CCN-CERT
The Spanish Government CERT

National Cryptologic Center (CCN)

Viena, September 2008
FORUM: TF-CSIRT Meeting

SESSION: CCN-CERT. Government CERT.

OBJECTIVE: Scope and goals of CCN-CERT to deal with Incidents in the Spanish Administration.

SPEAKER:
- National Cryptologic Center

DATE: 26th of September, 2008
• Legal Framework
• CCN-CERT:
  - Mission and Constituency
  - Services & Website
• CCN-STIC Series and STIC Courses
• Incident Response
• Critical Infrastructures
• Further Steps
• Conclusions
CCN acts under the following legal framework:

**Law 11/2002, 6th of May**, regulates the National Intelligence Center (CNI), which includes the National Cryptology Center (CCN).

**Royal Decree 421/2004, 12th of March**, regulates and defines the scope and functions of CCN.
Emerging Risks

Art. 4 a) Intelligence

Art. 4 b) Counterintelligence

Art. 4 c) Relations

Art. 4 d) SIGINT

Art. 4 e) INFOSEC

Art. 4 f) Protect Classified Information

Art. 4 g) Own Security

NATIONAL EU / NATO / INTERNATIONAL AGREEMENTS

UNCLASSIFIED
- **Prepare and disseminate** norms, instructions, guides and recommendations to ensure the CIS Security of Public Authorities.
- **Train** civil servants specialized in CIS Security.
- Set the **certification body** of the Spanish Evaluation and Certification Scheme of application to products and systems under its responsability.
- **Assess and accredit** the capability of crypto products and CIS systems (that include crypto media) to deal with information in a secure way.
- Coordinate the promotion, development, acquisition, operation and use of **security technologies** of systems above-mentioned.
- Ensure for the compliance with the rules concerning with **classified information** under its competence scope (CIS Systems)
- Establish the necessary **relations** and sign the pertinent agreements with similar organizations from other countries.
- To carry out the above-mentioned functions, the necessary Coordination with the National Commissions to whom laws give the responsibilities in the area of Information and Communication Technology Systems.
CERTs in Europe

- Germany
  - CERT-BUND
  - CERT-DE/CERTCOM
  - CERT-VM
  - ComCERT
  - DFN-CERT
  - ESACERT
  - FSC-CERT
  - GNS-CERT
  - Micro-BIT
  - PRE-CERT
  - RUS-CERT
  - MIS-CERT
  - SAP-CERT
  - SECURIS-CERT
  - Siemens-CERT
  - T-COM-CERT
  - Telekom-CERT

- Iceland
  - Rennet-CERT

- Norway
  - NRCCERT
  - UIO-CERT
  - UniNet-CERT

- Denmark
  - CERT-DK
  - DK-CERT
  - KMD-IAC

- Spain
  - CC-SEC
  - CERN-CERT
  - ESPCERT
  - ES-CERT
  - SWITCH-CERT
  - SICE-CERT

- Sweden
  - SITIC
  - SiNet-CERT
  - TS-CERT
  - Fiken CERT
  - Funet CERT
  - Nokia NRT

- Finland
  - CERT-FI
  - Ericsson PSIRT

- Estonia
  - CERT-EE
  - SKY-CERT

- Latvia
  - DODKV
  - CERT-NL

- Lithuania
  - CERT-LIT

- Russia
  - RU-CERT
  - WebPlus ISP

- Poland
  - CERT-GOV.PL
  - CERT-POLSKA
  - PIONIER-CERT
  - TF CERT

- Czech Republic
  - CESNET-CERTS

- Hungary
  - CERT-Hungary
  - MUNCERT
  - NIIF-CERT

- Slovakia
  - SI-CERT

- Croatia
  - CARnet CERT

- Turkey
  - TR-CERT
  - ULA-CERT

- Cyprus
  - CYPRUS

- United Kingdom
  - BP-SIGAC
  - BTCERTCC
  - Cisco PSIRT
  - CITIGROUP (UK)
  - CPNI
  - DAN-CERT
  - DCSIRT
  - E-CERT
  - ECSC/RT
  - GovCertUK
  - JANET-CERT
  - ML CERT (UK)
  - MODCERT
  - OxCERT
  - Q-CERT
  - RBB-CERT
  - RM CSIRT

- The Netherlands
  - AAB CSIRT
  - AMC-CERT
  - CERT-DC
  - CERT-KUN
  - CERT-RUG
  - CERT-LJU
  - GOVCERT.NL
  - KPN-CERT
  - ING Global CERT
  - SURFnet-CERT
  - Uva-CERT

- Belgium
  - BILJNET CERT
  - INORCC CC

- France
  - CERTA
  - Cert-IET
  - CERT-LEXIS
  - CERT-Renater

- Portugal
  - CERT-IP
  - CEBERT-UFP

- Switzerland
  - RESTENA-CERT

- Italy
  - CERT-DIVINA
  - CERT-ENEL
  - CERT-IT
  - EAPG
  - GARR-CERT
  - GovCERT.IT
  - INETCO-CERT

- Malta
  - mtcCERT

- Austria
  - AOSM-CERT
  - CERT.AT

- Greece
  - AUTH-CERT
  - GRNET-CERT

IRT - teams using their RIFE IRTPs – select for networks they serve

CERTs IN SPAIN

- Iris-CERT
- esCERT-UPC
  - Support to its constituency - Univer. Politécnica de Cataluña
- INTECO-CERT
  - CERT to SMEs and Citizens
- CSIRT-CV
  - Regional Government of Valencia
- eLaCaixa-CSIRT
  - Support to Bank La Caixa
- Other Regional Government CERTs Forseen:
  - Andalusia / Catalonia / Basque Country
Main Goal

- To contribute to the **improvement** of the security level in the Spanish Public Civil Service Information Systems.

Our Mission:

- To be the **center of alert and coordination** of security incidents, helping public authorities to respond to threats that affect their information systems in a fast and efficient manner.
• **Our Constituency:**
  - **Spanish Public Civil Service:**
    - Central, Regional and Local Governments.

• **Our Authority:**
  - **Classified Systems:**
    - Royal Decree 421/2004 gives CCN the authority to take the necessary actions to solve incidents on classified systems.
  - **Non-Classified Systems:**
    - Shared with our constituency, agreeing with them the necessary decisions and actions to fulfill our mission.
SCOPE OF CCN-CERT

Public Administration Systems

Citizens and SMEs

Telecommunications Companies and Service Providers

Security and Defence Classified Systems

Critical Infrastructure Strategic Sectors
WEB PORTAL – Main Features:

- Public Services:
  - Own Vulnerabilities Bulletins
  - Own and Third-party Statistics and Measures
  - Press Releases/ Publications / Tools
  - PILAR Risk Analysis Tool/ Glossary (CCN-STIC 401)

- Restricted Services for the constituency:
  - CCN-STIC Series / INFOSEC Courses
  - Incident Notification Interface
  - Alerts and Vulnerabilities
  - CCN-CERT Weekly/Monthly Reports

- Non-Web Publication Media:
  - News disclosure through e-mailing lists
  - Statistics and Other Contents by RSS threads
CCN-STIC-600 Guides for Other Environments

- CCN-STIC-601 Hardening (HP-UX 10.20)
- CCN-STIC-602 Hardening (HP-UX 11i)
- CCN-STIC-610 Hardening (Red Hat Linux)
- CCN-STIC-611 Hardening (SuSE Linux)
- CCN-STIC-612 Hardening (Debian)
- CCN-STIC-614 Hardening (RedHat Enterprise AS 4 y Fedora 5)
- CCN-STIC-621 Hardening (Sun Solaris 8.0)
- CCN-STIC-622 Hardening (Sun Solaris 9.0/Oracle 8.1.7)
- CCN-STIC-623 Hardening (Sun Solaris 9.0/Oracle 9i)
- CCN-STIC-624 Hardening (Sun Solaris 10/Oracle 9.2)
- CCN-STIC-625 Hardening (Sun Solaris 10/Oracle 10g)
- CCN-STIC-631 Hardening (Oracle 8.1.7/Solaris)
- CCN-STIC-641 Hardening (Routers CISCO)
- CCN-STIC-641 Template for Hardening Routers CISCO
- CCN-STIC-642 Hardening (Switches Enterasys)
- CCN-STIC-642 Template for Hardening Switches Enterasys
- CCN-STIC-671 Hardening (Web Server Apache)
- CCN-STIC-681 Hardening Mail Server (Postfix)

CCN-STIC-900 Technical Reports

- CCN-STIC-903 Hardening PDA (HP IPAQ 6340)
- CCN-STIC-951 Recommendations for using Ethereal Tool
- CCN-STIC-952 Recommendations for using Nessus Tool
- CCN-STIC-954 Advanced NMAP guide
New CCN-STIC Series

• **General Guides:**
  - CCN-STIC-433: Malcode Detection Tools
  - CCN-STIC-439: Anti-SPAM Tools

• **Windows Guides:**
  - CCN-STIC-517A: Security in Windows VISTA. Domain Member.

• **Other-Environment Guides:**
  - CCN-STIC-682: Hardening SENDMAIL

UNCLASSIFIED
Compromiso de root en Sun Java Runtime Environment

**Vulnerability classification**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Alto</td>
</tr>
<tr>
<td>Confidence level</td>
<td>Oficial</td>
</tr>
<tr>
<td>Impact</td>
<td>Compromiso Ficció</td>
</tr>
<tr>
<td>Difficulty</td>
<td>Experto</td>
</tr>
<tr>
<td>Required attacker level</td>
<td>Acceso remoto sin cuenta a un servicio estandar</td>
</tr>
</tbody>
</table>

**System information**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected platform</td>
<td>Commerical Software</td>
</tr>
<tr>
<td>Affected software</td>
<td>Sun JDK 5.0 &lt;= Update 13</td>
</tr>
<tr>
<td></td>
<td>Sun JRE 6.0 &lt;= Update 1</td>
</tr>
</tbody>
</table>

**Description**

Se han descubierto múltiples vulnerabilidades en Java Runtime Environment de Sun JDK y JRE 6 Update 1 y anteriores, y 5.0 Update 13 y anteriores. Las vulnerabilidades residen en un error no especificado relacionado con un aumento de los privilegios asignados en una aplicación o applet.

Un atacante remoto podría leer y escribir ficheros locales o ejecutar aplicaciones locales mediante una aplicación o applet Java.

**Solution**

Actualización de software

- SunJDK 1.2.61
- Windows / Linux / Solaris
- Sun JDK 6 Update 2
- Sun JRE 5.0 Update 14
- Solaris
- Java SE 5 Update 2 / patch 125135-02
- Java SE 6 Update 2 (64bit) / patch 125137-02
- Java SE 5,66 Update 2 / patch 125136-02
- Java SE 5,66 Update 2 (64bit) / patch 125139-02
- J2SE 5.0 Update 14 / patch 116665-15
- J2SE 5.0 Update 14 (64bit) / patch 116667-15
- J2SE 5.0 Update 14 (64bit) / patch 116669-15
Statistics Tables

Vulnerabilities per Month during 2007

- **Low Risk**
- **Medium Risk**
- **High Risk**
- **Very High Risk**
- **Total**

<table>
<thead>
<tr>
<th>Month</th>
<th>Low Risk</th>
<th>Medium Risk</th>
<th>High Risk</th>
<th>Very High Risk</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan</td>
<td>26</td>
<td>29</td>
<td>18</td>
<td>0</td>
<td>63</td>
</tr>
<tr>
<td>Feb</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mar</td>
<td>11</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>27</td>
</tr>
<tr>
<td>Apr</td>
<td>18</td>
<td>15</td>
<td>10</td>
<td>0</td>
<td>43</td>
</tr>
<tr>
<td>May</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>0</td>
<td>57</td>
</tr>
<tr>
<td>Jun</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jul</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Aug</td>
<td>14</td>
<td>18</td>
<td>0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>Sep</td>
<td>22</td>
<td>17</td>
<td>0</td>
<td>0</td>
<td>44</td>
</tr>
<tr>
<td>Oct</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nov</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dec</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Number of Vulnerabilities

Month

Total vulnerabilities exhibit a fluctuating pattern throughout the year, peaking in some months and dipping in others.
Environment for the Analysis of Risks

EAR/PILAR

- PROCEDIMIENTO INFORMATICO Y LOGICO DE ANALISIS DE RIESGOS
  (Computer and Logic Procedure for Analysis of Risks)
  - CCN Project → Developer A.L.H. J. Mañas
  - Validation Committee: CCN + MAP + FNMT + CCAA…
    - PILAR: exclusive use to public administration / business tool

- PILAR OBJECTIVE:
  - EASY TO USE. Help to unskilled users. Suggestions.
  - FLEXIBILITY. Adaptable to policies:
    - NATIONAL / ENTERPRISES
    - NATO / EU
  - PRIORITIZATION OF SAFEGUARDS.
  - Multilanguage
    - Spanish / English / French / Italian

UNCLASSIFIED
### Informe de Capacitación

**Estructura del Programa de Capacitación para Agentes de Servicio Civil Especializadas en Seguridad de Comunicación e Informática (STIC)**

- **Periodo:** 2006-2007
- **Número de Departamentos de Servicio Civil (Central, Regional y Local):** 87
- **Número de Agentes de Servicio Civil:** 700
- **Número de Horas de Enseñanza:** 1300
- **Número de Cursos:** 18
  - Informes y Concienciación: 2
  - Cursos Básicos de Seguridad: 4
  - Cursos Específicos de Gestión de Seguridad: 3
  - Cursos de Especialización en Seguridad: 9

### Calendario de Capacitación

#### CURSOS STIC 2008

| MESES / DIAS  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ENERO         |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| FEBRERO       |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| MARZO         |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| ABRIL         | IV CURSO STIC |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | IV CURSO STIC |
| MAYO          |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | IV CURSO ACRÉDITACIÓN LINUX |
| JUNIO         | III CURSO BASE DATOS | III CURSO INFRAEST. RED | I CURSO C. CRITERIA |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| JULIO         |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |
| AGOSTO        |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |
| SEPTIEMBRE    | III REDES INALÁMBRICAS | IV CORTAFUEGOS | IV CURSO STIC IDS |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| OCTUBRE       | II INSF. SEG. | I BUSQUEDA EV. |   | V CURSO GESTIÓN STIC |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| NOVIEMBRE     |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   | XX CURSO DE ESPECIALIDADES CRIPTOLÓGICAS (CEC) |
| DICIEMBRE     |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |

#### Clases de Capacidad

- **Cursos Básicos de Seguridad**: 2
- **Cursos Específicos de Gestión de Seguridad**: 4
- **Cursos de Especialización en Seguridad**: 3
- **Cursos Específicos de Gestion de Seguridad**: 4

*Fase de Correspondencia*
STIC Courses 2008

• **Informative and Awareness Security Courses**
  - STIC Workshop
  - STIC Course

• **Basic Security Courses**
  - STIC Basic Course - Windows
  - STIC Basic Course - Linux
  - STIC Basic Course - Network Infrastructure
  - STIC Basic Course – Database

• **Specific Management Courses**
  - STIC Management Course
  - Cryptologic Specialities Course
  - Common Criteria Course

UNCLASSIFIED
STIC Courses 2008 (II)

- Security Specialized Courses
  - Accreditation STIC Course - Windows
  - Accreditation STIC Course - Unix
  - Accreditation STIC Course - Linux
  - STIC Course - Firewalls
  - STIC Course - Intrusion Detection
  - STIC Course - Wireless Networks
  - STIC Course - Security Tools
  - STIC Course - Security Inspection
  - STIC Course - Forensic Analysis and Integrity Control
Por favor, cumplimente el siguiente formulario para informar del incidente.

**Fuente de la información:**

<table>
<thead>
<tr>
<th>Tipo de fuente de incidencia</th>
<th>Descripción de la fuente</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abierto (news, mailing lists, search engines, the Web, ...)</td>
<td>[Ingrese descripción]</td>
</tr>
<tr>
<td>Procedente de terceros (persona/equipo humano que comparte información)</td>
<td>[Ingrese descripción]</td>
</tr>
</tbody>
</table>

**Equpos afectados**

<table>
<thead>
<tr>
<th>Nombre host</th>
<th>IP del host</th>
<th>Zona Horaria</th>
<th>Función del host</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Ingrese nombre]</td>
<td>[Ingrese IP]</td>
<td>[Ingrese zona horaria]</td>
<td>[Ingrese función]</td>
</tr>
</tbody>
</table>

**Fuente del ataque**

<table>
<thead>
<tr>
<th>Nombre host</th>
<th>IP del host</th>
<th>Zona Horaria</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Ingrese nombre]</td>
<td>[Ingrese IP]</td>
<td>[Ingrese zona horaria]</td>
</tr>
</tbody>
</table>
**INCIDENT CATEGORIES:**

- **Non Classified Incidents**
  - National Level:
    - E-Mail & PGP/GPG Keys
    - Incident Response Guide & Form
  - International Level:
    - TI / TF-CSIRT / FIRST / ENISA
  - Trouble-Ticket & Tracking Incidents
    - CCN-CERT Incident Handling Policy

- **Classified Incidents**
  - National Level:
    - CNI-Internal Policies and Procedures
    - According to National/EU/NATO Policies
  - International Level:
    - NATO Poc → NCIRC…up to NATO SECRET WAN Incidents
    - MERIDIAN PoC → CIS Systems (Critical Infrastructure)
• OTHER CERTs and CSIRTs FORUM

• WHAT TO EXPECT FROM A CERT

• INCIDENT RESPONSE CHECK LISTS:
  - GENERAL CASE
  - INTRUSION ATTEMPT
  - MALCODE ATTACK
  - PHISHING
  - DDOS ATTACK

• CONTACTING LAW ENFORCEMENT AGENCIES
MALCODE ANALYSIS:

Changes in the system (Files, Registry entries, Processes…)
Capabilities (Connections, Hooks, Information capture: keyboard / e-mails / web pages / credentials…)

Tools:
Gmer, Regshot, Wireshark, Procesp, Filemon, RkDetect…

FORENSIC ANALYSIS:

Information recovery: Deleted files
Incident Analysis: Logs recovery,.exe files - Reverse engineering.

Tools:
EnCase, WinHex, Sleuth Kit…
• **International Level**
  - FIRST: Full Member
  - NATO Cyber Defense Workshops
  - National CSIRTs Meetings (CERT/CC)

• **European Level**
  - TERENA TF-CSIRT - TI Accredited Member
  - ENISA National CERTs Workshops

• **National Level**
  - Spanish CERTs Group (CSIRT.es)
  - Forum ABUSES: Spanish ISP Abuse Teams (RedIRIS)

• **Other Relations**
  - AntiPhishing WG
  - Microsoft (SCP Program)
  - SANS / Security Focus / HISPASEC / ...
Critical Information Infrastructure Protection

- Supporting CNPIC
  (National Center for the Protection of Critical Infrastructures)
  - Coordination at the national level
  - Knowledge about cyber incidents
  - Support law enforcement
  - Support the risk assessment task

- CIIP PoC at:
  - MERIDIAN Directory (CIS Systems)
  - NATO’s Cyber Defence Program
  - Government Level

UNCLASSIFIED
Further Steps

• Sensors Deployment (Early Warning System):
  - Roadmap coordinated with Civil Service Ministry
  - Access to the INTERNET / INTRANET of Central Government
  - Benefits:
    ♦ Own statistics and measures / Attack Detections
• Government Web Portal Audits
• MultiAntivirus Project…
• … Automatic Web Malware Analysis
Conclusions

• From CCN knowledge and expertise on CIS Security …
  - ... Improve security on CIS Government Systems
  - ... Government Capability on Incident Response
    ♦ CCN-CERT

• Handling Computer Incidents by:
  - Security-Related Information Services
  - Research, Training and Awareness
  - Support on Incident Response

• Relationships:
  - Public Civil Service Organizations
  - Other CERTs
  - ISPs, Critical Infrastructure Stakeholders
Thank you!!

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es

- **Websites:**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es