Poonam and Prabhu Goel Faculty Chair Annual Report 2016-2017

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/
Security Center URL: https://security.cse.iitk.ac.in/

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

Teaching

(i) Taught a course on “Computer Networks” in the July-November 2016 semester with 71 students (students from Computer Science, Electrical Engineering, Physics, Mathematics were in the course). The course introduced a lot of hands-on project developing client/server programs with socket layer programming, http server implementation, implementing TCP over a IP simulator, and implementing peer-to-peer networking. The course also emphasized network security towards the second half of the semester. A number of undergraduate projects came out the course as well – in particular one using a network simulator from the US Naval Research Labs called CORE simulator to model and simulate cyber physical systems and induce cyber-attacks to demonstrate physical effects of a cyber-attack.

(ii) Taught the course on "Computer Systems Security” for a 2nd time – this time with 142 students. Almost 30 students were at the post graduate level, and rest from undergraduate – from multiple departments. The course was offered in the “flipped class room” model where the lectures were recorded at the media center prior to the class, and once a week the students met with the instructor for further discussions, and additional information. The course had 3 extensive projects, and 2 “capture-the-flag” contests. The projects were based on finding security vulnerabilities in real web server, web client, and developing exploits to expose vulnerabilities. The system was confined within a pre-configured virtual machine so that the students do not compromise their own system during the project implementations. They also had to fix the vulnerabilities. In the two “capture-the-flag” contests, students competed against each other to find vulnerabilities as “flags”.

(iii) Launched an online MooC on Computer System Security to run during June-July completely free on the MooKIT platform developed at IIT Kanpur. The course has 1600+ registrations, but currently about 300 or so are actively watching video lectures and taking part in online quizzes. A number of CTF events will be part of this online course. Given the serious shortage of manpower in India in the field of cyber security, we believe this course would indeed make a difference.

(iv) Accepted 15 summer interns from various institutes in India for 2 months summer projects at IIT Kanpur so that these students get inspired to pursue a career in cyber security.

(v) In November (18th to 20th) 2016, Organized the 14th ACM/IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE 2016) conference at IIT Kanpur. It was attended by international experts in formal methods, especially those who apply formal methods in system design. This is the first time this conference was hosted in India – until now it was either in Europe or in North America. The conference also features an international contest on embedded system design.

(vi) Organized the Cyber Security Awareness week (CSAW) first time at IIT Kanpur in conjunction with the New York University's Tandon College of Engineering, and New York University, Abu Dhabi, concurrently during 10-12 Nov 2016. The CSAW featured capture-the-flag contest, embedded security challenge, Applied research competition and a mini symposium. While all north American participants contested in New York, all middle eastern contestants in Abu Dhabi, all Indian contestants came to IIT Kanpur campus and competed over 3 days. The competition was sponsored by NTRO. This year we are expanding the scope and scale of the CSAW 2017.

(vii) I also invited multiple researchers from India, as well as from the US for lectures at our department throughout the year, including several cyber security experts.

(viii) Admissions in Charge of PG Admissions: As admissions in charge of PG admissions, I helped admit over 15 new PhD students last year, and now our PhD student numbers have increased to over 50. In the recent recruitment, we will add more than 10 – and cross 60. Our goal is to reach 100 PhD students in steady state with at least 10-15 graduating each year. Currently, we graduate about 4-6 in a good year, but most years even less. We also revamped the MS by research program, and currently we have 5 MS by research students, and a few will be added in July.

(ix) Currently supervising 2 post doctoral fellow, 4 PhD students, and 12 Masters thesis students (including MS by Research). Also supervising 10 project engineers.

Research

(i) Our *interdisciplinary center for cyber security and cyber defense of Critical Infrastructures (C3I)* finally got funded this year for 14.43 crores over 5 years. The SCADA test bed similar to Idaho National Labs will come up in about a year. A new building for Cyber Security Center will be built on campus and the SCADA test bed will be built in the new building. The major focus of the center will be SCADA Security, Smart Grid Security, Manufacturing Automation Security, Malware repository and analysis, Block Chain based Monitoring of high privileged users in an IT system, cryptographic algorithms and mathematical attacks, and deep learning for power system monitoring and resiliency.

(ii) A SCADA lab in the CSE department of IIT Kanpur from the faculty initiation grant provided by the institute has been completed. Cyber Security vulnerabilities in SCADA systems, and various remediation techniques are main target of research in the SCADA Lab. We have discovered many vulnerabilities, some vendor specific, some standards specific in SCADA system, and reported one critical vulnerability to CERT-In.

(iii) We received an Indo-UK research grant on forecasting solar power output based on correlating past weather prediction vs past real weather data and modeling the solar output on weather data and uncertainty of prediction derived. It is part of a very large consortium led by IIT Kharagpur, but our work is confined to solar output prediction engine development using machine learning, and we received 48 lacs over 4 years.

(iv) US AFOSR (Air Force Office of Scientific Research) has funded our research on formal methods for detecting code-replacement attacks in SCADA systems, and remediation techniques by behavioral signature derivation technique. A project engineer is building a tool that extracts behavioral signature of control programs and use that to detect code replacement attacks. We are also collaborating with Prof. Ansuman Banerjee from Indian Statistical Institute, Kolkata in this project. We are also submitting a new proposal to AFOSR on a Science of resilient CPS systems.

(iv) A 1.3 crore funding was awarded to us from the UAY program of MHRD. UAY stands for "Ucchatar Aviskar Yojna" and it requires an academic team to work with an industry such that the industry pays 25% of the funding, and rest is paid by various ministries. Our UAY is paid by MHRD, and DST along with Nivetti system. We are developing cryptographic co-processor for IPSec implementation in the Nivetti routers, and also working on verification of OpenSSL and redevelopment of vulnerable components of OpenSSL. 3 engineers have been working on this project.

(v) We received a 4.4 crores worth IMPRINT project funded by MHRD and Railway Ministry to establish a virtual network center for formal methods research along with IIT Bombay and IIT Kharagpur. Working with a team of researchers in formal methods from IIT Kharagpur, and IIT Mumbai to develop a formal method based methodology and framework for critical software industry sector in India such as nuclear industry, railways, and automotive industry. Our funding portion in this proposal is about 1.2 crores over 3 years.

(vi) Overall, in the past one year, received over 20 crores in external funding for cyber security research, lab development, and manpower development.

(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) 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 (5 papers written so far) with post doctoral fellow Dr. Asan Basiri

b. Cyber Security of Wide Area Monitoring and control in Power Systems (with PhD student Avik Dayal at Virginia Tech)

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 PhD student Saurabh Kumar)

e. Malware analytics with Honey pots and Honey Nets (with 11 Master's thesis students – 6 are graduating, 5 taking over)

f. Development of Block chain based Authentication of IoT devices in IoT network (1 master's student, and 1 faculty collaborator in IIIT Allahabad)

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

B. Your accomplishment as a Faculty Chair

Academic Accomplishments during 2016-17

- 4 peer Conference Papers
- Three Invited Conference Papers
- Two Invited Conference Tutorials
- Two invited FDP (Faculty Development Program) Lectures
- Two Keynote talks at International Conferences
- Several talks at various Government and non-government organizations

Other Accomplishments during 2016-2017

- Continuing as the Editor-in-Chief of ACM Transactions on Embedded Computing
- A number of keynotes in 2017 to be delivered at various International Venues
- Continuing an Associate Editor for ACM Transactions on Cyber Physical Systems
- Served on Program committees of 6 International Conferences
- Serving as a General Chair of an International Conference in November 2017

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

Patents:

- Bottom-up approach for integrating models for software components using contracts, P Joshi, H Yu, **SK Shukla**, JP Talpin - US Patent 9,477,446, 2016

- Timing-oriented and architecture-centric system design using contracts, H Yu, JP Talpin, **SK Shukla** – US Patent 9,459,840, 2016

Conference Papers (Peer Reviewed)

- 2017 Mohamed Asan Basiri M and **Sandeep K Shukla**, "Flexible Composite Galois Field GF ((2*m*)2) Multiplier Designs", accepted for VDAT 2017: 21st International Symposium on VLSI Design and Test, Roorkee, India, June 2017
- Rourab Paul and **Sandeep Kumar Shukla**, "A High Speed KECCAK Coprocessor for Partitioned NSP Architecture on FPGA Platform", accepted at VDAT 2017: 21st International Symposium on VLSI Design and Test, Roorkee, India, June 2017
- Prachi Joshi, Haibo Zeng, Unmesh D. Bordoloi, Soheil Samii, S. S. Ravi and **Sandeep Shukla**, "The Multi- Domain Frame Packing Problem for CAN-FD" to be published in the European Conference on Real Time Systems (ECRTS 2017), Dubronvik, Croatia, June 2017.
- P Joshi, H Zeng, **SK Shukla**, C Lin, H Yu, Design space exploration for deterministic ethernet-based architecture of automotive systems, In the Proceedings of IEEE High Level Design Validation and Test Workshop (HLDVT), 2016, San Francisco, CA.

Tutorial at Conference

- **S. K. Shukla**, " Cyber Security of Cyber Physical Systems -- Resilient Critical Infrastructure Design," Tutorial *at 12 International Conference on Information Systems Security (ICISS 2016), Jaipur, India, December 2016.*
- S. K. Shukla, "Smart Grid and Cyber Security in Power Systems", Tutorial at the National Power Systems Conference (NPSC 2016), *Bhubaneshwar, India, December 2016.*

Journal Editorials

- **SK Shukla**, Editorial: Continuing the Course, ACM Transactions on Embedded Computing Systems (TECS) 16 (2), 28
- **SK Shukla,** Distributed Public Ledgers and Block Chains-What Good Are They for Embedded Systems? ACM Transactions on Embedded Computing Systems (TECS) 16 (1), 1
- **SK Shukla,** Editorial: Fence Itself Grazing the Field-Security from the Sentries, ACM Transactions on Embedded Computing Systems (TECS) 15 (3), 41e

List of Awards/Recognition/Honors if any:

- Keynote speaker at *Workshop on Cyber-Physical Smart Grid Security and Resilience, at IEEE GlobeCom 2016, Washington DC, 2016, December 2016.*
- Keynote speaker at 6th International Symposium on Embedded Computing and Systems (ISED 2016) at IIT Patna, December 2016.
- Invited speaker at Ashoka University, March 2016.
- Invited speaker at Indian Air Force Central Command Commander's Conference in December 2016
- Invited speaker on Anonymous Browsing with Tor at NTRO, February 2017.
- Invited speaker at the IIT Kanpur Technology Day Seminar, May 2017.
- Invited Speaker at the State Bank of India's Apex Level Information Security Committee, June 2016 on Security in Digital Banking.
- Invited to membership in the subgroup on mobile banking & security, and subgroup on card based payments & security formed by Reserve Bank of India's standing committee on Cyber Security. This standing committee was formed based on the statement on developmental and regulatory policies, issued along with sixth bimonthly monetary policy statement 2016-17 announced on February 8, 2017 by the RBI.
- Serving on the expert committee formed by the Niti Aayog on the CCTNS project of Home Ministry
- 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.
- General Chair, *Security, Privacy, and Applied Cryptography Engineering: 7th International Conference, SPACE 2017*, Goa, India, December 2017.

E. Details of Invited Talks/Seminars/Workshops

- Keynote speaker at *Workshop on Cyber-Physical Smart Grid Security and Resilience, at IEEE GlobeCom 2016, Washington DC, 2016, December 2016.*
- Keynote speaker at 6th International Symposium on Embedded Computing and Systems (ISED 2016) at IIT Patna, December 2016.
- Invited speaker at Ashoka University, March 2016.
- Invited speaker at Indian Air Force Central Command Commander's Conference in December 2016
- Invited speaker on Anonymous Browsing with Tor at NTRO, February 2017.
- Invited speaker at the IIT Kanpur Technology Day Seminar, May 2017.
- Invited Speaker at the State Bank of India's Apex Level Information Security Committee, June 2016 on Security in Digital Banking.

F. Organized the Following Advanced Workshop/Event during 2016-17

- Organized CSAW (Cyber Security Awareness Week) events, competitions and workshop in November 2016.
- Organized the ACM/IEEE MEMCODE Conference in November 2016 at IIT Kanpur, the 14th edition of an International Conference – first time outside US or Europe.

G. Details on the Thesis Supervised/ Students Guided During 2016-17 at IITK

PhD

Abhay Kumar – 2nd year PhD student
Tentative Thesis Topic – *Smart Grid Security Vulnerabilities and Mitigation*

Saurabh Kumar – 2nd year PhD student
Tentative Thesis Topic – *Android Security*

Subham Sahai – 4th year PhD student
Tentative Thesis Topic – *Formal Verification of Cryptographic Protocols*

Gufran Khan – 1st year Phd Student
Tentative Thesis Topic – *Ransomeware*

M.Tech Thesis completed

Harshavardhan Sharma (Co-advised with Subhajit Roy)
Thesis Title -- *Symbolic Simulation Based Program Analysis for Vulnerability Detection, August 2016*

Nisith Majithia
Thesis Title -- *Honey Systems – Design, Implementation and Attack Analysis, May 2017*

Rohit Sehgal
Thesis Title—*Tracing Cyber Threats with Honey Systems, May 2017*

P. Krishnaprasad --

Thesis Title – *Capturing Attacks on IoT Devices with Multi-purpose Honey Pot, May 2017*

MTech Thesis – near completion

Saptarshi Gan -- final year Btech-Mtech program
TentativeThesis Topic – *Block Chain Based Authentication Scheme for for Internet of Things (IoT) (expected July 2017)*

Vineet Purushwani -- final year Btech-Mtech program
TentativeThesis Topic – *Dynamic Malware Analytics and Trend Prediction (expected July 2017)*

Pranjul Ahuja -- 2nd Year M.Tech Student
TentativeThesis Topic – *Static Analysis for Malware Classification (expected July 2017)*

Ajay Singh --2nd Year M.Tech Student
TentativeThesis Topic – *Deep Learning Based Image Processing to Classify Malware (expected July 2017)*

MTech Thesis – initial phase

Mugdha Gupta -- 1st Year M. Tech Student
Tentative Thesis Topic – *Malware Classification with Deep Learning techniques*

K. Vijay Kumar – 1st Year M. Tech Student
Tentative Thesis Topic – *Formal Verification of OpenSSL implementation*

Anmol Srivastava – 1st Year M. Tech Student
Tentative Thesis Topic – *Malware Analytics*

Gaurav Raj -- 1st Year M. Tech Student
Tentative Thesis Topic – *Malware Analytics*

K. Amit – 1st Year M.Tech Student
Tentative Thesis Topic – *Honey Pot and Honey Nets*

Subham Singh – 1st Year M. Tech Student
Tentative Thesis Topic – *Honey Pots and Honey Nets*

M. S Thesis

Rohit Negi – 2nd year M.S by Research Student
Tentative Thesis Topic: Cross Layer Security in SCADA Networks

H. Administrative Endeavors During 2015-16

1. Assumed the department head position in the Computer Science and Engineering Department at IIT Kanpur from February 2017.

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

3. Served as the Institute Level Cyber Security Audit Committee Convener 2016-17

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

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 funding has come now, and we are building a new building for the cyber security center. We need to find a donor to name the center.

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.

Currently we are also working on building a digital governance center, and a financial infrastructure security center.