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

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.

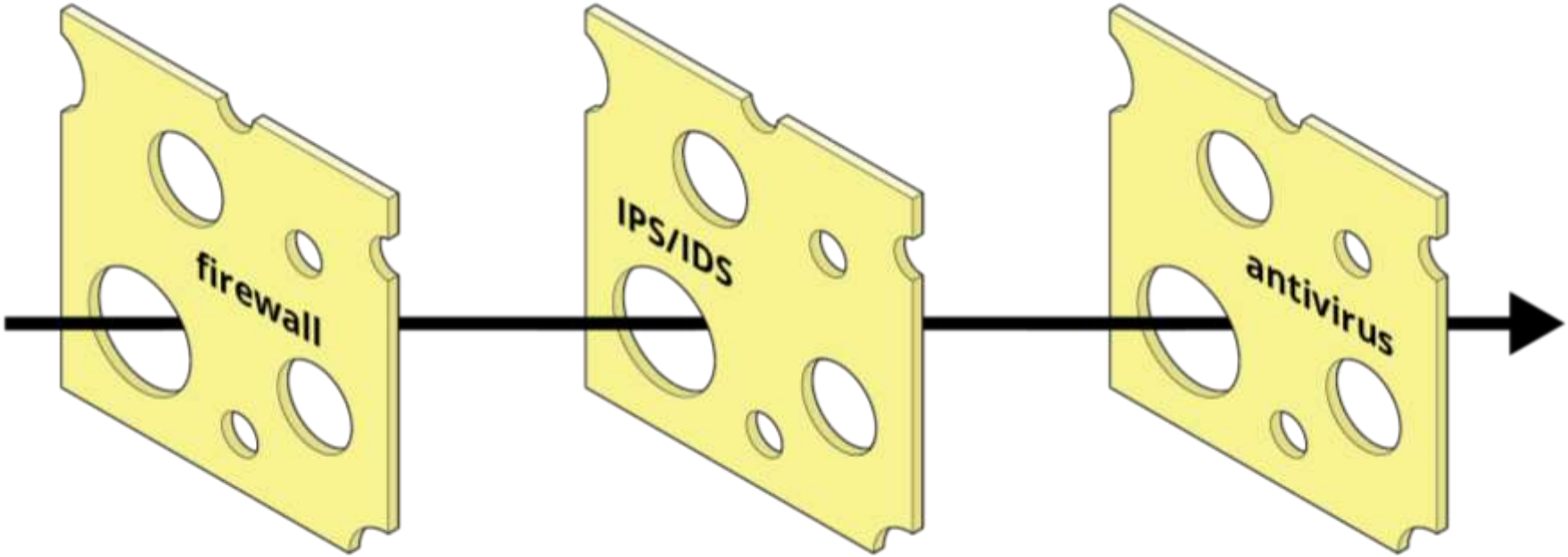
DM21-0571

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

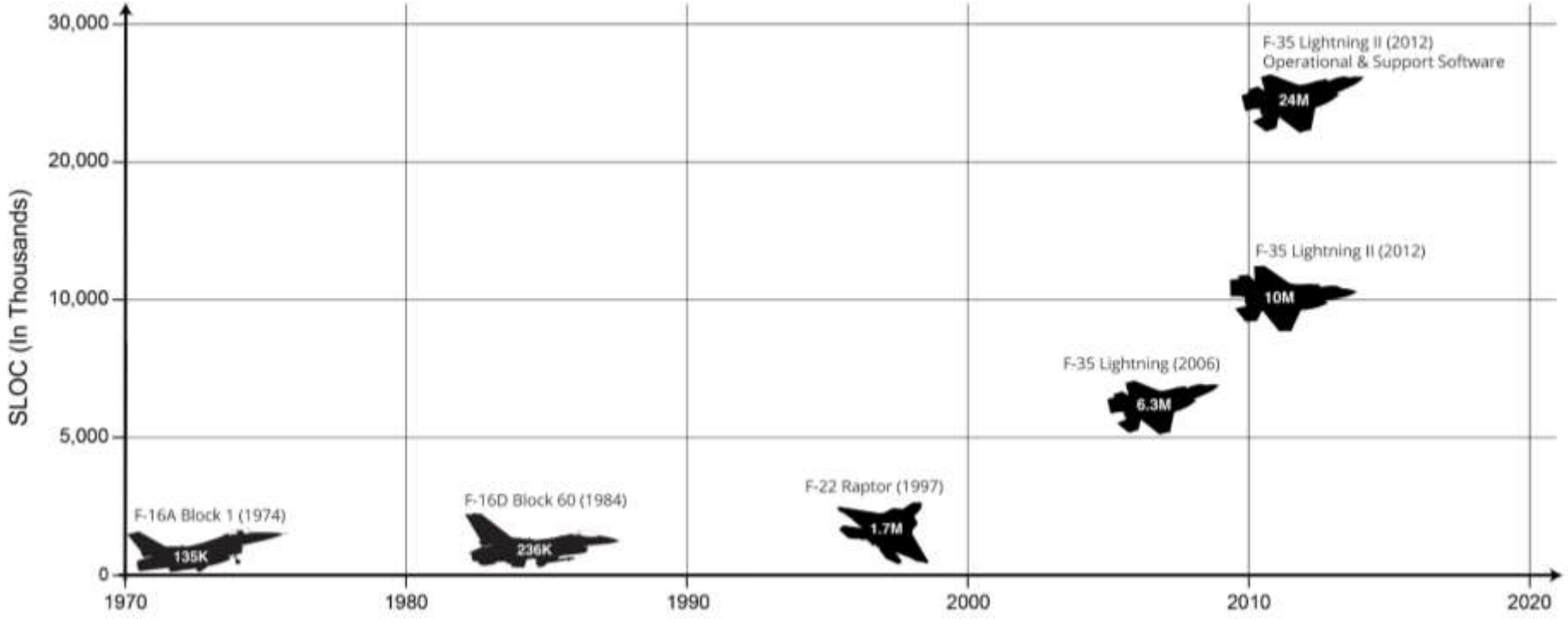
1970s security isn’t good enough

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
OPM
Target


ransomware
SolarWinds
Equifax
Shell
Heartbleed
JP Morgan

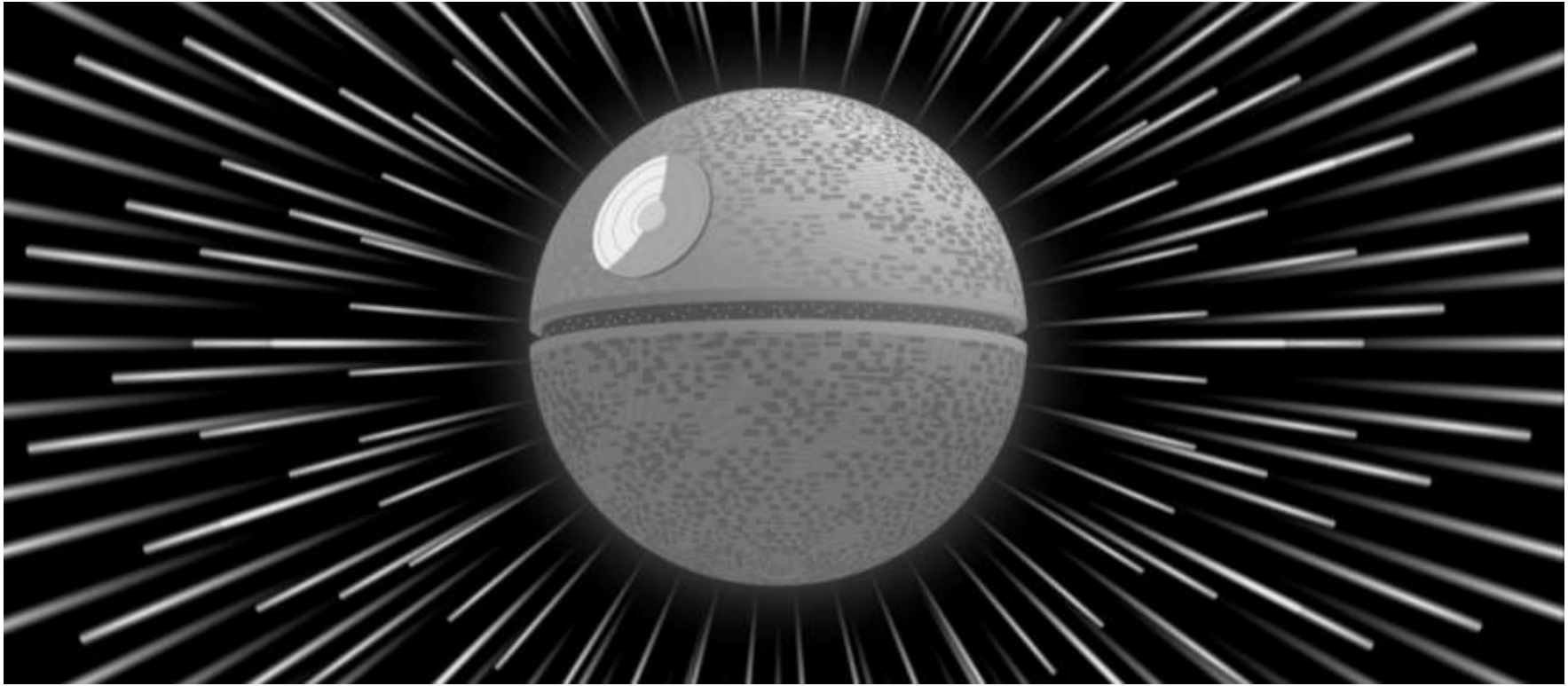
We live in a rough neighborhood

Rule of Acquisition #74 applies

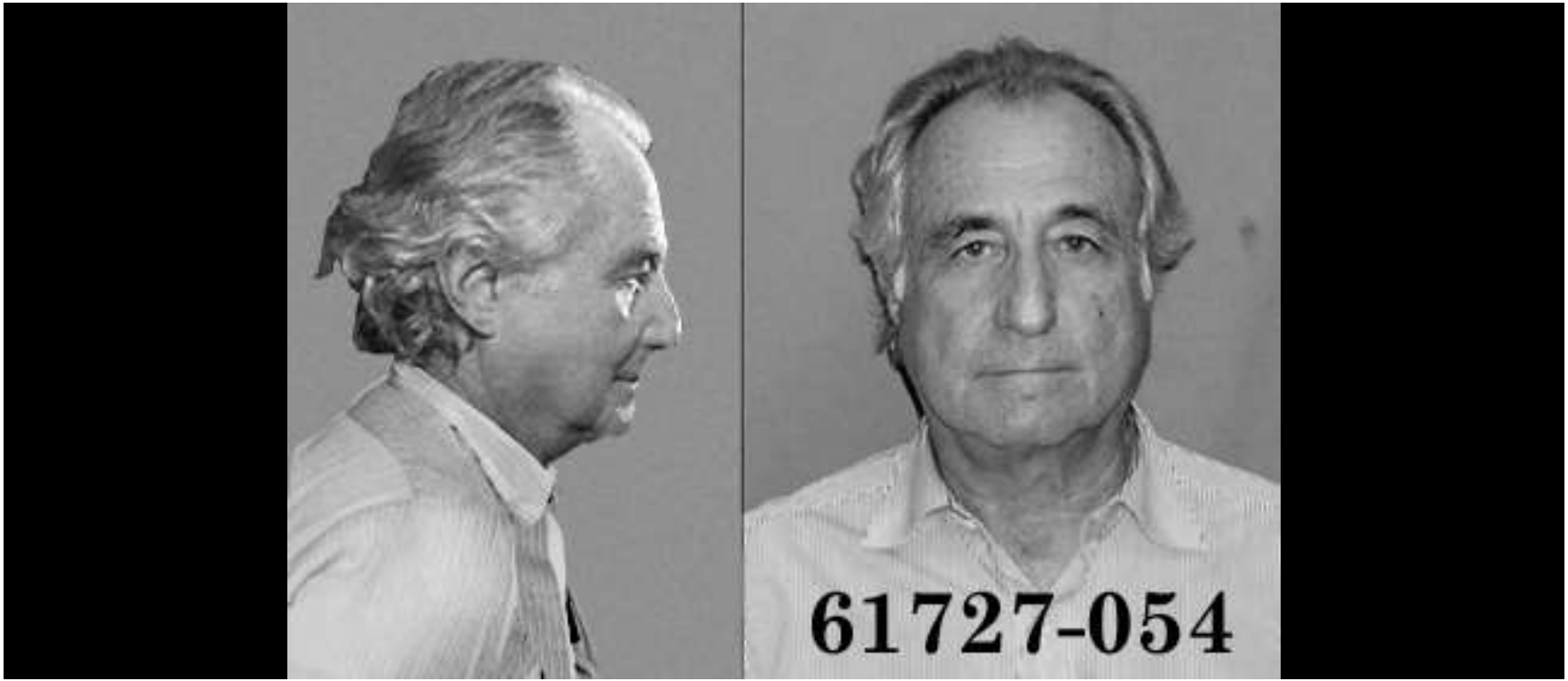
Photo credits: C-141B, by Rob Schleiffert, CC Attribution-Share Alike 2.0 Generic, https://commons.wikimedia.org/wiki/File:C-141B_(21793080516).jpg; Ilyushin Il-76MD, by Danny Yu, CC Attribution-Share Alike 4.0, ; F-35A Lightning II by U.S. Air Force photo/Staff Sgt. Darlene Seltmann, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/478441/f-35a-lightning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