Software Solutions Symposium 2017

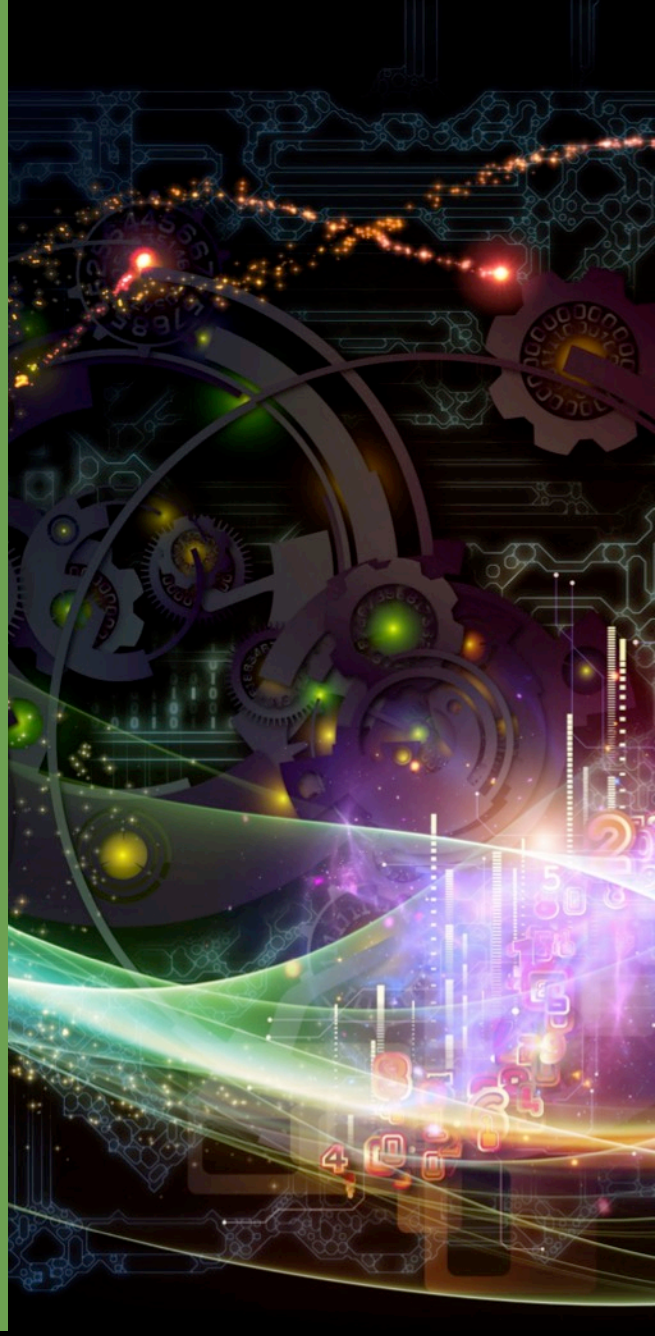
March 20–23, 2017

Secure Tactical Cloudlets for Mission Support at the Edge

Grace Lewis

glewis@sei.cmu.edu

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



© 2017 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Copyright 2017 Carnegie Mellon University. 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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* 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 external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

DM17-0032

Motivation

Soldiers, first responders and field personnel operating in tactical environments increasingly make use of mobile systems for mission support

However, dynamic context, limited computing resources, disconnected-intermittent-limited (DIL), network connectivity, and high levels of stress pose a challenge for mobile systems in tactical environments

© 2017 Carnegie Mellon University

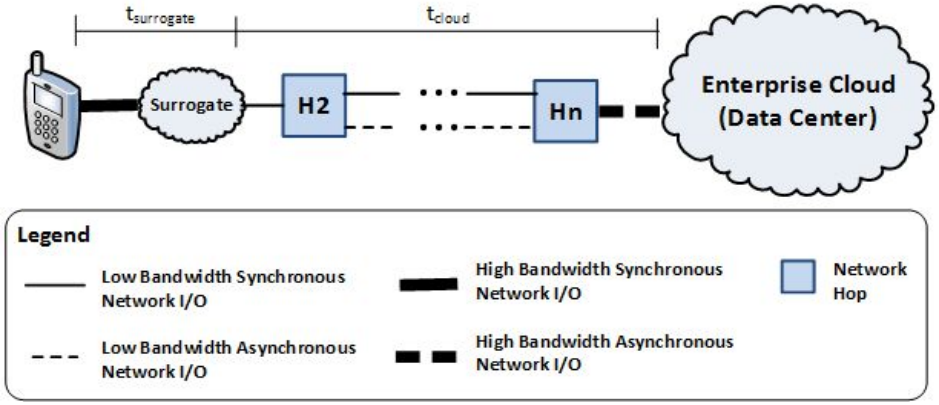
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Cyber-Foraging

Cyber-foraging* is the leverage of external resource-rich surrogates to augment the capabilities of resource-limited devices

Two main forms of cyber-foraging

- Computation Offload
  - Offload of expensive computation in order to extend battery life and increase computational capability
- Data Staging
  - Improve data transfers between mobile computers and the cloud by temporarily staging data in transit on surrogates



* Satyanarayanan, Mahadev (2001). "Pervasive Computing: Vision and Challenges". IEEE Personal Communications (IEEE)

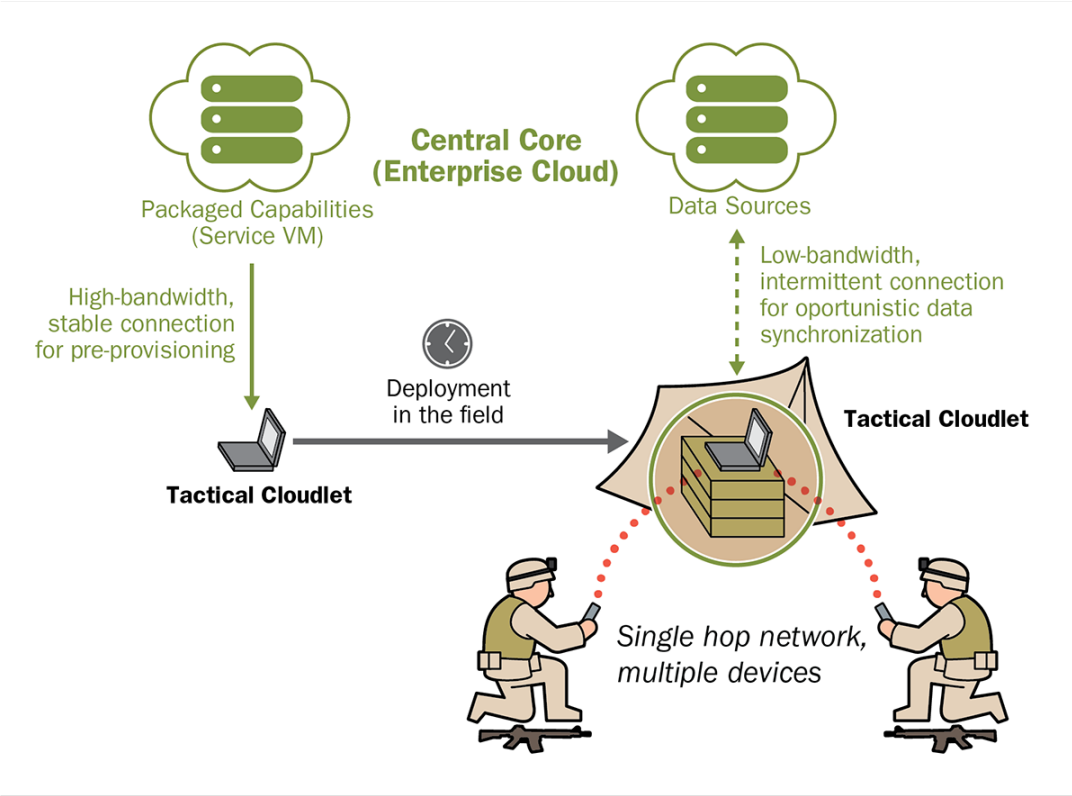
© 2017 Carnegie Mellon University

[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Tactical Cloudlets

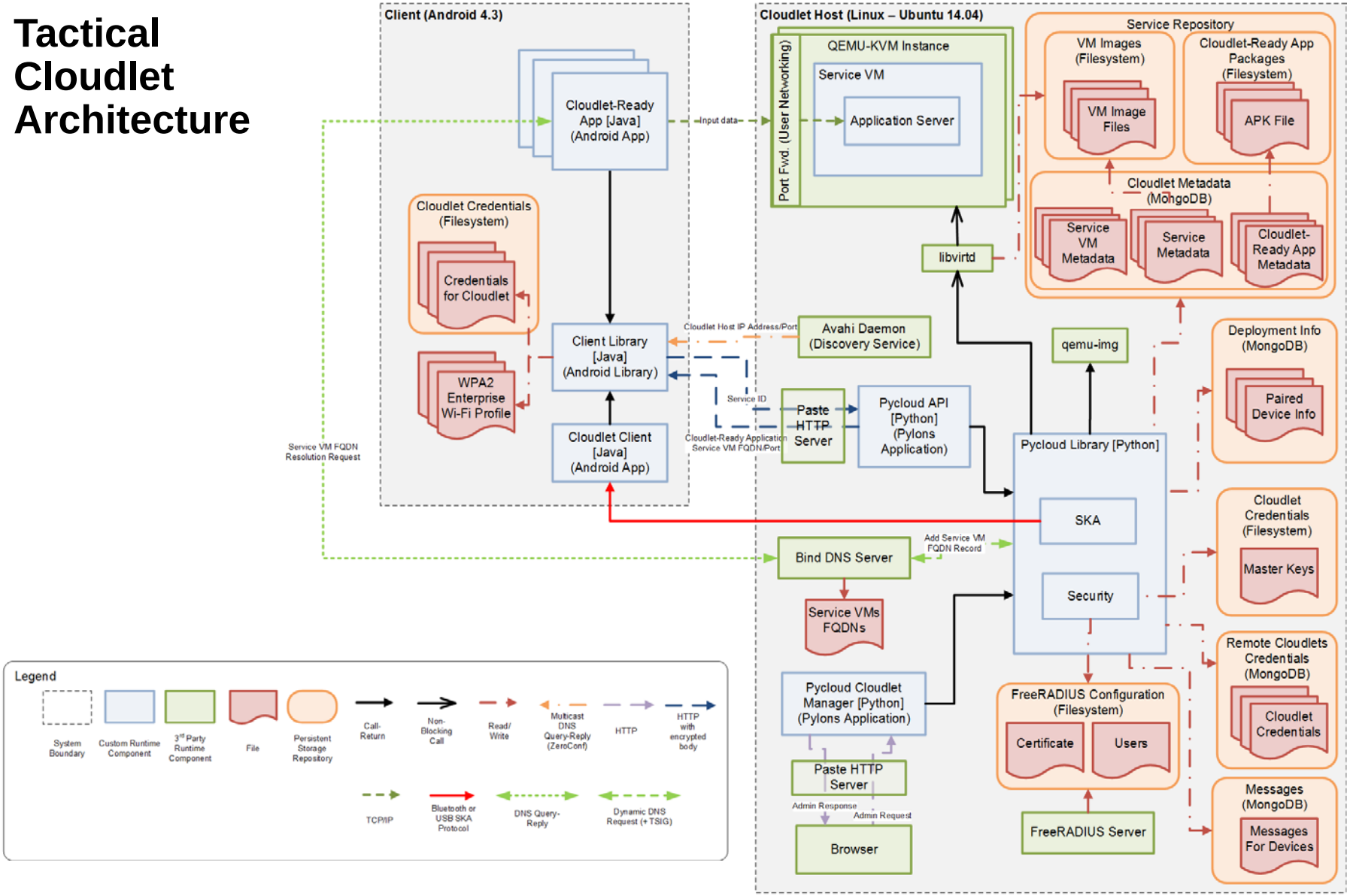
Forward-deployed, **discoverable**, virtual machine (VM) based com nodes that can be hosted on vehicles or other platforms to provide

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



© 2017 Carnegie Mellon University
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Tactical Cloudlet Architecture



© 2017 Carnegie Mellon University

[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Tactical Cloudlets Features

Edge Characteristics / Capabilities/Features	Intermittent cloudlet-enterprise connectivity	Mobility	Limited battery power	Dynamic missions	Limited technical skills in the field	Potentially hostile environments
System Requirements	*Disconnected operations*	*Quick response time*	*Low energy consumption*	*Ease of re-deployment*	*Ease of deployment*	*Trusted identities*
Pre-Provisioned Cloudlets with App Store	X	X	X	X	X	
Standard Packaging of Service VMs				X	X	
Optimal Cloudlet Selection	X	X				
Cloudlet Management Component				X	X	
Cloudlet Handoff/Migration		X		X		X
Secure Key Generation and Exchange	X					X

© 2017 Carnegie Mellon University

[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Pre-Provisioned Cloudlets with App Store

Applications statically partitioned into a client and server

- Very thin client runs on mobile device (App)
- Computation-intensive server runs on cloudlet (Service VM)

Capabilities as services

- Service VM provides a self-contained capability and exposes a simple interface

Virtual machines as service containers

- VMs can be started and stopped as needed based on number of active users therefore providing scalability and elasticity
- Also enables legacy system reuse

Request-Response interactions between clients and cloudlets

- Enables easy detection of failed communication between mobile devices and cloudlets
- Also minimal effect on mobile devices if computation needs to be restarted or migrated

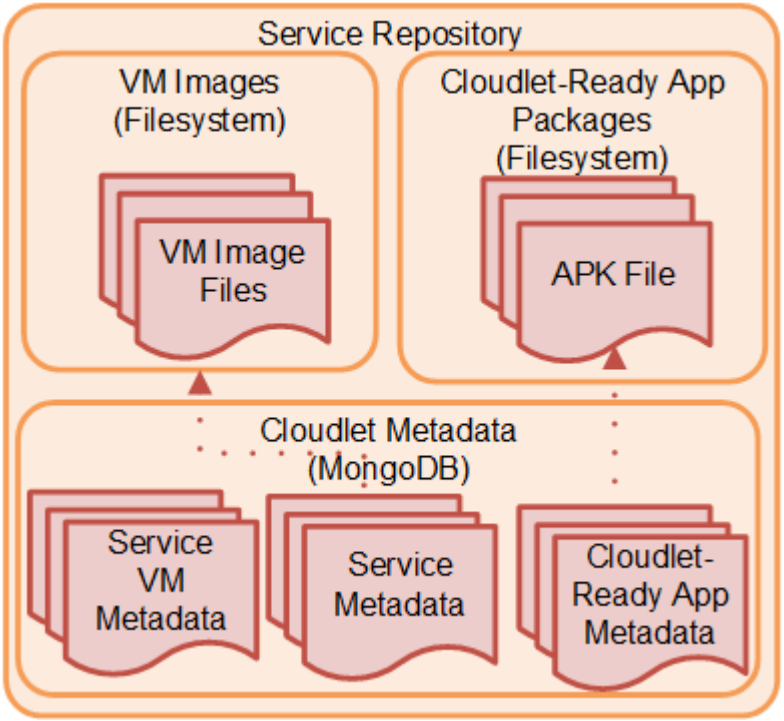
© 2017 Carnegie Mellon University

[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Standard Packaging of Service VMs

Standard format for Service VMs (.csvm) so these can be easily loaded from the cloudlet disk drive, an enterprise Service VM repository, a thumb drive, or a mobile device connected via USB or Bluetooth to the cloudlet

- Service metadata (JSON file): service ID, port, version, description, tags, shared/non-shared, minimum memory, ideal memory
- VM image files — one for the disk image and one for the state/memory image that contain a suspended Service VM



© 2017 Carnegie Mellon University
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

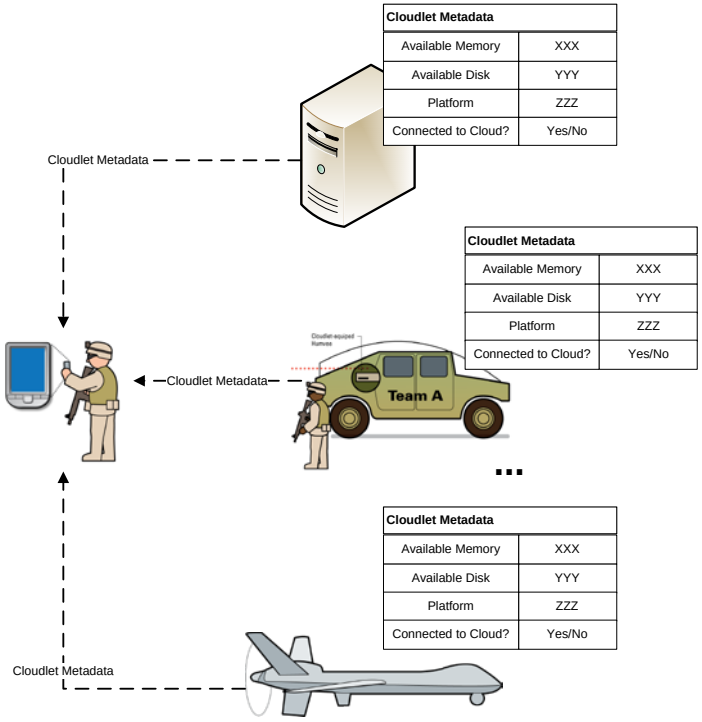
Optimal Cloudlet Selection

Useful when there is more than one cloudlet available

Architecture enables different algorithms to be plugged in

Implemented three algorithms

- CPU-Based Ranker: Selects the less loaded cloudlet based on CPU utilization
- CPU Performance Ranker: Also takes into consideration CPU speed
- Memory Performance Ranker: Takes into consideration free memory and CPU cache

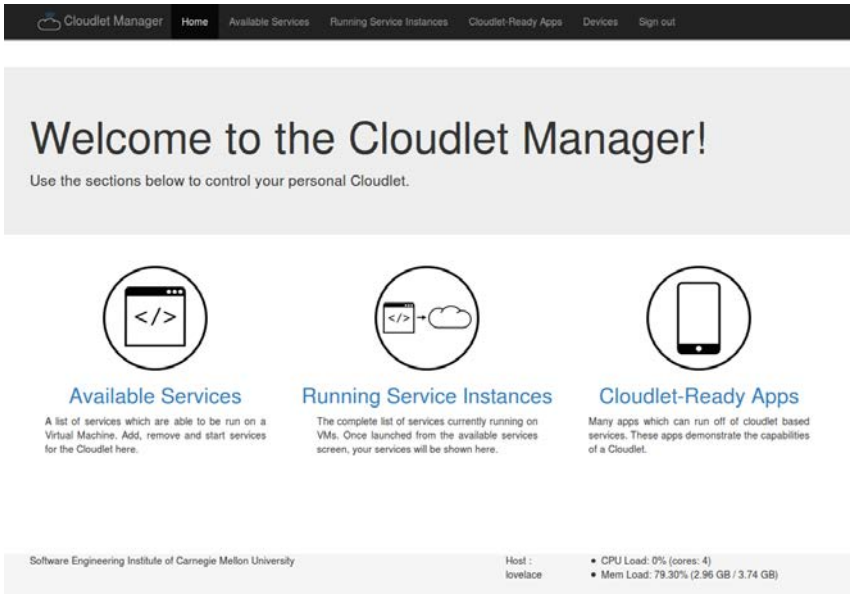


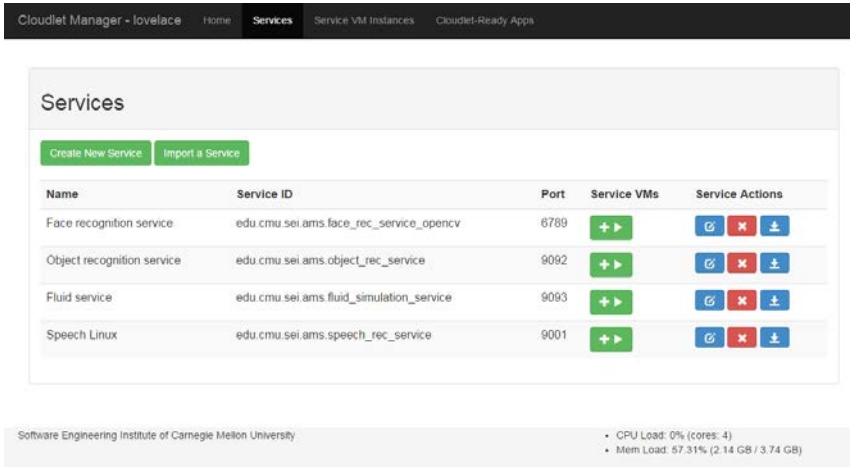
© 2017 Carnegie Mellon University
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Cloudlet Management Component

Lightweight, web-based interface that enables easy deployment and redeployment of capabilities

- Service VM creation, edit and deletion
- Service VM import and export
- Service VM Instance start, stop and migration
- Cloudlet-Ready App repository (i.e., app store)
- Credential management



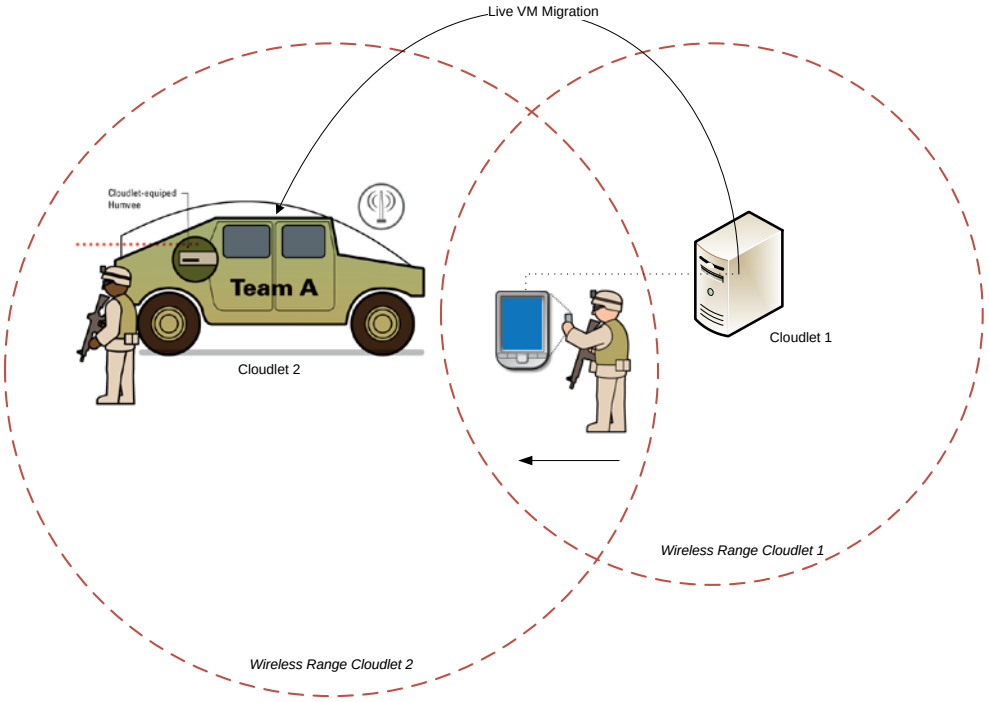


© 2017 Carnegie Mellon University
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Cloudlet Handoff/Migration

Manual handoff enables scenarios in which a user is migrating capabilities from a fixed cloudlet to a mobile cloudlet to support field operations, as well as reintegration back to the fixed cloudlet

Desire is to support automatic migration based on for example signal strength, load balancing or a more powerful surrogate in proximity



© 2017 Carnegie Mellon University
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Secure Key Generation and Exchange

Motivation

- Common solution for establishing trust is to create and share credentials in advance, and then use an online trusted authority for validation
- However, characteristics of tactical environments do not consistently provide access to a credential repository or online authority

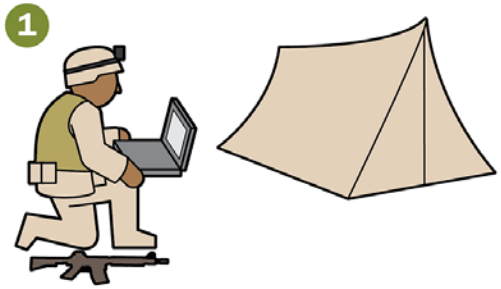
Solution Requirements

- Cannot require network connectivity to a third party for credential generation or validation
- Cannot place any specific security requirements on hardware
- Cannot require pre-provisioning of credentials on the mobile devices
- Must address the threats of a tactical environment

© 2017 Carnegie Mellon University

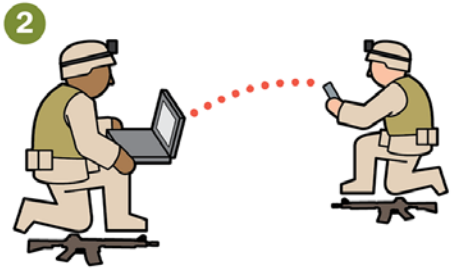
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Secure Communications



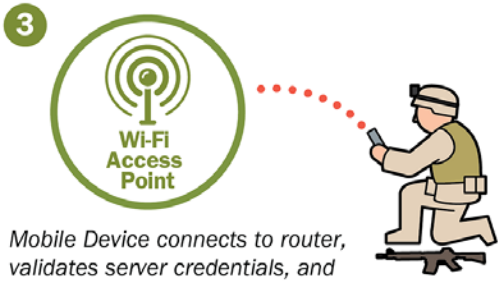
Admin logs into the Cloudlet Manager to start the Bootstrapping process

Bootstrapping
- Generation of *Cloudlet Credentials* using IBE (Identity-Based Encryption)
- Setup of *RADIUS Server* with *Cloudlet Credentials*



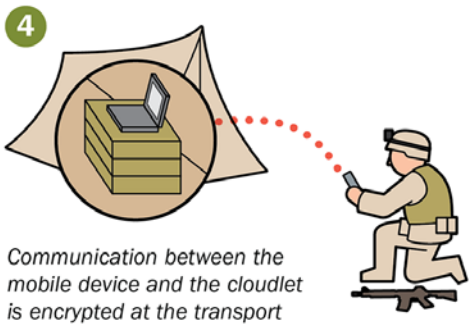
User connects mobile device to the cloudlet, and upon visual confirmation the admin starts the pairing process

Pairing
- Generation of *Device Credentials* using IBE
- Transfer to device using Bluetooth or USB, plus visual confirmation
- Transfer to *RADIUS Server*



Mobile Device connects to router, validates server credentials, and authenticates with RADIUS server

Wi-Fi Authentication *RADIUS Server* implements Wi-Fi WPA2-Enterprise 802.1X EAP-TTLS with PAP
- Device receives cloudlet credentials and validates
- Devices sends its credentials for validation



Communication between the mobile device and the cloudlet is encrypted at the transport and message level

API Requests
- Device exchanges encrypted messages with the cloudlet
- Each exchange is validated against authorized device list

Device Credential Revocation
- Automatic due to timeout: Bootstrapping requires setting up mission duration
- Manual due to known loss or compromise: Cloudlet Manager component has revocation option

© 2017 Carnegie Mellon University
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Secure Communications – Validation

Threat modeling

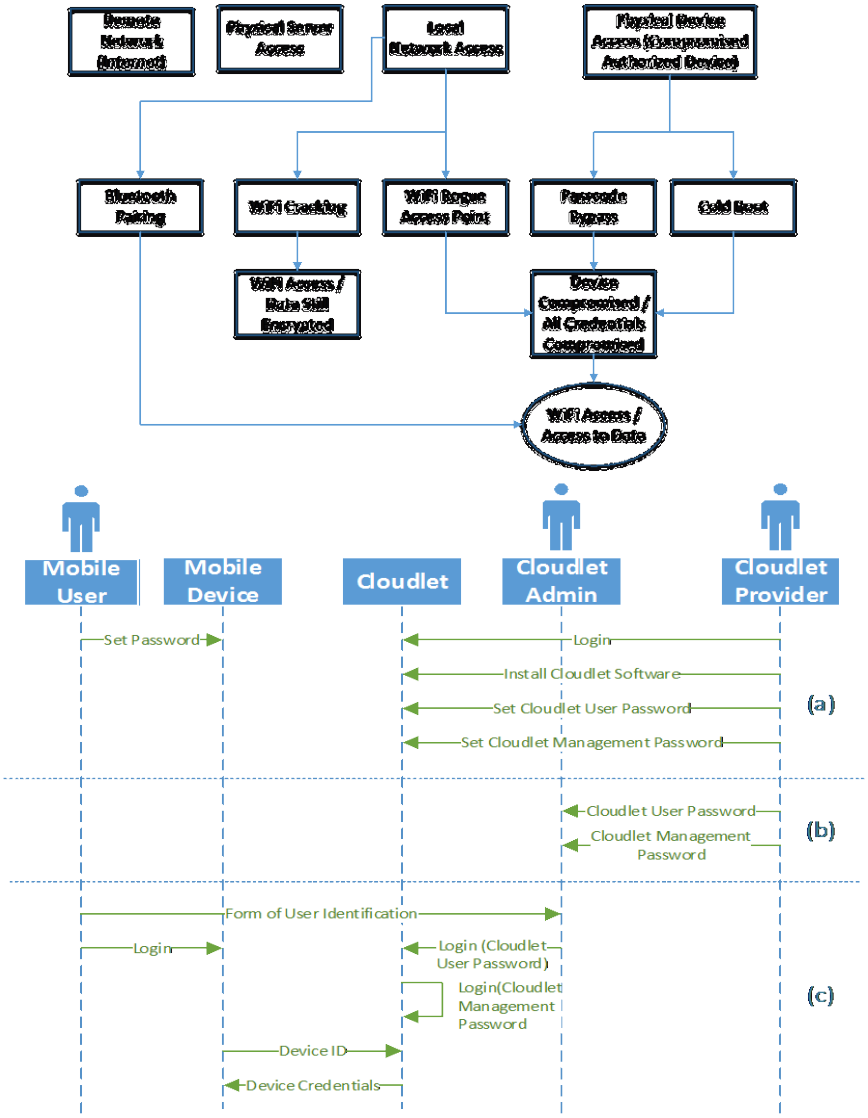
- Identified and prioritized 14 threats
- Solution addresses 12 threats (directly or indirectly)

Vulnerability analysis

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

Ceremony analysis

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



© 2017 Carnegie Mellon University
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

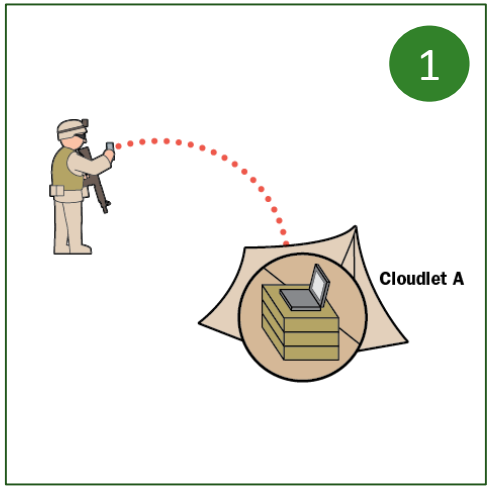
Secure Service VM Migration 1

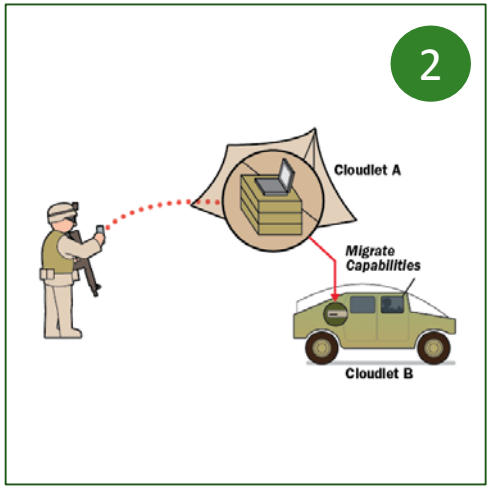
Service VM Migration involves transferring a running service VM on a source cloudlet to a target cloudlet

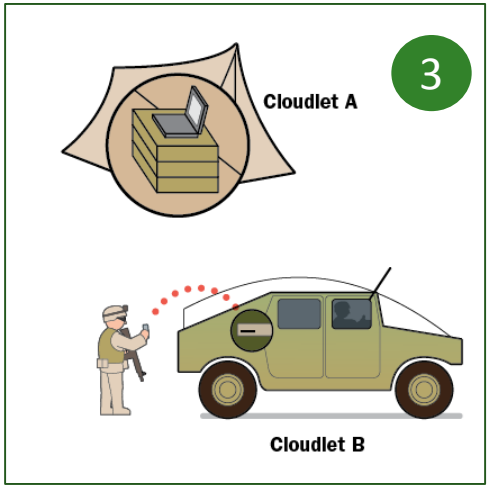
- VM migration
- Device "migration"

Challenges

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

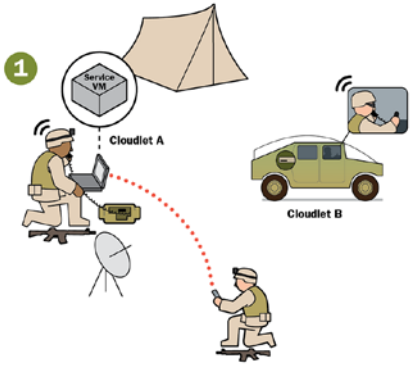






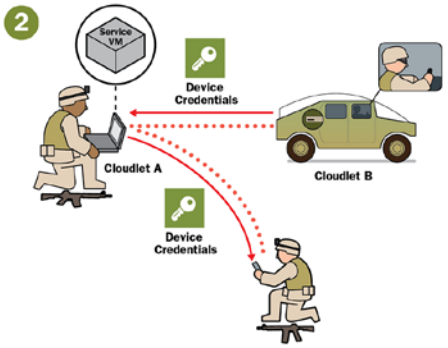
© 2017 Carnegie Mellon University
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Secure Service VM Migration 2



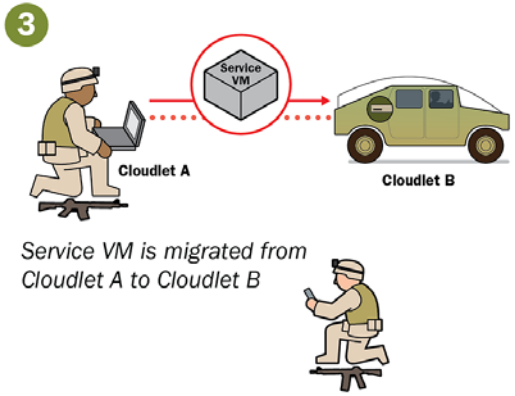
Cloudlet Admins exchange temporary keys using their radios

Cloudlet Pairing
- Cloudlet Admins exchange temporary keys over voice
- Keys are used to setup a temporary channel
- Cloudlet credentials are exchanged over the temporary channel



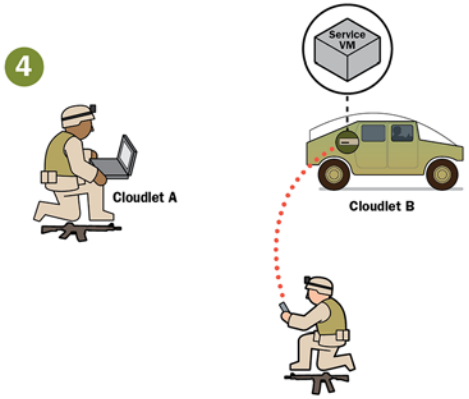
Cloudlet B generates and sends device credentials to Cloudlet A

Device Credential Generation
- Cloudlet A discovers and connects to Cloudlet B using exchanged credentials
- Cloudlet B generates new credentials for Device
- Cloudlet B sends credentials to Device via Cloudlet A



Service VM is migrated from Cloudlet A to Cloudlet B

Service VM Migration
- Cloudlet A migrates Service VM to Cloudlet B



Device connects to the migrated Service VM on Cloudlet B

Device Connection
- Device connects to Cloudlet B using new credentials
- Client App on Device connects to Service VM running on Cloudlet B

© 2017 Carnegie Mellon University
[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Future Challenges

Establishing Trust at the Edge

- Reduced human involvement
- Use of passive out-of-band channels
- Inclusion of IoT (sensors)

Cloudlets in Content-Delivery Networks

- Adaptation of applications and infrastructure to delay-tolerant networks and protocols
- Smarter decision making at the network layer for when, where, to whom, and how to deliver information

© 2017 Carnegie Mellon University

[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Summary

Tactical Cloudlets are forward-deployed, discoverable, virtual-machine-based computing nodes that provide secure computation offload and data staging capabilities for mobile devices in the field

We advocate the effectiveness of combined threat modeling, vulnerability analysis and ceremony analysis to develop end-to-end secure software systems

© 2017 Carnegie Mellon University

[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

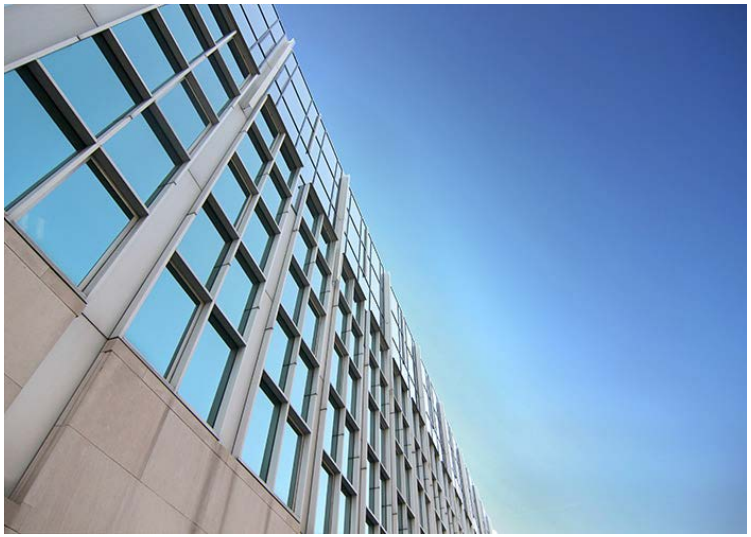
Contact Information

Principal Investigator

Grace A. Lewis
Principal Researcher (SSD/AMS)
Telephone: +1 412.268.5851
Email: glewis@sei.cmu.edu
WWW: http://www.sei.cmu.edu/staff/glewis/

Team

Jeff Boleng (SSD/AMS)
Sebastían Echeverría (SSD/AMS)
Dan Klinedinst (CERT/VUL)
Marc Novakouski (SSD/AMS)
Keegan Williams (SSD/AMS)



Tactical Cloudlets software available on GitHub as KD-Cloudlet

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

© 2017 Carnegie Mellon University

[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Software Solutions Symposium 2017

© 2017 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.