invited Paper) , to be published in the Proceedings of IEEE VDAT Conference, Guwahati, India, May 2016.

Tutorial at Conference

- **S. K. Shukla**, "Cyber Security of Cyber Physical Systems: Cyber Threats and Defense of Critical Infrastructures," *2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID)*, Kolkata, 2016, pp. 30-31. doi: 10.1109/VLSID.2016.153

Journal Editorials

- **Sandeep K. Shukla**. Editorial: Science of the Big and Small and Embedded Computing Systems. *ACM Trans. Embed. Comput. Syst.* 15, 2, Article 21e (April 2016), 2 pages. DOI=http://dx.doi.org/10.1145/2901293
- **Sandeep K. Shukla**. Editorial: Big Data, Internet of Things, Cybersecurity—A New Trinity of Embedded Systems Research. *ACM Trans. Embed. Comput. Syst.* 14, 4, Article 61 (October 2015), 2 pages. DOI=http://dx.doi.org/10.1145/2820608
- **Sandeep K. Shukla**. Editorial: Schizoid Design for Critical Embedded Systems. *ACM Trans. Embed. Comput. Syst.* 14, 3, Article 40e (May 2015), 3 pages. DOI=http://dx.doi.org/10.1145/2761728

D. List of Awards/Recognition/Honors if any:

- Key note speaker at *IEEE International Conference on Embedded Software and Systems (ICESS), New York, NY, USA, July 2015.*
- Keynote speaker at *the Security, Privacy, and Applied Cryptography Engineering: 5th International Conference, SPACE 2015*, Jaipur, India, October 2015.
- Invited speaker *at IEEE VDAT (VLSI Design and Test Conference)* at Guwahati, India in May 2016.
- Invited Tutorial Speaker at the *IEEE VLSI Design Conference*, Kolkata, India, January 2016.
- Ramanujan Fellowship, DST SERB, 2015.
- Editor-in-Chief, ACM Transactions on Embedded Computing Systems (ACM TECS)
- Associate Editor, ACM Transactions on Cyber Physical Systems (ACM TCPS)
- Book Series Editor, River Publishers Series in Information Science and Technology, River Publishers, Denmark.

E. Details of Invited Talks/Seminars/Workshops

- Key note speaker at *IEEE International Conference on Embedded Software and Systems (ICESS), New York, NY, USA, July 2015.*
- Keynote speaker at *the Security, Privacy, and Applied Cryptography Engineering: 5th International Conference, SPACE 2015*, Jaipur, India, October 2015.
- Invited speaker *at IEEE VDAT (VLSI Design and Test Conference)* at Guwahati, India in May 2016.
- Invited Tutorial Speaker at the *IEEE VLSI Design Conference*, Kolkata, India, January 2016.
- Invited talk at New York University -- Abu Dhabi Center, December, 2015.
- Invited talk at Keonics K-Talk Day in Bangalore, March 2016.
- Invited talk at the Integral University Cyber Security Day, Integral University, Lucknow, UP, April 2016.
- Invited talk at the Institute of National Bank for Agriculture and Rural Development, Lucknow, May 2016.
- 2 and half day course on Software and Systems Security at NTRO, New Delhi, December 2015.
- 2 day course on Software and Systems Security at C-DAC, Mumbai, December 2015.
- 2 day course on Software and Systems Security at C-DAC, Chennai, January 2016.
- Invited Tutorial at the IEEE VLSI Design Conference, Kolkata, January 2016.

F. Organized the Following Advanced Workshop during 2015-16

Organized a 4 day workshop at IIT Kanpur during February 8 to February 11, 2016 on "Side Channel Analysis and Cyber Security". The workshop had 4 days of tutorials on various aspects of side channel based cyber vulnerabilities, and remediation measures. The workshop was taught by Prof. Patrick Schaumont (Virginia Tech, USA), Prof. Ingrid Verbauwhede (University of Leuven, Belgium), Prof. Lejla Batina (Radboud University, The Netherlands), and Prof. Thomas Eisenbarth (Worcester Polytechnic University, USA). The workshop was attended by various government agencies, faculty and students of various IITs, and other universities in India. More information about this workshop can be found at http://wosca.cse.iitk.ac.in/. The video of all the tutorials are also available at this site. Since side channel based attacks on cryptographic processes is a major concern in the US, Israel and Europe, it was very valuable to bring these experts in the field to India, and have Indian government scientists as well as faculty and students getting exposed to this field, and its importance in cyber security.

G. Details on the Thesis Supervised/ Students Guided During 2015-16

PhD

Ankur Sharma -- 2nd year PhD student
TentativeThesis Topic -- *Formal Proofs of Security of Protocols and Software Systems*

Abhay Kumar -- 1st year PhD student
Tentative Thesis Topic -- *Protocol Reverse Engineering for Discovering Security Vulnerabilities*

Saurabh Kumar -- 1st year PhD student
Tentative Thesis Topic -- *Cyber Security of Multi-Robot Systems*

M.Tech Thesis

Harshavardhan Sharma (Co-advised with Subhajit Roy) -- Final year Btech-Mtech program
TentativeThesis Topic -- *Symbolic Simulation Based Program Analysis for Vulnerability Detection*

Saptarshi Gan -- Pre-final year Btech-Mtech program
TentativeThesis Topic -- *Cyber Security Models for Internet of Things (IoT)*

Vineet Purushwani -- Pre-final year Btech-Mtech program
TentativeThesis Topic -- *Malware Analytics and Trend Prediction*

Nisith Majithia -- 1st Year M.Tech Student
TentativeThesis Topic -- *Honey Pots for Trapping Attackers*

Rohit Sehgal -- 1st Year M.Tech Student
TentativeThesis Topic -- *Configuration of HoneyNets for Trapping Cyber Attacks*

Pranjul Ahuja -- 1st Year M.Tech Student
TentativeThesis Topic -- *Enhanced Virtual Network for Cyber Security Experimentation*

P. Krishnaprasad -- 1st Year M.Tech Student
TentativeThesis Topic -- *Honey Pots and Honey Nets for SCADA Systems*

H. Administrative Endeavors During 2015-16

1. Chaired the Departmental Ph.D Comprehensive Examination Reforms Committee and Successfully created new norms based on extensive surveys of past and present graduate students

2. Chairing the post graduate Admissions Committee for admissions to departmental PhD, M.S and M.Tech Programs

3. Starting to Chair an Institute level Committee to consider the current deficiencies of the institute student registration and grading system OARS, and recommendation of its improvement

4. Working as the CISO of the Institute interfacing with CERT India.

5. Worked on an ad hoc committee constituted under the instruction of the Honorable Lucknow High Court to investigate possible cyber security issues in an online examination system and completed a report for the Lucknow High Court

6. Working with the Home ministry in an expert committee to advise the implementation project of CCTNS (Crime and Criminal Tracking Network and Systems) by the Niti Aayog.

I. Your Future Vision as a Faculty Chair

Currently my goal is to build up the center of excellence in Cyber Security of Critical Infrastructure at IIT Kanpur. The establishment of the center has been approved by the IIT Kanpur Senate, but we are still waiting for the funding from the various government agencies. We have been promised funding amounts between 10 crores to 30 crores by various agencies but nothing has moved officially over the last year -- although we have been to a large number of meetings and we have been promised funding. So that will be my key goal --- raise funds for the center, and start the truly interdisciplinary research at the Center. Cyber Security requires interdisciplinarity -- from formal methods, program analysis, cryptography, VLSI, to Systems Software, application software, machine learning, and even techniques from data mining. Fortunately, we have 12 faculty from CSE who have joined hands towards this goal, and we also have domain specific researchers from the electrical engineering who have joined our effort.

The eventual goal is to establish our center as "the" center for cyber security research, education and training in India, and be counted as one of most productive research centers in cyber security in the world.

We also want to establish a large scale SCADA test bed similar to that in Sandia National Labs, and Idaho National Labs in the US, so we could help government entities such as NCIIPC (National Critical Information Infrastructure Protection Center) to accomplish their mission.

I have started to do security audit of IIT Kanpur network and systems recently and identified various vulnerabilities -- and we plan to carry this out as a yearly exercise to ensure that the institute network and systems is less risk prone.

Finally, carrying out research on my existing and pending funding proposals will be a top priority for the next year.