



Homeland
Security





Voltage
security

DHS S&T Partnerships with Industry

Secure Wireless Data Communications Program

Presented by:
Mark Schertler
December 2006


Agenda

-  Program Overview
-  Trial Architecture
-  Results
-  Summary

Program Vision

Use wireless communications to securely deliver information where and when needed to assist the mission of the Department of Homeland Security.

Program Objectives

 Evaluate and demonstrate cross-border interoperability of secure data communications architectures using commercially available wireless technologies and devices that will allow us to achieve our mission

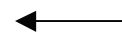
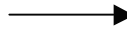
 Use results of program to improve the secure delivery of critical information via the wireless technologies used by public safety, emergency preparedness, and law enforcement communities of Canada and the United States

Market Issue

Wireless devices, like BlackBerry and other mobile data communication devices, are expected to proliferate within government agencies. Today most mobile data architectures are not sufficiently secure for high-level government security.

- BlackBerry devices deployed in government: 30,000+
- Mobile data communication devices: 100,000+ within government (by 2007, over 70% of new mobile devices will be able to exchange data)

Program Participants



Program Lead



Homeland Security



Government Participants

**DHS Science & Technology
Cyber Security
R&D CENTER**



**Secure Mobile
Networking Group**

Industry Participants



Research Focus

Research focuses on technologies that can be used to enhance security to the basic BlackBerry system.

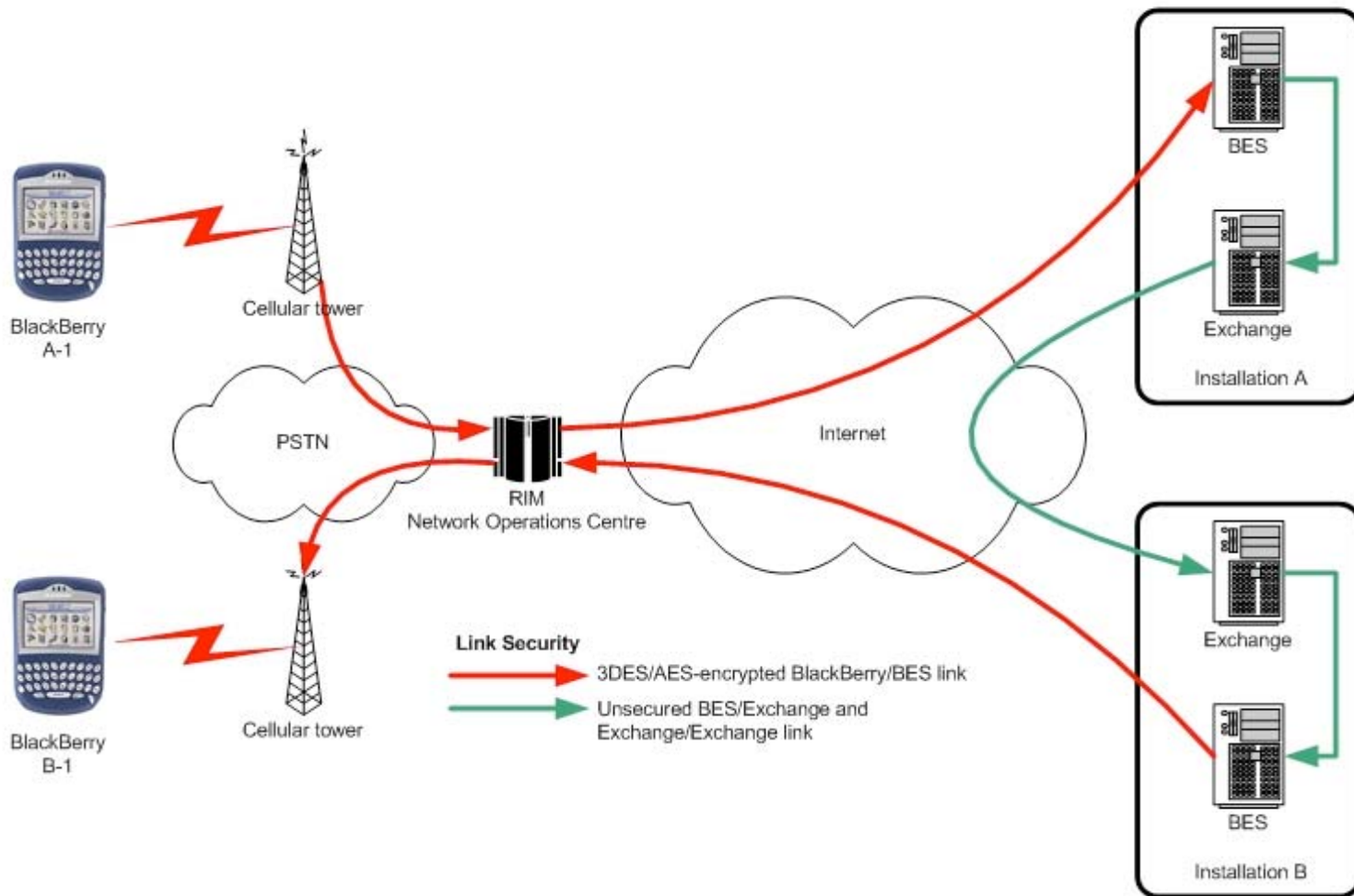
Infrastructure-level Research

- What solutions provide technology for cross-border mobile data encryption?
- What new technologies can be used for public key cryptography differently than traditional public key infrastructures?

Device-level Research

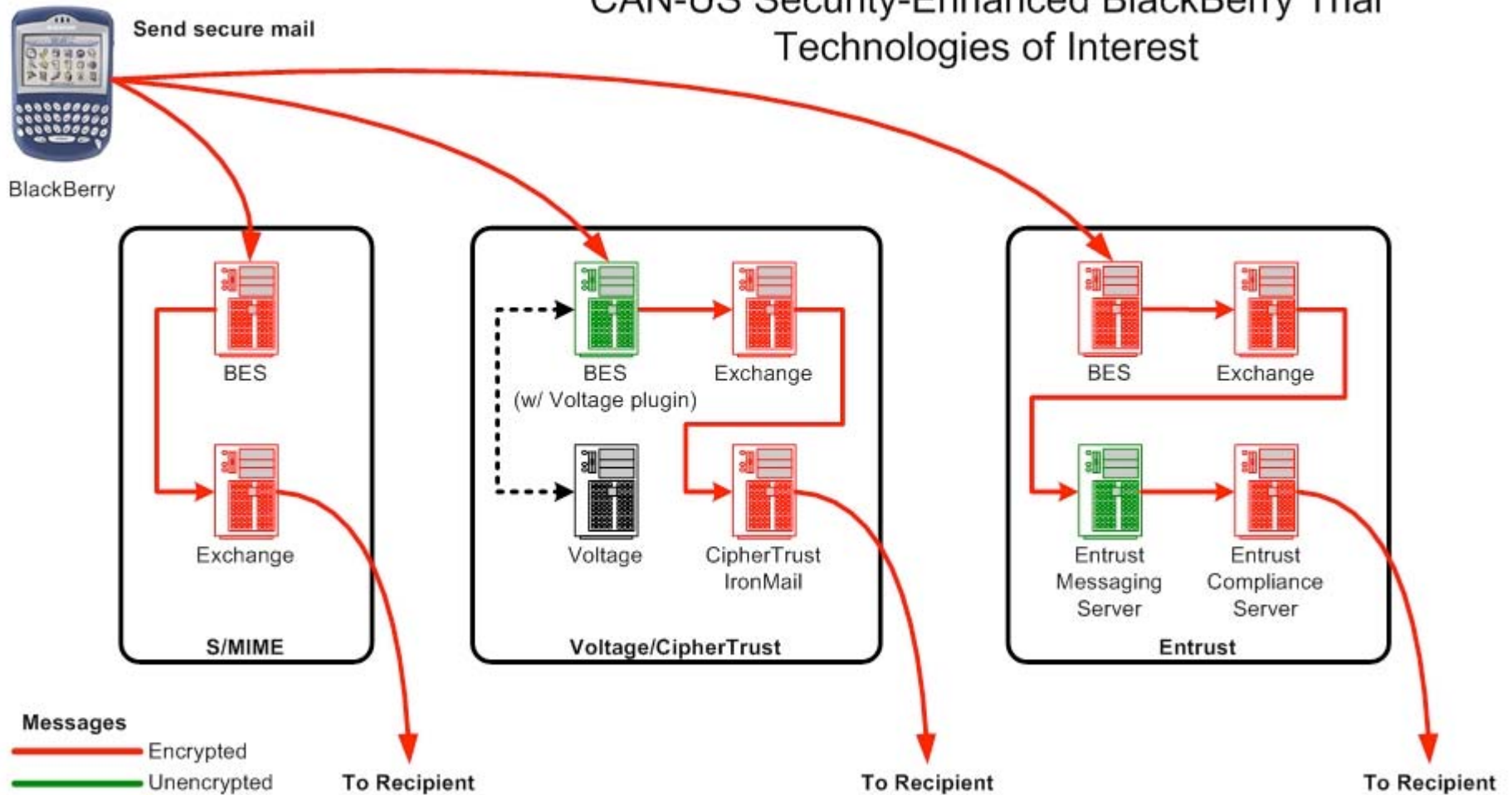
- How does enhanced security affect usability?
- How can security be enforced by improved policy or procedure?

Trial Architecture -- Traditional Setup

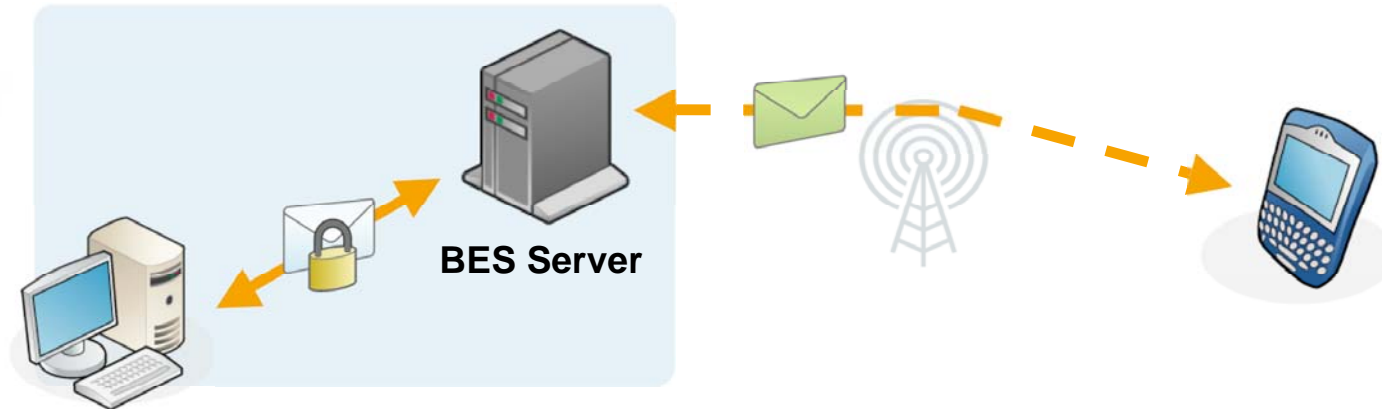


Trial Architecture

CAN-US Security-Enhanced BlackBerry Trial Technologies of Interest



Voltage SecureMail BlackBerry



- ▶ Integrates directly with BlackBerry Enterprise Server (BES)
- ▶ No device-level software required – leverages existing BlackBerry security model for device & link encryption
 - Eliminates complexities associated with deployment, maintenance
- ▶ Supports mandatory encryption rules
- ▶ Can be provided to partners for federated capabilities
 - Upcoming release will support ad-hoc BlackBerry usage with no software

US Trial: June 2005

❑ Objective

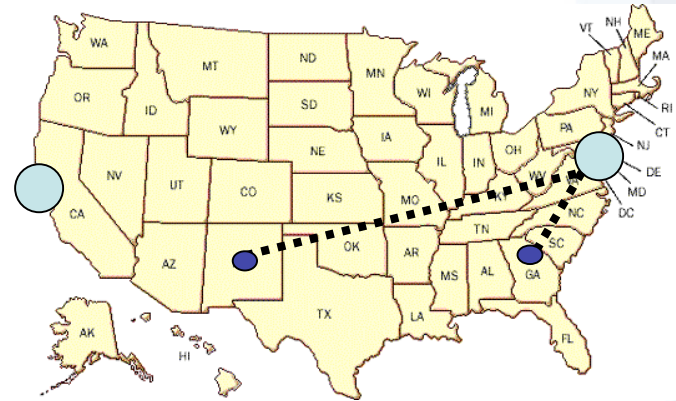
- Test effectiveness of US IBE based architecture to cope with real-time communication in variety of scenarios

❑ Trial Activity

- Four-day test period with 20 activities and 22 participants acting out homeland security scenarios
- Architecture was tested for Voltage's Enterprise Privacy Management
- Secure mail tested to devices without BlackBerry technology using either webmail-type system or Outlook

❑ Results

- No training was required for Blackberry users
- Over 4,000 messages corresponded
- 99% of messages were successfully encrypted



Washington DC

- 11 users (7 users in Washington DC, networked connection to 3 users in Atlanta and 1 user in New Mexico)

Menlo Park

- 11 users (10 full-time users, 1 test device)

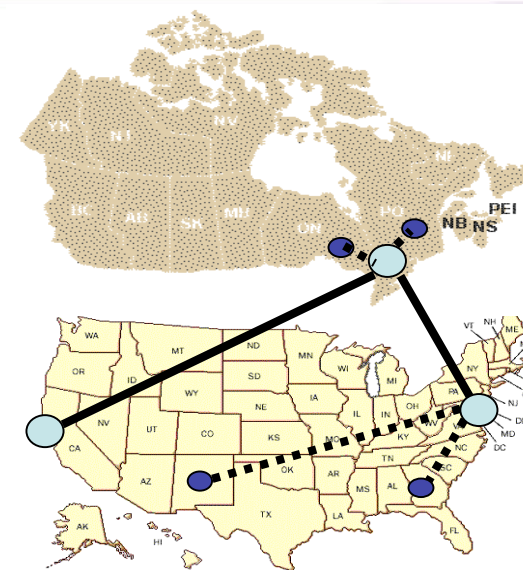
Canada-US Joint Trial: October 2005

❑ Objective

- Test effectiveness of CAN/US cross-border architecture to cope with real-time communication in variety of scenarios

❑ Trial Activity

- Month-long test period with 35 activities and with 25 participants acting out homeland security scenarios
- Test architecture for:
 - RIM's S/MIME package
 - Voltage's Enterprise Privacy Management
 - Alternative secure mail delivery
 - Network scalability for a large user base
 - Solutions to enforce compliance



Washington DC

- 11 users (7 users in Washington DC, networked connection to 3 users in Atlanta and 1 user in New Mexico)

Menlo Park

- 11 users (10 full-time users, 1 test device)

Ottawa

- 20 users (all full-time users)

Trial Results -- Usability

Encrypted Email User Survey		S/MIME		VOLTAGE	
		18-Oct	19-Oct	18-Oct	20-Oct
1	I was able to read messages (7: with ease; 1: with difficulty)	4.15	5.56	6.38	6.70
2	I was able to send messages (7: with ease; 1: with difficulty)	3.69	5.11	6.63	6.90
3	Sending an email to a new recipient was (7: easy; 1: difficult)	2.46	4.25	6.75	6.89
4	Sending and receiving encrypted makes me feel (7: more secure; 1: less secure)	5.69	6.11	5.38	5.30
5	If I had the choice, I would (7: turn on encryption capability; 1: turn it off)	4.23	5.11	6.00	6.40
Average end-user opinion after each product trial (questions are not weighted)		4.04	5.23	6.23	6.44
		57.47	73.74	88.54	91.22

Oct 18: shared certificates. In addition, one Voltage encrypted message was traded to ensure connectivity

Oct 19-20: ran the operational scenario

S/MIME score improved on the second day because no certificate sharing was needed

Scores show Voltage was much easier to use

Trial Results – Performance

	Plaintext	S/MIME	Voltage
East	31	94	68
West	83	173	174
DRDC	95	173	-

Time in seconds

- West domain Voltage messages went through two extra decrypt/encrypt phases
- S/MIME is 3.0 times slower than plaintext
- S/MIME is 1.4 times slower than Voltage
- Voltage is 2.2 times slower than plaintext



What the trial demonstrates

Technology exists that:

- Enables scalable encrypted data communications
- Provides useable encryption for mobile data devices without requiring extensive training of field operators
- Increases mobile data usability while not effecting performance factors
- Supports broader deployment of mobile data devices in government
- Provides cross-infrastructure/border interoperability
- Policy-based encryption is possible
 - However policies must be carefully constructed

Questions?

www.voltage.com