CERT/CC Overview
presented by Brian B. King
March 6, 2002

CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

The CERT Coordination Center is part of the Software Engineering Institute. The Software Engineering Institute is sponsored by the U.S. Department of Defense.
© 2002 by Carnegie Mellon University
some images copyright www.arttoday.com
Today’s agenda

- The CERT/CC
  - Incident Handling
  - Vulnerability Handling
  - Artifact Analysis

- Principles / Constituency

- Experiences / Observations

- Questions?
  Either raise your hand or wait until the end – I’m flexible.
## The Beginning of the CERT/CC

<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**

- **CERT/CC created**
- **Morris Worm**
- **Post mortem**
- **Worm attack**
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 related 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
NSS Program Strategies

- CERT Coordination Center
- Survivable Network Management
- Survivable Network Technology
- Technology evaluation
- Research results
- Repaired systems
- Protected systems
- Improved systems
CERT/CC Teams

CERT Coordination Center

Vulnerability Handling

- analyse flaws in Internet Systems

Artifact Analysis

- 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
• 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)

• analyzes 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 analyzes 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

• publicizes 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

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

• 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 organizations 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 109 million host computers
    (as of January 2001*)

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

*Source: Internet Software Consortium (http://www.isc.org/)
## Recent CERT/CC Experiences

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents Handled</td>
<td>3,285</td>
<td>4,942</td>
<td>9,859</td>
<td>21,756</td>
<td>52,658</td>
</tr>
<tr>
<td>Vulnerabilities reported</td>
<td>196</td>
<td>262</td>
<td>417</td>
<td>1090</td>
<td>2437</td>
</tr>
<tr>
<td>Email msgs processed</td>
<td>38,406</td>
<td>31,933</td>
<td>34,612</td>
<td>56,365</td>
<td>118,907</td>
</tr>
<tr>
<td>CERT Advisories</td>
<td>28</td>
<td>13</td>
<td>17</td>
<td>22</td>
<td>37</td>
</tr>
<tr>
<td>Vulnerability Notes</td>
<td>44</td>
<td>34</td>
<td>20</td>
<td>38</td>
<td>300</td>
</tr>
<tr>
<td>Incident Notes</td>
<td>6</td>
<td>15</td>
<td>13</td>
<td>14</td>
<td>15</td>
</tr>
</tbody>
</table>
Attack Sophistication vs. Required Intruder Knowledge

- **Sophistication of attacks**
- **Intruder knowledge required to execute attacks**

Dates indicate major release of tools or widespread use of a type of attack.
Intruder Technology

- Intruders use currently available technology to develop new technology.
Vulnerability Exploit Cycle (1)

- Advanced Intruders Discover Vulnerability
- Crude Exploit Tools Distributed
- Novice Intruders Use Crude Exploit Tools
- Automated Scanning/Exploit Tools Developed
- Widespread Use of Automated Scanning/Exploit Tools
- Intruders Begin Using New Types of Exploits

Advisory Typically Released
The exploitation cycles of various vulnerabilities will overlap.
For some vulnerabilities, there may be a resurgence in its exploitation.
Direction of Internet Security (1)

- What the Internet community is facing in terms of Internet security in the next few years can be summed up in the following statements:
  - the expertise of intruders is increasing
  - the sophistication of attacks and intruder tools/toolkits is increasing
  - the effectiveness of intruders is increasing (*knowledge is being passed to less knowledgeable intruders thus making them effective*)
Direction of Internet Security (2)

- the number of intrusions is increasing
- the number of companies and users of the Internet is increasing
- the complexity of protocols and applications run on clients and servers attached to the Internet is increasing
- the complexity of the Internet as a network is increasing
Direction of Internet Security (3)

• the information infrastructure has many fundamental security design problems that cannot be quickly addressed

• the number of people with security knowledge and expertise is increasing, but at a significantly smaller rate than the increase in the number of Internet users

• the number of security tools available is increasing, but not necessarily as fast as the complexity of software, systems and networks
Direction of Internet Security (4)

• the number of incident response teams is increasing, but the ratio of incident response personnel to Internet users is decreasing

• the vendor product development and testing cycle is decreasing

• vendors continue to produce software with vulnerabilities, including types of vulnerabilities where prevention is well-understood (such as buffer overflows)
CERT Hotline calls at 11:52 on Friday night...
“I can’t take the machine off-line to recover it.”

- to fully recover a compromised machine, it must be taken offline

- many sites do not have sufficient backup resources for mission critical systems to take them offline

- system administrators making this comment are frequent repeat customers
“I have no way to verify the integrity of my machine.”

- once a machine is compromised, the integrity of the entire machine must be verified

- most sites do not have an infrastructure that facilitates verifying the integrity
  - software
  - configuration files
  - logs

- only recourse for many sites is
  - reinstall operating system and applications
  - apply all security patches and workarounds
“How do I monitor my network?”

• many sites do not have sufficient host or network logging/monitoring

• insufficient logging makes it very difficult to determine how a compromise occurred

• without sufficient logging, intensive monitoring usually needed to determine what is going on

• many sites are not prepared to do this kind of monitoring
“What is a patch?”

• yes, system administrators have asked this question

• many system administrators who do know what a patch is, do not install all the security patches because they
  - do not know how
  - do not have the resources
  - do not maintain all of the machines
  - have users who will not let them
“How can I figure out what patches are available for my operating system?”

- most vendors distribute patches via the Internet
  - even if you do not have a support contract

- many system administrators do not know how to get patches from their vendors
“I am going to leave my systems open and try to catch the intruder.”

- have you consulted with your
  - management
  - legal counsel

- if you are not planning to involve law enforcement, to what end is effort being spent “catching the intruder?”
“When the intruder broke into my system, I exploited a vulnerability on his system and logged in to see who it was.”

- we do not recommend that sites attack back
- no matter what the intent is, it can be viewed as hostile activity by the remote site
- the remote site might be a victim as well
- it might expose the system administrator’s organisation to legal liability
“The system administrator quit and now I have to do it, in addition to my real job which is _______."

- fill in the blank with:
  - intern or graduate student
  - graphic artist
  - secretary
  - manager trainee
  - etc.

- many employees performing system administration functions are not adequately prepared or trained
“I don’t have backups for this machine.”

- when intruders compromise machines, the integrity of the software and data is in question

- many sites do not have sufficient backups to restore data that has integrity

- even with backups, integrity can still question because intruders might have been operating long before they were discovered
“But, I am not running an IMAP server on this machine...”

• Surprise! Yes, you are!

  • many services are installed by default when installing the operating system on a machine

  • system administrators might not realise that they are being installed

  • having unneeded services unknowingly installed
    - increases the likelihood of compromise
    - makes it more difficult for the system administrator to track down problems
“I don’t know where that machine is.”

• many sites do not have adequate tracking of machines attached to the network

• machines might suddenly appear (or disappear and reappear, or reappear somewhere else)
“Employees are not permitted to use modems.”

- modems provide convenient backdoors for intruders
- modems are used by employees, even against policy, because it is convenient
“No one knows our dialup number.”

- many sites are under the false impression that their unauthenticated modem connections will not be discovered

- intruders will discover them through “war dialling”
“But, I have a firewall…”

- Firewalls do not alleviate the need for host security

- Intruders might compromise some other machine, and use it as a launching point to attack other internal machines

- Firewalls generally do not protect against insider attacks
Layered Approach to Security

- Host
- Local sensor
- IDS
- Router
- Firewall
“This machine cannot talk to the Internet -- it is blocked at the router.”

- another compromised machine on the internal network might be the one attacking the machine
- an insider might be launching the attack
- a user might have cause the compromise by unknowingly running malicious code
“All of our email is filtered, so no viruses can enter.”

• how often are the filters/anti-virus software updated?

• can users read email from web-based email services, like Hotmail? can they download attachments from those services?
“No, I did not know that machine was compromised…”

• we have discovered many sites with compromised machines, based on reports from other sites

• when we contact many of these sites, they had no idea they were compromised
“Physical access is tightly controlled here.”

• many attacks are initiated by insiders who have authorised access

• some employees, such as janitors, have vast access
  - what background checks are performed on your janitors?

• who verifies the background of contractors
  - might contractors be formerly terminated employees?
The hacker is coming from Korea!

• the source address might be "a.example.kr",
  • the intruder might have altered DNS records
  • compromised a machine in Korea from another location
  • spoofed the source address

Korea

but that does not mean the intruder is in Korea.

"The hacker is coming from Korea!"
2001-2002 CERT/CC PGP Key

- **Key ID:** 0xD02361C9
- **Key Type:** RSA
- **Expires:** 10/01/2002
- **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 CERT/CC PGP key is an RSA key, and is constructed to provide maximum interoperability with as many versions of PGP as possible as well as with GPG.
CERT® Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213
USA

Hotline:  +1 412 268 7090  CERT personnel answer
8:00AM-5:00PM EST(UTC-5)/EDT(UTC-4),
and are on call for emergencies.

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