April 11, 2005 -- Lecture 31

22C:169 Computer Security

Douglas W. Jones

Department of Computer Science

Policy Ancillaries

Security Planning Team

Must represent all stakeholders, typically:

- *Hardware support*
- *System administrators*
- *System programmers*
- *Application programmers*
- *Data entry personnel*
- *Physical security personnel*
- *"The users"*

Need assurance of commitment to security!

- *This is frequently the weak link*
  - Upper management commitment frequently empty words

(Business) Continuity Plan

How will operation survive catastrophe

- *Accidental or malicious*
- *Origin in computer or outside computer*
  - More than mere computer security

Example situations

- Terrorists force you to evacuate
  - SENATE ANTHRAX STORY, WORLD TRADE CENTER
- Some key software fails hard
  - AT&T NETWORK OUTAGE
- Supplier of some critical service expires
  - MCI-WORLDCOM
- Natural disaster
  - UNION PACIFIC EXAMPLE

Continuity Planning:

Groundwork must be in place in advance!

Alternate suppliers and backups must be in place before disaster.

Planning requires

Assess needs: what do you rely on
Assess vulnerabilities: how could it fail
Assess options: what can be done

Develop response plan

Who takes charge, what do they do, what resources do they work with

Example: Anthrax attack on US Senate

OCT 16, 2001, WASHINGTON DC

Secretary of the Senate office

Responsible for Senate payroll

Did continuity plan as part of Y2K prep.

Plan included daily backups, GoPacks

Plan coordinated with Sergeant at Arms

On notice of evacuation

Grab GoPacks and run, decontaminate

Set up temp office at Sergeant at Arms

Back in business (in hallway) in a day!

Example: World Trade Center Bombing

New York City Election Office

- *2 blocks from WTC*
- *Did continuity plan after WTC bombing*
- *Plan included GoPacks, off site backup*
- *Plan included staff directories at home*

After WTC collapse

- *Employees worked from home*
- *Found borrowed space for office*
- *Rented computers*
- *Up and running in days*
- *Able to hold election after 2 weeks*

Example: Union Pacific Railroad

Dispatching Center in Omaha

- *Central point of vulnerability for half a continent of railroad network*

Physical security

- *Built in a bunker*
- *Able to run a week without resupply*
- *Redundant data paths to bunker*
- *Redundant computer system*

Disaster preparedness drills

- *One Sunday a month*
- *Force failure of all primary resources*

Risk Analysis

For each threat

P(*threat*) = *likelihood of threat*

C(*threat*) = *cost of threat, if it occurs*

Where threat implies specific damage

We assess the risk of a particular threat as

R(*threat*) = *P*(*threat*)*C*(*threat*)

that is, risk is weighted cost

Obviously

Use risk to prioritize threats!

Risk assessment is difficult

First *P*(*threat*) is not easy to assess

- *accurate values for routine cases*
- *can only guess uncommon cases*
  - What was *P*(*WTC attack*) ?

Second *C*(*threat*) is not always easy

- again, accurate for routine cases
- which consequences do you dollarize?
  - What was *C*(*WTC attack*) ?

Indeterminate results are common:

- *R* = *PC* = *infinity* x *infinitesimal*

Bad risk assessment is common!

Example: Diebold's estimate of MTBF

Quote MTBF of system as minimum over the MTBF of all components

Correct statistical model is daunting

Must know distribution functions

Diebold right for one unlikely distribution

Analytical solution

Possible for well behaved distributions

Impossible in general case

The art of risk assessment

Make educated guesses

Do so using very structured methods

Be aware of weakness of results

Do not let structured methods lead you to overestimate the resulting precision

Be aware that completely wrong might work

The Y2K efforts for the Senate protected against unrelated threats!

Scientific risk assessment may primarily serve to convince management that resources should be devoted to security.