Scientific Research and Essays Vol. 6(29), pp. 6095-6103, 30 November, 2011
Available online at http://www.academicjournals.org/SRE
DOI: 10.5897/SRE11.742
ISSN 1992-2248 ©2011 Academic Journals

*Full Length Research Paper*

# Proposed methodology to enhance C4I systems security on architectural level

**Abdullah Sharaf Alghamdi, Tazar Hussain, Gul Faraz Khan, Khalid Alnafjan and Abdul Haseeb**

Department of Software Engineering, College of Computer and Information Sciences, King Saud University, P.O. Box 51178 Riyadh 11543 Saudi Arabia.

Accepted 3 June, 2011

**Command control, communication, computer and intelligence (C4I) systems are the back bone complex information and communication systems for modern information warfare (IW). Managing security in C4I systems is a challenge due to complexity and criticality of these systems. This paper elaborates design methodology to incorporate security in the C4I systems in systematic and consistent way instead of patching and random approach. The approach in this work exploits the opportunity provided by architecture frameworks (AF) to capture threats and devise security measures. Assurance cases have been used to model security of the C4I system in order to enhance the process of security design and overcome challenges.**

**Key words:** C4I systems, information security, department of defense architecture framework, assurance cases, interoperability.

## INTRODUCTION

Information warfare is the concept of using information to achieve information superiority in the battlefield. Modern world is equipped with sophisticated technologies and information systems, information warfare use these technologies to achieve information superiority in land, sea and air (Zehetner, 2004). C4I systems works as backbone distributed, dispersed information and communication systems to support the concept of information superiority. Today C4I systems are used in military, transport, medical and communication systems especially where command and control C2 scenario exists. C4I systems also enable military commanders to make superior decisions in the battlefield and overall mission objectives rely on the accurate performance of these systems. Command and control C2 provide the necessary equipments, facilities, sensors, shooters to achieve the strategic objective of military forces. The operations of C4I systems rely on communication and computer infrastructure that process or transmit military classified and unclassified data. The increase reliance on information and communication systems makes these systems vulnerable to various types of attacks due to the fact that security is not treated as built in function of system design and development. In general IT systems, it is impossible to build defect free systems but in C4I systems the process is further complicated by high interoperability, network centricity and emergent nature. Threats to C4I systems are severe and normally are carried out in an organized way (Hancock, 2001). Computer emergency response team CERT statistics shows that the numbers of threats are increasing each year (CERT, 2008). Similarly, wireless sensor networks WSNs and mobile ad hoc networks MANET are the integral constituents of IW. Both WSNs and MANET have certain constraints with respect to security of these systems and give rise to complicated security threats (Hu and Sharma, 2005). The fact is that information security goals cannot be achieved only through sophisticated technology and security mechanisms but rather these technologies and mechanisms should be used as part of broader risk analysis process. In most cases security is not considered as built in process and when security vulnerability gets compromised patches are installed.

*Corresponding author. E-mail: imileusnic@gmail.com. Tel: (381) 13 351 292. Fax: (381) 13 366 582.

For example eye is one of the delicate organs of the human body which has the most crucial function of sighting but eyes are protected naturally by built in surrounding bones and eyelids and an involuntary natural actions have the ability to respond accordingly. But unfortunately, in information system functionality remains the top priority and the security mechanisms are considered only when vulnerability gets exploited. In this paper we have identified a methodology to suggest a systematic, built in mechanism so that security can be incorporated right from strategic to technical level.

Architecture frameworks (AF) break the complexity of systems in the shape of different viewpoints and models and this provide us the opportunity to capture security requirements. Once we capture the security concerns as built in process, systems can be modeled for security considerations, we have used assurance cases for modeling security. Assurance cases are like legal cases and are based on claim, argument and evidence structure and have already been used in the field of software assurance.

## NATURE OF C4I SYSTEMS

To achieve the strategic and operational goals of a military mission, C4I systems make use of technologies, software, commercial of the shelf COTS, legacy systems and weapon systems; to integrate these systems is difficult and complex. To manage and break complexity of C4I systems, different architecture frameworks have been developed such as department of defense architecture framework (DODAF) (Officer, 2010), UK ministry of defense architecture framework MODAF (Ministry, 2008) and NATO architecture framework NAF (NATO, 2007), these architectures are interrelated. In DODAF and MODAF, the C4I systems have been divided in different viewpoints, these different viewpoints highlight the different perspective of these systems for compliance and collaboration purposes among different stakeholders and units. To implement strategic and operational objectives systems and services are deployed to achieve goals of information warfare both in war and peace time. C4I systems are prone to various types of attacks because of the vulnerabilities which were not anticipated in design of these systems. C4I systems requirements are different from traditional systems and are under more stress because of high mobility, interoperability and net centricity. Interoperability is the ability of systems, units and forces to provide services and accept services from other systems and operate effectively together both at operational and technical level (Defense, 2007).

Network centricity also known as net centricity is an emerging theory of war that seeks to translate an information advantage into a competitive war fighting advantage through the robust networking of well informed, geographically-dispersed forces allowing new forms of war fighting (Renner, 2003).

## C4I SECURITY DIMENSIONS

Military's increase reliance on information and information systems increases the value of information infrastructure as military target. C4I systems are subject to various threats which compromise the confidentiality, integrity and availability of operations. Security engineering is the process of risk analysis to identify threats and propose counter measurements to reduce vulnerabilities. C4I systems are vulnerable to attacks from different dimensions (Wnnergren, 2009; Officer, 2010; Tselkov and Pargov, 2000); the following study identifies areas of security concerns for C4I systems in general.

### Physical

C4I nodes, communication infrastructure are deployed in hostile conditions for war fighting purposes; therefore measurement must be taken to protect computers, communication links and command and control facilities. Fences, guards, access control mechanisms and surveillance are the key measurements to secure the systems physically.

### Procedures and security policy

In C4I systems personnel having different access control authority to various resources for example the missile launching systems must not be activated without the prior permission of strategic level authority and commander in chief. In these situations, insider threat is the genuine type of threat that cannot even be stopped by sophisticated security technology and cryptographic mechanisms. Special personnel security clearance and trust is the key to evaluate that certain capability can be assigned to individuals. To protect sensitive information, set of rules and practices must be implemented so that only authorized personnel have access to command control and information systems. Security policy is normally mentioned in terms of subjects (processes, users, programs) and object (files, C2 facilities, devices), which evaluate who have access to what? (Trcek, 2000). DODAF and MODAF provides the opportunity to capture and design in security policy right from strategic level through operational and system level so that there may be alignment between subjects and objects. A range of access control mechanisms such as mandatory access control (MAC) and role based access control (RBAC) can be easily implemented.

### COMSEC

Managing communication security is difficult because C4I

systems are geographical dispersed and the links are f and broken frequently due to high mobility and hostile conditions (WSNs, manned and unmanned aerial vehicles). Other aspect of C4I systems is that it is heavily dependent on civilian communication systems such as internet which are not protected up to the military level. Encryption, security protocol and key management are the mechanisms that are applied to protect communication links. Both symmetric and asymmetric encryptions are required at different level such as link encryption, net encryption, bulk and end to end encryption.

**COMPUSEC**

COMSEC secure information in transit but large amount of classified and sensitive information resides on C4I computers and network nodes. COMPUSEC is concern to protect information from unauthorized use according to the stated procedures. Military information is normally protected through multiple level securities (MLS), discretionary access control and access control lists (ACLs).

**TEMPEST**

Weapon systems and C2 systems uses electromagnetic transmission such as WSNs and UAV and these systems are prone to jamming and interception. TEMPEST is about to secure electromagnetic transmission and to make sure that the resources are available with enough bandwidth and signal strength.

**INFOSEC**

INFOSEC (encompass COMPUSEC and COMSEC) is used to secure IT related systems and services in term of confidentiality, integrity, availability (CIA) and accountability. Confidentiality, Integrity and availability are the key features of C4I systems which are normally targeted through technical and non technical means (Smith, 2006; Tassabehji, 2011).

***Confidentiality***

Protection of sensitive data from unauthorized disclosure is the first priority specially in military systems. Unauthorized access to C4I computer through malware could enable the adversary to pass wrong messages in order to deceive military commander.

***Integrity***

To ensure that changes or alteration to information and programs can be made according to the security procedure so that information can be protected from unauthorized changes.

***Availability***

C4I users and systems must have reliable, accurate access to resources, bandwidth when ever required. For example, denying or delaying access to shooters systems may lead to disaster of the friendly forces. The aforementioned requirements must be implemented through accountability, authentication and authorization so that functions and activities can be audited and trace back to security policies.

**RELATED WORK**

In one of our previous work (Alghamdi et al., 2010) we applied goal oriented threat modeling to enhance the security of C4I systems on architectural level. This approach highlights and models the threats and associated counter measures in order to avoid known attacks. Assurance cases have been used for design analysis of complex systems of systems software for hypothetical military systems (Blanchette, 2009). The work in this paper discusses the application of assurance cases as a means of building confidence that the software design of a complex system of systems will actually meet the operational objectives set forth in the project's top-level requirement. Intrusion detection system and intrusion prevention system is another direction to secure the C4I systems. Therefore, an approach is provided to analyze denial of service attack by using a supervised neural network (Ahmad et al., 2009). The methodology used sampled data from Kddcup 99 dataset, an attack database that is a standard for judgment of attack detection tools. The system uses multiple layered perception architecture and resilient back propagation for its training and testing. Maule (2005) presented the architecture to support secure communication in joint and coalitions forces. The objective is to enable a more ready exchange of secured information within distributed environments. Military systems are composed of legacy systems, commercial of the shelf product (COTS) and new systems are constantly integrated to meet new operational and strategic requirements.

Bloomfield et al. (2006) have discussed in detail how assurance cases can be applied to US department of defense (DoD) projects. This study explains how assurance cases help in design analysis of defense systems.

**PROPOSED METHODOLOGY**

According to the open group architecture framework (TOGAF)

**Table 1.** DODAF operational, system and service views models and descriptions.

| Model | Description |
|---|---|
| OV-1: High level operational concept graphic | The high-level graphical/textual description of the operational concept. |
| OV-2: Operational resource flow description | A description of the resource flows exchanged between operational activities. |
| SV-1: Systems interface description | The identification of systems, system items and their interconnections. |
| SV-2: Systems resource flow description | A description of resource flows exchanged between systems. |
| SvcV-1: Services context description | The identification of services, service items and their interconnections. |
| SvcV-2: Services resource flow description | A description of resource flows exchanged between services. |

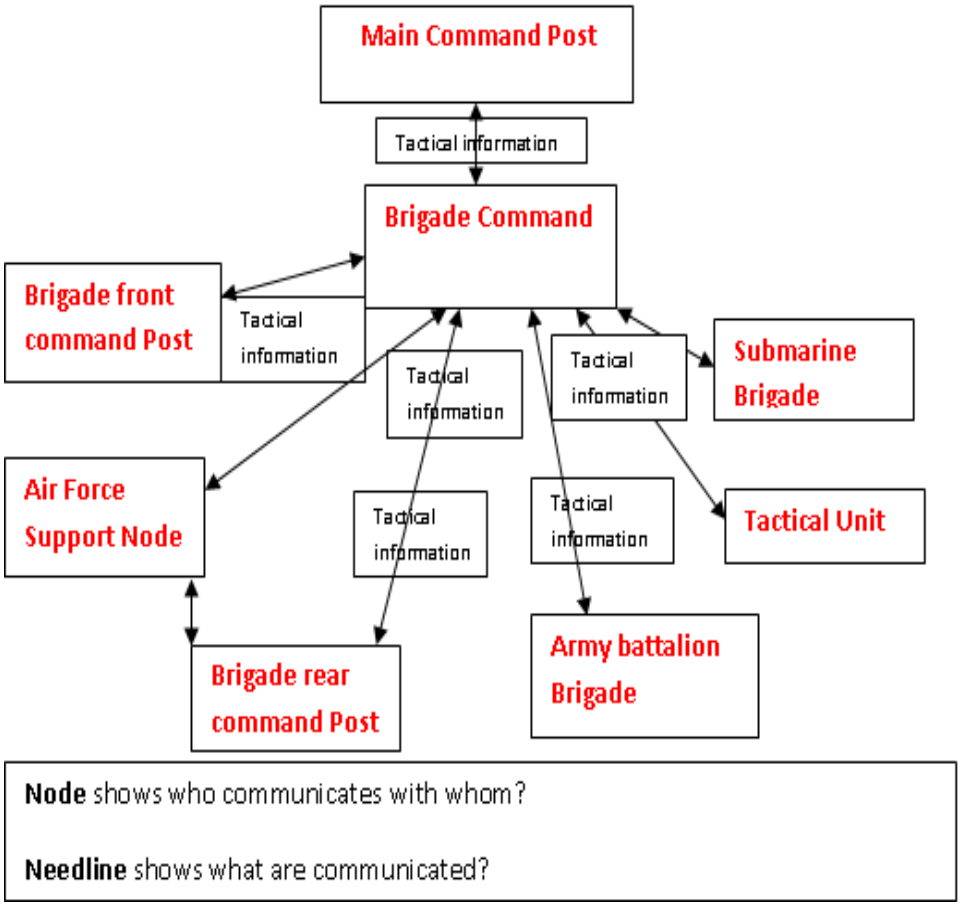


**Figure 1.** High level operational connectivity diagram.

(Group, 2011), an architecture framework is the tool to design information systems in terms of a set of building blocks and to show how building blocks fit together; it should also include common vocabulary and standards to implement building blocks. The goals of DODAF and MODAF as enterprise frameworks are to manage complexity, align business strategies and implementations, facilitate change, understanding holistic view and also facilitate the use of common principles, assumption and terminologies (Anderson et al., 2008; Mosto, 2004). The viewpoints in both DODAF and MODAF highlight different perspectives of the systems and describe the organizations in textual, tabular and dashboard formats. Table 1 shows two models of each DODAF operational, system and service viewpoints (Wnnergren, 2009). For example an operational viewpoint denotes operational activities in graphical or textual form and system and services viewpoints identify systems to support operational level activities. The main point in the aforementioned discussion to be noted is that there is a great opportunity to capture the associated security risks in a consistent way. We in this paper exploit this opportunity to design security on system level; this process has further been elaborated in the following study. In practical C4I operation, the forces are divided in different battalion; Figure 1 represents the different brigades from operational viewpoint OV1. OV represents the requirements, tasks and activities, information flow to achieve mission objectives. It is worth noting that these tasks and activities remain in line with the overall strategic objectives. Operational requirements are not designed in

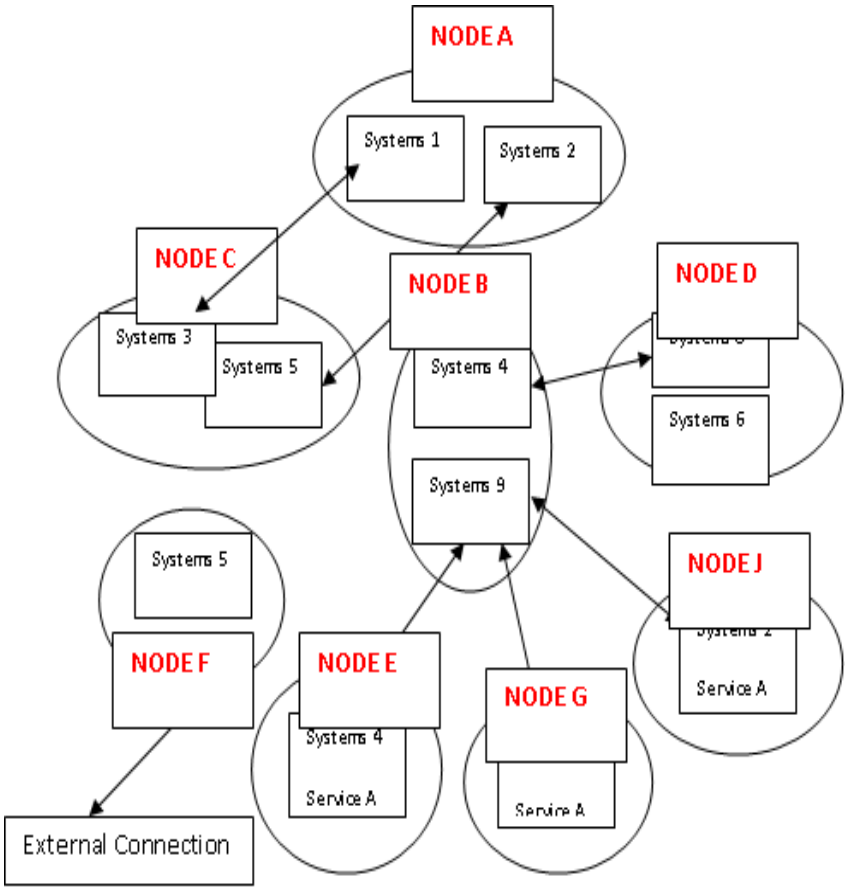


**Figure 2.** System and services viewpoints support operational activities.

isolation but rather are derived from the strategic viewpoint which is beneficial in many ways; for example, the sensitivity of information is decided on strategic level not at operational or system level. Operational viewpoints represent war fighting in terms of what tasks and activities to be carried out to meet mission objective; in DODAF version 2, OV also represent rules and constraints for any function. Figure 1 present only a fraction of the big picture while an enterprise architecture framework encompasses the whole enterprise (war fighting, business, intelligence etc). DODAF capture all the tasks and activities necessary and thus gives an opportunity to capture, identify critical nodes, links, classified and unclassified information.

The following useful information can be derived from Figure 1 which ultimately helps in security design right from operational and strategic level instead of patching:

i) Security level, criticality, environment and associated risks.
ii) Systems and services that can support the operational requirements.
iii) Security can be prioritized in terms of confidentiality, integrity and availability.
iv) Critical communication lines, resource flow and what is communicated can be understood accordingly.

Figure 2 represents the system and service viewpoints of DODAF to identify systems, system components, interconnections and software/services; it also relates systems characteristics to operational needs. DODAF thus provide a consistent, build in approach so that systems and services can be related and trace to operational needs. The following information can be derived to build in security according to requirement of the systems:

i) Critical systems, nodes, services can be identified in terms of associated threats, vulnerabilities, security level, strengths and weaknesses of particular operating systems and technologies.
ii) The type of information that reside on systems and transmitted through communication links can be derived so that security mechanisms can be implemented. This built in approach is very useful because in security engineering implementation of correct mechanism against set of vulnerabilities that can be prevented through that mechanism is crucial. For example intrusion detection systems are useful tool to detect and prevent anomalies but placement of such systems on wrong position or level could make these systems useless.
iii) According to mission requirements availability, confidentiality and integrity can be prioritized; for example availability may be preferred to confidentiality in some systems. Security mechanisms measurements for example access control methods, cryptographic tools, digital signatures, mechanisms to prevent denial of service attack DoS can be design based on risks analysis that we have from operational and system level requirements.
iv) Communication links and interfaces or connecting points are under great stress and strain because C4I systems are geographically dispersed and mobility requirement is high and condition remains hostile. In such scenario, weak links and points can be identified and counter measurements can be suggested. For

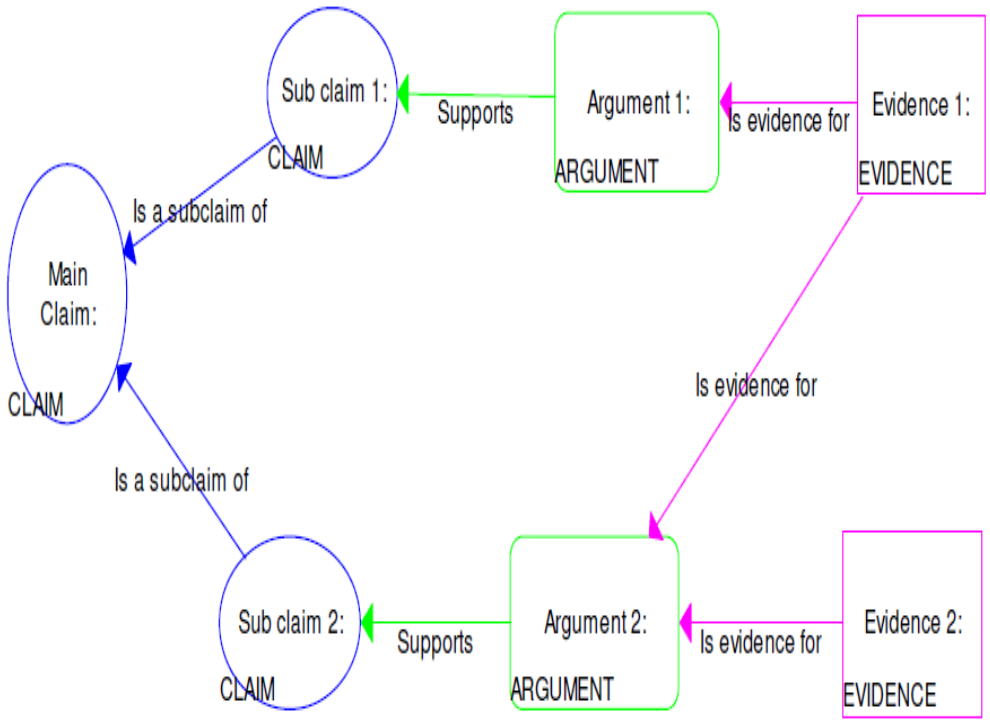


**Figure 3.** Basic components of assurance case and interrelationship.

example managing WSNs are very difficult to be managed due to hostile conditions, mobility and energy requirements. But loads of research has been done in this direction and effective mitigation can be applied.

v) Weak systems, connections and interconnection points can be identified and thus redundant links and systems can be installed as backups and even systems can be removed if these systems do not support operational requirements.

The aforementioned security concepts that have been derived from DOADAF are limited to two views from OV, SV and SvC each and on the other hand AF is like urban planning and covers all aspects of enterprise. But all other aspects can be modeled and captured in the same way where security can be engineered in consistent way through various viewpoints. The aforementioned methodology describes how to capture security requirements from DODAF which cover nearly all aspects and building blocks of organizations. Although DODAF (Wnnergren, 2009) and MODAF (Ministry, 2008) identify different viewpoints, security characteristics and countermeasures but there is a space for improvement. Different viewpoint identify processes and activities and how those process and activities are supported by information systems but it does not identify the associated risks and counter measures.

## APPLICATION OF ASSURANCE CASES TO C4I SYSTEMS

Data confidentiality, integrity and availability are the basic tenets and must be satisfied; other security services include non repudiation, accountability, authorization and authentication. Assurance case allows to reason about complex systems and assures that certain requirements have been met. In the following study, we have explained how to apply assurance cases to a hypothetical C4I system in accordance with the proposed methodology to assure that security has been built in as design process.

### Assurance cases

“A security assurance case uses a structured set of arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security requirements. The case should be amenable to review by a wide variety of stakeholders (Lipson, 2008)”. The security assurance case starts with a claim which satisfies the security requirements of particular system or part of systems in question. The claim is supported by sub claims and a related set of arguments until the claim and sub claims are satisfied by concrete evidence. Figure 3 shows how different sub claims and a set of arguments link the main claim to acceptable evidences. In the process of claiming, arguments and concluding evidences, all stakeholders review the security of the system and decide whether the case is credible. Like legal case, the arguments play a major role, but credibility of the arguments and of security case itself depends on the foundation of the evidences (Lipson and Weinstock, 2008).

### Elements of assurance cases

Claim is a statement which represents a property or characteristic of a system; in our case it represents the security of the system. Claim is further tested for truthfulness through sub claims, arguments and evidences. What kind of claims should be made depends on the available standard procedure and satisfaction among stakeholders of the systems. Arguments are the supporting statements, judgments and are derived through brainstorming, reasoning in particular context of the claim. Developers, system

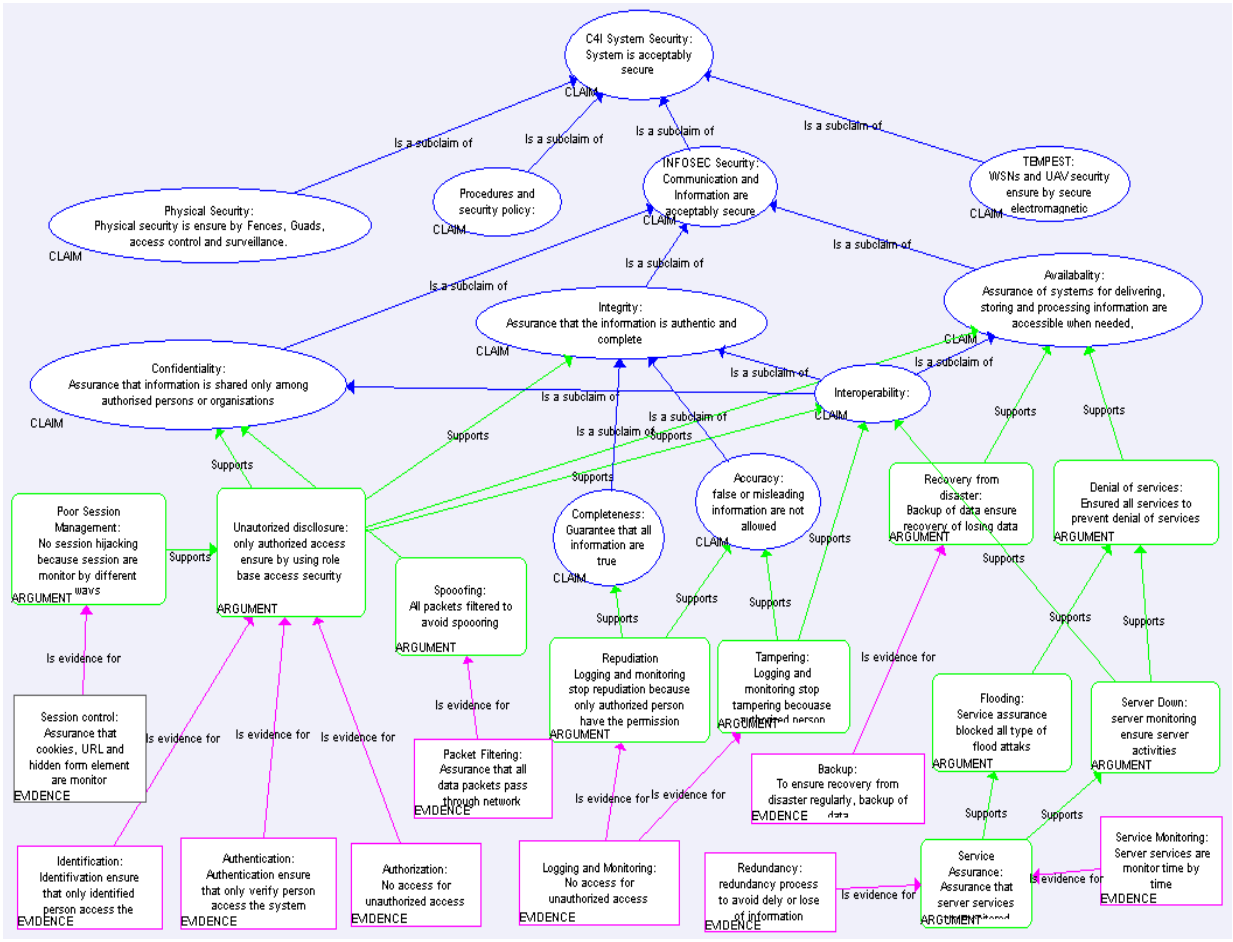


**Figure 4.** Assurance case model of C4I security.

engineers, managers and users may have different set of arguments but assurance case provides the opportunity to see the system transparently. Evidence confirm and verify the truthfulness in the context of the claim being made, evidence must be undisputable among stakeholders. The strength of the evidence depends on the knowledge and available mechanisms about the system in question. Evidence emerges as final product of claims and arguments therefore authenticity and originality of evidence depends on correctness and accuracy of arguments, sub claims and claims in the particular environment.

### Tools

Creating assurance case for a system is complex and cumbersome therefore automated tools are good in facilitating the process. Goal structuring notation (GSN) (Kelly and Weaver, 2004) and claims arguments evidence (CAE) (Rhodes et al., 2010) are the types of tools that can be used. We have used CAE to create assurance cases for C4I system security modeling CAE represent system in graphical notation.

## Assurance cases results

It has been identified earlier how security requirements of C4I systems can be captured. In the following study, we demonstrate an example to show how to model the captured information so that all aspect of security can be covered. Fundamental security goals of security for example confidentiality, integrity and availability have been modeled. Figure 4 starts with the top level claims about the security of the system for example “the C4I system is acceptably secure” and then there are different dimensions of securing C4I systems but we have extended only the INFOSEC in order to ensure the claims about confidentiality, integrity and availability. The process subsequently continues to identify arguments and provide evidences to the threats in shape of counter measurements. For example spoofing and unauthorized access is a threat to confidentially but unauthorized disclosure can also affect availability and integrity as shown. WSNs, weapon systems, shooters and other systems can be identified in terms of confidentiality, integrity and availability so that security concerns can be prioritized. Flooding is a threat for availability but can be medicated through service assurance technique but it also help to mitigate poor session which is also threat to availability. This systematic way of modeling assures that

every prioritized threat in particular system gets mitigated and also duplicated mitigations can be avoided. Multilayer security can be applied for example role base, discretionary and mandatory access control mechanism can be applied as required. When different units and systems interoperate, interconnections are crucial and may rise to threats as identified in the model.

Interoperability is an unanticipated behavior of the system and can affect confidentiality, integrity and availability. Claim is the positive statement about security of the systems, threats to a claim have been considered as arguments and counter measures are depicted as evidences.

### *Claim*

**INFOSEC:** Communication and information are acceptably secure.

### *Sub claim*

**Confidentiality:** Assurance that information is accessed only by authorized persons or organizations.

### *Arguments*

1) Unauthorized access is threat to confidentiality; 2) Poor session management leads to session hijacking; and 3) spoofing is also a threat to confidentiality.

### *Evidences*

Application of identification, authorization and authentication techniques is evidence (Figure 4) which satisfies argument 1. Session control is ensured through URL, cookies and hidden form elements monitoring which satisfies arguments and similarly packet filtering according to policy satisfies argument 3.

## DISCUSSION

We applied the proposed methodology to a hypothetical system and the process proved affective in securing this system in organized way because correct mitigation techniques were implemented as a result. Creating assurance case was advantageous for C4I systems in many ways for example it resolve the stakeholders diversity issue in C4I systems (Office, 2008). Managing security for complex information systems like C4I systems is multifaceted because these system are based on the concept of system of systems for example one C4I systems may represent missile launching systems, weapon system and WSNs. Every component system integrates and interoperates with other systems and makes it hard to engineer security. But assurance case provides us with the opportunity to model security in systematic and consistent way as a system engineering process. Assurance cases provide the opportunity for the analysis team to reason through arguments on all level to assure that all the related requirements have been satisfied through evidences. There are certain limitations to approach applied in this paper as this approach has been tested only on hypothetical system and actual C4I system may not produce similar results. The research in this paper covers the limited section of C4I systems and architecture framework's models. The approach also has limitation in terms of how actually military brigade commands are deployed in practical environments.

## CONCLUSION AND FUTURE WORK

Complex information and communication systems are difficult to be mange in terms of security engineering due to diverse infrastructure, heterogeneous technology, high mobility and interoperability. This paper demonstrates how assurance cases are capable in dealing with 'security' concerns of complex systems especially when security requirements can be captured through architecture frameworks. Research in this paper also helps in achieving the concept of security built instead of applying security in random and ambiguous way. The work in this paper is just the beginning and in future much needs to be done for example: 1) Structure mechanism to capture and model threats from architecture frameworks. 2) The security case needs to be validated and 3) needs mechanism for credible arguments and claims? To achieve more credible results the modelling technique in this paper must be tested with a simulation approach so that we can edit the required input and output.

## ACKNOWLEDGEMENT

This work was supported by the Research Center of College of Computer and Information Sciences, King Saud University. The authors are grateful for this support.

## REFERENCES

Ahmad I, Abdullah AB, Alghamdi AS (2009). Application of Artificial Neural Network in Detection of DOS Attacks. ACM International Conference on Security of Information and Networks. Gazimagusa, North Cyprus, Turkey. pp. 229-234.

Alghamdi, AS, Hussain T, Khan GF (2010). Enhancing C4I Security Using Threat Modeling. 12th International Conference on Computer Modelling and Simulation (UKSim), pp. 131-136.

Anderson MS, Martin SM, Dagli C, Miller A, Boeing Co, Rolla MO (2008). Implementing an Architectural Framework to Define and Deliver Net-Centric Capability to Legacy Military Air Assets Operating within a System of Systems. 2nd Annual IEEE Systems Conference.

Blanchette S (2009). Assurance Cases For Design Analysis Of Complex System Of Systems Software.American Institute of Aeronautics and Astronautics, Software Engineering Institute, Pittsburgh, PA, 15213.
Bloomfield RE, Guerra S, Miller A, Masera M, Weinstock CB (2006). International Working Group on Assurance Cases (for Security),‖ IEEE Security Privacy, 4(3): 66-68.
CERT (2008). CERT Statistics (Historical). Retrieved, from http://www.cert.org/stats/.
Defense UDO (2007). The Defense Acquisition System. from http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.
Group TO (2011). The Open Group Architecture Framework. from http://pubs.opengroup.org/architecture/togaf8-doc/arch/.
Hancock B (2001). Information Warfare Highlighted as a Concern by US Government. Comput. Security, 20(1): 8-9.
Hu F, Sharma NK (2005). Security considerations in ad hoc sensor networks. Ad Hoc Networks 3(1): 69-89.
Kelly T, Weaver R (2004). The Goal Structuring Notation - A Safety Argument Notation. in Proceedings of the Dependable Systems and Networks Workshop on Assurance Cases, Department of Computer Science and Department of Management Studies University of York, York, YO10 5DD UK.
Lipson H (2008). Assurance Cases Overview. The Build Security In Software Assurance Initiative (BSI). Retrieved 10 April, 2011, from https://buildsecurityin.us-cert.gov/bsi/about_us.html.
Lipson H, Weinstock C (2008). Evidence of Assurance: Laying the Foundation for a Credible Security Case. Build Security In, Carnegie Mellon University Software Engineering Institute.
Maule RW (2005). Enterprise knowledge security architecture for military experimentation. IEEE International Conference on Systems, Man and Cybernetics, (4): 3409.
Ministry UD (2008). UK Ministry of Defense Architecture Framework MODAF revision version 1.2. Retrieved 15 March 2011, from www.mod.org.uk
Mosto A (2004). DoD Architecture Framework Overview. Retrieved 12 April 2011, from www.enterprise-architecture.info/Images/.../DODAF.ppt.
NATO (2007). NATO architecture framework NAF version 3.0. Retrieved 17 March 2011, from http://www.nhqc3s.nato.int/ARCHITECTURE/_docs/NAF_v3/ANNEX 1.pdf.
Officer DDCI (2010). Department of defense architecture framework DODAF V 2.0. from http://cio-nii.defense.gov/sites/dodaf20/.
Office of the Deputy under Secretary of Defense for Acquisition and Technology (2008). Systems and Software Engineering. Systems Engineering Guide for Systems of Systems, Version 1.0. Washington, DC: ODUSD(A&T)SSE
Renner S (2003). Building Information Systems for Network-Centric Warfare. In the proceedings of 8th Int. C2 Research and Technology Symposium. Washington DC.
Rhodes T, Boland F, Fong E, Kass M (2010). Software Assurance Using Structured Assurance Case Models. J. Res. Natl. Inst. Stand. Technol., 115(3): 209-216.
Smith DJ (2006). Information Operations Primer, Dept. of Military Strategy, Planning and Operations, US Army War College, AY07 Edition.
Tassabehji R (2011). Information Security: Evolution To Prominence. from http://encyclopedia.jrank.org/articles/pages/6627/Information-Security-Threats.html.
Trcek D (2000). Security policy conceptual modeling and formalization for networked information systems. Comput. Commun., 23(17): 1716-1723.
Tselkov V, Pargov D (2000). Information Assurance in C4I systems. International Relations and Security Network (Information Assurance and security).
Wnnergren DM (2009). Department of defense Architecture Framework Version 2.0, Volume 1 Introduction, Overview, and Concepts, Manager's Guide.
Wnnergren DM (2009). Department of defense Architecture Framework Version 2.0, Volume 2, Architectural Data and Models, Architect's Guide
Zehetner AR (2004). Information Operations: The Impacts on C4I Systems. Association of Old Crows AOC International Symposium and Exhibition Adelaide, Australia, Information Security Group Electronic Warfare Associates - Australia.