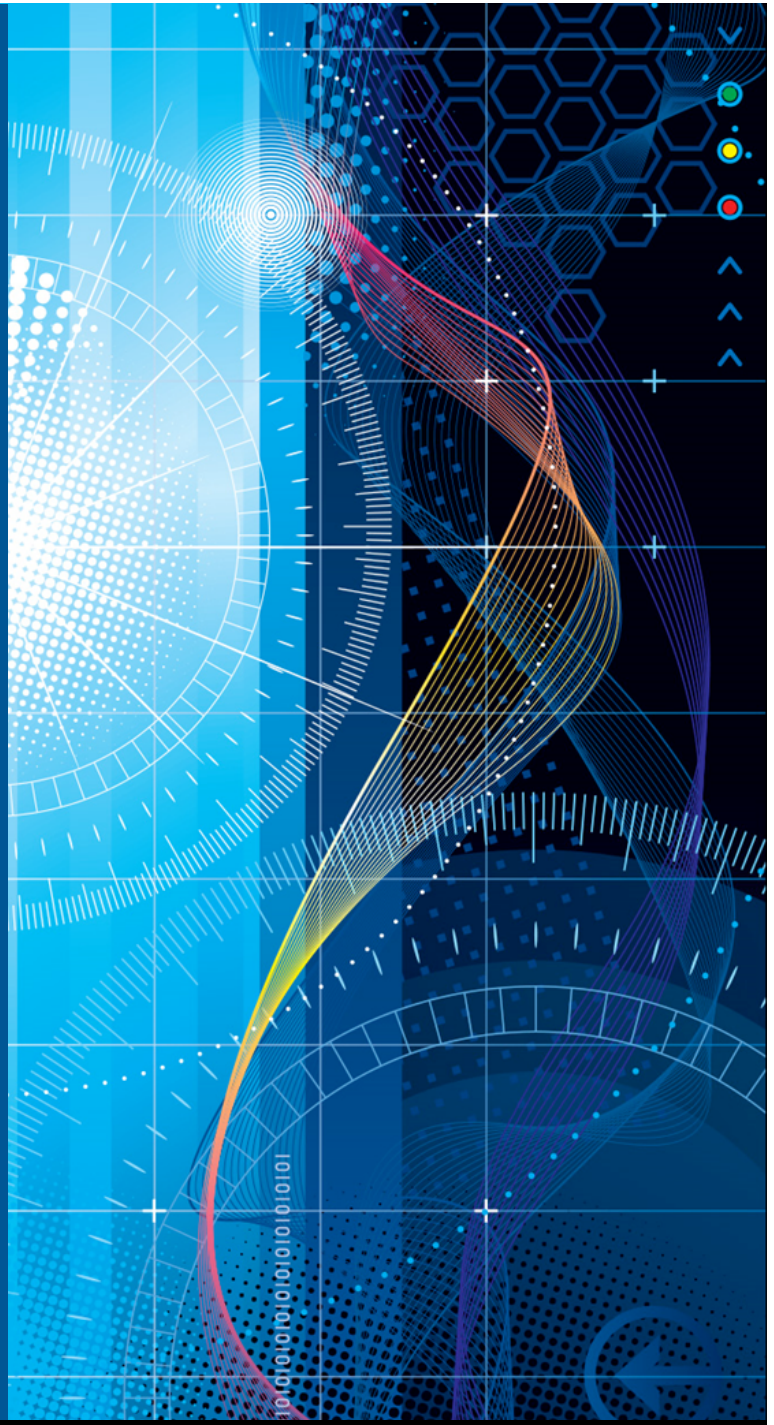
Secure VM Migration in Tactical Cloudlets

Grace Lewis

glewis@sei.cmu.edu

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



© 2017 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution

Copyright 2017 Carnegie Mellon University and IEEE. All Rights Reserved.

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.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

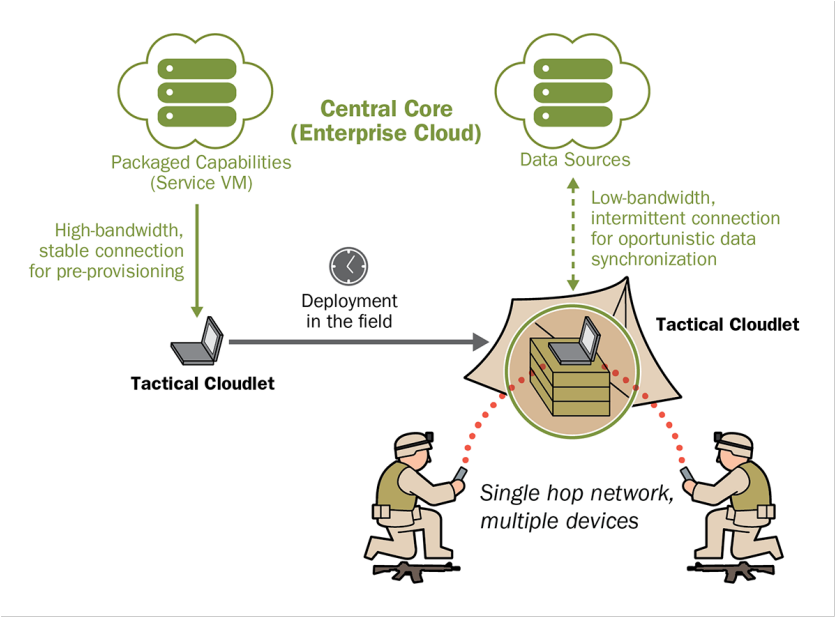
This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM17-0829

Background: Tactical Cloudlets

Forward-deployed, discoverable, virtual machine (VM) based cloudlets that can be hosted on vehicles or other platforms to provide

- infrastructure to offload computation
- forward data-staging for a mission
- data filtering to remove unnecessary data from streams intended for dismounted warfighters
- collection points for data heading for enterprise repositories



Features

- Pre-Provisioned Cloudlets with App Store
- Standard Packaging of Service VMs
- Optimal Cloudlet Selection
- Cloudlet Management Component
- Cloudlet Handoff/Migration
- Secure Key Generation and Exchange

© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Background: Security 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. Does not require pre-provisioning of credentials on nodes
4. Addresses the threats of a tactical environment

In previous work we developed a solution for establishing trust between mobile devices and tactical cloudlets based on Identity-Based Encryption (IBE) and the use of out-of-band (OOB) channels (i.e., physical proximity and visual confirmation)

© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

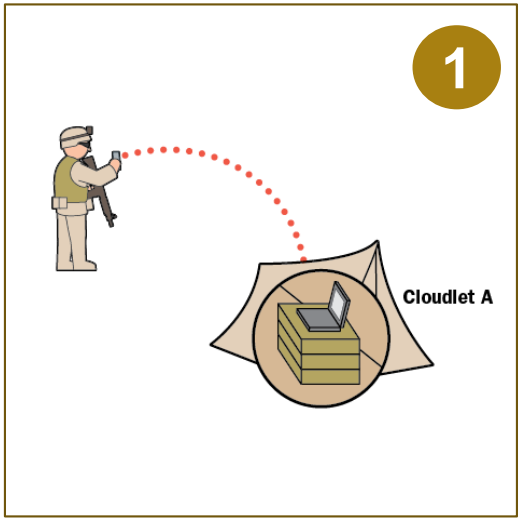
Secure VM Migration

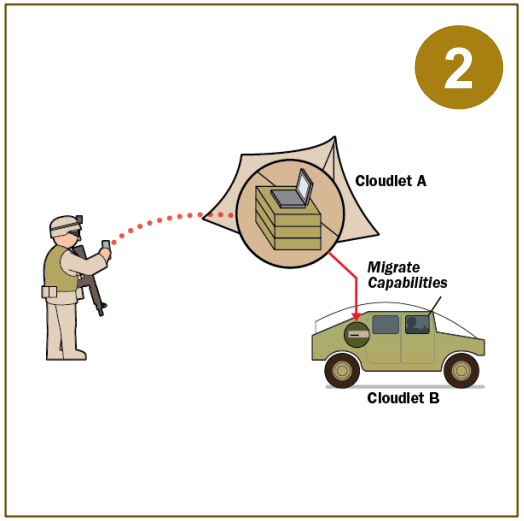
Service VM Migration involves transferring a running service VM on a source cloudlet to a target cloudlet

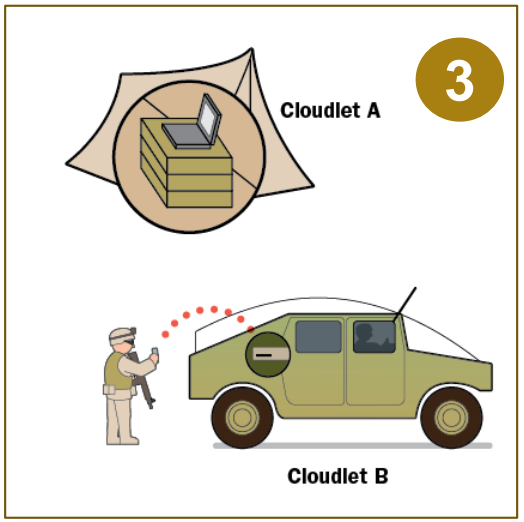
- VM migration
- Device “migration”

Challenges

- Establishing trust between cloudlets for credential exchange
- Transferring device trust from source to target cloudlet

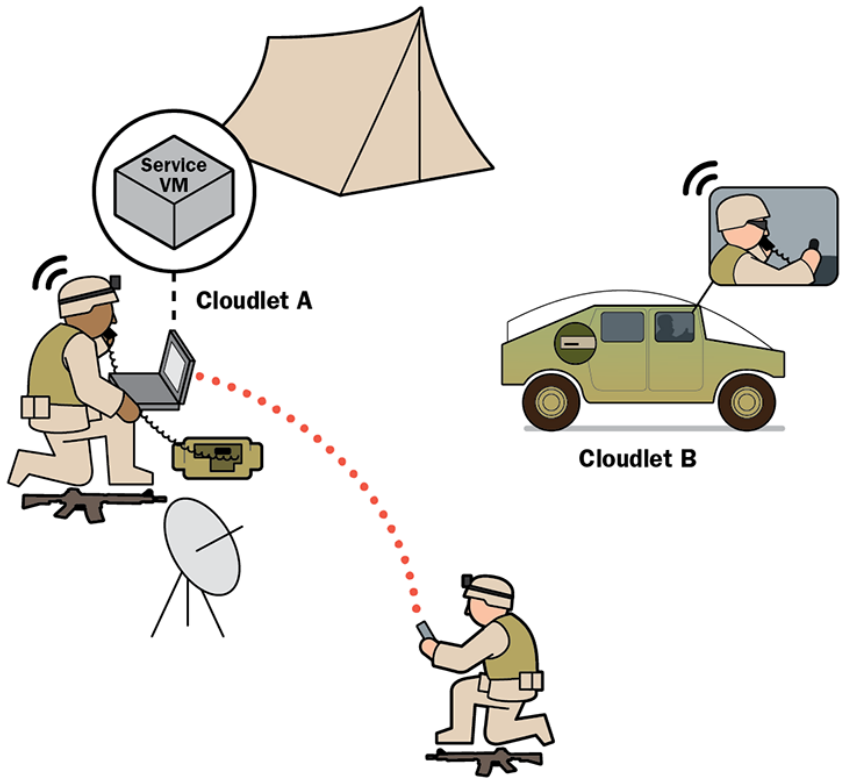






© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Secure VM Migration
Step 1: Cloudlet Pairing



Cloudlet Admins exchange temporary keys using their radios (voice)

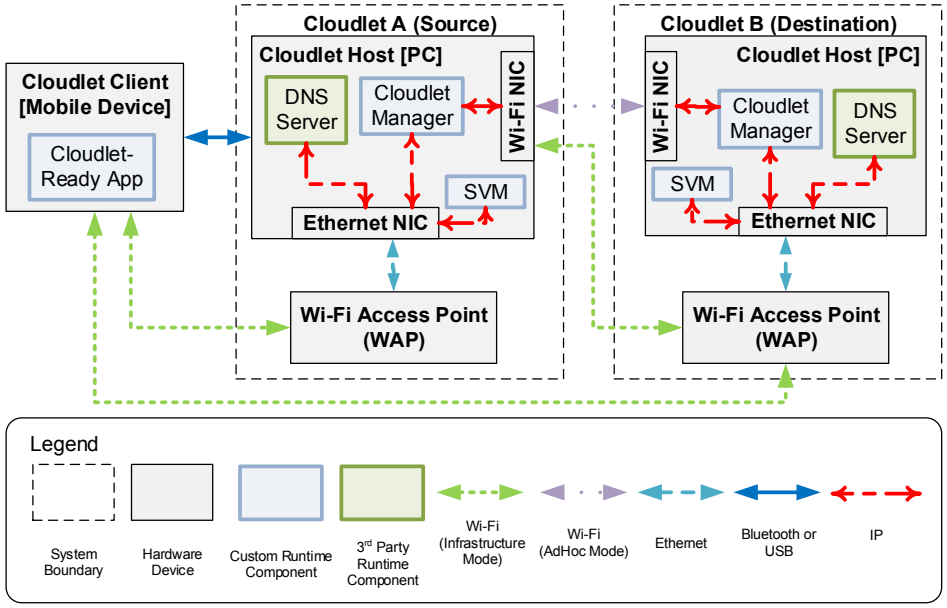
1. Cloudlet Admins exchange temporary keys over voice
2. Keys are used to setup a temporary Wi-Fi ad hoc connection between the two cloudlets
3. Cloudlet credentials are exchanged over the temporary connection
4. WiFi ad hoc connection is terminated after pairing is completed

© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Secure VM Migration
Step 2: Cloudlet Discovery and Connection

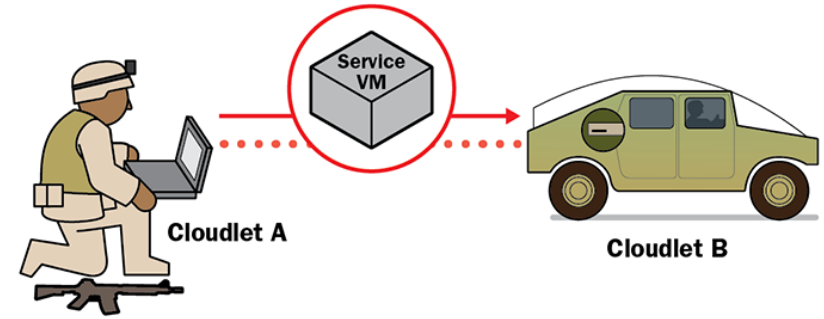
2.1. **Cloudlet Network Discovery and Connection**: Cloudlet A connects to Cloudlet Network B using information obtained during pairing

2.2. **Cloudlet Discovery and Connection**: Cloudlet A discovers the IP address and port of the Cloudlet Manager API instance running on Cloudlet B



© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Secure VM Migration
Step 3: Service VM Migration

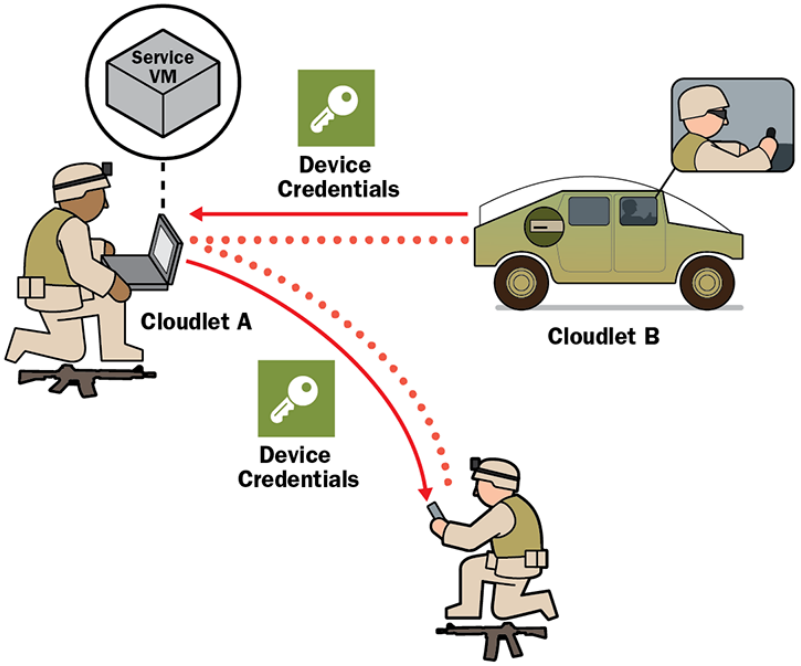


Service VM is migrated from Cloudlet A to Cloudlet B

1. Service VM Metadata is sent to Cloudlet B so that it can be added to the Service VM Repository.
2. KVM Migration feature is used to perform the actual VM migration

© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Secure VM Migration
Steps 4 and 5: New Credential Generation for Mobile Device

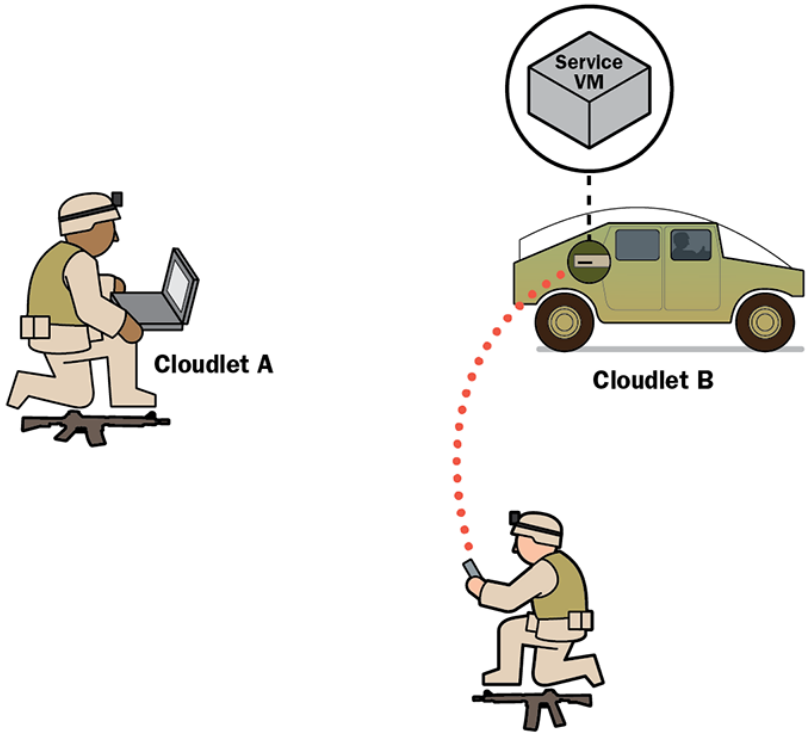


Cloudlet B generates and sends device credentials to Cloudlet A

1. Cloudlet A requests Cloudlet B to generate credentials for each of the mobile devices that are paired to Cloudlet A and are using the migrated VM
2. Cloudlet A stores new device credentials in a Message Repository
3. Each device receives message from Cloudlet A and retrieves new credentials for Cloudlet B

© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Secure VM Migration
Steps 6 and 7: Device Connection to Destination Cloudlet and Migrated Service VM



Device connects to the migrated Service VM on Cloudlet B

1. Device automatically connects to Cloudlet B Network with new credentials
2. Cloudlet-Ready App is ready to communicate with the migrated Service VM (using its FQDN – fully-qualified domain name)

© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Validation — Threat Modeling

Fully Addressed by Implementation
1: *Impersonating a Client*
2: *Finding an Active Client*
3: *Finding an Inactive Client*
7: Sniffing Wireless
14: *Impersonating a Cloudlet*
Partially Addressed by Implementation
6: Lost Credentials (usability tradeoff)
Not Addressed by Implementation
4: Altered Software
5: *Daisy Chaining (device-device-cloudlet)*

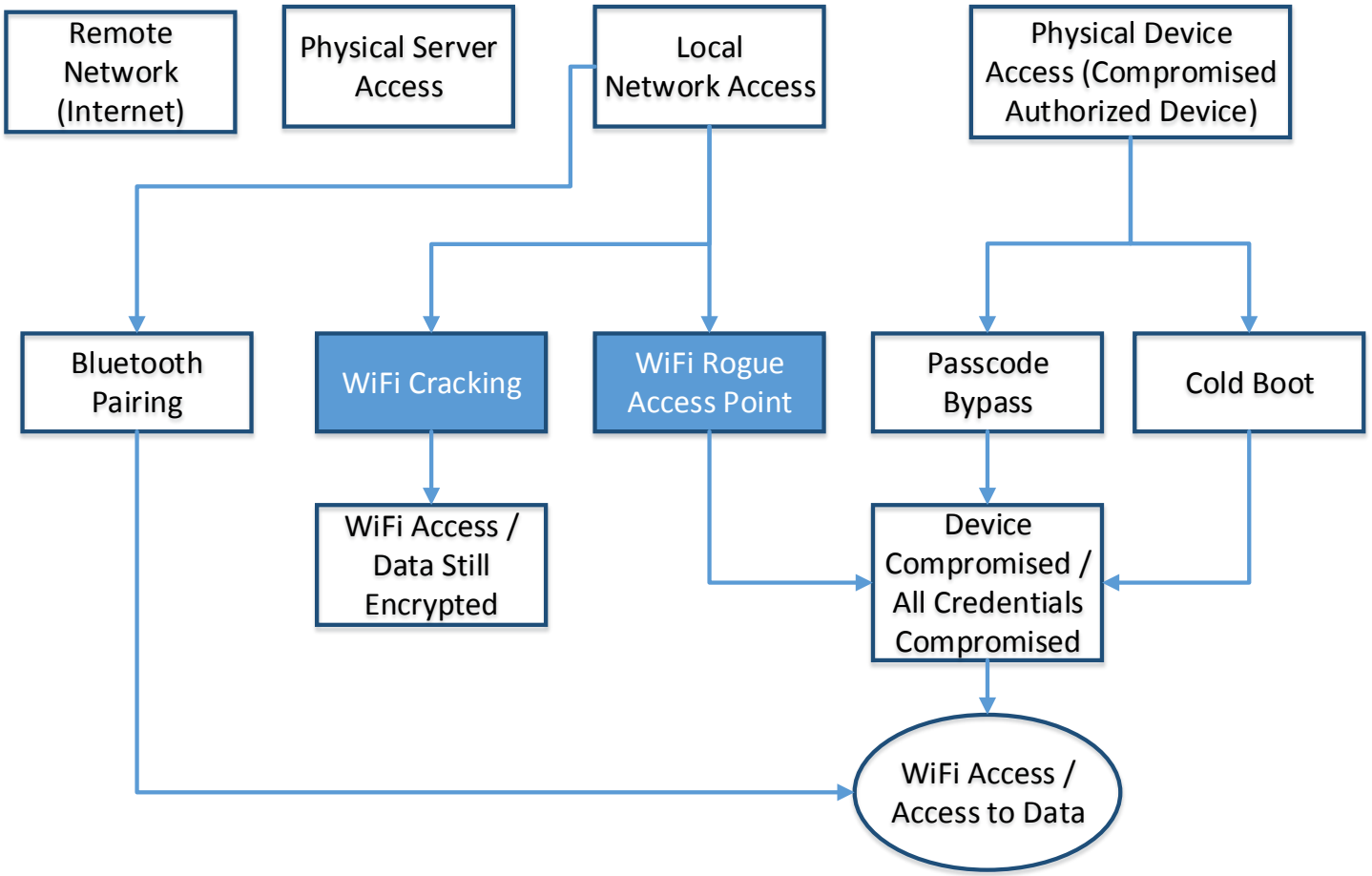
Addressed Outside the Implementation
8: Site Intrusion
9: On the Net (WAP)
10: On the Box
11: Super-User Compromise
12: Application Compromise
13: Seeing Everything
15: On the Net (NIC)
16: Daisy Chaining (device-device-cloudlet)

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

© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Validation — Vulnerability Analysis

Architectural and technical analysis of possible vulnerabilities using a simple attack tree based on the threat model



© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Validation — Ceremony Analysis

Ceremonies include all protocols, applications with a user interface, and security provisioning workflows — nothing is out of band

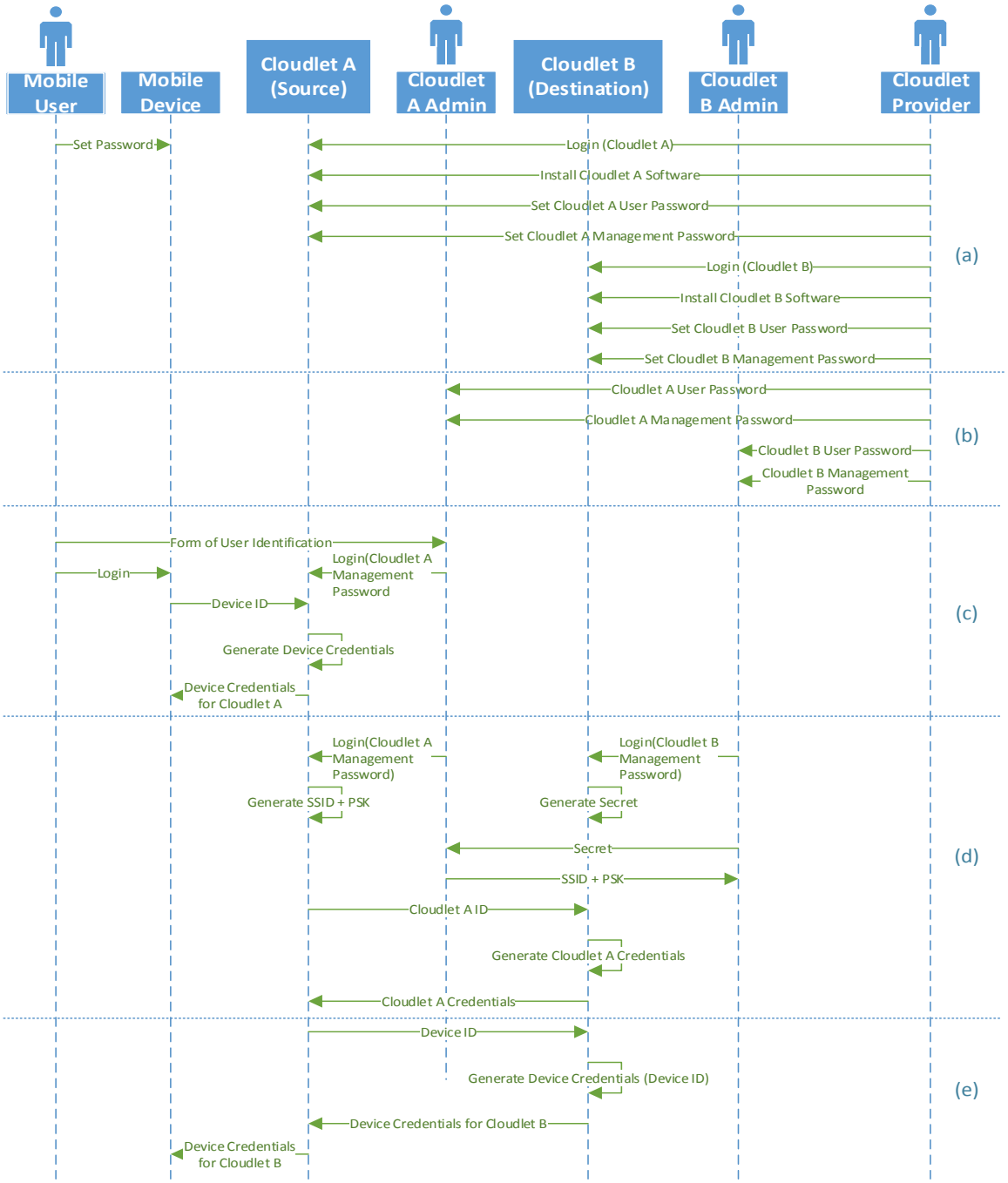
a) Cloudlet Setup

b) Cloudlet Delivery

c) Device Credential Generation (for pairing with Cloudlet A)

d) Cloudlet Credential Exchange

e) Device Credential Generation (for pairing with Cloudlet B)



© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Summary and Conclusions

Presented a solution for secure VM migration in tactical cloudlets that combines Identity-Based Encryption (IBE) with mechanisms for Secure Key Exchange without a Trusted Third Party.

Evaluation of the implementation was done against the threat model and using vulnerability and ceremony analysis

- 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

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.

© 2017 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution

Contact Information

Principal Investigator

Grace A. Lewis

Principal Researcher (SSD/TTG)

Telephone: +1 412.268.5851

Email: glewis@sei.cmu.edu

WWW: http://www.sei.cmu.edu/staff/glewis/

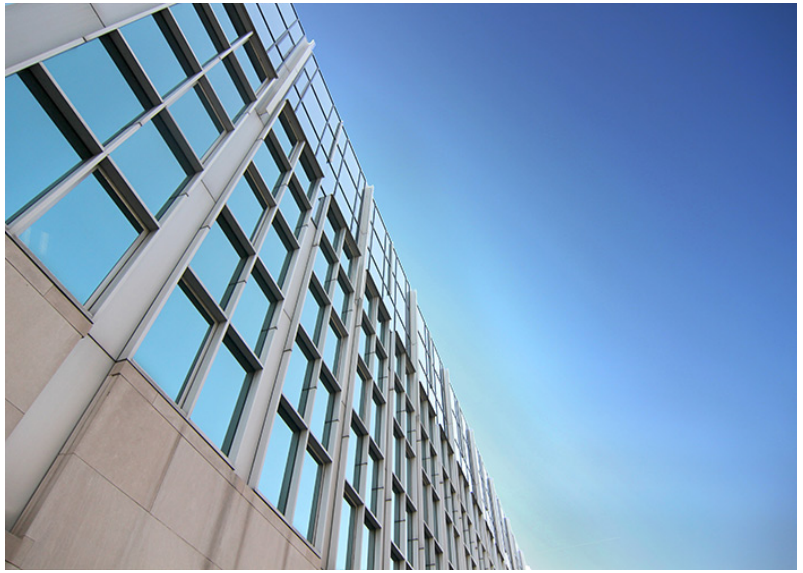
Current Team

Sebastían Echeverría (SSD/TTG)

Chris Grabowski (SSD/TTG)

Dan Klinedinst (CERT/VUL)

Keegan Williams (SSD/TTG)



Tactical Cloudlets software available on GitHub as KD-Cloudlet

https://github.com/SEI-AMS/pycloud

© 2017 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution