INSTITUTE FOR DEFENSE ANALYSES

Mobile Ad Hoc for Enterprise Level Security

William R. Simpson

Kevin E. Foltz

October 25, 2018

Approved for public release;
distribution is unlimited.

IDA Non-Standard
NS D-9113

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BC-5-2283, "Architecture, Design of Services for Air Force Wide Distributed Systems," for USAF HQ USAF SAF/CIO A6. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For more information:

William R. Simpson, Project Leader
rsimpson@ida.org, 703-845-6637

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Mobile Ad Hoc for Enterprise Level Security

William R Simpson and Kevin E. Foltz

***Abstract*—Threat intrusions to enterprise computing systems have led to a formulation of guarded enterprise systems. The approach was to put in place steel gates to prevent hostile entities from entering the enterprise domain. The current complexity level has made the fortress approach to security, which is implemented throughout the defense, banking, and other high-trust industries, unworkable. The alternative security approach, called Enterprise Level Security (ELS), is the result of a concentrated fourteen-year program of pilots and research. The primary identity credential for ELS is the Public Key Infrastructure (PKI) certificate, issued to the individual who is provided with a Personal Identity Verification (PIV) card with a hardware chip for storing the private key. All sessions are preceded by a PKI mutual authentication, and a Transport Layer Security (TLS) 1.2 communication pipeline is established. This process was deemed to provide a high enough identity assurance to proceed. However, mobile ad hoc networking allows entities to dynamically connect and reconfigure connections to make use of available networking resources in a changing environment. These networks range from tiny sensors setting up communications based on a random or unknown configuration to aircraft communicating with each other, the ground, and satellites. Scenarios have differing requirements in terms of setup, reconfiguration, power, speed, and range. This paper presents an adaptation of the ELS principles to the mobile ad hoc scenario.**

***Index Terms* — Enterprise Level Security, Mobile Ad hoc, Networking, Service Requirements**

I. INTRODUCTION

Mobile ad hoc networking includes a broad range of possible implementations. These implementations range from unstructured networks like MANETS [1], where there is no existing infrastructure and nodes must dynamically configure themselves into a functioning network, to situations in which a mobile node connects to existing infrastructure. This document focuses on situations in which fixed infrastructure exists and nodes come in and out of communication range and situations in which nodes dynamically connect and disconnect to each other and different networks. These situations allow many of the higher-layer functional and security protocols to function properly. The following sections describe different aspects of the networking infrastructure that together support the concept of ad hoc connections and mobility. Figure 1 illustrates those network types.

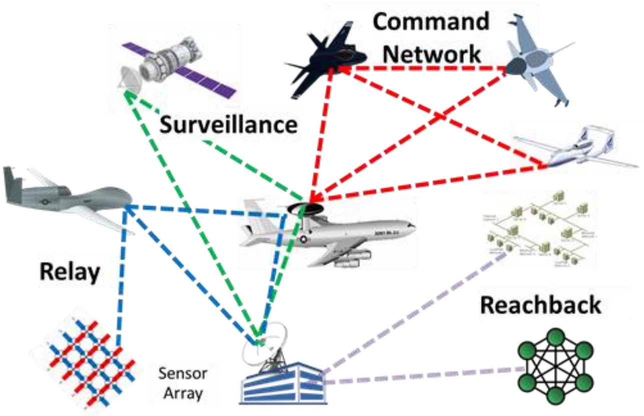

Figure 1 Ad Hoc Networking

Enterprise Level Security (ELS) is a capability designed to counter adversarial threats by protecting applications and data with a dynamic claims-based access control (CBAC) solution. ELS helps provide a high assurance environment in which information can be generated, exchanged, processed, and used. It is important to note that the ELS design is based on a set of high-level tenets that are the overarching guidance for every decision made, from protocol selection to product configuration and use [2].

II. NETWORK OVERVIEW

The network consists of many different technologies that are split into different layers. One conceptual model for this layering is the Open Systems Interconnect (OSI) [3] seven-layer model, as shown in Figure 2. The network layer is the highest layer considered in this document. This layer provides addresses that are unique within a network, allowing communication through IP routers to any other node that is connected to the same network. The use of bridges and network address translation (NAT) allows different networks with overlapping IP addresses to communicate with each other. However, this often relies on the use of Transmission Control Protocol (TCP) port numbers to distinguish endpoints when traversing network boundaries. The IP layer can use IPv4 or IPv6. Each includes a version of IPSec that allows authenticated and encrypted communication between devices.

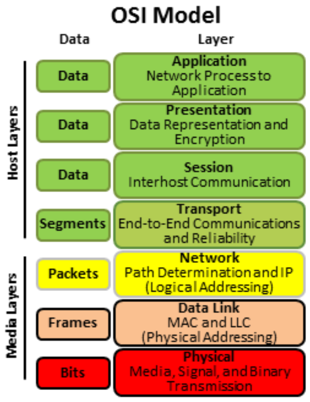
OSI Model
Data
Layer
Host Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Communications and Reliability
Media Layers
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical Addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Figure 2 OSI Layer Model

Below the network layer is the data link layer, which connects one device to another. This layer has two sub-layers, the logical link control (LLC) and media access control (MAC) layer. The LLC is the higher sublayer,

Manuscript received 25 May 2018; revised 15 July 2018. This work was supported in part by the U.S. Secretary of the Air Force and The Institute for Defense Analyses (IDA). The publication of this paper does not indicate endorsement by any organization in the Department of Defense or IDA, nor should the contents be construed as reflecting the official position of these organizations

Kevin E. Foltz is with the Institute for Defense Analyses. (email: kfoltz@ida.org)
William R. Simpson is with the Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, Virginia 22311 USA and is the corresponding author phone: 703-845-6637, FAX: 703-845-6848 (e-mail: rsimpson@ida.org)

focusing on multiplexing, while the MAC layer handles addressing and channel access control.

The MAC address is unique to different hardware instances on a subnetwork, allowing unambiguous point-to-point local communication. This can be wired (Ethernet), or wireless, (Wi-Fi). It can be point-to-point, such as a wire from one machine to another, or broadcast, such as Ethernet or Wi-Fi. Wi-Fi provides security through various protocols, such as Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) [4].

Ethernet and Wi-Fi include not just data link layer protocols but also specifications for the underlying physical properties of the waveforms and the structure of signals. These can provide some security through frequency-hopping patterns, beam-forming, or other physical layer techniques.

In some cases, such as Link 16 [5], multiple layers are integrated into a single protocol. This facilitates communication between layers. And it reduces modularity and portability, but it can allow functions like basing higher-layer coding rates and transmission windows on physical layer signal-to-noise ratios. This could distinguish network congestion from jamming and initiate appropriate responses.

III. MOBILE AD HOC NETWORK SERVICES

The services described in this section are shown in Figure 3. These services are automated, and seek only operator confirmations when and if required. They reside on each element participating in the networks shown in Figure 2. Each element in Figure 3 must participate in a handshake that identifies compatible protocols, waveforms, and drivers to establish a connection. These services act as the initial end-points for connection management. The connection is followed by a bi-lateral authentication and secure channel to the end-point device manager service [6]. The end-point device manager service is the entry point for the requester to access domain services. This must be followed by bi-lateral authentication at the device level. Basic services are shown on the left, building from basic hardware capabilities to supported protocols. Mobile Ad Hoc Network services are on the right, building from hardware and software management to the "Send Data" service that takes data and a destination as an input and sets up appropriate connections and initiates the communication using the supplied data. Arrows indicate dependencies, where arrows point from the service that is used to the service that uses it.

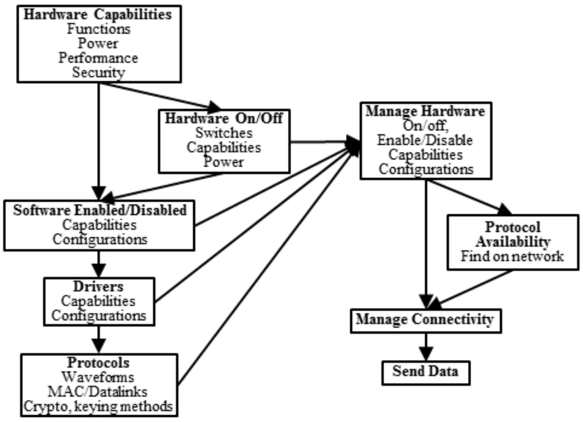

Figure 3 Mobile Ad Hoc Services and Dependencies

A. *Detection of Hardware Capabilities*

This section describes the basic services that provide information about the available hardware and the software that directly controls it. These are typically duplicated for each piece of communication hardware in a device so that higher layer services have direct and independent control over each hardware interface. The interfaces to the hardware may be specific to the hardware so that higher layer services provide and use mediation services to interface with these lower-level services.

In order for a node to join a mobile or ad hoc network it must know that the network exists. This can be done by continuously polling for available connections or looking for connections when a request is made to connect. Polling involves more ongoing work and power but provides continuous feedback, while on-demand connection uses fewer resources but requires explicit instruction and incurs a delay. To bridge these two methods, a local service can be invoked that periodically polls for connections and provides the latest data to higher-layer services. This provides a configurable method to trade off between power and responsiveness across all possible connection types.

Connections at the lowest layer involve the hardware that actually does the signal generation and transmission. This hardware is controlled by drivers or other software that provide an interface to the operating system and local applications and services. The following information is of interest:

- Hardware capabilities that exist for a given device:
  - Capabilities that are supported,
  - Power and other performance that is supported;
- Hardware that is enabled or disabled by physical switches or other hardware mechanisms;
- Hardware that is enabled or disabled by software:
  - Capabilities that are enabled or disabled in the software;
- Hardware that has the appropriate software drivers and other code in place for use:
  - Capabilities that are supported by the drivers or software;
- Protocols that are supported for the hardware:
  - Waveforms,
  - MAC/Datalink protocols and versions,
  - Crypto protocols, versions, keying methods.

Each of these translates into local services for mobile and ad hoc networking. The services described in this section provide basic information about what networking is available, what could be made available, and the capabilities associated with what is and what could be available. In addition, some configuration of the lower layer hardware and software is made available through these services to other services.

The capabilities list for a device describes what hardware is available. This may take different forms. For some devices it could provide a list of standard hardware regardless of what is currently available, such as standard-issue mass-produced units. Such a service would rely on outside or fixed data sets and not the system itself. Other services describe the hardware interfaces associated with the device. For example, a description of whether Universal

Serial Bus (USB) 3.0 is supported or just USB 2.0 would be useful when deciding which hardware device to attach through a USB port. Such services could be offline, static, or based on querying the actual device to determine what is available. Other services describe what hardware is actually connected. Unlike some of the services described above that rely on fixed or external information sources, this service actually queries the system to determine what is connected. For hardware that is found, additional information can sometimes be provided, such as the capabilities of the hardware in terms of speed, power, or supported frequencies.

In some cases hardware is available but switched off. This service provides information about the current state of such hardware. In some cases, hardware that is switched off is indistinguishable from hardware that is not present, but when possible, a distinction is made. This allows a service to inform a user that a physical action must be taken to enable communication.

In addition to hardware switches, there are ways to enable and disable communication hardware through the use of software. This can be through an application, the operating system, registry items, or device driver settings. A service is provided to describe the current state of the communication hardware and allow changing this state as permitted through software. In addition to a simple on/off switch, software can provide detailed capability and configuration information, such as frequencies, versions, protocols, security settings, and many others.

In order to use the communication hardware, appropriate drivers and other software must be available and correctly functioning. This service checks hardware for proper operation and reports the status of the hardware and its drivers. This service may simply examine the driver and perform what amounts to static analysis of the system, or it may actually attempt to use the system and check that it responds appropriately. This service provides not just information about the system, but information about how it is currently operating. This includes whether the device is functioning, as well as which of its capabilities are working, such as transmission speeds, error rates, or power consumption, and potentially how well they are working.

This service provides information about particular protocols that run over different communication hardware. The protocols of interest are the protocols specific to the communication hardware. For example, a Wi-Fi protocol service would provide information about the Wi-Fi protocol, not IP or TCP. This service provides information about which protocols are supported by the hardware and which versions of each of these supported protocols are available. Additional information includes which frequencies, waveforms, data link, or MAC layer protocols are supported, and what type of cryptography or other cryptographic protections are available.

B. Detection of Network Opportunities

This service provides the ability to test enabled hardware for its protocol support at the network layer. This goes beyond the protocol-based services discussed in the previous section, which apply to the hardware protocols. It looks, for example, for Dynamic Host Configuration Protocol (DHCP) servers, network gateways, DNS servers, and other services that would be available in the presence of a network. These are the services that will be used for web service and web application requests. It is important to know whether these services are available, and to what extent they are provided. Knowledge about whether the connection is local or connected to other networks provides important information about the type of connection that can be used by other services.

This service includes tests for proxies, gateways, and other forms of network intermediaries. For example, proxies can be detected by accessing known sites and checking the certificate provided through Hypertext Transfer Protocol Secure (HTTPS). If it does not match the known good certificate, then a proxy is in the middle. This informs decisions about which network to use, since networks with proxies make ELS communication impossible by preventing end-to-end authentication through TLS, but they would be acceptable for low-security traffic.

C. Selection of Waveforms and Protocols

This service is used to turn hardware on and off in order to use a specific set of communication hardware. In some cases this capability can function fully in software using the software interfaces described in the previous section. In other cases, in which physical action is required, a notification to a human or other interface, such as a machine or robot, is required to initiate the hardware action. In either case, the goal is to have the appropriate hardware on and enabled and everything else off or disabled. This can be for power conservation, stealth, or just a general security practice to reduce unneeded interfaces.

In addition to just turning hardware on and off, this service allows configuration of the hardware, to include selection of frequencies, protocol versions, waveforms, and other hardware-level information. This service acts somewhat like a mediation service that provides a standard interface for higher-level protocols to manage the underlying hardware. It translates the hardware and low-level software controls into standard interfaces for the higher layers. This enables a consistent treatment of communication channels and re-use of higher-layer services across the enterprise and different devices within it.

This service dynamically maintains a set of connections that provide an optimal allocation of resources to available potential connections based on provided performance metrics. For example, if high-speed connectivity to a particular IP address is desired, the service may continuously poll for available connections and choose the fastest one that has connectivity to the desired endpoint. Other parameters can be weighed against each other as well, such as power consumption, cost, and combinations such as power per bit or power per bit/sec. Additional inputs would be required for this service to operate effectively, including power consumption models, pricing models, and latency and throughput measurements and models.

This service uses the Manage Hardware service to actually make changes to the system and its connectivity. It uses a set of defined metrics, measured and provided information about the available networks and connections, and optimization logic to make decisions about how to invoke Manage Hardware to best provide what is desired.

This service not only determines which protocols are available, as described above, but also performs handshakes and information exchanges to establish Internet Protocol (IP) addresses, secure connections, and other functions that actually initiate protocols for connectivity. Examples include DHCP requests, Domain Name System (DNS) queries, and other protocols that are common first steps toward data transfer after initial basic connectivity is established. Any ongoing "ping"-type communication is handled by this service as well to establish and update what protocols are available.

D. Service Discovery

Lower-level service discovery is addressed by the Protocol Availability service, but for ELS web services a separate method must be used. In a connected network the claims query service is used to determine a list of all applications and services to which an ELS requester entity has claims or access through identity. In a Disconnected, Intermittent or Low-latency (DIL) mobile ad hoc environment, this service may not be accessible, but a local copy may be available. If so, this can be used for service discovery. This local copy must be hosted in a canonical place that is accessible to anyone on the network so that it can be used as an initial access point to any other ELS services and applications available in the local environment. Although the claims query service is not part of Mobile Ad Hoc services (it is part of the ELS suite of services), it is mentioned here for context. For all communication, the Send Data service is used to choose the hardware, protocol, and associated settings to provide the data transmission and receiving of any associated responses.

This service provides network communication based on any request and uses available connections to send and receive data. Software on a device calls this service to perform any network-based communication, and this service handles all network requests, sets up appropriate connections if available, and takes care of sending the requests and receiving the responses. It notifies the end entity making requests of the status of the current connections. It uses the metrics and parameters for performance, cost, and power as input and passes these on to the Manage Connectivity service to allow it to maintain a set of appropriate connections for communication. However, the Send Data service can override these settings based on current requests. For example, if cost and power are a primary concern, most communications will be disabled by Manage Connectivity. However, when a short high-priority message must be sent on a hardware module that is disabled, Send Data can override the default settings and make performance for that communication a priority for the duration required for the communication.

E. Query/Response Capabilities

Like the service discovery described above, query and response capabilities are based on ELS. After mobile ad hoc services are used to establish connectivity ELS queries can proceed. If network connectivity provides access to the EAS and other network resources, then a standard ELS query can follow. If the local network is isolated and has its own EAS instance, then the local instance can be used to provide ELS-based access to local resources. If the local network is isolated and does not host its own instance of EAS, then access is limited to the non-ELS services provided on the local network. For intermittent connectivity, asynchronous messaging may be offered as a service even if synchronous communication is not, since asynchronous communication can be queued until connectivity returns. As with service discovery, the Send Data service handles the sending and receiving of data over the appropriate connections.

The following sections describe the steps in setting up a connection. It is expected that this service will handle all of these either directly or indirectly using the previously mentioned services.

F. Network Broadcast

The first step for a mobile or ad hoc connection is for the network to identify itself to the mobile node. This is typically done through some sort of network broadcast that identifies the transmitter, the network it represents, its address, the protocols supported, the security offered and required, and other relevant information. For Wi-Fi, for example, a beacon message is sent 100 times per second with this type of information.

In some cases, this function is disabled or limited. For Wi-Fi, the Service Set Identifier (SSID) can be hidden so that only nodes that explicitly request the proper ID are allowed to connect. The beacons can be disabled entirely so that the mobile node must know of the network's existence in advance in order to connect.

Other techniques exist to either hide connections or make detection and connection more difficult for unauthorized entities. These are more difficult to implement on wireless networks because the communications are broadcast to an entity in the vicinity, making replay attacks possible. In general, security protocols are a more robust method of limiting access than simple message content-, formatting-, or timing-based methods. WPA2 for Wi-Fi and IPSec for IP-based network layer communications are examples of such security protocols.

For wired networks, security is often minimal, allowing anyone with physical access and connectivity to use available network services. An Ethernet connection usually is initiated automatically when a wire is plugged in to an Ethernet port. Higher-layer services may require further actions for access, but the lower-level connectivity provides little, if any, security.

G. System Discovery

After the network identifies itself, if it chooses to do so, the mobile node must discover what is available and how to connect [7-10]. With current systems, many possible network connections are available, such as Satellite, Wi-Fi, Military Link Systems, Broadband, and others. The networks provide information about different connections, and the node must make sense of this and discover which networks are accessible, which protocols and options are supported, which security is supported and sufficient to meet policy requirements, and which connections support higher-layer applications. ELS requires bi-lateral authentication, but it may be based on Identity for access.

H. Request to Join

The mobile node, though some internal logic, determines which network to join and initiates a "request to join" handshake [10, 15]. This may involve the exchange of identification information, it may include security parameter negotiation, and it may include protocol negotiation. Wi-Fi often includes security information. Link systems use device profiles to set the message formats and protocols. In any case, this is where the connection from the mobile node to the network node is established, along with any required parameters.

As part of the request to join, physical layer attributes may be collected, such as signal strength, noise level, signal quality, multi-path parameters, location information, and supported waveforms and formats. Wi-Fi 802.11n and 802.11ai support beamforming, allowing the multiple antennas at the transmitter and receiver to be used to determine the direction of transmission, which can boost the signal in the vicinity of the communicating entities and reduce it elsewhere. This allows reduced power, slightly increased security, and potentially better use of available network resources by reducing interference with other transmissions.

Other more advanced techniques may allow the use of multipath and complicated urban obstacles to be used to enhance channel security, quality, power efficiency, and data rates. The transmitter sends a test signal to the receiver, which then relays the received signal properties back to the transmitter. The transmitter can then reshape the transmission to "invert" the environmental distortion and allow positive reconstruction of signals at the receiver. Listeners at other physical locations will not be able to properly reconstruct the signal. This allows lower power transmission, better signal to noise, and potentially better privacy against eavesdroppers.

IV. EXCHANGE OF CERTIFICATES

One important part of the request to join includes the exchange of certificates. The certificates are assigned to devices and allow authentication based on a trusted certificate authority. For ELS, certificates are stored in hardware, such as a Hardware Security Module (HSM) [11] or Common Access Card (CAC) [12]. For lower layer exchanges, the device Trusted Platform Module (TPM) [13] is the preferred location. Each device is equipped with a TPM or TPM-like hardware certificate and key store, which is used to authenticate to the network or to the mobile node when required.

For mobile devices without hardware stores, a derived credential may be used for the certificate exchange. This derived credential is issued by a trusted registration authority (RA) in the enterprise. The derived credential uses the same original certification as the primary credential. If the primary credential is revoked for reasons relating to certification, the derived credential is also revoked, since its certification is no longer secure. If the primary credential is revoked due to issues specific to the credential instance, then the derived credential may remain valid independently. Revocation of the derived credential similarly may or may not lead to revocation of the primary credential, based on the reasons for revocation.

V. DEVICE REQUIREMENTS AND SETUP

Devices allowed to join enterprise networks are registered and managed by the enterprise use restrictions. All devices have a PKI certificate (DoD PKI or derived) in hardware storage (preferably in a TPM). The device and the domain controller perform bi-lateral PKI-based mutual authentication before establishment of the channel to the end-point device manager service. The device may also contain one or more individual user certificates (DoD PKI or derived) that are activated when the user signs on to the device. The device may be required to register with the AFCO domain and report attestation from the TPM and other data such as location (where appropriate).

After joining the network and properly authenticating, it may be desirable to set up an end-point device manager service connection to a remote network. This provides an IP-layer secure tunnel through which higher layer data can be sent. The initial network connection only applies to the link layer, or device-to-device connection.

The end-point device manager connection uses machine certificates to authenticate the mobile node to the end-point device manager server and the end-point device manager server to the mobile node. The end-point device manager server then makes internal network services available to the mobile node. Particular attention must be paid to which nodes are allowed to connect to the end-point device manager server. The devices must have controls, through mobile device management or some other verifiable machine hardware and software integrity checks, that ensure that the device is protected from compromise to a level comparable to that of the internal nodes on the network.

VI. SERVICE DISCOVERY

After connecting through the end-point device manager, or just to the local network, service discovery can begin. This starts the use of higher-layer protocols, which talk using various protocols over TCP, UDP, or other transport layer protocols. Requesters (all active entities must have a credential (derived credentials for entities residing on mobile platforms are permitted) to initiate a request. For example, the requester may use a known URL, such as the EAS Claims Query service to retrieve a list of available services. These services are provided based on the requesting entity's identity, as provided in a CAC, PIV, an NPE certificate, or derived credential, HSM, or other certificate or key store.

Service discovery [14-17] can be initiated locally for DIL environments with a local cache of the claims repository and EAS Claims Query service. The claims query service may be modified to provide identity-based access-only claims. For mobile devices that are provided network connectivity to the primary EAS instance, no cache is required and a normal request is sent. Discovery may be accomplished initially using a Claims Query service. The initial handshake is bi-lateral PKI mutual authentication. This service is identity-based and returns links to claims for service that the requester has. The requester must know the local Uniform Resource Locator (URL) for that service in the connected network.

VII. REQUEST FOR SERVICE

When access to the EAS is established, the request for service can be sent to the desired application or service or a link in the Claims Query Service return page may be executed. The EAS-provided link redirects to an STS, which provides authorization information in a Security Assertion Markup Language (SAML), and then redirects back to the service. The service's ELS handler processes the request and allows access.

Mobile and ad hoc networking requires some level of performance to support higher-layer protocols and applications [15-16]. In some cases, such as poor wireless links or intermittent connectivity, the networking protocols do not function well enough to support the higher-layer protocols. In other cases, the implementation of the protocols is inefficient, uses improper configuration, or adds extra components that reduce performance, such as monitoring or filtering. Those factors under the control of the implementer must combine with those not under control to provide a level of service that supports higher-level protocols and applications appropriate for the network and network participants.

VIII. SUMMARY

We have reviewed the mobile ad hoc issues in a high assurance security system. We have also described an approach that relies on high-assurance architectures and the protection elements they provide through PKI. The basic approach becomes compromised when identity is not verified by a strong credential for unique identification (such as holder-of-key in a PKI, or a credential derived from that credential). The PKI usage is so fundamental to this approach that we have provided non-certificated users a way to obtain a temporary PKI certificate based upon their enterprise need and the level of identity assurance needed to provide access and privilege to applications. The process is fully compatible with ELS and works as a complement to existing infrastructure. This work is part of a body of work for high-assurance enterprise computing using web services. Elements of this work are described in [17-23].

REFERENCES

[1] MANET Definition, http://techterms.com/definition/manet

[2] Simpson, William R., CRC Press, "Enterprise Level Security – Securing Information Systems in an Uncertain World," by Auerbach Publications, ISBN 9781498764452, May 2016, 397 pp.

[3] The OSI Model's Seven Layers Defined and Functions Explained, https://support.microsoft.com/en-us/kb/103884.

[4] WEP vs WPA Encryption, NETGear Support, http://kb.netgear.com/app/answers/detail/a_id/20043/~/wep-vs-wpa-encryption?cid=wmt_netgear_organic

[5] Understanding Voice and Data Link Networking, .Northrop Grumman's Guide to Secure Tactical Data Links, http://www.northropgrumman.com/Capabilities/DataLinkProcessingAndManagement/Documents/Understanding_Voice+Data_Link_Networking.pdf

[6] William R. Simpson, and Kevin E. Foltz, Lecture Notes in Engineering and Computer Science, "Enterprise End-point Device Management," *In Process*, Proceedings of the World Congress on Engineering, July 2018, Imperial College, London, pp. TBD.

[7] S. Ghemawat, H. Gobioff, and S.-T. Leung. The Google filesystem. In SOSP, 2003.

[8] G. Graefe. Query evaluation techniques for large databases.ACM Comput. Surv., 25(2), 1993.

[9] J. Hammerbacher. Managing a large Hadoop cluster. Presentation, Facebook Inc., May 2008.

[10] P. Mishra and M. H. Eich. Join processing in relational databases. ACM Comput. Surv., 24(1), 1992.

[11] Hardware security module, Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Hardware_security_module

[12] Common Access Card (CAC) http://www.cac.mil/common-access-card/

[13] Trusted Platform Module (TPM) Summary, http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/

[14] C. Olston, B. Reed, U. Srivastava, R. Kumar, and A. Tomkins. Pig latin: A not-so-foreign language for data processing. In SIGMOD, pages 1099–1110, 2008.

[15] Pavlo, E. Paulson, A. Rasin, D. J. Abadi, D. J. Dewitt,S. Madden, and M. Stonebraker. A comparison of approaches to large-scale data analysis. In SIGMOD, 2009.

[16] D. A. Schneider and D. J. DeWitt. A performance evaluation of four parallel join algorithms in ashared-nothing multiprocessor environment. In SIGMOD, 1989.

[17] William R. Simpson, and Kevin E. Foltz, "Enterprise Level Security: Insider Threat Counter-Claims," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2017, 25–27 October, 2017, San Francisco, USA, pp. 112–117.

[18] William R. Simpson and Kevin E. Foltz, Proceedings of the 22nd International Command and Control Research and Technology Symposium (ICCRTS), "Escalation of Access and Privilege with Enterprise Level Security," Los Angeles, CA. September 2017, pp. TBD.

[19] William R. Simpson and Kevin E. Foltz, Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017), Volume 1, pp. 177–184, Porto, Portugal, 25–30 April, 2017, "Enterprise Level Security with Homomorphic Encryption," SCITEPRESS – Science and Technology Publications.

[20] Kevin Foltz, and William R Simpson, "Enterprise Considerations for Ports and Protocols," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2016, 19–21 October, 2016, San Francisco, USA, pp.124–129.

[21] Kevin E. Foltz, and William R Simpson, "Simplified Key Management for Digital Access Control of Information Objects," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2016, 29 June–1 July, 2016, London, U.K., pp. 413–418.

[22] Kevin E. Foltz and William R. Simpson, Proceedings of The 20th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI, "Enterprise Level Security – Basic Security Model," Volume I, WMSCI 2016, Orlando, Florida, 8–11 March 2016, pp. 56–61.

[23] Kevin E. Foltz and William R. Simpson, Wessex Institute, Proceedings of the International Conference on Big Data, BIG DATA 2016, "Access and Privilege in Secure Big Data Analysis," 3–5 May 2016, Alicante, Spain, pp. 193–205.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY) 25-10-18	2. REPORT TYPE Non-Standard	3. DATES COVERED (From – To)

4. TITLE AND SUBTITLE Mobile Ad Hoc for Enterprise Level Security	5a. CONTRACT NUMBER HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS
6. AUTHOR(S) William R. Simpson, Kevin E. Foltz	5d. PROJECT NUMBER BC-5-2283
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	8. PERFORMING ORGANIZATION REPORT NUMBER NS D-9113
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Frank P. Konieczny USAF HQ USAF SAF/CIO A6 United States Air Force SAF-CIO A6, 1800 Air Force Pentagon, Washington DC 20330-0001	10. SPONSOR'S / MONITOR'S ACRONYM USAF SAF/CIO A6
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

This draft has not been approved by the sponsor for distribution and release.

13. SUPPLEMENTARY NOTES

Project Leader: Kevin Foltz

14. ABSTRACT

Threat intrusions to enterprise computing systems have led to a formulation of guarded enterprise systems. The approach was to put in place steel gates and prevent hostile entities from entering the enterprise domain. The current complexity level has made the fortress approach to security implemented throughout the defense, banking, and other high trust industries unworkable. The alternative security approach called Enterprise Level Security (ELS) is the result of a concentrated fourteen year program of pilots and research. The primary identity credential for ELS is the Public Key Infrastructure (PKI) certificate, issued to the individual who is provided with a Personal Identity Verification (PIV) card with a hardware chip for storing the private key. All sessions are preceded by a PKI mutual authentication and a Transport Layer Security (TLS) 1.2 communication pipeline is established. This process was deemed to provide a high enough identity assurance to proceed. However, mobile ad hoc networking allows entities to dynamically connect and reconfigure connections to make use of available networking resources in a changing environment. These networks range from tiny sensors setting up communications based on a random or unknown configuration to aircraft communicating with each other, the ground, and satellites. Scenarios have differing requirements in terms of setup, reconfiguration, power, speed, and range. This paper presents an adaptation of the ELS principles to the mobile ad hoc scenario.

15. SUBJECT TERMS

Enterprise Level Security; Mobile Ad-hoc; Networking; Service Requirements

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Frank P. Konieczny
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	Unlimited	6	19b. TELEPHONE NUMBER (Include Area Code) 703-697-1308