

# Software Encryption Initiative

29 April, 1997

Albert Kondi & Russell Davis

# Discussion Topics

- Current Reserve Component Automation System (RCAS) architecture
- How a software approach increases security
- Security Protocols

# The RCAS Mission

The RCAS mission is to provide the Army Reserve Component (RC) with an integrated information delivery system with data and application systems that will support day-to-day operations and mobilization functions for the Army National Guard (ARNG) and the U.S. Army Reserve (USAR).

# The RCAS

- The RCAS consists of a classified up to Secret and sensitive but unclassified (SBU) subsystem
- Today's presentation is limited to the SBU subsystem
- The Sites range in size from a single workstation to a small, medium, or large site

# Current RCAS Environment

- Data Encryption Standard (DES) performed at the router interface (gateway) implemented in hardware
- No information on the Local Area Network (LAN) is encrypted
- Protection is network facing
- The network is not transparent to the user

# Current RCAS Environment

(continued)

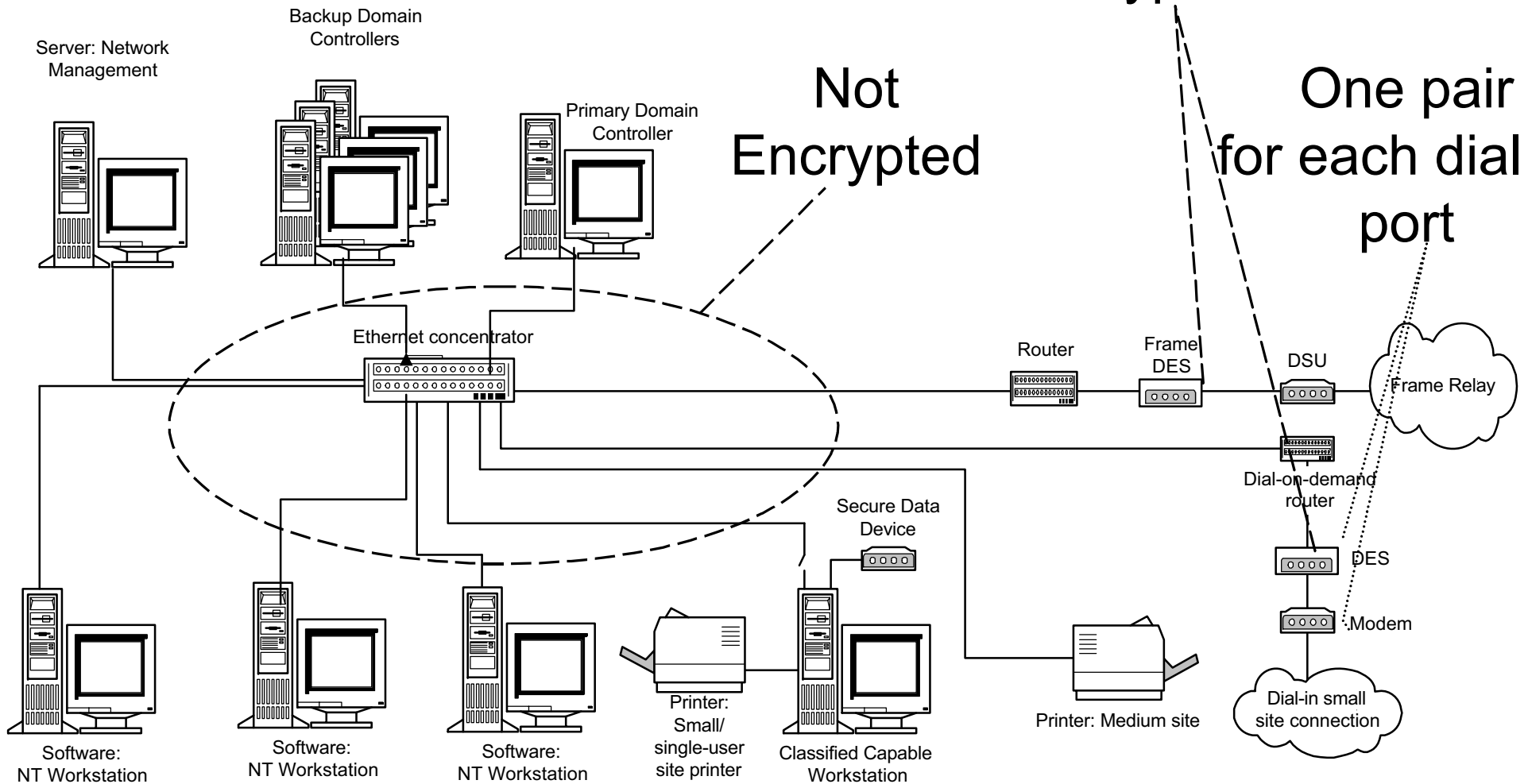
- Transition glide path to the Defense Message System (DMS)
- The user owner of the information cannot exercise options for protection
- Protection for his or her information is a difficult problem to solve

# Large Site Configuration

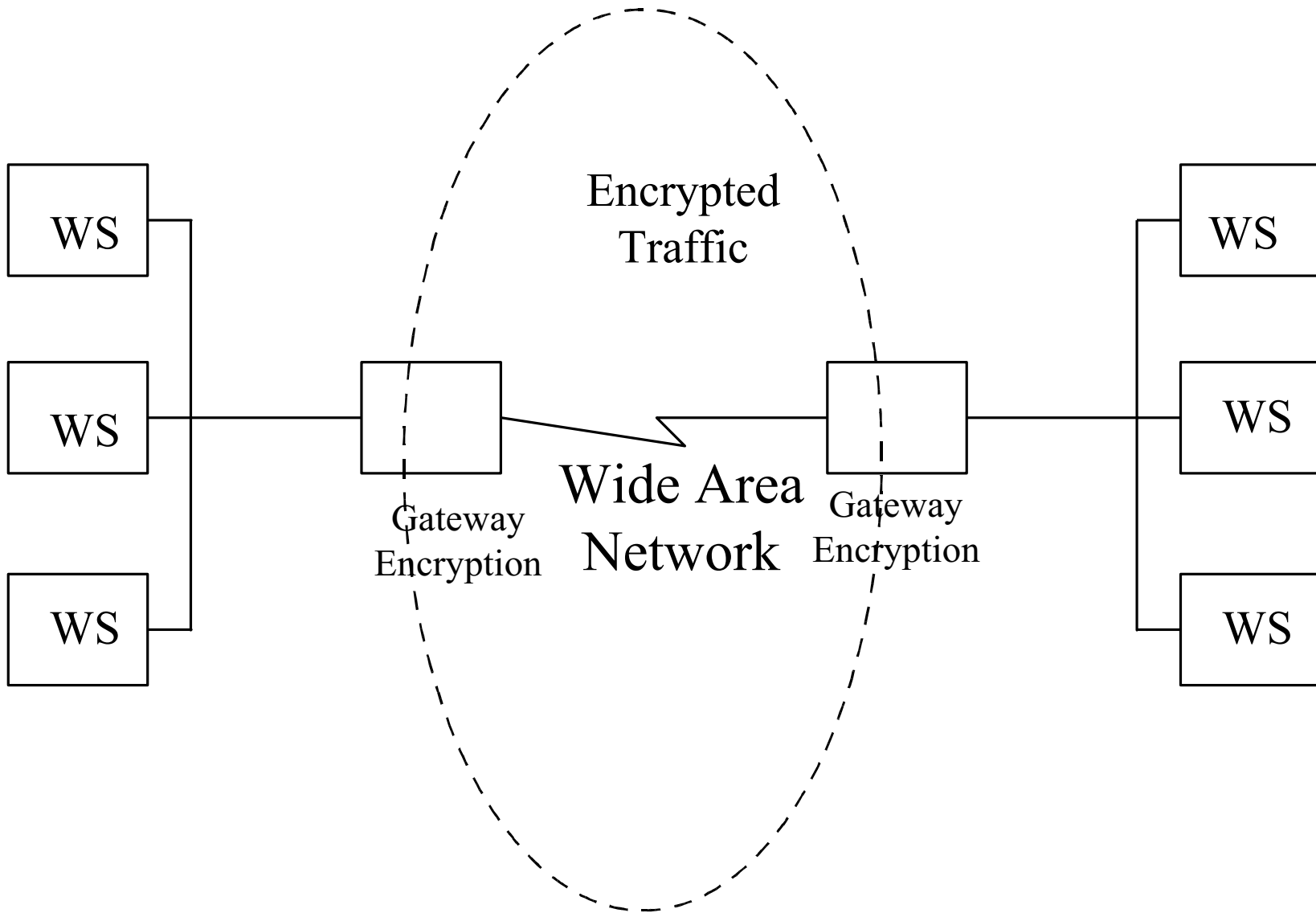
Existing Hardware Encryption

Not Encrypted

One pair for each dial in port



# Current Baseline



# What's Wrong With This Picture

- Hardware implementation of DES provides no security at the low level
- Hardware implementation is an affordability problem
- How would key management be accomplished across the wide area network?

# What's Wrong With This Picture (continued)

- How is interoperability accomplished in a joint environment?
- Hardware results in vendor dependence (no free and open competition)

# Alternatives

- Hardware Encryption
  - Fortezza (SKIPJACK 80-bit key)
  - DES (56-bit key - Current RCAS solution)
- Software
  - DES (56-bit key)
  - Triple-DES (112-bit Key)
  - Advanced Encryption Standard

# How Software Improves Security

- Software will encrypt all traffic before it enters the LAN
- It is possible to encrypt Standard Army Management Information System (STAMIS) environments
- Each session will utilize a unique and new encryption key for a single session

# Microsoft Windows NT

- Microsoft Windows NT version 3.5 was evaluated by the National Computer Security Center (NCSC) and rated class C2
- The Final Evaluation Report, dated 1 March 1995, indicated that the B2 Trusted Path and the B2 Trusted Facility Management requirements were also satisfied.
- The current version of Windows NT (4.0) is undergoing evaluation by the NCSC

# FIPS Pub 140-1

- Applicability. “This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect unclassified information within computer and telecommunications systems”
- “This standard shall be used in designing, acquiring and implementing cryptographic-based security systems”

# FIPS Pub 140-1

(Continued)

- The FIPS defines four increasing, qualitative levels of security (Level 1, 2, 3, & 4).
- Security Level 2

“Level 2 also allows software cryptography in multi-user time shared systems when used in conjunction with a C2 or equivalent trusted operating system”

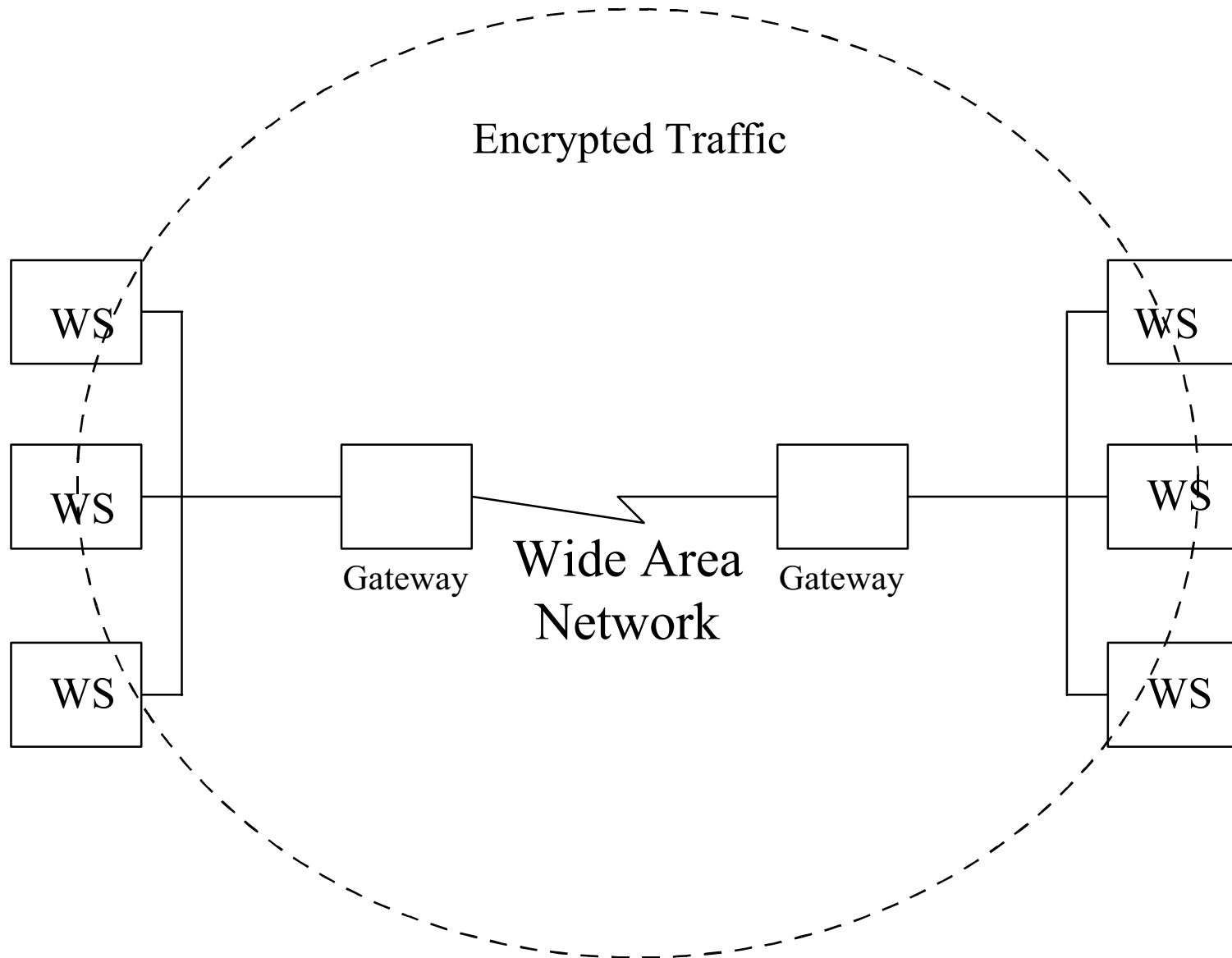
# Software Encryption Advantages

- Affordable
- Supportable
- Interoperable with the Fortezza (on the DMS glide path)
- Compatible with direction of DMS, COE, JTA, and ATA
- Combines COMSEC and COMPUSEC resulting in information systems security

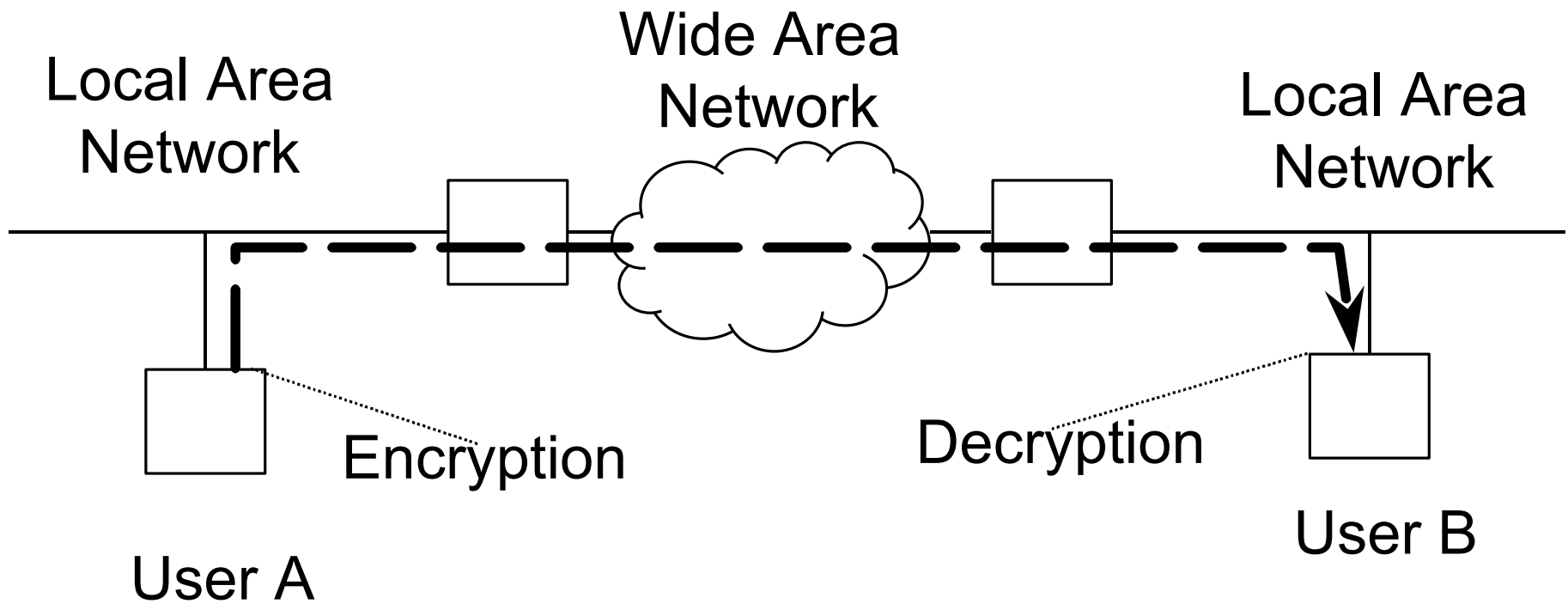
# Software Encryption Advantages (continued)

- Provides LAN security in open systems
- Provides transparent user protection
- Eliminates maintenance and the sustaining of hardware devices
- Decreased network traffic due to compression

# User-to-User Security

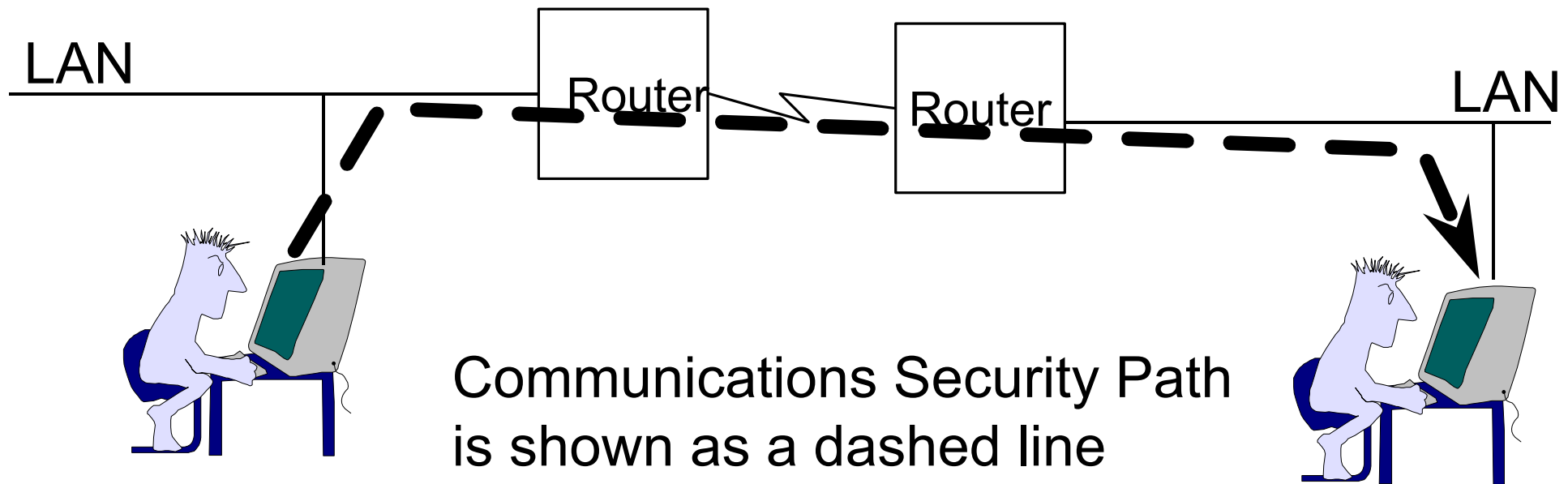


# User-to-User Security



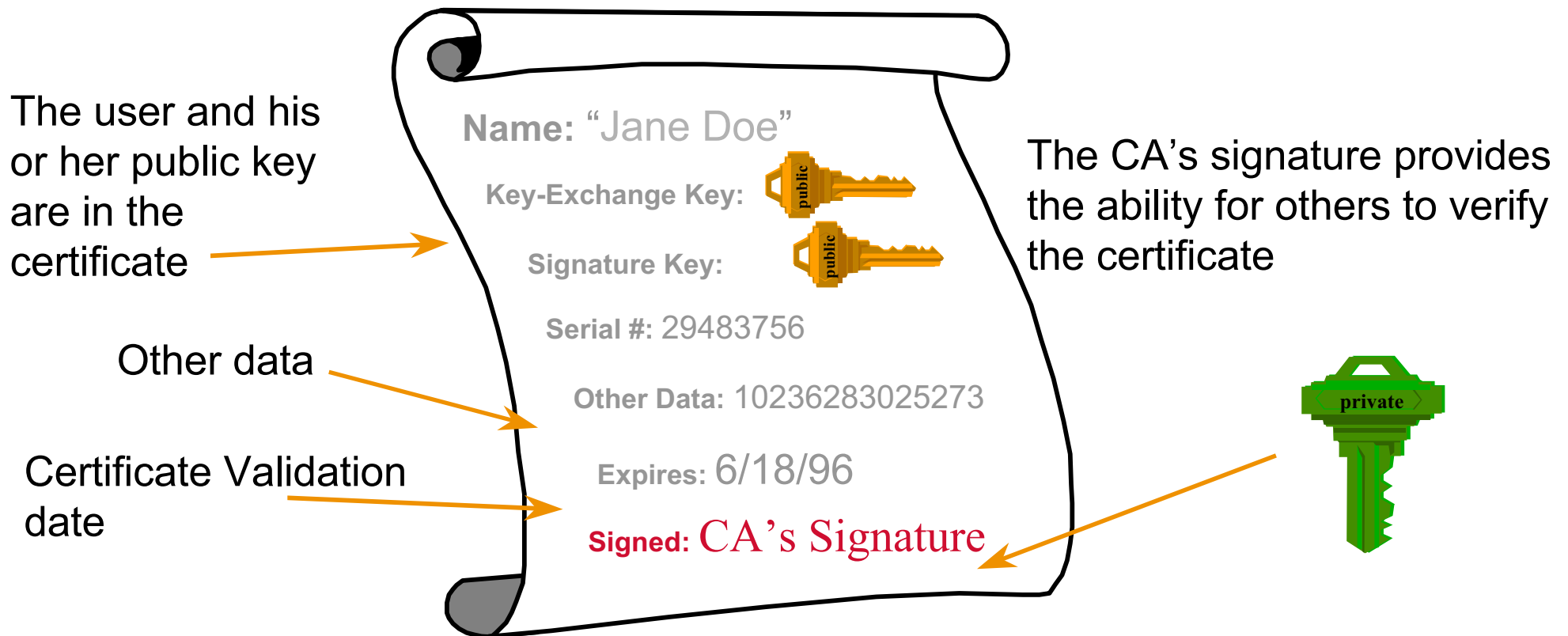
# Session Security

- Certificates contain public key component
- Public key is used for authentication and/or key exchange
- A DES session key is generated for each session
- There is no easy method for cracking DES

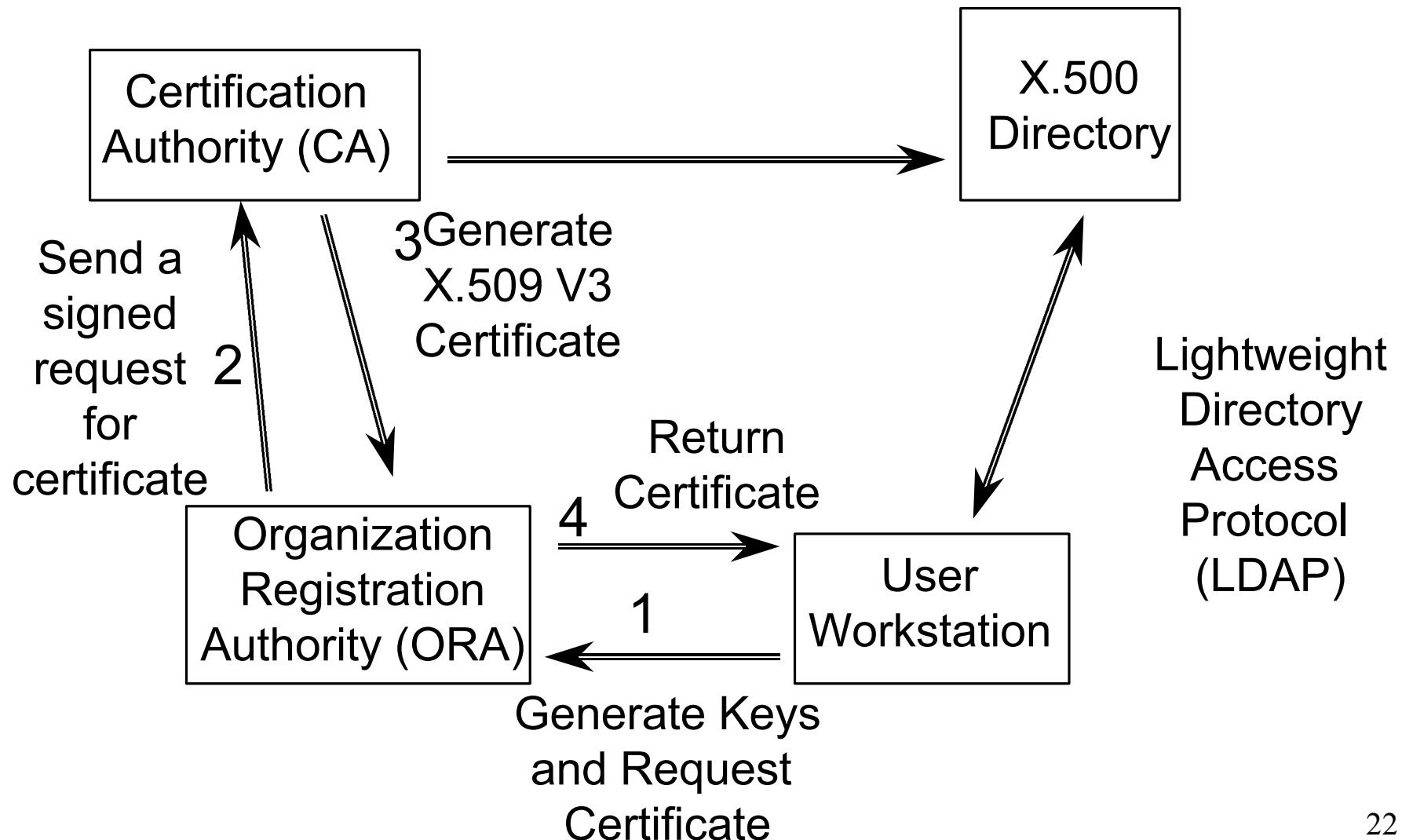


When using a C2 operating system, software encryption provides a low risk alternative to hardware encryption.

# What is a Certificate



# Public Key Infrastructure



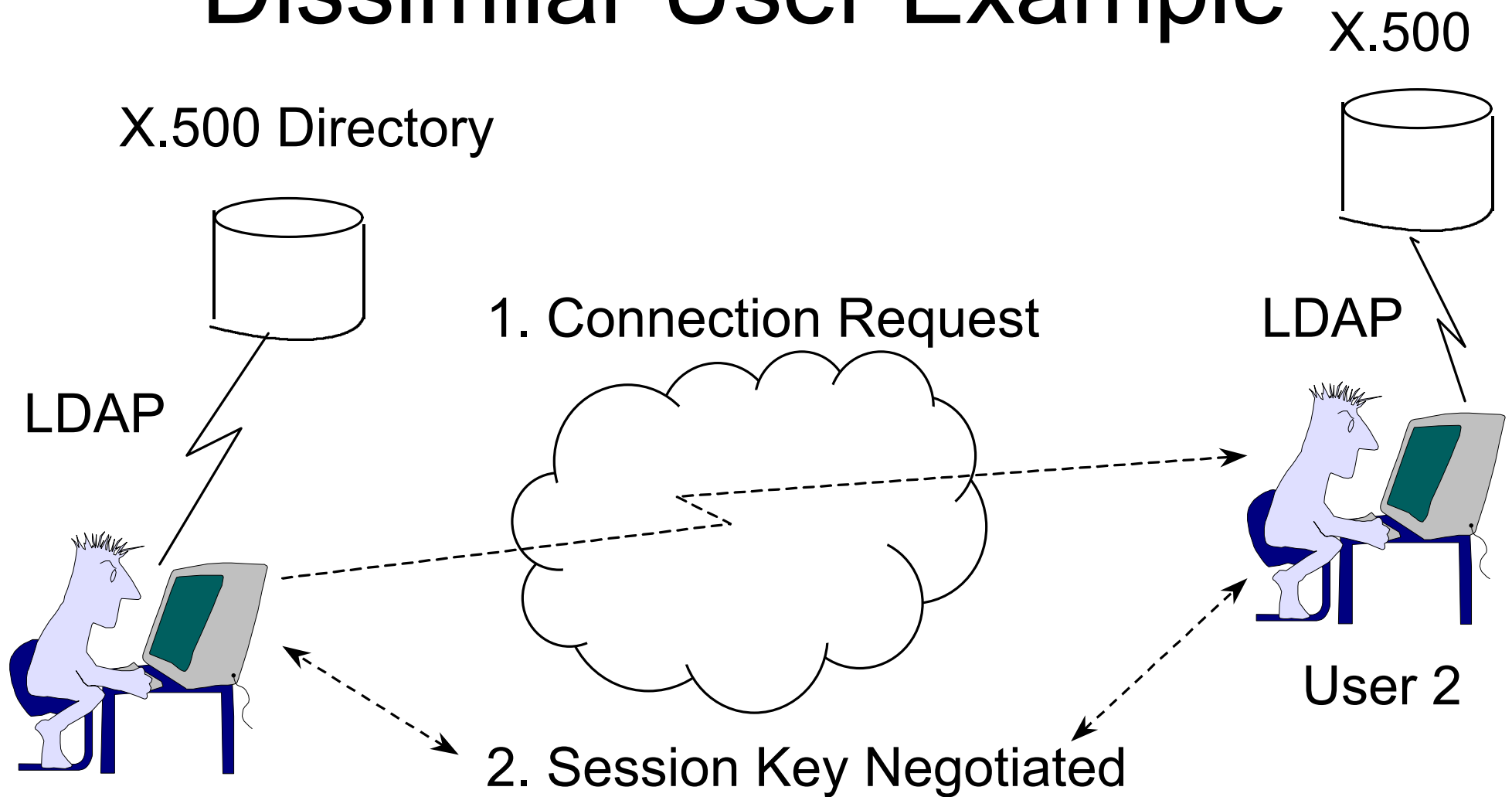
# Key Management

- The next Certificate Authority Workstation (CAW - part of the Defense Messaging System) will work with X.509 V3 certificates, thereby allowing software implementations to use the CAW.
- Public Keys are distributed in the form of X.509 V3 certificates.
- Unlike hardware based key management, the software approach is transparent to the users.
- Microsoft will introduce a certificate server this quarter.

# Key Management (Continued)

- Netscape has a UNIX certificate server and will introduce an NT certificate server.
- Certificates are normally cached locally on the workstation.
- Non-cached certificates can be obtained using Lightweight Directory Access Protocol (LDAP) products which access X.500 directories.

# Dissimilar User Example



User 1

Note: If User 2 Does Not Have 1's Certificate,  
Then It Is Pulled From The X.500 directory.

# Advanced Encryption Standard

- On 2 January, 1997, the NIST placed a request for comments for the Advanced Encryption Standard (AES)
- The AES will eventually replace the Data Encryption Standard (DES)
- A NIST requirement is that the AES must be implementable in software
- Software provides an easy upgrade path

# Escrowed Encryption

- The NIST Escrowed Encryption Standard (EES) allows Fortezza to be used for unclassified encryption
- Professional organizations, such as the Association for Computing Machinery, are publicly opposed to the EES
- There are ongoing efforts in Congress to have the EES removed as a mandatory standard
- If rescinded, the current Fortezza card would have to be upgraded to something new

# Software Encryption Approaches

- IPsec - Listed in the Army Technical Architecture (ATA) and the Joint Technical Architecture (JTA) under emerging standards
- SSL - Fortezza enabled Netscape Web implementation currently available
- CAPI - Microsoft Crypto API forces encryption to be done within the operating system (a Fortezza CAPI is available)

# IPSec

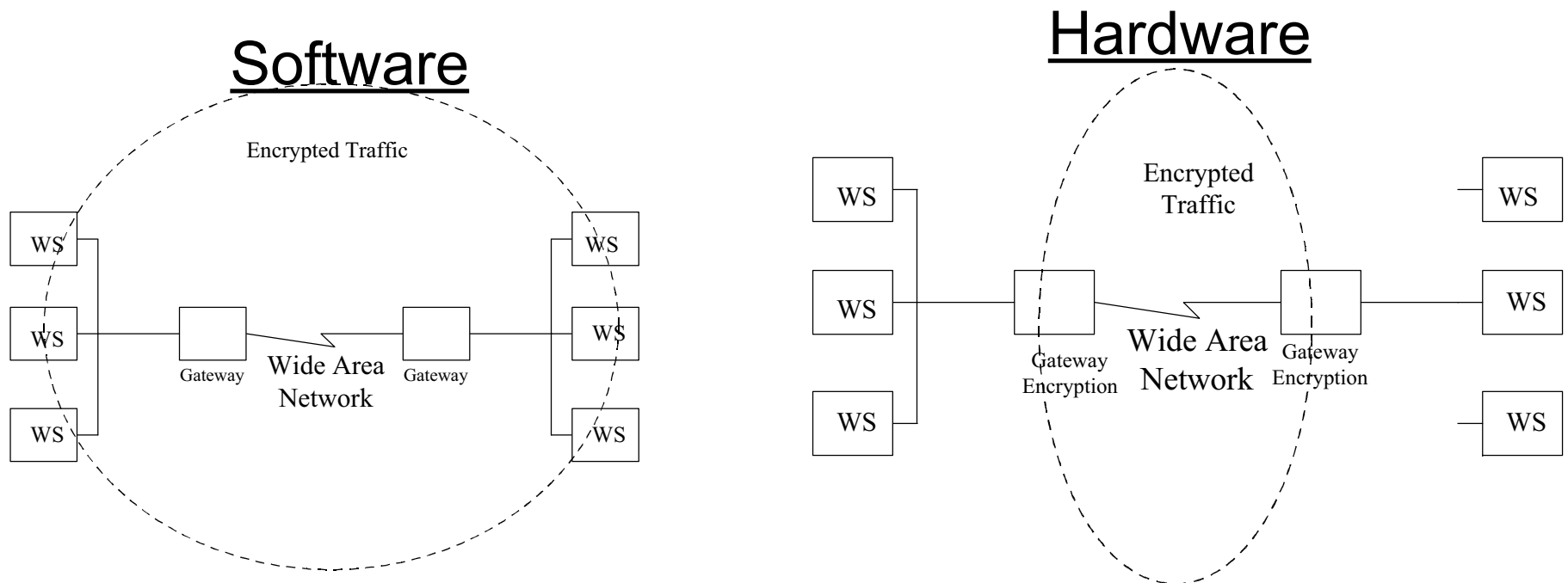
- Is mandated for IP version 6
- DOD, Office of Information Security Research, has made available its Internet Security Association & Key Management Protocol (ISAKMP) key management protocol for use with IPSec
- Different types of encryption can be performed using this protocol

# Progress To Date

- The RCAS Program Management Office (PMO), with support from the Program Executive Office
- The Army has approved the RCAS PMO request to defer further fielding of the hardware encryption pending resolution of software encryption of selection of a standard architecture

# Summary

Software offers an affordable, supportable, and Interoperable alternative to hardware encryption



What is a necessary condition is commitment on the part of our leaders to specify software as an acceptable alternative to hardware encryption

# Questions

Albert Kondi  
RCAS PMO  
8510 Cinder Bed Road  
Suite 1000  
Newington, VA 22122-8510  
(703) 339-9323

Russell Davis  
Boeing IS Inc.  
MS CV-84  
7990 Boeing Court  
Vienna, VA 22182