

ITS World Congress

Dan Klinedinst

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Software Engineering Institute

Carnegie Mellon University

© 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.

REV-03.18.2017.0

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Homeland Security 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 sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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.

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.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0860



Software Engineering Institute

Carnegie Mellon University

ITS World Congress

Oct 30, 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.

DM17-0860

Who am I?

- Vulnerability Researcher at Carnegie Mellon University
- Part of the CERT Coordination Center / Attack Modeling Team

CERT Coordination Center	
From Wikipedia, the free encyclopedia	
Industry	Software and Network Security
Founded	1988
Headquarters	Pittsburgh, PA, United States

- I research threats and vulnerabilities in connected vehicles, ITS platforms, robotics, and embedded systems.
- As part of the SEI Tactical Technologies Group, I prototype secure systems for disconnected environments.
 - Military, disaster response, harsh environments (e.g. Antarctica)

Qualifying risk in CAVs

- Total motor vehicle thefts in US, per year: **~700,000**
- Theft of goods from cars, per year: **\$1.255B in 1.85M thefts**
- Proven criminal hacks* of cars, to date: **0**
- Most common “car hacking” tool:



* Not including key fob spoofing

Great! Let's go home.

Why would anyone bother to hack cars instead of stealing them / their contents the old fashioned way?

- Scale
 - Jeep hack: ~471,000 vehicles
 - Fleet mgmt devices: Hundreds of thousands
- Distance
 - For some classes of attack, can be done over the Internet
- No damage and/or evidence*
- New classes of crimes
 - Ransomware
 - “Autonomous kidnapping”
 - Remote control VBIED

No damage and/or evidence?

- How would you know if software or data is corrupted / altered?
- We need “black boxes” in cars
- Please log everything
 - Write-once
 - Encryption / Non-repudiation
 - Timestamp

Potential Attacks / Impact

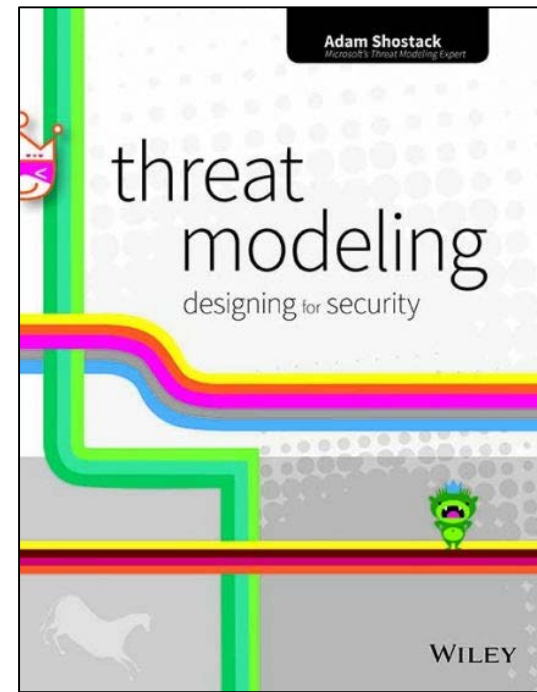
- Remote unlock / theft of contents
- Start car / theft of car
- Control car / cause accidents, panic, traffic jams
- Tracking vehicle's whereabouts
- Fingerprinting vehicle via RF signatures
- Espionage / eavesdropping via microphones or cameras
- Theft of information (e.g., contacts stored on car's IVI)
- Compromise other mobile devices
- Use mobile device to create Internet accessible back door

Threat modeling

We're big fans of threat at modeling at CERT.

Shostack's three types of threat modeling

- Software-centric
- Attacker-centric
- Asset-centric



Software-centric

Focuses on “risky” operations in software

(Microsoft)

STRIDE

S: Spoofing

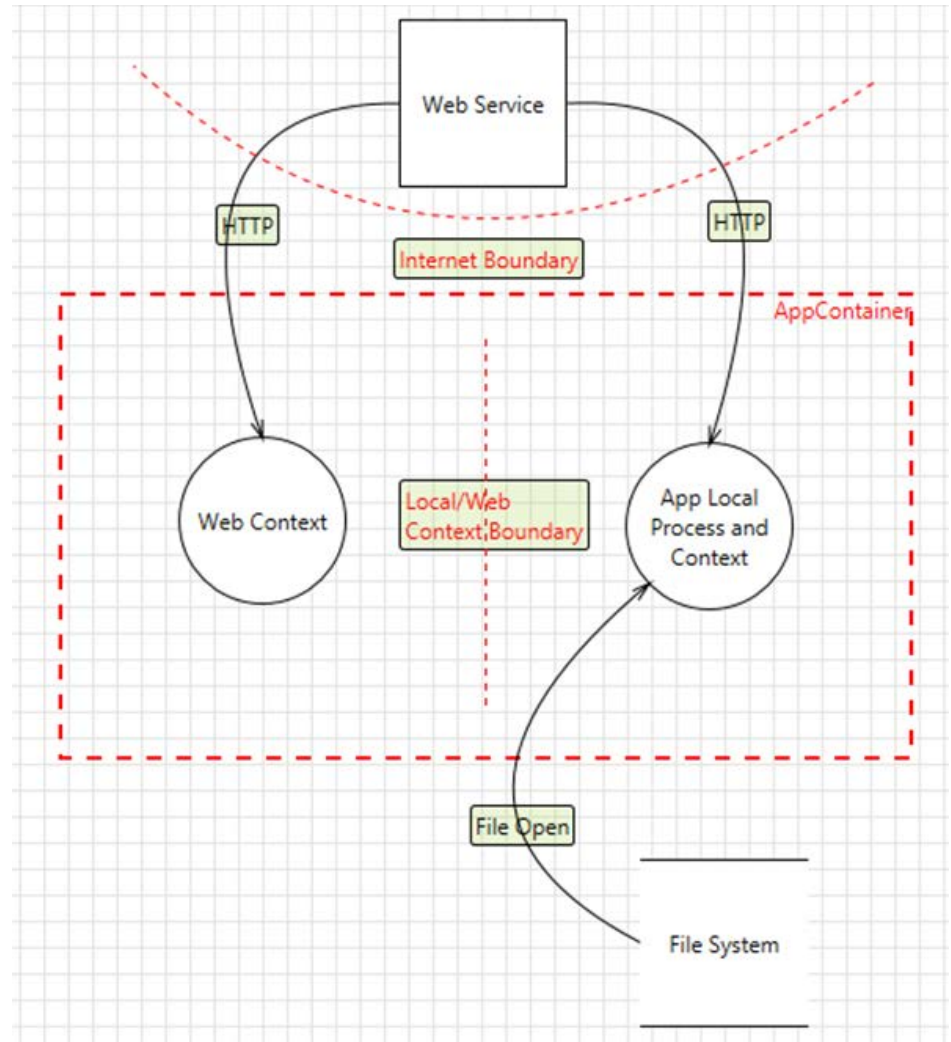
T: Tampering

R: Repudiation

I: Information Disclosure

D: Denial of Service

E: Escalation of Privilege



Attacker-centric

(Sandia National Laboratory)

Table 1. Generic threat matrix

Threat Level	THREAT PROFILE						
	Commitment			Resources			
	Intensity	Stealth	Time	Technical personnel	Knowledge		Access
					Cyber	Kinetic	
1	H	H	Years to decades	Hundreds	H	H	H
2	H	H	Years to decades	Tens of tens	M	H	M
3	H	H	Months to years	Tens of tens	H	M	M
4	M	H	Weeks to months	Tens	H	M	M
5	H	M	Weeks to months	Tens	M	M	M
6	M	M	Weeks to months	Ones	M	M	L
7	M	M	Months to years	Tens	L	L	L
8	L	L	Days to weeks	Ones	L	L	L

Reproduced from Duggan et al. [8].

Asset-centric

How would an attacker reach an asset?

Attack Tree (Schneier)

