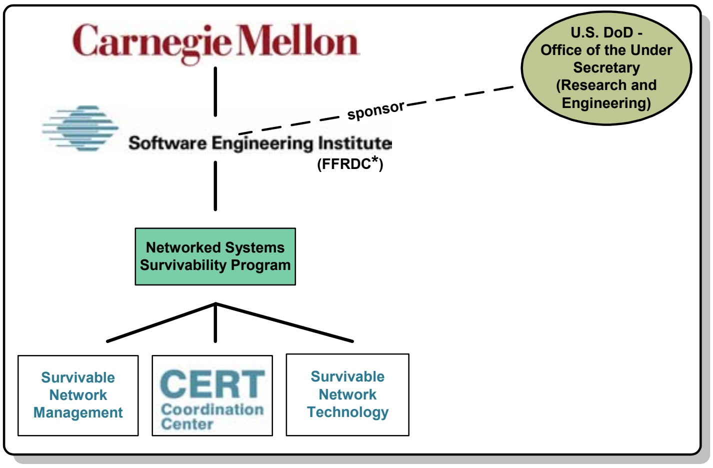
Overview of the CERT/CC and the Survivable Systems Initiative

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



Carnegie Mellon

Software Engineering Institute
(FFRDC*)

sponsor

U.S. DoD - Office of the Under Secretary (Research and Engineering)

Networked Systems Survivability Program

Survivable Network Management

CERT Coordination Center

Survivable Network Technology

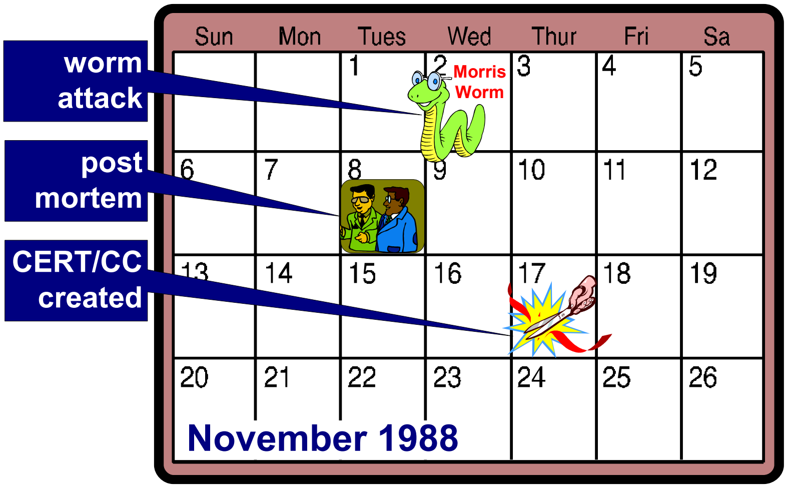
FFRDC - Federally Funded Research and Development Center

Talk Overview

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

CERT Coordination Center

The Beginning of the CERT/CC



worm attack

post mortem

CERT/CC created

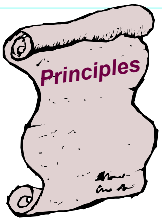
Sun	Mon	Tues	Wed	Thur	Fri	Sa
		1	2 Morris Worm	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26

November 1988

CERT/CC Mission

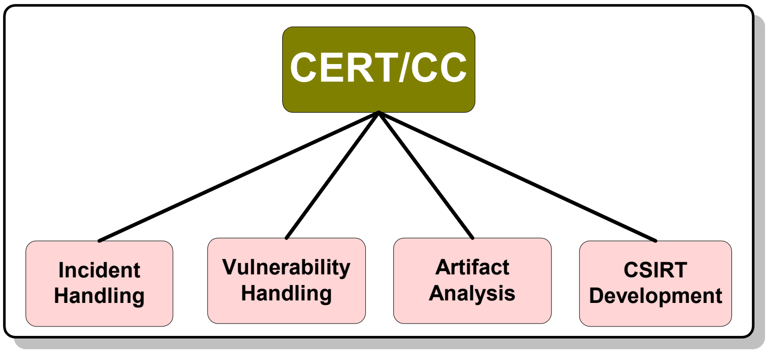
- Respond to security emergencies on the Internet
- Serve as a focal point for reporting security *vulnerabilities* and *incidents*
- Raise awareness of security issues
- Serve as a model to help others establish incident response teams

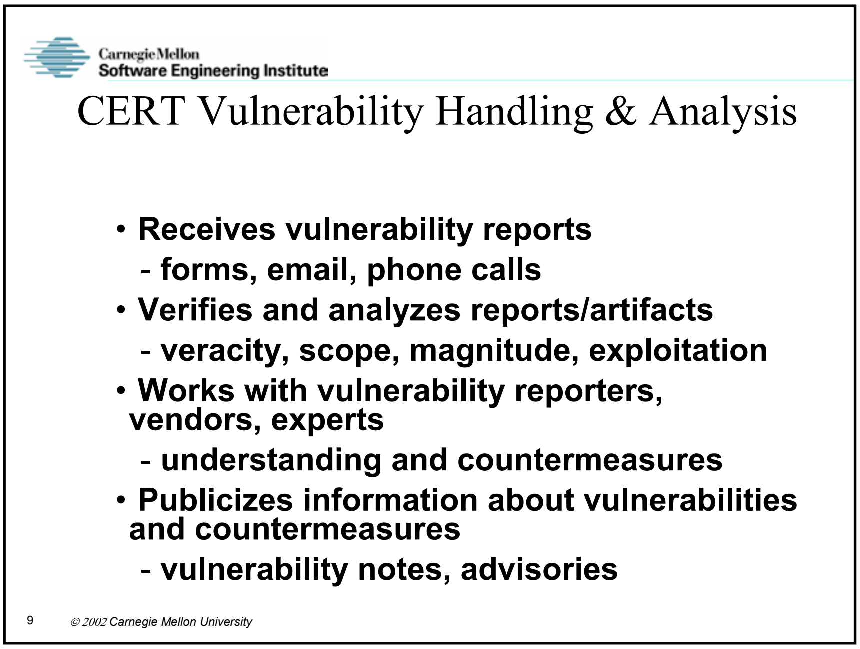
CERT/CC Principles



- 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)

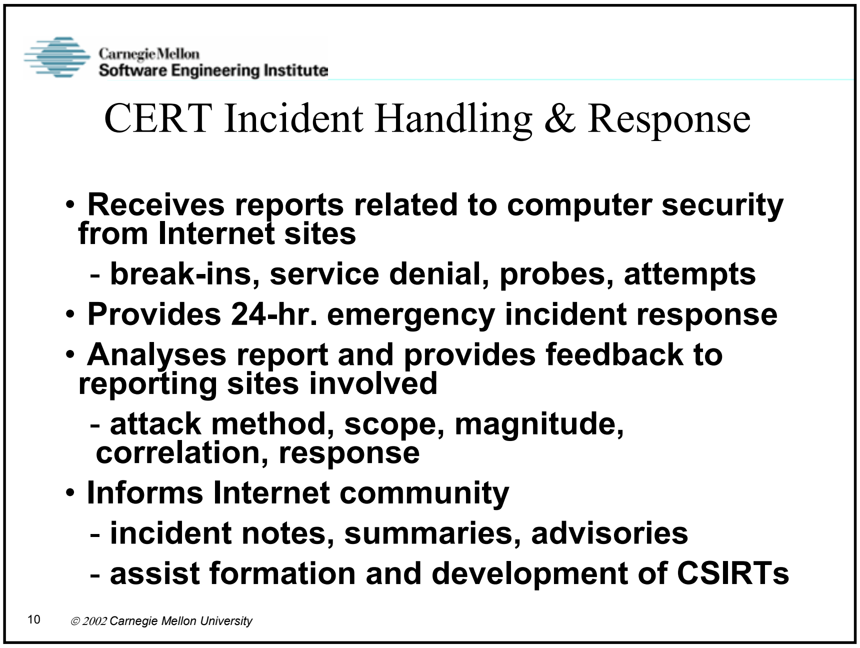
CERT Coordination Center Teams





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



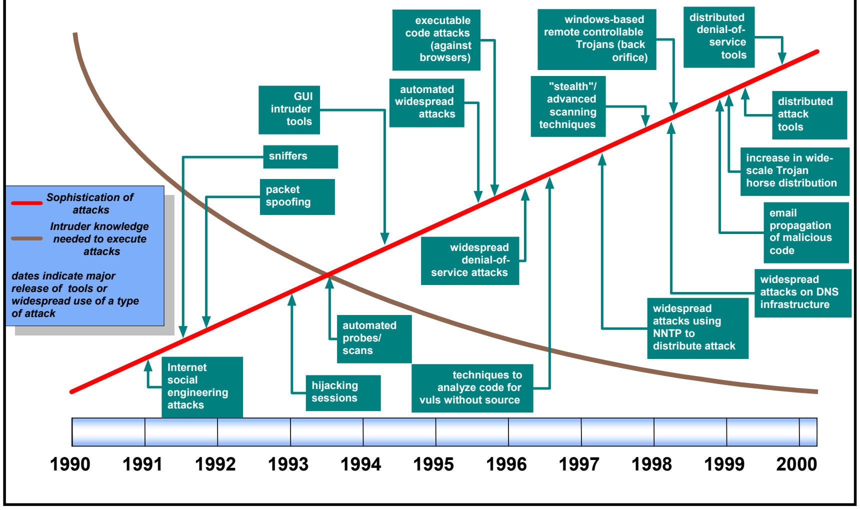
CERT Incident Handling & Response

- 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

	1997	1998	1999	2000	2001
Incidents Handled	3,285	4,942	9,859	21,756	52,658
Vulnerabilities reported	196	262	417	1,090	2,437
Email msgs processed	38,406	31,933	34,612	56,365	118,907
CERT Advisories, Vendor Bulletins, and Vul Notes	44	34	20	69	363
CERT Summaries and Incident Notes	6	15	13	14	19

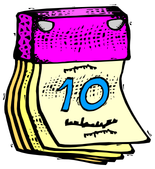
Attack Sophistication vs. Required Intruder Knowledge



Major Event Response Time Declining

March 1999

Melissa



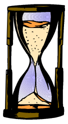
days

May 2000

Love Letter

hours

?



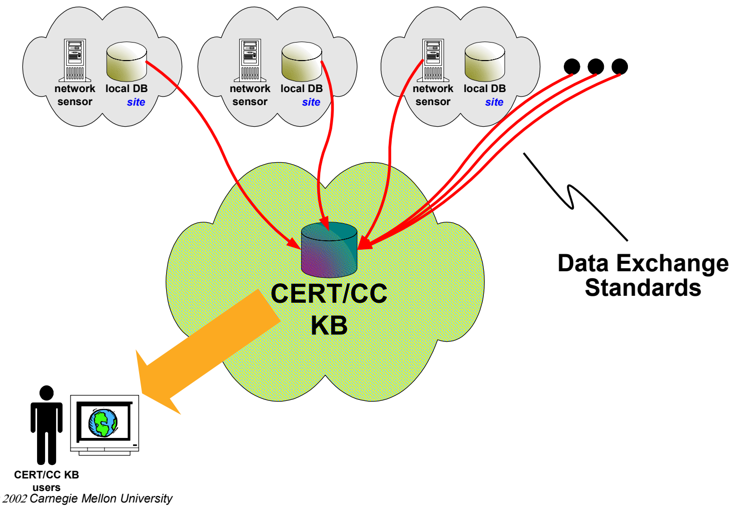
minutes

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



network sensor

local DB

site

network sensor

local DB

site

network sensor

local DB

site

CERT/CC KB

Data Exchange Standards

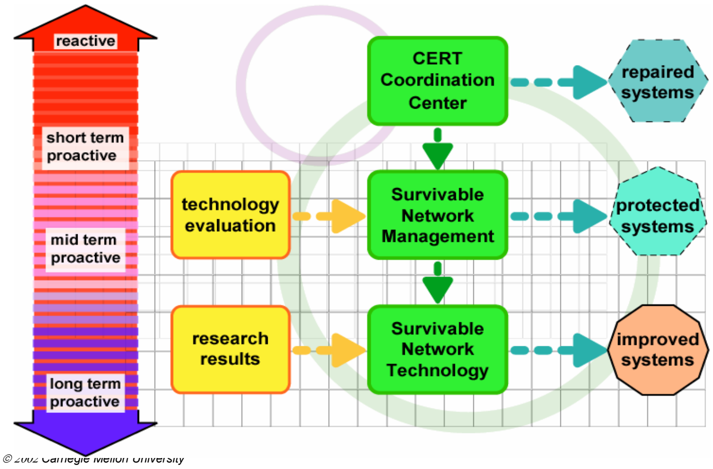
CERT/CC KB users

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

Survivable Systems Initiative



reactive

short term proactive

mid term proactive

long term proactive

technology evaluation

research results

CERT Coordination Center

Survivable Network Management

Survivable Network Technology

repaired systems

protected systems

improved systems

Initiative Goal

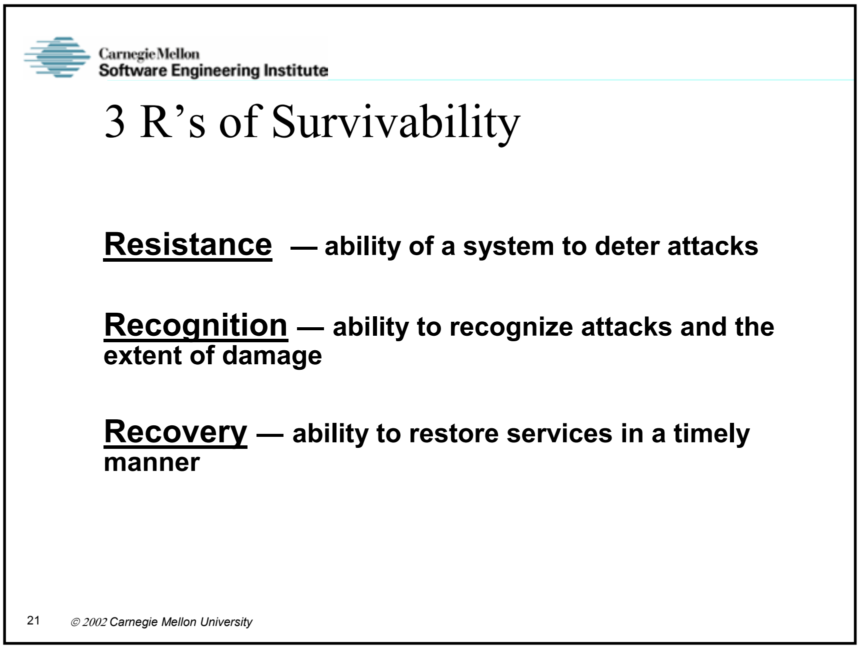
Ensure that appropriate technology, systems management practices, and supporting infrastructures are used to limit damage and to ensure continuity of critical services in the presence of attacks, accidents, and failures

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.**

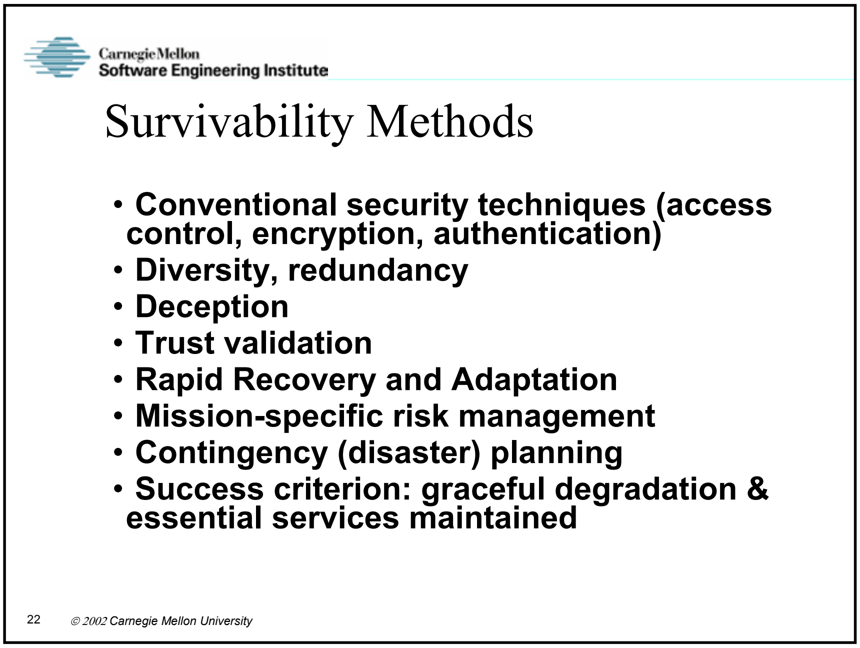


3 R’s of Survivability

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

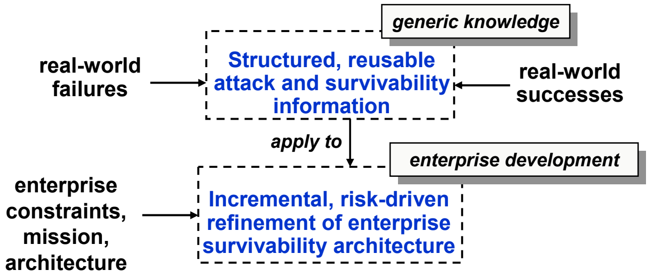
intrusion scenario

- **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)



generic knowledge

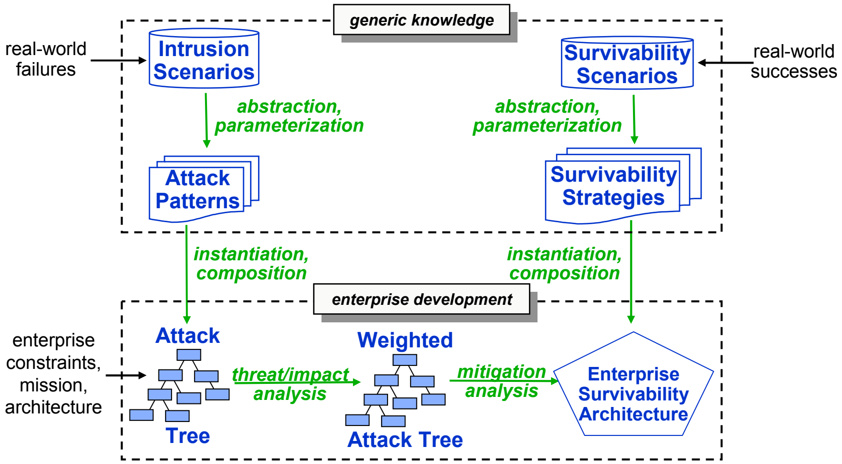
real-world failures → Structured, reusable attack and survivability information ← real-world successes

apply to

enterprise development

enterprise constraints, mission, architecture → Incremental, risk-driven refinement of enterprise survivability architecture

IAD Approach (expanded)



generic knowledge

real-world failures → Intrusion Scenarios

abstraction, parameterization

Attack Patterns

Survivability Scenarios ← real-world successes

abstraction, parameterization

Survivability Strategies

instantiation, composition

instantiation, composition

enterprise development

enterprise constraints, mission, architecture → Attack Tree

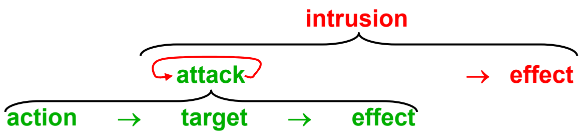
threat/impact analysis

Weighted Attack Tree

mitigation analysis

Enterprise Survivability Architecture

Structured Intrusion Analysis



intrusion

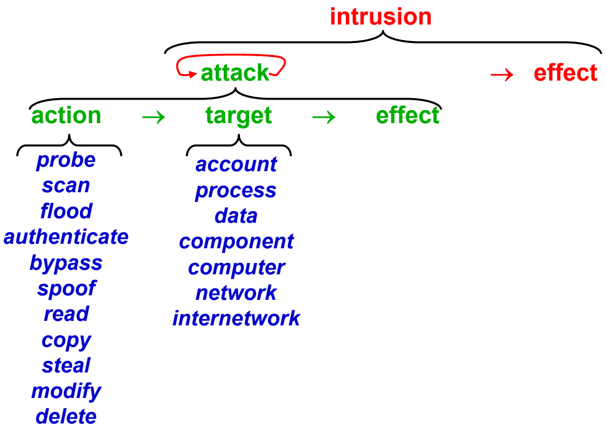
attack → effect

action → 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

* adapted from Howard, Longstaff, "A Common Language for Computer Security Incidents," Sandia Report SAND98-8667, 1998.

Computer & Network Attacks



intrusion

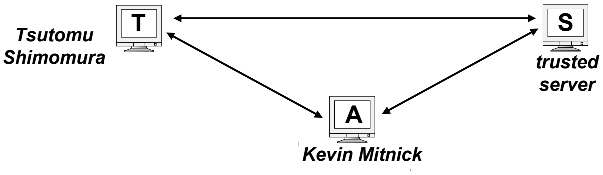
attack → effect

action → target → effect

probe
scan
flood
authenticate
bypass
spoof
read
copy
steal
modify
delete

account
process
data
component
computer
network
internetwork

Mitnick Attack



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

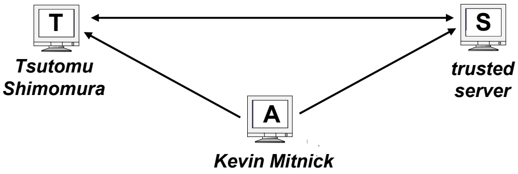
3. Determine means to masquerade as S
- identify predictable TCP sequence numbers

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

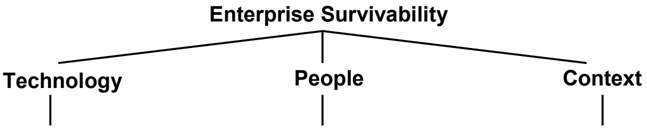
6. Extend trust to A

Parsed Mitnick Attack



Intrusion step	Attributed action	Qualified target	Attack effect
Attack 1	A *scans*	T's web site *data*	determining possible trust relationships
Attack 2	A *probes*	T's interface *component*	verifying T's trust in S
Attack 3	A *probes*	S's interface *component*	determining how to masquerade as S
Attack 4	A *floods*	S's *internetwork* access	preventing S from communicating with T
Attack 5	A *spoofs*	T's interface *component*	masquerading as S
Attack 6	A *modifies*	T's rhost *data*	extending trust to A
Intrusion effect	**A has privileged access to T's data and function.**		

Classes of Enterprise Attacks



Technology

Target computing and networking technology
- information gathering
- information corrupting
- malicious agents
- disabling

Attacks can
- exploit data/service
- corrupt data/service
- disrupt/deny service

People

Target peoples' wants, needs, capabilities, perceptions
- social-engineering
- semantic attacks
- extortion
- disabling

Attacks can
- exploit greed, fear, gullibility
- corrupt morals
- incapacitate

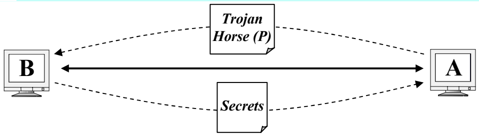
Context

Target context in which people perform their jobs
- work support
- customer demand
- enterprise stocks
- legal constraints

Attacks can
- exploit resources
- damage market, capability, assets
- deny resources

We have developed an attack specification vocabulary.

Trojan Horse Attack



Intrusion step	Attributed action	Qualified target	Attack effect	Attack type
Attack 1	A *lures*	B's *user*	into reading email that masquerades as legitimate and useful software	People
Attack 2	A *deceives*	B's *administrator*	into installing trojan horse program (P) onto B's computer	People
Attack 3	P *modifies*	B's interface *processes*	creating a backdoor for remote entry	Technology
Attack 4	P *modifies*	B's audit and status *data*	deleting record of P's malicious activity	Technology
Attack 5	P *deceives*	B's *administrator*	further hiding P's malicious activity	People
Attack 6	A *bypasses*	B's authentication *process*	entering B though backdoor created by P	Technology
Attack 7	A *scans*	B's *network*	looking for valuable information	Technology
Attack 8	A *copies*	B's *data*	stealing B's proprietary rights	Technology
Attack 9	A *sells*	B's *secrets*	giving B's competitors a business advantage	Context
Intrusion effect	B's competitive edge is diminished.			

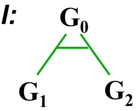
Attack Trees

Provide a means of organizing related intrusion scenarios

Decompose attacker goal

- *AND* **decomposition describes time-ordered sequence of sub-goals**

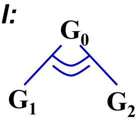
graphical:



textual: Goal G_0
AND G_1
G_2

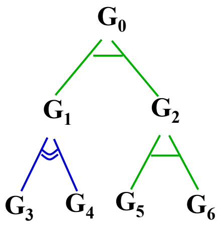
- *OR* **decomposition describes alternative sub-goals**

graphical:



textual: Goal G_0
OR G_1
G_2

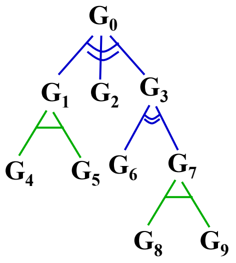
Generating Intrusion Scenarios from Attack Trees



⇓

$\langle G_3, G_5, G_6 \rangle$

$\langle G_4, G_5, G_6 \rangle$

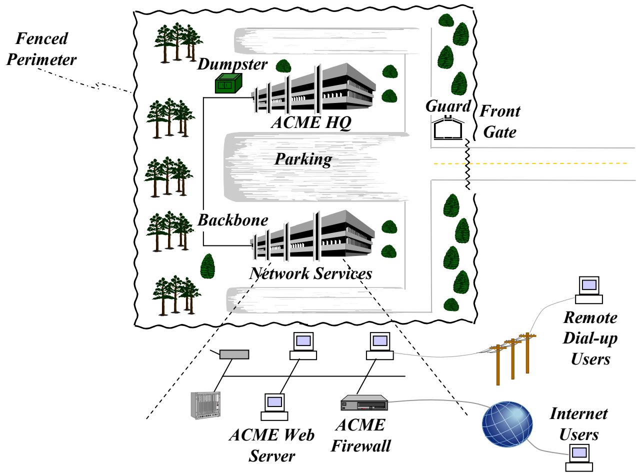


⇓

$\langle G_4, G_5 \rangle \langle G_6 \rangle$

$\langle G_2 \rangle \langle G_8, G_9 \rangle$

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
  – http://www.cert.org/archive/pdf/intrusion-aware.pdf

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