Evaluation of Security Risks Using Mission Threads

Carol Woody, Ph.D.

December 12, 2013

Focus Problem

One third of the 940 common weakness enumerations (CWEs) are design weaknesses (http://cwe.mitre.org/)

11 of the top 25 are design weaknesses(http://cwe.mitre.org/top25/)

How do we analyze operational security risks early in the software life cycle to address security risks in

- Requirements
- Architecture
- Design

Design Weakness: Unanticipated Response

Threat

If a malicious attacker gains control of an UAV

Consequence

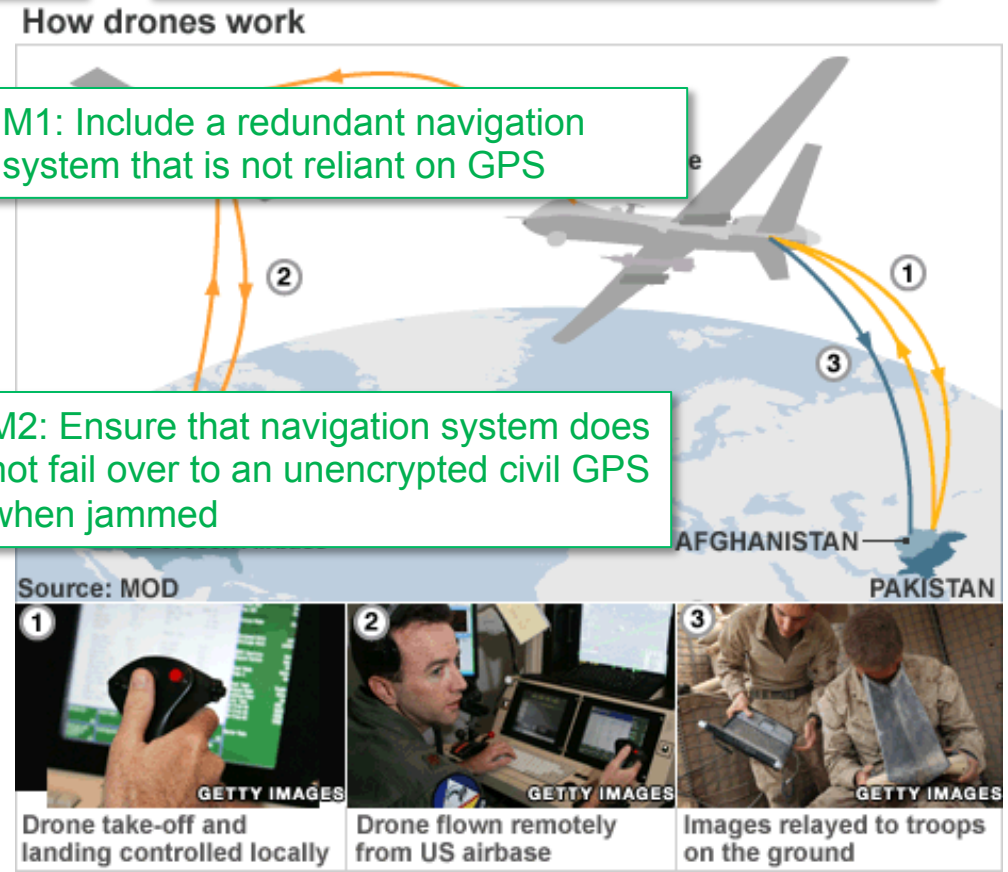
Then the UAV could be used to attack US forces

Attack Steps

1. Encrypted GPS signal is jammed.
2. Navigation system fails over to an unencrypted civil GPS.
3. Authentic GPS signal is overpowered.
4. UAV is under the control of a malicious attacker.

M1: Include a redundant navigation system that is not reliant on GPS

M2: Ensure that navigation system does not fail over to an unencrypted civil GPS when jammed



Possible GPS Spoofing of a UAV ***(see slide 21 for references)***

Security Engineering Risk Analysis (SERA)

Goal:

- To identify and address design weaknesses that impact security early in the life cycle (i.e., build security in)

Approach:

Project the operational context for security analysis

- Integration of a functional and security perspective
- Systems do not exist in isolation
- Threats do not occur in isolation
- Design weaknesses provide opportunities for mission failure

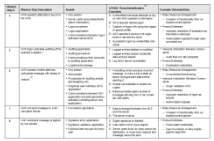
Employ structured, systematic risk analysis to handle the complex nature of security risk

SERA Method

Our Focus

1. Establish operational context.
2. Identify risk.
3. Analyze risk.
4. Determine control approach.
5. Develop control plan.

Mission Thread Worksheet

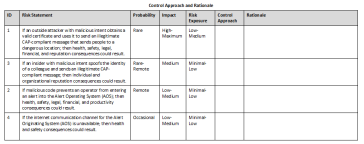


Risk Identification Worksheet

Risk Evaluation Criteria

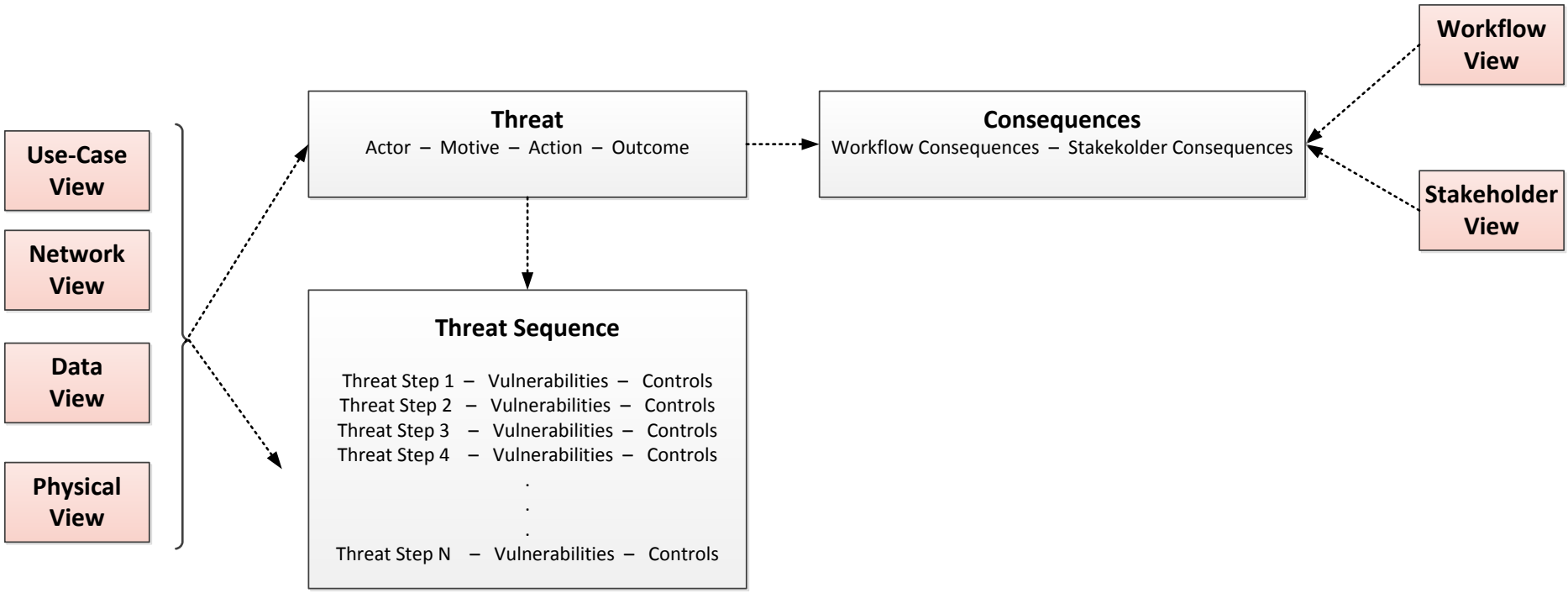
Risk Analysis Worksheet

Control Approach Worksheet



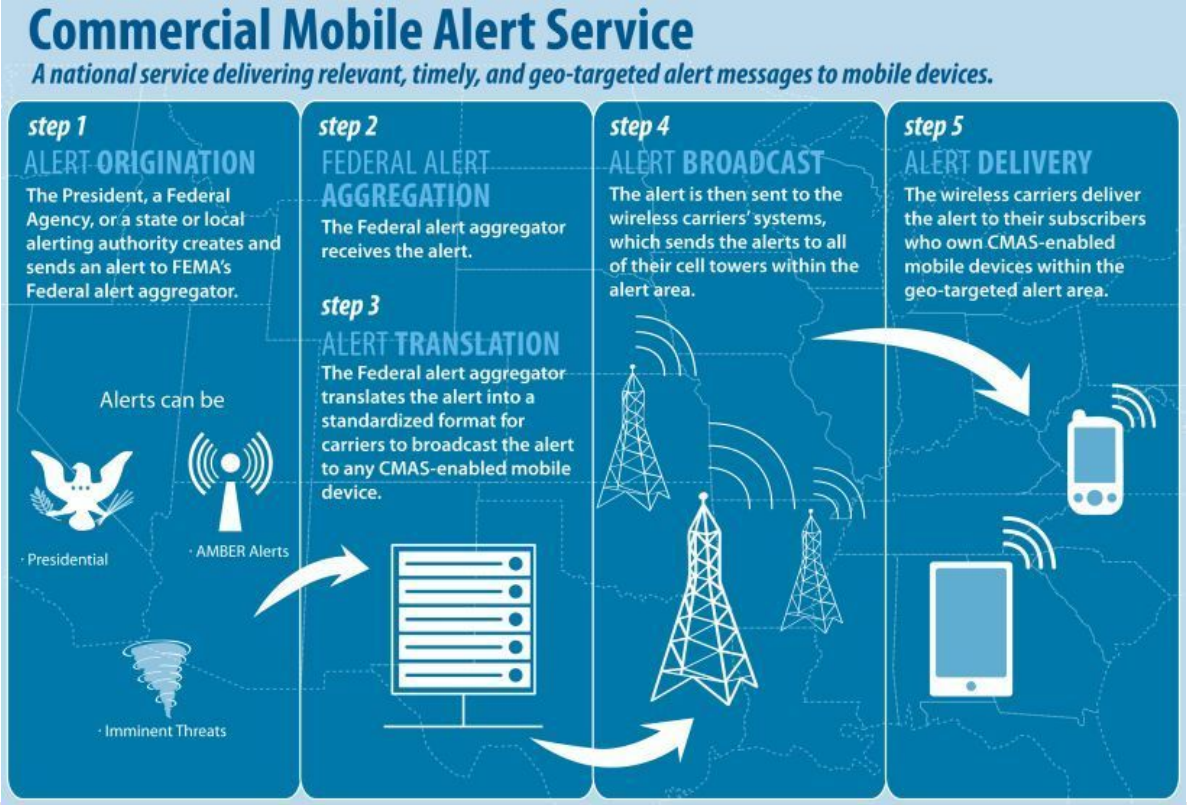
Control Plan Worksheet

Security Event Model

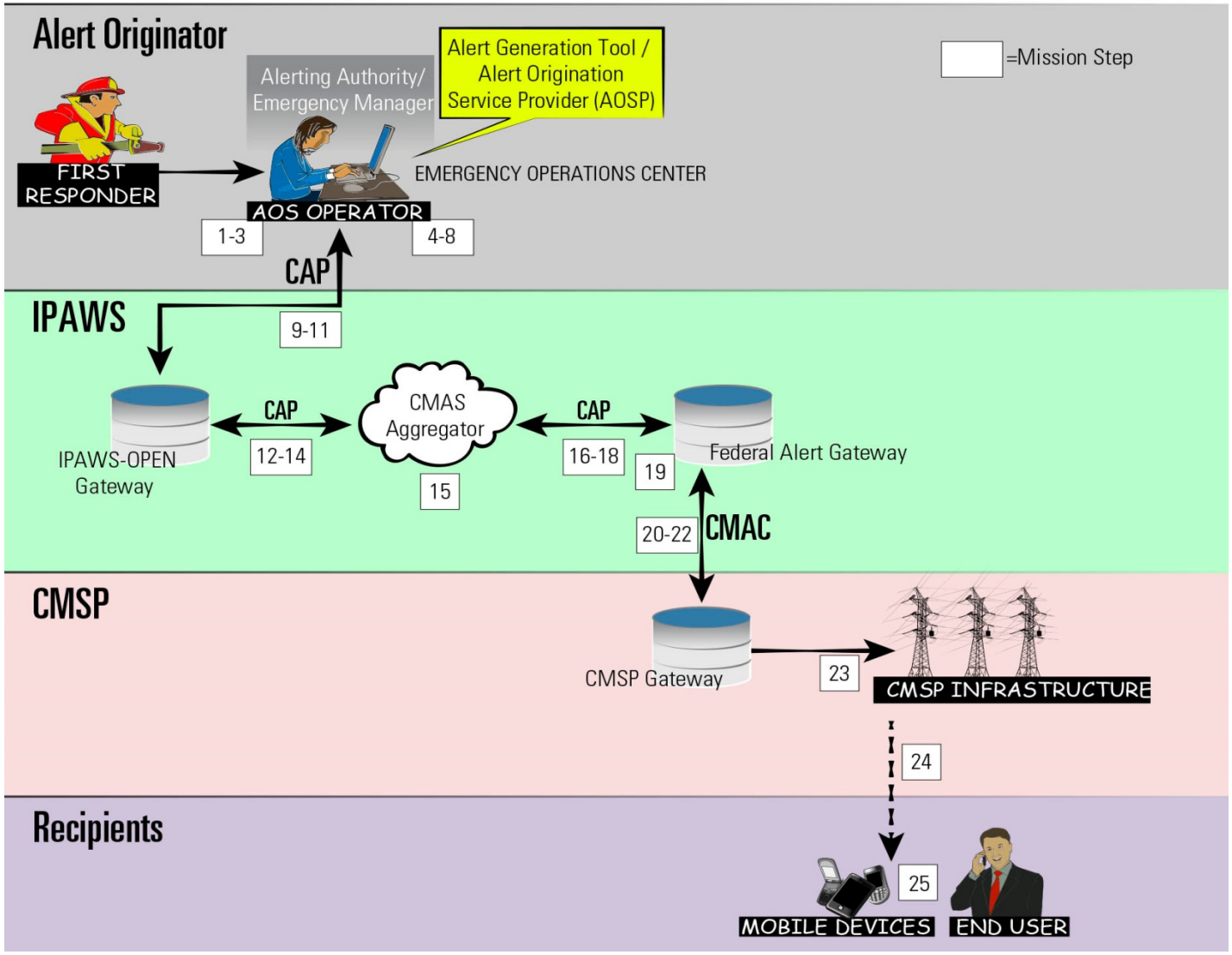


Example: *Commercial Mobile Alert Service (CMAS)*

New component of the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS); Enables federal, state, territorial, tribal, and local government officials to send targeted text alerts to the public via commercial mobile service providers (CMSPs) to all phones in the target area



Example: *Swimlane Diagram for the CMAS Service*



Example: *Mission Thread -1*

Step	Supporting Technologies
Alert Originating System (AOS) operator attempts to log on to the AOS.	• Server (valid accounts/authentication information) • Logon application • Communications between logon software/ server/AOS
AOS logon activates auditing of the operator's session.	• Auditing application • Communications from accounts to auditing application • Local/remote storage devices
AOS operator enters alert/cancel/update message with status of "actual."	• Alert scripts • Graphical user interface (GUI) application • Communications between GUI application and alert-generation software (including server and application)
AOS converts message to Common Alerting Protocol (CAP) compliant format.	• Conversion application

Example: *Mission Thread -2*

Step	Supporting Technologies
CAP-compliant message is signed by two people.	• Signature entry application • Signature validation application • Public/private key pair for every user
AOS transmits message to the IPAWS OPEN Gateway.	• Application that securely connects to IPAWS • AOS and IPAWS

Identifying Threats using STRIDE

Threat modeling tool used by Microsoft to help non-security experts consider security issues

Threat	Property we want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

http://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx

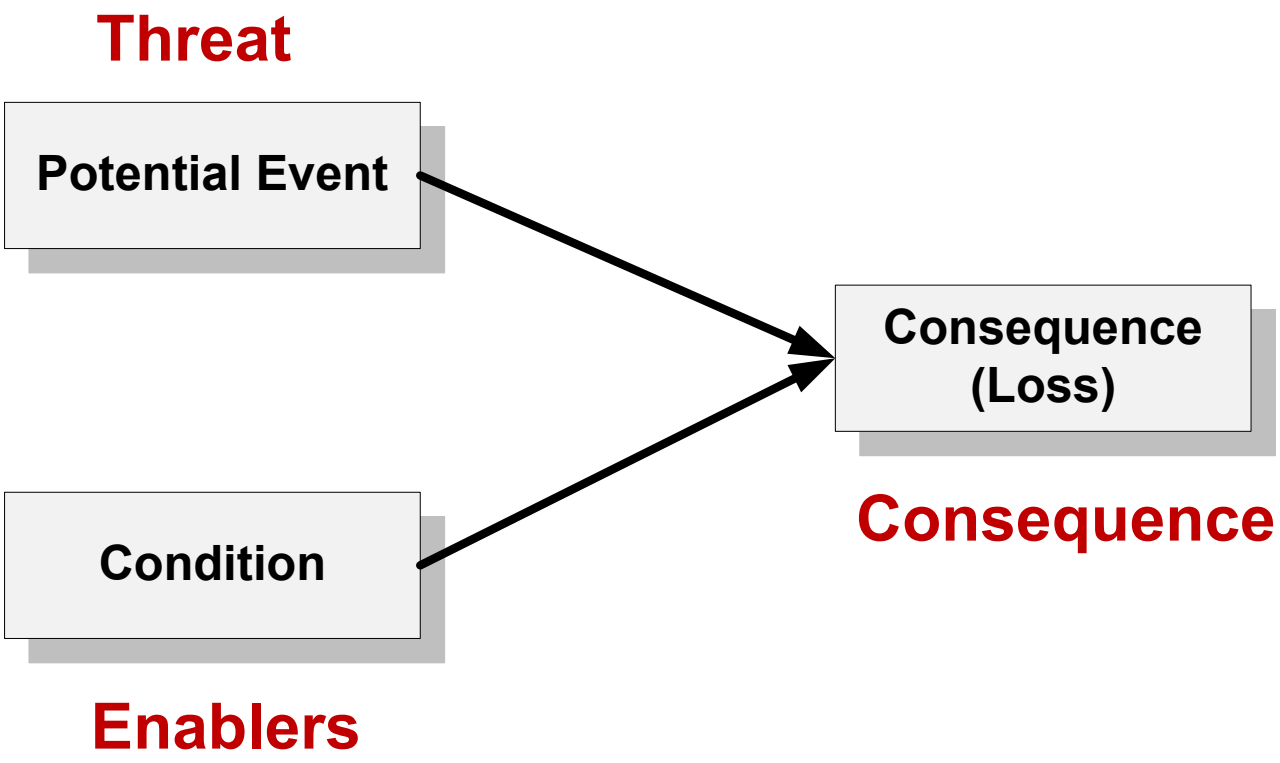
Example: Security Analysis of Mission Step

Step 1

Step #	Step	Assets	STRIDE Threat Identification Examples
1.	AOSP operator attempts to log on to the alert origination system.	– One person – Server (valid accounts/ authentication information) – Logon procedure – Logon application – Username/ password data in database – Communications between logon software/ server/ AOSP	S: Unidentified individual attempts to logon with AOSP operator's information T: (none identified) R: AOSP operator denies having logged on I: Capture of logon info using key logger or packet sniffer D: AOSP operator's account not registered / servers are down E: Successful log on by an unidentified and unauthorized individual

[1] S: Spoofing; T: Tampering with data; R: Repudiation; I: Information disclosure; D: Denial of service; E: Elevation of privilege.

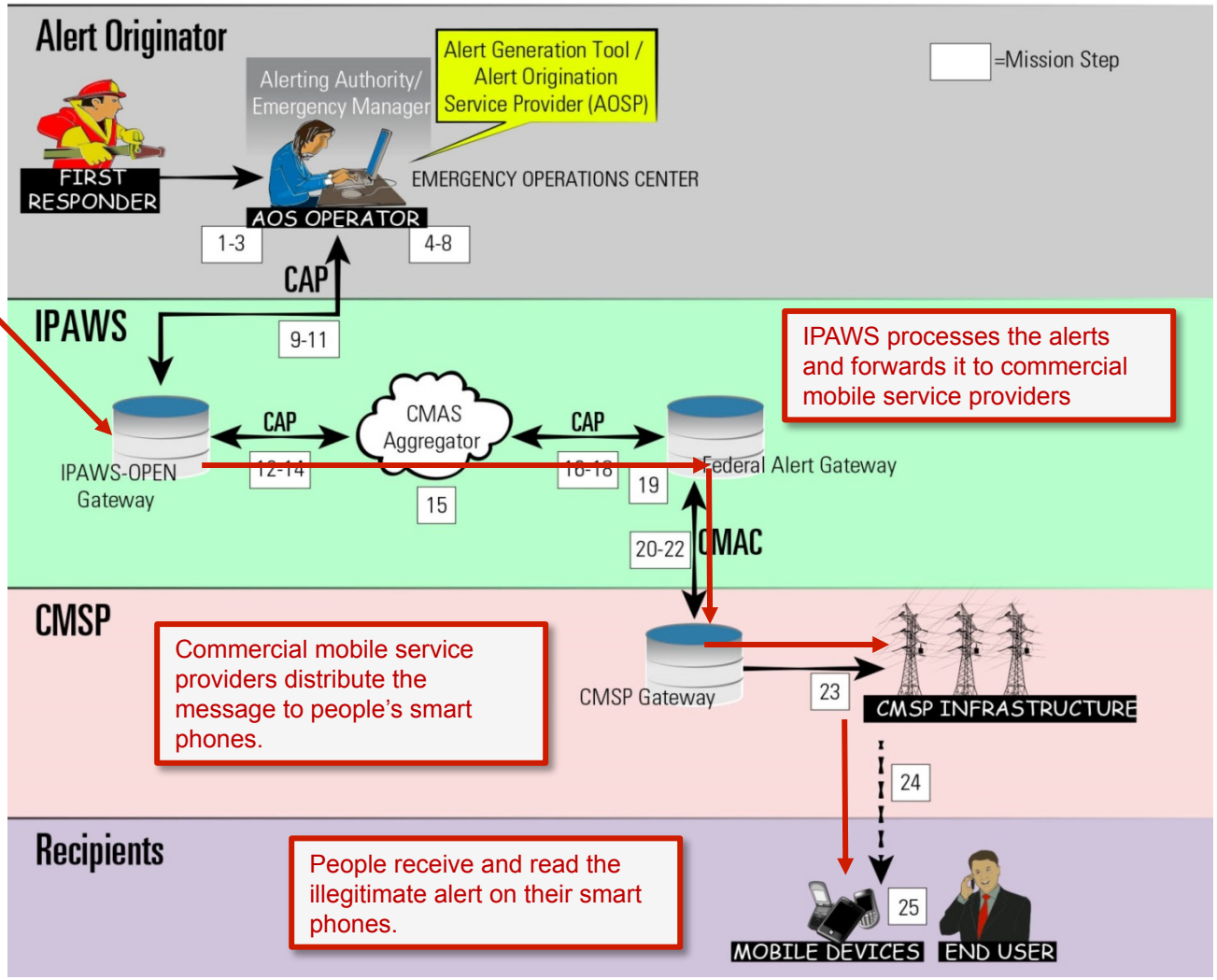
Security Risk Components



Example: *Workflow Consequences*

Threat

An outside attacker with malicious intent gets a WEA certificate through social engineering and sends a WEA alert intended to incite panic in a crowd.



Example: *Enablers*

A valid certificate could be captured by an attacker.

- Certificates are sent to recipients in encrypted email. This email is replicated in many locations, including
  - Computers of recipients
  - Email servers
  - Email server/recipient computer back-ups
  - Off-site storage of backup tapes
- The attacker could compromise the Emergency Operations Center or vendor to gain access to the certificate (e.g., through social engineering).
- Limited control over the distribution and use of certificates could enable an attacker to obtain access to a certificate.

Unencrypted certificates could be stored on recipient's systems.

Management of certificates is performed manually.

Example: *Threat Sequence (Top Level) -1*

1. The threat actor performs reconnaissance to determine who to target for social engineering.

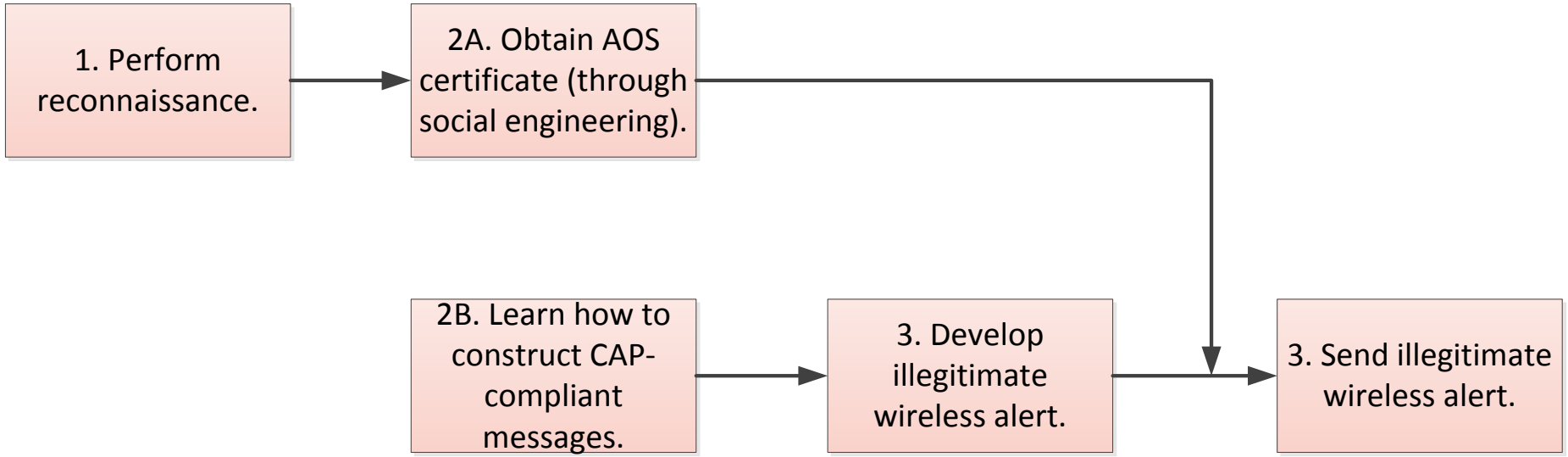
2A. The threat actor obtains an AOS certificate from an employee at the AO (through social engineering). The employee provides an electronic copy of the certificate to the threat actor.

2B. The threat actor finds information about constructing CAP-compliant messages from public documents.

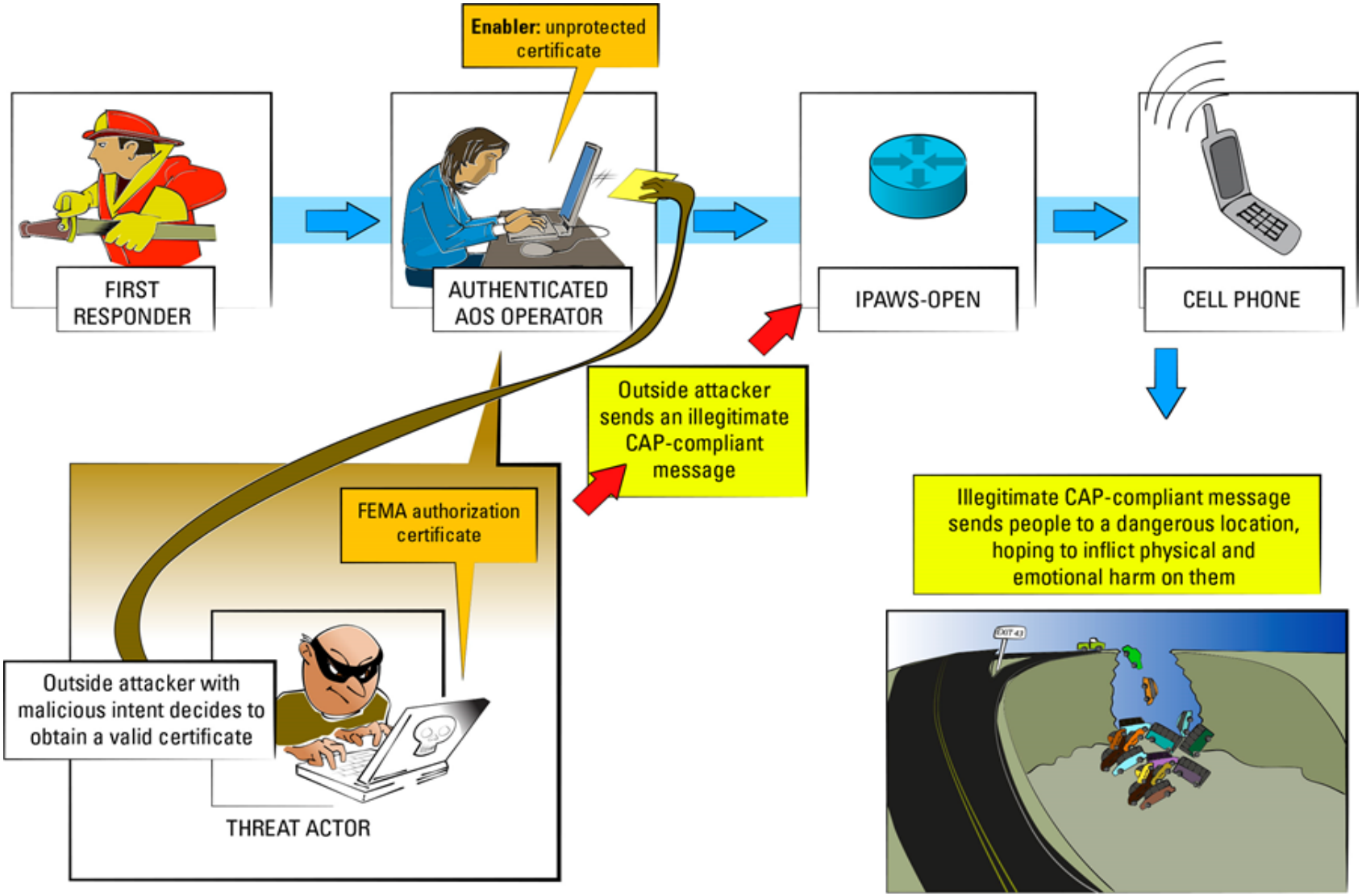
3. The threat actor creates an illegitimate CAP-compliant message intended to incite panic in a crowd that a bomb is about to explode in their location (e.g., an alert message of a bomb in Times Square on New Year's Eve).

4. The threat actor sends the illegitimate CAP-compliant message and certificate to the OPEN-PAWS gateway.

Example: *Threat Sequence (Top Level) -2*



Example: *Risk Scenario Diagram*



Next Steps

Build further risk scenarios for CMAS and explore ways to evaluate completeness

Refine steps 3-5 of the SERA methodology

Explore ways to express threats, risk scenarios, and mitigations to effectively communicate with stakeholders (campus collaboration)

Publications and Resources

Cyber Security Engineering (CSE) Team Web Page
http://www.cert.org/sse/

Alberts, Christopher & Dorofee, Audrey. *Mission Risk Diagnostic (MRD) Method Description* (CMU/SEI-2012-TN-005). Software Engineering Institute, Carnegie Mellon University, 2012.
http://www.sei.cmu.edu/reports/12tn005.pdf

Alberts, Christopher; Allen, Julia; & Stoddard, Robert. *Risk-Based Measurement and Analysis: Application to Software Security* (CMU/SEI-2012-TN-004), Software Engineering Institute, Carnegie Mellon University, 2012.
http://www.sei.cmu.edu/reports/12tn004.pdf

Woody, C., "Mission Thread Security Analysis: A Tool for Systems Engineers to Characterize Operational Security Behavior", INCOSE/INSIGHT, July 2013, Vol. 16, Issue 2

References: GPS Spoofing of UAV

Media reports – Lockheed Martin RQ-170 Incident

- http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video
- http://www.nytimes.com/2012/04/23/world/middleeast/iranians-say-they-took-secret-data-from-drone.html?_r=1&

Humphreys, Todd. *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*. http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf (2012).

Tippenhauer, Nils O.; Pöpper, Christina; Rasmussen, Kasper B.; & Capkun, Srdjan. “On the Requirements for Successful GPS Spoofing Attacks,” 75–85. *Proceedings of the ACM Conference on Computer and Communications Security (CCS*). Chicago, IL, Oct. 2011. ACM, 2011.

Contact Information

Carol Woody

(412) 268-9137

cwoody@cert.org

Web Resources (CERT/SEI)

http://www.cert.org/

http://www.sei.cmu.edu/