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)
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

- BlackBerry A-1
- BlackBerry B-1
- Cellular tower
- PSTN
- Network Operations Centre
- RIM
- Internet
- BES
- Exchange
- Installation A
- Installation B

Link Security:
- 3DES/AES-encrypted BlackBerry/BES link
- Unsecured BES/Exchange and Exchange/Exchange link
Trial Architecture

CAN-US Security-Enhanced BlackBerry Trial Technologies of Interest

- BlackBerry
  - Send secure mail
  - S/MIME
  - Exchange
- BES
- Exchange (w/ Voltage plugin)
- Voltage
- CipherTrust
- IronMail
- Entrust
  - Messaging Server
  - Compliance Server

Messages:
- Encrypted
- Unencrypted

To Recipient

Voltage/CipherTrust

Entrust
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
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
- All inter-domain mail was scanned for viruses and spam

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)
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

<table>
<thead>
<tr>
<th>Location</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Washington DC</td>
<td>11 users (7 users in Washington DC, networked connection to 3 users in Atlanta and 1 user in New Mexico)</td>
</tr>
<tr>
<td>Menlo Park</td>
<td>11 users (10 full-time users, 1 test device)</td>
</tr>
<tr>
<td>Ottawa</td>
<td>20 users (all full-time users)</td>
</tr>
</tbody>
</table>
Trial Results -- Usability

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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 I was able to read messages (7: with ease; 1: with difficulty)</td>
<td>4.15</td>
<td>5.56</td>
<td>6.38</td>
<td>6.70</td>
</tr>
<tr>
<td>2 I was able to send messages (7: with ease; 1: with difficulty)</td>
<td>3.69</td>
<td>5.11</td>
<td>6.63</td>
<td>6.90</td>
</tr>
<tr>
<td>3 Sending an email to a new recipient was (7: easy; 1: difficult)</td>
<td>2.46</td>
<td>4.25</td>
<td>6.75</td>
<td>6.89</td>
</tr>
<tr>
<td>4 Sending and receiving encrypted makes me feel (7: more secure; 1: less secure)</td>
<td>5.69</td>
<td>6.11</td>
<td>5.38</td>
<td>5.30</td>
</tr>
<tr>
<td>5 If I had the choice, I would (7: turn on encryption capability; 1: turn it off)</td>
<td>4.23</td>
<td>5.11</td>
<td>6.00</td>
<td>6.40</td>
</tr>
<tr>
<td>Average end-user opinion after each product trial (questions are not weighted)</td>
<td>4.04</td>
<td>5.23</td>
<td>6.23</td>
<td>6.44</td>
</tr>
<tr>
<td></td>
<td>57.47</td>
<td>73.74</td>
<td>88.54</td>
<td>91.22</td>
</tr>
</tbody>
</table>
### Trial Results – Performance

<table>
<thead>
<tr>
<th></th>
<th>Plaintext</th>
<th>S/MIME</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>East</td>
<td>31</td>
<td>94</td>
<td>68</td>
</tr>
<tr>
<td>West</td>
<td>83</td>
<td>173</td>
<td>174</td>
</tr>
<tr>
<td>DRDC</td>
<td>95</td>
<td>173</td>
<td>-</td>
</tr>
</tbody>
</table>

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
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