Secure VM Migration in Tactical Cloudlets

Grace A. Lewis, Sebastián Echeverría, Dan Klinedinst, Keegan Williams
Carnegie Mellon Software Engineering Institute
Pittsburgh, PA USA
{*glewis, secheverria, djklinedinst, kmwilliams*}*@sei.cmu.edu*

***Abstract*—Tactical cloudlets are forward-deployed, discoverable, virtual-machine-based servers that can be hosted on vehicles or other platforms to provide a computation offload and data staging infrastructure for mobile devices in the field. Because of the mobility of cloudlets in the field, as well as dynamic missions, a mobile user of a cloudlet might need to migrate active capabilities (computation and data) to another trusted cloudlet. A common solution for establishing trust between two nodes is to create and share credentials in advance, and then use a third-party, online trusted authority to validate the credentials of the nodes. However, the characteristics of tactical environments do not consistently provide access to that third-party authority or certificate repository because they are DIL environments (disconnected, intermittent, limited). The goal of this paper is to present a solution for secure VM migration between tactical cloudlets based on secure key generation and exchange in the field.**

1. Introduction

Soldiers and first responders operating in tactical environments increasingly make use of mobile systems for mission support. However, dynamic context, limited computing resources, and disconnected-intermittent-limited (DIL) network connectivity in the field are challenges for continued operations. Tactical cloudlets help to overcome some of these challenges by providing a forward-deployed, discoverable, virtual machine (VM) based infrastructure to provide (1) extended computing power, (2) forward-data-staging for a mission, (3) data filtering to remove unnecessary data from streams intended for dismounted warfighters, and (4) collection points for data heading for enterprise repositories.

Tactical cloudlets can be deployed in the field as fixed cloudlets, but can also be hosted on vehicles as mobile cloudlets. Because of this mobility, as well as dynamicity of missions, a mobile user of a cloudlet might need to migrate active capabilities (computation and data) to another trusted cloudlet. A common solution for establishing trust between these cloudlets would be to create and share credentials in advance, and then use a third-party, online trusted authority to validate the credentials of the nodes. However, because of the DIL characteristics of tactical environments it is not possible to guarantee consistent access to that third-party authority.

In previous work [1] we developed a solution for establishing trust between mobile devices and cloudlets based on Identity-Based Encryption (IBE) [2] and the use of out-of-band (OOB) channels (i.e., physical proximity and visual confirmation) that satisfies the following requirements: (1) does not require network connectivity to a third party such as the Internet, an enterprise or wide-area network (WAN), or a Certificate Authority (CA), (2) does not place any specific security requirements on hardware, such as a Trusted Platform Module (TPM) processor [3], (3) does not require pre-provisioning of credentials on the mobile devices, and (4) addresses the threats of a tactical environment (Section 3). The goal of that work was to develop a solution that would not make any assumptions about the nfrastructure.

The solution consists of four sub-processes: (1) *Bootstrapping* to set up the cloudlet as a key generation center for an established period of time (mission duration), (2) *Device Pairing* for authorizing a mobile device access to the cloudlet and transferring the required credentials, (3) *Wi-Fi Authentication* using RADIUS [4] for enabling mobile devices to connect to the cloudlet's Wi-Fi Access Point (WAP) and request access to the network, and (4) *API Requests* for mobile devices to securely access cloudlet-hosted capabilities inside Service VMs (SVMs). The first two sub-processes perform the actual trust establishment; the other two are used to authenticate a paired mobile device requesting access at the Wi-Fi and network level respectively. In addition, there are two ways to revoke device credentials: automatic when mission duration expires, and manual if a device is reported as lost or compromised.

In this paper we present a similar solution for secure VM migration between tactical cloudlets that satisfies the same set of requirements and builds on this previous work. Section 2 presents related work in the area of VM migration and security. Section 3 presents an extended threat model for tactical environments. Section 4 presents the design and implementation of the secure VM migration solution. Section 5 presents the results of the evaluation of the solution against the threat model, vulnerability analysis, and ceremony analysis. Finally, Section 6 concludes the paper.

2. Related Work

Live VM migration — moving a running virtual machine between different physical machines without disconnecting

978-1-5386-0595-0/17/$31.00 ©2017 IEEE

its clients [5] — is an out-of-the-box feature of most virtual machine management software such as KVM and VMWare. It is commonly used in cloud data centers to support load balancing, fault tolerance, energy efficiency, and hardware maintenance. Consistent with these use cases, most research related to VM migration focuses on performance (i.e., reduced downtime) and not on security [6].

There is some work in secure VM migration but most violates the requirements for tactical environments outlined in Section 1. To cite some examples, Shibli et al [6] propose a solution called SV2M that provides protection against active and passive attacks during a VM migration process between cloud servers. However, SV2M requires access to a trusted third party for certificate generation, and then certificate storage in the cloud for access during the migration process. Danev et al [7] propose a solution based on the migration of virtual TPMs (vTPMs) along with VMs. However, regardless of the establishment of a vTPM key hierarchy that introduces an intermediate layer of keys between the TPM and vTPM, the solution still relies on TPM. Zeb et al [8] propose a solution that is not based on TPM, but the pre-requisite is for source and destination cloud servers to have X.509 certificates from a trusted CA. These certificates are used for mutual authentication and then, similar to our solution, a separate shared key is generated for encrypting further communication between source and destination servers. Finally, Hou et al [9] propose a mechanism based on vTPMs that relies on access to a property server for the generation of keys and certificates. However, they introduce a mechanism for user control of the migration process on the source side which in traditional attestation protocols only happens on the destination side. Mutual verification during the migration process is consistent with our proposed solution which is explained in detail in Section 4.

3. Threat Modeling

The threat model for disconnected environments that was developed in the context of a mobile device connecting to and interacting with a source cloudlet [1] was extended to account for the source cloudlet connected to a destination cloudlet at moments in time to support VM migration between the source and the destination cloudlet, as shown in Figure 1 (details in Section 4). The threat model was developed using Microsoft's SDL Threat Modeling Tool [10] which generated 85 potential threats. These threats were examined by a threat modeling expert on our team, evaluated for their applicability to tactical environments, prioritized, and grouped into the 16 relevant threats shown in Table 1. Names of modified threats with respect to our previous work are noted in italic. Names of new threats are noted in bold. The term client refers to a mobile device connecting to a cloudlet, or a cloudlet connecting to another cloudlet. The threat model was used as input for the development ot the solution presented in Section 4. Results of evaluation against the threat model are shown in the last column of Table 1 and described in Section 5.

4. Design and Implementation

To implement the secure VM migration solution, we modified the system described in [1]. VM migration was already a feature of tactical cloudlets as described in [11], but due to the credentials required to connect to a cloudlet, the device using the VM would not be able to continue using it after migration to the destination cloudlet, unless it had been previously paired to the destination cloudlet. To allow for more opportunistic VM migration, it is necessary to migrate the trust established between the source cloudlet and the device to the destination cloudlet. This in turn requires the destination cloudlet to trust the source cloudlet. The method we implemented extends VM migration to (1) add a new process to establish trust or "pair" one cloudlet to another, (2) generate new credentials for a device during migration so it can securely connect to the destination cloudlet after a migration, and (3) deliver these credentials to the device during the migration process. Components added to the system include:

- **Remote Cloudlet Credentials Repository**: This is a new repository that stores credentials used by a cloudlet to connect to another cloudlet. The credentials are generated by a process called Cloudlet Pairing, which is very similar to Device Pairing in [1]. It is implemented as a database containing the encryption passwords, and a Wi-Fi profile stored in the OS with the rest of the credentials.
- **Messages Repository**: This is a new repository to store messages that clients will poll from time to time to see if there are new events, such as the migration of a Service VM (SVM).
- **Bind DNS Server**: When a SVM is created it is assigned a fully-qualified domain name (FQDN), which is registered to a DNS server running on the cloudlet. Cloudlet-Ready Apps use this FQDN instead of an IP address to communicate to SVMs. This will allow them to continue communicating with a SVM, even if it is migrated to another cloudlet and its IP address changes.

The following steps summarize the design of the new migration process to support secure VM migration. For simplicity the source cloudlet is referred to as *Cloudlet A* and the destination cloudlet as *Cloudlet B*:

Step 1: Cloudlet Pairing: This step has to be done before a cloudlet can migrate VMs to another cloudlet and is executed only once. After Cloudlet A is paired to Cloudlet B, Cloudlet B trusts Cloudlet A, and therefore Cloudlet B allows Cloudlet A to connect to its Wi-Fi Access Point and to migrate VMs to it.

Cloudlet pairing is performed through a temporary Wi-Fi ad hoc connection [12] between the two cloudlets. The information needed to set it up is shared verbally between the cloudlet admins (i.e., out-of-band channel). On Cloudlet A, its admin accesses the Cloudlet Manager to generate and show a temporary Wi-Fi SSID and WPA2 Pre-Shared Key

TABLE 1. THREAT MODEL FOR TACTICAL CLOUDLETS SUPPORTING SERVICE VM MIGRATION

#	Name*	Description	Pr.**	Mitigation
Threats Fully Addressed				
1	*Impersonating a client*	Unauthorized client (device or cloudlet) attempts to gain access to the cloudlet environment	H	During the pairing process, client credentials are sent to the RADIUS server running on the cloudlet. Clients authenticate with the RADIUS server when connecting to the Wi-Fi network using 802.1X with EAP-TTLS and PAP.
2	*Finding an active client*	Authorized client (device or cloudlet) is lost or captured with an established connection to the cloudlet environment	H	(1) Fixed deployment duration in bootstrapping process, (2) Manual and automatic client credential revocation, and (3) Validation of API requests against list of valid clients.
3	*Finding an inactive client*	Authorized client (device or cloudlet) is lost or captured without a connection to a currently operating cloudlet	H	(1) Manual and automatic client credential revocation, and (2) Out-of-band channels used in pairing process.
7	Sniffing wireless	Wi-Fi signal is monitored by an external party providing visibility of traffic stream	H	Two-level encryption: WPA2-Enterprise (802.1X) CCMP (AES) encryption with 128-bit key based on a 256-bit password at the transport level, and AES (CBC) encryption with 256-bit key and random IV at the message level.
14	*Impersonating a cloudlet*	Impersonating a trusted cloudlet environment and enticing devices or other cloudlets to connect	H	During the bootstrapping process, cloudlet credentials are stored on the RADIUS server running on the cloudlet and sent to clients during the pairing process. Clients validate cloudlet credentials before connecting to the Wi-Fi network.
Threats Partially Addressed				
6	Lost credentials	Authorization information is obtained by a malicious person who then tries to spoof a client	H	Main mitigation is manual and automatic client credential revocation processes. All API Requests are validated against the list of paired clients before responding to a request. Anything stronger would require TPM and/or encrypting the client's credentials.
Threats Addressed Outside Implementation				
8	Site intrusion	Physical access to cloudlet is obtained providing hands-on access to the equipment	H	In addition to requiring strong passwords for the root user and the cloudlet admin, cloudlet would have to reside in a safe, protected site.
9	*On the net (WAP)*	Network access to a cloudlet's wireless access point (WAP) is obtained	H	Cloudlet is (1) disconnected from the network, and (2) only accepts connections that are authorized by the RADIUS Server.
10	On the box	Access to cloudlet operating system is obtained	H	Strong passwords for the root user and the cloudlet admin are required.
11	Super-user compromise	System admin access to cloudlet is compromised and software and data can be stolen or changed impacting services and integrity	H	Cloudlets only have two users: root and cloudlet admin. Strong passwords for the root user and the cloudlet admin are required. Cloudlet admin does not know the root password. Cloudlet admin account does not have root privileges.
12	Application compromise	Application controls on cloudlet are compromised	L	There are settings in place so that the Cloudlet Manager can only be run locally.
13	Seeing everything	Data management controls on cloudlet are compromised	L	Strong passwords for root user and cloudlet admin are required. Service VMs are responsible for encrypting data residing within the VM.
15	**On the net (NIC)**	Network access to the cloudlet network interface card (NIC) is obtained	H	NICs are only briefly in ad hoc mode, which is when they are vulnerable. WPA2 authentication in ad hoc mode is used.
16	**Daisy chaining (device-cloudlet-cloudlet)**	Device connected to an authorized cloudlet is able to connect to another cloudlet and exploit its approved access	H	Linux by default does not allow IP forwarding and should not be enabled. API does not have any commands that could be used by a device to communicate to another cloudlet with which it is not paired.
Threats Not Addressed				
4	Altered software	Software on an approved device is changed due to downloaded malicious code, tampering, unintended changes, or some other means	M	Mitigation would require integration with TPM or code signing.
5	*Daisy chaining (device-device-cloudlet)*	External device is able to connect to an authorized device and exploit its approved access to the cloudlet environment	M	Mitigation would require device controls that do not allow connections to a mobile device.

* Names of modified threats with respect to our previous work are noted in italics. Names of new threats are noted in bold.

** Priority: H=High, M=Medium, L=Low

for the connection. On Cloudlet B, its admin accesses the Cloudlet Manager to generate and show a random secret for the connection. Each admin verbally shares the information on their screens with one another, and then enters the received information in their respective Cloudlet Managers to start the pairing process.

Once both users start the process, each Wi-Fi NIC is configured using *wpa_supplicant* [13] to work in ad hoc

mode with the SSID and Pre-Shared Key defined above. Temporary, pre-defined static IP addresses are assigned to each cloudlet to allow them to connect through TCP/IP. Cloudlet A starts listening for incoming TCP connections on a pre-defined port. The pairing process that is then started is equivalent to the one used by mobile devices to pair to cloudlets, but using a slightly different communication protocol. We developed a WiFiSKA (Wi-Fi secure key agreement) protocol as a variation of the BluetoothSKA protocol used for device pairing in [1]. WiFiSKA uses TCP over Wi-Fi with WPA2-PSK encryption for communication. It encrypts each message between cloudlets using AES with the secret that both admins shared in the previous step as the AES encryption key. After receiving the credentials from Cloudlet B, Cloudlet A creates a Wi-Fi profile to store all connection information needed to later connect to Cloudlet B's Access Point. Also, Cloudlet A stores its new private key in its remote cloudlet credentials repository, to be later used for encrypting API requests to Cloudlet B.

When the pairing process finishes, the wpa_supplicant daemon is stopped on both cloudlets, terminating the Wi-Fi ad hoc network. After this process, the cloudlets are ready to migrate VMs from one to another when needed, and as many times as needed. Cloudlet Pairing uses the same credential revocation mechanisms briefly described in Section 1.

Step 2: Cloudlet Discovery and Connection: Migration is currently done manually between two cloudlets. When a cloudlet wants to migrate a SVM, it first needs to find available cloudlet networks in the area, and then obtain information about the actual cloudlet host inside that network.

Step 2.1: Cloudlet Network Discovery and Connection: When starting SVM migration in the Cloudlet Manager, the screen to perform the migration allows the user to connect to a nearby Wi-Fi network. This screen will only show networks of cloudlets that this cloudlet has previously paired to in the previous step. Once a network is selected from the list, the system will connect to that Wi-Fi network using its stored profile.

Step 2.2: Cloudlet Discovery and Connection: When the user clicks on the migrate button, information about the cloudlet available on the Wi-Fi network that the cloudlet is connected to will be displayed. The discovery mechanism is the same used by mobile devices, which is Zeroconf though Avahi [15]. This discovers the IP address and port of the Cloudlet Manager API instance running on the destination cloudlet.

Step 3: Service VM Migration: The actual VM migration process is the same as in the original system [11]. SVM metadata is sent to the target cloudlet so that it can be added to its SVM metadata repository. The KVM migration feature is used to perform the actual VM migration [16].

Step 4: Remote Credential Generation for Mobile Device: Right after the last step of the VM migration completes (the memory state migration), a new API message was added to request the target cloudlet to generate and return credentials for each of the mobile devices that are paired to Cloudlet A and are using the migrated VM. This request sends the device ID of each device, and the ID of the SVM that was just migrated.

When Cloudlet B receives the request, it pairs each device exactly as if it was connected to it physically. This results in a set of credentials for each device. Cloudlet B then creates a JSON structure that includes the same information that a device being paired directly would receive: the Device Private IBE Key and Device RADIUS Authentication Password for this cloudlet; as well as Cloudlet B's information: its SSID, RADIUS Server SSL Certificate, and Public IBE Key.

Cloudlet A receives the reply, and stores it the new Messages Repository so that it can later be retrieved by each device. Messages are tagged with (Device ID, Service ID) pairs so that a device can only retrieve its own messages and know what SVM was migrated.

Step 5: Device Obtains Migration Notification (and New Credentials): The mobile device polls the cloudlet every 10 seconds for incoming messages. This is implemented with a dedicated thread that is started once a Cloudlet-Ready App is granted access to a SVM. The thread will periodically send a Cloudlet Manager API request to get all messages for the specific device and Service ID (associated to the SVM it is using).

The cloudlet returns all unread messages in JSON format in the reply to that API command. After a migration, this message contains all the information and credentials to connect to Cloudlet B. The device then stores these credentials in its internal credential storage and creates a new Wi-Fi profile to connect to Cloudlet B's access point.

Step 6: Device Connection to Cloudlet B's Access Point: After becoming aware of the VM migration through the message polling described above, the device will automatically connect to Cloudlet B's Access Point with

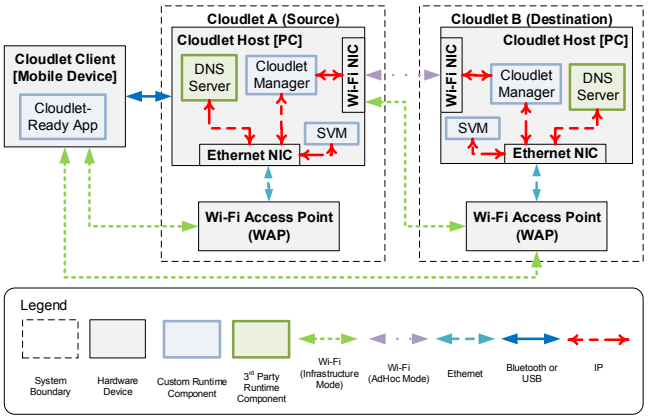

Figure 1. Physical Connections between Nodes

the information it received in the message.

Step 7: Cloudlet-Ready App Communication to Migrated Service VM running on Cloudlet B: The Cloudlet-Ready App is assumed to be using the SVM's FQDN when sending requests to it. Once connected to the new AP, any further DNS requests for the migrated SVM's FQDN will return the new IP address of the migrated SVM, without the app having to know that the VM was migrated and that its IP address may have changed.

Figure 1 shows all the physical connections that are made during a secure SVM migration. Note that not all these connections are active at the same time; in particular:

- Ethernet connections are always enabled.
- The Bluetooth/USB connection is only used when pairing a device directly to a cloudlet.
- The Wi-Fi ad hoc connection is only used when pairing a cloudlet to another cloudlet.
- During normal use of the cloudlet, the Cloudlet Client connects through Wi-Fi to the AP of the source cloudlet; this is the only wireless connection enabled.
- During the Secure SVM Migration process, the source cloudlet connects to the destination cloudlet's AP through its Wi-Fi NIC, and disconnects after the migration is completed.
- The client disconnects from the source cloudlet's AP and connects to the destination cloudlet's AP through Wi-Fi after it is is notified that the migration is complete.

5. Evaluation

Mitigations for the identified threats drove the implementation and testing of the system and are shown in the last column of Table 1. Many are unchanged from our previous work in establishing trust between devices and cloudlets [1]. Most of the changed threats involve an unauthorized cloudlet. The change in the threat vector is that cloudlet-to-cloudlet pairing uses Wi-Fi to exchange credentials rather than USB or Bluetooth. The ad hoc Wi-Fi connection used for pairing is protected with WPA2 Pre-Shared Key (PSK) encryption, and the encryption keys are exchanged verbally. Without these keys, the credentials to connect to a cloudlet's Access Point cannot be obtained. These credentials can be set to timeout or can be manually revoked, as with devices.

The threat *Daisy Chaining* has changed, as a cloudlet can potentially connect through another cloudlet to a device with which it shares no trust relationship (cloudlet to cloudlet to device). This is primarily mitigated by the fact that Linux prevents IP forwarding by default, so while a cloudlet may have authorized connections both to its own clients and to other cloudlets, those two connections cannot communicate to each other.

We then conducted vulnerability analysis using simple attack trees to determine potential attack vectors [17]. We extended the attack tree created in [1] to include new attack surfaces for VM migration, specifically the ad hoc Wi-Fi network used for cloudlet pairing. As an attacker, the end goal would be to gain access to the data being shared between cloudlets. We identified four possible paths to access that data, of which only Local Network Access is relevant when considering the secure VM migration solution. The resulting attack tree is shown in Figure 2. Based on the analysis we concluded that all new vulnerabilities in the Local Network Access Path are mitigated (dark nodes in the figure) because the ad hoc Wi-Fi connection uses strong WPA2 PSK authentication, coupled with an out-of-band (verbal) secret key. It is also far too short lived for an attacker to conduct a successful brute force attack on the key. An attacker could create a Wi-Fi Rogue Access Point, but without the Pre-Shared Key they could not access the credentials. A full analysis of the attacks that are not related to VM migration can be found in [1].

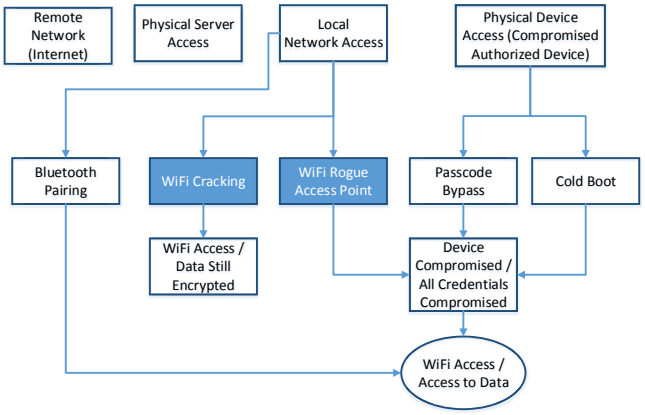

Figure 2. Simple Attack Tree

We also performed a ceremony analysis, which extends the concept of network protocol analysis by including human beings as nodes in the network [18]. Ceremony nodes in the exchange of credentials between two cloudlets for Service VM Migration from Cloudlet A to Cloudlet B are shown in Figure 3. The human nodes are: Mobile User, Cloudlet A Admin, Cloudlet B Admin, and Cloudlet Provider. The figure shows five distinct credential exchanges: (a) Cloudlet Setup, (b) Cloudlet Delivery, (c) Device Credential Generation (for pairing with Cloudlet A), (d) Cloudlet Credential Exchange, and (e) Device Credential Generation (for pairing with Cloudlet B). We concluded that the full process provides a sufficient level of assurance for the credentials and data. Several process elements are included as mitigations for threats addressed outside of the implementation in Table 1.

6. Summary and Conclusions

The paper presented a solution for secure VM migration in tactical cloudlets that combines Identity-Based Encryption (IBE) with mechanisms for Secure Key Exchange

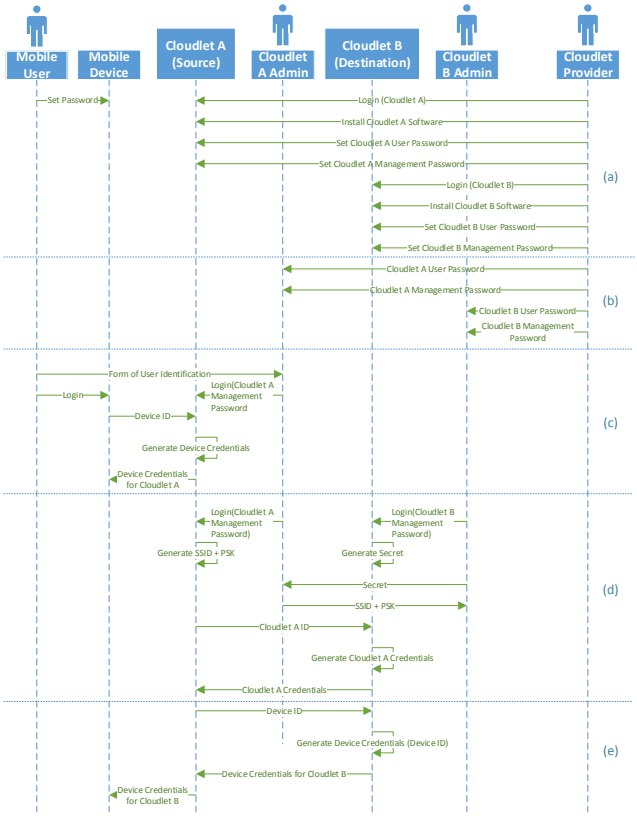

Figure 3. Ceremony Analysis

without a Trusted Third Party. The solution was developed based on an extended threat model for disconnected environments and implemented in our open-source tactical cloudlets project targeted at deployment in these types of environments. Evaluation of the implementation was done against the threat model and using vulnerability analysis. The results show that it is a resilient solution that addresses most of the threats and characteristics of disconnected environments if combined with proper application-, OS-, network- and site-level controls. An additional ceremony analysis was conducted to provide guidance on threats that are addressed outside of the secure VM migration solution. Current and future work is focusing on reduced human involvement and use of passive out-of-band channels, especially as tactical systems start to incorporate resource-constrained IoT (Internet of Things) devices such as sensors.

The implementation of the tactical cloudlets system that includes secure VM migration is available at https://github.com/SEI-AMS/pycloud/wiki.

Acknowledgments

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center (DM17-0044).

References

[1] S. Echeverría, D. Klinedinst, K. Williams, and G. A. Lewis, "Establishing trusted identities in disconnected edge environments," in *Proceedings of the 2016 IEEE/ACM Symposium on Edge Computing*, 2016, pp. 51–63.

[2] L. Chen, "An interpretation of identity-based cryptography," in *Foundations of security analysis and design IV*. Springer, 2007, pp. 183–208.

[3] *ISO/IEC 11889-1:2015: Information Technology – Trusted Platform Module Library – Part 1: Architecture*, International Organization for Standardization Std., 2015.

[4] Cisco Systems. (2006) How does RADIUS work? [Online]. Available: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

[5] P. G. J. Leelipushpam and J. Sharmila, "Live VM migration techniques in cloud environment: A survey," in *2013 IEEE Conference on Information Communication Technologies*, April 2013, pp. 408–413.

[6] M. A. Shibli, N. Ahmad, A. Kanwal, and A. Ghafoor, "Secure virtual machine migration (SV2M) in cloud federation," in *Security and Cryptography (SECRYPT), 2014 11th International Conference on*. SCITEPRESS, 2014, pp. 1–6.

[7] B. Danev, R. J. Masti, G. O. Karame, and S. Capkun, "Enabling secure VM-vTPM migration in private clouds," in *Proceedings of the 27th Annual Computer Security Applications Conference*, ser. ACSAC '11. New York, NY, USA: ACM, 2011, pp. 187–196.

[8] T. Zeb, A. Ghafoor, A. Shibli, and M. Yousaf, *A Secure Architecture for Inter-cloud Virtual Machine Migration*. Cham: Springer International Publishing, 2015, pp. 24–35. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-23829-6_2

[9] C. Hou, C. Huang, H. Dai, Y. Ding, L. He, and M. Ji, "Enabling user-policy-confined vm migration in trusted cloud computing," in *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*, Sept 2016, pp. 66–71.

[10] Microsoft Corporation, "SDL Threat Modeling Tool," 2017. [Online]. Available: https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx

[11] S. Echeverria, G. Lewis, J. Root, and B. Bradshaw, "Cyber-foraging for improving survivability of mobile systems," in *Military Communications Conference (MILCOM), 2015 IEEE*, Oct 2015, pp. 1454–1459.

[12] *ISO/IEC/IEEE 8802-11:2012: Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*, International Organization for Standardization Std., 2012.

[13] J. Malinen, "Developers' documentation for wpa_supplicant and hostapd," 2015. [Online]. Available: https://w1.fi/wpa_supplicant/devel/index.html

[14] R. Chandra, J. Padhye, L. Ravindranath, and A. Wolman, "Beacon-stuffing: Wi-fi without associations," in *Mobile Computing Systems and Applications, 2007. HotMobile 2007. Eighth IEEE Workshop on*. IEEE, 2007, pp. 53–57.

[15] "Zero Configuration Networking (Zeroconf)." [Online]. Available: http://www.zeroconf.org/

[16] KVM, "Migration — KVM," 2015. [Online]. Available: https://www.linux-kvm.org/index.php?title=Migration&oldid=173268

[17] B. Schneier, "Attack trees," *Dr. Dobb's Journal*, vol. 24, no. 12, pp. 21–29, 1999.

[18] C. M. Ellison, "Ceremony design and analysis." *IACR Cryptology ePrint Archive*, vol. 2007, p. 399, 2007.