RSAConference2021
May 17 – 20 | Virtual Experience

SESSION ID: TECH-W13

DHS CISA Strategy to Fix Vulnerabilities Below the OS Among Worst Offenders

Boyden Rohner

Associate Director Vulnerability Management
Cybersecurity and Infrastructure Security Agency (CISA)

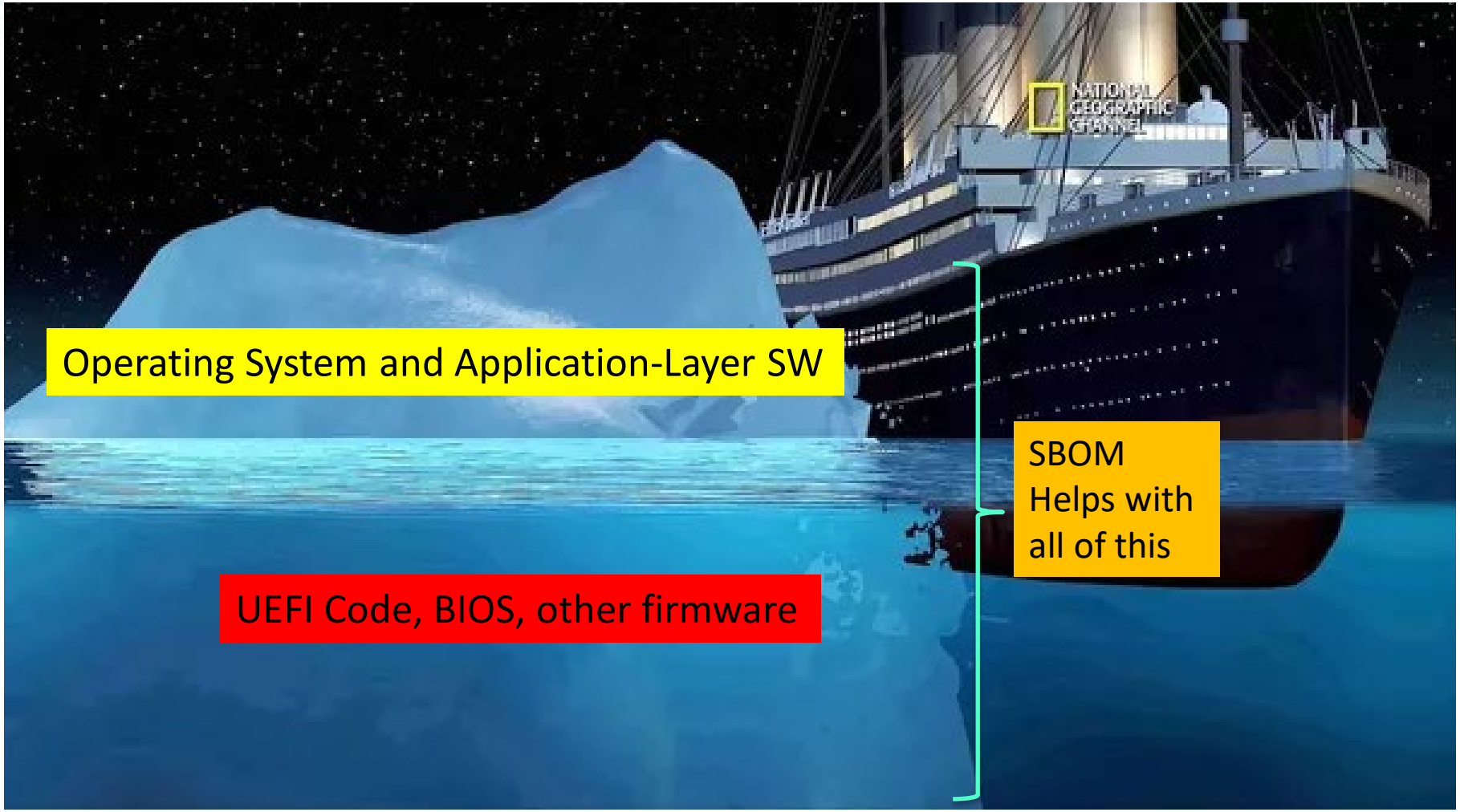
Thomas Ruoff

Methodology Branch Chief of Vulnerability Management
Cybersecurity and Infrastructure Security Agency (CISA)

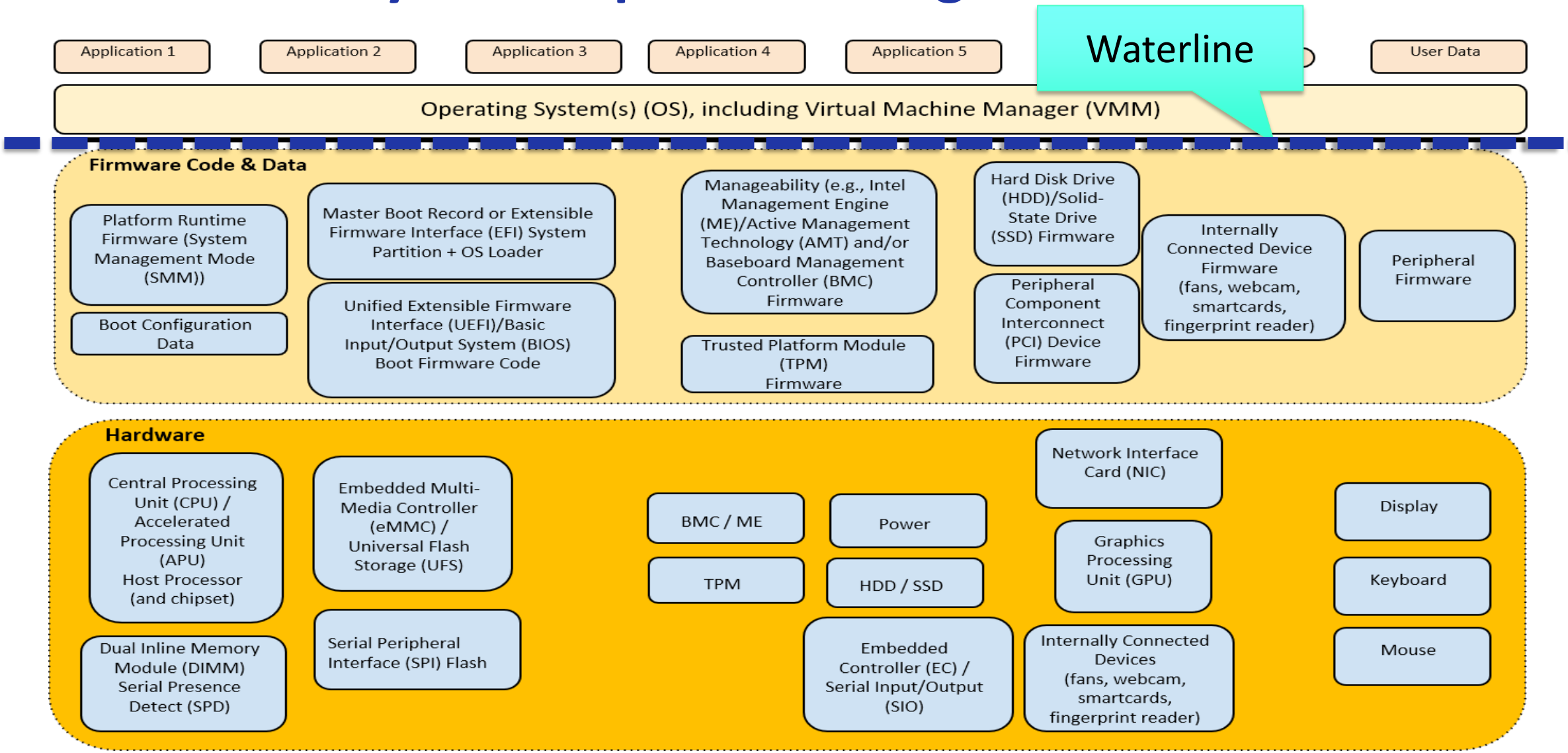
The Software Illusion

You thought the iceberg was this big…

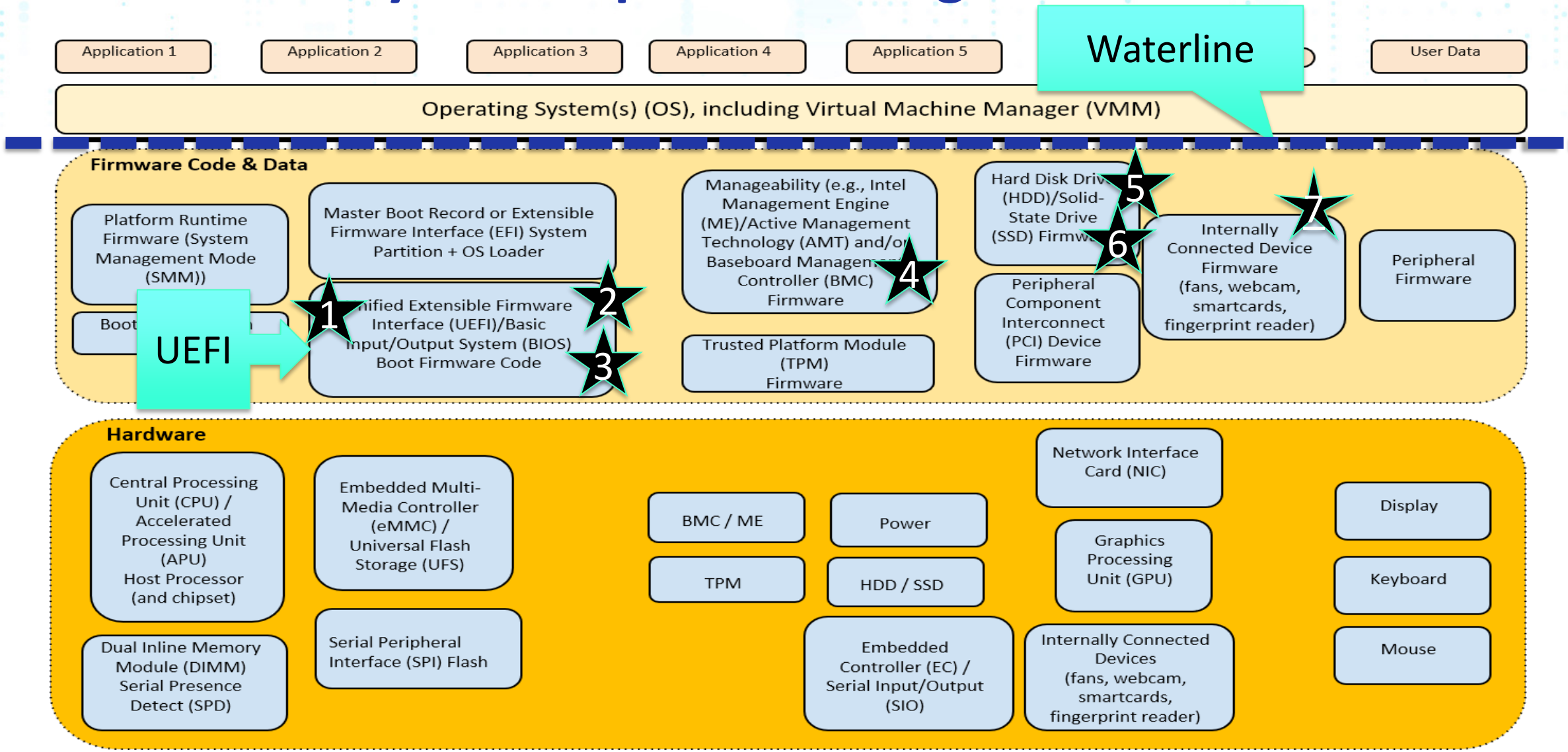
…but you forgot VBOS



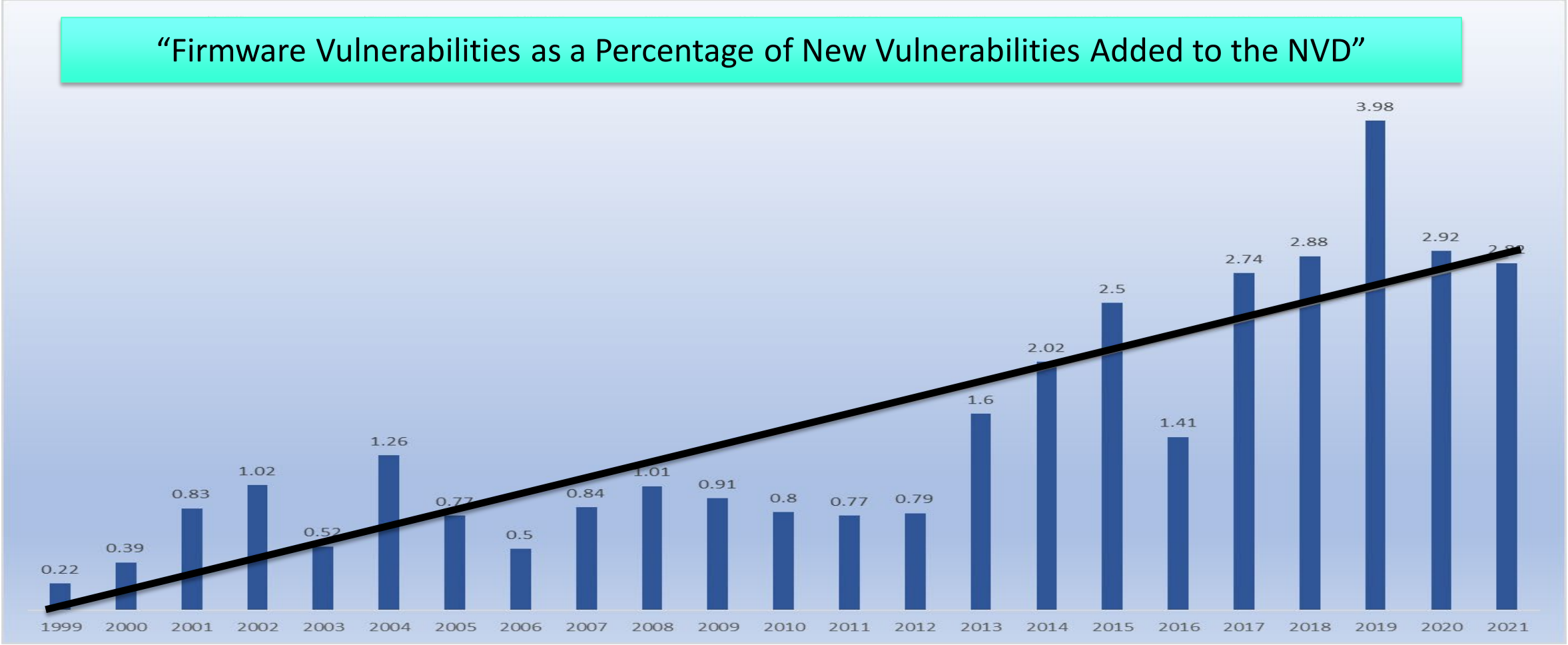
VBOS Taxonomy of Computer Icebergs



VBOS Taxonomy of Computer Icebergs – Incidents



A Growing Problem

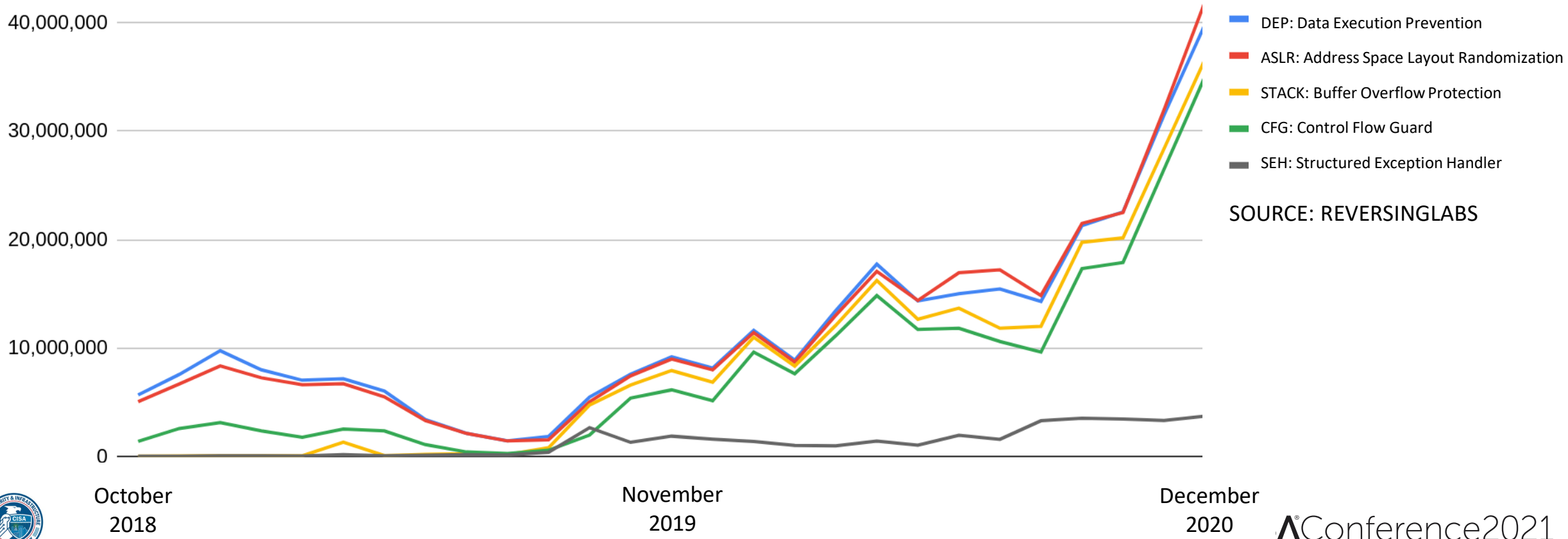


Source: NIST NVD, 3/17/21

Takeaway: This is getting worse

GOOD NEWS: Files above OS are increasingly being armed with vulnerability mitigation techniques

UNIQUE FILES WITH VULNERABILITY PROTECTIONS PER MITIGATION TECHNIQUE



SOURCE: REVERSINGLABS

NOT SO GOOD NEWS: Developers are using mitigation techniques first developed in 2005 and not uniformly

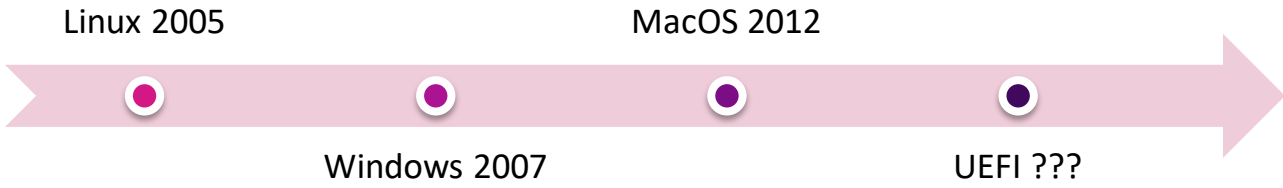
Vulnerability Mitigation Techniques	Successful Implementation in Commercial Products
DEP - Data Execution Prevention	89.123%
ASLR - Address Space Layout Randomization	88.790%
STACK - Buffer Overflow Protection	61.400%
CFG - Control Flow Guard	56.868%
SEH - Structured Exception Handler	12.200%
SDL – SDLC Enforcement	0.640%
CET – Intel Control Enforcement Technology	0.040%
RFG – Return Flow Guard	0.014%
MPX – Memory Protection Extension	0.005%

AREAS FOR IMPROVEMENT: HIGH PRODUCT VULNERABILITY RISK

SOURCE: **REVERSINGLABS**

BAD NEWS: There are no ways to apply Vulnerability Mitigations below the OS

Address
Space
Layout
Randomization



MORE BAD NEWS: Most criminal and advanced threat actors exploit Vulnerabilities Below the OS that affect UEFI

EVEN MORE BAD NEWS: In general, existing memory protections (NX) are not enforced due to vendor non-compliance

UEFI – The Worst Offenders

The popularity of UEFI and its lack of memory protection enforcements attract exploitation.

VBOS – Twinkie Analogy

Imagine a world where the contents of food are not regulated – no FDA.
This is where we are with software.

https://www.foodmatters.com/article/whats-really-in-a-twinkie

Problem Statement – what are we trying to solve

IT and OT systems are being compromised by:

- threat actors exploiting poorly written or maliciously written code,
- modular dependencies, and
- reused code – the existence of which is unknown and what it does is unknown.

The place we find the majority of exploits (most, not all) are in UEFI code

What CISA Thinks Success Looks Like

1. Vendors disclose SW content and what the SW is supposed to do (Ingredients Label and claim it is human food)

The section in the EO requiring the SBOM is a great place to start but is not sufficient

Note: *SBOM is easy and beginning to happen today, OEM intent is an add-on*

What CISA Thinks Success Looks Like

1. Vendors disclose SW content (Ingredients Label)
2. Adopt vulnerability mitigations for all SW, focus on UEFI code writing community. (FDA recognizing Twinkies are food too)

Note: *This is difficult but there is a path forward if we ask for it as a capability requirement*

What CISA Thinks Success Looks Like

1. Vendors dis… …ingredients Label)
2. Vendors sha… …otes. (Twinkie manufacture claims it is food)
3. SW analysis capabilities available to investigate what the SW is capable of doing. (FDA Test Reports on effects of eating Twinkies)

Note: This is hard – we are optimistic our researchers can make progress

What CISA Thinks Success Looks Like

1. Vendors dis[illegible] SW content (Ingredients Label)
2. Vendors sha[illegible] notes. (Twinkie manufactur[illegible]
3. SW analysis capabilities av[illegible] SW is capable of doing. (FDA Test Reports on effects of eating Twinkies)

Note: This is **really hard** – we are optimistic some big brains will make progress if we ask

4. Risk Indicator Scoring – what is the SW supposed to do and what can it do; the classic definition of SW risk. (FDA approval to market and sell Twinkies as human food)

"Good" code can only do what it is written to do, independent of input. Lets go old school on figuring out how risky code is.

What CISA Thinks Success Looks Like

1. Vendors disclose SW content (Ingredients Label)
2. Vendors share what the SW is intended to do – design notes. (Twinkie manufacture claims it is food)
3. SW analysis capabilities available to investigate what the SW is capable of doing. (FDA Test Reports on effects of eating Twinkies)
4. Risk Scoring – what is the SW supposed to do and what can it do; the new definition of SW risk. (FDA approval to market and sell Twinkies as human food)
5. Readily available detailed test reports to substantiate indictors of risk. (Reports on FDA web sites)

The risk indicators need to be backed up with test data to provide integrity and make risk decisions data driven, moving from hope to knowledge

What CISA Thinks Success Looks Like

1. Vendors disclose SW content (Ingredients Label)
2. Vendors share what the SW is intended to do – design notes. (Twinkie manufacture claims it is food)
3. SW analysis capabilities available to investigate what the SW is capable of doing. (FDA Test Reports on effects of eating Twinkies)
4. Risk Scoring – what is the SW supposed to do and what can it do; the new definition of SW risk. (FDA approval to market and sell Twinkies as human food)
5. Readily available detailed test reports to substantiate risk scores. (Reports on FDA web sites)
6. Promote policies discouraging procurement of the worst offenders. (FDA banning products from US markets as human food)

Making a Risk Based Decision

1. Can you provide me with the Software Bill of Materials (SBOM)?
2. Can you tell me what the software is intended to do?
3. What vulnerability mitigation techniques have been included in the software?

CISA: Putting Security into Practice

1. Convene the community
2. Updating CISA services to help CI owners and CISA get visibility
3. Work with researchers develop a specification for automated code analysis to verify vendor code claims and explore getting risk indicator scores.

How to Get Involved

1. Read the Executive Order
2. Ask new questions about SBOM when procuring IT equipment
3. If you can’t fix it, control it. 3. Contact us to set up a relationship so we can support you
4. Join the conversation!

RSAConference2021

Questions?