EBU Networks Seminar
EBU Headquarters, Geneva

In the trenches

The military approach to IT security

Alan Woodroffe
ebu@SecureSystemsSupport.co.uk

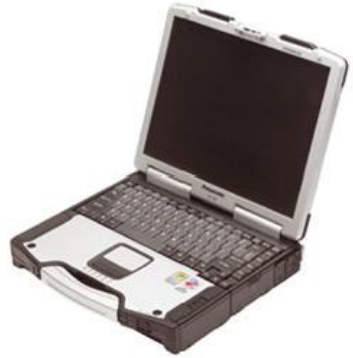
SECURE SYSTEMS SUPPORT LIMITED

www.SecureSystemsSupport.co.uk

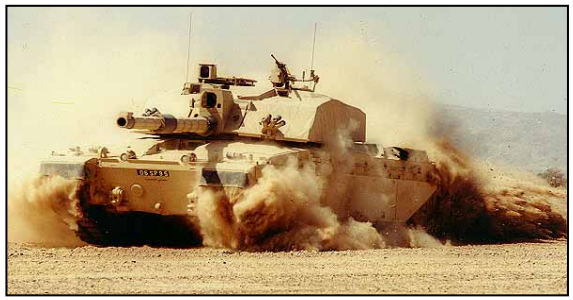
IT Security Issues

- Design and Training considerations
- Interoperability / Complex Systems
- Resilience
- Reliability / Encryption
- In-Service Updates
- Disposal - Emergency and Scheduled
- The classic: Confidentiality - Integrity - Availability

- Design Considerations
  - "Squaddie proof" – able to be dropped from the back of a truck and still function
    - Modern rugged laptops



  - Extremes of temperature
    - Desert
    - Polar regions

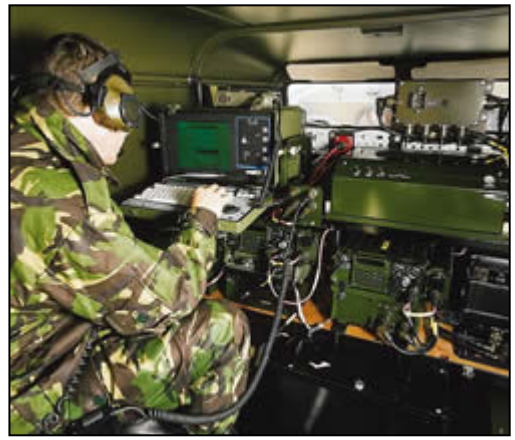


- Accreditation
  - The UK Defence Security Standards Organisation (DSSO) tests UK MoD IT systems
    - Identify key risks to the project
    - Ensure correct user procedures
    - Ensure correct secure system configuration
    - Ensure strong enough encryption
    - User education is a major part of System Security

- Training
  - UK MoD staff are often “in post” for only 2 years
    - Staff require training when posted in to a job
    - Staff are given varied careers and may have little prior IT experience
    - Thorough and comprehensive standards are required so new staff can learn without a handover

Interoperability

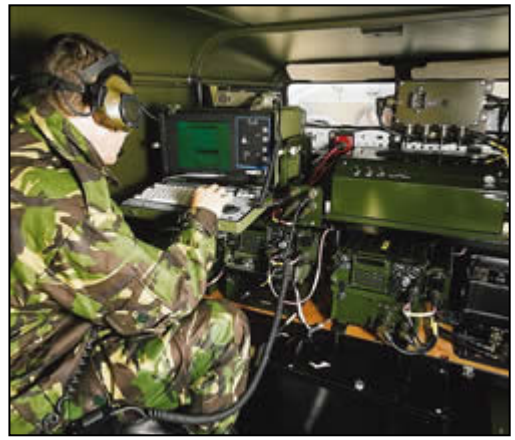
- UK MoD project procurement used to be 10 years
  - New equipment must operate with old



- UK MoD often operates in Coalition scenarios
  - Equipment must operate with Coalition partners'

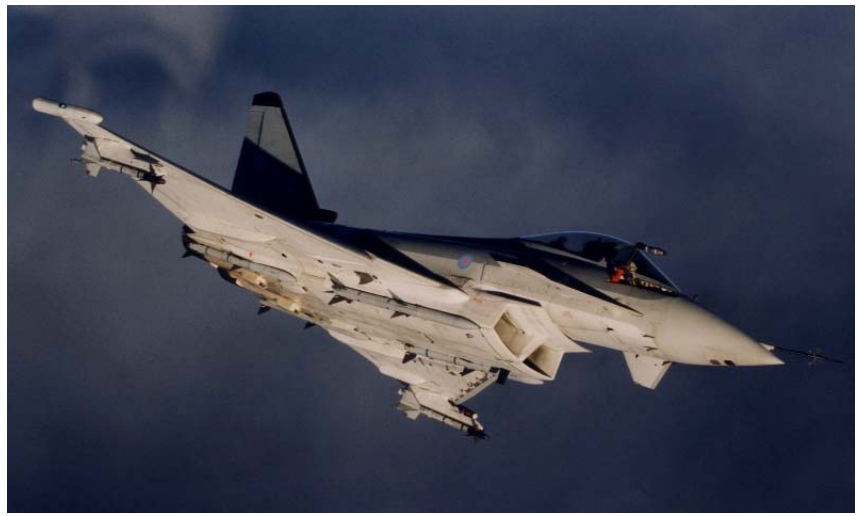
Complex Systems

- Example: BOWMAN
  - 48,000 radios & 26,000 computers
  - 9,500 Local area Sub-System installations
  - 20,000 vehicles
  - 43 capital ships (158 all types)
  - 350 aircraft
  - 100,000+ trained servicemen



Complex Systems

- Example: Eurofighter
  - 4 nation interoperability
  - On-going development
  - Ground-breaking
  - Use of biometrics
  - PKI
  - Air system supported by wide range of ground systems



Resilience

- Military systems must be resilient and continue to operate when under attack from an enemy force
  - Resilience can be built into IT systems nodes (and spares)
  - Resilience can be built into IT systems networks
  - ARPANET (1969 – 4 nodes!) relied upon network resilience
  - UUCPNet (1983 – 550 nodes – including alan@rocc) relied upon resilience in customised scripts and “hosts” files
  - TCP/IP (official protocol on ARPANET from Jan 1983) relies upon resilience in the hosts and network nodes

- Reliability / Encryption
  - Military systems must be reliable
    - Systems should work first time
    - Systems should guarantee to do their task; once a command has been given a user should assume that the action has been successfully completed
  - Military systems must guarantee that any message transmitted or stored cannot be accessed by an enemy
  - False/idle data may be sent to prevent traffic analysis

In Service Updates

- The DSSO Accreditation is not a one off process
  - Technology will be enhanced, software will be updated
  - Systems and connectivity to them will change over time
  - System usage will change over time as requirements evolve
  - New threats to systems will emerge and must be countered
  - In time, the business reason behind the original system will change
- Systems should be re-accredited during their life

Disposal - Emergency

- Items of most value: equipment or Data?
  - May not be possible to recover equipment
  - Equipment destruction at point of no return
  - Data must be destroyed if lost
  - Remote device disabling
  - Remote data destruction
  - Recognition of data compromise if destruction not possible

- Disposal - Scheduled
  - Data must be purged from equipment before that equipment may be re-used within an organisation
  - Data must be erased from equipment before that equipment may be disposed of from an organisation
  - Data disposal is a key part of a system design
  - Data disposal must be available through system's life

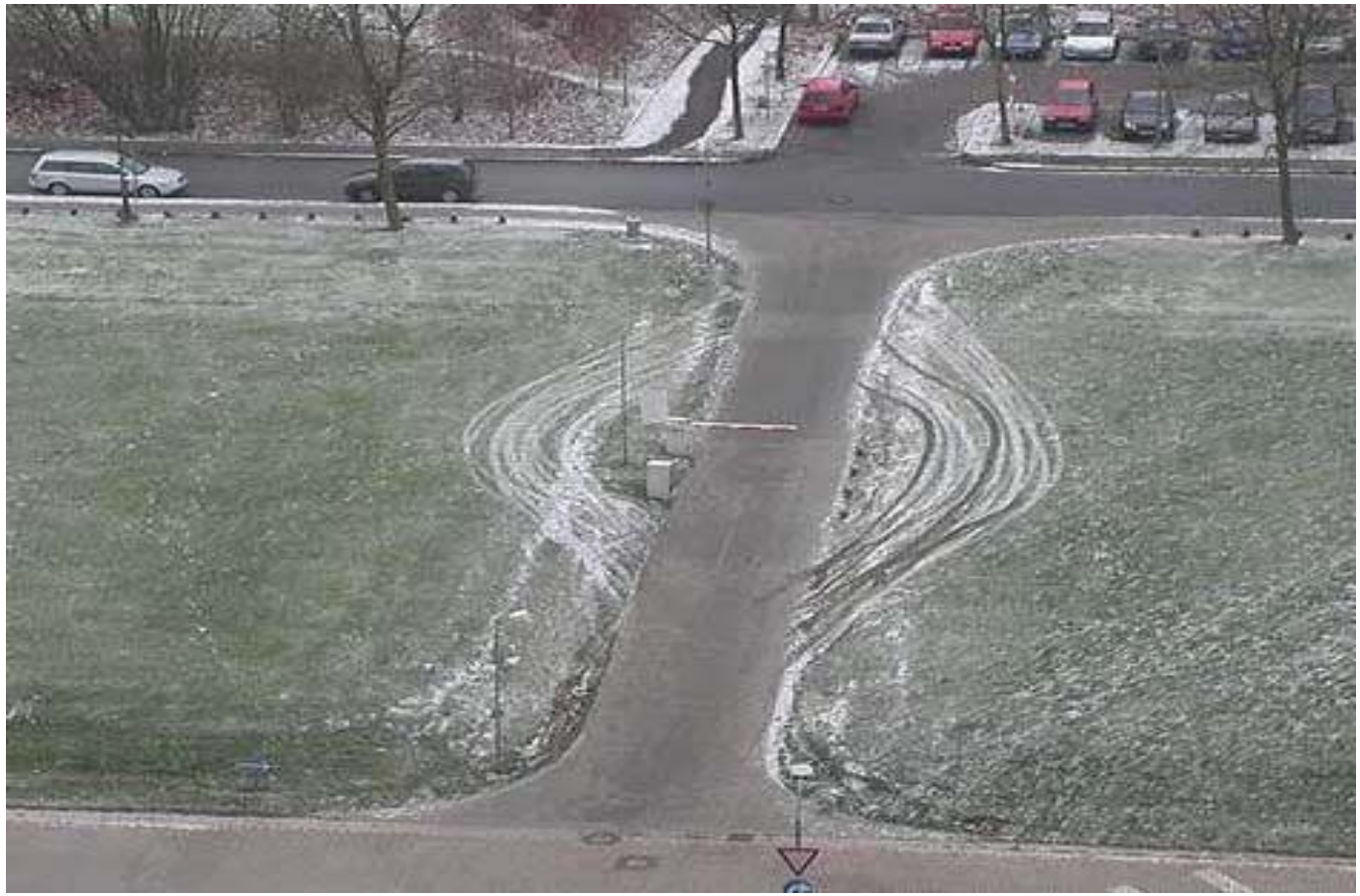
- Information Security Classic - CIA
  - Confidentiality
    - You don't want your enemy to eavesdrop on your communications or read your files if they capture your equipment
  - Integrity
    - When you send an instruction, you expect it to be received exactly as you sent it, not garbled
  - Availability
    - You need to be able to use your systems as and when you need to, you don't want them knocked out just as you start an offensive

- Confidentiality
  - Military
    - Intentions
    - Capabilities
  - Broadcast
    - Information sources

- Integrity
  - Military
    - Intelligence must be reported correctly
    - Orders must be disseminated without corruption
  - Broadcast
    - Must report facts correctly in order to maintain credibility and trust of listeners/viewers

- Availability
  - Military
    - To be able to report intelligence when it occurs
    - To be able to issue orders when required
  - Broadcast
    - To file stories when the journalist wants/needs to
    - To transmit programmes on schedule
    - To distribute on-line content on demand from user

- One of the main aspects of Information Security is the provision of effective barriers to prevent users from doing what they shouldn't … ☺



- Military v Broadcast Information Security
  - Military tends towards the C and I of CIA
    - **Confidentiality** **Integrity** Availability
  - Broadcast tends towards the I and A of CIA
    - Confidentiality **Integrity** **Availability**

EBU Networks Seminar
EBU Headquarters, Geneva

Questions ?

Alan Woodroffe

ebu@SecureSystemsSupport.co.uk

SECURE SYSTEMS SUPPORT LIMITED

www.SecureSystemsSupport.co.uk