Data at Rest Security in Navy/NMCI

Steven Gillis
ONR Information Assurance Manager
10 January 2008
Agenda

- Data at Rest Security – What is it? What are the policies?

- Existing Solutions in Navy – Do DAR solutions currently exist in Navy/NMCI?

- Planned DAR Solutions in Navy/NMCI – What are the details on the NMCI GuardianEdge deployment?
Data at Rest Security
What is Data at Rest security?

- Encryption of user data stored on hard drives and removable storage media, such as USB thumb drives, CDs, DVDs, etc.

- Protection against unauthorized access to data should the storage media become physically compromised.
Why is Data at Rest security needed?

Because we’ve been told to do it...

- Office of Management and Budget – Memo M-06-16 – “Protection of Sensitive Agency Information”
- DoD CIO – Memo Dated 03 July 2007 – “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media”
- DON CIO – Message DTG 091256Z OCT 07 – “DON Encryption of Unclassified Data at Rest Guidance”
- Related USN and USMC direction
Why is Data at Rest security needed?

...and because we want to avoid:

Vast Data Cache About Veterans Is Stolen

By DAVID STOUT and TOM ZELLER Jr.
Published: May 20, 2008

WASHINGTON, May 22 — Personal electronic information on up to
26.5 million military veterans, including their Social Security numbers
and birth dates, was stolen from the residence of a Department of
Veterans Affairs employee who had taken the data home without
authorization, the agency said Monday.
What kind of data are we securing?

- **Personally Identifiable Information (PII)**
  - “...that is either accessed remotely or physically transported outside of the agency’s secured, physical perimeter” (OMB Memo M–06–16)
  
  [http://www.whitehouse.gov/omb/memoranda/](http://www.whitehouse.gov/omb/memoranda/)

- **Sensitive Unclassified Information**
  - “All unclassified DoD data at rest that has not been approved for public release...” (DoD 03 Jul 07 Memo)


What is the scope of NMCI Data at Rest?

Unclassified Department of Defense Networks

Removable Storage Media

Laptops, Workstations and PDAs

Network Storage Infrastructure

FY07
- Interim DAR Solutions

FY08
- DoD DARTT Solution
- Server DAR Solutions
What are the DOD DAR Requirements?

103 DAR Requirements included:
- FIPS 140–2 compliance for encryption
- Pre Boot Authentication for Full Drive Encryption
- Ability to use Single Sign On

Enterprise Software Initiative / SmartBuy
- 10 DAR solutions approved for Department of Defense
Existing Data at Rest
Solutions in Navy/NMCI
Microsoft Encrypting File System

File system–level (file and folder) encryption available in Microsoft Windows 2000 and later

Key Point
- Encryption of NTFS volumes only
Microsoft Encrypting File System

**File Encryption**
- File encrypted using symmetric File Encryption Key (FEK)
- FEK encrypted using user’s public key
- Encrypted file stored with encrypted FEK

**File Decryption**
- EFS decrypts FEK using private key that matches public key
- File decrypted using FEK

*Image by Jérôme BLUM 2006 and used with permission under Creative Commons ShareAlike 2.0 licensing*
Key Features

- Secure tape data for offsite storage and transfer between sites
- Maintain compartmentalization for tape backups
- FIPS 140–2 Level 3 validated
- Integration directly into SAN infrastructure – transparent to end users and commands

NMCI–led project underway to implement at NOCs and select server farms
Key Features

- Encryption of user data stored on BlackBerry
- Content protection key and user keys generated and stored on BlackBerry device
- Data protected when BlackBerry device is locked
- Centralized BES policy management for users and groups

NMCI BlackBerry security settings have been implemented in accordance with DISA STIG and DAA-approved configurations

http://www.blackberry.com/security
GuardianEdge Data at Rest Solutions in NMCI
GuardianEdge DAR Solutions

GuardianEdge Encryption Anywhere
GuardianEdge Encryption Plus
GuardianEdge Device Control
GuardianEdge Hard Disk Encryption

Key Features
- Full Disk Encryption of local drives
- Pre-Boot Authentication (PBA) integrates with Common Access Card

User Experience
- User will see new PBA screen before Windows logon
- PBA can support CAC or username and password logon
- User may experience a nominal, one-time slowdown in disk performance while the disk is being encrypted (average 2–4 hours)
- Full disk encryption is otherwise user-transparent requiring no additional action by the user
GuardianEdge Encryption Anywhere
Removable Storage Media

► Key Features
- All removable storage media can be encrypted
- Application can be copied to storage media with data
  • Allows decryption on workstation without GuardianEdge installed

► User Experience
- Contingent upon Enterprise policy configuration
  • Some removable media may no longer be allowed
  • Some removable media may have its contents automatically encrypted – this may render some media unusable (e.g. IPODs or other MP3 players)
  • Some removable media may be forcibly formatted before it can be used
- Users will need to understand policy before connecting removable media
Key Features

- File and Folder level encryption solution

User Experience

- Contingent upon Enterprise policy configuration
  
  - User data can be automatically encrypted when placed in designated folders

- Encrypted folders managed administratively via Enterprise policy configuration

- Solution is user-transparent requiring no user intervention for folder encryption
Key Features

- Policy-based control of user access to workstation ports and the devices that connect to them
- Prevent leakage of sensitive data based on granular user and group policies

User Experience

- Contingent upon Enterprise policy configuration
  - Users may be restricted as to what devices can be connected to their computer
  - Users may not be authorized to connect personal hardware to business assets that they were formerly able to access
  - Users may be required to submit requests for exceptions to policy to allow certain devices to be connected
Will the DAR deployment impact NMCI users?

- **Backup of User Data Prior to Encryption**
  - Less than 1% error rate with full disk encryption solution
  - Potentially results in the loss of all data stored on the seat
  - Mitigated by user backup of all local data prior to disk encryption

- **Registration to Workstation for Pre–Boot Authentication (PBA)**
  - In order to support CAC logon at Pre–Boot, users must register their CAC certificates with the DAR solution on the local seat

- **Impact to Use of Removable Storage Media**
  - Removable storage media can be configured to be read–only or set to require encryption before allowing data to be written
  - Dependent on Navy and Marine Corps security policies
When will GuardianEdge be deployed in NMCI?

- Solution Engineering and Testing – March 08
- DITSCAP Certification and Accreditation – April 08 *
- Begin Deployment to Enterprise – August 08 *
- Complete Deployment to Enterprise – October 08 *

* Tentative Dates Dependent on USN and USMC Certification and Accreditation of Solution
Questions?

Steven Gillis
Office of Naval Research
Information Assurance Manager
703.696.5693
gilliss@onr.navy.mil
► Back Up Slides
What Is FOUO?

Is this document or information (no matter how important or no matter how trivial it may seem) related solely to the internal personnel rules and practices of ONR? Is it correspondence from ONR which is advisory in nature?

Is this document or information already protected from public disclosure by any prohibitions in federal statutes besides the Freedom of Information Act?

Does this document or information pertain to commercial or financial information or trade secrets?

Is this document or information privileged interagency or intra-agency correspondence which is advisory in nature?

Does this document or information pertain to the personal privacy of another individual? Would its disclosure constitute an unwarranted invasion of the individual’s privacy?

Was this document or information compiled for law enforcement purposes? Would its disclosure interfere with law enforcement proceedings? Would its disclosure deprive an individual of a fair trial or impartial adjudication? Does it pertain to an individual’s personal information in law enforcement records? Would its disclosure compromise the identity of a confidential source? Would its disclosure expose techniques and procedures for law enforcement investigations or prosecutions? Would it jeopardize the physical safety or a wide range of individuals if disclosed?

Does this document or information pertain to the records of financial institutions or the agencies responsible for regulation or supervision of financial institutions?

Is this document or information geographical or geophysical in nature, specifically concerning wells?