

# **Wireless Internet Security with Dynamic Intrusion Response for M-Commerce**

**Kai Hwang**

**Internet and Wireless Security Laboratory  
University of Southern California**

**Presentation at ICA3PP2002,  
Beijing, China, October 23, 2002**

## **Presentation Outline:**

- ❖ **Wireless Public Key Infrastructure (WPKI) for Securing M-Commerce**
- ❖ **Mobile IPv6 and Wireless TCP for Hybrid 3G Wireless/All-IP Networks**
- ❖ **Risk Assessment for Dynamic Intrusion Response to Multiple Network Attacks**

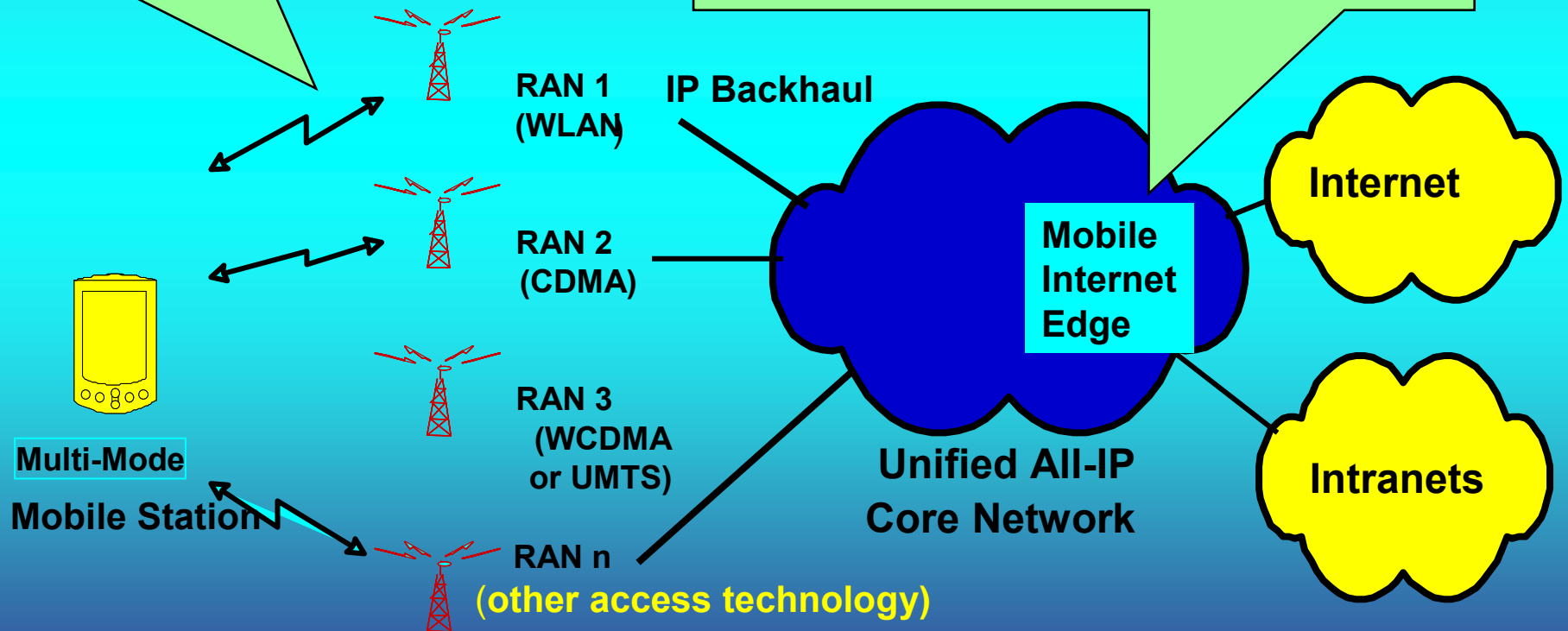
# Core Technology in Wireless Internet

## Multi-mode Mobile Station:

- Mobile IPv6, WTCP
- WTLS
- 1x EV DO + WLAN
- Chipset

## Mobile Internet Edge :

- Mobile Internet Edge Product
- WTCP and WTLS Software Suites
- Cluster Platform for Wireless Gateway
- Storage-area Networking and RAID



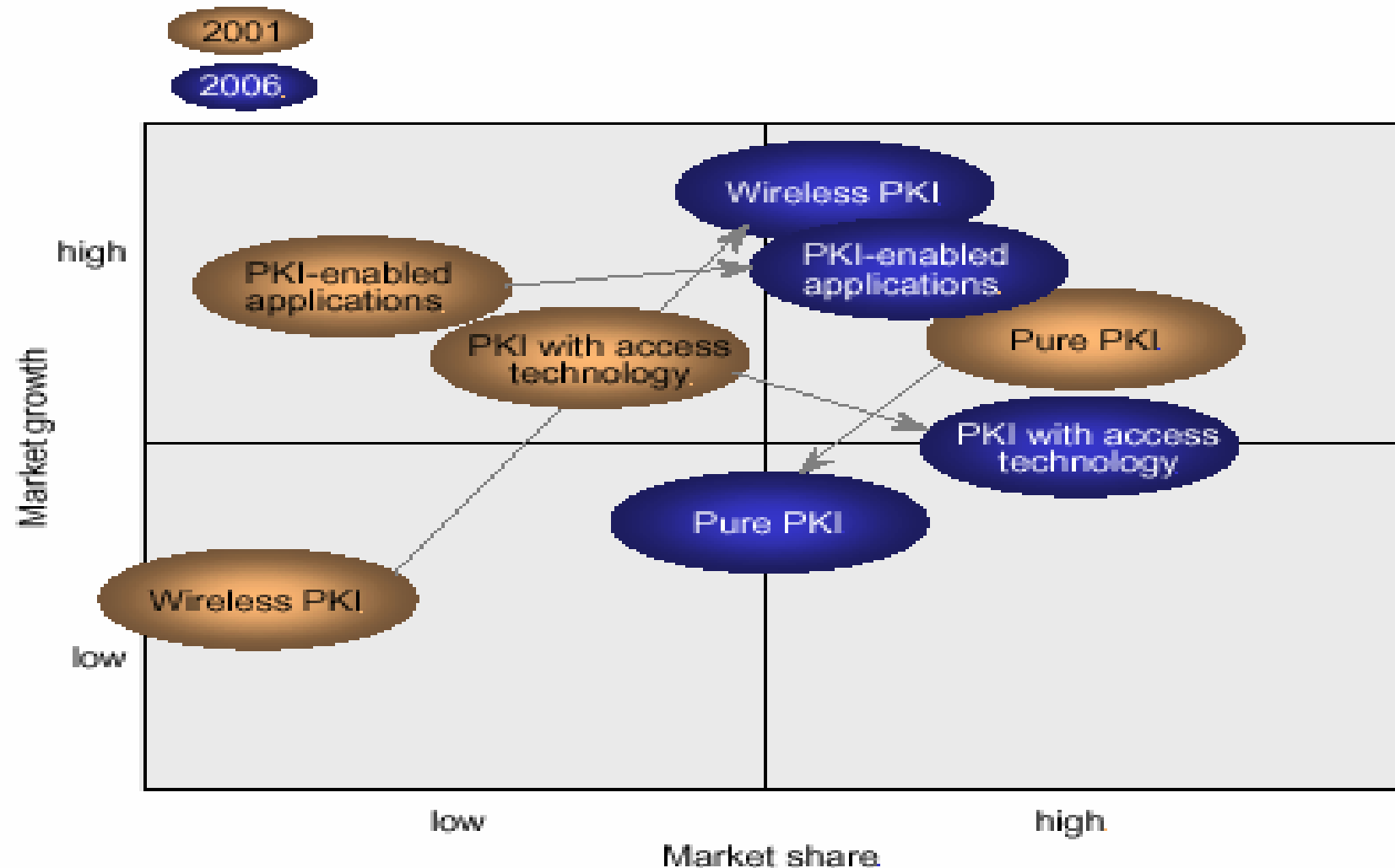
# Basic Wireless Security Requirements:

- ❑ Confidentiality of exchanges – make sure that nobody can listen in.
- ❑ Authentication – Certify the identities of the parties involved.
- ❑ Data Integrity - assurance that data is not tampered on its journey.
- ❑ Non-repudiation of transactions – assure agreements are legally binding.

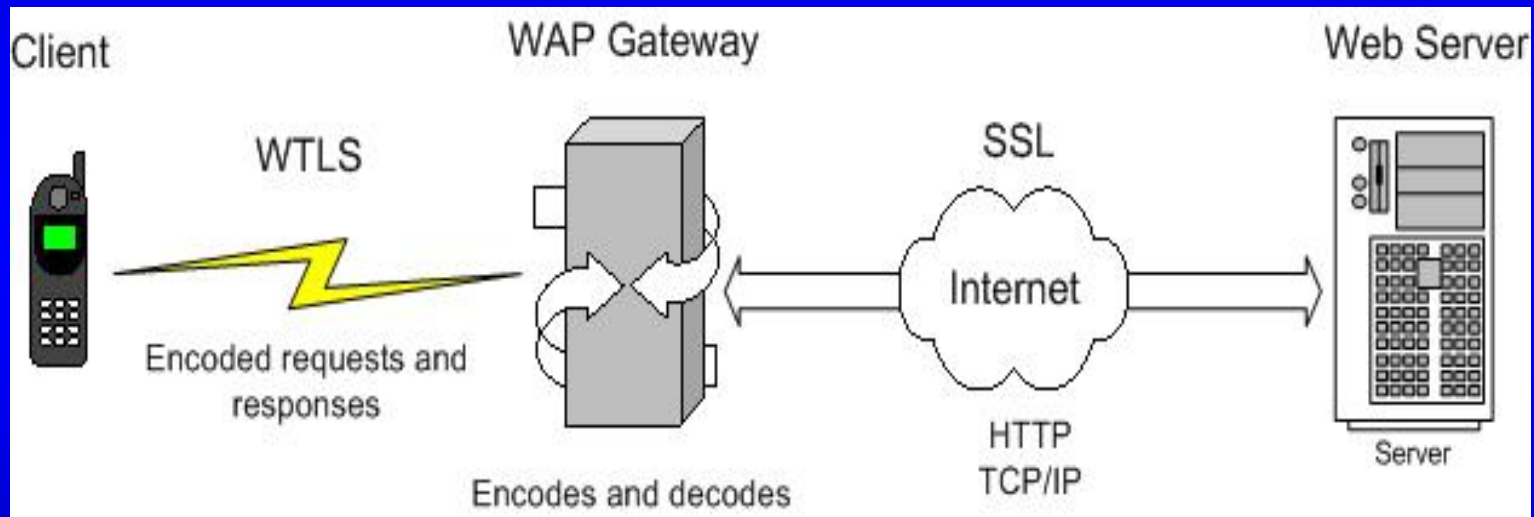
# **Increasing Security Demand in M-Commerce and Pervasive Applications:**

- LANs, clusters, Intranets, WANs, Grids, and the Internet all demand security protection hacker-proof operations, crucial to the acceptance of a trust-based digital society**
- Innovative mobile wireless services, E-transactions, telemedicine, and digital government; all demand high security, privacy protection, and data integrity.**

# Public Key Infrastructure Development Trend



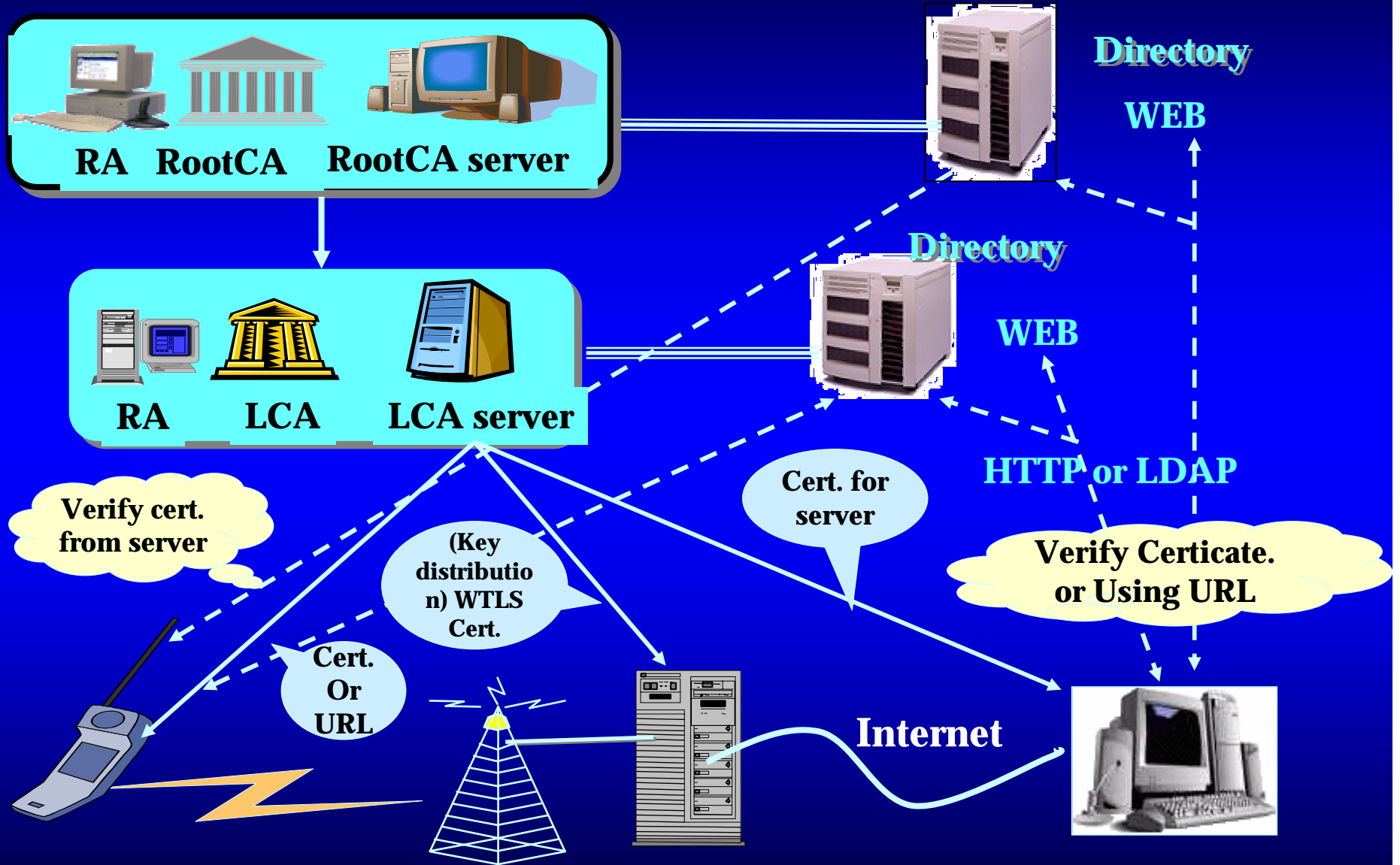
# Wireless Internet Access and WAP Gateway Functionality Based on WTLS Technology



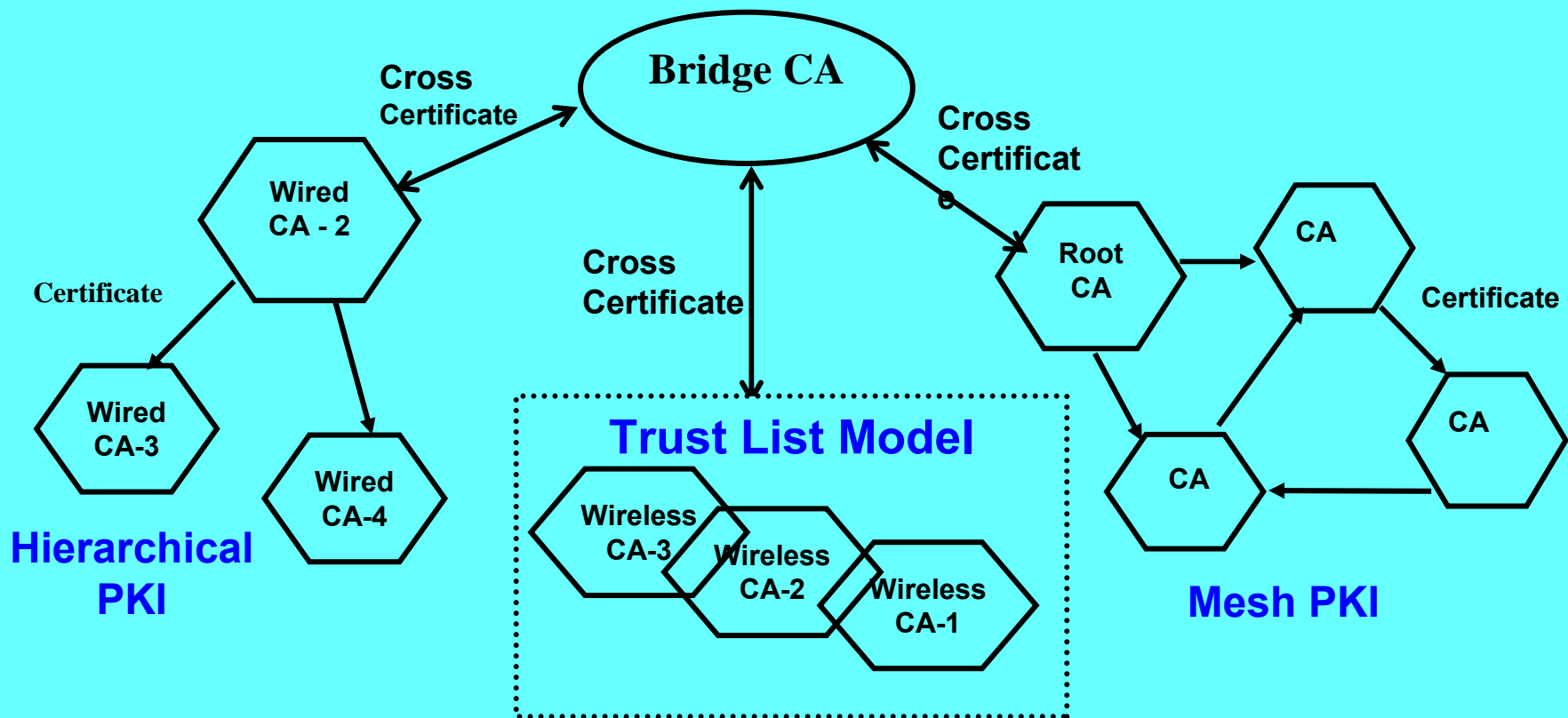
## WTLS: Wireless Transport Layer Security

The Protocol to implement wireless security in the WPKI (Wireless Public Key Infrastructure)

# Conceptual Wireless PKI Model



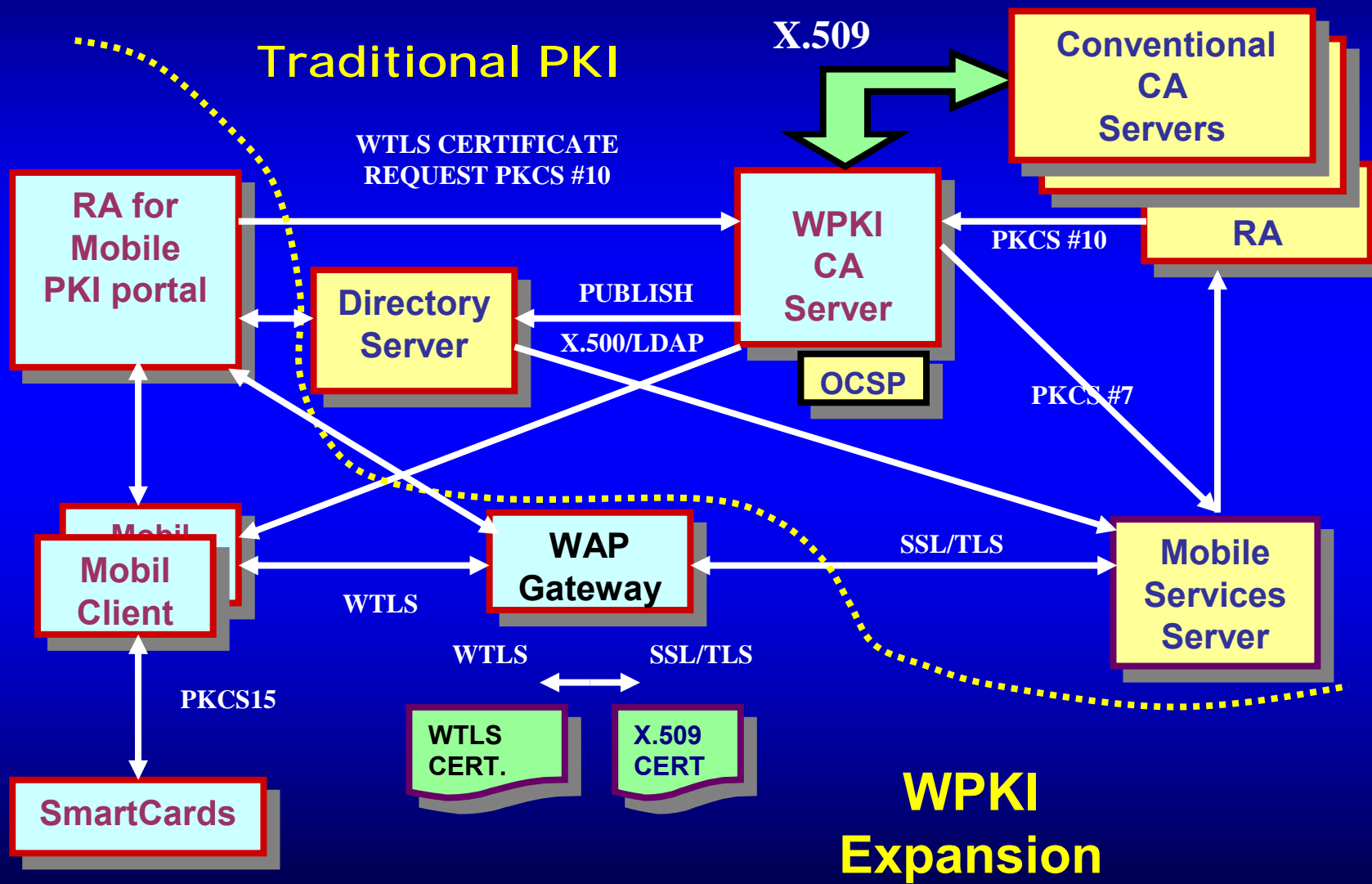
# Trust Propagation by Bridging PKI Domains over Wireline and Wireless Networks



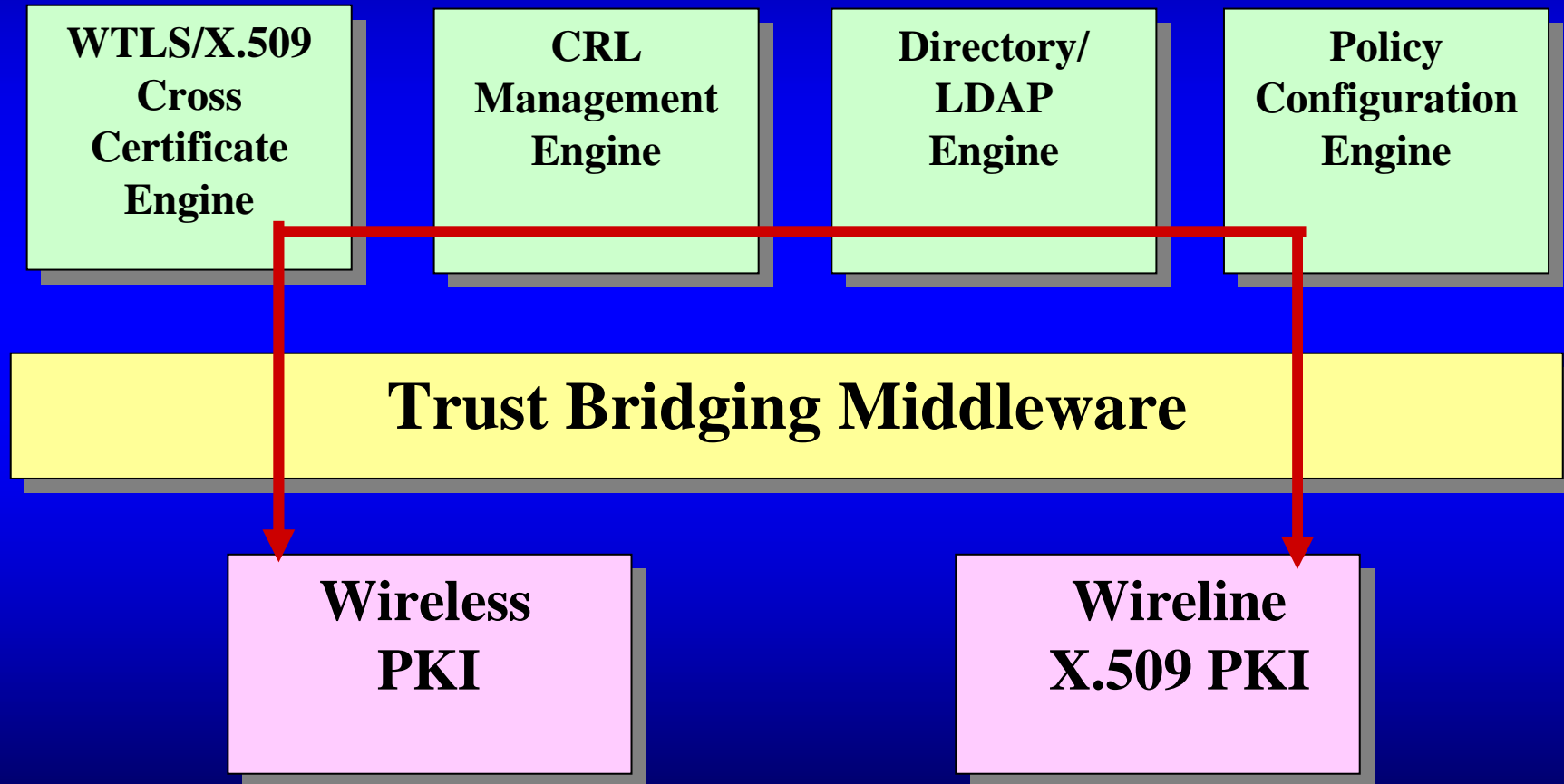
Example Trust Path construction from wired CA-3 to wireless CA2:

**Wired CA-3 → Wired CA-2, Wired CA-2 → Bridge CA,  
Bridge CA → Wireless CA-1, Wireless CA-1 → Wireless CA-2**

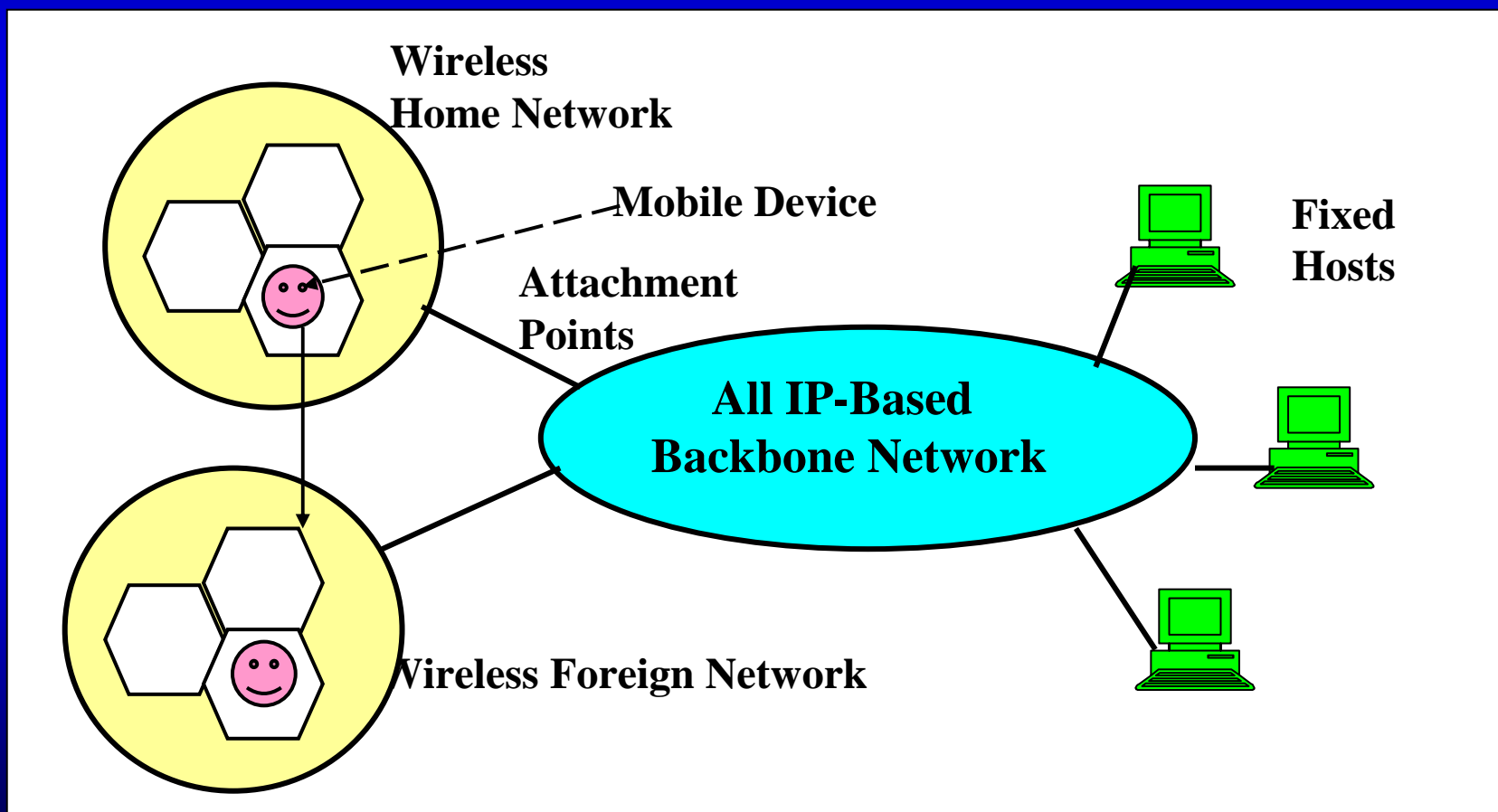
# Interoperability of WPKI with Traditional PKI



# Middleware for Trust Management on the Bridge CA Cluster



# Mobile IPv6, WTCP, and WTLS Protocols for Security in Hybrid Wireless and IP-Based Networks



# Home Agents vs. Foreign Agents in Mobile IP Communication

- ❖ Each mobile has a **Home Agent (HA)** and a **Foreign Agent (FA)**. They work jointly to track the network links for tunneling datagrams destined to a mobile device.
- ❖ **Operation of Mobile IP:** The HA and FA make themselves known by advertisement. Agent discovery, registration, and tunneling are 3 major processes
- ❖ **Tunneling (routing)** The HA encapsulates the message from the IP host to the mobile device via its FA. It is desired to achieve optimized routing of the packets destined for a mobile device

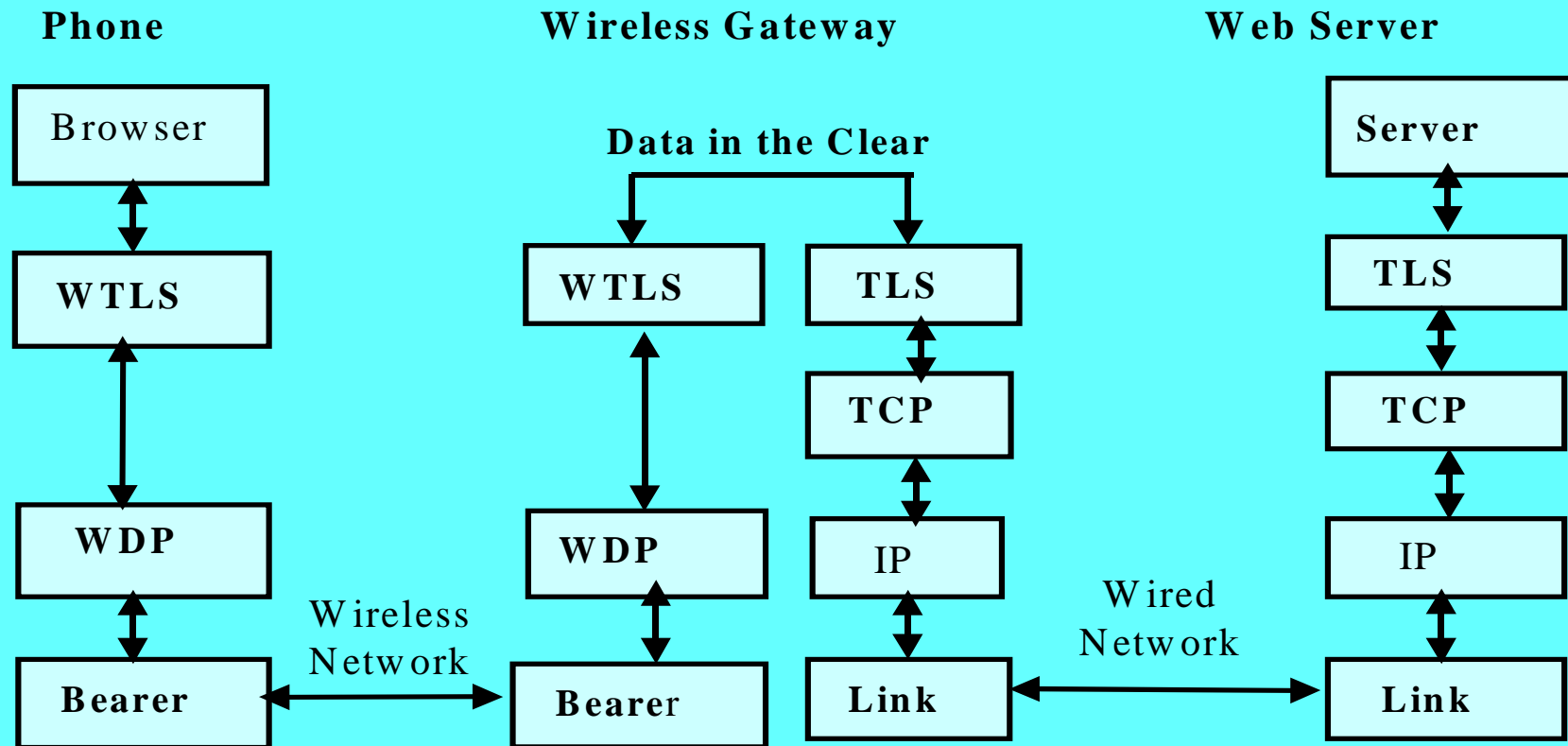
# Security Features in Proposed IPv6

- ❖ Support five security Standards published by IETF
  - ❖ RFC 1825 - Security architecture for the IPv6
  - ❖ RFC 1826 - IP Authentication Header
  - ❖ RFC 1827 - IP Encapsulating Security Payload (ESP)
  - ❖ RFC 1828 – IP Authentication using keyed MD5
  - ❖ RFC 1829 - The ESP DES-CBC Transform
- ❖ IP security association and authentication are combined to transmit IP packets
- ❖ IPv6 offers options for future expansion in authentication, data integrity, and confidentiality.

# Ultimate Goal: Mobile IPv6

- ❖ **Mobile IPv6** uses the improved IPv6 routing header, along with the authentication header. Other IPv6 functionalities are optimized to simplify routing to the mobile device
- ❖ **Mobile IPv6 applies no FA.** The mobile device uses an address auto-configuration feature in IPv6 to acquire a care-of-address on a foreign link.
- ❖ With the care-of address, a fixed correspondent can send packets directly to a mobile node using the **routing header**. Otherwise, a correspondent sends the packets, indirectly, thru the home network using **source routing**

# WTLS Stack over Wireless Gateway



## Wireless Transport Layer Security

# WTLS Service Classes

(M-Mandatory O-Optional, NA- Not applicable)

Functional Features	Class 1	Class 2	Class 3
Public-key exchange	M	M	M
Server certificates	O	M	M
Client certificates	O	O	M
Shared-secret handshake	O	O	O
Compression	NA	O	O
Encryption	M	M	M
MAC	M	M	M
Smart card interface	NA	O	O

# Wireless TCP (WTCP) for 3G Mobile Wireless Communications

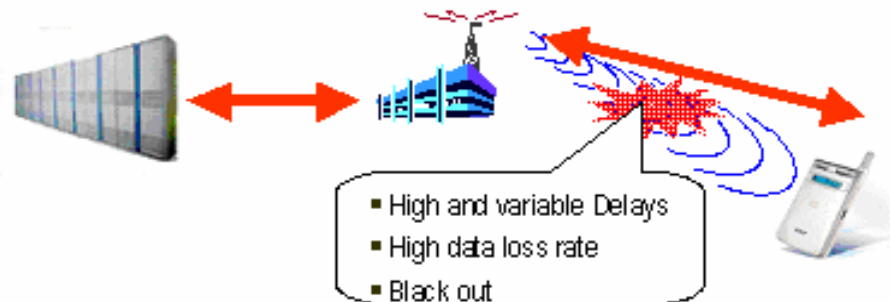
Mobile communication network  
= The integrated network of wired and wireless

- Wireless connection has long latency nature
- Wireless link highly interfered by environment

Need:

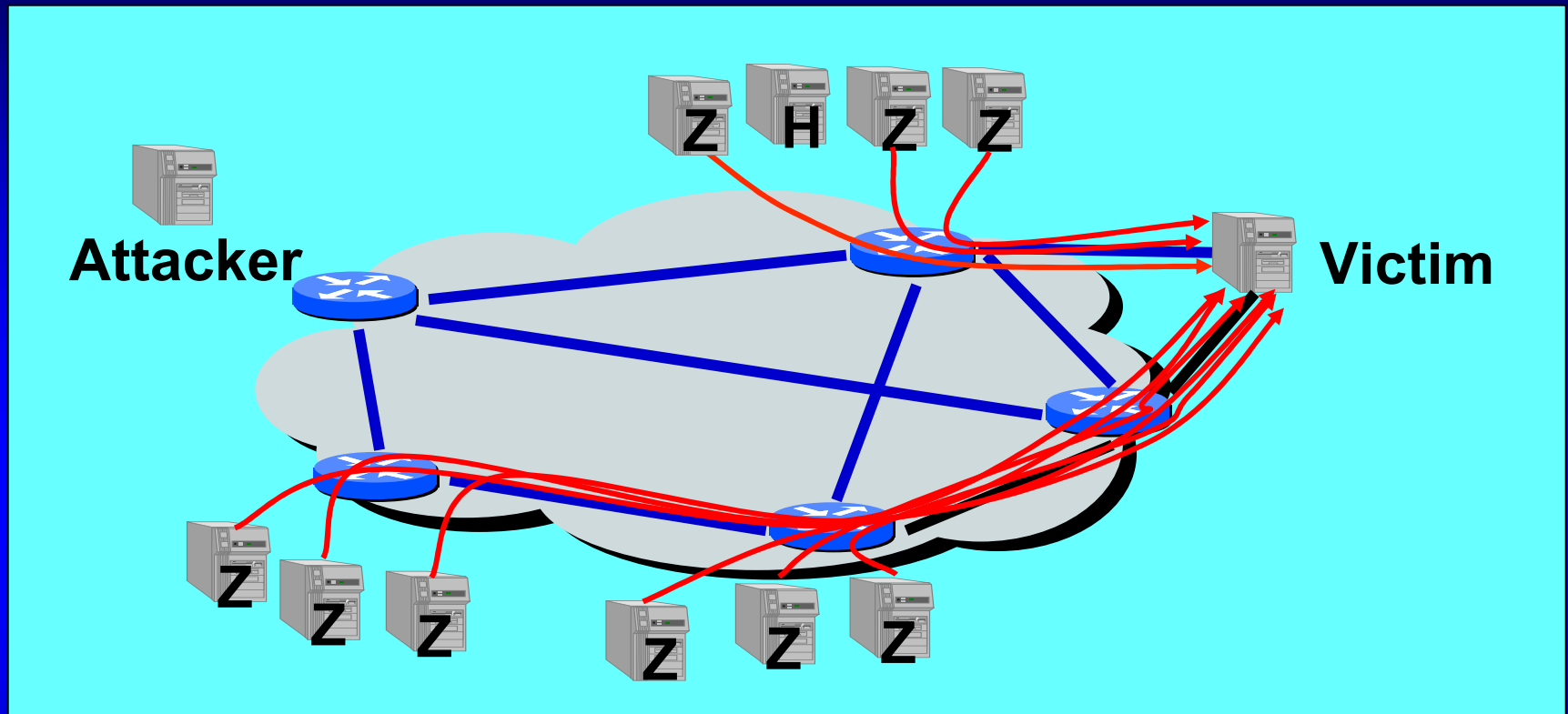
- Faster (re)connection
- Maintain stable link
- Keep High functionality  
And reliability
- End-to-end Transparency

W-TCP



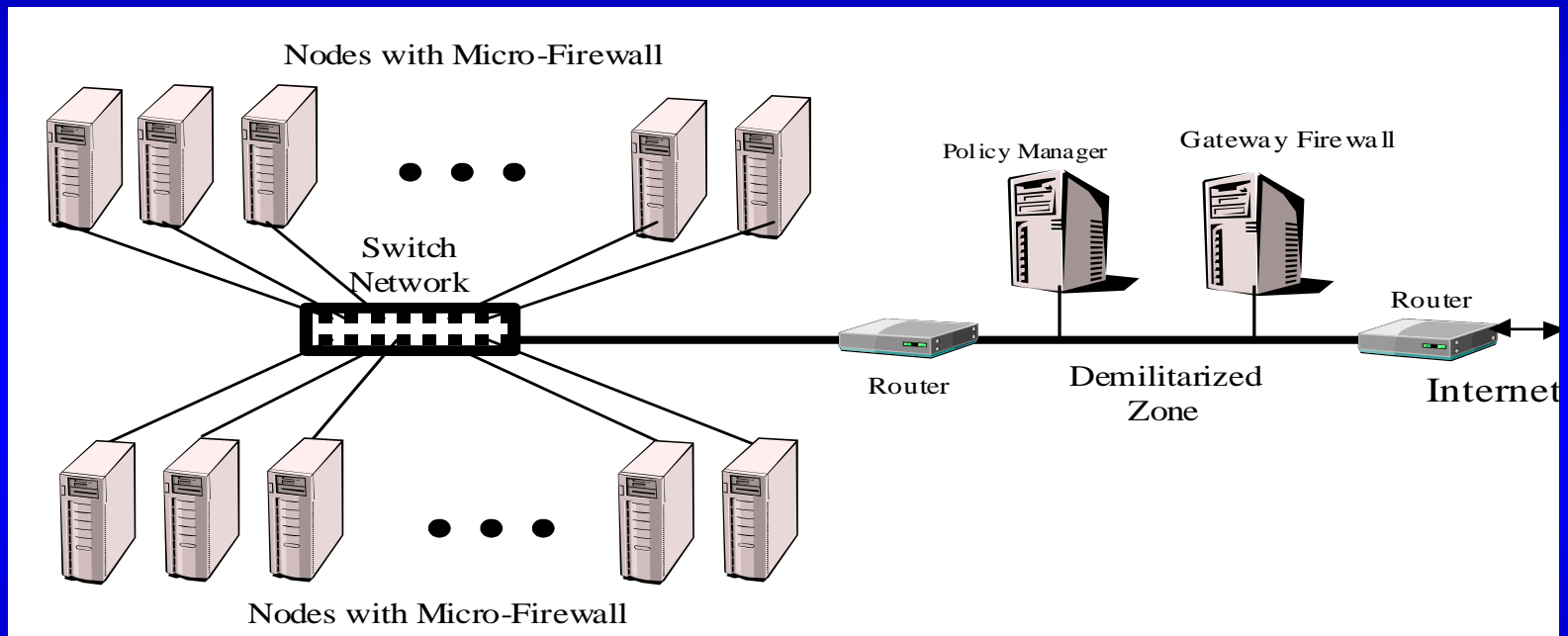
- ❖ IST International has implemented 11 WTCP algorithms on Linux servers
- ❖ Up-to-6 times of improvement achieved with a subset of the algorithms turned on

# Distributed DoS Attacks



1. Attacker infiltrates hosts and commands a handler (H).
2. Handler sends commands to zombies (Z).
3. Zombies attack the victim, damaging CPU, Memory and network resources.

# Clustered Security Testbed built at University of Southern California

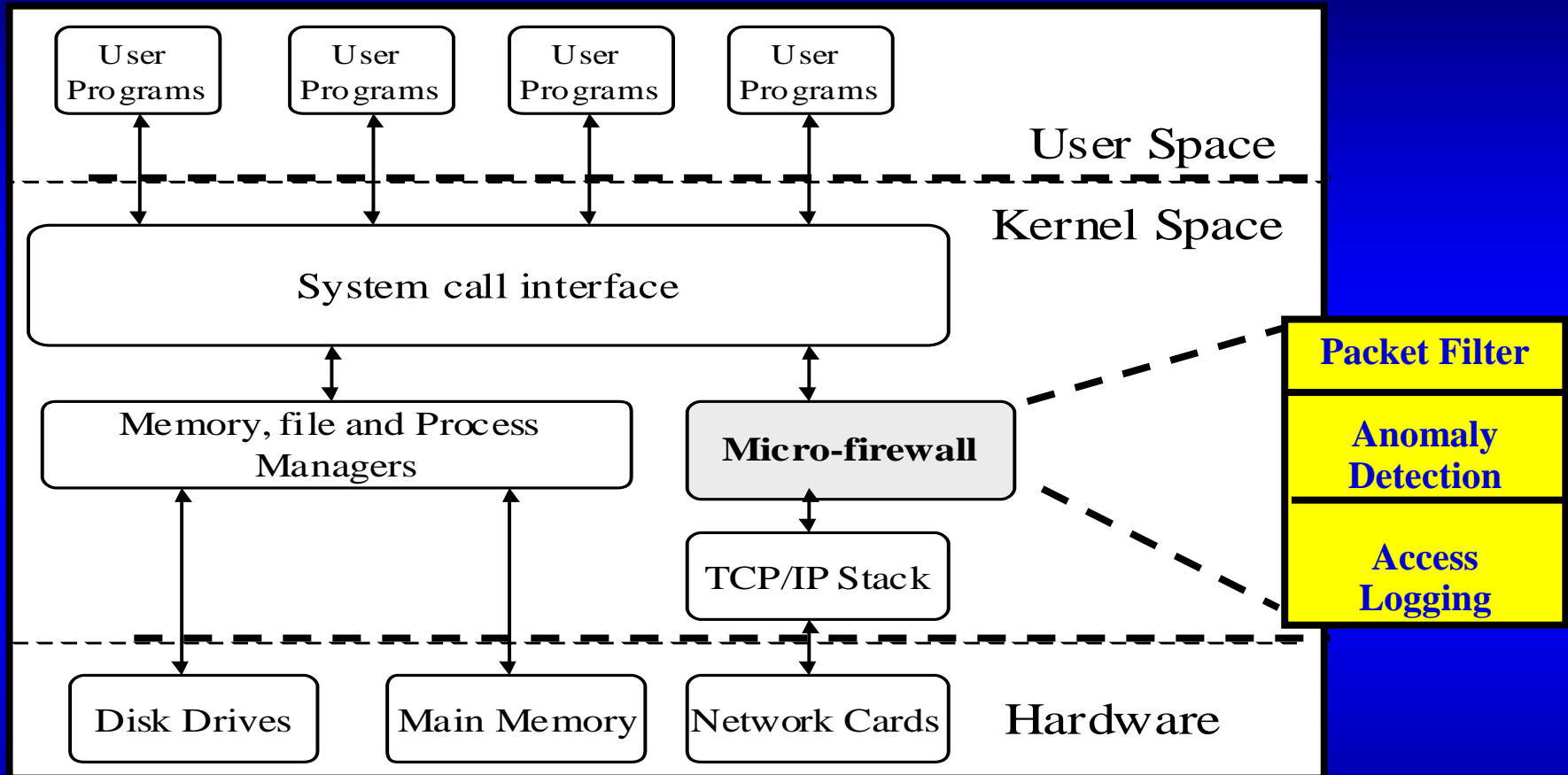


**Micro-Firewalls, Benchmark IDS, RADAR  
Scheme, and Trust Middleware for Developing  
Cost-Effective BCA and AAA Servers**

# **Securing Clusters and Intranets with AAA, Micro-Firewalls, XML, WPKI, and RADAR Technologies**

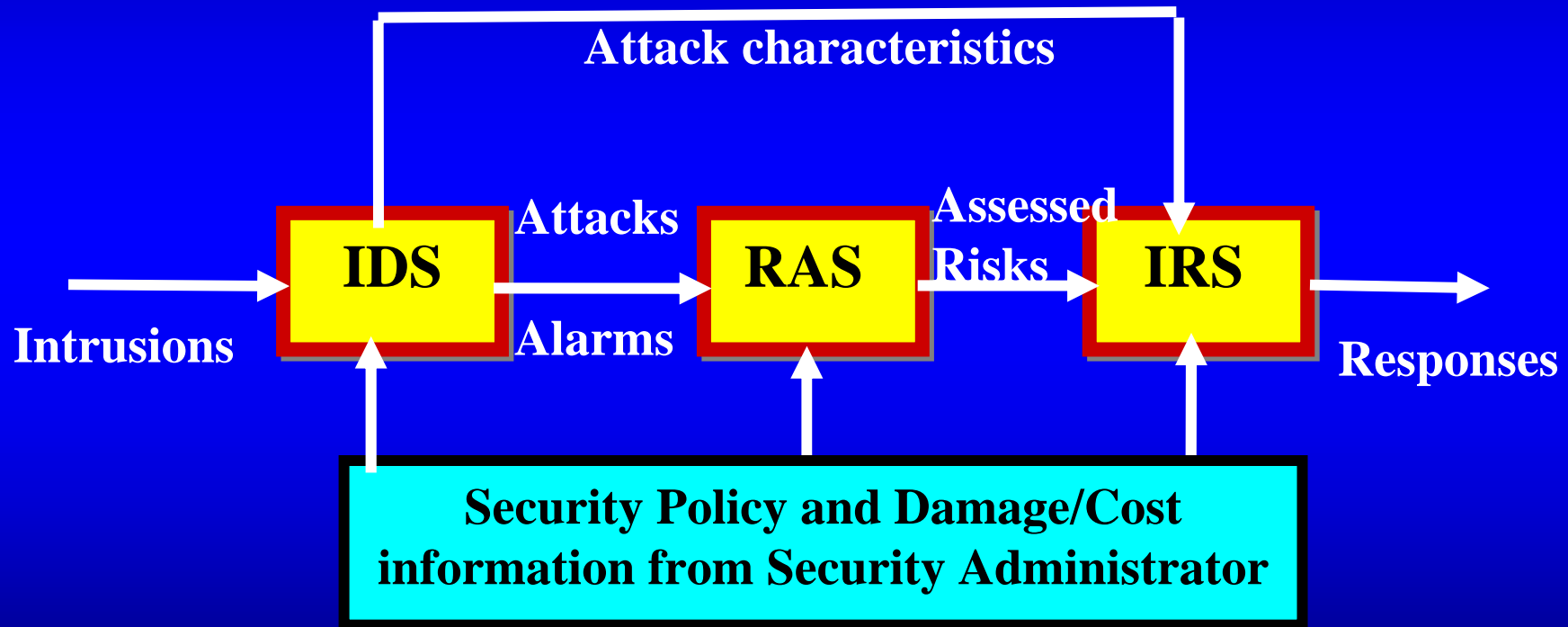
- **Distributed micro firewalls, IDS, and IRS built in the RADAR architecture at USC Labs.**
- **XML, RMI, CORBA, FTP, HTTP, SMTP, and Aglets evaluated for dynamic security updates**
- **Provide a full spectrum of VPN, pervasive, and grid-computing security infrastructures using the IPSec, XML, AAA, WPKI, and RADAR technologies**

# Implementing Micro-Firewall in The Linux Kernel



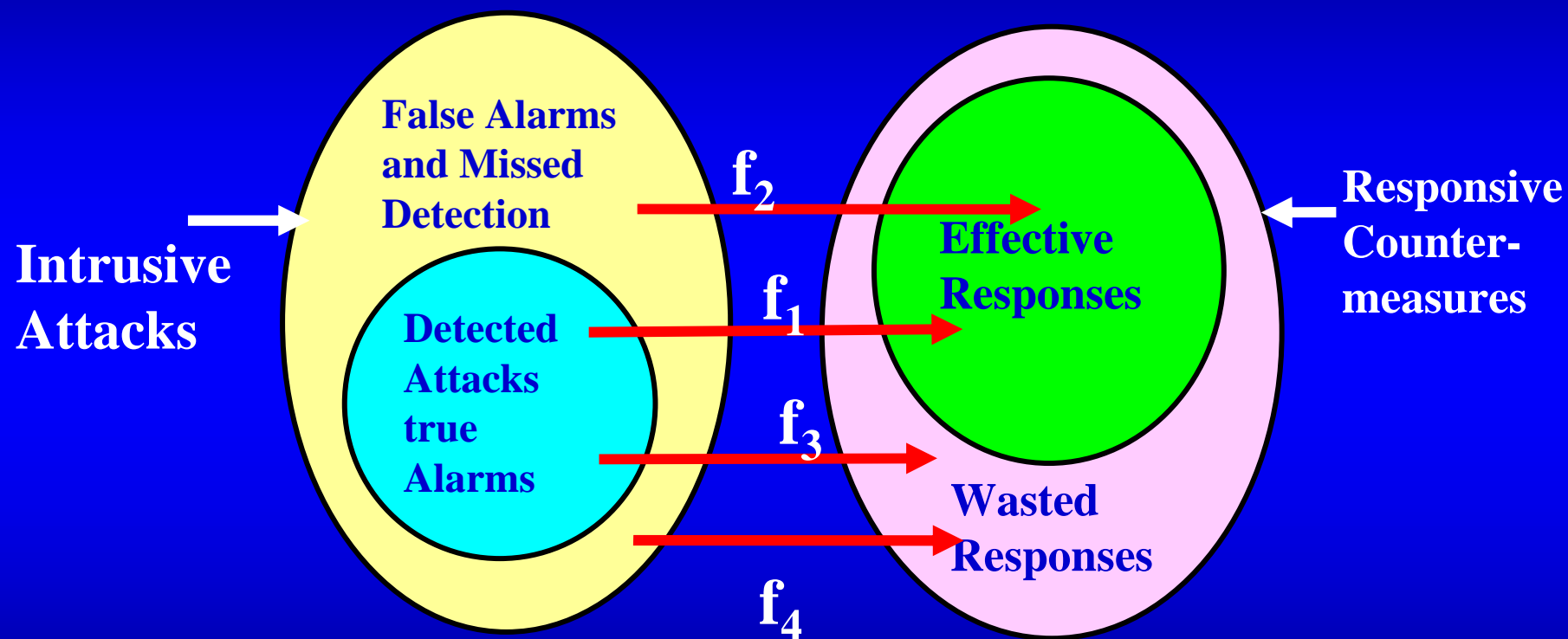
K. Hwang and M. Gangadharan, "Micro-Firewalls for Dynamic Security with Distributed Intrusion Detection", *IEEE International Symposium of Network Computing and Applications*, Cambridge, MA. Oct. 8-12, 2001

# RADAR: Risk Assessment for Intrusion Detection with Armed Response



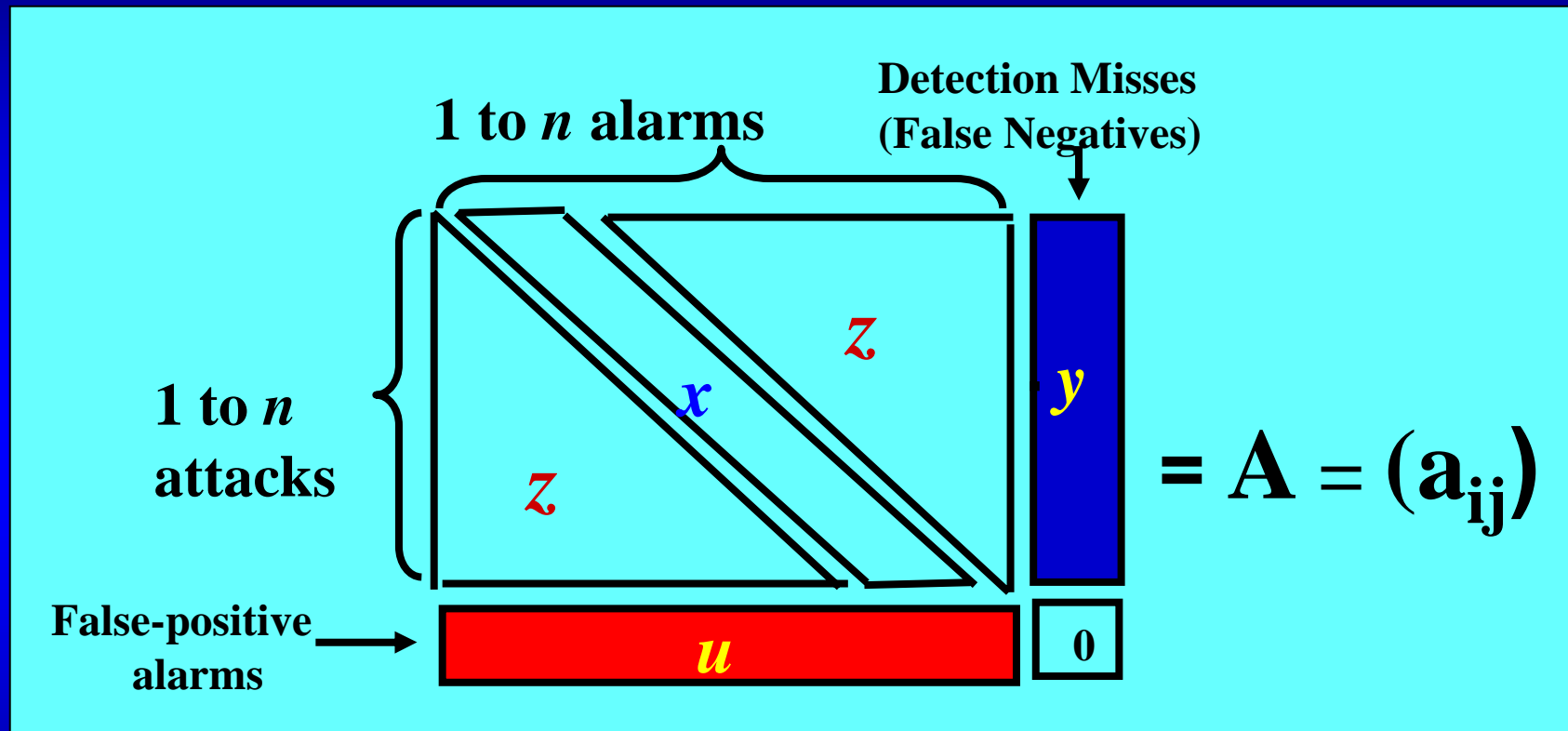
(**IDS**: intrusion detection system, **RAS**: risk assessment system, and **IRS**: intrusion response system)

# Set-theoretic Relationships between intrusive attacks and possible responses



Mappings  $f_1$  and  $f_2$  are desired,  
but  $f_3$  and  $f_4$  are not wanted

# Alarm Matrix from IDS Report



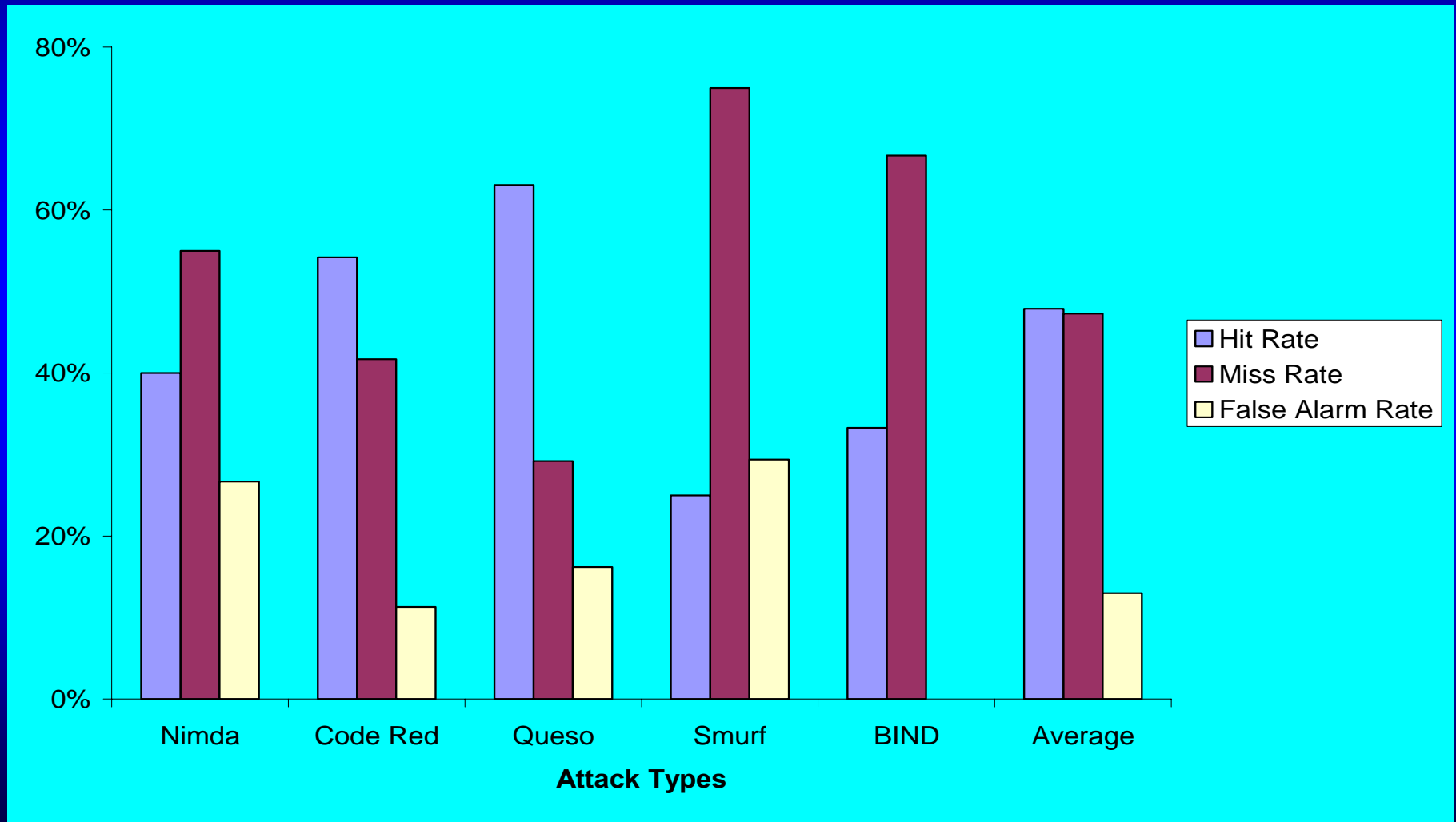
$x$  : Detection hits

$z$  : False Alarms

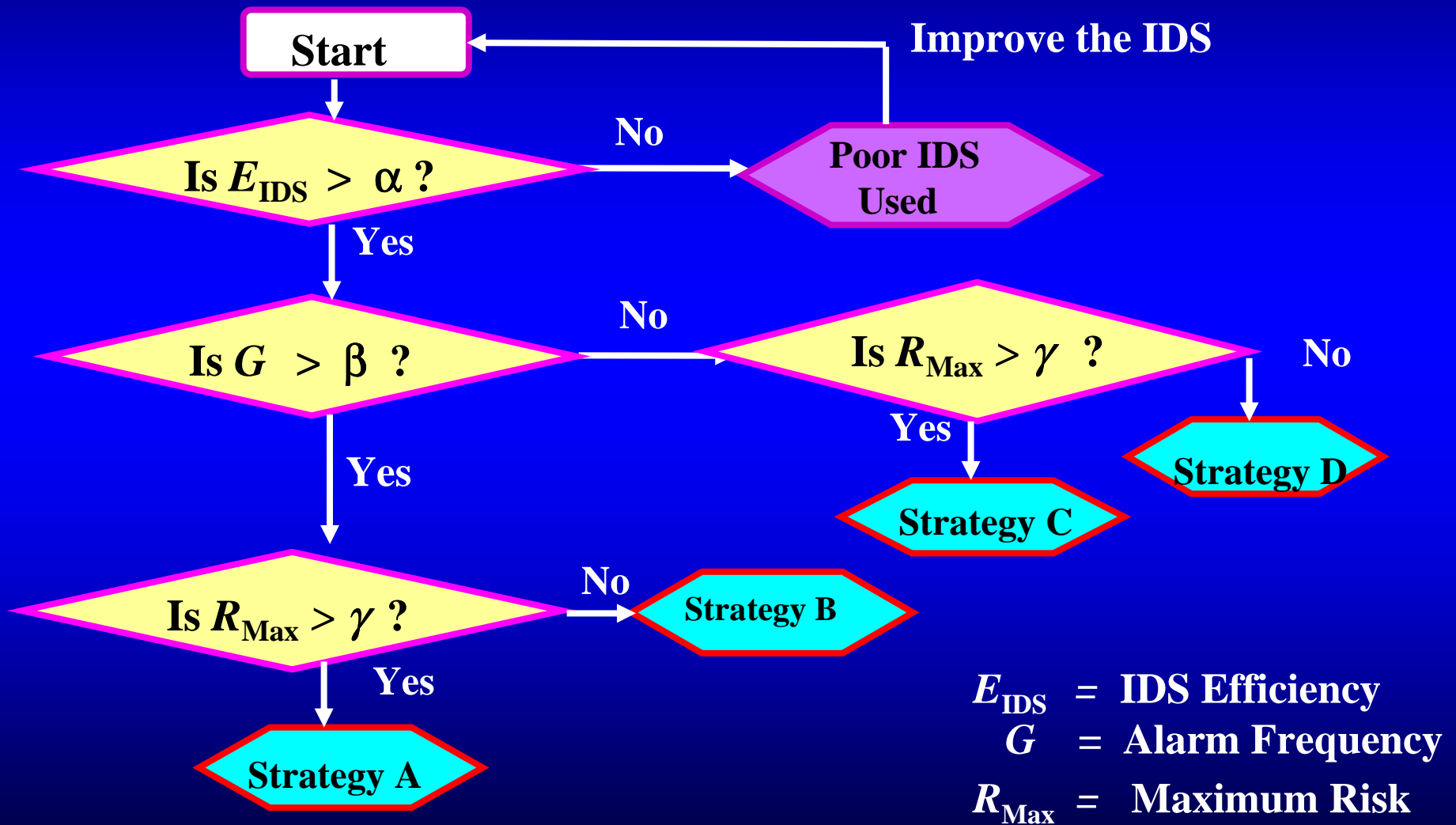
$y$  : False negatives

$u$  : False positives

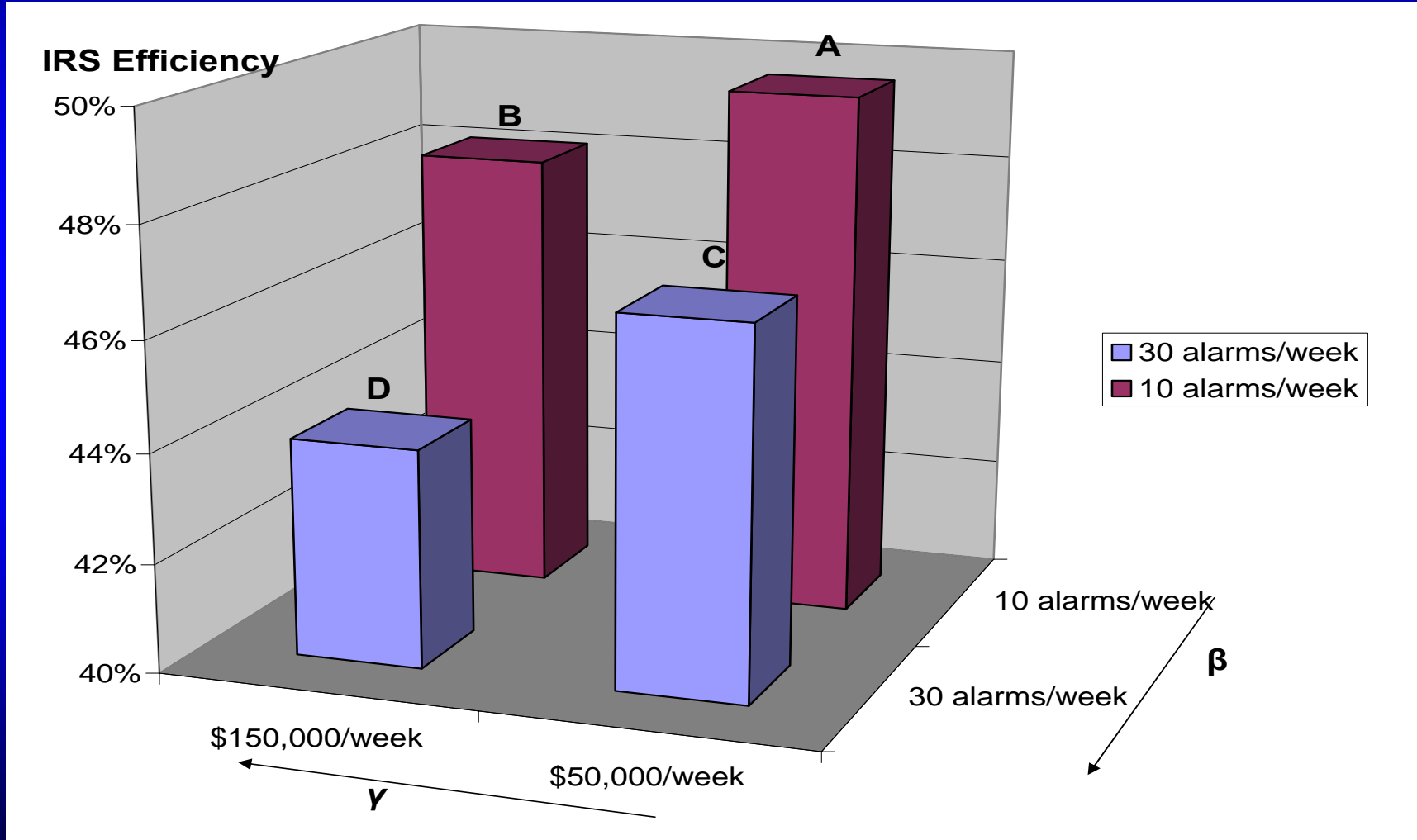
# IDS Performance of 5 Attack Programs on USC Linux Cluster



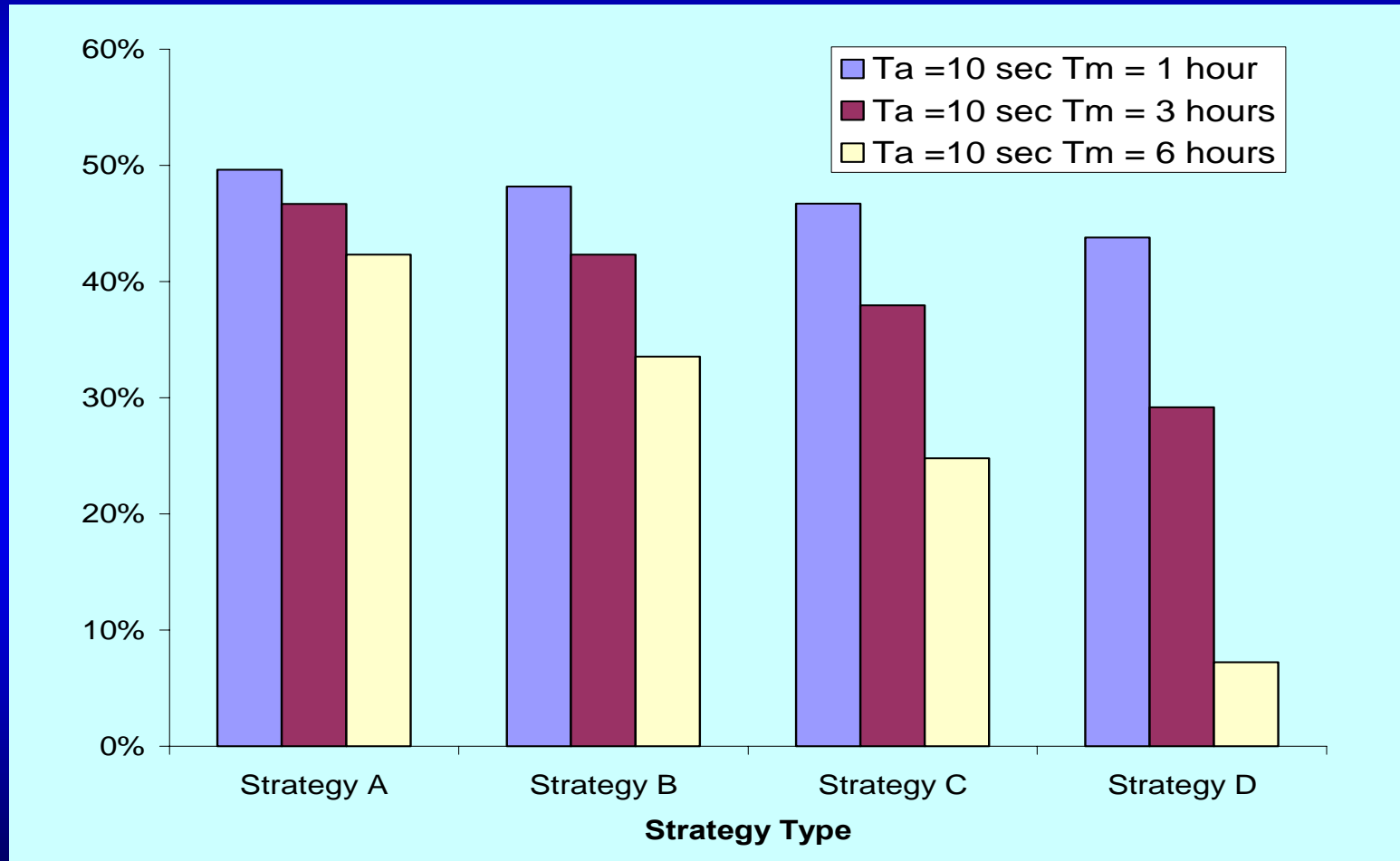
# Dynamic Selection of Intrusion Response Strategies



# Effects of Threshold in Selecting Intrusion Response Strategies



# IRS Efficiency for Different Intrusion Response Strategies



# Conclusions:

- ❑ **Wireless Internet security for M-Commerce relies on the successful deployment of Mobile IPv6, WTLS, WTCP, and WPKI**
- ❑ **WPKI architecture optimization and its interoperability with wireline PKI are the most challenging R/D tasks**
- ❑ **The RADAR scheme offers dynamic security policy update with respect to changes in threat patterns and network conditions**

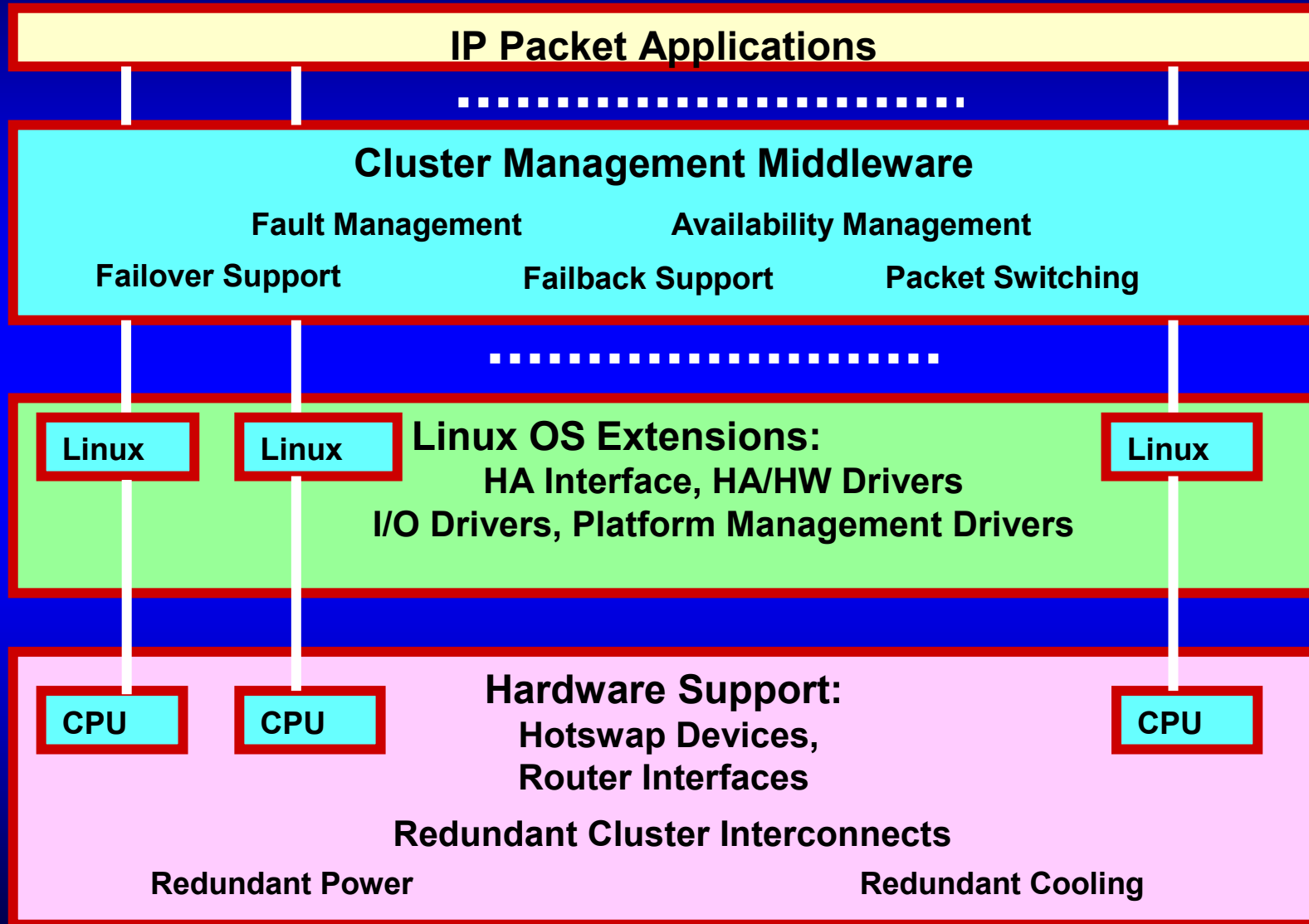
## Recent Papers and Presentation:

- ❑ K. Hwang, “Wireless PKI and Distributed IDS for Securing Intranets and M-Commerce”, Keynote Address, *IEEE Third Int’l Conf. On Parallel and Distributed Computing, Applications, and Technologies (PDCAT2002)*, Kanazawa, Japan, Sept.4-6, 2002
- ❑ K. Hwang and M. Gangadharn, “Micro-Firewalls for for Dynamic Security with Distributed Intrusion Detection”, *IEEE Int’l Conf. On Network Computing and Applications*, Cambridge, MA. Oct. 8, 2001
- ❑ S. Tanachaiwiwat, K. Hwang, and Y. Chen, ” Adaptive Intrusion Response to Multiple Network Attacks with Minimal Risk”, submitted to *ACM Transactions on Information and System Security*, August 19, 2002, (under reviewing).

# **Upgrading AAA to Secure Mobile Internet Accesses through Wireless Gateways**

- **Access equipment include SGSN, GGSN, FA, HA, or PDSN, which can be prototyped on the 3G wireless platform.**
- **To improves the AAA services with higher reliability, performance, and scalability in billing, auditing, and network planning.**
- **Must consider the interoperability issues including multi-vendor support, multi-access support, and multiple accounting record supports.**

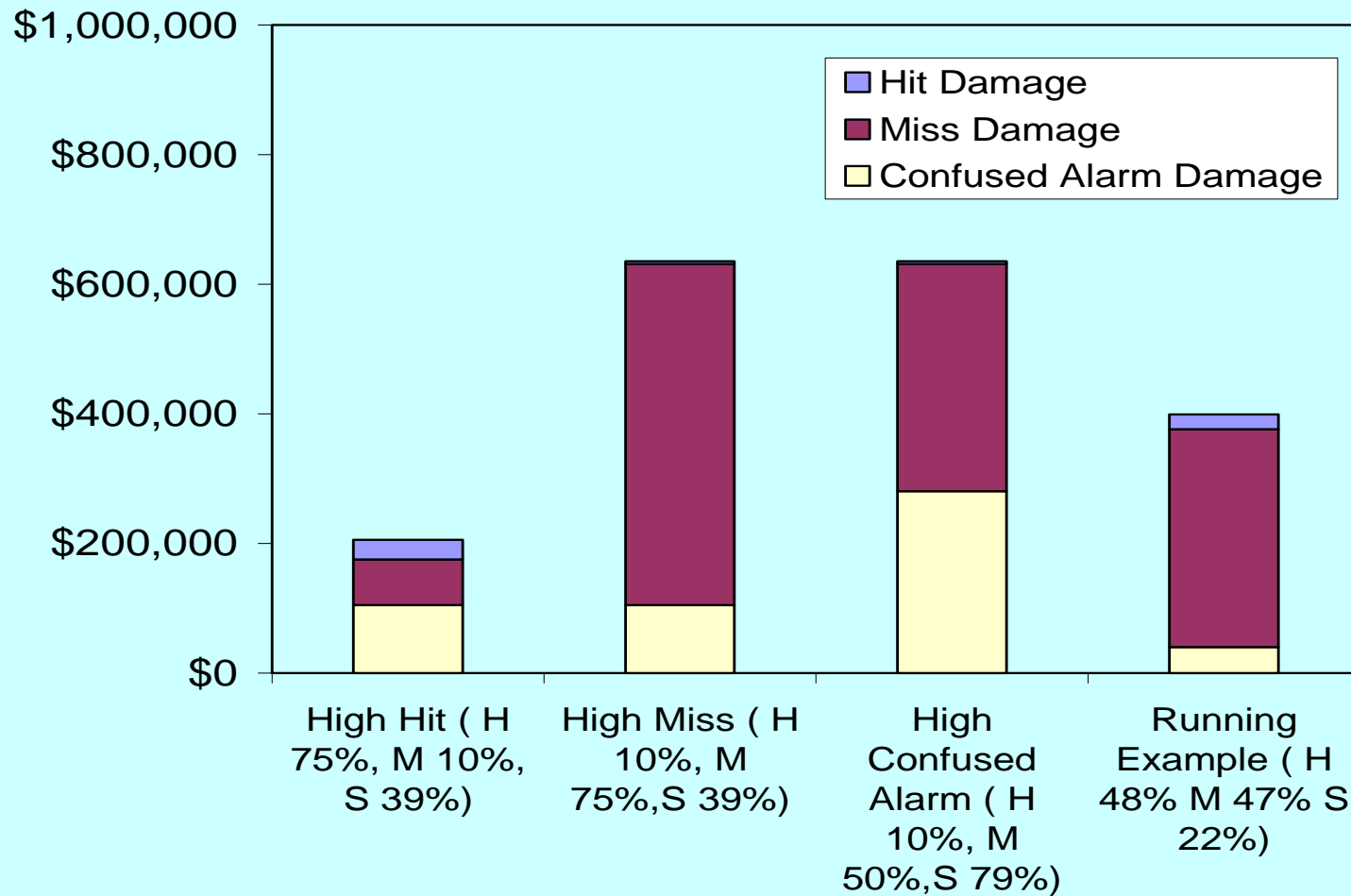
# Cluster Middleware, Linux Extensions, and Hardware Support of High-Security



# Design Choices of Bridge CA and Wireless PKI Portal at USC

Component	Vision	Operations	Standards
Bridge CA Cluster	Client Perspective	Certificate Issue, update, renew, and revoke	X.509 V3 certificate, WPKI certificate
		Client Certificate handling	PKCS #10
		Certificate status inquiry/response	OCSP, RFC2560
	Other PKI Perspective	Interact with other X.509 PKI	CMP, CMC
		Directory Certificate Publish	LDAP
PKI Portal	Client Perspective	Certificate request forwarding	PKCS#10
		Wireless certificate requests	WMLScript
		Client Certificate URLs in LDAP	LDAP
	Other PKI	Interact with X.509 PKI	CMP, CMC

# Residue Risk for 4 Attack Patterns



# Key Concepts of Mobile IP

- ❖ A mobile device has a home IP address residing in its home cellular network. When the device moves to a foreign network, it is given a care-of address
- ❖ The IETF (Internet Engineering Task Force) has proposed the Mobile IP as an interface between the home and foreign networks where the mobile device currently resides.
- ❖ Mobile IP is a protocol that keeps track the whereabouts and deliver the message to the device at its current location
- ❖ A mobile device at home applies the traditional IP in routing packets. When the device moves to a foreign network, the mobile IP is applied using the care-of address.