Reprint of Article

“Cyber Threat Model for Tactical Radio Networks”

By

Michael T. Kurdziel PhD

Originally Presented at the
SPIE 9103, Wireless Sensing, Localization, and Processing IX Conference
May 21, 2014
Baltimore, Maryland

Harris Corporation, RF Communications Div.
Core Networking and Cyber Security
1680 University Ave
Rochester, NY 14610

Cyber Threat Model for Tactical Radio Networks

Michael T. Kurdziel
Harris Corporation, RF Communications Division
1680 University Avenue Rochester, New York 14610

ABSTRACT

The shift to a full information-centric paradigm in the battlefield has allowed ConOps to be developed that are only possible using modern network communications systems. Securing these Tactical Networks without impacting their capabilities has been a challenge. Tactical networks with fixed infrastructure have similar vulnerabilities to their commercial counterparts (although they need to be secure against adversaries with greater capabilities, resources and motivation). However, networks with mobile infrastructure components and Mobile Ad hoc Networks (MANets) have additional unique vulnerabilities that must be considered. It is useful to examine Tactical Network based ConOps and use them to construct a threat model and baseline cyber security requirements for Tactical Networks with fixed infrastructure, mobile infrastructure and/or ad hoc modes of operation. This paper will present an introduction to threat model assessment. A definition and detailed discussion of a Tactical Network threat model is also presented. Finally, the model is used to derive baseline requirements that can be used to design or evaluate a cyber security solution that can be scaled and adapted to the needs of specific deployments.

Keywords: Cyber-security, Tactical Networks, Threat Modeling, Threat Profile, STRIDE, DREAD, Microsoft Security Development Lifecycle (SDL)

1. INTRODUCTION

Modern tactical communications networks offer unprecedented communications and data access capabilities. With these capabilities come new cyber security challenges. A major distinction between the threat profile for a Military Tactical Network and the civilian equivalent is the adversary [5]. A military adversary is presumed to be a National Intelligence Agency with **w**orld-class skills, resources and the motivation to compromise Government and Military targets. Another important distinction is the value of the Government/Military information being protected precludes a classic cost trade-off from being applied.

Starting in 2004, Microsoft began formalizing the threat modeling process for code development with the Microsoft SDL. See [9] for detailed discussion. Elements of SDL are useful when analyzing a military communications system. This paper will introduce a threat modeling process that allows threats to be identified and then mitigated at a system and at a configuration item level [1] [8]. The result is a set of cyber security requirements that can be tailored to different types of Tactical Networks. It is important for developers and suppliers to understand these requirements so that appropriate solutions can be implemented.

The paper is introduced in Section 1. Section 2 provides a brief overview of the concept of threat modeling. This is followed in Section 3 by discussion on the specifics of a Tactical Network Threat Model. The paper is concluded in Section 4. A list of references is provided in the final section.

2. THREAT MODELING OVERVIEW

2.1 Types of Threat Models

A threat model can be attacker, architecture or asset focused [11]. An attacker focused threat model uses a characterization of potential adversaries to identify target areas and therefore vulnerabilities and subsequent potential attack modes. Key to this type of threat model is an assessment of an adversary's capabilities, resources and motivation that can be applied to exploit a given vulnerability. This assessment will drive the identification of which system vulnerabilities are considered to be real threats. It will also drive the prioritization of the final threat list and will be a primary factor in the development or procurement of appropriate mitigation solutions. It also enables classic cost trade-off studies to be performed. As an example, threats with attacks that require greater computing power to execute than is accessible by the adversary can be deemed as not worth mitigating. In other words the dollar cost of the solution, the impact to user accessibility or impact to platform performance is considered to be too high given the relatively low probability of an exploit. This model might be used to analyze consumer entertainment or communication devices where low cost, features, quality, etc. are important factors to the user, but security is assumed. This type of threat analysis is also appropriate for systems where, by some measure, the impact of a breach is not significant to the user.

An architecture focused threat model examines the components of a system to identify vulnerabilities and potential attacks on those components. The analysis begins with a hierarchical decomposition of the system into security relevant components. This can be a hardware, software or functional decomposition depending on characteristics of the system under analysis. The objective is to be able to group component vulnerabilities into classes with common mitigation methods. Once vulnerabilities are identified and categorized, the sequence of events that would be required to exploit a given vulnerability is examined. This is called penetration analysis. A common tool for performing penetration analysis is threat or attack tree construction. The results of this analysis are used to determine which vulnerabilities present the highest threat and allow the threats to be prioritized. Mitigation method deployment can then be planned appropriately. This approach is used in the Microsoft SDL threat modeling process. Processes based on this model type tend to require the most effort. However since modeling is not constrained to existing attacks, adversary behavior can be anticipated and a true defensive response is possible.

Asset focused threat modeling examines threats to specific assets or trusted resources. It seeks to increase system security and mitigate threats through the implementation of targeted protection mechanisms. This type of process is often used along with a system wide analysis to identify protection mechanisms for high priority targets. For example, sensitive data that is transmitted wirelessly will be directly accessible by the adversary and is at risk of being manipulated or intercepted. Integrity verification and source authentication may be applied to the data stream to defend against spoofing attacks. Encryption mechanisms may also be applied to provide data confidentiality. This type of modeling approach is also used to determine the scale of the protection mechanisms that will be required. An assessment of the adversary's motivation is made and used to estimate the value of a compromise to them. The assumption is that an adversary will not spend more to execute an attack than they will gain if a breach is achieved. The protection mechanism is then scaled to force the attack cost above this threshold.

2.2 Military Threat Modeling

Threat modeling of Military Tactical Networks has additional challenges. The adversary has advanced skills, resources and aggressive objectives. In addition, the adversary is "in-theater" and has full access to the wireless channel. Future threats, Denial of Service attacks, restoration of system services, etc, must all be considered. Therefore, a defensive strategy is necessary using a tailored process that incorporates elements from each type of threat model.

2.3 Methodology

This section will provide an overview of the threat modeling methodology. The process is adapted to the unique challenges of analyzing a military communication system operating on a battlefield. Refer to Figure 1 for the process flow described in the following sub-sections.

Characterize System from a Security Point of View

The process begins with a characterization of the system from a security point of view. The system assets should be clearly identified. Simply stated, the system assets are anything of value to the adversary and authorized users. The purpose of system security is to protect these assets. Next an architecture overview is created. This can be a simple system diagram with supporting text on the system's purpose, primary use cases, operating environment, intended users, etc. Lastly, a system decomposition is performed. This can consist of block diagrams and/or text descriptions. The decomposition should be hierarchical. First, segment the system into security relevant subsystems and continuing down to the component or configuration item level. Infrastructure, entry points, data flows, etc. should be indicated and discussed. The system characterization should be sufficiently detailed to allow development of the system threat profile.

Characterize System from a Security POV→

Develop Threat Profile →

- *Identify/Characterize Adversary*
- *Identify Target or Objective*
- *Identify Vulnerabilities*

Form Prioritized List of Threats/Mitigations →

- *Enumerate the threats*
- *Prioritize the threats*
- *Enumerate potential threat mitigations*

Close High Priority Threats →

- *Design/Procure Threat Mitigation Features*
- *Implement Threat Mitigation Features*
- *Test Threat Mitigation Features*

Revise periodically

Figure 1. Tactical Network Threat Model Process Flow

Develop Threat Profile

The Threat Profile will begin with an examination and characterization of the adversary. This should include estimates on level of expertise, financial resources, system and data access, computing resources, etc. Specific, accurate and verifiable data on the adversary is often difficult to obtain and conservative assumptions will need to be made. This is especially true for a government or military adversary where this data will be controlled as classified information.

Next, the adversary's objectives and motivation are examined. Knowledge of the adversary's ultimate goals and the value of achieving these goals will provide an indication of the types of attacks that can be expected. If there is a monetary value to achieving the objective, then attacks which have a lower cost will be emphasized. Likewise, any time value of achieving the objective will also indicate types of attacks that will need to be mitigated. For example, information such as military strike orders will only have value to the adversary if a compromise can be achieved before the strike occurs. In these cases, attacks which require more than a few hours to execute will not be employed. The adversary's goal may not be to acquire information at all. It may be to disrupt communications or to reduce the user's capability in some other way. These types of attacks are referred to as "Denial of Service (DOS)" attacks. Strong counter measures are often required to mitigate DOS attacks. These counter measures can be costly to implement and manage and must be considered carefully.

Lastly, the system itself needs to be examined to identify potential vulnerabilities. An adversary will perform the same analysis and then focus attacks on the least protected components of the system. This step in the process begins with a decomposition of the system down to the component level. Then the "STRIDE per Element" modeling tool is applied to each component. Refer to figure 2. The objective of STRIDE is to examine each component's potential vulnerability to six key attack categories. These are Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The tool then models the security of the entire system in the context of Concept of Operation (ConOps) scenarios, use cases, various service roles, data flows through the network and the system components, external dependencies, etc. As vulnerabilities are identified, appropriate countermeasures can be implemented.

	Threat	Definition	Property	Standard Counter-Measures
S	Spoofing Identity	Adversary imitates an authorized user to achieve some unintended objective	Authentication	• IPSec/HAIPE • Digital signatures • Message authentication codes • Hashes
T	Tampering with Data	Adversary manipulates data to achieve some unintended objective	Integrity	• Encryption • Access Control Lists • Digital signatures • Message Authentication Codes
R	Repudiation	Users dispute transactions to achieve some unintended objective	Non-repudiation	• Strong Authentication • Secure logging and auditing
I	Information Disclosure	Adversary achieves unauthorized access to information	Confidentiality	• Encryption • Access Control Lists
D	Denial of Service	Adversary seeks to disrupt operation of the system to authorized users	Availability	• Access Control Lists • Quotas • High availability designs
E	Elevation of Privilege	Adversary attempts to elevate their privileges to a higher role in the system (ex. Administrative)	Authorization	• Group or role membership • Input validation • Least Privilege Access • Intrusion prevention and detection (IPS/IDS)

Figure 2. “STRIDE per Element” Summary

Form Prioritized List of Threats

Closing all vulnerabilities is not possible from a technology, cost or practical point of view. The list of known vulnerabilities also continues to expand. For example, the internet has over 40,000 known vulnerabilities [10]. Many of these are not exploitable by any adversary and therefore pose no real threat. Vulnerabilities with corresponding attacks that exist with a high probability are considered high priority threats. These need to be closed first. The list of vulnerabilities identified in the previous step must, therefore, be prioritized. This is essentially a risk ranking of the vulnerabilities.

Risk analysis/ranking is modeled using the “DREAD” tool [9]. Each of the previously identified vulnerabilities is rated against the DREAD criteria:

- **D**amage - How much damage would an attack cause?
- **R**eproducibility - Is the attack repeatable?
- **E**xploitability - What resources are required to launch the attack?
- **A**ffected users - How broad is the user impact?
- **D**iscoverability - Is the threat known or can it be easily discovered?

A simple spread sheet is used. Refer to Figure 3. A four point rating system is applied where 1 corresponds to low, 2 to medium, 3 to high and 4 to critical. The rankings are totaled and the vulnerabilities are arranged in descending order. Expert understanding of the system is required to separate the list into 4 categories. The first category consists of vulnerabilities that represent an aggressive threat and must be mitigated immediately. The second category consists of threats that need to be mitigated but with less urgency. The third category consists of vulnerabilities that should be monitored with mitigation applied if advancement to a higher threat category is detected. The fourth category consists of vulnerabilities that do not pose a threat and do not need to be mitigated.

Vulnerability	D Damage	R Reproducibility	E Exploitability	A Affected users	D Discoverability	Total
V_1						
V_2						
V_3						
…						
V_n						

Figure 3. “DREAD” Ranking

Close/Mitigate the Threats

Finally, the critical and high threats are enumerated and mitigation is planned. To mitigate the threats, appropriate countermeasures must be identified. The results of the threat analysis can be used to define requirements. These requirements are used to procure or develop appropriate countermeasures. If a standard countermeasure that meets the corresponding requirement exists, then it can be procured. However, if an appropriate countermeasure does not exist, it must be developed.

Once the countermeasures are acquired, they need to be integrated into the system and tested. Once the countermeasure operation is verified, the system can be deployed. Note that the system’s operating environment is dynamic. Therefore, the threat profile needs to be revised periodically. Any changes to the requirements may require re-verification of existing countermeasures or implementation of new ones.

3. TACTICAL NETWORK THREAT MODEL

3.1 Characterize System from a Security Point of View

This section will present a characterization or overview of the system including a description of the system assets, an architecture overview and a high-level system decomposition.

System Assets

The primary system asset is the information carried by the network. Traffic consists of field intelligence, surveillance and reconnaissance information, Situational Awareness (SA) data, operations data, mission orders, etc. This information can be in the form of voice, data, and real time video. Compromise of this asset would be of significant value to the adversary and will be a high priority target.

Another system asset is the network functionality itself. Administrators and users will depend on the system to be fully available at all times to support peer to peer battlefield communications, access network assets, access higher echelon command systems, etc. As a first priority, the adversary will target system information, but a tactical advantage can also be gained by the adversary through disruption of the communications system. In addition to protection of information assets, security against DOS attacks is required.

Architecture Overview

The Tactical Network system architecture can be considered a heterogeneous Wide Area Network (WAN) with wired Local Area Network (LAN), Mobile Network and Ad hoc Network subsystems. Partitioning and scaling between the subsystems depends on the deployment requirements. For example, see Figure 7. The system operates in a battlefield environment where security ranges from challenging to hostile. The component equipment is ruggedized for the tactical environment and is designed to be fail-safe and tamper proof. The system administrators are thoroughly trained on the operation of the equipment and unlikely to introduce errors or cause unintentional damage. The users are trained on the operation of the equipment and only given Least Privilege Access. As military personnel, the administrators and users are subject to extensive background investigations and are bound by military law where consequences for malicious behavior are severe. Therefore, administrators and users are not likely to cause intentional damage.

System Decomposition

Tactical Networks are composed of three types of subsystems; LANs, Mobile Networks and Wireless Ad hoc Networks. Standard LANs (Figure 4) are used in semi-permanent installations such as those in Brigade/Battalion Headquarters and Tactical Operations Centers (TOCs). For these subsystems, servers, routers, switches and terminal devices are deployed in fixed installations with wired or wireless interconnects. Broadband wireless links and satellite transceivers are often included to provide connectivity with upper echelon networks. Peer to peer and lower echelon connectivity is usually provided via high capacity data radios.

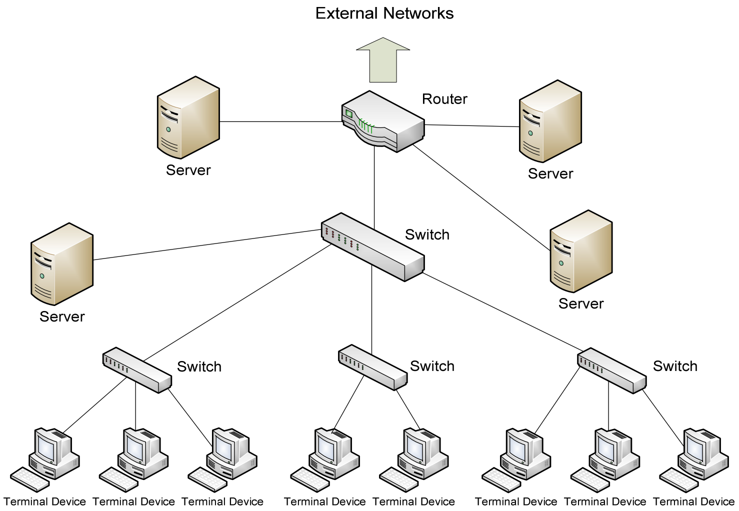

Figure 4. Local Area Network Subsystem

Mobile Networks such as the “Warfighter Information Network – Tactical” (WIN-T), shown in Figure 5, deploy network infrastructure (servers, routers, switches) on vehicular platforms. The WIN-T Increment 2 vehicles include high capacity data radios for peer to peer (TOCs and other vehicles) and lower echelon connectivity. Satellite transceivers are also included for redundant connectivity to upper echelon networks. Mobile Networks allow infrastructure to be quickly redeployed and allow network connectivity to be extended to the front lines of the battlefield. Multiple vehicular platforms are often deployed to provide redundancy and enhance the availability of network service in a hostile environment. Terminal equipment includes military handheld radios, manpack radios, ruggedized computers and video terminals. This equipment is designed to be fail-safe and tamper proof.

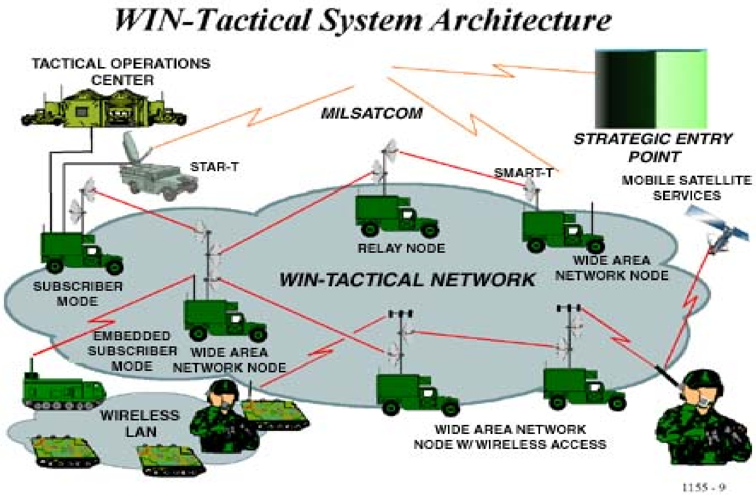

Figure 5. Mobile Network Example WIN-T Increment 2

The “Wireless Ad hoc Network” type (Figure 6) requires no infrastructure to establish connectivity. Each node in the network not only includes a wireless transceiver, but also message routing functionality. Each node establishes peer to peer connectivity until a connected “mesh” structure is established. One or more nodes may also have the ability to communicate with upper echelon networks. Network connectivity is self-configuring and self-healing if nodes are lost or repositioned. Messages can be routed through the network from source nodes to destination nodes through intermediate nodes. Direct connections between the source and destination are not required. In addition, multiple routes between source and destination nodes are possible. This provides redundant connectivity and enhances the reliability and availability of the network. Other advantages include lower power operation and lower detectability. Ad hoc Networks can be challenging to secure. Network services and protection mechanisms are distributed and strong authentication mechanisms are required.

There are two main types of Wireless Ad hoc Networks; these are MANets and Fixed Location Ad hoc Networks. With a MANet, member nodes are on the move. Network membership and connectivity requirements are dynamic. For example, Platoon level soldier to soldier communications could be facilitated using a MANet. For Fixed Location Ad hoc Networks, once the nodes are deployed, they establish mesh connectivity and do not change their positions from that point on. Sensor webs use this network structure to enable fast and easy deployment. Component nodes in military Ad hoc Networks consist of network enabled tactical radios with integrated router capability. They are designed to be fail-safe and tamper proof.

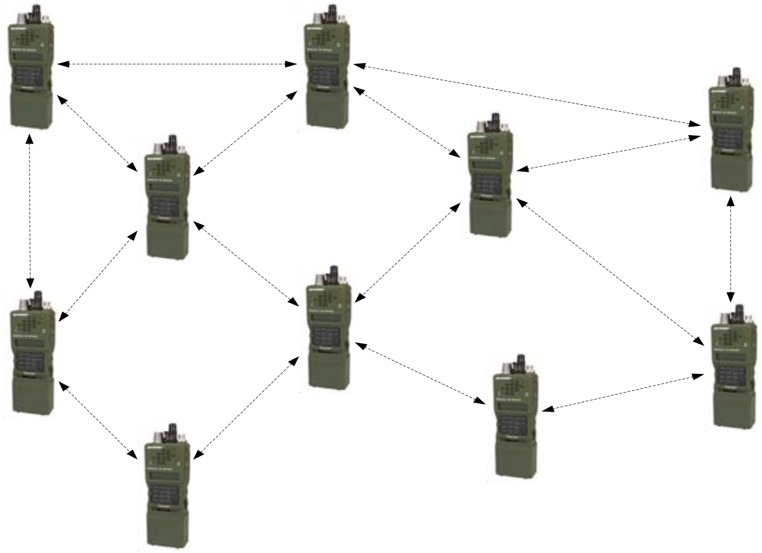

Figure 6. Example Ad hoc Network

3.2 Threat Profile

Characterization of the Adversary

The threat modeling process was applied to a WAN consisting of the LAN, Mobile Network and Ad hoc Network subsystems described in the previous sections. The threat profile is described in this section. A military threat profile addresses a very sophisticated adversary, that is, a national intelligence agency. These agencies employ world-class expertise on information assurance and cyber security. Of course, specific data is not available on any of these agency’s capabilities, but it can be assumed that they exceed anything available in the public sector. Tactical Network threats and attacks may even be discovered by these agencies before they are available in the public sector. Further, national intelligence agency cyber security professionals are funded by the resources of a government and often beyond the level of their public sector equivalent. The value to the adversary of compromising their opponents’ communications network is high and would offer a significant strategic advantage on the battlefield.

It is assumed that the intelligence agencies of world powers possess leading edge technology. They could even possess computing resources that are not yet available in the public sector. In the absence of verifiable information, it must be assumed that the adversary has access to powerful computing technology and has the resources to construct custom hardware if required.

Target and Objectives

The adversary will pursue anything that provides an advantage on the battlefield. To that end, all of the system assets described in section 3.1 will be targeted. The information carried by the network will be the primary target. Most information on the wireless channels will be protected by a high quality encryption mechanism. The adversary will not be able to determine the value of this information until it is compromised. Therefore, all information and any equipment that processes it will be targeted.

As stated in section 3.1, another system asset is the network functionality itself. Reliable and secure communications is more important to mission success than offensive capability. Disruption of the system will provide a significant advantage to the adversary on the battlefield and will certainly be a primary objective. Protection against DOS attacks is required at all cost.

Potentially Vulnerable System Components

The "STRIDE by Element" process was used to identify vulnerabilities in each of the Tactical Network subsystem types described in the previous sections. Table 1 shows the results of this analysis. Column 3 represents the LAN vulnerabilities, column 4 represents the Mobile Network vulnerabilities and column 5 represents the Ad hoc Network vulnerabilities. Even though each subsystem may have identical vulnerabilities, potential countermeasures are often distinct between subsystems. Therefore, vulnerabilities are shown separately. In the next section, these vulnerabilities will be enumerated and ranked.

Table 1. Tactical Network Vulnerabilities by Subsystem

	Threat Category	**Vulnerability**		
		Local Area Network (LAN)	**Mobile Network**	**Wireless Ad hoc Network**
S	Spoofing Identity	• Unauthorized access	• Unauthorized access • Compromised nodes	• Unauthorized access • Compromised nodes • No physical security boundary
T	Tampering with Data	• Channel access (headers and payloads)	• Channel access (headers and payloads)	• Channel access (headers and payloads)
R	Repudiation	• Network protocol vulnerabilities	• Network protocol vulnerabilities	• Network protocol vulnerabilities
I	Information Disclosure	• Channel access (headers and payloads)	• Channel access (headers and payloads) • Traffic flow analysis	• Channel access (headers and payloads) • Traffic flow analysis • No physical security boundary
D	Denial of Service	• Human error or malice • Malicious code (viruses, worms, etc) • Limited resources: Interfaces, memory, link bandwidth, computational bandwidth • Vulnerable centralized management • Catastrophic disruption	• Human error or malice • Malicious code (viruses, worms, etc) • Limited resources: Interfaces, memory, link bandwidth, computational bandwidth • Vulnerable centralized management • Compromised nodes • Network protocol vulnerabilities • Wireless signal detection/ disruption • Catastrophic disruption	• Human error or malice • Malicious code (viruses, worms, etc) • Limited resources: Interfaces, memory, link bandwidth, computational bandwidth • No centralized network management or security management • Compromised nodes • Network protocol vulnerabilities • No physical security boundary • Dynamic network position, topology and scale • Wireless signal detection/ disruption • Catastrophic disruption
E	Elevation of Privilege	• Human error or malice • Unauthorized access • Network protocol vulnerabilities	• Human error or malice • Unauthorized access • Compromised nodes • Network protocol vulnerabilities	• Human error or malice • Unauthorized access • Compromised nodes • Network protocol vulnerabilities

3.3 Form Prioritized List of Threats

Once the potential vulnerabilities have been identified, the next step is to enumerate and prioritize them. The highest priority vulnerabilities are considered to be threats. Each of the vulnerabilities identified in Table 1 were first listed sequentially in a spread sheet similar to the template shown in Figure 3. Ranking is performed according to the deployment shown in Figure 7. For this network deployment, Battalion Headquarters, Brigade Headquarters, Tactical Operation Centers and shipboard installations all use LAN subsystems. Mobile Network subsystems are distributed throughout the battlefield on vehicular platforms. MANets are restricted to the platoon level for soldier to soldier communications. As we will see this is partly due to the difficulty of securing MANets on the battlefield.

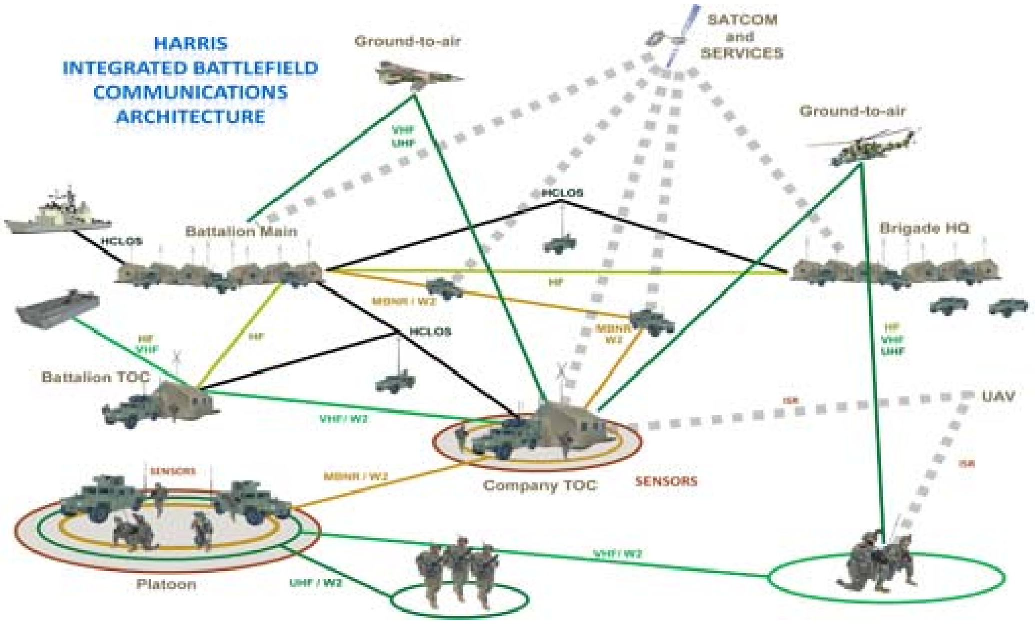

Figure 7. Harris Integrated Battlefield Communications Network Architecture

Vulnerabilities were ranked using the “DREAD” risk/ranking tool that was described in Section 2.6. Table 2 shows the results of this part of the process. Each vulnerability is listed in descending order of total DREAD score. The results are then colored coded according to the following categories:

- RED - Aggressive threats that must be mitigated with high priority
- YELLOW - Threats that need to be mitigated but with less urgency
- GREEN - Vulnerabilities to be monitored with mitigation applied if required
- BLUE - Vulnerabilities that pose no threat and do not need to be mitigated

Table 2. Prioritized Vulnerabilities by Subsystem

No.	Subsystem	Vulnerability	DREAD Total
1	Mobile Network	Vulnerable centralized management	18
2	Local Area Network (LAN)	Unauthorized access	15
3	Mobile Network	Unauthorized access	15
4	Wireless Ad hoc Network	Unauthorized access	15
5	Mobile Network	Traffic flow analysis	13
6	Mobile Network	Channel access (headers and payloads)	13
7	Mobile Network	Limited resources: Interfaces, memory, link bandwidth, computational bandwidth	12
8	Mobile Network	Wireless signal detection/disruption	12
9	Local Area Network (LAN)	Catastrophic disruption	12
10	Mobile Network	Catastrophic disruption	12
11	Wireless Ad hoc Network	Catastrophic disruption	12
12	Local Area Network (LAN)	Vulnerable centralized management	11
13	Wireless Ad hoc Network	Channel access (headers and payloads)	11
14	Wireless Ad hoc Network	Limited resources: Interfaces, memory, link bandwidth, computational bandwidth	11
15	Mobile Network	Network protocol vulnerabilities	11
16	Wireless Ad hoc Network	Network protocol vulnerabilities	11
17	Wireless Ad hoc Network	No centralized network management or security management	10
18	Wireless Ad hoc Network	Dynamic network positioning, topology and scale	10
19	Wireless Ad hoc Network	Wireless signal detection/disruption	10
20	Local Area Network (LAN)	Malicious code (viruses, worms, etc)	9
21	Mobile Network	Malicious code (viruses, worms, etc)	9
22	Wireless Ad hoc Network	Compromised nodes	9
23	Wireless Ad hoc Network	No physical security boundary	9
24	Wireless Ad hoc Network	Traffic flow analysis	9
25	Wireless Ad hoc Network	Malicious code (viruses, worms, etc)	9
26	Mobile Network	Compromised nodes	7
27	Local Area Network (LAN)	Human error or malice	6
28	Mobile Network	Human error or malice	6
29	Wireless Ad hoc Network	Human error or malice	6
30	Local Area Network (LAN)	Channel access (headers and payloads)	5
31	Local Area Network (LAN)	Network protocol vulnerabilities	5
32	Local Area Network (LAN)	Limited resources: Interfaces, memory, link bandwidth, computational bandwidth	5

Enumerate Potential Threat Mitigations

In this section, potential methods are identified to mitigate the threats and vulnerabilities considered in the previous sections. Table 3 provides a summary of controls, countermeasures, policies and processes that can be considered to secure Tactical Networks.

Table 3. Summary of Potential Threat Mitigations

No.	Subsystem	Vulnerability	Mitigation
1	Mobile Network	Vulnerable centralized management	Some physical security, Access control system, Functional redundancy in case of a compromise
2	Local Area Network (LAN)	Unauthorized access	Access control system, Intrusion Prevention/Detection (IPS/IDS), Audit logs, Secure terminals, Least privilege access, Defense in Depth, etc.
3	Mobile Network	Unauthorized access	Access control system; Intrusion Prevention/Detection (IPS/IDS), Audit logs, Secure terminals, Least privilege access, Defense in Depth, etc.
4	Wireless Ad hoc Network	Unauthorized access	Secure terminals, Least privilege access, Distributed ACS and Distributed IPS/IDS (active research area), Defense in Depth
5	Mobile Network	Traffic flow analysis	Channel encryption (header and payload), Secure enclaves, Closed network
6	Mobile Network	Channel access (headers and payloads)	Channel encryption (header and payload), Secure enclaves, Closed network
7	Mobile Network	Limited resources: Interfaces, memory, link bandwidth, computational bandwidth	Authenticated control/configuration commands, Restricted addresses, Active security management and monitoring, IPS/IDS, etc.
8	Mobile Network	Wireless signal detection/disruption	Anti-jam, LPI/LPD waveforms
9	Local Area Network (LAN)	Catastrophic disruption	Mission Continuity and Disaster Recovery (BC&DR) capability
10	Mobile Network	Catastrophic disruption	Mission Continuity and Disaster Recovery (BC&DR) capability
11	Wireless Ad hoc Network	Catastrophic disruption	Mission Continuity and Disaster Recovery (BC&DR) capability
12	Local Area Network (LAN)	Vulnerable centralized management	Physical security boundaries, Functional redundancy in case of a compromise
13	Wireless Ad hoc Network	Channel access (headers and payloads)	Channel encryption (header and payload), Low power, reduced range signaling, LPI/LPD waveforms, Closed network, Active research area
14	Wireless Ad hoc Network	Limited resources: Interfaces, memory, link bandwidth, computational bandwidth	Authenticated control/configuration commands, Restricted addresses, Remote security management and monitoring, Distributed IPS/IDS, Active research area
15	Mobile Network	Network protocol vulnerabilities	Channel encryption (header and payload), Authenticated control/configuration commands, Firewalls, Defense in Depth
16	Wireless Ad hoc Network	Network protocol vulnerabilities	Channel encryption (header and payload0, Authenticated control/configuration commands, Closed network, MANet tailored signaling, Defense in Depth, Active research area
17	Wireless Ad hoc Network	No centralized network management or security management	Channel encryption (header and payload), Authenticated control/configuration commands, Closed network, Distributed IPS/IDS, Remote security management and monitoring, Active research area
18	Wireless Ad hoc Network	Dynamic network positioning, topology and scale	Channel encryption (header and payload), Authenticated control/configuration commands, Closed network, MANet

			tailored signaling, Active research area
19	Wireless Ad hoc Network	Wireless signal detection/disruption	Low power, reduced range signaling, Anti-jam, LPI/LPD waveforms, Active research area, etc.
20	Local Area Network (LAN)	Malicious code (viruses, worms, etc)	Malware protection software, White listing, Defense in Depth
21	Mobile Network	Malicious code (viruses, worms, etc)	Malware protection software, White listing, Defense in Depth
22	Wireless Ad hoc Network	Compromised nodes	Access control system; Intrusion Prevention/Detection (IPS/IDS), Audit logs, Secure terminals; Least privilege access, Defense in Depth, Active research area, etc.
23	Wireless Ad hoc Network	No physical security boundary	Secure terminals, MANet protocols, Active research area, etc
24	Wireless Ad hoc Network	Traffic flow analysis	Channel encryption (header and payload), Secure enclaves, Closed network, Active research area, etc.
25	Wireless Ad hoc Network	Malicious code (viruses, worms, etc)	Malware protection software, White listing, Defense in Depth, Closed network, Active research area, etc.
26	Mobile Network	Compromised nodes	Access control system; Intrusion Prevention/Detection (IPS/IDS), Audit logs, Secure terminals; Least privilege access, Defense in Depth, etc.
27	Local Area Network (LAN)	Human error or malice	Training, Background investigations, Dependence on mission success, Least privilege access
28	Mobile Network	Human error or malice	Training, Background investigations, Dependence on mission success, Least privilege access
29	Wireless Ad hoc Network	Human error or malice	Training, Background investigations, Dependence on mission success, Least privilege access
30	Local Area Network (LAN)	Channel access (headers and payloads)	Physical security boundary, Channel encryption (header and payload)
31	Local Area Network (LAN)	Network protocol vulnerabilities	Physical security boundary, Access Control, Authenticated commands, Firewalls
32	Local Area Network (LAN)	Limited resources: Interfaces, memory, link bandwidth, computational bandwidth	Physical security boundary, Restricted addresses, Active security management and monitoring, IPS/IDS, etc.

3.4 Close/Mitigate High Priority Threats

Table 3 presents a summary of controls, countermeasures, policies and processes that form the basis of a sound Tactical Network security strategy. When considering the security of Tactical Networks, the following essential requirements must be addressed [2].

- Counter-measures - Technology solutions deployed to mitigate threats
- A Layered Defense - Not depending on a single technology or method to provide security
- Defense in Depth - Security is addressed with personnel, operations, and technology
- Best Practices - For example, mission plans and policies
- Future Capability - Anticipation of new attacks including vulnerability management and tracking

Once a strategy is developed, threat mitigation features, controls, processes and policies must be designed or procured. Next, Network and Computer Security elements are implemented, tested and deployed. Operational Security is then employed to maintain the security effectiveness of the deployed system. Detailed discussion follows.

Network Security

The core of any information system is the network that permits the sharing of information between systems. Multiple network security capabilities should be included to address risks. These include access control lists on routers, firewalls, network intrusion detection, and channel encryption. The following sections list the requirements for each one of these required technologies.

Access Control System

Access must be restricted to those who are authorized and have a need to know. Access control ensures that the system maintains confidentiality and integrity of information through role-based access control. Access control systems implement least privilege access, authentication, authorization, and accountability. Requirements include:

- Centralized authentication, authorization, and accountability of administrators and users
- Role-based management of administrators, users and machines
- Tracking of audit trails to enforce policies and regulations and to provide accountability for the actions of the system's administrators and users

Firewalls

Firewall protection is one element in an overall cyber security "Defense-in-Depth" strategy. Firewalls are enclave boundary protection devices located between wireless communications systems and other upper and lower echelon networks. Their primary purpose is to control access to communications systems, enforce policies (Restricted addresses, white listing, etc.) and prevent abnormal network behavior. Firewalls provide filtering of incoming or outgoing information. They must be uniquely configured to ensure that the correct information is allowed to proceed without negatively impacting system performance.

Intrusion Prevention System/Intrusion Detection System (IPS/IDS)

IPS/IDS allows a combination of vulnerability and anomaly-based inspection methods to analyze network traffic and prevent threats from damaging the network by alerting system administrators of suspicious network behavior. These systems compliment or are part of a larger security system that also contains firewalls, anti-virus software, etc.

Channel Encryption

Channel encryption allows information traversing the network to be enciphered and most importantly protects the integrity and confidentiality of the data. This protects information being sampled over the air, from revealing any information including IP headers, which can be used to learn about the network infrastructure. For wireless communications systems, encryption levels vary by application and subsystem. Note also that channels are also protected using specialized waveforms that reduce signal detectability and increase resistance to disruption. These are discussed in the "Specialized Waveforms" section.

Functional Redundancy

Where possibly, key network operations should be redundant. TOCs should be able to assume the responsibilities of any of their peer TOCs. Upper echelon headquarters should also be able to assume the functions of lower echelon command centers if required. Mobile platforms should provide spare capacity so that network traffic can be maintained at acceptable data rates if the operation of any single platform is disrupted. Finally, Ad hoc networks used by individual soldiers should be able to reform with the addition or loss of a node.

Physical Security Boundaries

Physical security boundaries are key to any security plan. The system should be capable of maintaining the integrity of these boundaries. Components in a Tactical Network are designed to be tamper evident and tamper proof. If the equipment enclosures are breached, the equipment will automatically delete all sensitive information such as plaintext or encryption keys. On the battlefield, command posts (TOCs, headquarters, shipboard CPs, etc), mobile platforms and even fielded terminals have aggressively monitored and maintained security boundaries. Armed warfighters protect these systems to ensure mission success and to protect their very lives.

Computer Security

Tactical Networks are composed of computer systems. These systems are a primary objective for the adversary for either data gathering or destruction. Computer systems are the security end point and require protection mechanisms to minimize the risk associated with the information they contain and the trusted capability they provide.

Security Policies

Wireless communications systems should include configuration and periodic updates of security policies for the operating systems to ensure reliable operation, maintenance and administration.

Host-based Security

Host platforms provide role-based administration of centralized servers that operate authentication and authorization subsystems and are responsible for management, updating, and monitoring of the Tactical Networks directly and remotely. Host-based security provides a suite of software that protects network platforms from malicious behavior. Malware detection and antivirus software are required to protect subsystems, workstations and servers from malicious code. Comprehensive, host-based security provides protection from intentional attacks through bugs, viruses, malware, or even accidental administrator or user actions. A host-based solution is necessary for ensuring proper protection from known attack vectors and unallowable behaviors.

Operational Security

A Layered Defense and Defense in Depth strategy requires that operational elements as well as technological elements be considered. This section will discuss the minimum operational security requirements [3].

Human Error or Malicious Behavior

Unlike their civilian counterparts the administrators and users of tactical networks have a low probability of disrupting network operation due to human error or malicious behavior. They hold security clearances and have been subject to in-depth background investigations. Training on the administration of the system is rigorous and users are granted Least Privilege Access only. They also depend on the system for mission success and even their very lives. Lastly, malicious behavior is considered treasonous, a crime with severe penalties.

Vulnerability Management and Tracking

Recall that vulnerabilities identified in the GREEN category in Tables 2 and 3 must be monitored with mitigation applied if required. This process is called Vulnerability Management and Tracking [7]. A vulnerability management program consists of four key elements:

- Countermeasures - Countermeasures are methods or controls for mitigating vulnerabilities that have become threats
- Metrics - Metrics allow the vulnerability domain to be monitored for emerging threats and that the implemented countermeasures are effective and reliable
- Intelligence - Intelligence is the collection and interpretation of metrics to allow appropriate responses to be implemented in real- time

Security Log Management

Security log management involves the collecting, monitoring, and analyzing of security-related data from computer logs. Log data includes security information generated from numerous sources, including antivirus software, intrusion-detection systems, file systems, firewalls, routers and switches, and servers.

Mission Continuity and Disaster Recovery (BC&DR)

MC&DR, sometimes referred to as backup and recovery, uses processes and technology to allow administrators and users to restore essential functions after system disruption or failure. Maintaining replacements for mission critical equipment or even redundant standby system components should be provided. Backups and snapshot images should also be maintained to restore system functions from as close to point of failure as possible.

Additional Security Considerations

Ad hoc Networking on the Battlefield

In Section 3.1, many of the advantages that Ad hoc Networks provide to communications on the battlefield were discussed. For example, these networks do not depend on potentially vulnerable centralized infrastructure, they require minimal configuration and they deploy quickly. Dynamic and adaptive routing protocols provide redundant connectivity which enhances the reliability of the network.

Ad hoc Networks are challenging to secure. Since there is no centralized infrastructure, there is also no centralized security management. Protection mechanisms need to be distributed and bandwidth is consumed keeping these mechanisms synchronized. Depending on the application, remote security management and monitoring is required which also consumes bandwidth. If not correctly implemented, Ad hoc Networks can serve as entry points for the adversary into the entire communication system. See [4] and [6] for additional detailed discussion.

The degree, to which a technology can be secured, drives the degree to which the technology can be used. Pure MANets currently have irresolvable security issues in the tactical environment. Until solutions are found to these issues, Ad hoc Networks will have a limited role on the battlefield. Today, they are used in closed networks secured by preplaced key material with predefined allowable membership. Defense in Depth strategies are also employed so that operational and personnel based security measures can assist.

Ad hoc Networks are generally restricted to platoon and company level peer to peer communications. Ad hoc modes in Mobile Networks with centralized management can also be used for peer to peer connectivity at higher echelons. The layered security mechanisms that are already in place provide security here.

Specialized Waveforms

Use of Low Probability of Intercept and Low Probability of Detect (LPI/LPD) and low power/short range waveforms enhance the security of the network by hiding the system's operation from the adversary. Anti-jam waveforms, such as those employing frequency hopping, make it more difficult for the adversary to disrupt communications even if the system's operation is detected.

Secure Network Components

The components of Tactical Networks (servers, routers, switches computers, radios, etc.) are ruggedized for the battlefield. Equipment is designed to operate under extreme physical and environmental conditions. Equipment enclosures are designed to be tamper evident or tamper proof. Tamper evidence mechanisms allow administrators or users to detect when security boundaries have been breached so that appropriate corrective action can be taken. Tamper proof enclosures allow the equipment itself to take action when its security boundary is breached. These actions could be as simple as erasing cryptographic keys and sensitive information to rendering the equipment nonoperational.

Limited System Resources

All system components have practical limitations to their features. There are only a limited amount of network assets such as interfaces, memory, link bandwidth, etc. A common DOS attack is for the adversary to take some action to consume these resources and reduce the effectiveness of the communication system. Targeted security mechanisms are therefore required to protect these resources against attack.

4. CONCLUSION

This paper presented a threat modeling process that is targeted to Tactical Networks. The process was applied to the "Harris Integrated Battlefield Communications Architecture". Threats were defined for this network. Mitigation methods were identified and described. The main goal of this paper is to demonstrate that information systems intended for operation in the tactical environment differ in significant areas from their civilian counterparts and that a civilian security strategy is not appropriate for these systems. Further, a security strategy designed for a Tactical Network not only guides the choice of risk mitigation methods, but also on the deployment of the technology itself.

Acknowledgement

The author wishes to acknowledge valuable feedback and discussions with many expert colleagues at Harris Corporation. Although this work cannot be a comprehensive treatment of the broad discipline of Tactical Network Cyber Security, their contributions have enabled this paper to be an excellent starting point for those interested in increasing their own expertise. Special gratitude is extended for the contributions of Gregory Harris, a good friend and colleague. Greg is an expert in Cyber Security of Land Mobile Radio Networks and is also a former U.S. Marine communications officer. His experience and expertise provided insights of immeasurable value to the objectives of this paper.

REFERENCES

[1] Burns, S., "Threat Modeling a Process to Ensure Application Security," GIAC Security Essentials Certification (GSEC) Practical Assignment, (2005). [Online] Available: <http://www.sans.org/reading room/whitepapers/securecode/threat-modeling-process-ensure-application-security 1646 (2006).

[2] Harris, G., “Cyber Security for Wireless Communications Systems,” Harris Corporation White Paper, (2013).

[3] IBM Global Technology Services, “IBM Security Services Cyber Security Intelligence Index,” (2013). [Online] Available: <http://www-935.ibm.com/services/us/en/security/infographic/cyber securityindex.html>.

[4] Kidston, D., Li, L., Tang, H., Mason, P., “Mitigating Security Threats in Tactical Networks,” IST Panel Symposium, Military Communication and Networks, Wroclaw, Poland , (2010).

[5] Kurdziel, M., Fitton, J., “Baseline Requirements for Government and Military Encryption Algorithms,” Proc. IEEE, Mil. Comm. Conf., Oct. (2002).

[6] Li, W., Joshi, A., “A Survey of Security Issues in Mobile Ad hoc Networks,” Dept. Computer Science Electrical Engineering, University of Maryland, (2008).

[7] Mateski, M., “Cyber Threat Metrics,” Sandia National Laboratories, (2012).

[8] Myagmar, S., “Threat Modeling as a Basis for Security Requirements,” Symposium on Requirements Engineering for Information Security (SREIS) in conjunction with 13th IEEE International Requirements Engineering Conference (RE), Paris, France, (2005).

[9] Swiderski, F., Snyder, W., [Threat Modeling], Microsoft Press, (2004).

[10] Symantec Corporation, “Internet Security Threat Report 2013,” 2012 Trends, Volume 18, April (2013).

[11] Wikipedia, “Threat Model,” 2 February (2014), <http://en.wikipedia.org/wiki/Threat_model>.