Module 1

CERT/CC Overviews

The Beginning of the CERT/CC

- Worm attack
- Post mortem
- CERT/CC created

<table>
<thead>
<tr>
<th>Sun</th>
<th>Mon</th>
<th>Tues</th>
<th>Wed</th>
<th>Thur</th>
<th>Fri</th>
<th>Sa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
</tr>
</tbody>
</table>

November 1988
What is the CERT/CC? (1)

- responsibilities include providing
  - Internet security information for
    › system and network administrators
    › technology managers
    › policy makers
  - guidance and coordination for major Internet
    security events
    › Melissa virus
    › Y2K
  - leadership in the response team community
    › CSIRT formation and development assistance

What is the CERT/CC? (2)

- the CERT/CC focuses specifically on technical
  issues relating to Internet security

- the CERT/CC does not focus on
  - who the intruders are
  - where intruders are located (physically)
  - motivations of intruders
  - monitoring/surveillance of intruders
    › other than understanding the technical implications
      of what the intruder community is doing
CERT/CC Teams

CERT Coordination Center

Vulnerability Handling  ↔  Artifact Analysis

- analyse flaws in Internet Systems
- study intruder developed code to exploit flaws

Incident Handling

- measure exploitation of flaws, assist in remediation

CERT Incident Handling Team (1)

- receives reports related to computer security from sites connected to the Internet
  - attack attempts, probes, scans
  - successful attacks
    › compromises
    › denial-of-service
    › other
  - new types of attacks/intruder tools
  - proactively looks at Internet information sources for incident-related issues
    › mailing lists
    › web sites
CERT Incident Handling Team (2)

- provides 24-hr. emergency incident response for
  - possible life-threatening activity
  - threats or attacks on the Internet infrastructure, such as:
    › root and other DNS servers
    › routing infrastructure
    › major archive sites
    › network access points (NAPs)
  - widespread automated attacks against Internet sites
  - new types of attacks or new vulnerabilities
  - threat or attacks involving U.S. government machines

CERT Incident Handling Team (3)

- analyses reports
  - determine attack method
  - correlate with other reports
    › determine scope and magnitude
  - what can be learned from this attack
    › determine if new type of attack
    › identify a change in frequency of attack method
    › identify need for new defences or countermeasures

- provides feedback to reporting sites involved
CERT Incident Handling Team (4)

- informs the Internet community about
  - current activity
  - new types of attacks
  - detection and recovery from attacks
  - defence against attacks

- Internet community informed through
  - CERT advisories, incident notes and summaries
  - current activity page on www.cert.org
  - tech tips and other documents on CERT/CC web site

CERT Vulnerability Handling Team (1)

- receives vulnerability reports
  - direct reports
  - proactively looks at Internet information sources for incident-related issues
    - mailing lists
    - web sites
CERT Vulnerability Handling Team (2)

- verifies and analyses reports
  - is this really a vulnerability?
  - what is effect of vulnerability?
  - how many systems or types of systems are affected?
  - are exploits available or in circulation?
  - is the vulnerability actively being exploited?

CERT Vulnerability Handling Team (3)

- works with vulnerability reporters, vendors, Internet experts to
  - better understand vulnerability
  - develop countermeasures and fixes

- publicises information about vulnerabilities and countermeasures
  - CERT advisories and vulnerability notes
  - tech tips and other documents on www.cert.org
  - CERT/CC Knowledgebase Vulnerability Reports Catalog
CERT Artifact Analysis Team (1)

• focused on code written by intruders
  - viruses
  - Trojan horses
  - exploit scripts

• analyse code
  - what does it do?
  - what vulnerabilities are exploited?
  - how do you defend against it?
  - who might be victims or targets?

CERT Artifact Analysis Team (2)

• develop capability to predict trends in malicious
code development and functionality
CERT/CC Principles

• provide valued services
  - proactive as well as reactive

• ensure confidentiality and impartiality
  - we do not identify victims but can pass information anonymously and describe activity without attribution
  - unbiased source of trusted information

• coordinate with other organisations and experts
  - academic, government, corporate
  - distributed model for incident response teams (coordination and cooperation, not control)

The CERT/CC Constituency - Internet

• global distribution
  - more than 147 million host computers as of January 2002*

• diverse user demographics
  - government agencies
  - academic and research institutions
  - corporate users
  - home users

*Source: Internet Software Consortium (http://www.isc.org/)
CERT/CC Field of Vision

- U.S. DoD
  - .mil
- FedCIRC / U.S. federal government
  - .gov, .fed.us
- National
  - .com, .edu, .net, .org, .us
- International
  - .au, .br, .ca, .de, .jp, .kr, .kw, .mx, .ps, .ru, ...

CERT/CC Relationships
## Recent CERT/CC Experiences (1)

<table>
<thead>
<tr>
<th></th>
<th>1998</th>
<th>1999</th>
<th>2000</th>
<th>2001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents Handled</td>
<td>4,942</td>
<td>9,859</td>
<td>21,756</td>
<td>52,658</td>
</tr>
<tr>
<td>Vulnerabilities reported</td>
<td>262</td>
<td>417</td>
<td>1090</td>
<td>2437</td>
</tr>
<tr>
<td>Email msgs processed</td>
<td>31,933</td>
<td>34,612</td>
<td>56,365</td>
<td>118,907</td>
</tr>
<tr>
<td>CERT Advisories, Vendor Bulletins, and Vul Notes</td>
<td>34</td>
<td>20</td>
<td>38</td>
<td>363</td>
</tr>
<tr>
<td>CERT Summaries and Incident Notes</td>
<td>15</td>
<td>13</td>
<td>14</td>
<td>19</td>
</tr>
</tbody>
</table>

Incidents Handled: 1988 - 2001

![Incidents Handled Chart](chart.png)

Vulnerabilities Reported: 1995 - 2001

FedCIRC

- a collaborative partnership of computer security incident response, security and law enforcement professionals
- provides both proactive and reactive security services to the U.S. federal government
- handles computer security incidents
- CERT/CC provides incident response services for FedCIRC under contract from GSA

See: www.fedcirc.gov
2000-2001 PGP Key - CERT/CC

Key ID: 0xD02361C9
Key Type: RSA
Expires: 2002/10/01
Key Size: 1024
Fingerprint: 8F E3 1F 95 94 BE FD E7
              9B EE 92 06 D7 35 AC F5

UserID: CERT Coordination Center
        <cert@cert.org>

The new key is an RSA key, and it is constructed so as to provide maximum interoperability with as many versions of PGP as possible as well as with GPG.

2000-2001 PGP Key - FedCIRC

Key ID: 0xE06B1467
Key Type: RSA
Expires: 2002/04/11
Key Size: 2048
Fingerprint: FE 54 54 2D 3F AE B8 BB
              71 CA 5D 61 54 D1 91 B7

UserID: Federal Computer Incident Response Center
        <fedcsrc@fedcsrc.gov>

The new key is an RSA key, and it is constructed so as to provide maximum interoperability with as many versions of PGP as possible as well as with GPG.
This primary author and maintainer of this CERT/CC presentation is:

Jeffrey J. Carpenter

CERT® Contact Information
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA

Hotline: +1 412 268 7090 CERT personnel answer 8:00 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax: +1 412 268 6989
Web: http://www.cert.org/
Email: cert@cert.org