CLARA: Security in Latin American Academic Networks

Jornadas sobre Seguridad Informática

Buenos Aires, 1-7 Octubre, 2005

Liliana Velásquez Solha
CAIS/RNP - Brazil

Juan Carlos López Guel
UNAM-CERT – Mexico

(on behalf of CLARA – Latin American Cooperation of Advanced Networks)

Agenda

- About CLARA
- Security overview in LA&C academic networks today
- CLARA: The proposal
- CLARA Security Task Force (GT-Seg)
- Collaborative activities among LA&C CSIRTs: projects in progress
- References

Cooperación Latino Americana de Redes Avanzadas

(Latin American Cooperation of Advanced Networks)

http://www.redclara.net

CLARA backbone

- Latin American Research, Education and Development network.
- Association of NRENs (*National Research and Education Networks*).
- Interconnects 19 countries
- Academic and Research community:
  - Universities and Higher Education Schools
  - Technology Centers
  - Research Centers and Institutions
  - etc
- Miillions of Internet users!

CLARA Members

The following Latin American NRENs are members of CLARA:

- Argentina
- Brazil
- Bolivia
- Colombia
- Chile
- Costa Rica
- Cuba
- Dominican Republic
- Equador
- El Salvador
- Honduras
- Guatemala
- Mexico
- Nicaragua
- Panama
- Paraguay
- Peru
- Uruguay
- Venezuela

+ Caribbean countries *(in the near future)*

http://www.redclara.net/en/01/07.htm

Security overview in LA&C academic networks today

- Poor security awareness
- Security: expense vs. investment!
- Lack of expertise in security among Sys Admins
- Difficulties in tracking vulnerabilities and keeping the systems up-to-date
- Systems and networks not properly configured
- Absence of security policies and best practices
- Poor culture of security incidents report
- Misuse of computer resources
- etc, etc, etc.

So, what can be done? ...

- There is no a single solution!
- A multiple-level security strategy is needed

CSIRT

A CSIRT can be one of your best allies!!!

CLARA Approach

- Creation of the **CLARA Security Task Force (GT-Seg),** based on CSIRTs participation.

  → **GT-Seg was set up in April, 2004**

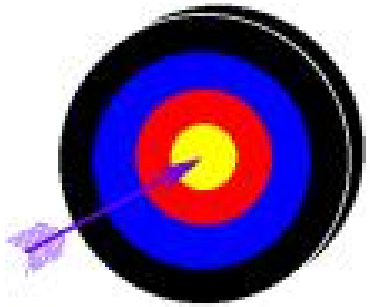
- Mission:

  "To promote the security culture in Latin American and Caribbean region"

- *Initial challenge:*

  - *To build CSIRT capabilities in each NREN and to promote collaborative actions among the ones already established.*

GT-Seg: Goals

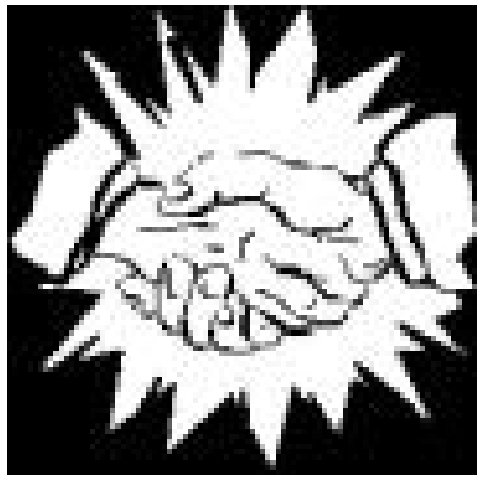


- Establish a computer security framework in each NREN.
- Promote the development of new CSIRTs in the LA&C region and train their staff in security issues.
- Provide a discussion forum to share knowledge and experiences in security area, especially in incident response.
- Facilitate the exchange and data correlation of security incidents related information.
- Promote a coordinated (and timely) response to security incidents.

GT-Seg: Goals [cont]

- Have a global view of security incidents in LA&C region.
- Establish pilot services for CSIRTs community in LA&C region
- Create and disseminate security best practices for academic environments
- Build an updated database of security point-of-contact for each NREN.
- Cooperate with other regional initiatives
  - TF-CSIRT → Europe
  - APCERT → Asia & Pacific

GT-Seg: Participation



- Primarily, open to:
  - CLARA members NRENs
  - organizations connected to them
- Other participants can be allowed to join as long as their participation contributes to achieve the CLARA goals.

→ The CLARA Technical Comission will evaluate each request and approve it (or not) on a case-by-case base.

GT-Seg: Action Plan for 2005-2006

- **Conduct a first LA&C general security situation survey**
- **Conduct a first LA&C CSIRT situation survey**

- **Promote the establishment of new CSIRTs**

  → priorizing NRENs and then the institutions connected to them.

- **Build a db of security point-of-contacts for each NREN.**
- **Continue the Security Training and Education Program (STEP)**

GT-Seg: Action Plan for 2005-2006 [cont]

- Build a security best practices digital repository
- Organize regular meetings and seminars as part of the Security Awareness Program (SAP).
- Collaborate with other CLARA Task Forces / Working Groups.
- Promote collaboratives activities among existent CSIRTs in LA&C
- Cooperate with other competent organisms.

Collaborative projects among LA&C CSIRTs

- **Forensics Analysis**

→ The Forensic Challenge (“Reto Forense”)

1o Reto Forense: Organized by REDIRIS (Spain)

http://www.rediris.es/cert/ped/reto [December, 2004]

2o Reto Forense: Co-organized by REDIRIS (Spain) and UNAM-CERT (Mexico)

http://www.seguridad.unam.mx/eventos/reto [May, 2005]

(*) CAIS/RNP (Brazil) staff members were invited to participate as judges at both events.

Collaborative projects among LA&C CSIRTs [cont]

- **Security Training and Education Program (STEP-I and STEP-II)**

LEVEL I: NRENs **LEVEL II**: Universities and Institutions connected to them

→ 1st "FIRST/TRANSITS" Course – Training of Network Security Incident Team Staff

During the 1st CLARA Technical Meeting – November 25-26, 2004 – Rio de Janeiro, Brazil

Collaboration: CAIS/RNP (Brazil), UNAM-CERT (Mexico)

Audience: LEVEL I - Management and Technical staff from NRENs of Latin America countries

→ 2nd "FIRST/TRANSITS" Course – Training of Network Security Incident Team Staff

During the "Congreso de Seguridad en Cómputo 2005" – May, 2005 – Mexico City, Mexico

Collaboration: CAIS/RNP (Brazil), UNAM-CERT (Mexico),), IRIS-CERT (REDIRIS, Spain)

Audience: LEVEL II - Management and Technical representatives of the Mexican universities.

Collaborative projects among LA&C CSIRTs

- **Meetings and Workshops**

→ 1st “CLARA Security Task Force” Meeting

During the 2nd CLARA Technical Meeting – April 25-27, 2005

Collaboration: UNAM-CERT (Mexico), CAIS/RNP (Brazil)

Participants: Management and Technical representatives from NRENs of the LA&C countries

- **Collaborative projects among LA&C CSIRTs**
  - **Early Warning Systems**

    → "CAIS.Stormcenter" Project

    Collaboration: CAIS/RNP (Brazil)

    [A CAIS/RNP initiative today but it shall be expanded, collecting data from different sensors – honeypots, honeynets, darknet, etc - and generating statistics for Latin America region].

  - **Anti-Spam and Anti-Virus**

    → HERMES Project: **S**ecurity in **A**cademic **M**ail **S**ervers

    Collaboration: REUNA (Chile), RETINA (Argentina), CAIS/RNP (Brazil), REDIRIS (Spain)

    →RESCATA/NAS Project: **N**etwork of **A**ntivirus **S**ensors

    Collaboration: REDIRIS (Spain) and others [Ref http://alerta-antivirus.red.es]

    [A REDIRIS initiative today but it is being expanded, collecting data from distributed antivirus sensors and generating statistics for Latin America region]. CAIS/RNP from Brazil has already joined it.

Contact Information

CLARA - Cooperación Latino Americana de Redes Avanzadas

http://www.redclara.net

CAIS/RNP – Brazilian Academic and Research Network CSIRT
http://www.rnp.br/cais

UNAM.CERT – National Autonomous University of Mexico
http://www.unam-cert.unam.mx