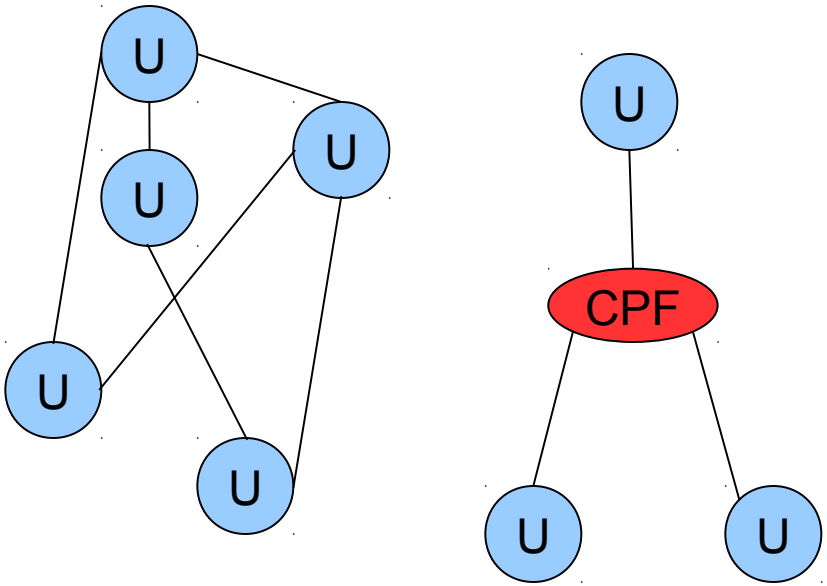
Security vs. Security Architecture

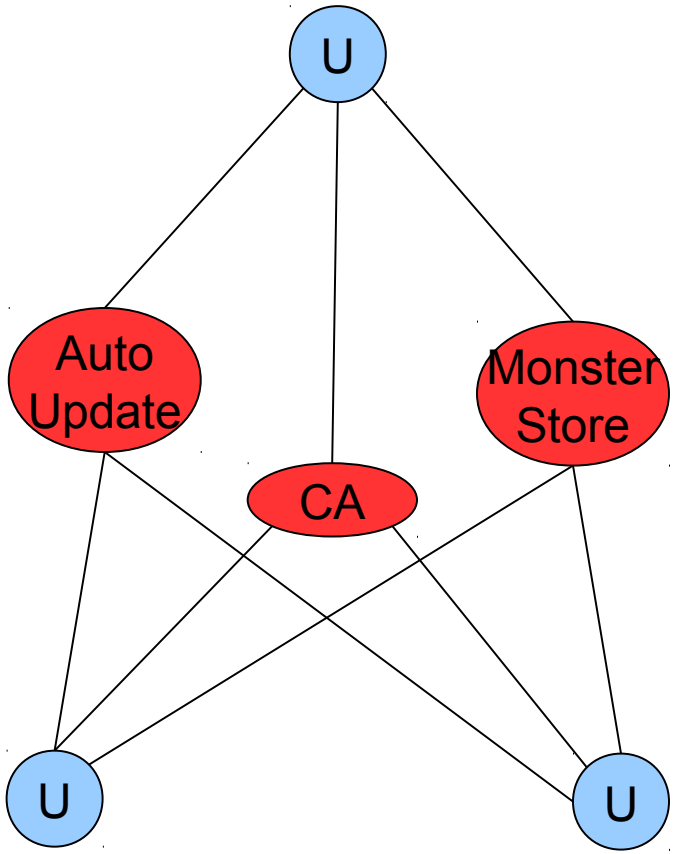
Marc Stiegler
HP Labs
Exascale Computing

What is a Security Architecture?

- Layout/interrelationship of security elements
- Can a system be more secure than its architecture?
  - No
- Can a system be more secure than the implementations of its elements?
  - Yes *if it is a good architecture*

Central Points of Failure: A Great Idea?





“Anything that can be done for you can be done to you”

- Certificate authorities and spoofing keys
  - Sold to anyone who pretends to be a fed
- How can anyone be surprised?

> The company in question is known as Packet Forensics.... According to the flyer: "Users have the ability to import a copy of any legitimate key they obtain (potentially by court order) or they can generate 'look-alike' keys designed to give the subject a false sense of confidence in its authenticity." The product is recommended to government investigators, saying "IP communication dictates the need to examine encrypted traffic at will." And, "Your investigative staff will collect its best evidence while users are lulled into a false sense of security afforded by web, e-mail or VOIP encryption."

Bruce Schneier:
http://www.schneier.com/blog/archives/2010/04/man-in-the-midd_2.html

Popular Modern Day Security Architectures

Independence Day Evil Alien

Barn Door

Street Lamp

Gilded Cage

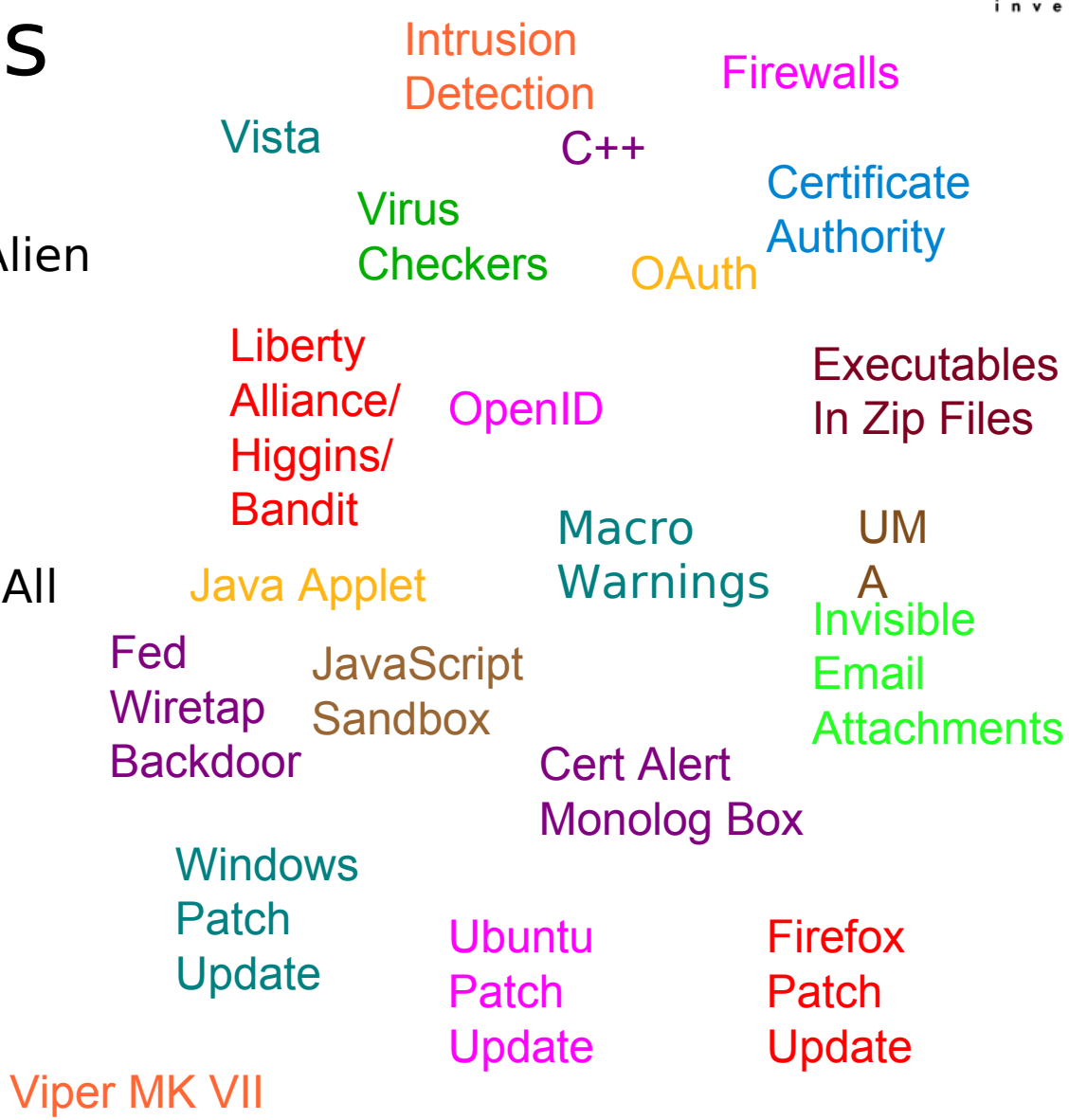
One Word to Rule Them All

Gone Phishin’

Eggshell Perimeter

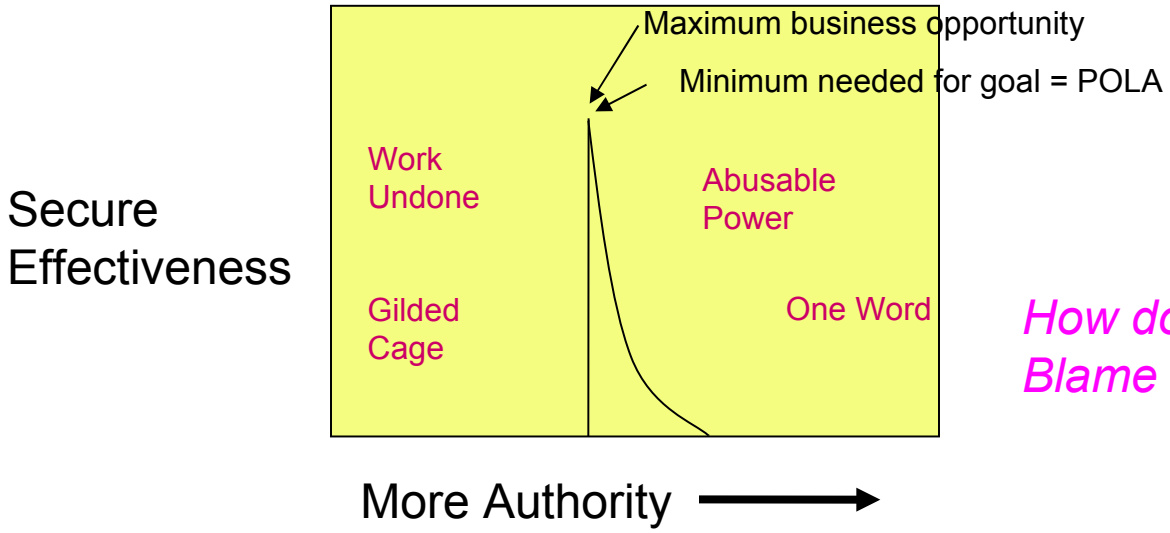
Theater in the Round

Blame the Victim



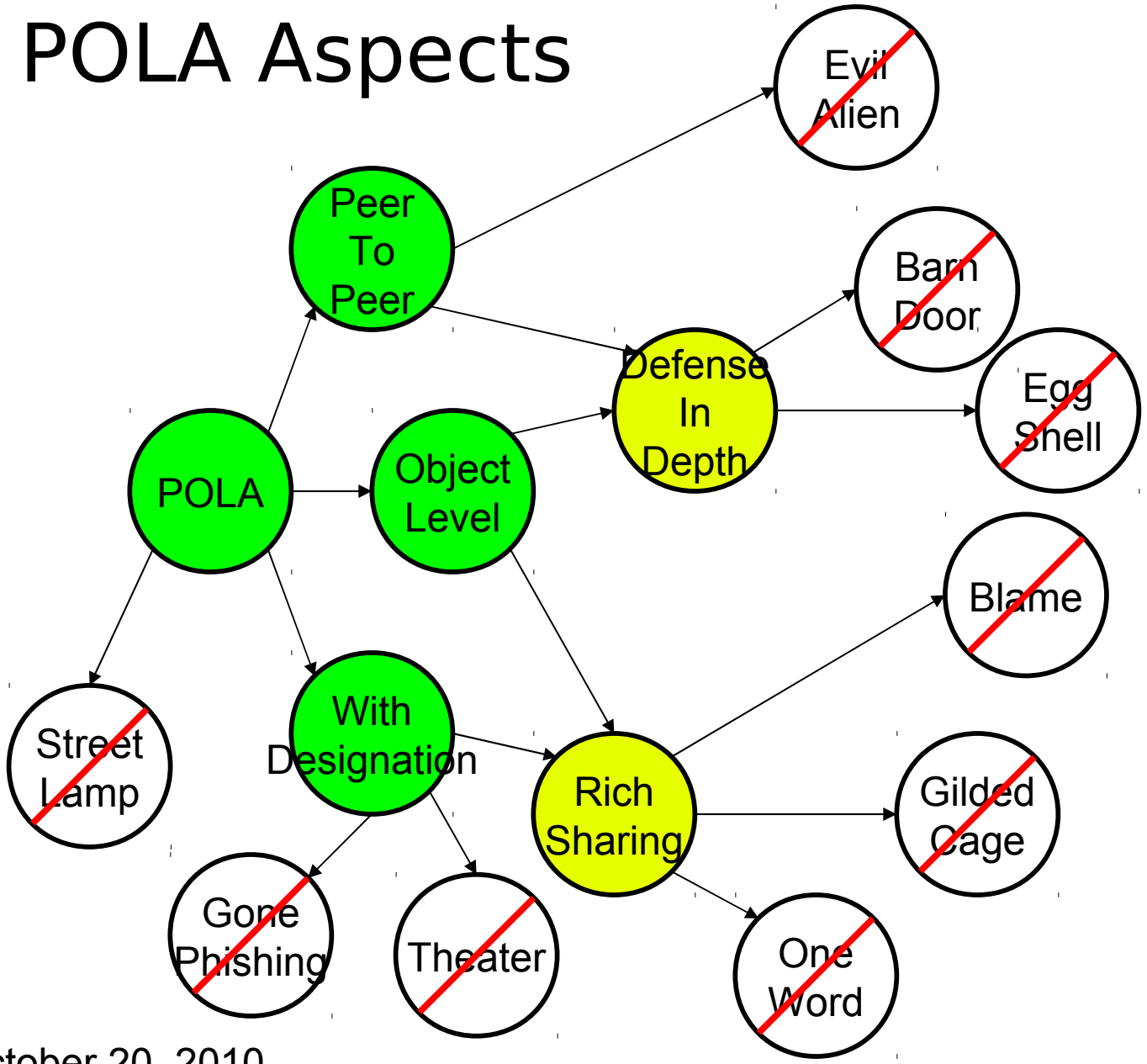
Principle of Least Authority(POLA)

Give person/object *everything* they need and *nothing else*



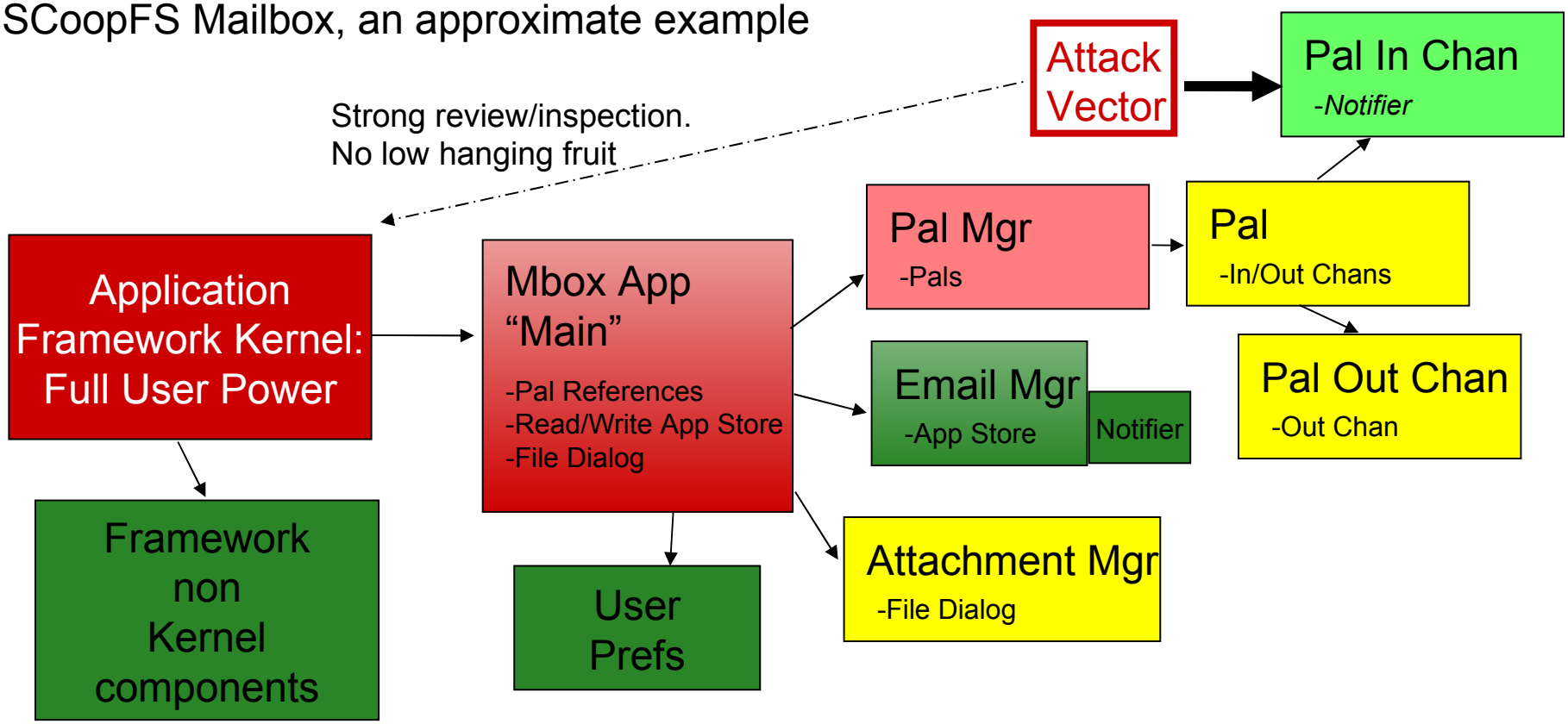
How do Theater and Blame fit in?

POLA Aspects



Defense In Depth vs. Eggshell

SCoopFS Mailbox, an approximate example



As we move away from core, less authority needed

Gilded Cage vs. Rich Sharing

Dynamic

Attenuated

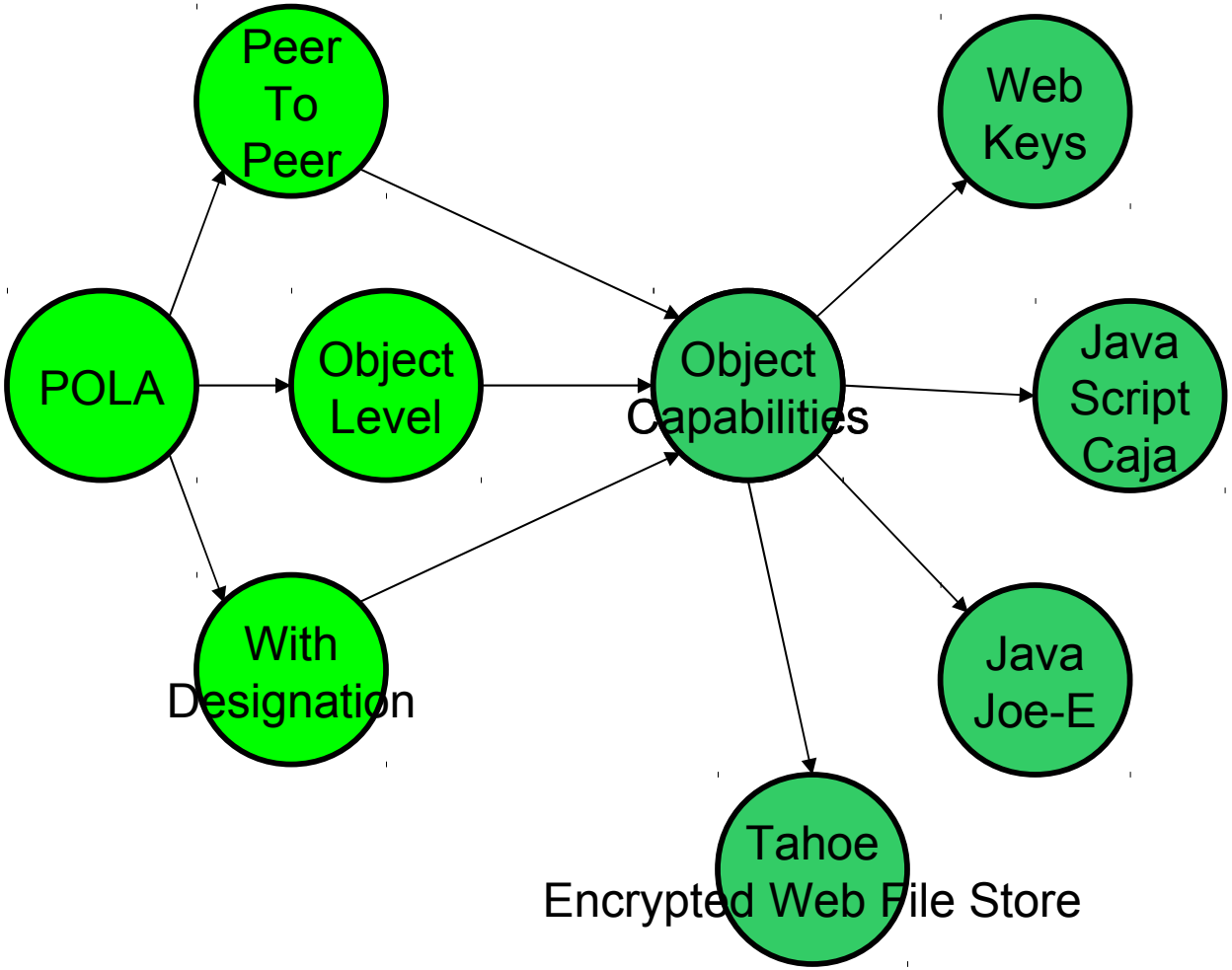
Chained

Cross Domain

Recomposable

Accountable

POLA Implementation



Demos

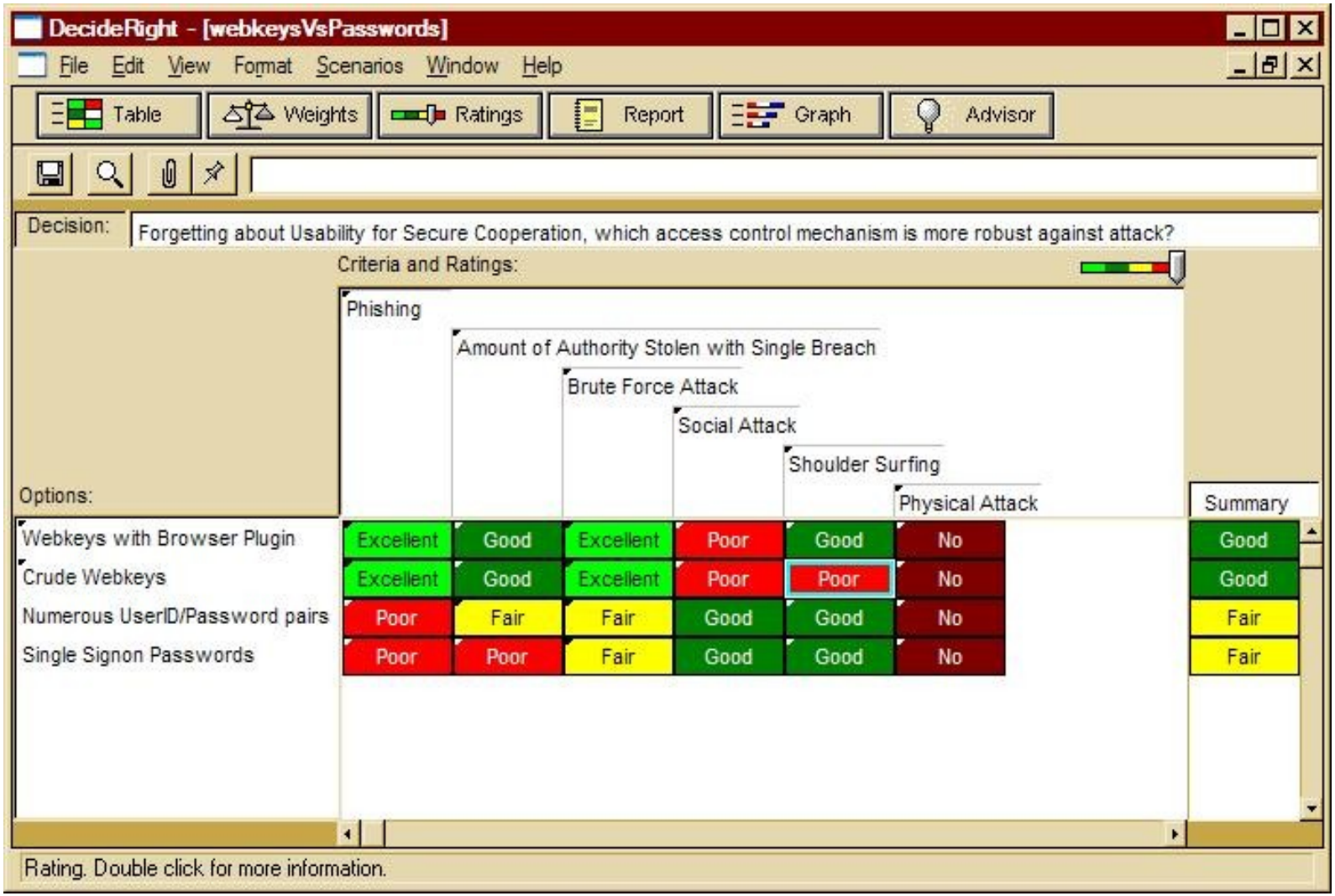
- Purse
- ShareShell

ShareShell: Scoring

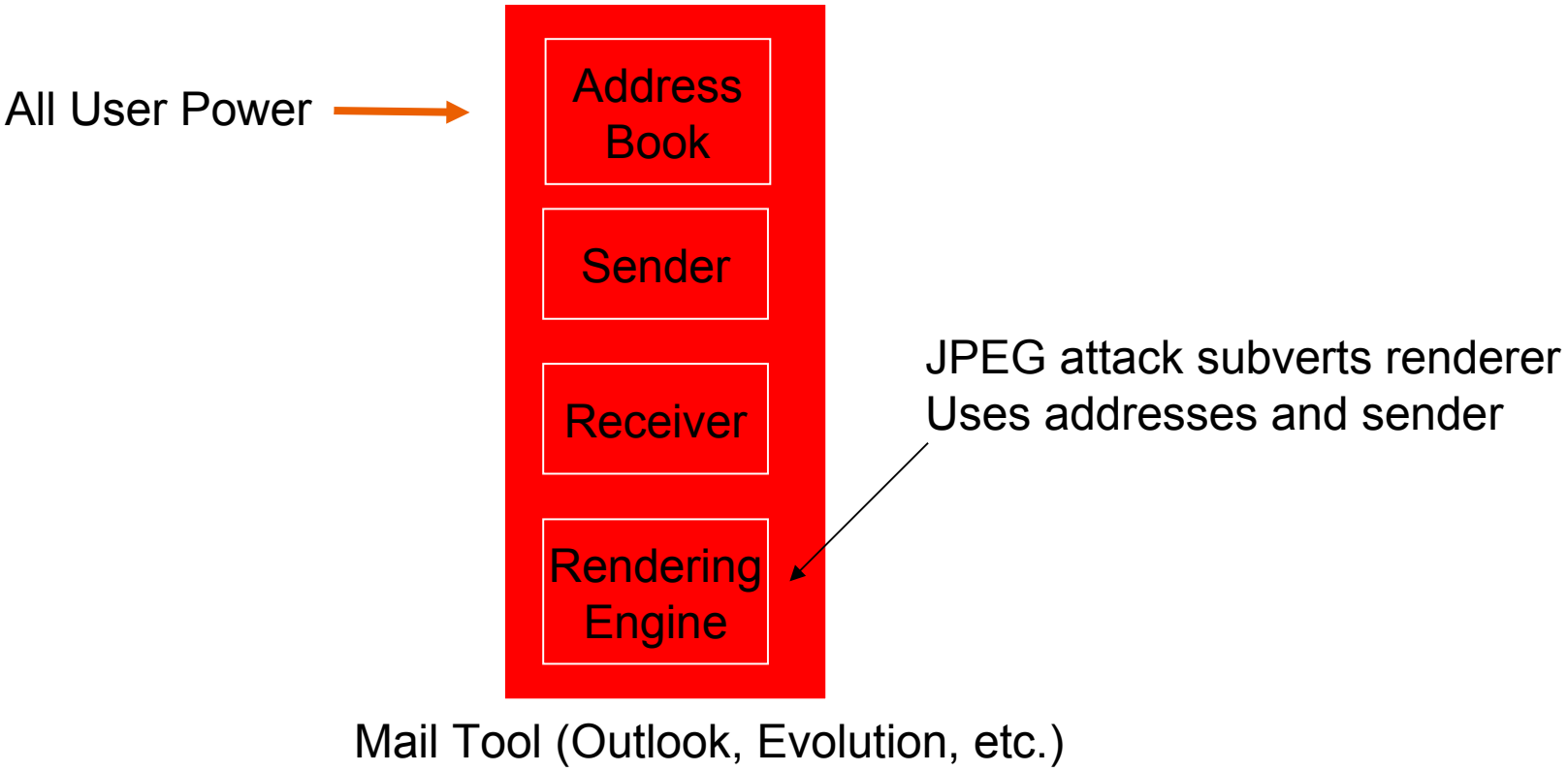
Independence Day Evil Alien	8 (insecure OS, Windows/Linux)
Barn Door	9 (Revocation if abused)
Street Lamp	7 (https, java, os standards)
Gilded Cage	9 (inexpressible attenuations)
One Word to Rule Them All	10
Gone Phishin’	9 (vulnerable at first connect)
Eggshell Perimeter	9 (shallow defense in depth)
Theater in the Round	9 (cert at first connect)
Blame the Victim	10

Backups

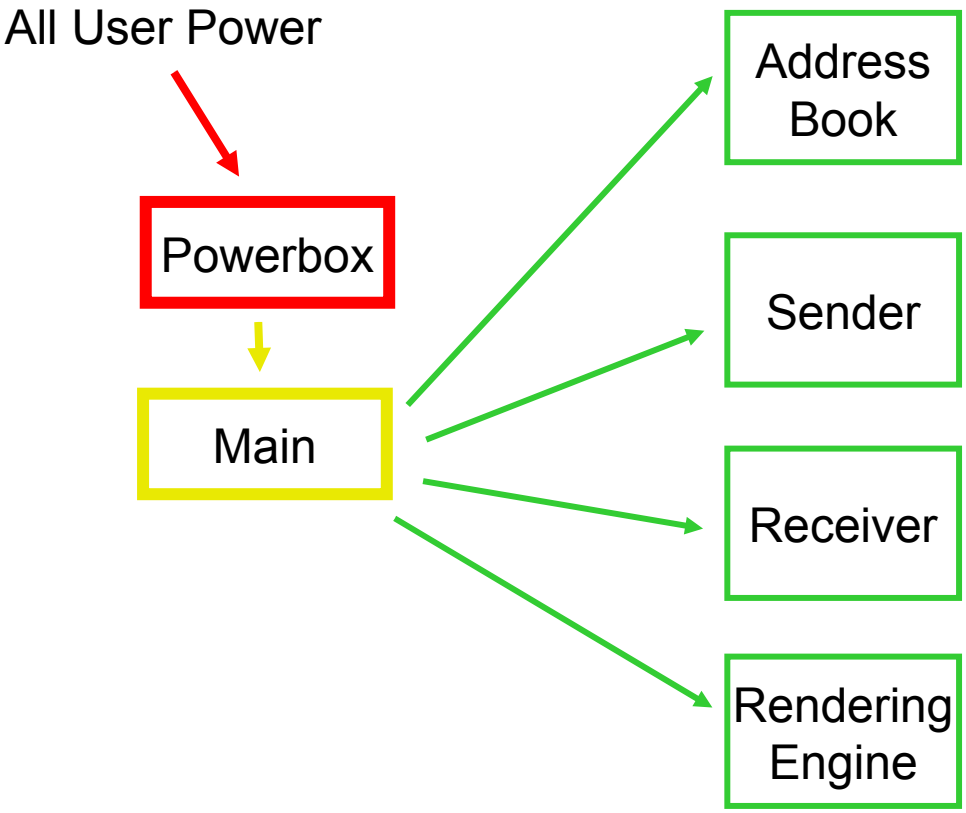
Webkey Decision Matrix



Eggshell/Barn Door



Defense In Depth/POLA



JPEG attack subverts renderer
No access to sender, addresses