Centro de Investigación
en Computación

Instituto Politécnico Nacional

CISEG

Cybersecurity Laboratory

Computing Research Center

Inatituto Politécnico Nacional

MÉXICO

http://www.ciseg.cic.ipn.mx

http://www.cic.ipn.mx

http://www.ipn.mx

ciseg@cic.ipn.mx

About us

The Laboratory of Cybersecurity (CISEG) at the Computing Research Center, National Polytechnic Institute (CIC-IPN), arises as a institutional effort to contribute to the search of innovative solutions to address the problem of secure the cyberspace and its users, by s the research on security of information and critical assets of Information and Communications Technologies (ICT).

The creation of CISEG at CIC-IPN is an effort to opportunely align human resources and institutional assets in order to promote research and education on Cybersecurity with the objective to contribute to knowledge and technology generation, as well as educating high specialized professionals on the field. The main topics to be covered by CISEG are:

Infrastructure Security

- Security on Operating Systems and Protocols
- Computer Incident Information Recovery: Forensics
- New Architectures for Intrusion Detection Systems
- Malware detection and propagation and Advanced Persistent Threats (APT)
- Security in the Internet of Things
- Security on Critical Infrastructure Monitoring Technologies
- Analysis and Design of Security Protocols
- Cryptographic Implementations>/
- Cryptanalysis
- Application of Evolutionary Algorithms for Cybersecurity
- Biometrics

The Laboratory of Cybersecurity offers you a great experience for your academic and professional development. There are several ways you can get involved with it according with your current academic status:

- Attending CISEG research seminar as first semester student of CIC-IPN.
- Attending CISEG as full time student of CIC-IPN.
- Visiting CISEG for summer seminar under Delfin stay program.
- Running your social service at CISEG (bachelor's program).
- Running your graduation project with us (for last year at bachelor's program)

Research Topics

Security in Cyberspace

This research brings together the work related to the infrastructure involved in Cyberspace, such as application servers, networking equipment, access points, fixed and mobile customers and Firewalls, intrusion detectors, VPNs, Honey Pots, etc. . The generation and application of knowledge in this line considers design, analysis and evaluation of architectures, Layout, Protocols, Algorithms, controls and tools that have defensive, offensive, preventive, reactive and recovery purposes. This research is made up of the following topics:

- **Safety Data Networks and the Internet:** Study of network attacks and techniques to defend against them. Includes topics Intrusion Detection, Access Control and Filtering, event correlation, Virtual Private Networks, architecture analysis and pattern generation and anomalous behavior.
- **Host Security:** Study models and security controls for operating systems, applications and specific software. It addresses topics hardening techniques, evaluation and design of secure systems, high availability architectures, embedded systems and mobile devices.
- **Network Forensics:** Study of the processes of collecting and analyzing digital evidence originated on the network, topics related to the extraction, processing and correlation of volatile information and records from network equipment and specialized methodologies and capture tools are addressed.
- **Host Forensics:** Study of the process of forensic analysis, planning, acquisition, analysis and reporting of security incidents targeting systems. Software tools specialized hardware to perform the various tasks of systems analysis process and its elements in server platforms, regular customers, mobile connectivity systems and equipment.
- **Evaluation of the safety of infrastructure:** Study of methodologies, techniques and tools for evaluation algorithms, protocols, schemes and security architectures. The purpose considers improvements, exploitation, prevention, mitigation and recovery thereof.

IoT Security

The Internet of Things (IoT for its acronym in English) represents the radical evolution of the current Internet to an interconnected network of 'smart objects' that not only collect information from the environment (sensing) and interact with the physical world (action, command and control), but also use the Internet to provide transfer services, analysis, applications and communication of information. This new paradigm enables the development of a variety of applications such as tracking of goods and people, smart homes, smart cities, control and remote command, pedestrian navigation, location-based services, remote patient monitoring, environmental monitoring; to name a few examples.

According to some estimates is expected that by 2020 there are between 50 and 100 billion devices or "things" connected to the IoT. This brings many challenges, including the security issue is of particular relevance. Although the IoT could be seen as an evolution of the traditional Internet, due to the characteristics of IoT security protocols used in traditional Internet can not be directly used or adopted in the IoT. This means that there is a niche opportunity for research and technological development in the three main security challenges in the IoT, confidentiality of information, privacy and trust. In particular, in the context of IoT in this research investigation was conducted in safety:

- **Mobile Devices**
- **Wireless Sensor Networks**
- **Machine to Machine (M2M)**
- **Supervisory Control and Data acquisition (SCADA)**
- **RFID and NFC**

Cryptography

Today the information derived from the business processes of organizations and infrastructure that processes, stores and transfers are subject to a number of scenarios cyberspace where their security can be breached. To protect such information strategies have been developed consisting of: architectures, mechanisms, tools and / or security controls, of which the majority relies on the use of cryptographic components, such as: Secure communications protocols, Management systems cryptographic keys, Authentication systems, Integrity verification systems, Secure storage, etc.

Which together enable the establishment of at least one of the services of information security: confidentiality, integrity, authenticity and / or non-repudiation.

In this context within Cybersecurity Laboratory of the research is grown Cryptography, under which the study of primitive, algorithms, implementations, protocols, procedures, and cryptographic controls commonly done, highlighting a special interest in the following items:

- **Side channel attacks.**
- **Cryptanalysis.**
- **Elliptic Curve Cryptography**
- **Cryptographic Implementations**
- **Electronic payments.**
- **Electronic voting.**
- **Cryptography for Cloud Services and Big Data.**

Evolutionary Algorithms for Cybersecurity

Evolutionary biologically inspired heuristic algorithms have shown in recent decades have broad applicability in solving optimization problems in engineering and the sciences in general. In the case of Cybersecurity, some algorithms such as Artificial Immune System, Genetic Algorithm and Differential Evolution among others, have been successfully used for intrusion detection, optimization tasks used in cryptographic blocks as efficient exponentiation computation, design S substitution boxes, generating pseudo-random numbers and so on. In this line are analyzed and pose some problems in the area of cybersecurity as optimization problems to be solved by the above evolutive algorithms.

Biometric Security

In this line of research to be related to the identification, classification, and user authentication through biometric features work. In most technological applications of biometrics is associated with access control and pattern recognition, in particular the facility has generated product research and technological developments considering voice, iris, retina, fingerprint, and typing cadence. Additionally, it is important to specify that investigations considered to mobile devices, fixed platforms, embedded systems, including sensors capture.

- **Construction of biometric systems:** Study tools for processing, filtering and adapting the information obtained from the sensors capture, in addition to the pattern recognition model and decision making. The study includes HW & SW aspects.

- **Biometric Authentication:** Study focuses on ensuring the identity of human beings with respect to a biometric characteristic. This includes the characterization of valid and invalid patterns, aspects related to the application scenarios, design and implementation of security policies.
- **Access Controls:** Study covering authentication and authorization of individuals considering one or more biometric traits. This area discusses the advantages and disadvantages offered by each of the biometric characteristics that based on them, controls that provide access to legitimate users and deny service to counterfeiters, usually in designing distributed architectures jacks contemplated are designed centralized decision.

Current Projects founded by CONACYT

Unauthorized Remote Access Monitoring for Private Information

Grant: Project supported by CONACYT grant number 216747 (800,000 MXP)
Duration: 2014-2015.
Status: Currently running

Design of Cryptographic Protocols natively implemented on Android OS

Grant: Project supported by CONACYT grant number 216533 (800,000 MXP)
Duration: 2014-2015.
Status: Currently running