

Information Management Security
LCol R. Mazzolin
A/Director IM Security, NDHQ

Reported by Dave Edmunds

Unfortunately, I was unable to attend the January 2004 meeting, and I cannot provide the usual type of report. However, much information can be gathered from the presentation slides, available separately on this web site.

A great deal of useful information is included in the Notes part of some of the slides. It is a bit difficult to extract, so I am giving it below.

Slide 8, Vulnerabilities

I have talked about threats. But what are the generic vulnerabilities associated with information systems.

Design complexity

- Pentium chip example, (math unit error)

- operations errors - DNS example

- protocol weaknesses, constraints and assumptions

susceptibility to malfunctioning hardware and software - example of cascading failure of SS7 switches disabling major telecomms network

Amount of information

No. users - system scalability, extremes of behaviour

Wide distr - harder to control

Ease of access - accessible to more users

Speed of access - susceptible to rapid attacks

- aggregation/inference problem,

More opportunities to introduce errors

Harder to check for abuse or misuse - due to more users, more activity

Slide 11, Secret and Above

DND's mandate is to provide operational Land, Sea and Air capability to meet objectives set by the Canadian Government. Information systems have taken on an ever increasing role in enabling the DND/CF to develop, deploy, command and sustain these forces. <CLICK> In order to meet the command, control and intelligence requirements of deployed forces, classified networks have been implemented. These networks deal with information that could cause significant or greater damage to the nation, and have been therefore been designed to operate at SECRET and higher classification levels. These systems employ significant protections, including type one Military grade cryptography to ensure the safeguarding of the highly sensitive information. The protection of this information is an integral part of force protection activities, as divulging command, control and intelligence information can have extremely negative impacts on deployed Canadian Forces personnel and mission success.

Insert info on designated systems

There are a number of Enterprise Resource Planning (ERP) Application Systems that play a significant role in the provision of logistical support: Canadian Forces Supply System (CFSS), Departmental Human Resource Management System (DHRMS), Financial Management Accounting System (FMAS) and Materiel Acquisition Support Information System (MASIS). These systems have become critical to the daily operation of DND and must be available wherever and whenever required by any personnel in DND in order to ensure operational capability is maintained.

The Command & Control systems have always been managed as being SECRET, or greater. The ERP systems have never had the same measure of clarity with respect to security that was available to the Command & Control systems. Throughout the 70s and 80s, part of the ERP systems, at least the HR and CFSS used dedicated periods processing on the mainframes to allow the processing of data and information considered classified. This practice ceased in the 90s, even though paper versions of some input/output documents remained classified (for example: Immediate Operational Requirement, Operational Deficiency, Naval ammunition holdings).

Up until very recently system sensitivity analysis has been based on a concept of peacetime vs wartime. This worked well for DND in a Cold War context and also for peacekeeping operations where the threat level was relatively low.

Slide 12, ERP Interconnections - DWAN

In addition to the big 4 ERP Application Systems previously mentioned - CFSS, FMAS, DHRMS & MASIS - there are a number of other associated systems that provide information to, or consume information from these large systems. These additional systems are:

NMDS - National Materiel Distribution System

AIMS - Ammunition Inventory Management System

MASS

FMS - Fleet Management Systems (for wheeled or tracked vehicles)

CFRIMS - Canadian Forces Recruiting Information Management System

PERMIS - Personnel Record Management Information System

CMIS - Chief Maritime Information Systems

CF-18 DMS - Data Management System

ADAM - Automated Data Aircraft Management

CBMSS - Condition Based Maintenance ??

FSIS - Flight Safety Information System

Special mention must be made of the Defence Total Asset Visibility (DTAV) system and of Defence Information System Broker (DISB) system as these are 2 different types of data aggregators. DTAV has a predefined database that gathers and processes data from numerous sources and provides an interface to the collected data. DISB will allow a user to specify a data view and determine the data sources to be used in construction of that view. DISB will have connections to all DND information systems. DTAV is running today, and DISB may be running within 2-3 years.

The criteria for inclusion are:

* Information about operational capability, deficiency or vulnerability of an operationally deployed combat capable unit

* Information about operational capability, deficiency or vulnerability of a class of combat capable units

These systems all contain a great deal of data about various items subject to deployment on operations, or of deployed units. Today this information is up to date, accurate and contains significant historical detail. This is a quantitative and qualitative change from the systems of the past.

Other large scale ERP systems not show here are Centralized Computational Pay System (CCPS) including the Reserve Pay System and the connection to PWGSC for civilian pay services.

ERP Systems will largely continue to function as they do today. Each system will be required to perform a complete information and data analysis that must be conducted under the auspices of command qualified staff from the appropriate environmental commands. Systems in the DESC, or that are relocated to the DESC, will be managed first as resources and procedures are already being developed for systems within that facility.

Slide 15, Comprehensive Security Environment

A complete information system security solution consists of a large number of elements, many of which are not technology based. In addressing the IS security problems, the Enterprise Security Environment initiatives will take into consideration all aspects of IS security shown here. IS security is not purely a technical issue.

[LCol Mazzolin's presentation slides, giving contact information, can be found at www.afcea.ca Ottawa Chapter]