Electronic Security Implications of NEC: A Tactical Battlefield Scenario

Zia Hayat[*], Jeff Reeve
University of Southampton, UK

and

Chris Boutle
BAE Systems, UK

Introduction

In [1] three principal themes are identified by the UK MoD (Ministry of Defence) in order to deliver the vision of *NEC* (Network Enabled Capability): Networks, People and Information. It is the security of information, which is discussed in this article. The drive towards NEC is due to many factors; one defining factor is to provide an increase in *operational tempo* in effect placing one ahead of their enemy in terms of acting within their OODA (Observe, Orient, Decide, Act) loop. However as technical and procedural systems are being advanced to achieve the vision of NEC, what impact does this have on the traditional information security triangle, of preserving the *confidentiality*, *integrity* and *availability* of information? And how does this influence current security engineering and accreditation practices, particularly in light of the *proliferation problem*? This article describes research conducted into answering these questions, building upon the findings of the NITEworks® [2] ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) Theme studies and focusing on a tactical battlefield scenario. This scenario relates to the IFPA (Indirect Fire Precision Attack) [3] project where the efficient synchronisation of potentially numerous sources of information is required, providing real-time decisions and delivery of effects, in accordance with the requirements of NEC. It is envisaged that the IFPA systems will consist of numerous sub-systems each of which will provide a unique effecting capability to the UK army with differing levels of speed, accuracy and range.

[*] Sponsored by BAE Systems and EPSRC, UK.

Evolution of Information Security Requirements

The underlying theme of NEC is to provide the UK military organisation with *decision superiority* through *information superiority*. A vital tenet of information superiority is *information sharing*. According to [1] information sharing in the NEC sense implies rapid & simultaneous information transfer through **automated** processes. All four of these pillars are inherently reliant upon information security as illustrated in figure 1. Many current and future military CIS (Communication & Information System) developments are driven by the pillars of NEC. It is envisaged that if fulfilled these pillars will provide agile and dynamic business processes, based upon an efficient and effective electronic infrastructure.

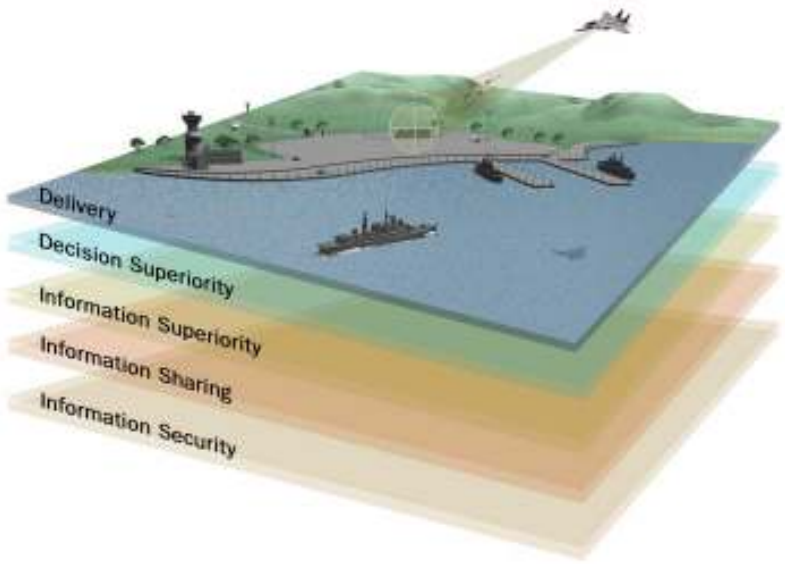

Figure 1: Fundamental building blocks required to achieve NEC.

From an information security point-of-view network enabled systems still require the confidentiality and integrity of information to be preserved. The third dimension of availability is a broad requirement, which has traditionally related to robustness (operational continuity or graceful degradation). However from an NEC and tactical battlefield point-of-view it is argued that availability necessitates *timeliness* on a par with robustness, where timeliness implies that all relevant information is delivered to authorised entities at the correct time enabling efficient information sharing.

Proliferation Problem

There is currently a significant increase in the utilisation of COTS (Commercial Off The Shelf) products in military CIS; this is evident in a number of projects [3, 4]. As well as this the requirement for high-levels of interoperability with foreign nation systems, along with the need to adhere to the security principle of least-privileges (or need-to-know), has lead to increased fragmentation[1] of the military CIS. In this context this is called the proliferation problem, where vulnerable connections are no longer confined to communications interfaces between multi-level classification systems. This is illustrated in figure's 2 and 3, where it can be seen that the risks to security have traditionally

[1] Due to the varying degrees of trust one may have in such systems.

related to inter-classification communications, however the problem domain has now augmented to an intra-classification level as well.

Figure 2: The traditional security issue of interfacing at the inter-classification level.

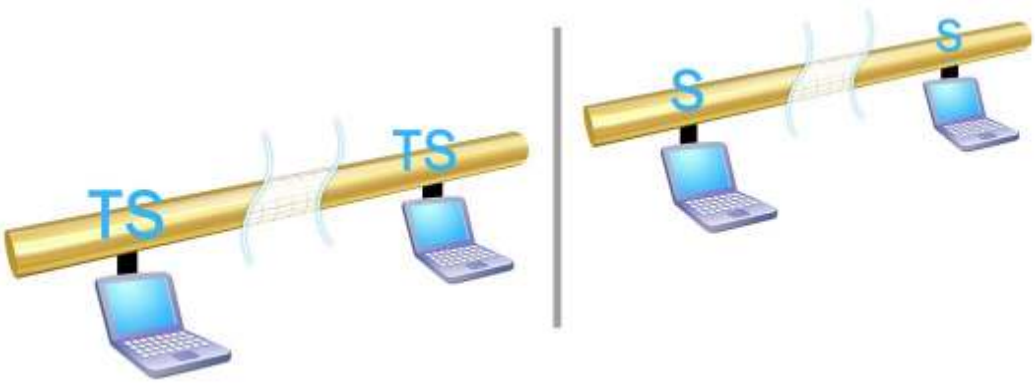

Figure 3: The new security issue of interfacing at the intra as well as inter-classification level.

Partitioned Infrastructures

It is currently standard practise to satisfy all high-risk connections whether inter or intra-classification with a partitioned infrastructure (or air-gap) solution, their attractiveness is their provably simple and inexpensive approach towards managing risks and therefore gaining security accreditation. Air-gaps however impose severe restrictions on operational efficiency, therefore impacting upon the information security requirement for timeliness. Limitations imposed by air-gap solutions such as manual medium transfer and re-typing include:

- Allow for only primitive data transfers
- Error prone due to human deficiencies
- Constrain rapid C2 (Command & Control) requirements

Significant advances in providing efficient alternatives to air-gaps have been made ever since the requirement for MLS (Multi-Level Security) was formally identified in the orange book [5]. However, the overheads of implementing and maintaining such systems primarily for the military, in accordance with common criteria requirements has

proved to be very expensive for such a niche market. This has lead to the continuation in use of partitioned infrastructures.

If all high-risk connections utilise partitioned infrastructures then in combination with the proliferation problem this will prohibit the information security requirement for timeliness, effectively *disabling* the vision of true NEC. This is illustrated in figure 4, where it is shown that numerous air-gaps may be utilised to separate systems and subsequently sub-systems for the reasons described previously. In [6] an experiment was carried out where it was shown that manual information transfer introduces administrative overheads into the kill chain (Find, Fix, Track, Target, Engage & Assess) from an air force point-of-view.

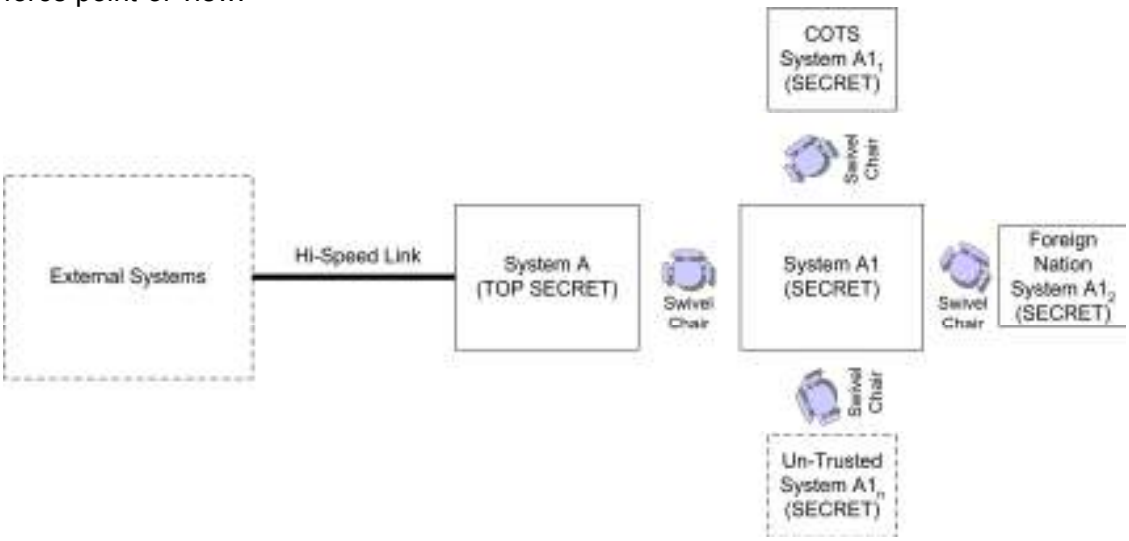

Figure 4: Generic high-level overview of potential configuration of future military systems.

Inefficiencies in the kill chain would limit the ability of systems such as IFPA to engage high value TSTs (Time Sensitive Target), which is a fundamental operational requirement. This is exemplified in the current conflict in Iraq, where it can be seen that enemy targets are no longer in the form of large relatively static forces such as the Red Army or Republican Guard. Instead highly dynamic and agile terrorist cells are a new kind of enemy, the *invisible enemy* who if located must be rapidly engaged for maximum effect. However this requires minimal latency from the moment that a potential target has first been identified to all other stages in the kill chain.

Previous drives towards reducing the total time of the kill chain have focused considerably on processes and technologies, for the efficient commitment and delivery of munitions. These include *all weather* and *precision guided* munitions as well as *integrated sensing & effecting* capabilities. Such developments have significantly reduced the launch and flight times of munitions. However, in order to realise the potential of such information intensive enhancements it is important to remove any unnecessary steps in the information flow and decision chain as alluded to in [7]. Partitioned infrastructures are such an unnecessary step, particularly in future battlefield systems, which require increased information processing and sharing for BDA (Battle Damage Assessment) and SA (Shared Awareness) purposes.

Non-Partitioned Infrastructures
NITEworks® carried out two sequential programmes of work within the ISTAR Theme. The NITEworks® ISTAR Theme, Phase 1 study [8] which addressed the UK Information Requirement Management processes, demonstrated significant benefits to NEC of automated information transfer in the form of non-partitioned infrastructures. Principal improvements were identified in information sharing and therefore shared situational awareness. In relation to information security, these improvements can be seen to enhance the requirement for timeliness. However, confidentiality & integrity were not considered in this phase in order to highlight the deficiencies of non-partitioned infrastructures from an information security point-of-view.

It is suggested that the security of partitioned and the operational efficiency of non-partitioned infrastructures are required in combination, giving logically partitioned infrastructures. Logically partitioned infrastructures would therefore, increase the chances of successful security accreditation and enable true NEC through automated information transfer. This was also established in the NITEworks® ISTAR Theme, Phase 2 study [9] which addressed UK Collection Co-ordination issues whilst utilising a US-provided planning tool which would be used in a US-led US-UK coalition, supporting expeditionary operations. The core of this work was the identification of a security architecture that permitted a high level of data flow enabling the effective transfer of ISTAR information between UK/US and US/UK; as a result demonstrating the ability to achieve enhancements in timeliness, whilst implementing strict security controls to preserve the confidentiality and integrity of information.

Logically Partitioned Infrastructures
From figure 5 it can be seen that as information filters down the command chain, from highly complex *strategic aims* (high-level government policy directives) down to low-complexity *actions* (i.e. precise military orders e.g. formatted messages), the requirement for timeliness increases, moreover the resolution of the information also increases, resulting in well-defined and unambiguous commands. The tactical battlefield can be seen to be at the actions level in the command chain. From this it is argued that although the combination of communications in time-critical tactical battlefield scenarios such as IFPA are numerous; such exchanges exhibit sufficient precision and redundancy for pre-definition according to well-defined sets. These communications may then be securely executed in the form of automated M2M (Machine-to-Machine) communications removing the overheads associated with manual information transfer. This is in-line with contemporary risk management thinking, which proposes the limitation of processes[2] to only operate on data, for which the interpretation is bounded.

[2] A process in this context does not strictly relate to a software process, instead relating to any abstract computing capability operating on information in any way.

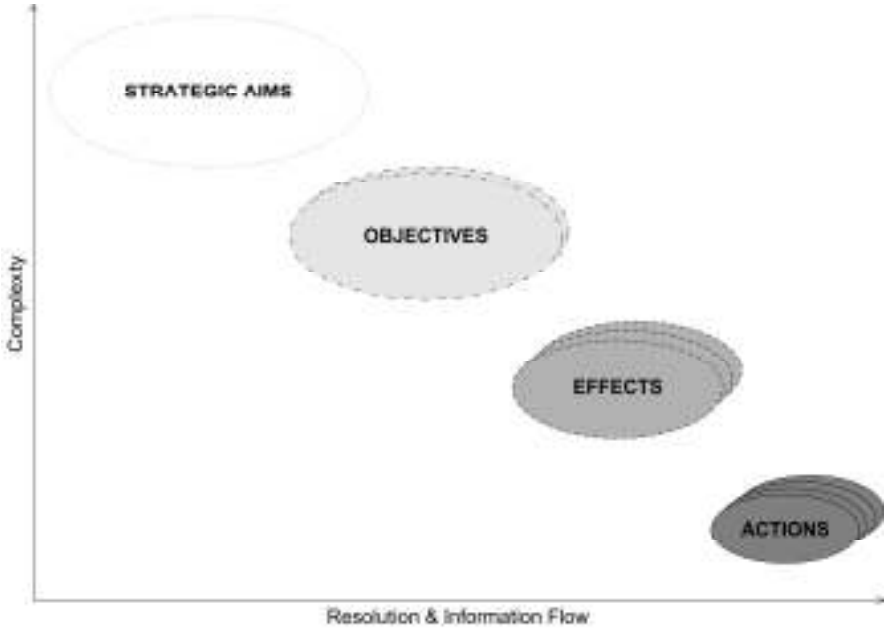

Figure 5: Illustration of the complexity of information in the command chain.

Research has been conducted into potential solutions for achieving logically partitioned infrastructures through automated information transfer processes as described in [1]. A method known as intra-system message filtering has been proposed which uses XML (Extensible Markup Language) as the messaging format. The main advantage of utilising an XML based solution is due to the schema definition functionality provided in the XML standard. This allows for an off the shelf solution for the *pre-definition*, *classification* and *validation* of messages. Systems may only receive data for which they have the necessary need-to-know (privilege). This can be seen to be analogous to the traditional computer security *subject-privilege-object* model. In which *users* are *subjects* who have an associated set of *privileges* (read, write etc.) over objects such as files, the user in this sense can be replaced by *machines*; the privilege relates to a machines' *need-to-know* with regards a particular object, which is the *communication*. Another major driver for using an XML based solution for electronic communications particularly M2M is due to its requirement as stated in [10], where XML is mandated as a non-tradable standard for data exchange, between UK MoD systems.

A high-level view of the architecture for intra-system message filtering is given in figure 6, where it can be seen that a trusted interface converts messages from proprietary formats to XML, individual system owners such as IFPA would need to define authorised communications for distinct sub-systems, using XML schemas. The trusted filter mechanism will be used to enforce restrictions on communications between sub-systems based upon the pre-defined schemas.

From an information security point-of-view the intra-system message filtering capability will preserve the *confidentiality* and *integrity* of information by ensuring only authorised information is communicated by all sub-systems. By removing the human in the loop for the actual transfer of data from one machine to another the issue of *timeliness* is also addressed, whilst removing the inaccuracies inevitably introduced by a human operator particularly under stressful conditions. Such an approach would limit potential bottlenecks in information flow due to air-gaps, allowing secure and rapid transfer of

information through automated processes. Another potential advantage of this method is that current systems using infrastructures such as BOWMAN, would not have to adapt their network interfaces or messaging formats in any way if they do not require segregation.

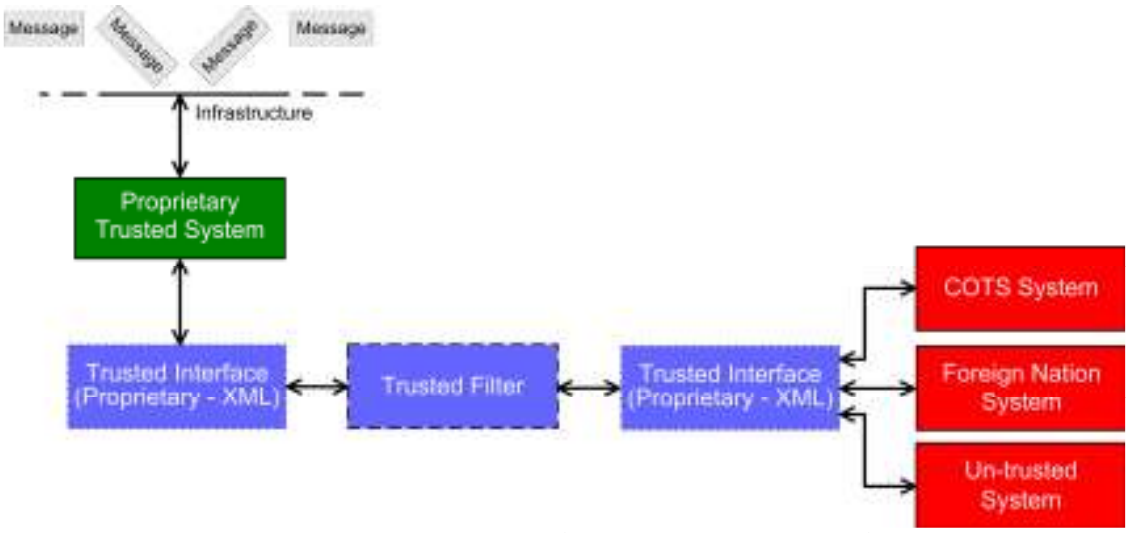

Figure 6: High-level overview of intra-system message filtering.

Summary

The traditional information security triangle has evolved with increased emphasis on the aspect of timeliness. This is reflected in the UK MoD's request in [1] for rapid information transfer through automated processes. The proliferation problem highlights how current security engineering and accreditation practices do not cater for these changing requirements.

Although the focus in this article has been on the immediate challenge of a tactical battlefield scenario it is argued that, as military CIS become more network enabled, the proliferation problem will become increasingly prevalent in other scenarios as demonstrated in the NITEworks® ISTAR Theme studies. If alternative solutions to the current cautious approach of partitioned infrastructures are not sought, then it is likely that security accreditation requirements will prove a major stumbling block in allowing the military of not just **doing things better** but **doing better things**, which according to the MoD [1] is necessary to realise the potential of NEC. Intra-system message filtering, which is a method for achieving secure and automated information transfer (logical infrastructure partitioning) has briefly been described as a way of overcoming the proliferation problem. Intra-system message filtering is the subject of on-going research at BAE Systems.

References

[1] MoD, *NEC Handbook: JSP777*, London, UK, 2005.

[2] NITEworks®*, www.niteworks.net*, UK, last visited 2005.

[3] MoD, *www.mod.uk/dpa/ipt/ifpa-jipt/index.html*, last visited 2005.

[4] MoD, *www.mod.uk/dpa/projects/cvf/page 2.htm*, last visited 2005.

[5] Assistant Security of Defense C3I, *Orange Book: Defense Trusted Computer System Evaluation Criteria*, USA DoD, 5200.28-STD, 1985.

[6] A.J. Herbert, *Compressing the Kill Chain*, Air Force Magazine, Arlington, Virginia, USA, 2003.

[7] K. Robinson, *Breaking Down the Barriers*, RUSI Defence Systems Journal, pp.62-65, London, UK, 2004.

[8] S. Philips, *ISTAR Theme Phase 1: Customer Report*, NITEworks® team, Technical Report NW/TH/IST/25, Farnborough, Hampshire, UK, 2004.

[9] S. Philips, *ISTAR Theme Phase 2: Customer Report*, NITEworks® team, Technical Report NW/TH/IST/102, Farnborough, Hampshire, UK, 2005.

[10] MoD, *Data Management Policy Set: JSP329*, London, UK, 2004.