April 13, 2005 -- Lecture 32

22C:169
Computer Security

Douglas W. Jones

Department of Computer Science

Let's Get Physical

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.

Physical Security

Security against natural disasters

- *Flood*
- *Earthquake*
- *Fire*
- *Wind*

Security against unnatural disasters

- *Riot*
- *Bombing*
- *Attacks on critical infrastructure*
- *Carelessness*

Security against direct attack on system

- *Theft*
- *Alteration*

Natural Disaster Risk Assessment

FEMA Floodplain Maps show

Expected water level in 100 and 500 years

Elevate or floodproof critical equipment

USGS National Seismic Hazard Mapping Proj.

Expected ground motion in 50 years

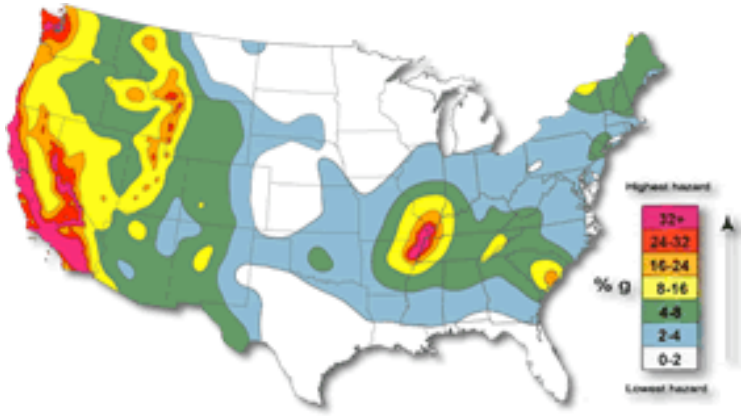
Move critical servers to low hazard area

Use shockproof equipment mountings

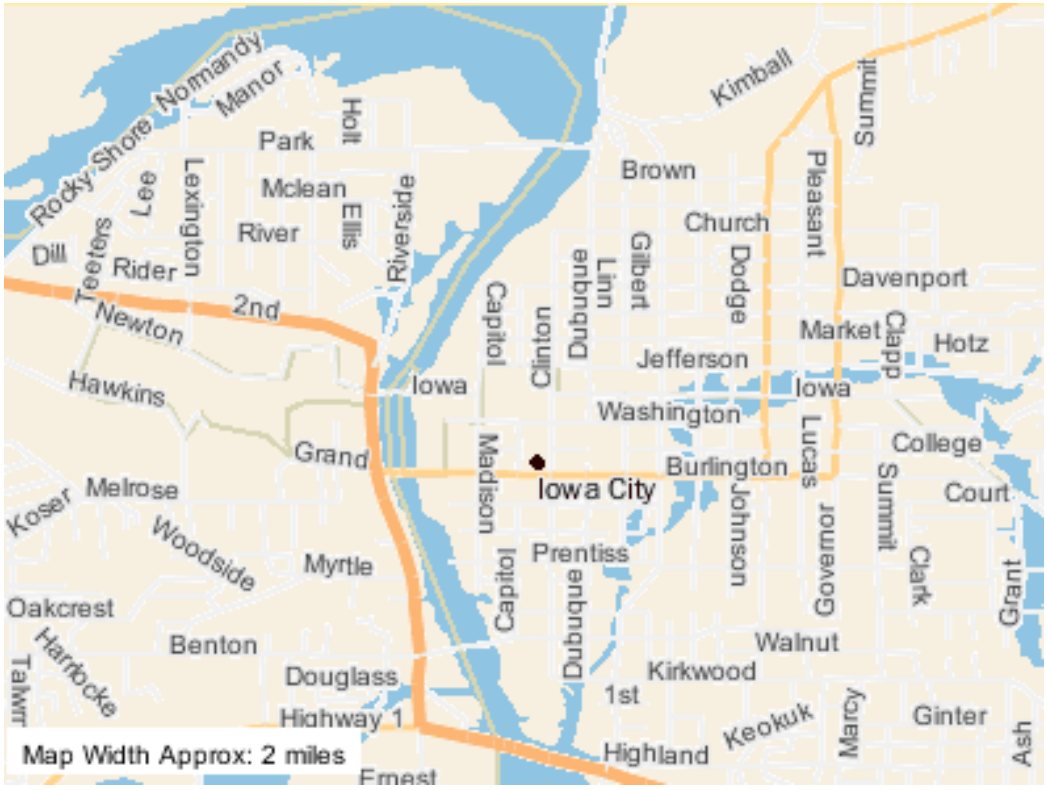
HazardMaps.gov

Current gateway to various US maps

USGS Earthquake Map of the United States



HazardMaps floodplain map of Iowa City



Defense against direct attack

Security cameras

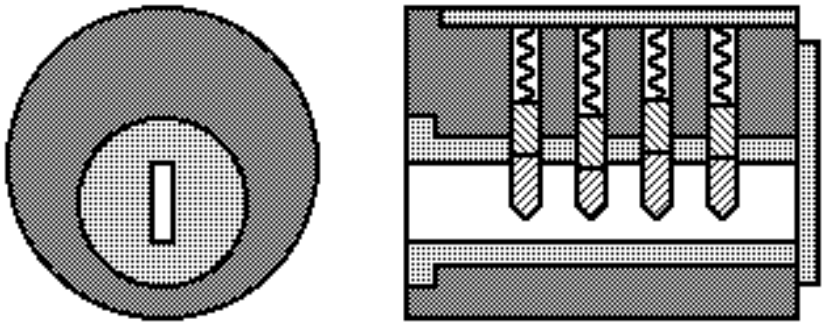
- *act as deterrent*
- *record evidence*
  - New York RNC story
- *can alert security personnel*
  - but only if actually monitored

Guards

- *act as deterrent*
- *serve as witnesses*
- *call for help*
- *actually defend against small scale attack*

Locks

The classic pin-tumbler lock



The idea is ancient

The technology is 19th century

Modern locks

Computerized smartcards

Biometrics

How fragile is this technology?