CERIAS

the center for education and research in information assurance and security

Reliability On The Poly^2 Framework

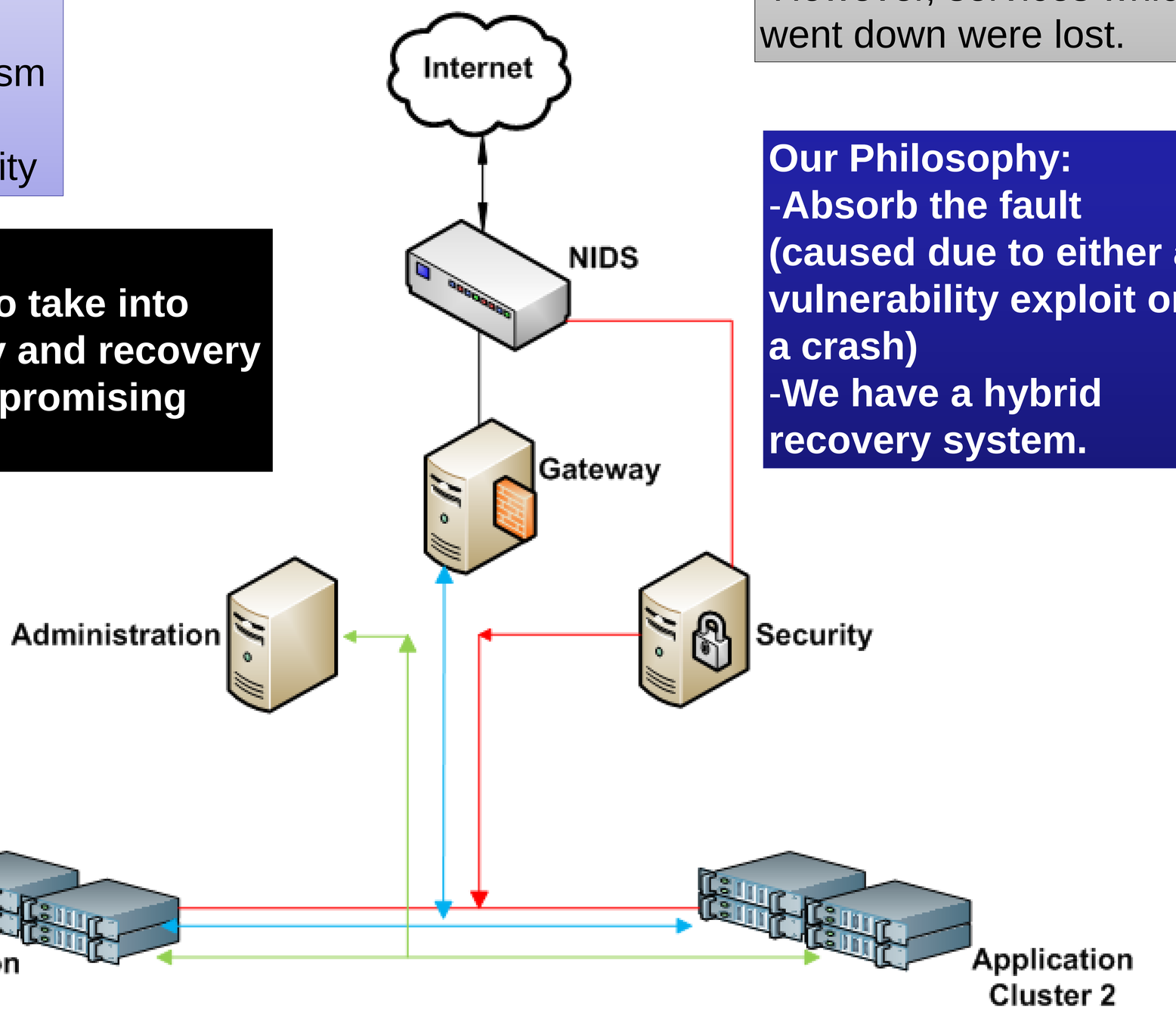
Ankur Chakraborty
CERIAS

Original Design Principles:
- Economy of Mechanism
- Least Privilege
- Separation of Privilege
- Complete Mediation
- Fail-Safe Defaults
- Least Common Mechanism
- Open Design
- Psychological Acceptability

Original Philosophy:
-Attack absorption
-Attack isolation

-However, services which went down were lost.

Our Goal:
Improve the framework to take into consideration availability and recovery without excessively compromising original design.



Our Philosophy:
-Absorb the fault (caused due to either a vulnerability exploit or a crash)
-We have a hybrid recovery system.

Recovery Delegation:
-Active Replication
-Checkpointing

Active Replication:
To maintain the state inspite of crashes,

Checkpointing: To prevent persistence of vulnerabilities

PURDUE UNIVERSITY

CERIAS

Discovery Park
e-Enterprise Center