Overview of the CERT/CC and the Survivable Systems Initiative

Andrew P. Moore
apm@cert.org

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

Sponsored by the U.S. Department of Defense
Talk Overview

• CERT Coordination Center
• Survivable Systems Initiative
• Intrusion-Aware Design and Analysis

CERT Coordination Center
The Beginning of the CERT/CC

CERT/CC Mission

- Respond to security emergencies on the Internet
- Serve as a focal point for reporting security vulnerabilities and incidents
- Raise awareness of security issues
- Serve as a model to help others establish incident response teams
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)

CERT Coordination Center Teams
CERT Vulnerability Handling & Analysis

- Receives vulnerability reports
  - forms, email, phone calls
- Verifies and analyzes reports/artifacts
  - veracity, scope, magnitude, exploitation
- Works with vulnerability reporters, vendors, experts
  - understanding and countermeasures
- Publicizes information about vulnerabilities and countermeasures
  - vulnerability notes, advisories

CERT Incident Handling & Response

- Receives reports related to computer security from Internet sites
  - break-ins, service denial, probes, attempts
- Provides 24-hr. emergency incident response
- Analyses report and provides feedback to reporting sites involved
  - attack method, scope, magnitude, correlation, response
- Informs Internet community
  - incident notes, summaries, advisories
  - assist formation and development of CSIRTs
Recent CERT/CC Experiences

<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents Handled</th>
<th>Vulnerabilities reported</th>
<th>Email msgs processed</th>
<th>CERT Advisories, Vendor Bulletins, and Vul Notes</th>
<th>CERT Summaries and Incident Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>52,658</td>
<td>2,437</td>
<td>118,907</td>
<td>363</td>
<td>19</td>
</tr>
<tr>
<td>2000</td>
<td>21,756</td>
<td>1,090</td>
<td>56,365</td>
<td>69</td>
<td>14</td>
</tr>
<tr>
<td>1999</td>
<td>9,859</td>
<td>417</td>
<td>34,612</td>
<td>34</td>
<td>13</td>
</tr>
<tr>
<td>1998</td>
<td>3,285</td>
<td>262</td>
<td>31,933</td>
<td>34</td>
<td>15</td>
</tr>
<tr>
<td>1997</td>
<td>3,285</td>
<td>196</td>
<td>38,406</td>
<td>44</td>
<td>6</td>
</tr>
</tbody>
</table>

Attack Sophistication vs. Required Intruder Knowledge

Sophistication of attacks Intruder knowledge needed to execute attacks dates indicate major release of tools or widespread use of a type of attack

Sophistication of attacks Intruder knowledge needed to execute attacks dates indicate major release of tools or widespread use of a type of attack

Internet social engineering attacks

Sophistication of attacks Intruder knowledge needed to execute attacks dates indicate major release of tools or widespread use of a type of attack
Automated Incident Reporting (AIR-CERT)

- **Motivation**
  - Ability to recognise and respond faster
  - Collect better incident data
  - Provide better information on activity/trends

- **Central repository being developed**
  - CERT/CC KnowledgeBase (KB)
  - Defining incident data exchange format
  - Working with IETF working group on standards
AIR CERT Vision

Data Exchange Standards

CERT/CC KB

Survivable Systems Initiative
Internet-based System Realities

- Open, highly distributed systems
- Unknown perimeters
- No central administrative control
- No global visibility
- Unknown components (COTS, Java, etc.)
- Unknown participants
- Untrusted insiders
- Large-scale coordinated attacks
Initiative Goal

Ensure that appropriate technology, systems management practices, and supporting infrastructures are used to limit damage and to ensure continuity of critical services in the presence of attacks, accidents, and failures.

Survivability

*Definition:* The ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, accidents, and failures.

*Assumption:* No individual component of a system is immune to all attacks, accidents, and failures.

*Goal:* The mission must survive.
3 R’s of Survivability

Resistance — ability of a system to deter attacks

Recognition — ability to recognize attacks and the extent of damage

Recovery — ability to restore services in a timely manner

Survivability Methods

- Conventional security techniques (access control, encryption, authentication)
- Diversity, redundancy
- Deception
- Trust validation
- Rapid Recovery and Adaptation
- Mission-specific risk management
- Contingency (disaster) planning
- Success criterion: graceful degradation & essential services maintained
Intrusion-Aware Design (IAD)

IAD Problem Addressed

Sophisticated intruders can and do
• Share tools and knowledge to amplify capability
• Escalate attack with intensity of political conflicts
• Target people (perceptions), resources, workflows
• Hide their tracks, fly under the radar of existing IDS

Engineers not using security failure data
• Same security mistakes continually repeated
• Properties must emerge from architectural interaction
• Survivability considered too late, if at all
Objective

Develop cost-effective methods for using our understanding of known and hypothesized patterns of attack to build more survivable systems.

Definitions

intrusion scenario
• description of people, systems interacting
• characterizes malicious behavior
• causes harm to enterprise

survivability scenario
• description of people, systems interacting
• in way that resists, recognizes, recovers from attacks on enterprise
IAD Approach (abstract)

real-world failures

enterprise constraints, mission, architecture

generic knowledge

Structured, reusable
attack and survivability
information

apply to

real-world successes

Incremental, risk-driven
refinement of enterprise
survivability architecture

IAD Approach (expanded)

real-world failures

enterprise constraints, mission, architecture

generic knowledge

Intrusion Scenarios

abstraction, parameterization

Survivability Scenarios

abstraction, parameterization

Attack Patterns

instantiation, composition

Survivability Strategies

instantiation, composition

Weighted
mitigation analysis

Enterprise Survivability Architecture

threat/impact analysis
Structured Intrusion Analysis

attack → target → effect

- attacks may or may not be completely successful
- attackers execute some action on some target
- intrusions compromise enterprise survivability
- sequence of attacks that result in compromise
- only critical actions need to be included


Computer & Network Attacks

attack → target → effect

- probe
- scan
- flood
- authenticate
- bypass
- spoof
- read
- copy
- steal
- modify
- delete
- account
- process
- data
- component
- computer
- network
- internetwork
attacker (A) wants to attack target site (T)
1. Identify server site (S) trusted by target
   - not sure how Mitnick did it (web site scanning, dumpster diving, etc.)
2. Verify sufficiency of trust relationship between T and S
   - probe T using finger, showmount, rpcinfo
3. Determine means to masquerade as S
   - identify predictable TCP sequence numbers
4. Shut down S’s ability to communicate with T
   - anonymous DoS on S (SYN Flood)
5. Masquerading as S, use trust to access T’s assets
   - hijack TCP connection
6. Extend trust to A

### Intrusion Effect
A has privileged access to T’s data and function.
We have developed an attack specification vocabulary.
**Attack Trees**

Provide a means of organizing related intrusion scenarios

Decompose attacker goal
- **AND** decomposition describes time-ordered sequence of sub-goals
  - *graphical*: $G_0 \rightarrow G_1 \rightarrow G_2$
  - *textual*: Goal $G_0 \ AND \ G_1 \ AND \ G_2$

- **OR** decomposition describes alternative sub-goals
  - *graphical*: $G_0 \rightarrow G_1 \ OR \ G_2$
  - *textual*: Goal $G_0 \ OR \ G_1 \ OR \ G_2$

---

**Generating Intrusion Scenarios from Attack Trees**

\[ \langle G_3, G_5, G_6 \rangle, \langle G_4, G_5, G_6 \rangle \]

\[ \langle G_4, G_5 \rangle \langle G_6 \rangle, \langle G_2 \rangle \langle G_8, G_9 \rangle \]
ACME, Inc. Enterprise

ACME High-Level Attack Tree

Survivability Compromise: Disclosure of ACME proprietary secrets

OR 1. Physically scavenge discarded items from ACME
   OR 1. Inspect dumpsters content on-site
   2. Inspect refuse after removal from site
   2. Monitor emanations (e.g., electromagnetic, visual) from ACME machines
   AND 1. Survey physical perimeter
   2. Acquire necessary monitoring equipment
   3. Setup monitoring site
   4. Monitor emanations from site
   3. Recruit help of trusted ACME insider
      OR 1. Plant spy as trusted insider
      2. Use existing trusted insider
   4. Physically access ACME networks or machines
      OR 1. Get physical, on-site access to Intranet
      2. Get physical access to external machines
   5. Attack ACME Intranet using its connections with Internet
      OR 1. Monitor communications over Internet for leakage
      2. Get trusted process to send secrets to attacker over Internet
      3. Gain privileged access to ACME Web Server
   6. Attack ACME Intranet using its connections with PTN
      OR 1. Monitor communications over PTN for secrets
      2. Gain privileged access to machines on Intranet connected via Internet
Additional Information

CERT/CC and Survivable Systems Initiative
- General: http://www.cert.org/
- Incident/vulnerability trends
  – http://www.cert.org/present/cert-overview-trends/

Intrusion-Aware Design
- General: http://www.cert.org/sna/
- Attack pattern specification, reuse, composition:
  – http://www.cert.org/archive/pdf/01tn001.pdf
- Attack Tree analysis

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. — 8:00 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