

Secure BlackBerry



Robert Nowak
V34,
Wired/Wireless
Applications

BlackBerry

- BlackBerry proved its value on 9/11
 - System latency negligible
 - More bandwidth used in 1 two min. cell call than 1 month of BB messages
- Fast becoming the PDA platform of choice in DoD

BlackBerry

- Unclassified information in aggregate extremely valuable
 - USS Coca-Cola
- During crisis situation system became “unauthorized” perishable secret channel

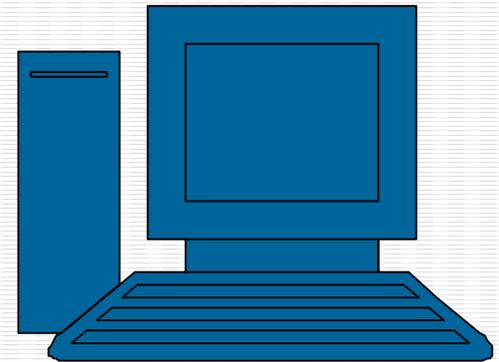
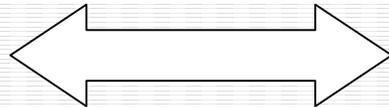
Crypto BlackBerry

- NSA and RIM formed a cooperative effort to enhance the general security of the:
 - Handheld Device
 - BlackBerry Enterprise Server
 - BlackBerry Desktop
- Crypto BlackBerry Coined

BlackBerry

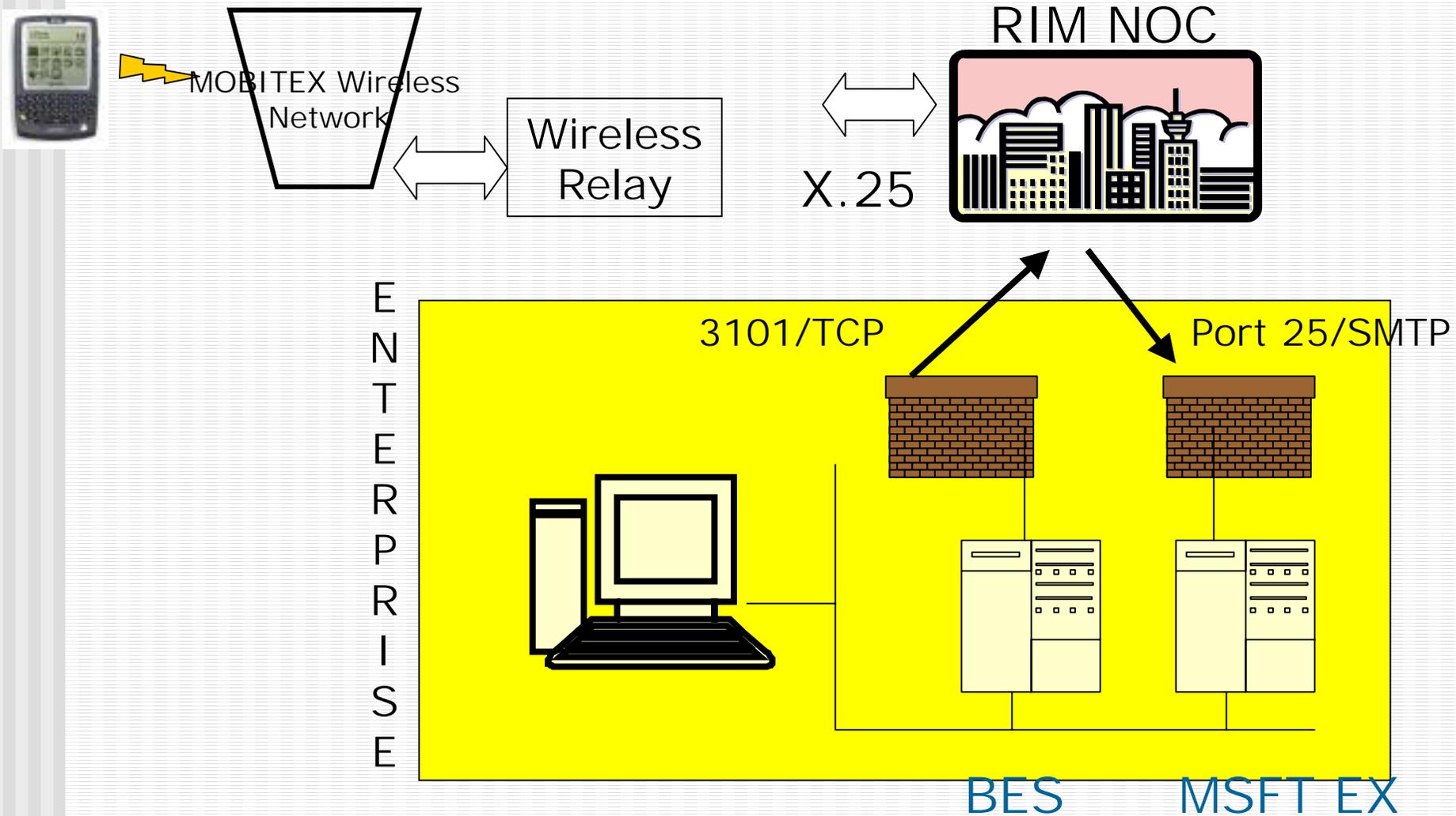
- 2 General Classes of Vulnerabilities identified in BB for DoD use
 - Standard RF Vulnerabilities
 - NSA Solution DOES NOT address RF Vuls.
 - Policy Enforcement and End user Education
 - Network Vulnerabilities
 - NSA Solution Does NOT address “normal” Wired Network Concerns
 - OS Hardening, Firewall Mgmt etc.

BlackBerry



Emails are forwarded between
The handheld and the enterprise

BlackBerry Architecture



BlackBerry

System
Vulnerabilities

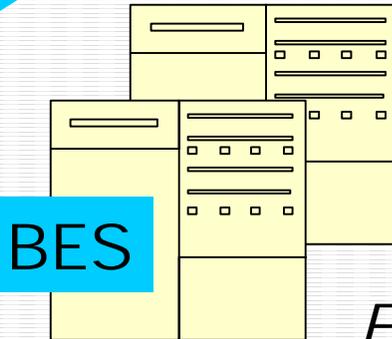
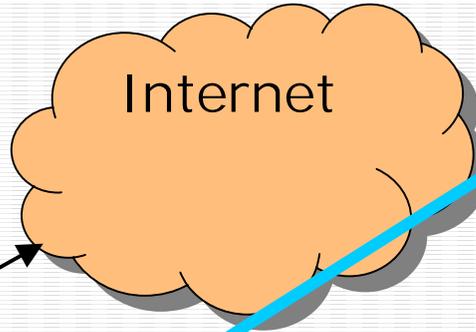


Crypto BlackBerry
Approach

BlackBerry

2 Versions:

Internet Version



Enterprise Edition

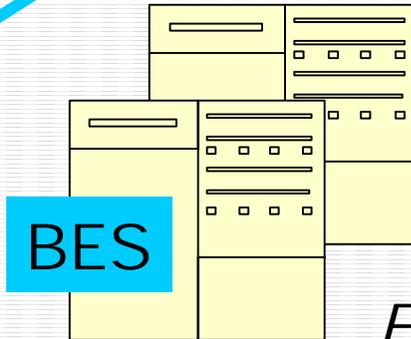
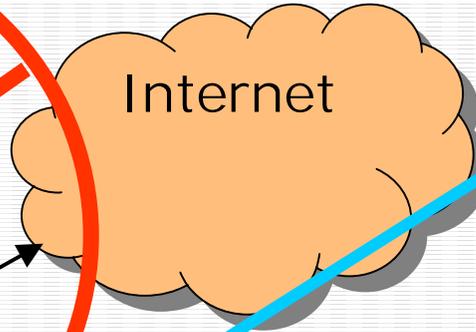
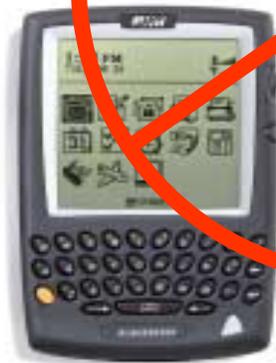
CRYPTO BlackBerry

Not Authorized

2 Versions:

Internet Version

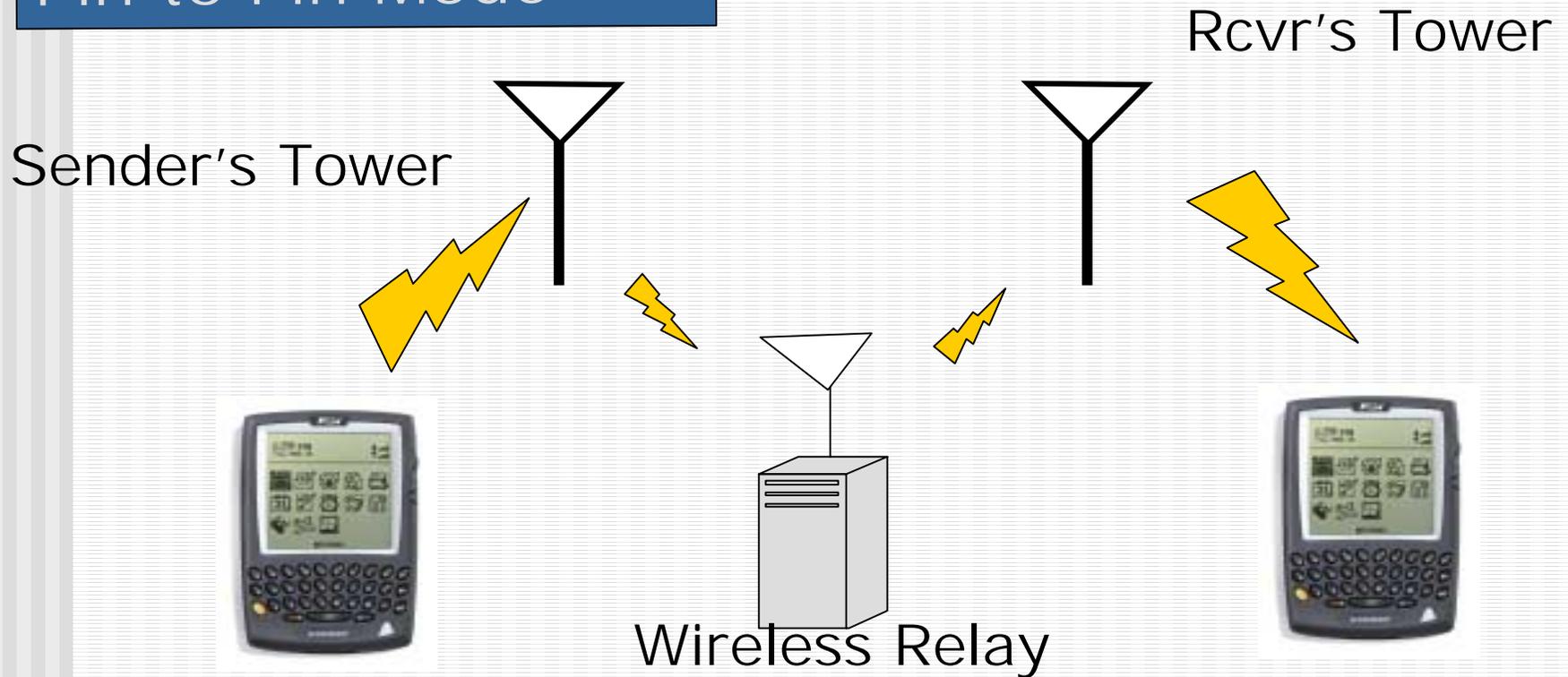
Internet



Enterprise Edition

BlackBerry

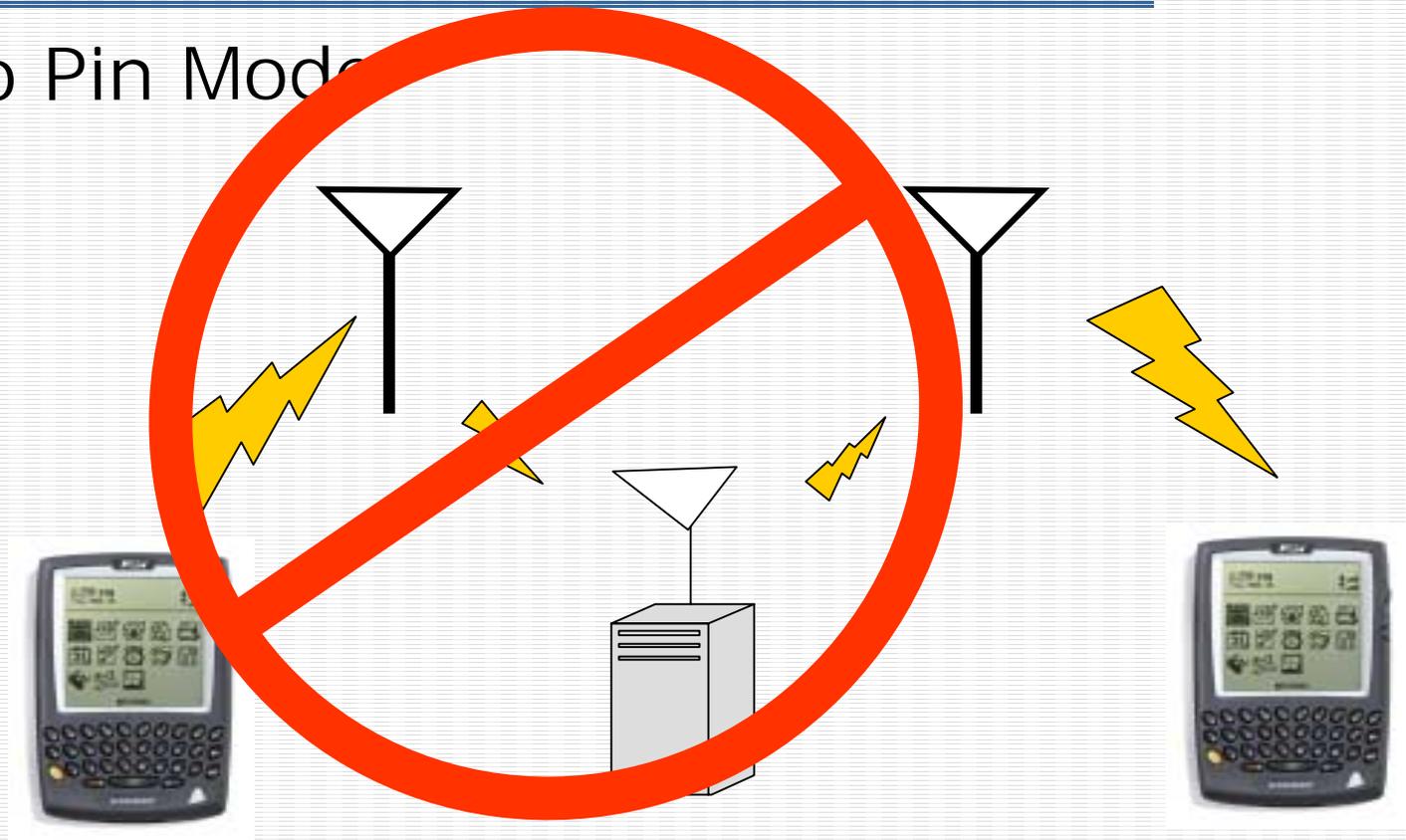
Pin to Pin Mode



Messages Scrambled-3DES Not Used in P-P Mode

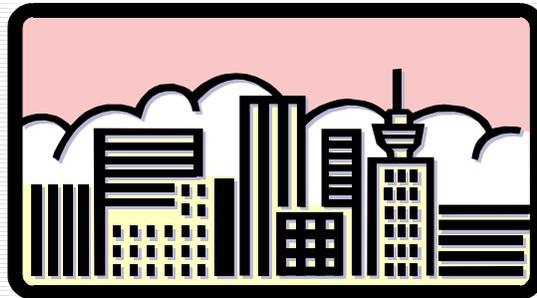
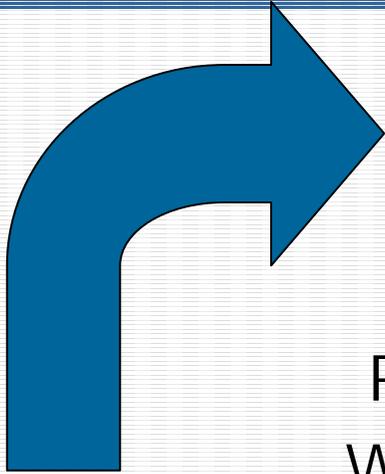
Crypto BlackBerry

Pin to Pin Mode

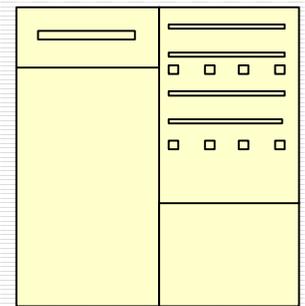
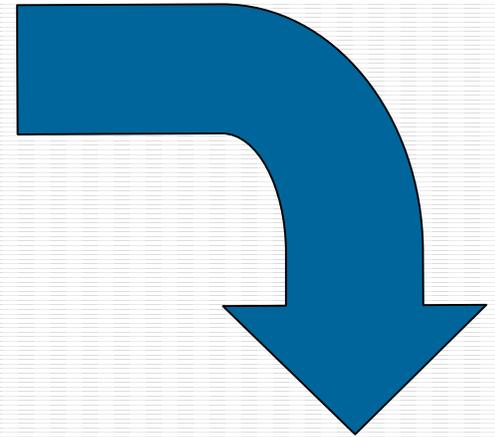


Pin to Pin Disabled in Crypto BlackBerry

BlackBerry



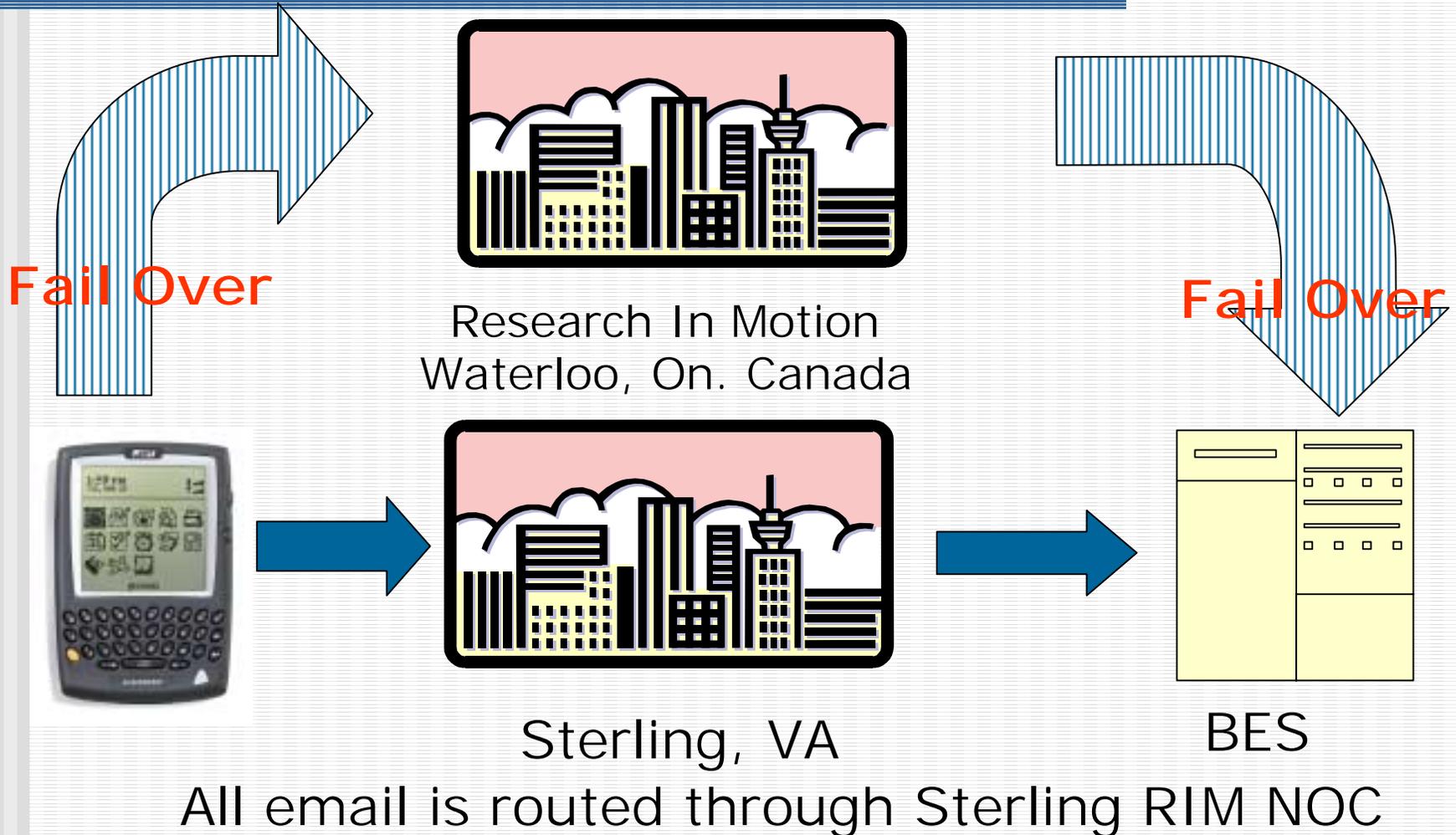
Research In Motion
Waterloo, On. Canada



BES

All email is routed through RIM NOC

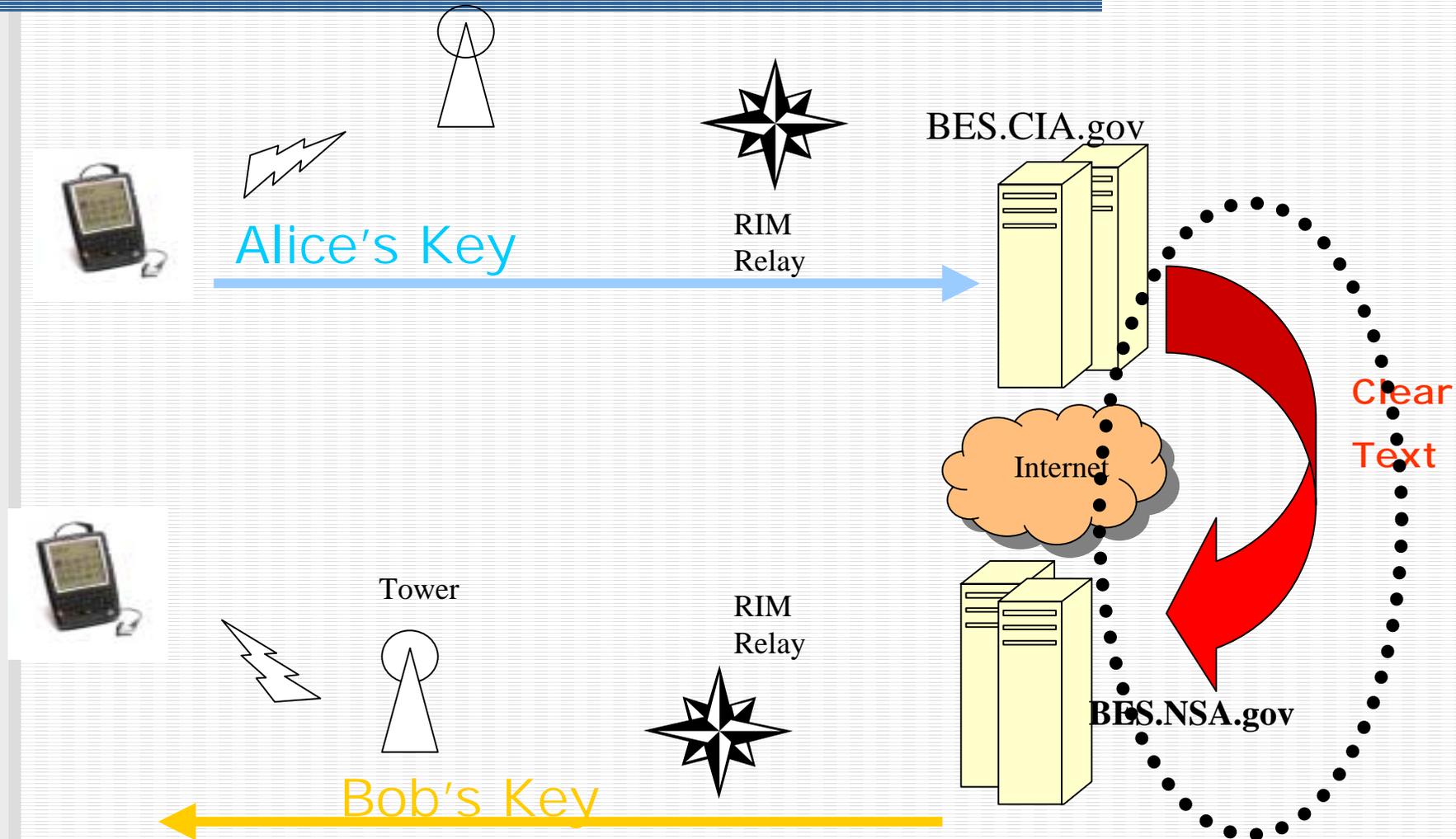
CRYPTO BlackBerry



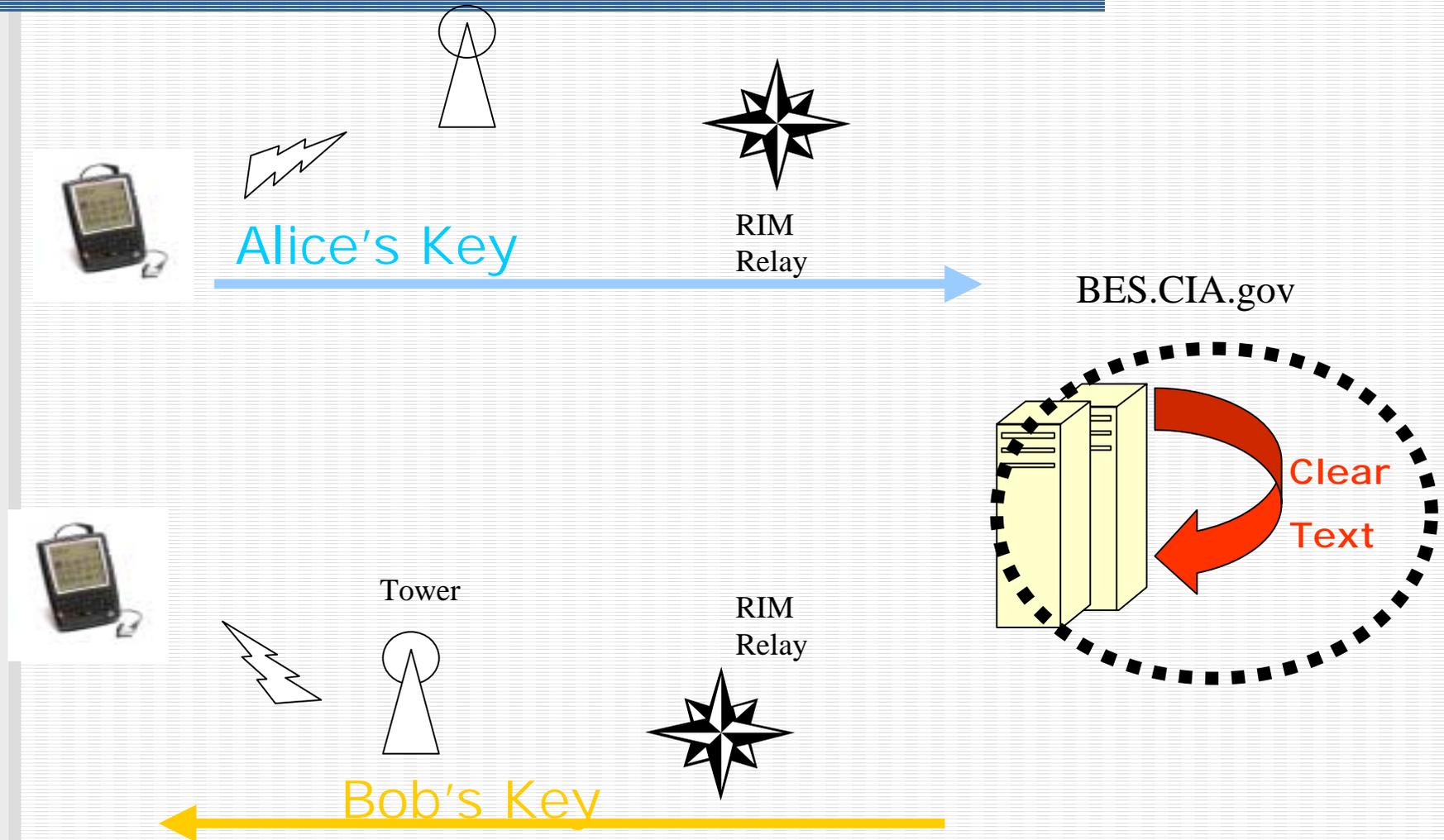
BlackBerry

- 3 Scenarios Where email is vulnerable on BlackBerry System:
 - BlackBerry-BlackBerry on Different Networks
 - BlackBerry-BlackBerry Same Network
 - BlackBerry-to Internet Mail

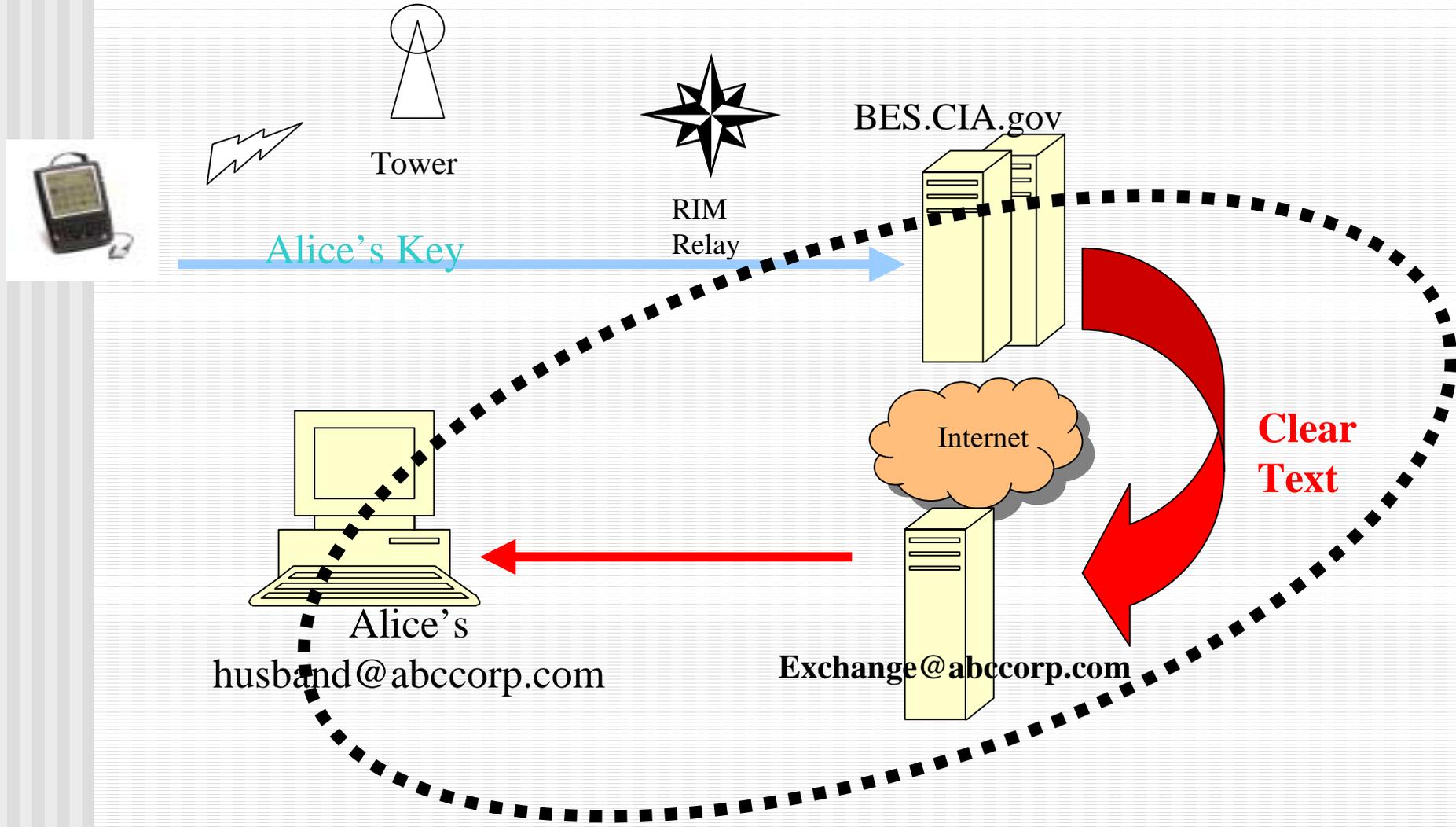
BlackBerry-BlackBerry Different Networks



BlackBerry-BlackBerry Same Network



BlackBerry-to-Internet Mail

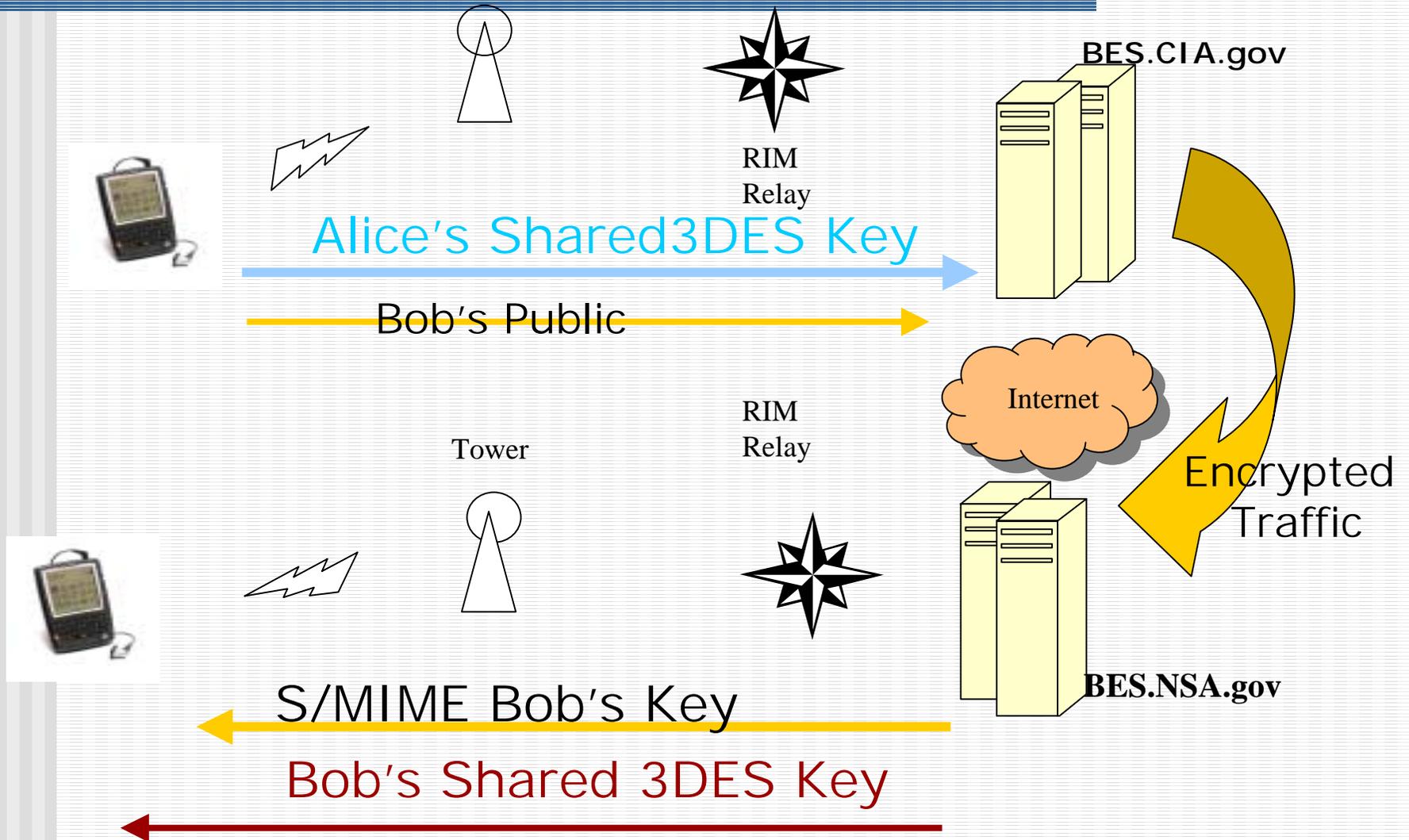


Crypto BlackBerry

- 3 Scenarios Where email is vulnerable on BlackBerry System:
 - BlackBerry-BlackBerry on Different Networks
 - BlackBerry-BlackBerry Same Network
 - BlackBerry-to Internet Mail

ADD S/MIME and PKI

Crypto BlackBerry- (Crypto)BlackBerry Different Networks



BlackBerry

Device
Vulnerabilities



Crypto BlackBerry
Approach

Secure BlackBerry

- What the NSA solution DOES provide
 - True Writer to Reader security
 - Via PKI and S/MIME
 - Strong I&A (Phase II)
 - Via Smart Card (CAC)
 - Enhanced Password Rule Sets
 - More malleable for policy compliance
 - Virus Protection
 - Java Sandbox
 - Signed Applications
 - Version Control
 - Signed Upgrades/Patches

BlackBerry

Password Protected

HOWEVER



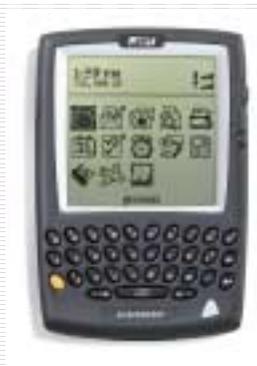
Bypassing could allow

- reading of email
- modify the OS
- modify apps
- load rogue apps

Crypto BlackBerry

Password Protected

HOWEVER



Bypassing could allow:

- reading of email
- modify the OS
- modify apps
- load rogue apps

- ✓ S/MIME Encrypted email stored encrypted
- ✓ Strong I&A with Common Access Card (Phase II)
- ✓ Java OS and Signed OS and Apps
- ✓ J2ME OS will not run any app without valid signature
- ✓ App may load but will not run
- ✓ S/W patches and upgrades signed

Crypto BlackBerry



Provides:

- Compliance for DoD PKI Policy
- Compliance for DoD Overarching Wireless Policy
- BES Distributable Policy files
- Ability to Sign, Sign and Encrypt
- Memory Cleaning Capability
- Local Certificate Cache associated with Adx. Book
- Compatible with MS Outlook 5.5 and 2000
- Strong I&A through Common Access Card
- S/MIME with 1024 bit 3DES for end to end security
- FIPS 140-2 Level I Certification

Crypto BlackBerry

- Ok, So what's the Catch??
 - NSA requires Crypto module to be controlled
 - Central loading facility for the addition of the module to the handheld
 - BES Upgrade
 - Extra Cost for Crypto License
 - Procurement details to follow

Secure BlackBerry

- What Else????????????????
 - ONLY for the 957 device
 - J2ME on a C++ device
 - Other models not useable
 - Somewhat Slower
 - Message decryption/encryption adds ~5-7 Sec. to operation
 - Reduced Functionality
 - Calendar functioning in a limited mode
 - Notepad, task list, calculator omitted

Crypto BlackBerry

Tim Havighurst

tjhavig@missi.ncsc.mil

410-854.7005

Robert Nowak

rjnowak@missi.ncsc.mil

