



The Old Ways Aren't Good Enough

Best Practices for Cybersecurity

Greg Touhill
Brigadier General, USAF (ret)
CERT Director
Software Engineering Institute
Carnegie Mellon University

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2021 Carnegie Mellon University.

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.

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.

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® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM21-0571

How good or bad is our cybersecurity posture?

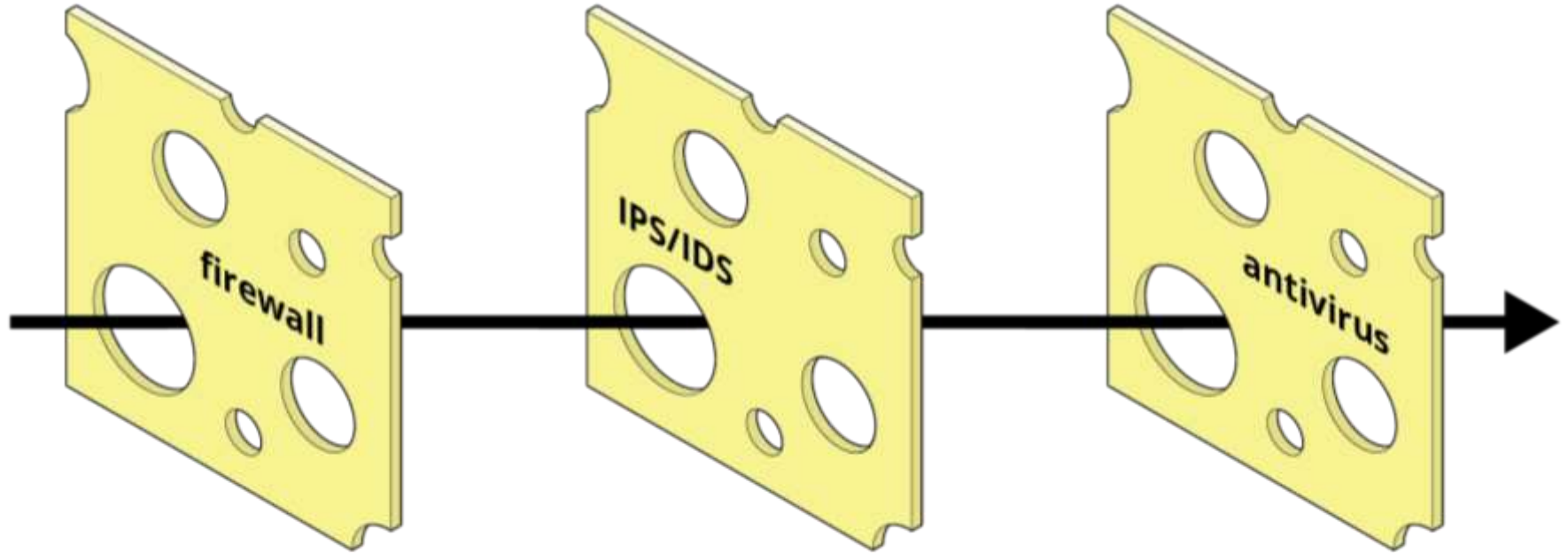


Photo by Jason Weingart, CC Attribution-Share Alike 4.0, https://commons.wikimedia.org/wiki/File:Evolution_of_a_Tornado.jpg

1970s security isn't good enough



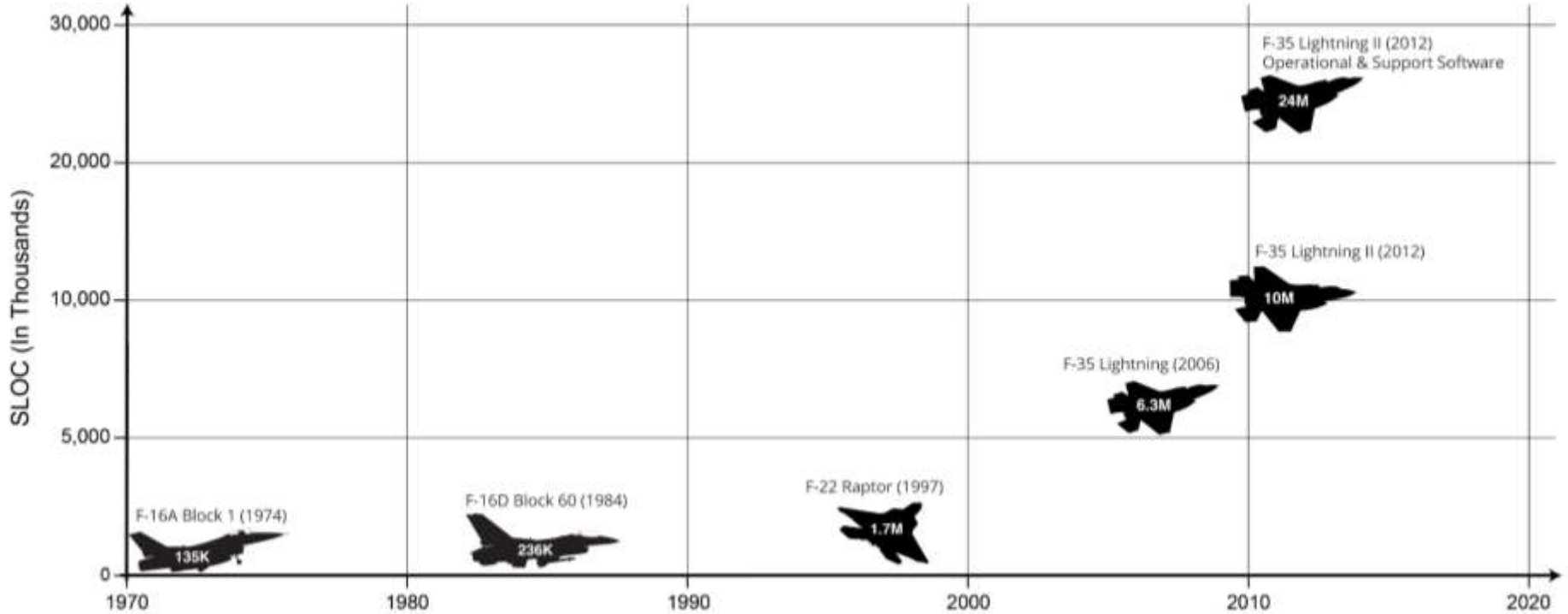
1980s security isn't good enough



1990s security isn't good enough



Software complexity is growing



Source: Data modified from Scilab, "Human in the Loop Testing," <https://www.scilab.org/human-loop-testing>

Bolting on security?



Why worry?

data breach

exfiltration

Shellshock

supply chain

malware

Target

OPPM



ransomware
SolarWinds

Equifax

Shell

Heartbleed

JP Morgan



We live in a rough neighborhood



THE FBI FEDERAL BUREAU OF INVESTIGATION

REPORT THREATS • A-Z INDEX • SITE MAP

CONTACT US ABOUT US MOST WANTED NEWS STATS & SERVICES SCAMS & SAFETY JOBS FUN & GAMES

WANTED BY THE FBI

CHINESE PLA MEMBERS, 54TH RESEARCH INSTITUTE

Computer Fraud; Economic Espionage; Wire Fraud; Conspiracy to Commit Computer Fraud; Conspiracy to Commit Economic Espionage; Conspiracy to Commit Wire Fraud

ALEXANDR intentionally
Dana J. Boe Assistant Di
was accepto
Wolberg wa
Wolberg fac
According to
worked as a
provider he

 Wang Qian	 Xu Ke	 Liu Lei	 Wu Zhiyong
---	--	--	---

Rule of Acquisition #74 applies

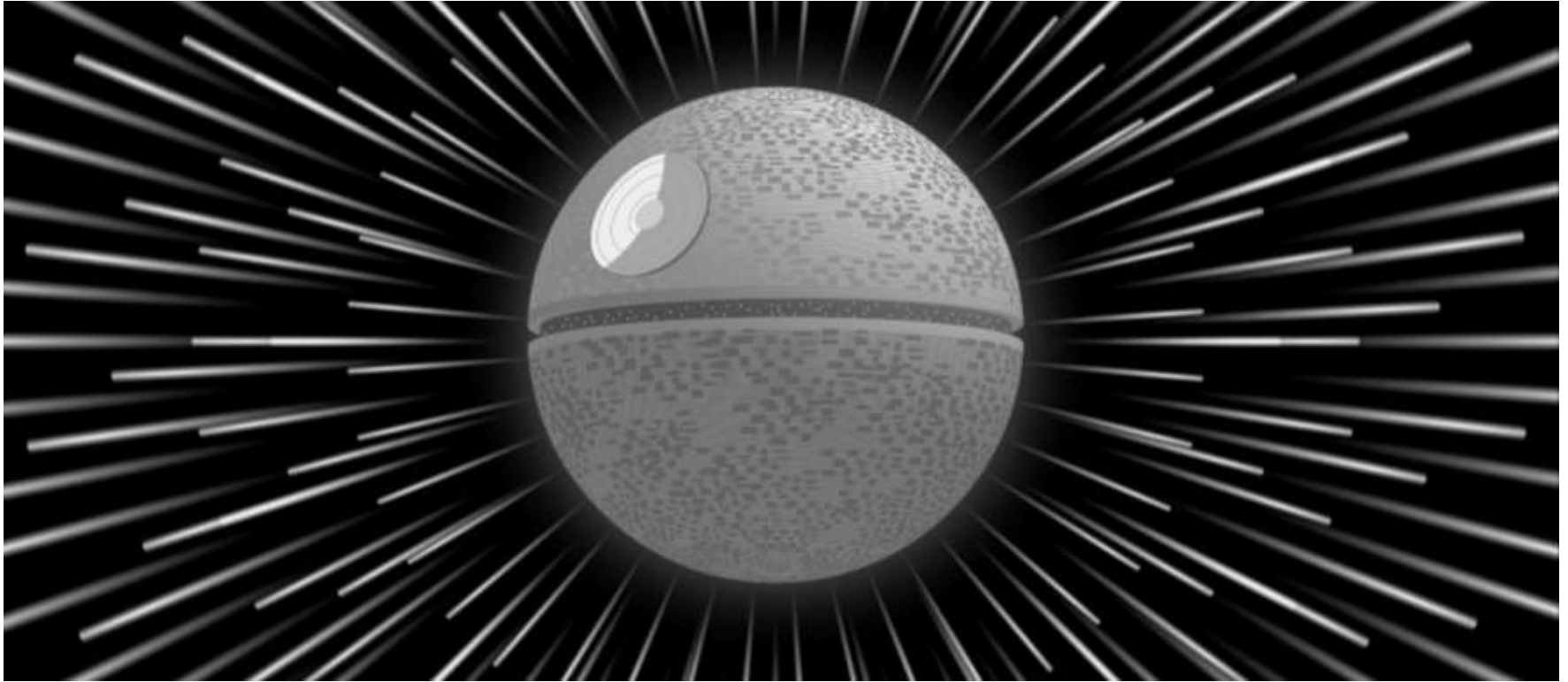


Photo credits: C-141B, by Rob Schleiffert, CC Attribution-Share Alike 2.0 Generic, [https://commons.wikimedia.org/wiki/File:C-141B_\(21793080516\).jpg](https://commons.wikimedia.org/wiki/File:C-141B_(21793080516).jpg); Ilyushin Il-76MD, by Danny Yu, CC Attribution-Share Alike 4.0, https://commons.wikimedia.org/wiki/File:Ilyushin_Il-76MD.jpg; F-35A Lightning II by U.S. Air Force photo/Staff Sgt. Darlene Seltmann, <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/478441/f-35a-lightning-ii-conventional-takeoff-and-landing-variant>

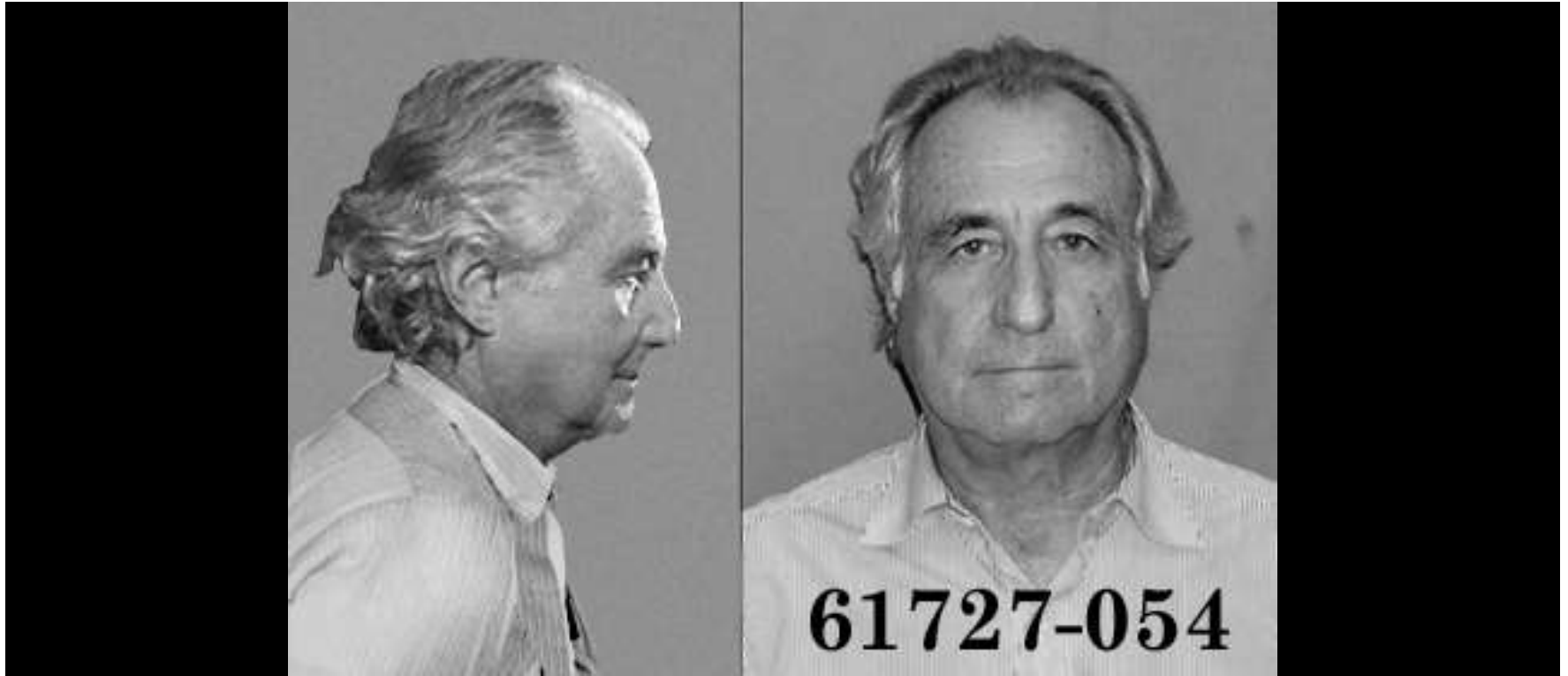
Think like a hacker



Bake security in



Adopt a zero-trust model



Remain continually vigilant



Best Practices = Due Care + Due Diligence

1. Understand the value of your data
2. Implement a zero-trust security strategy
3. Tightly control and log access
4. Employ multifactor authentication
5. Implement microsegmentation
6. Use Active Directory whitelisting
7. Reduce and tightly control privileged user accounts
8. Guard your back door; limit and control third-party access



Contact Us



Greg Touhill

Director, CERT Division

Carnegie Mellon University

Software Engineering Institute

4500 Fifth Avenue

Pittsburgh, PA 15213

888-201-4479

info@sei.cmu.edu

www.sei.cmu.edu