Secure & Interconnected Mobility: Integrated Security for Mobile, Automotive, and Cloud Computing

Prof. Dr. Ahmad-Reza Sadeghi
TU Darmstadt
Academic Principal Investigator
and Director

Dr. Matthias Schunter
Intel Labs
Principal Investigator
and Chief Technologist

Abstract
The new Intel Collaborative Research Institute for Secure Computing (Intel CRI-SC) that has been founded on May 23, 2012 as a public-private partnership between Intel Labs and Technische Universität Darmstadt, Germany including the Center for Advanced Security Research (CASED). This whitepaper introduces the mission and strategy of the Intel CRI-SC and outlines the initial key research themes that focus on secure computing for interconnected mobility.

Intel Collaborative Research Institute for Secure Computing (Intel CRI-SC)
01.08.2012

Executive Summary

The Intel Collaborative Research Institute for Secure Computing (Intel CRI-SC) is jointly operated by Intel Labs and CASED/Technische Universität Darmstadt, Germany. The Institute conducts **security research for mobile and embedded systems**. It sponsors industry and scientific research to improve the trustworthiness of mobile and embedded devices as well as the ecosystem around them. In this whitepaper, we will introduce the Intel CRI-SC and present its research agenda.

The need for Secure Computing

This Institute is motivated by three key industry trends. The first trend is the Internet of Things (IoT), which motivates interaction between a broad diversity of electronic devices. Today, devices such as phones, tablets, and appliances are becoming even more pervasive and internetworked. We expect this trend to continue with an increased need for secure interconnection, integration, and interaction of those devices. The second trend is the importance of ecosystems that support a particular platform. Since end users make buying decisions based on the overall utility and user experience, the importance of device characteristics decreases while the overall experience delivered by the supporting ecosystem gains importance. This trend creates a need for end-to-end security of a platform that covers the device, supporting clouds, as well as the software ecosystem. The third trend is the convergence of devices with their cloud backend systems. We believe that users will expect their digital assets to be secure on all their devices including the cloud.

These trends create rich new user experiences while bearing the potential for new emerging risks.

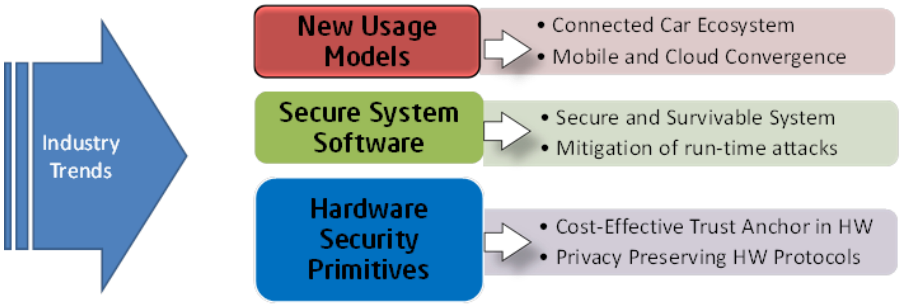
Goals of the Institute

Our mission is to mitigate the emerging risks created by industry trends while still allowing a rich user experience where security mechanisms are seamlessly integrated. In order to achieve this mission, we pursue the following strategic goals in order to enhance security of the mobile and embedded ecosystems:

- **Advance State of the Art:** The first and most important goal is to conduct research in order to enhance the state of the art in securing embedded and mobile systems. This includes conducting our own research on key problems as well as creating research communities that tackle large and complex emerging challenges in this space.
- **Generate Industry Value:** The benefit for users and society is amplified once new research is translated into innovative products and services. As a consequence, the second goal of our institute is to ensure that new ideas are translated into industry value.

Strategy and Initial Research Thrusts

The Institute executes on a user-centric research strategy. This means that we aim at innovative security technologies that are derived from real-world application scenarios and corresponding user needs. This is achieved by developing new concepts and corresponding prototypes that bring tangible benefit to each individual user as well as the society as a whole.



Initial Research Thrusts of the Intel CRI-SC

This is achieved by strategic themes within our research:

1. **Novel Usage Models:** Examine trends in society, derive use cases from these trends, and then develop application level security technologies as well as platform requirements. Our initial focus areas are Mobile, Automotive, and their convergence with the cloud.
2. **Secure System Software:** The second thrust identifies common security needs in order to evolve the state of the art in secure systems. By providing secure platforms, this thrust will transparently provide enhanced security to the ecosystem while minimizing the design effort needed by individual application developers.
3. **Hardware Security Primitives:** This thrust translates the protection needs and gaps of the novel usage scenarios and secure systems into proposed hardware extensions. The main goal is to identify lightweight hardware extensions that provide maximum security benefit.

For each of these areas, we pursue our goals to enhance the state of the art while creating value for industry with a focus on the mobile and embedded ecosystems.

1. Increased Demand for Secure Computing

We live in a digital age; going about our daily lives invariably involves interacting with a diversity of electronic devices which are increasingly pervasive, mobile and highly integrated. Many such devices offer computing power exceeding that of desktop personal computers of only a decade ago. Moreover, digital devices are becoming increasingly interconnected via a range of connectivity options, in many cases wirelessly. Such advances have prominently revolutionized the way we communicate, entertain, access information and conduct financial transactions. Other, perhaps less obvious, aspects of our lives have been positively affected such as transportation, infrastructure and health. While the benefits to society are enormously valuable, they go hand-in-hand with myriad security and privacy risks. We will only be able to harvest these efficiency gains if we can demonstrate how to mitigate these risks.

Diversity of Mobile and Embedded Systems

Mobile and embedded systems are widely represented across the compute continuum ranging from high-end smartphones and tablets through embedded microcontrollers to extremely resource constrained devices such as smartcards and RFIDs. Additionally, many devices and systems combine computational with physical aspects. Such cyber-physical systems interact with their physical environment using sensors and actuators, for example, enabling haptic technologies on smartphone devices or sophisticated safety functions in the automotive sector. As Moore's law continues to hold true, mobile and embedded systems will continue to become more highly integrated, computationally powerful and inter-connected, enabling as a result many new application scenarios. In particular, converged solutions combining personal mobile devices such as smartphones with the many embedded systems we interact with on a day-to-day basis are emerging, in many cases additionally leveraging cloud services. These promise to offer increased benefits to users across diverse applications such as transport, ticketing, parking and access control.

Security and Privacy Threats

The growing popularity and deployment of mobile and embedded systems, together with the fact that they increasingly store and process security-critical and privacy-sensitive data, make them an attractive target for attacks ranging from malware-based attacks to sophisticated side-channel and invasive attacks targeted at the hardware itself. As the diversity and power of connected computing devices grow, a single, highly mobile device has the capability to manage many aspects of an individual's life, from personal and professional communications, financial transactions and information access to media consumption, gaming and entertainment. The potential to span such a broad spectrum with a single powerful device poses significant risks due to the different threat profiles associated with these usages.

At the same time, lower-end devices, such as embedded controllers and the sensors and actuators that interact with the physical environment present unique attack surfaces and opportunities for compromise. The cyber-physical systems that are built on such components are open to attack from both the physical domain and the cyber domain resulting in a wide and challenging threat landscape. Additionally, sensors and actuators are typically resource constrained which present an impediment to the deployment of heavyweight security features. A holistic approach that addresses the security capabilities of these less capable devices and the more sophisticated devices they communicate with will be critical to maintaining the appropriate security posture.

Mobile and Embedded Systems Convergence

As powerful mobile devices such as smartphones become near-ubiquitous, they increasingly intersect with the multitude of embedded systems we interact with on a daily-basis. As an example, consider the automotive sector where modern vehicles consist of tens of networked embedded controllers performing diverse functions. Imagine a world where Susan only has to touch her smartphone against the door to deactivate her vehicle's locking system. As she and her friend enter and make themselves comfortable, a combination of on-board camera and Susan's smartphone has already unobtrusively and seamlessly authenticated her with the vehicle systems. The playlist she was enjoying at home is playing seamlessly on the infotainment system and her preferred seating position, favorite mobile apps and a plethora of other settings are already in place. Conveniently with Susan's permission, this behavior can be replicated on any vehicle, whether her own or a rental, and is extended to other vehicle occupants as appropriate. On stating her chosen destination to the navigation system, she sets off and the vehicle interacts with cloud services to optimize the route based on real-time traffic information, driving preferences and driving style in order to maximize fuel-efficiency, journey time and other parameters. Susan's friend decides that he wants to do a little work on the trip and on verbal command his work environment is replicated from the cloud, allowing him to review a working document using a combination of voice and gestures. As the journey progresses, the vehicle communicates with other vehicles in the vicinity in order to autonomously maintain safe driving distances, relay information on road surface conditions or give early warning on collision avoidance. This information may of course be uploaded to the cloud thus allowing optimization of the driving experience across the wider driver population. Susan and her fellow traveler arrive at their destination in comfort and above all safely, having taken the most efficient route possible.

This vision requires the placement of an enormous level of trust in the safety and reliability of the underlying technologies. A significant portion of this trust revolves around the security and privacy properties of the deployed solutions, where a compromise may have outcomes ranging from user inconvenience to loss-of-life in the most extreme case. Creating the appropriate security foundations requires an end-to-end and holistic approach across a number of research vectors. *Novel Usage Models* such as those described above must be systematically explored in order to investigate the threat landscape and develop security architectures and requirements that deliver enhanced trustworthiness across a range of market segments. The deployment of increasingly powerful mobile devices and vehicle infotainment systems will require a focus on increasing the resilience of *Secure System Software* to today's sophisticated malware. An emphasis on behavioral approaches such as control-flow integrity enforcement will have an important role in moving beyond traditional signature-based anti-malware defenses. *Hardware Security Primitives* which enable security solutions to be extended to resource-constrained mobile and embedded devices must be investigated with a focus on lightweight cryptographic building blocks, privacy preserving protocols and cost-effective hardware trust anchors. Addressing these research vectors will provide the solid foundation that is required to enable these and other novel and interesting usages.

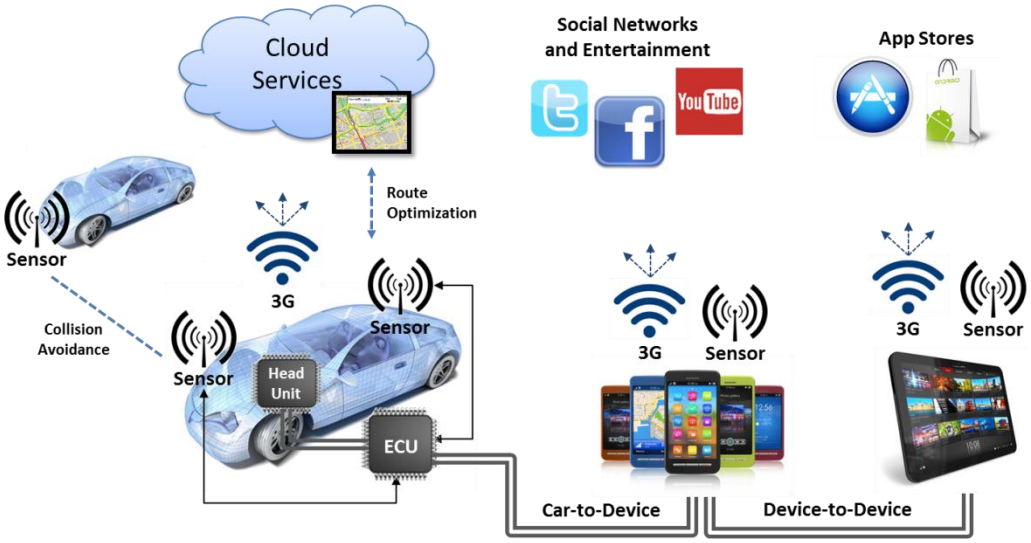


Figure 1: Convergence of the Automotive and Mobile Platforms

Contribution of the Intel CRI-SC

The Institute will bring together thought leaders and drive research to dramatically advance the trustworthiness of mobile and embedded devices from across the compute continuum. Specifically, we place a strong emphasis on the embedded and smartphone segments while addressing the security challenges of the resource-constrained devices that are integral to complex, distributed embedded systems. We will explore several emerging usages at sufficient depth in order to understand the end-to-end frameworks for cyber-physical security. The goal will be to map out threat profiles and generate security requirements that can inform future security architectures in the mobile phones and embedded at levels ranging from the network and platform, through System-on-Chip (SoC) down to resource constrained embedded controllers. For each usage, we need to understand the attack surfaces and predominant vulnerabilities. Based on this analysis, we will propose new approaches to security, from architecture and cryptographic support to infrastructure features and policy frameworks. The specific research areas of the Institute reflect progression from analysis to the development of new technology approaches.

Mission and initial Research Thrusts of the Intel CRI-SC

The Intel CRI-SC will focus on the following research thrusts.

1. **New Usage Models:** Our main research target will be on security and privacy aspects of Cyber Physical Systems used in different scenarios and contexts. We will systematically investigate threats in end-to-end environments and necessary mitigation approaches applicable to the use in various market segments (including automotive, smartphones, and others). This will motivate enhancement of existing security techniques, exploration of novel approaches to resource-constrained security, and establishing trust in various classes of embedded devices and smartphones.
2. **Secure System Software:** Control-flow or runtime attacks are a prevalent attack vector against today's software programs. These attacks are feasible on a broad range of platforms, starting from desktop PCs up to mobile and embedded systems. We will work on defining a new generation of technologies in this area. In this context, a major challenge is tackling runtime attacks (e.g. code injection and return-oriented programming). One goal in this area is to ensure that applications will execute under the enforcement of control-flow integrity

(CFI), particularly on smartphone platforms. This framework ensures that the control-flow of a program follows only legitimate paths determined in advance. In particular, our focus is on Android and the embedded Intel Atom processor.

3. **Hardware Security Primitives:** Highly embedded devices, like RFID chips and low-cost sensor nodes, are typically subject to strict resource constraints that prevent the deployment of standard security hardware. Hence, these systems are subject to hardware and side channel attacks. One of the projects will focus on security protocols to establish trust in a remote embedded device by assuring that the device is in the software state and its hardware is genuine and has not been tampered with. A challenge for achieving this goal using today's standard cryptographic and security protocols is that these solutions often exceed the computational and memory resources of resource-constrained embedded systems. This holds even more once strong privacy guarantees need to be given. Hence, we will explore lightweight cryptographic and security protocols specifically designed for mobile embedded system environments, focusing on privacy-preserving solutions.

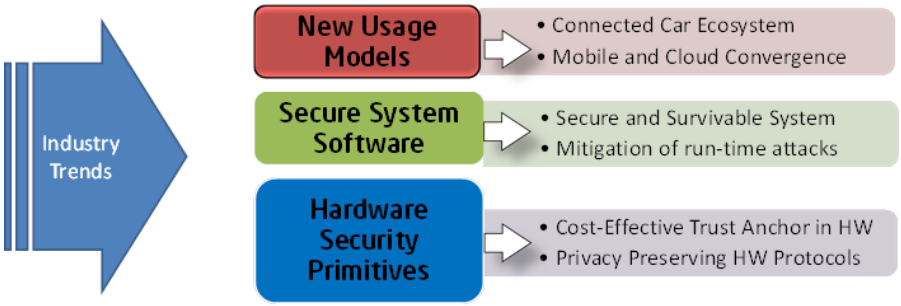


Figure 2: Initial Research Thrusts of the Intel CRI-SC

2. Initial Research Thrusts in Focus

Thrust 1: New Usage Models

Converged solutions combining mobile devices with complex embedded systems are emerging in many sectors. Examples are payment systems, ticketing, smart grid and transport. Meeting the security and privacy challenges of these and other usage models will require a deep, end-to-end understanding of the technologies and the threat landscape in order to extract security requirements that can inform security architectures that provide the highest possible level of assurance. We will begin our investigation by focusing on the automotive sector, initially exploring Car-to-Device applications that integrate mobile devices such as smartphones with in-vehicle systems in order to deliver converged solutions that enable improvements in driver and occupant comfort and safety. Novel usages such as credential management frameworks that allow users to non-intrusively and seamlessly authenticate themselves with vehicles promise to revolutionize diverse market segments such as car rental and car insurance as well as vehicle taxation and driver licensing. Personalization of vehicle functions and vehicle services, some of which may be cloud based, will be enabled. This systematic analysis of novel usages will provide the inputs for designing secure systems software as well as novel hardware primitives. This ensures that our innovations are highly relevant to the actual end user experience.

Thrust 2: Secure System Software

The market penetration of mobile applications is almost everywhere. Global players such as Apple and Google provide hundreds of thousands applications for different purposes on their "App Stores", e.g., games, lifestyle, books, entertainment, to name a few. A recent download statistic for Google Android's App Store shows that over 10 billion apps have been downloaded over the last 4 years. Furthermore, smartphone manufactures increasingly provide mobile cloud services and applications allowing users to store data (photos, calendar, contacts, etc.) in the cloud so that a user can access his data from whichever device.

The high number of downloaded applications increases the attack surface of the underlying platform, because many of the applications available today are the product of inexperienced and security unaware developers. Hence, though most of the applications may have no malicious intent, they may suffer from diverse vulnerabilities allowing an adversary to compromise the device and steal sensitive information by means of runtime or control-flow attacks. The basic principle of these attacks is shown in Figure 3, where mobile applications are represented by their corresponding control-flow graphs (CFGs). Whenever an application or its linked libraries suffer from a software bug, the adversary can exploit the bug to subvert the targeted execution-flow of an application and transfer it to malicious injected code, or already existing code pieces.

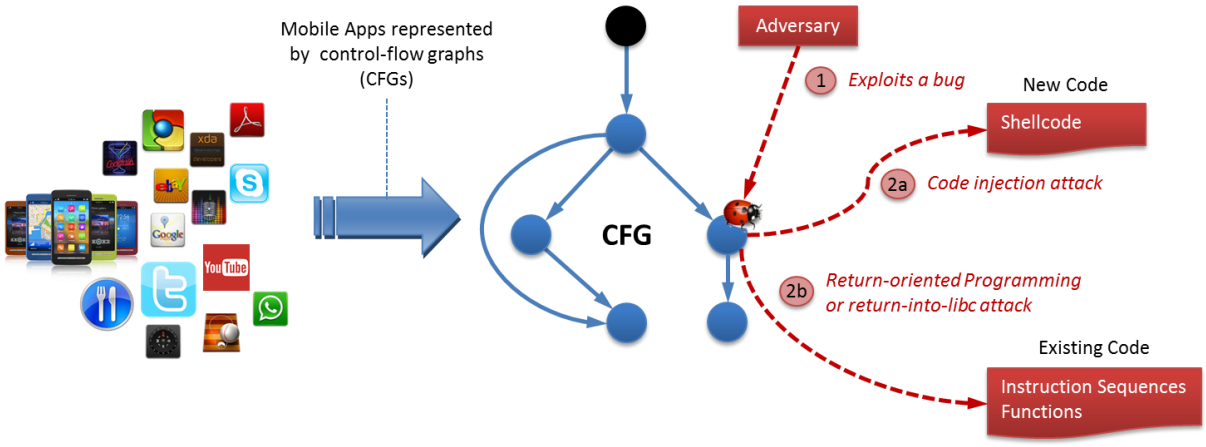


Figure 3: Basic Principle of Control-Flow Attacks against Mobile Apps

These attacks affect all mobile operating systems of today and often result in the leakage of sensitive information such as SMS or contacts. These attacks affect the Android platform as well. Although Android applications are mainly developed in the type-safe Java language they link to a number of native libraries which are subject to traditional control-flow attacks. Moreover, control-flow attacks are increasingly utilized to break out from the application's sandbox by launching privilege escalation attacks such as root exploits.

In this research thrust we aim to develop novel and innovative security technologies to protect mobile and embedded systems from being compromised by control-flow attacks, while our focus will be on the Android operating system running on an underlying Intel Atom processor. One particular research target is the development of a control-flow integrity (CFI) framework for Android. CFI is accepted as a general countermeasure to prevent control-flow attacks by monitoring if the application always follows a valid path of the control-flow graph (CFG). In particular, we aim to use

CFI as an enabler for secure software services. One security service we envision is runtime attestation of mobile and embedded systems, a mechanism that allows a remote verifier to attest mobile devices regarding their runtime state, i.e., if they have been compromised by means of a control-flow attack. This goes a step further than existing remote attestation mechanisms which are mainly based on load-time attestation, i.e., checking if a given program binary has been altered offline. The second security service we envision is enhanced data sandboxing at the memory-level. We aim to design a fine-grained access control framework that ensures that runtime attacks cannot be utilized to overwrite security-critical data structures residing in the memory space of an application. Finally, we will explore cloud-based applications to identify novel use-cases that build upon CFI protection of the browser and web applications at the client-side.

Thrust 3: Novel Hardware Primitives

Many complex embedded systems can be described as networks of one or more control units supported by a variety of subsystems, such as sensors and actuators. Smart energy grids have been proposed, where a communication gateway and several cost-sensitive, networked measurement sensors are installed at each household and facility. Other deployments include the control and monitoring of industrial manufacturing plants and critical infrastructures. In particular, modern automobiles rely on a diverse mix of embedded processors, sensors, actuators and human interface devices, networked over one or more buses, for functions including engine, transmission and chassis control, passenger safety and entertainment. Such heterogeneous and distributed systems can exhibit large attack surfaces and fundamental approaches are required to harden these systems. As malicious code injection is a primary attack vector, techniques that can automatically detect and possibly disable malicious code at individual nodes in the system are of particular interest. Such attestation techniques are typically concerned with the validation of the software state of a device. In a typical software attestation scheme, the verifier challenges the prover which returns a response unambiguously identifying the prover's state to the verifier.

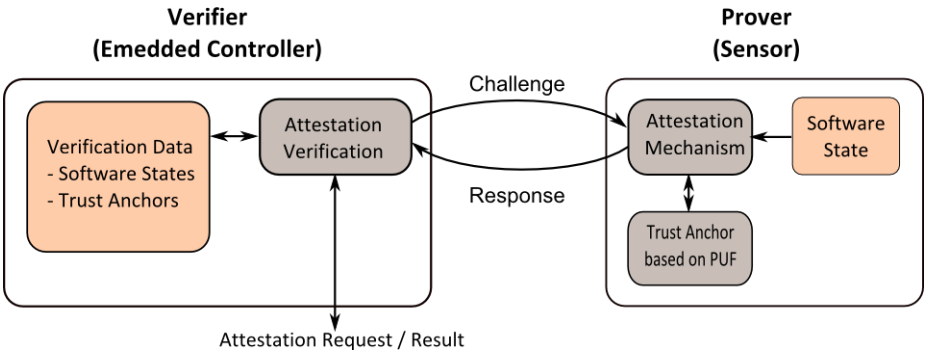


Figure 4: Attestation of Embedded Devices

As part of this research, we aim to enable attestation in environments where there is an asymmetry in computational resources between the verifier and the prover, where the prover is resource-constrained in terms of computational power, physical area and in some cases electrical power. In order to implement attestation, the resource requirements at the prover must be sufficiently minimal to allow deployment on typical nodes, where complex cryptographic techniques, such as asymmetric cryptography, are not feasible. We recognize that meeting these objectives will require some level of platform support at the hardware level and aim to identify a minimal set of security requirements in order to inform future platform design. Furthermore, it should not only be verified whether a

prover's software is in an appropriate state but that the hardware of the prover is correct and authentic. In effect, we extend the attestation concept to cover the hardware state of the device, i.e., to verify that a device is not only executing the correct software but that the software is executed on correct and authentic hardware. Physically Unclonable Functions (PUFs) are promising security primitives that enable the creation of trust anchors which enable the binding of attestation methods to hardware in such a way that it is economically unviable to counterfeit or clone a device.

3. A Safer Mobile and Embedded World

We delegate more and more responsibility to the near-ubiquitous digital devices that pervade our lives. Ensuring security and privacy of these devices and of the services of the associated ecosystem is a key requirement of society. The majority of work today is focused on secure architectures for these new classes of devices and their components. This is important, but with large numbers of devices engaged in complementary or joint activities in diverse security contexts, building a new generation of architectures is not enough. Each usage requires a deep understanding of the platform technologies necessary to provide the highest possible level of security while seamless use of diverse devices for the same tasks will require a different level of interoperability and support in the ecosystem. At the Intel Collaborative Research Institute for Secure Computing, we aim to meet these objectives with a layered approach to the research agenda with work in novel usage models informing and driving research at the system software and hardware primitive levels. We believe that only an integrated and end-to-end approach, which is cognizant of the technologies from the resource-constrained embedded controller right up to the cloud-based server, is capable of delivering the safer mobile and embedded world we all depend on.

4. Acknowledgements

This whitepaper is based on contributions and feedback from the extended Intel CRI-SC Team. Contributors include Meiyuan Zhao, Manoj Sastry, and Anand Rajan from the Intel Labs in USA as well as Patrick Köberl, Christian Wachsmann, Steffen Schulz, Lucas Davi, and Pouyan Sepehrdad from our local team.