W. P. CAREY
SCHOOL of BUSINESS

A Game-theoretic Approach to the Design of Self-Protection and Self-Healing Mechanisms in Autonomic Computing Systems

Birendra Mishra

Anderson School of Management, U C Riverside

T. S. Raghu

W. P. Carey School of Business, Arizona State University

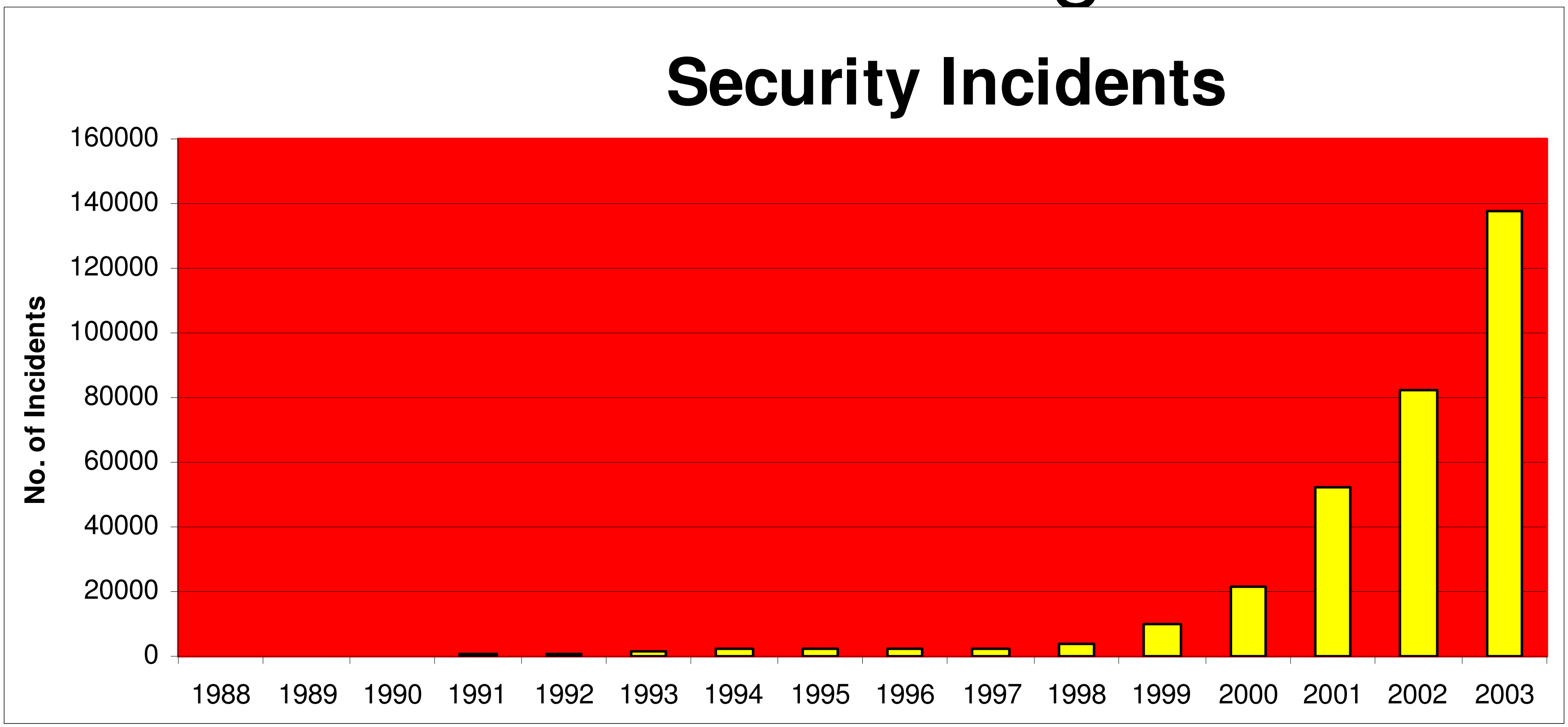
ASU ARIZONA STATE UNIVERSITY

Overview

- Background
- Research Objective
- Approach
- Model
- Results
- Extensions

W. P. CAREY
SCHOOL OF BUSINESS

Threats to Information Security Are Increasing



Source:CERT Report

ARIZONA STATE UNIVERSITY

Background

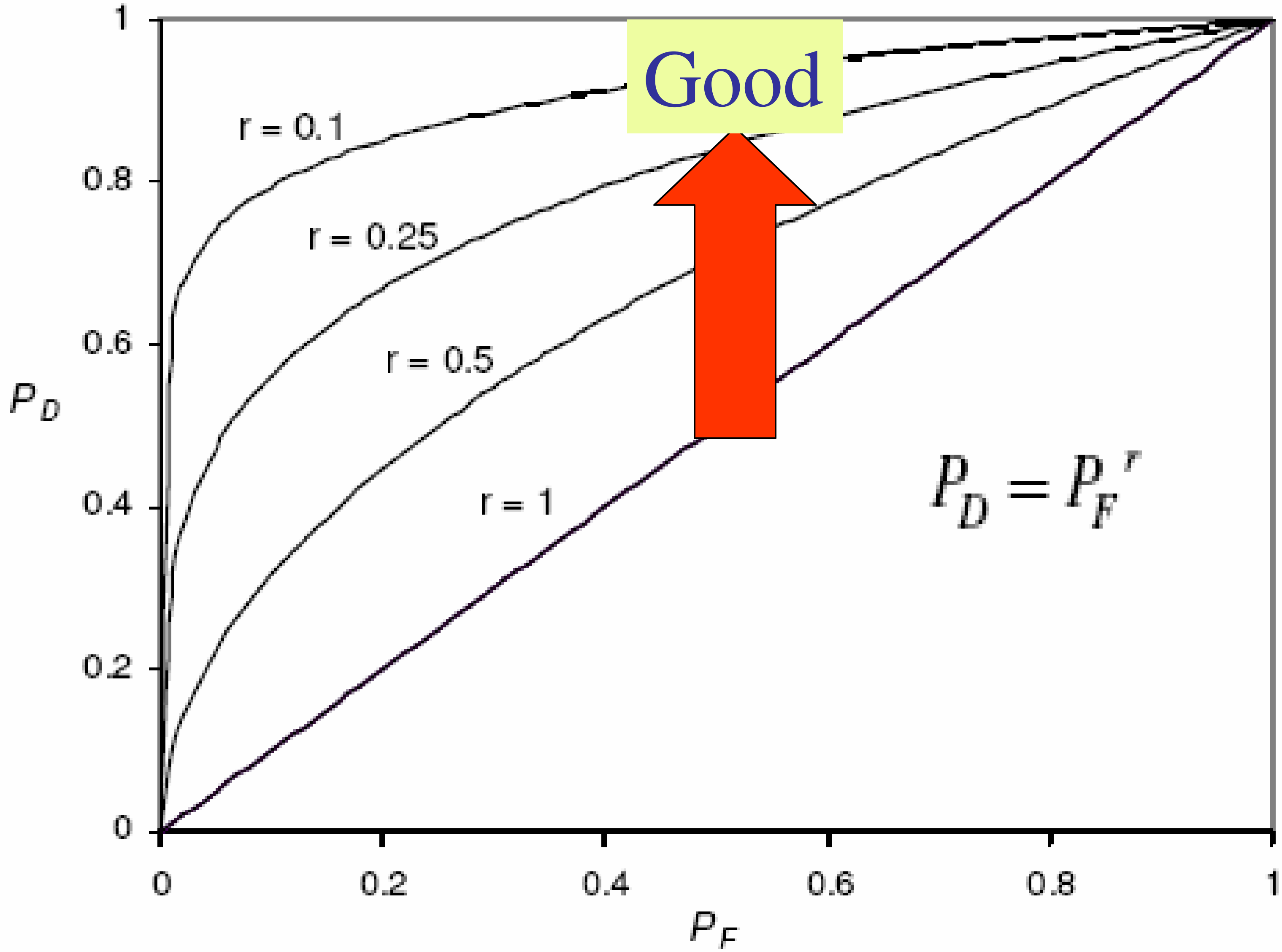
- Two Orientations
  - Technical aspects of IDS
  - Business aspects of IDS
- Technical aspects
  - Network IDS
    - Scan patterns: known attacks and abnormal traffic
  - Host based IDS
    - Anomaly: based on normal behavior, Misuse: signature based

Business orientation

- Value of IDS
  - Low detection rates
  - High false alarm rates
- Base rate fallacy (Axellson 2000)
  - Low hacker to user population
- Focus on preventive controls
  - Firewalls, access controls

Human Intervention

- IDS profile
  - Technology, design parameters, configuration (Lippmann 2000)
- Receiver Operating Characteristics (ROC) curve (Trees 2001)
  - Detection and false alarm probabilities


1
0.8
0.6
0.4
0.2
0
P_D
0
0.2
0.4
0.6
0.8
1
P_F
r = 0.1
r = 0.25
r = 0.5
r = 1
Good
$P_D = P_F^{\,r}$

Case for autonomic computing

- Manual investigation is expensive
- High false alarm rates not going away
- High volume attack/traffic can overwhelm human resources
- Move to automated detection, response and healing is beneficial

Research objective

- High level systems objectives drive self-protection and self-healing properties
- Self-configuration is inherent in autonomic computing concept
- Allocation of computing resources to detect and counter attacks
- How do we best model intrusion game to optimally determine broad system level objectives?
  - Can autonomic systems automatically reconfigure in response to change in hacker patterns?

Approach

- Game theoretic approach
- Inspection games
  - Applied in piracy control, auditing, arms control
- Focus on detection and verification
- Stylistic model of intrusion detection and verification

Approach

- Three models
- Case 1: Manual intervention (base case)
- Case 2: Computational effort allocation on investigating alarms
- Case 3: Dynamic configuration of IDS to impact detection and false alarm probabilities

W. P. CAREY
SCHOOL OF BUSINESS

Assumption

- Exponential distribution $P_D(d,t) = \int_t^\infty \theta_H(d) e^{-\theta_H(d)x} dx$
- Yields the relation

$$P_D = P_F^{\,r}$$

and $$P_F(t) = \int_t^\infty \theta_N e^{-\theta_N x} dx$$

- Other distributions can be used, implicit relation between detection and false alarm probabilities through *t* is needed.

ARIZONA STATE UNIVERSITY

$\underset{(\psi,d)}{Max}\ \psi d - \psi\beta P_D(d,t)$

W. P. CAREY
SCHOOL OF BUSINESS

Model (Case 2)

- Threshold parameter fixed exogenously
- Hacker maximizes his expected utility

$$\underset{(\psi,d)}{Max}\ \psi d - \psi\beta P_D(d,t)$$

- Similarly the autonomic agent maximizes

$$Max\ F(t,E) = \lambda.\ddot{d}(E).P_D(d,t) - \lambda\ddot{C}_D(E)P_D(d,t) -$$

$$(1-\lambda)\ddot{C}_F(E)P_F(t)$$

Case 2

- Consider

$$cd := Cd\,E^{\alpha}$$

$$cf := Cf\,E$$

D=d*E

$$E := 1 - \mathrm{e}^{(-effort)}$$

Results (Case 2): Damages incurred

- Damage potential (d_{max}) increases damages incurred
- Detection penalty (β) decreases damages caused to the system
  - Deterrence improves IDS performance
- Increase in threshold parameter (t) and distribution parameter for hacking (θ) increases damages incurred

Results

- For a given IDS quality profile and damage potential
  - Low enforcement penalty possibility on hackers leads to higher threshold level for detection (low detection and low false alarms)
  - Higher enforcement penalty possibility on hackers leads to lower threshold level for detection (high detection and high false alarms)

Computational Effort

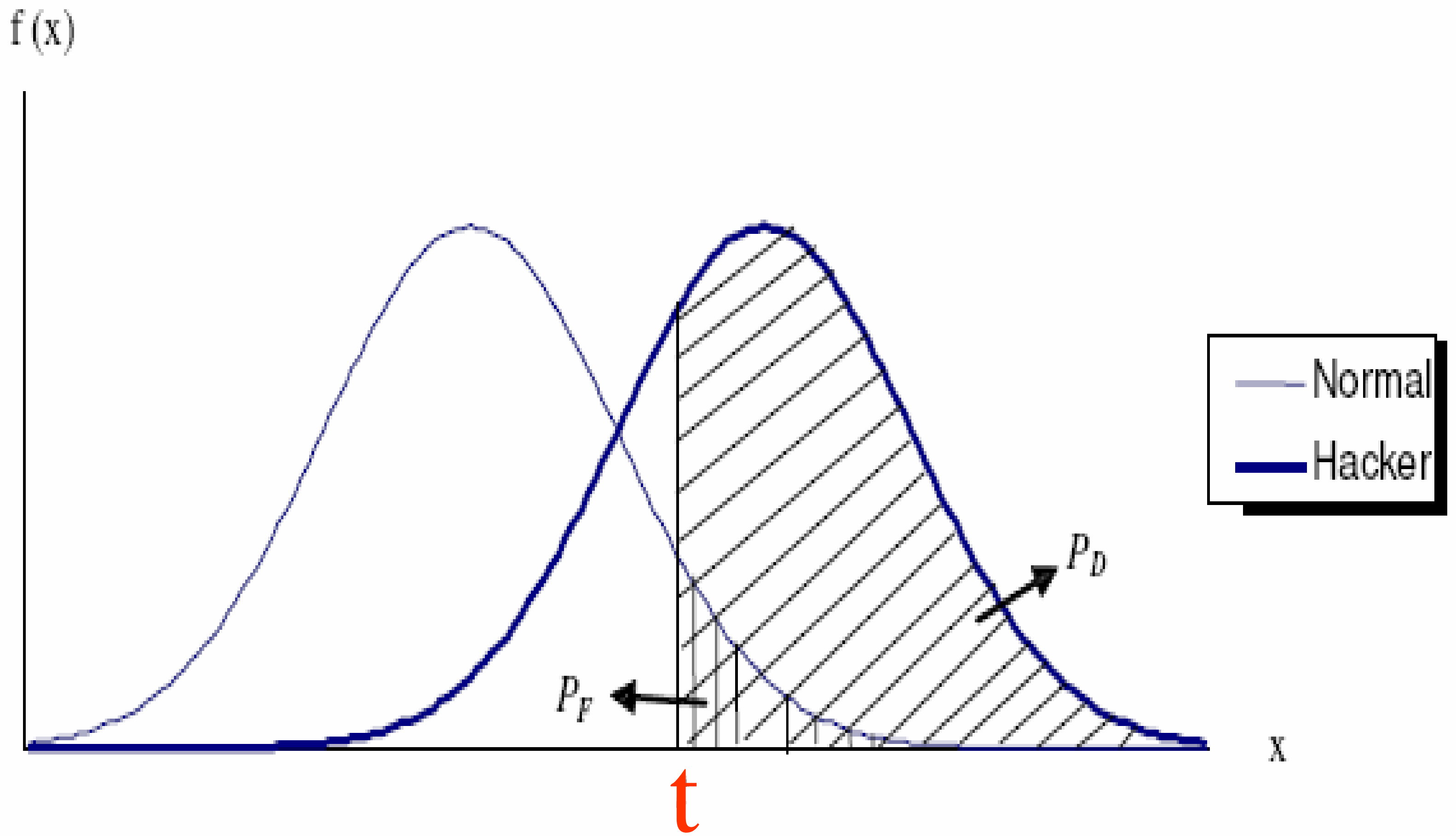
- Allocation of computational effort to detect and heal intrusions
  - Reduces with reduced convexity of cost function (parameter α)
- Increased cost of false alarm detection (or true alarm detection) decrease overall computational effort allocation to detection efforts
- Allocation of effort reduces with reduced damage potential

Implications

- Autonomic systems can adapt to different environmental and system conditions by varying the computational resources dedicated to self-healing and self-protection efforts
- Damages incurred by systems still depend on deterrence impact of detection efforts

W. P. CAREY
SCHOOL OF BUSINESS

Results (Case 3)



Continuous adaptation

- Self-tuning or self-configuration
  - Adapt to changing event conditions through a gaming framework
- Optimization with respect to both computational effort allocation and threshold parameter
- Analytical solution not tractable
- Numerical solutions, however, are possible

Further work

- Numerical experiments currently underway
- How do we set effective policies to detect changes in the system environment to affect threshold changes?
- What are the implications of threshold parameter changes in an adaptive system?
- Can parameters used to specify threshold be domain independent?