Rajkumar R

rraj.be@gmail.com { +91-9740077760 };

Objective

Seeking admission to MS in CS, through which I can build a further strong foundation in computer science and pursue PhD in one of my interested area. My major interest is in applied mathematics and computer science. It spans across areas like security and privacy, cryptography, machine learning, data mining, algorithm design and operating systems.

Education

Bachelor of Engineering in Electronics and Communication Engineering *May 2010*
Nandha Engineering College [Anna University, Chennai], Erode, Tamilnadu, India

Short Term Course on DSP Programming, Applications and its Math *December 2009*
Indian Institute of Technology - Madras, Tamilnadu, India

Career History

Lead Engineer, *Mobile Security Team -* ***Samsung R&D Institute, Bangalore*** *January 2012 - Present*
On-Device Encryption, OEM software integrity measurement, tampering detection and prevention, DM-Verity, Reactivation lock, HDCP 2.x software stack, Mobicore and Qualcomm trustzone and Secure Voice.

Software Engineer, *DSP Team -* **Allgo Embedded Systems, Bangalore** *June 2010 - October 2011*
Implemented and optimized several core modules of MP3 and AAC audio Codecs for ARM cortex M3 and MIPS platforms.

Skills

Domain Skills	:	Cryptography and related math, trusted computing and trustzone technologies, classifiers and recommendation systems, Bayesian algorithms, Linux system programming, software engineering, computer architecture, DSP algorithms.
Languages	:	Assembly, C, C++, Java, Python, Latex, Bash Shell Scripting.
Libraries	:	GMP, OpenSSL, RELIC, PBC, MIRACL, NumPy, PyCrypto, PyBrain, NLTK, NTL, Sage.
OS	:	Linux, Android, Tizen.
+	:	Compiler optimizations, build systems, bare metal programming, GNU toolchain porting, qemu, virtualization, Android and Linux kernel building and deployment, Raspberry Pi, ARM Cortex and MIPS cores, Optimizations for Out-Of-Order execution.

Recognitions and Awards

Employee of the Month, *June 2013.*
For design and development of OEM software integrity measurement and tampering detection solution.

Spot award, *February 2014.*
For research proposal and POC development to obfuscate data in executable's using mealy state machine.

Spot award, *August 2014.*
For research proposal and POC development to detect dangerous executable files using static and dynamic analysis.

Spot award, *July 2015.*
For research paper titled 'Dynamic Verifiable Encrypted Keyword Search Using Bitmap Index and Homomorphic Signature'.

Spot award, *August 2015.*
For research paper titled 'Forward Secure On-Device Encryption Scheme Withstanding Cold-Boot Attack'.

Publications

1. "**Forward Secure On-Device Encryption Scheme Withstanding Cold-Boot Attack**," Rajkumar Ramasamy, S.Sree Vivek, *IEEE International Conference on Cyber Security and Cloud Computing (CSCloud'15).*
2. "**Biometric Key-derivation with Application in On-Device Encryption**," Rajkumar Ramasamy, S.Sree Vivek, *International Conference on Innovations in Information Technology (IIT'15).*
3. "**Dynamic Verifiable Encrypted Keyword Search Using Bitmap Index and Homomorphic Signature**,"Rajkumar Ramasamy, S.Sree Vivek, *ACM Conference on Data and Application Security and Privacy (AFRICACRYPT'16).*(Under submission)
4. "**A Novel Homomorphic Signature With Improved Performance**,"Rajkumar Ramasamy, S.Sree Vivek.(Work Under Progress)
5. "**Identity Management for Devices in Internet of Things**," Rajkumar Ramasamy, S.Sree Vivek, Reuben Varghees George, Naveen Kumar Budda (Under submission for patenting)

Leadership Activities

Initiator and Lead, Linux Club during under graduation *December 2006 - May 2010*
Involved in FOSS movement, conducted workshops, weekend meet up's and tech talks.

Module Lead, Mobile Security Team, Samsung R&D Institute, Bangalore *March 2013 - Present*
Mentored & lead a team of 5 engineers for development of security assurance solution for Android and Tizen OS.

Summary of Selected Work

Owner of **OEM Software Tampering Detection and Prevention** modules (Rooting Detection, Integrity Check Daemon and Rooting Prevention), *for Android and Tizen.*

- Threat modelling and analysis of CVE and methods for privilege escalation in Mobile devices.
- Designed algorithm to detect insidious files, which can escalate privilege, using binary analysis.
- Designed algorithm to detect privilege escalation by unauthorized process.
- Designed and implemented Integrity Check Daemon (ICD).
- Made changes in Android kernel to authenticate the applications which request privilege escalation.
- Designed Mealy state machine to obfuscate data inside executables.
- Implemented trustzone components to store and share the results.
- Made changes in Android and Tizen platform services like secure boot, Systemd, init system, SMACK and SE-Linux to support the module.

Maintainer of **Full Disk Encryption and Verified Boot**, *in SRI-B, for Android and Tizen flagship models*

- Implemented key management module (Using scrypt, Samsung hardware key manager and trustzone).
- Implemented OEM signing module for Verified boot.
- Added support for default encryption and SD card encryption feature for all Samsung flagship models.
- Added support for Samsung secure key store and scrypt PBKDF for key management.
- Made changes in services like VOLD, filesystems, device bootup sequences and device mapper targets.
- Made auxiliary changes in build system, init services and filesystem.
- Developed POC using "Merkle Tree" to bootstrap Verified Boot project

Development of **Popularity Prediction of Photo in Social Network** for Samsung Secure Voice Solution

- Implemented a neural network based classifier and Naive Bayse based classifier for performance comparison.
- Integrated the solution with Gallery and Facebook interface and collected photos using Facebook API.
- Precision is collected based on grand truth.

Development of **MIKEY-SAKKE key exchange module** for Samsung Secure Voice Solution

- Implemented MIKEY-SAKKE protocol using Barreto-Naehrig curves in RELIC Library.
- Implemented F_p^{12} arithmetic & Barreto-Naehrig curves using OpenSSL.
- Integrated the solution with Linphone application.

Development of **HDCP 2.x Software Stack**, *for Android and Tizen*

- Developed Mobicore and QSEECOM trustlets for key management and crypto modules.
- Implemented control path and involved in implementation of whitebox AES.
- Implemented authentication protocol subsystems like key derivations, key agreement and locality check.
- Developed test application for Android and Tizen.

Development, Porting and Optimization of **MP3, AAC Codec and auxiliary DSP modules**

- Optimized Huffman decoding algorithm for the AAC decoder.
- Implemented a highly optimized division algorithm using Newton-Raphson method.
- Optimized computationally heavy modules like TNS, IMDCT, Windowing and Huffman.
- Participated in design, analysis and review of algorithmic optimizations.
- Integrated codecs with multimedia frameworks (Stagefright and GStreamer).

Personal Independent work, *for self learning*

- I have developed immense interest towards mathematical areas like abstract algebra (groups and finite fields), number theory, pairing, bilinear maps and their applications in cryptography.
- I have created a dictionary to display meaning, usage, etymology of a given word using python and NLTK.
- I enjoy my hands-on experiments in bare metal programming, Raspberry pi, Linux kernel, Cyanogenmod ROM's, U-boot, GNU toolchain etc.

Independent Courses

Independent Course works, *for self learning*

- Computer Language Engineering [MIT]
- Theory of Computation [MIT Mathematics]
- Linear Algebra [MIT Mathematics]
- Abstract Algebra [Harvard]
- Foundations of Formal & applied Cryptography. [MIT OCW]
- Selected and Advanced topics in Cryptography. [MIT OCW]
- Trust and Trusted Computing. [Stanford Courseware]
- Foundations and Advanced topics in Natural Language Processing. [Stanford Courseware]
- Winter School of Cryptography series. [Bar-Ilan University]
- Machine Learning. [Stanford Coursera]

Abstracts

1. **Forward Secure On-Device Encryption Scheme Withstanding Cold-Boot Attack**, CSCloud'15

   Encryption of data residing on the permanent memory of a device, also known as On-Device Encryption (ODE), is a well studied problem with many popular software available these days. We consider the adversary who is capable of taking one RAM snapshot (e.g: Cold Boot Attack) when the device is in locked state. Writing data securely, when the device is in locked state can be handled in the presence of this strong adversary, by employing public key encryption techniques. When it comes to reading of data from a locked device, it is not known until now, whether it is possible. In this paper, we state the impossibility of performing the read operation securely, when the device is in locked state. Moreover, we propose a new forward secure ODE scheme which supports secure writing in locked state and is more efficient when compared to the public key based solution. We have proposed the security model for forward secure ODE and proved the security of our scheme in the proposed security model.

2. **Biometric Key-derivation with Application in On-Device Encryption**, IIT'15.

   Secret key plays a pivotal role in every cryptographic protocols. The cryptographic key should be easy for a user to reproduce and at the same time, very hard for an adversary to predict. Inherent nature, permanence and difficulty to impersonate enables biometric as a strong candidate to derive cryptographic keys. In this paper, we propose a novel biometric key generator (BKG) based on Shamir's secret sharing scheme, using bilinear mapping. We have reviewed the security requirements for a Biometric Key Generator formally and have mathematically proved the security of our scheme. We have used our new BKG scheme to generate cryptographic key in a forward secure On-Device Encryption scheme, which can withstand cold-boot attack.

3. **Dynamic Verifiable Encrypted Keyword Search Using Bitmap Index and Homomorphic Signature**, AFRICACRYPT'16 (Under Submission)

   Outsourcing data storage to the cloud securely and retrieving the remote data in an efficient way is a very significant research topic, with high relevance to resource constrained system like mobile devices. With the ever growing security and privacy concerns, encrypting the data stored remotely is inevitable but using traditional encryption thwarts performing search operation on the encrypted data. Encrypted keyword search is a cryptographic scheme, which offers search functionality and at the same time, ensures security and privacy of the remotely stored data. In this paper, we consider Searchable Symmetric Encryption (SSE) in the presence of a Semi-Honest-But-Curious Cloud Service Provider (SHBC-CSP). We have defined a new security notion for SSE in presence of SHBC-CSP, contrived two new SSE schemes and proved their security formally in the proposed security notion. Dynamic Verifiable Encrypted Keyword Search (DVSSE), among the two new schemes, is the first SSE scheme which is both dynamic and verifiable. We have implemented our schemes and compared their performance and complexity with existing schemes.

4. **A Novel Additively Homomorphic Signature With Improved Performance**, (Work Under Progress)

   A homomorphic signature scheme allows certain operation to be performed on digital signature of different messages, while preserving the authenticity and integrity. There are various cryptographic schemes like RSA, Paillier which offer partial homomorphism in the context of encryption and a few cryptographic encryption schemes which offer full homomorphism. There are several practical relevance to the homomorphic signature schemes, like, network coding, integrity check for secure database outsoursing, Proofs of Retrievability in the cloud, to name a few. In this paper, we study the security requirements for homomorphic signature schemes and a few signature schemes that allow homomorphic computations. We propose a novel homomorphic signature scheme based on Composite Residuosity and prove the scheme to be existential unforgeable under adaptive chosen-message attacks (EUF-CMA).

5. **Identity Management for Devices in Internet of Things**, (Under Submission for patenting)

   Abstract withheld as its under submission for patenting.