13TH ICCRTS

Final Student Paper #086

February 25, 2008

Title: **Potential Benefits & Implications of Privacy Protection and Anonymity for Command & Control through "Hidden Communications Services"**

Topics:	Military and Civilian C2
	Networks and Network Systems
Name of Author:	John A. Sturm
Point of Contact:	same
University:	PhD Candidate - Indiana State University
Name of Organization:	NuParadigm Government Systems, Inc.
Complete Address:	12977 North Forty Drive, Suite 200
	St. Louis, MO 63141
Telephone:	(314) 401-6850
E-mail Address:	jsturm@nuparadigm.com

Abstract

As the style of warfare has changed to support sudden regional conflicts and ad hoc humanitarian missions for disaster relief (e.g., Hurricane Katrina), so has the style of Command & Control (C2) needed to incorporate civilian intelligence sources (non-government organizations-NGOs) and embrace government authorities. It is difficult to predict in advance what sources of intelligence will be used, and if one is communicating with "small civilian cells"; the Internet might be the only available channel. However, the need still exists to protect the sources & methods employed for intelligence gathering from disclosure. Likewise the deployment of military resources, such as naval vessels, needs to be protected even if serving civilian aid. One possible method of protecting intelligence and C2 communications would be through the creation of a "Hidden Communications Web Service" in which the source and destination of IP messaging was kept hidden/anonymous, but authentication and authorization for access could be maintained as needed. The concept of "Onion Routing" (Tor) was developed

several years ago by Goldschlag, Reed, and Syverson at the Naval Research Laboratory to provide anonymity on the Internet and has led to many "civilian" implementations world-wide through open-source software (e.g., Tor).

Introduction

The Internet offers tremendous value for consumers to receive information, entertainment, education, etc., but it is also a very dangerous and unregulated environment. In addition, the Internet has become the essential channel for world-wide purchasing and distribution of goods. By analogy it is also as lawless as the Wild West of the 1800s when mail, money and goods were routinely stolen and personal travel was dangerous (due to personal attack or viruses like Small Pox).

The "Onion Routing" (Tor) technology mentioned above has been used by various human rights groups for maintaining individuals' anonymity in various countries and providing uncensored Internet access to those behind the "Great Firewall of China". But it has also been used to protect both DoD personnel communicating from remote locations and open intelligence gathering. The potential exists for various military services to achieve some degree of "anonymity" through using a robust version of Tor as a web services application for C2 communications and intelligence input from civilian sources.

NuParadigm has served as part of the GIG Information Assurance (IA) SPO Working Group to the NSA that drafted the original GIG IA Reference Capability Documents (RCD). Since then NuParadigm has continued to work under contract with Navy SPAWAR to develop concepts for innovative IA tools & techniques. As mentioned, the Naval Research Laboratory developed the Onion Routing (Tor) concept for information assurance several years ago (Goldschlag, Reed, and Syverson 1998) and it has been reproduced in many "civilian" implementations world-wide. In their 1998 paper on Tor they stated:

> *Onion Routing is an infrastructure for private communication over a public network. It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. Onion routing's anonymous connections are bidirectional and near real-time, and can be used anywhere a socket connection can be used. Any identifying information must be in the data stream carried over an anonymous connection. An onion is a data structure that is treated as the destination address by onion routers; thus, it is*

used to establish an anonymous connection. Onions themselves appear differently to each onion router as well as to network observers. The same goes for data carried over the connections they establish. Proxy aware applications, such as web browsing and e-mail, require no modification to use onion routing, and do so through a series of proxies.

NuParadigm has studied the feasibility of creating a "Hidden Communications" Web Service for Command & Control (C2) use and has a proposal pending. The Hidden Communications service could be employed as the situation warrants and offers the promise of enhanced information assurance capabilities for C2. It is important for Combatant Commanders (COCOMs) to trust the authenticity, integrity and delivery of distributed data sources while maintaining the privacy of users and be able to audit information within the GIG-NCES (Global Information Grid - Net-Centric Enterprise Services) framework. In essence we view the implementation of Onion Routing (Tor) or other "Anonymizing Techniques" as a valuable component of Information Assurance for the Global Information Grid (GIG) in the future. If implemented properly, Tor could be one of a family of Information Assurance tools for COCOMs to use.

In fact, implementation of Tor serves to add "High Assurance" capability as defined in the Common Criteria (see References) for High Assurance systems. For instance the Common Criteria specifications include privacy, anonymity, pseudonymity (secure auditing), unlinkability, unobservability, etc. as components of a High Assurance device such as a HAIPE (High Assurance Internet Protocol Encryptor) for Certification & Accreditation. If possible, why not add selected High Assurance capabilities into the IA for Command & Control to be used as needed?

The increasing focus on network-centric warfare means that the ability to ensure the source and the integrity of data while protecting the privacy and prioritization of the user will be key to military operations. The "anonymity" service also offers benefits to empower & protect the Warfighter by assessing the offensive/defensive effectiveness of that service (which is analogous to "Laundering money" and "Following the money trail"----in other words, preventing counterintelligence).

Our approach has been to study the feasibility of deploying a family of services that aid the Warfighters and other designated "roles" by tailoring the implementation of Information

Assurance (IA) technology to proactively support and enhance their mission tasks. Without understanding the unique challenges faced by Warfighters in different contexts, IA can represent a costly burden by consuming their resources while leaving a trail for the enemy to use to decipher their mission intentions. Many times the Common Criteria (CC) has been viewed as a necessary evil that slows system development and adds cost, but clever planning can turn the CC into a real benefit by protecting Warfighters in the execution of their mission.

The Common Criteria offers High Assurance Benefits for C2 & Warfighters

In fact, NuParadigm has studied the Common Criteria guidance alongside the Onion Routing technology in order to illustrate their synergy. The following diagram is from Part 2 of the Common Criteria Security Evaluation (see References) and highlights the concept of "Target of Evaluation" (TOE) as the context for study. Conceptually, the "Hidden Communications Service" capability would be considered the "TOE" and the "TSF DATA" is the set of "TOE Security Functions" (TSF) that includes Authentication Data and Security Attributes (for User, Object, Subject and Information). Thus our work will serve to "bridge the needs" of the Warfighter and GIG IA Requirements into a Model for high assurance and accreditation.

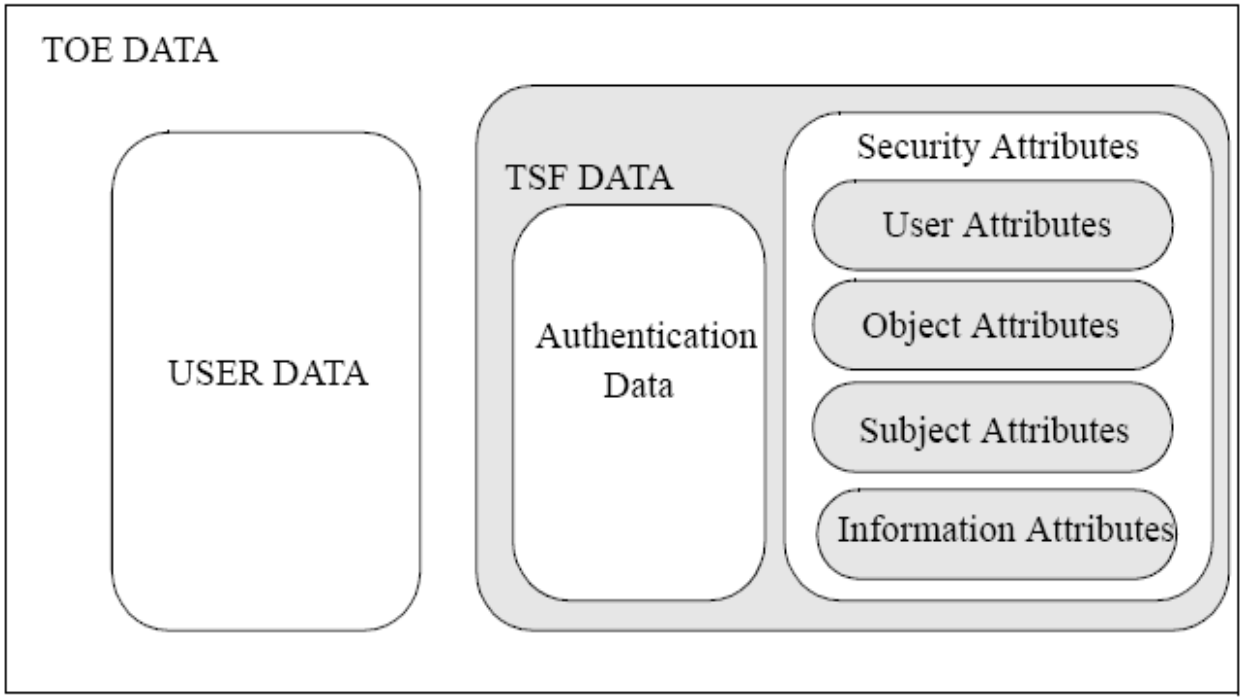

Figure 1.3 – Relationship between user data and Target of Evaluation (TOE) Security Function Data (TSF) – (From Part 2 of the Common Criteria Security Evaluation)

The research challenge spans multiple levels and faces several paradoxes that we need to solve. The NuParadigm Foundation™ software provides a sophisticated Service Oriented Architecture (SOA) development environment to create & model the secure object framework required for managing access to distributed data sources. The development environment creates layered object encryption boundaries which allow for separation of the "data and control planes" that is key to exposing data/tags/attributes as necessary, yet keeping data encrypted/hidden ("cloaked") per the CC guidelines.

Object-Oriented Solution Approach to Connect C2 with the "Edge"

In addition, NuParadigm has extensive experience building object-oriented integration frameworks allowing the "Edge Connection Tasks" to mediate connections locally as required rather than relying on backbone processes to serve requirements. Further, such a system implies a high degree of capability to extend and customize the "Edge" to adapt to the peculiarities of the systems being connected and enable QoS, CoS, SoM, etc. Any effective Edge gateway will have to accommodate highly detailed MOUs (Memo of Understanding) between consumers of information and suppliers, such as real-time C4I and "Intel" systems. The "Edge Process" gateway will be responsible for implementing the MOUs and supplying assured context among the "System of Systems". This implies the ability to support an "n-dimensional" mapping of the applications context at the connection and the translation of the context to a common framework. The MOU would then be represented as a "rule base" for deciding whether a transaction or its data content is permitted by the MOU or not. This approach would also provide an effective tool for protecting sources & methods of intelligence gathering by employing "Hidden Web Services" for anonymity as required. In addition, the "rule base" can intelligently provide logging & alerting of transactions and handle mal-formed requests or data. These "policy control points" can be layered to aggregate and disaggregate policy from the "rule base" with increasing or decreasing levels of granularity to insure Warfighters' security while providing access to the data they need.

The concept includes an interface that allows both sides of the "Edge Process" (gateway) to directly control and audit the operation of the portion of the gateway under their jurisdiction. This separation assures both C2 and Warfighters that they continue to have objective control of what is happening in their own system. In other words, the Warfighter can set their rules for

access to data (without revealing their whereabouts) and the COCOM can also invoke the appropriate security policies to insure that they (or the Warfighter) have not been compromised.

As stated, the authenticity of data, the reliability of the transport, and the privacy/anonymity of users are critical to mission success in the network-centric warfare paradigm. The NCES framework currently lacks sufficient definition in these areas and further research is warranted. Any uncertainties about sources providing key battle management data, its dependability, or the possibility of compromising the identity of the user, are critical shortcomings for the Warfighter. As we all follow the GIG IA Architecture intent (see diagram below), and provide more automated systems to the Warfighters (where "non-person-entities - NPE" such as servers, PEP/PDP, etc are "users" as well and have identities), all aspects of "distributed trust" must be accounted for, including anonymity and pseudonymity. As an example, the GIG IA Architecture below illustrates the exchange of Identity information among participants through a Security Management Infrastructure (potentially a secure object framework) based on the type of IA Attributes described in the earlier Figure (user, object, subject, information-QoS, QoP, etc.).

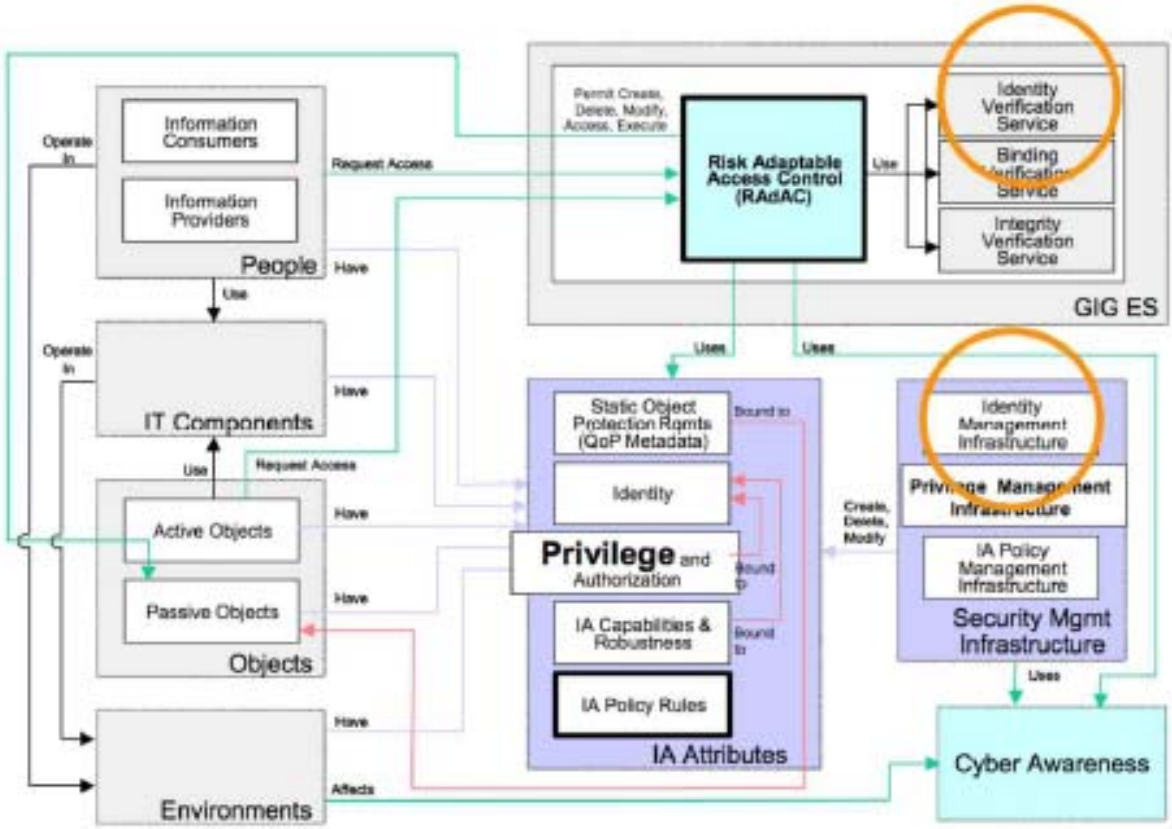

Figure – Global Information Grid (GIG) Information Assurance Architecture

Additionally, this concept of “Hidden Communications Services” adds either direct or indirect support for the five major IA gaps stated by OSD:

- *Trusting the Edge (Distributed Trust Model)* ----
    - through a Distributed Trust Model for nodes & users,
    - through High Assurance platforms,

- *Security Management Infrastructure* ----
    - through Automated and adaptable dynamic policy applications,
    - through Risk Adaptive Access Control (RAdAC),

- *Secure mobility for future GIG warfighter networks* ----
    - through wireless security architectures,
    - through authenticated User/Devices,

- *Assured Information Sharing* ----
    - through Cross Domain Solutions,
    -
- *Situational Awareness and Response/Enterprise Health* ----
    - through Node-based situation assessment, and
    - through Automated network reconfiguration, recovery and reconstitution.

Prioritization of Traffic for C2

As mentioned, Naval Research Labs has conducted considerable research (see References) into anonymous routing methods for privacy protection. However, the same methods of concealment must also enable prioritization of traffic based on QoS and CoS metrics. The challenge is to solve the paradox of maintaining privacy/anonymity while enabling prioritization of selected message streams. In addition, applications should be able to negotiate "prioritization" of transport with the network layer for QoS, CoS and SoM (Strength of Method). This effort is in-line with NSA’s “Quality of Protection” (QoP) vision. The NuParadigm approach is to extend our family of IA Services to enable prioritization of traffic based on QoS and CoS metrics. In our concept, we would enable applications to negotiate "prioritization" of transport with the network layer for QoS, CoS and SoM.

The complexity of managing these factors is multiplied in the event of operations involving coalition forces across diverse networks that support dynamic communities of interest. The ability to dynamically deliver the right information to the Warfighter in the field in a trusted and reliable manner needs to be built on the negotiation and exchange of data between the supplying & consuming systems. Systematically planning and verifying these exchanges, through

Modeling & Simulation of the GIG based on the direct needs of the Warfighters, would insure that all such systems released into the field will be readily accepted and used by their recipients. All of these driving factors are critical to achieving the operational system vision of the net-centric Warfighter of the future. The vision, however, must also be balanced with the realization that these highly valued services are key targets for the enemy. As such, it is also necessary to provide facilities to insure that all of these resources can be actively monitored in a highly secured and controlled manner so that any suspicions of their falling into enemy hands can be reacted to swiftly and appropriately. Modeling & Simulation of the IA family of services described earlier provides valuable insight into the value/cost/benefit of various IA services to the Warfighter. The value of M&S is in its ability to observe the behavior of different IA methods across different contexts and in combination with different communications channels and/or protocols.

Key High Assurance System Requirements for SOA & IA within the Common Criteria

As the GIG evolves into a complex system of systems, it is also reasonable that the GIG should adhere to many of the Common Criteria requirements for "High Assurance" devices such as Privacy, Anonymity, Pseudonymity, Unlinkability, Unobservability, etc. It is interesting to quote James Moffat (2003, pg.48) from the OSD publication on Complexity Theory and Network Centric Warfare, "Combat is, by its nature, a complex activity…….to properly control such a system, the variety of the controller (the number of accessible states which it can occupy) must match the variety of the combat system itself. The control system itself, in other words, has to be complex." Thus one of the jobs of IA (and SOA as the communications path) is to protect & defend the complex network capabilities essential to Command & Control (C2). In other words, the Warfighter needs to be better "connected" than the enemy to maintain military superiority.

Following is a condensed version of the relevant sections of the Common Criteria Part 2 requirements for protection of High Assurance devices & systems. Since many of the same challenges & issues listed above are contained in the CC requirements, we have used the CC as a starting point to define the SOA & IA architectures since any design must eventually be accredited according to the same requirements:

The "Common Criteria" (CC) for High Assurance (HA) systems provides the base level requirements for HA systems. Per the CC, "These requirements describe the desired security behavior expected of a Target of Evaluation (TOE) ..... Security functional components express security requirements intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organizational security policies and assumptions. Figures 1.1 and 1.2 (and Figure 1.3 shown previously) depict some of the key concepts of the paradigm.

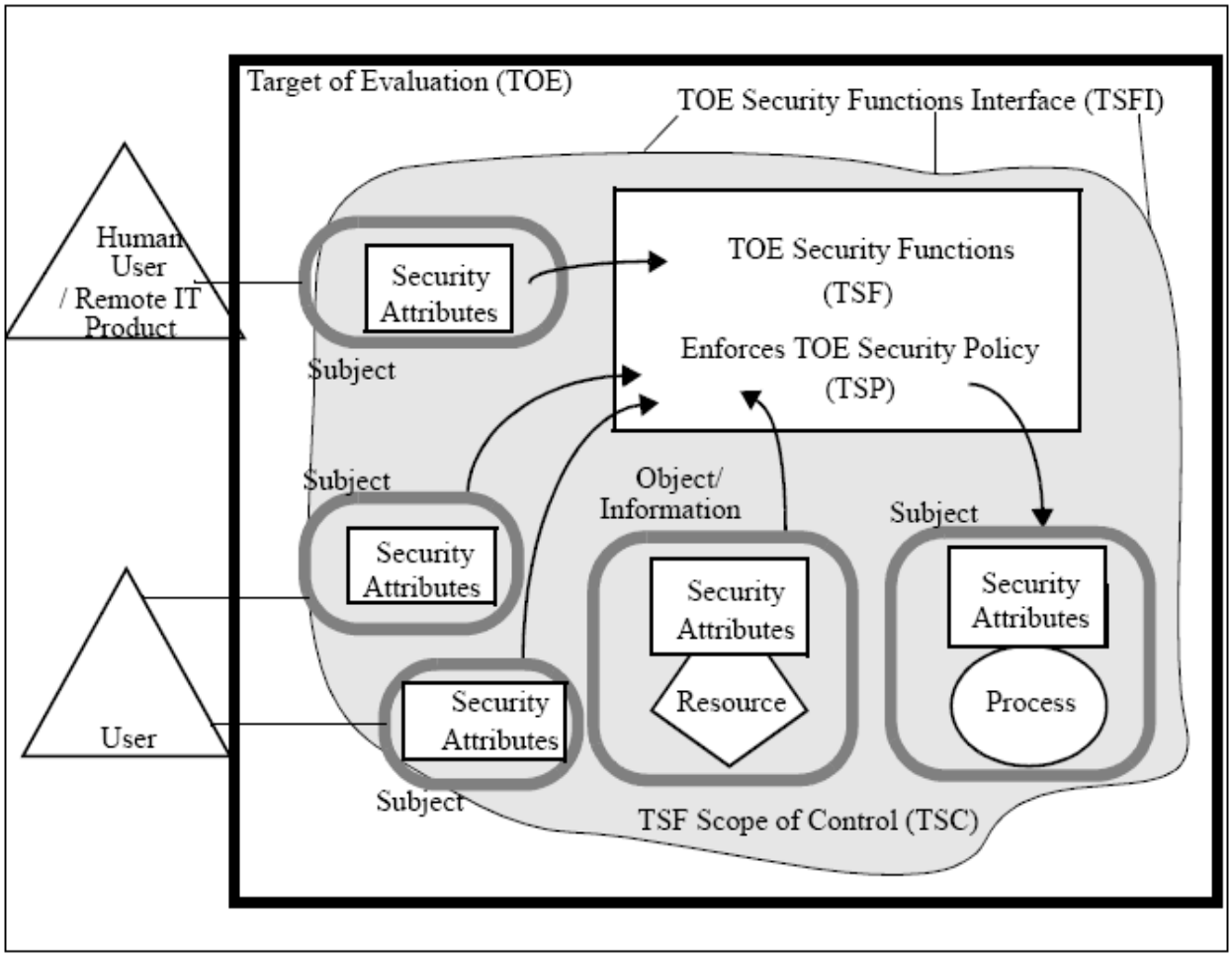

Figure 1.1 - Security functional requirements paradigm (Monolithic TOE)

This part of the CC is a catalogue of security functional requirements that can be specified for a ***Target of Evaluation (TOE)****. A TOE is an IT product or system (along with user and administrator guidance documentation) containing resources such as electronic storage media (e.g. disks), peripheral devices (e.g. printers), and computing capacity (e.g. CPU time) that can be used for processing and storing information and is*

the subject of an evaluation **(namely the "Secure Edge Process" gateway described earlier)**. *TOE evaluation is concerned primarily with ensuring that a defined* ***TOE Security Policy (TSP)*** *is enforced over the TOE resources. The TSP defines the rules by which the TOE governs access to its resources, and thus all information and services controlled by the TOE.*

The TSP is, in turn, made up of multiple ***Security Function Policies (SFPs)****. Each SFP has a scope of control, that defines the subjects, objects, and operations controlled under the SFP. The SFP is implemented by a* ***Security Function (SF)****, whose mechanisms enforce the policy and provide necessary capabilities. Those portions of a TOE that must be relied on for the correct enforcement of the TSP are collectively referred to as the* ***TOE Security Functions (TSF)****. The TSF consists of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement.*

The TOE may be a monolithic product containing hardware, firmware, and software **(such as the "Secure Edge Process" gateway)**. *Alternatively a TOE may be a distributed product that consists internally of multiple separated parts* **(such as the System of Web Services that manage secure, anonymous access to distributed data sources from the "Edge")**. *Each of these parts of the TOE provides a particular service for the TOE, and is connected to the other parts of the TOE through an* ***internal communication channel****. This channel can be as small as a processor bus, or may encompass a network internal to the TOE* **(i.e. the Control Plane)**.

When the TOE consists of multiple parts, each part of the TOE may have its own part of the TSF which exchanges user and TSF data over internal communication channels with other parts of the TSF. This interaction is called ***internal TOE transfer*** **(i.e. Control Plane information)**. *In this case the separate parts of the TSF abstractly form the composite TSF, which enforces the TSP.* **(Separation of the multiple Data Planes & Control Planes is critical to support the Common Criteria recommendations.)**

TOE interfaces may be localized to the particular TOE, or they may allow interaction with other IT products over ***external communication channels****. These external interactions with other IT products may take two forms:*

a) The security policy of the 'remote trusted IT product' **(such as the "Secure Edge Process" gateway)** *and the TSP of the local TOEs have been administratively coordinated and evaluated. Exchanges of information in this situation are called* ***inter-TSF transfers****, as they are between the TSFs of distinct trusted products.*

b) The remote IT product may not be evaluated, indicated in Figure 1.2 as 'untrusted IT product'; therefore its security policy is unknown. Exchanges of information in this situation are called ***transfers outside TSF control****, as there is no TSF (or its policy characteristics are unknown) on the remote IT product.* **(This would be an example of an internet-based civilian intelligence source (non-government organization-NGO) that needs to be accommodated in the overall security policy framework.)**

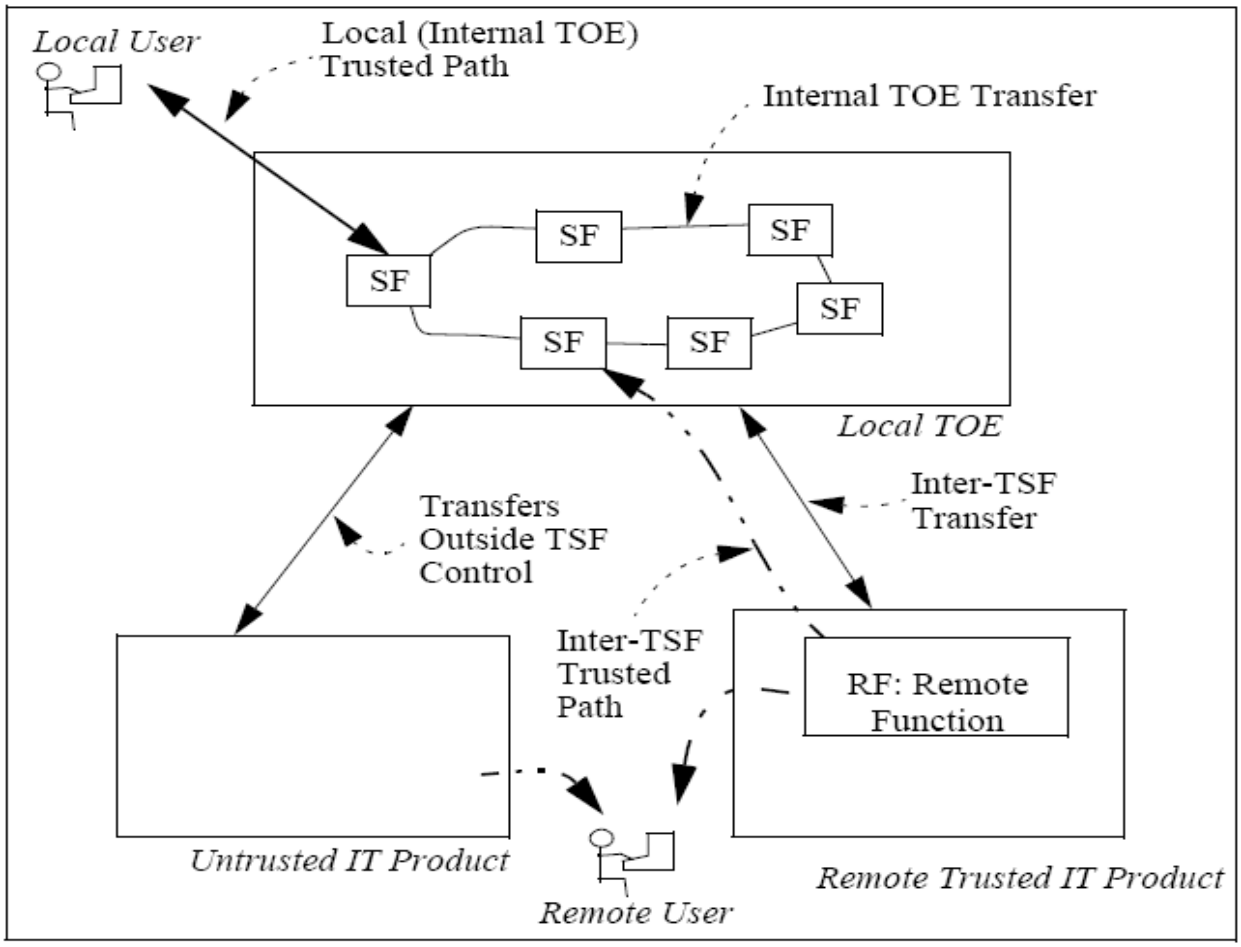

Figure 1.2 - Diagram of security functions in a distributed TOE

Conclusions & Suggested Direction

In conclusion, we would like to recommend the Tor technology as a means of creating the "Inter-TSF Transfer" channel (see Fig. 1.2) described in the previous section through the use of a secure, encrypted object-based framework for communications that satisfy the Common Criteria. As mentioned, separation of the multiple Data Planes & Control Planes is critical to support the Common Criteria recommendations and the object-based framework provides the necessary security boundaries within the "Inter-TSF Transfer" channel. The NuParadigm secure object framework provides security, system continuity, and reliability in a unique way: The framework routes objects through a "Secure Edge Process (Gateway)" rather than routing messages through traditional transport channels. Object state data is maintained within the service object itself instead of as system overhead associated with processing the messages related to a service. Possible benefits to the Warfighter include:

- Reliability – achieved through context specific object message constructs. Just as the DOD promotes "defense-in-depth" for network security, it is equally important to promote "reliability-in-depth" by adding peer-to-peer "application layer" technology for reliable data transfer. Message objects can be tracked for confirmation of delivery at the application layer just as TCP/IP traffic is acknowledged and resent if necessary at the "transport layer".
- Security - validation, authentication, and authorization are directly managed within the object
- Object-based monitoring and auditing – object activity is directly captured within the object as it goes through the service cycle for audit and reporting purposes. In other words, an encryption boundary is created within the object to provide secure auditing and satisfy the CC requirement for pseudonymity.
- Resiliency - Object routing also increases attack prevention capability since all objects are easily validated or rejected within the secure object framework.

Summary

As mentioned, the style of warfare has changed to support sudden regional conflicts and ad hoc humanitarian missions for disaster relief (e.g., Hurricane Katrina), so the style of Command & Control (C2) has also changed to incorporate civilian intelligence sources (non-government organizations-NGOs) and embrace government authorities. It is difficult to predict in advance what sources of intelligence will be needed on future missions, and if one is communicating with

"small civilian cells"; the Internet might be the only available channel. However, the need still exists to protect the sources & methods employed for intelligence gathering from disclosure. Likewise the deployment of military resources, such as naval vessels, needs to be protected even if serving civilian aid. Hopefully, the concept presented in this paper for a "Hidden Communications Web Service" and its benefits for C2 & Warfighters might generate interest and additional discussion.

In addition, the rapid growth of electronic commerce in the civilian domain is increasing the demand for trusted sources of financial messaging in terms of security, reliability and privacy. Since these market trends show no signs of slowing, it is safe to assume that the need for trustworthy and reliable sources with private access to distributed commercial data will also become more and more critical over time.

REFERENCES:

Atkinson, S. R. & Moffat, J. (2005) - The Agile Organization: From Informal Networks to Complex Effects and Agility.
Publisher: DoD Command and Control Research Program, Washington, D.C.

Common Criteria Security Evaluation Part 2: Security functional requirements
Version 2.1 CCIMB-99-032
Publisher: NSA, August 1999 Annotated with interpretations as of 2003-12-31

Dingledine, R., Mathewson, N., and Syverson, P. (2004). Tor: The Second-Generation Onion Router. Paul Syverson - Naval Research Lab syverson@itd.nrl.navy.mil
Publisher: Naval Research Laboratory

H. Haury (2005) - Resolving the Problem of Aligning Communities of Interest, Data Format Differences, Orthogonal Sensor Views, Intermittency, and Security – DoD Homeland Security Command and Control Advanced Concept Technology Demonstration.
Whitepaper presented by J. A. Sturm at 10th CCRTS in June, 2005.
Publisher: NuParadigm Government Systems, St. Louis, MO

Moffat, J. (2003) – Complexity Theory and Network Centric Warfare
Publisher: DoD Command and Control Research Program, Washington, D.C.

O'Morain, Titov, V., and Verbugen, W. Onion Routing for Anonymous Communications.
http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group10/index.html

Sturm, J. A. (2007) - An Architecture and Model For Multi-Level Secure Chat Services.
Presented at the IEEE Sarnoff Symposium, May 2007 at Princeton University

Sturm, J. A. (2007) - Integrating Military and Civilian C2
Presented at the 12th CCRTS in June, 2007.
Publisher: NuParadigm Government Systems, St. Louis, MO