Towards Resilient Systems in an Increasingly Hostile World

Kathleen Fisher

Director, Information Innovation Office (I2O)

February 2025

Efficiency vs. Resiliency

The supply chain crisis overwhelmed US ports during Covid

Mario Tama / Getty Images file

Container ships are anchored by the ports of Long Beach and Los Angeles as they wait to offload

VCG/Getty Images

Containers wait to be loaded at the Long Beach port as cargo ships sit idle in the distance

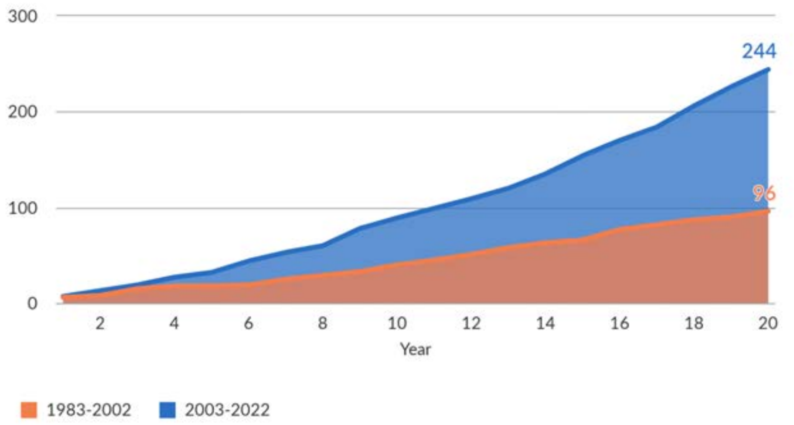
Given the shift in world dynamics, we're overly focused on efficiency

https://www.nbcnews.com/business/100-ships-idle-offshore-california-communities-see-rise-toxic-pollutan-rcna3984
https://www.theguardian.com/business/2021/oct/20/supply-chain-crisis-california-ports-cargo-ships

Natural disasters are becoming more costly

Billion-dollar disasters take a growing toll

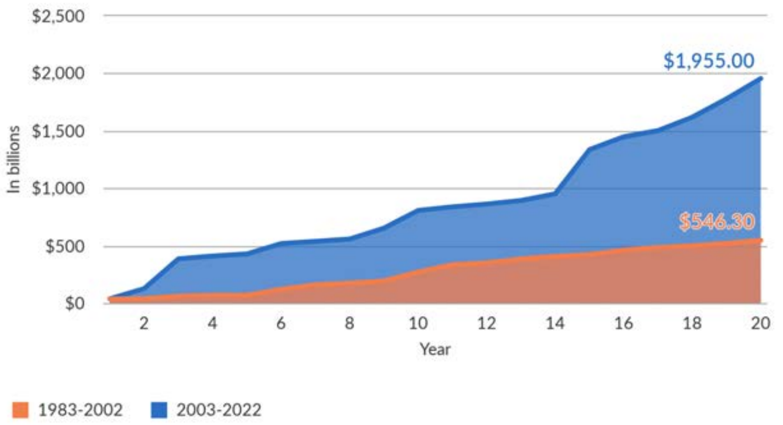
Number of Billion-Dollar Disasters



Source: National Oceanic and Atmospheric Administration (https://www.ncei.noaa.gov/access/billions/events.pdf)

© 2023 The Pew Charitable Trusts

Cumulative Cost of Billion-Dollar Disasters



Source: National Oceanic and Atmospheric Administration (https://www.ncei.noaa.gov/access/billions/events.pdf)

© 2023 The Pew Charitable Trusts

More frequent and costly disasters are becoming a "new normal"

https://www.pewtrusts.org/en/research-and-analysis/articles/2023/10/12/whats-driving-the-boom-in-billion-dollar-disasters-a-lot#:%7E:text=Unfortunately%2C%20these%20events%20are%20not,reached%20or%20exceeded%20$1%20billion

We live in an increasingly hostile world

Global conflicts double over the past five years

1 in 8 people

are estimated to have been exposed to conflict so far in 2024

50 countries

rank in the Index categories for extreme, high, or turbulent levels of conflict

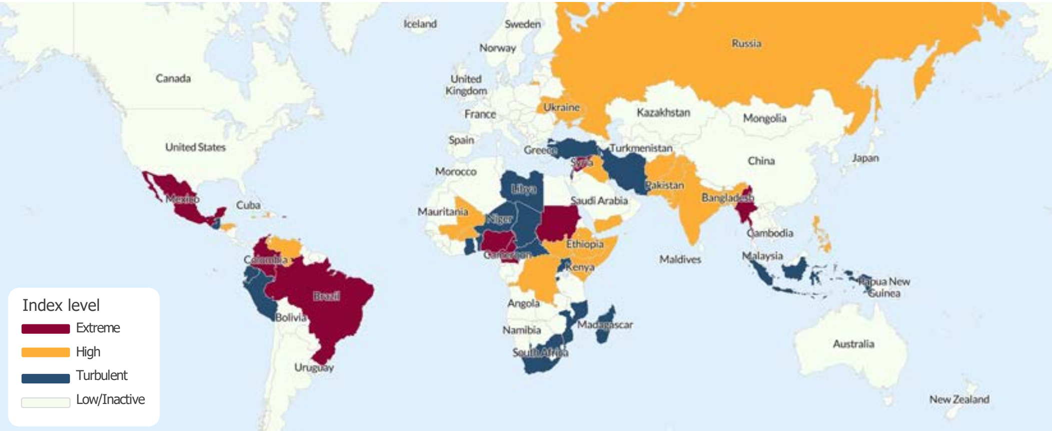
25% increase

in political violence incidents recorded in the past 12-month period

Palestine, Myanmar, Syria, and Mexico

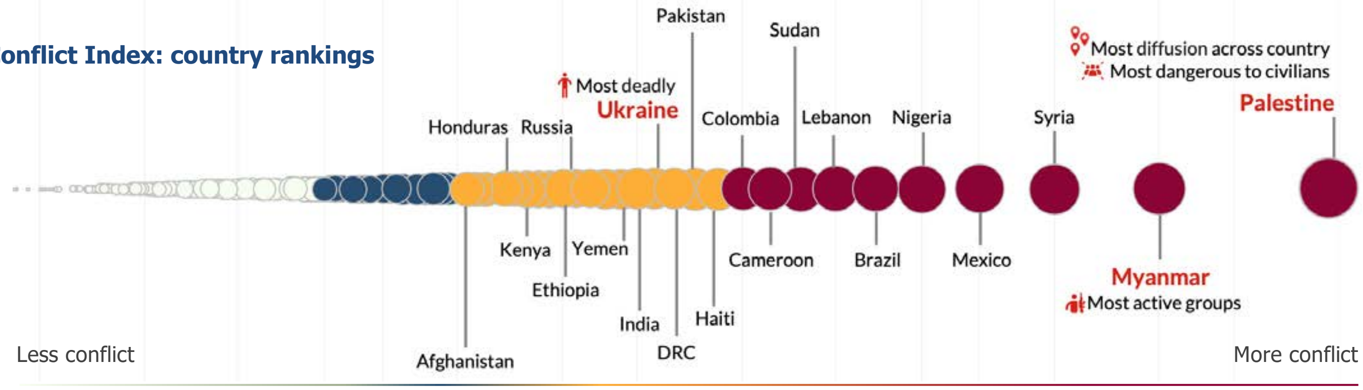
hold the highest positions in the Index

Where is conflict happening as of December 2024?



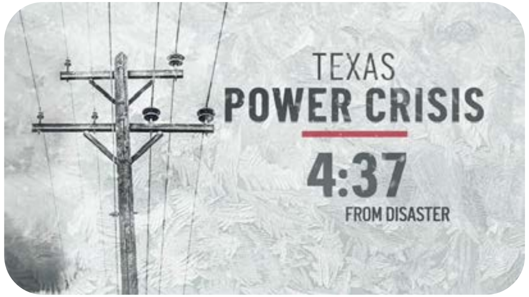
Armed Conflict Location & Event Data (ACLED)

Conflict Index: country rankings



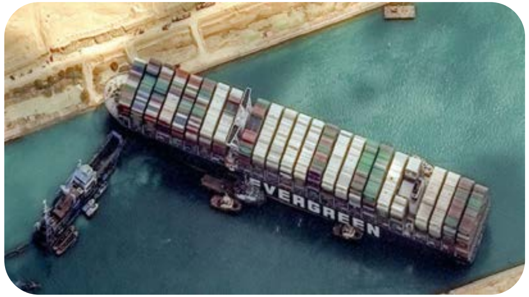
https://acleddata.com/conflict-index/

Growing interdependencies in mega-systems



www.nbcdfw.com

2021 Texas grid crisis collapse – multi-day power outage affecting over 11 million people



www.theatlantic.com

2021 The Evergreen container ship control failure causes a closure of the Suez Canal

SYSTEM CRASH:
THE FAA NOTAM OUTAGE OF JANUARY 2023
AND ITS IMPACT ON AVIATION

brotallion.com

2023 FAA Notice To Air Missions (NOTAM) outage – All air operations in US suspended for over 12 hours

techmonitor.ai

2023 EUROCONTROL – British National Air Traffic System (NATS) outage – 100s of flights disrupted

microtime.com

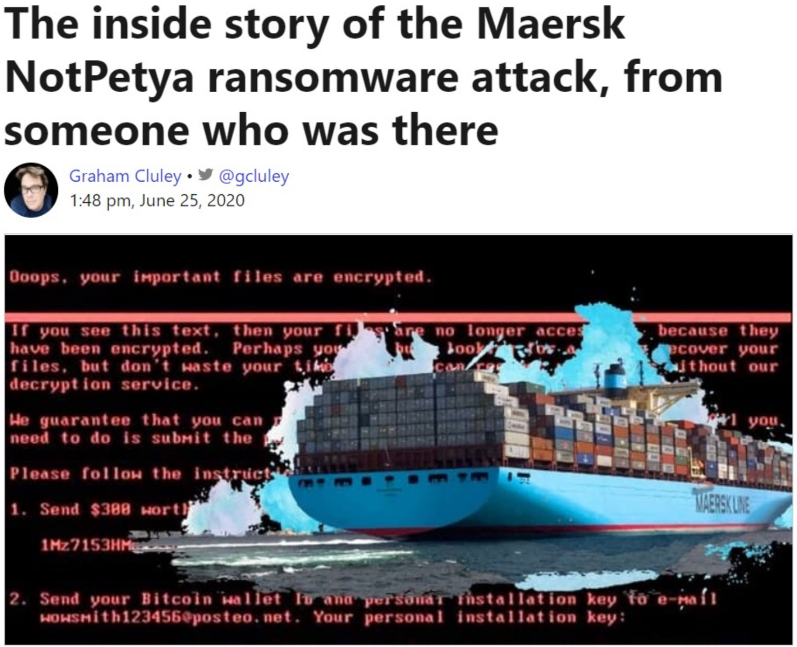
2024 Change Healthcare payment system experienced a crippling ransomware attack

nextgov.comnextgov.com

2024 CrowdStrike software errors melted down the world's computer systems

Society is dependent on many marginally stable mega-systems that have multiple exposed tipping points and may not be restorable if/when they go down

Cyber attacks can have broad impact on infrastructure

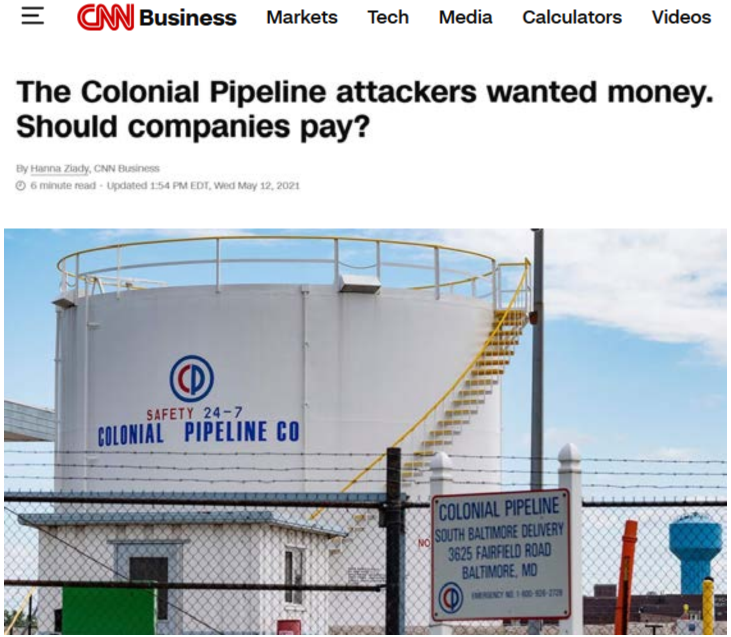


The inside story of the Maersk NotPetya ransomware attack, from someone who was there

Graham Cluley • @gcluley
1:48 pm, June 25, 2020

```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer acces      because they
have been encrypted.  Perhaps you               recover your
files, but don't waste your time              without our
decryption service.

We guarantee that you can r                       l you
need to do is submit the

Please follow the instruct

1. Send $300 worth

   1Mz7153HM

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:
```

The shipping conglomerate Maersk, hit by the NotPetya ransomware in June 2017, estimated that it cost them as much as $300 million in lost revenue.



The Colonial Pipeline attackers wanted money. Should companies pay?

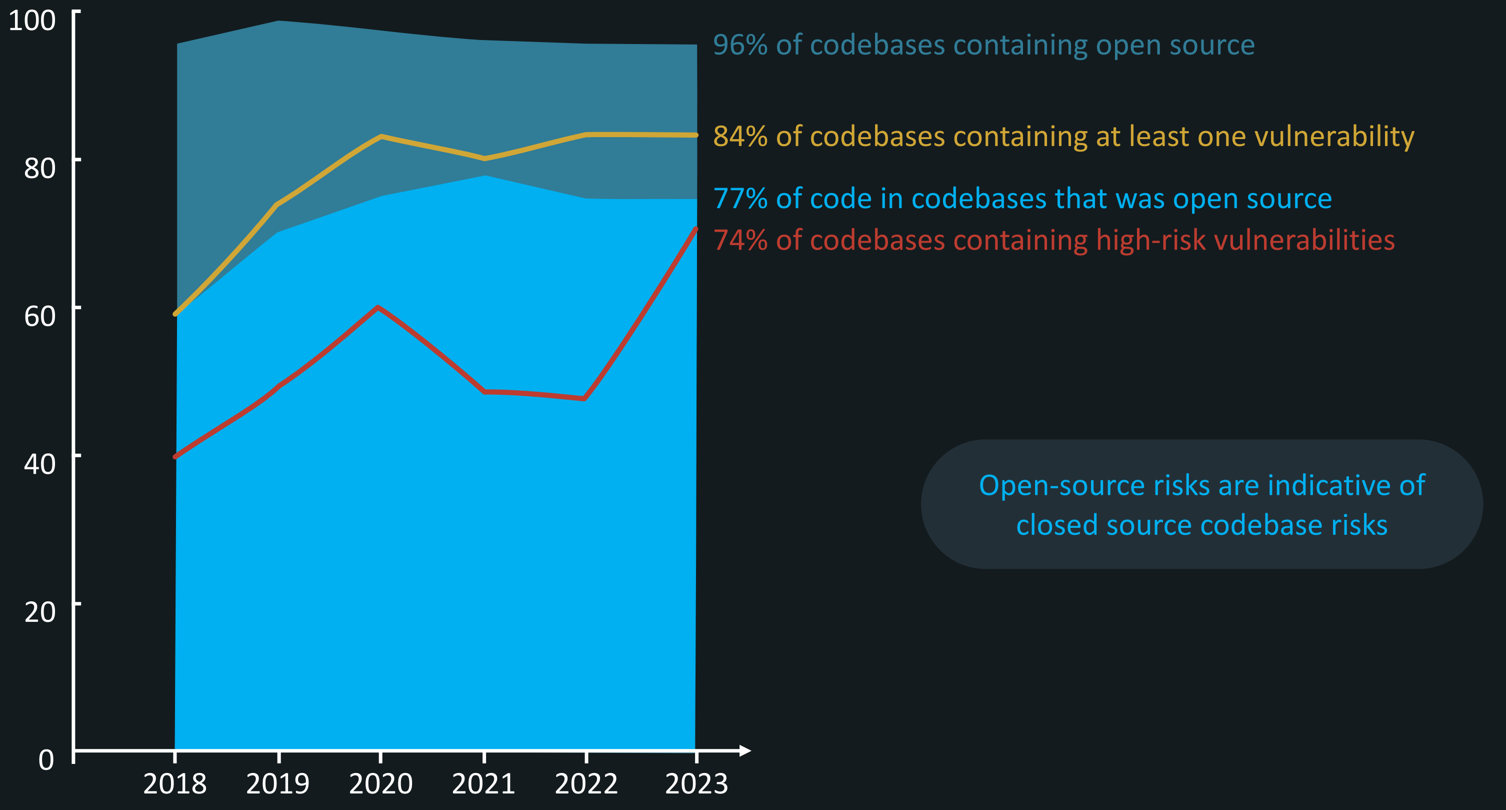
By Hanna Ziady, CNN Business
6 minute read · Updated 1:54 PM EDT, Wed May 12, 2021

cnn.com

2021 Colonial Pipeline ransomware attack –
first high profile corporate cyber attacks

We may lose before day one

Huge exposure continues: open source risk assessment



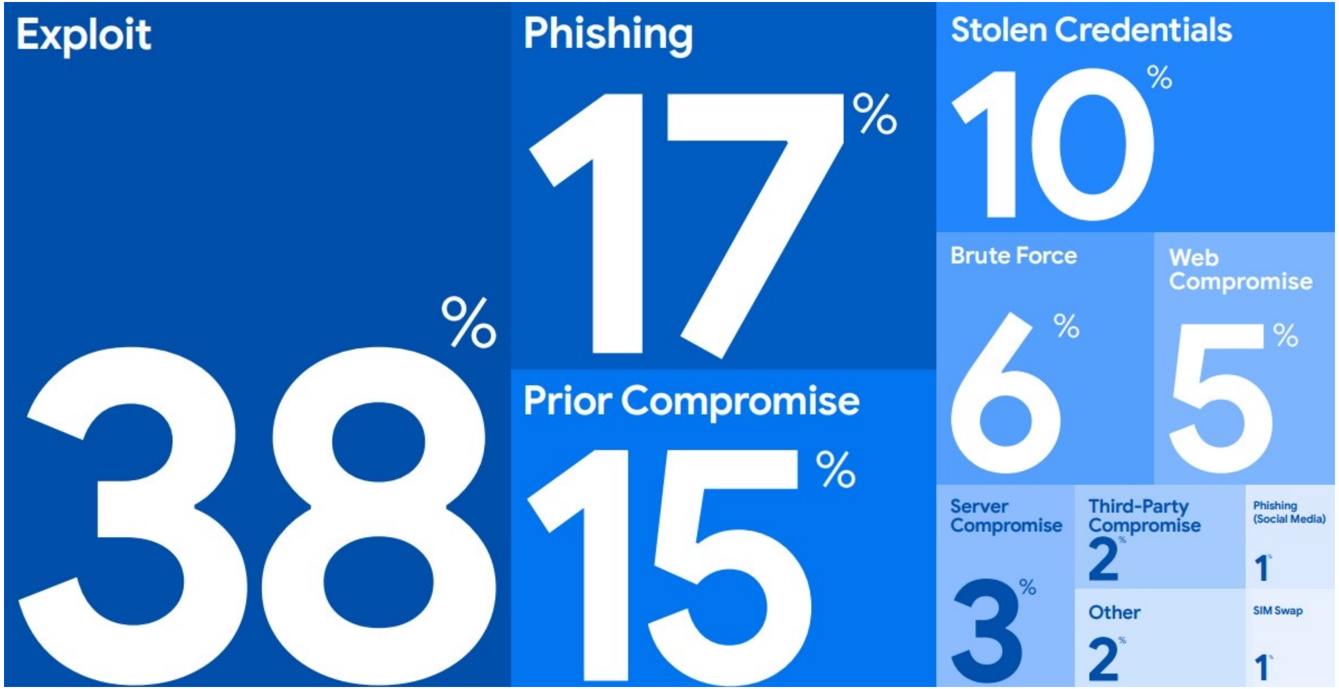
OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT, synopsys.com

Open-source risks are indicative of closed source codebase risks

Distribution Statement A: Approved for Public Release, Distribution Unlimited.

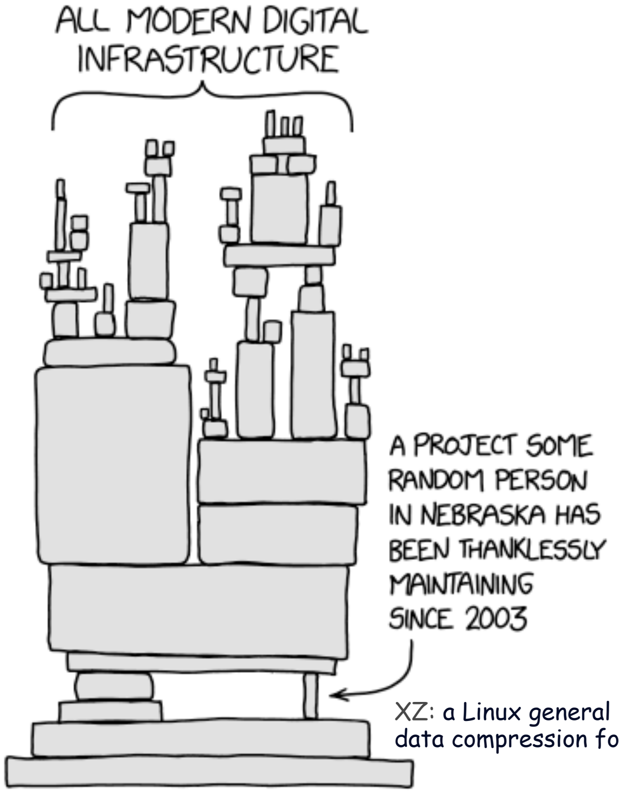
Software vulnerabilities enable ransomware attacks

We depend on software that is pervasively vulnerable and increasingly under attack.
This includes critical infrastructure software where system failure has dire consequences.



Initial Ransomware Infection Vector, “Mandiant M-Trends 2024”

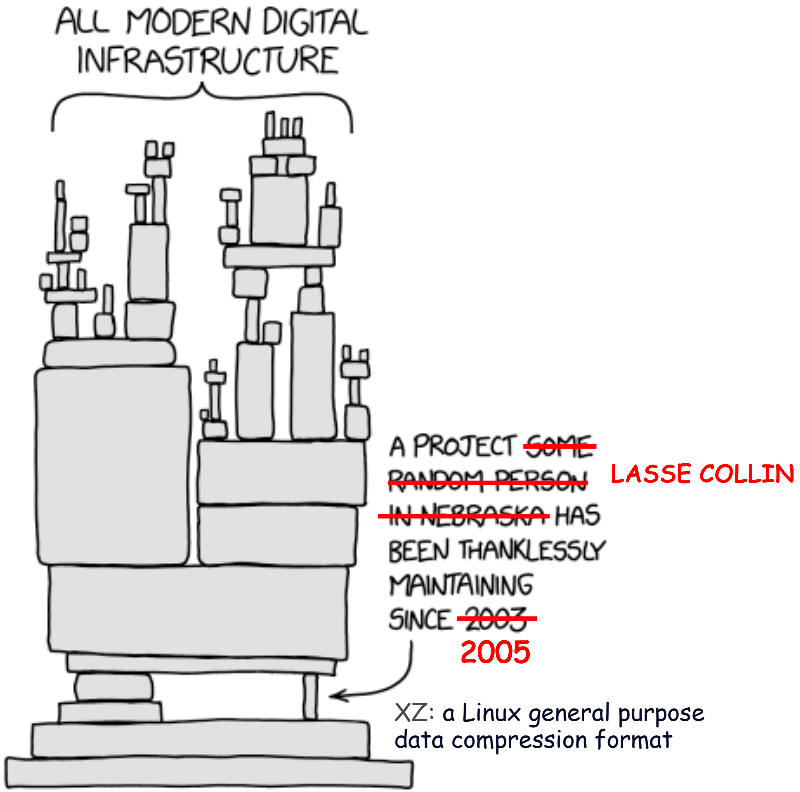
Some guy in Nebraska


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

XZ: a Linux general purpose data compression format

https://xkcd.com/2347/

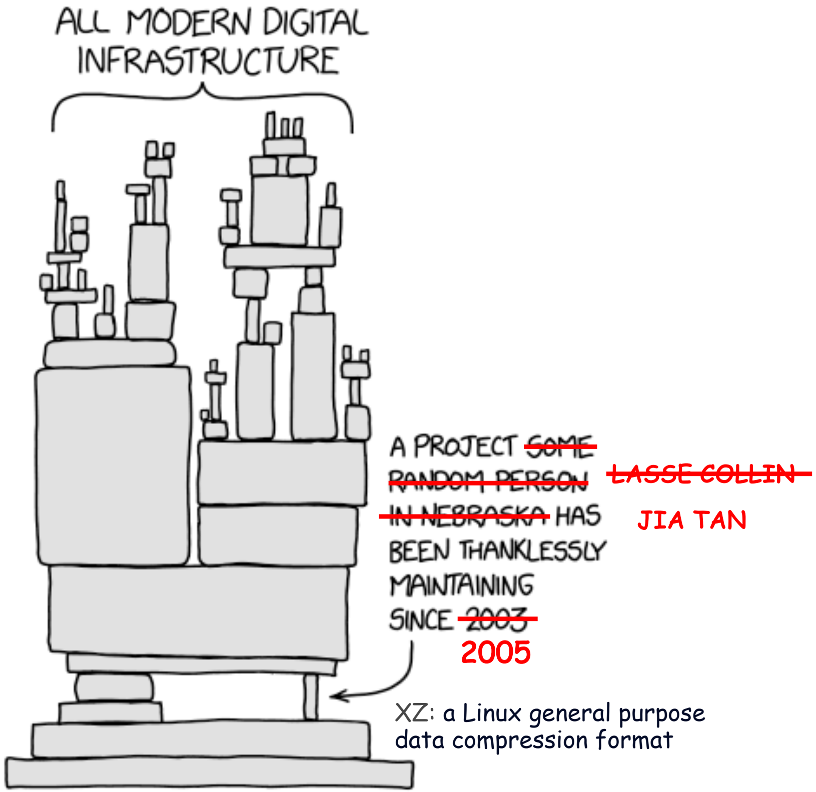
Some guy in Nebraska


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT ~~SOME RANDOM PERSON IN NEBRASKA~~ HAS BEEN THANKLESSLY MAINTAINING SINCE ~~2003~~
LASSE COLLIN
2005

XZ: a Linux general purpose data compression format

https://xkcd.com/2347/

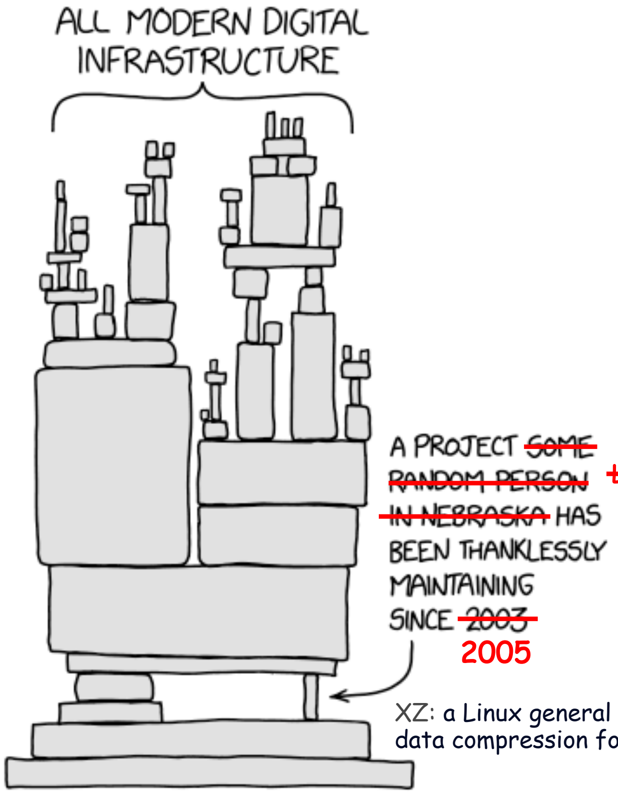
Some guy in Nebraska


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT ~~SOME RANDOM PERSON IN NEBRASKA~~ HAS BEEN THANKLESSLY MAINTAINING SINCE ~~2003~~
~~LASSE COLLIN~~
JIA TAN
2005

XZ: a Linux general purpose data compression format

https://xkcd.com/2347/

Some guy in Nebraska


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT ~~SOME RANDOM PERSON IN NEBRASKA~~ HAS BEEN THANKLESSLY MAINTAINING SINCE ~~2003~~

~~LASSE COLLIN~~

JIA TAN

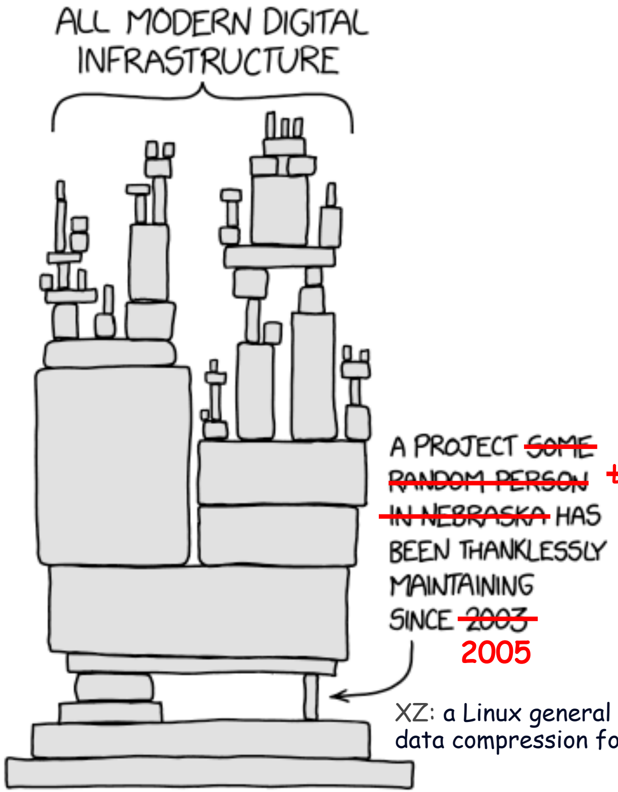
VOUCHED BY FIVE OTHER GITHUB USERS

2005

XZ: a Linux general purpose data compression format

https://xkcd.com/2347/

Some guy in Nebraska


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT ~~SOME RANDOM PERSON IN NEBRASKA~~ HAS BEEN THANKLESSLY MAINTAINING SINCE ~~2003~~

~~LASSE COLLIN~~

~~JIA TAN~~

VOUCHED BY FIVE
OTHER GITHUB USERS

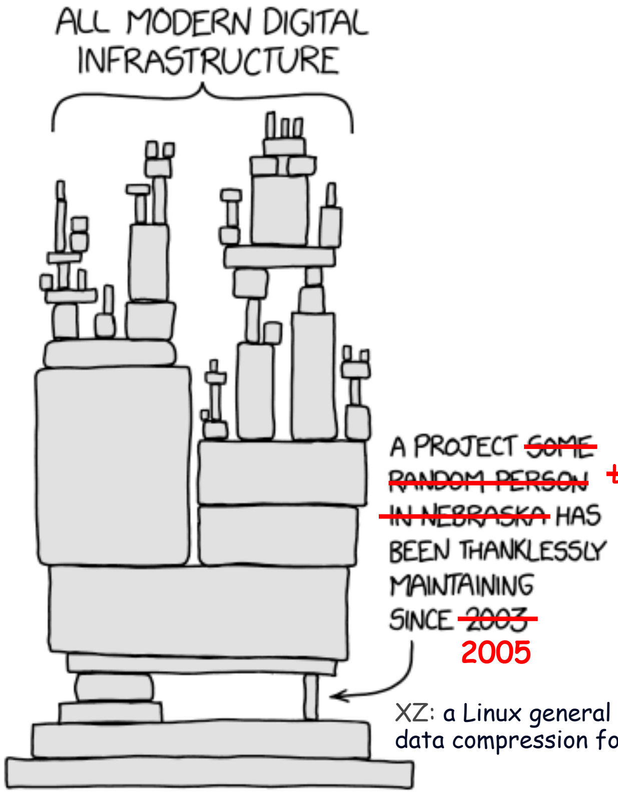
SOME RUSSIAN GUY

2005

XZ: a Linux general purpose
data compression format

https://xkcd.com/2347/

Some guy in Nebraska


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT ~~SOME RANDOM PERSON IN NEBRASKA~~ HAS BEEN THANKLESSLY MAINTAINING SINCE ~~2003~~

~~LASSE COLLIN~~

~~JIA TAN~~

VOUCHED BY FIVE
OTHER GITHUB USERS

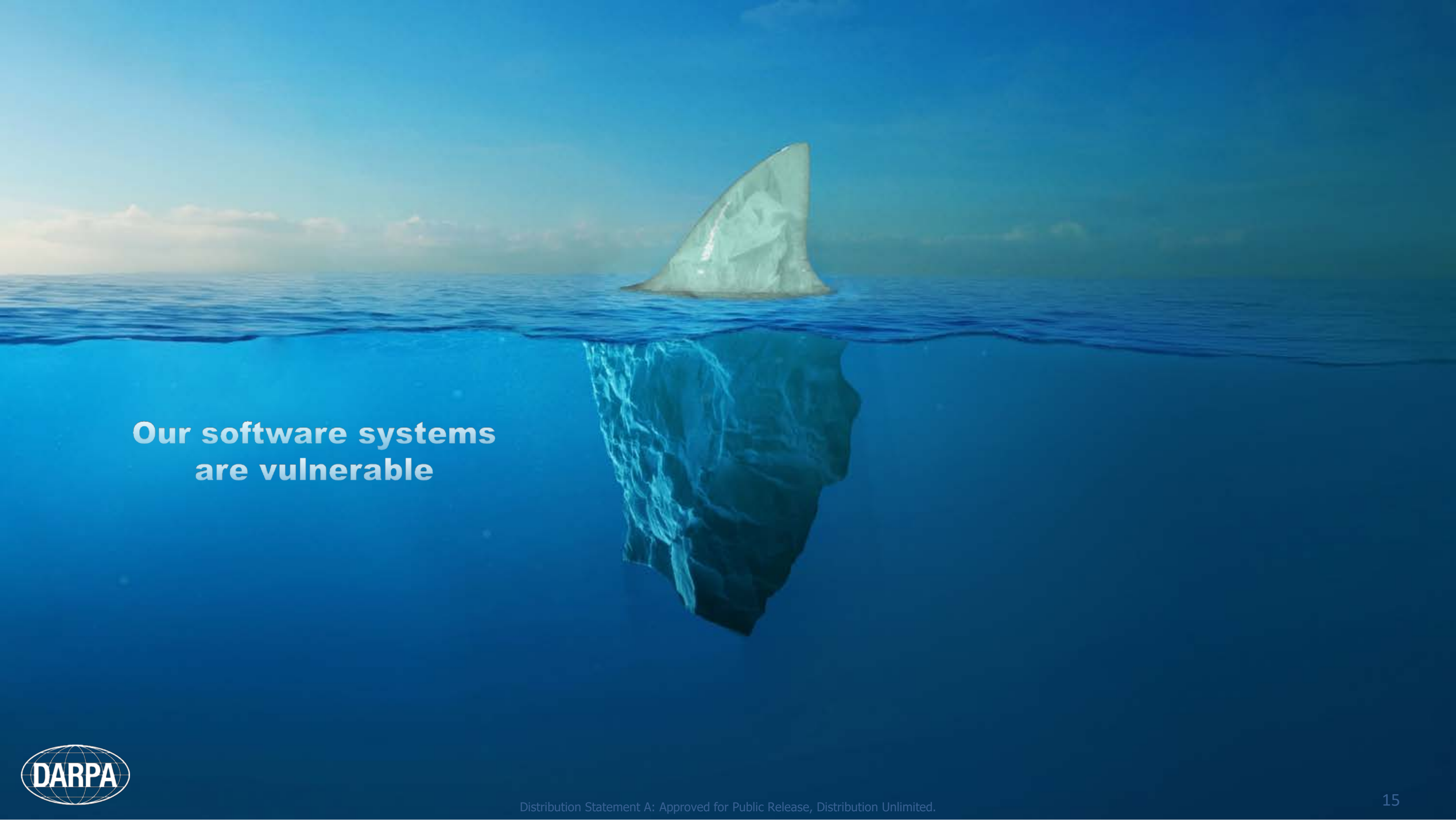
~~SOME RUSSIAN GUY~~

ANDRES FREUND,
A SOFTWARE ENGINEER AT MICROSOFT

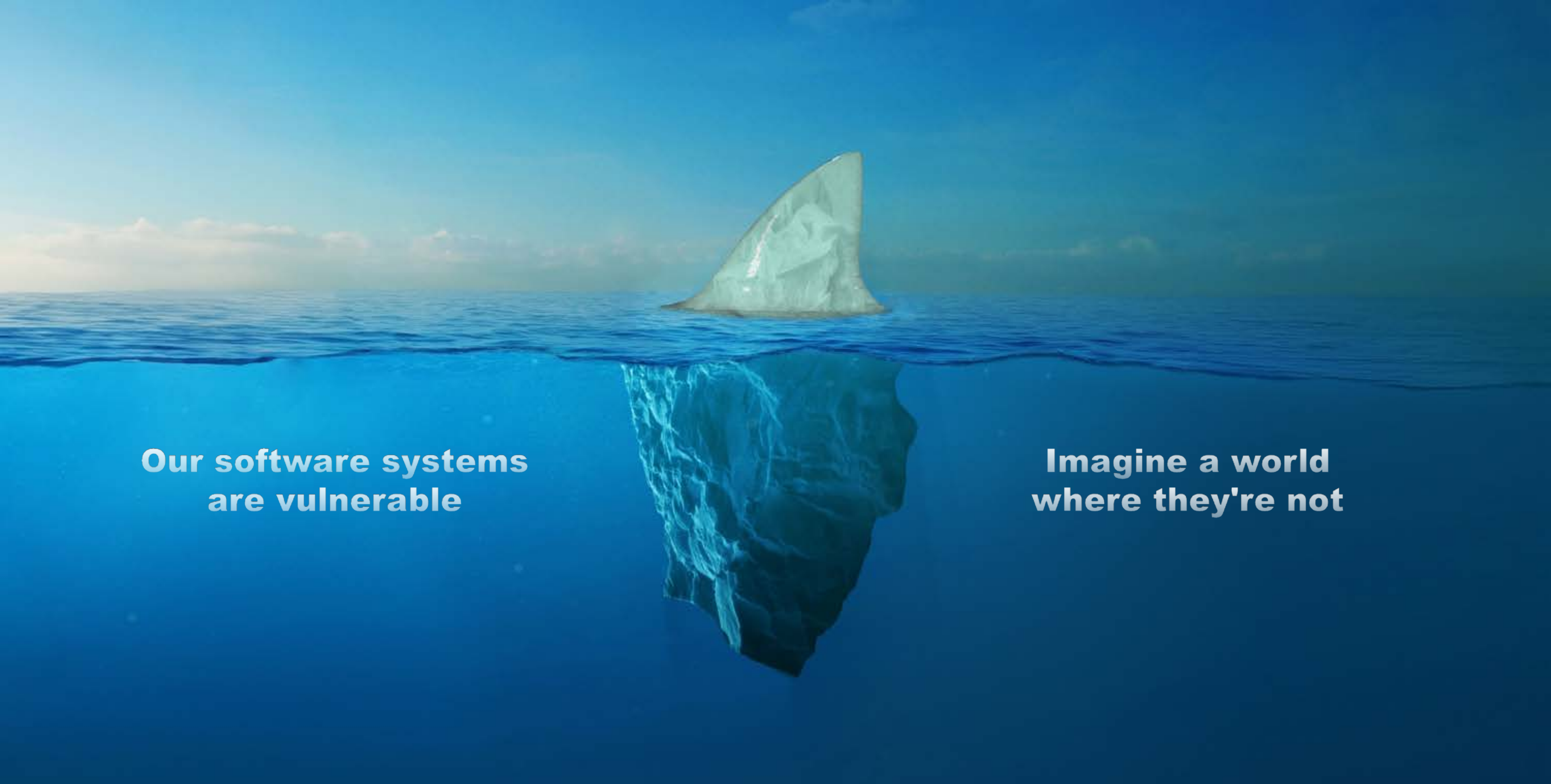
2005

XZ: a Linux general purpose
data compression format

https://xkcd.com/2347/



Our software systems are vulnerable



Our software systems are vulnerable

Imagine a world where they're not

DARPA investment in formal methods for resilient software systems

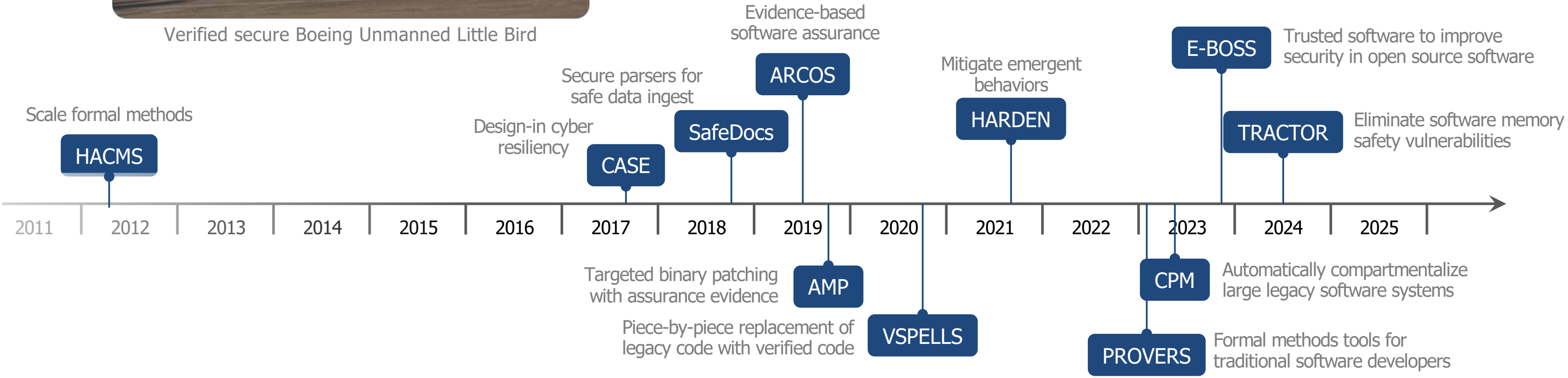
High Assurance Cyber Military Systems (HACMS)

Skilled red teams were unable to compromise HACMS hardened platform

Verified secure Boeing Unmanned Little Bird

DARPA has delivered formal methods tools to make our software inherently less "hackable"

- Ingest data safely
- Block exploitation
- Make secure code easy to write
- Fix bugs in legacy systems



HACMS: Scale formal methods

CASE: Design-in cyber resiliency

SafeDocs: Secure parsers for safe data ingest

ARCOS: Evidence-based software assurance

AMP: Targeted binary patching with assurance evidence

VSPELLS: Piece-by-piece replacement of legacy code with verified code

HARDEN: Mitigate emergent behaviors

PROVERS: Formal methods tools for traditional software developers

CPM: Automatically compartmentalize large legacy software systems

E-BOSS: Trusted software to improve security in open source software

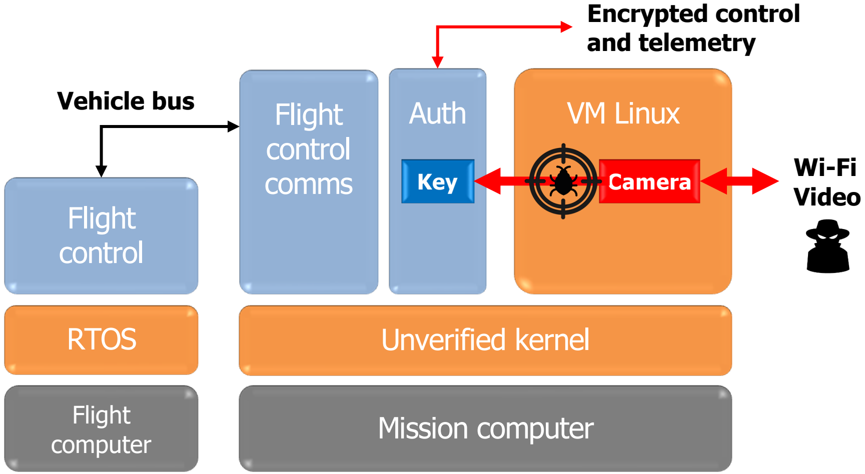
TRACTOR: Eliminate software memory safety vulnerabilities

HACMS: What's the "magic"?

Before

Unverified unsecure

Keys were overwritten and a nefarious ground station took control



Encrypted control and telemetry

Vehicle bus

Flight control

RTOS

Flight computer

Flight control comms

Auth

Key

VM Linux

Camera

Wi-Fi Video

Unverified kernel

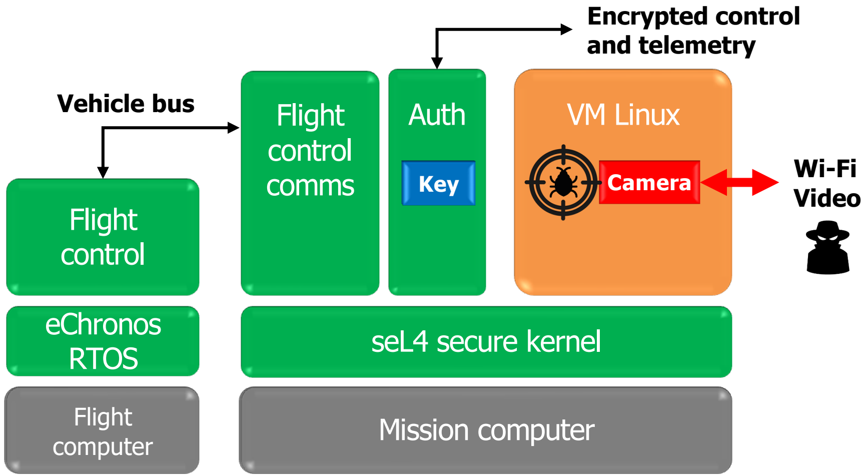
Mission computer

HACMS: What's the "magic"?

After

Verified secure

Skilled red teams were **unable** to compromise HACMS hardened platform



Formal methods provide rigorous correctness guarantees to make hardware and software systems inherently more secure

- Architecture Analysis and Design Language (AADL)
  - SAE international standard
  - Used for design documentation, analyses, or code generation
    - Verify that a selected hardware and software architecture meets timing requirements
    - Guarantee that a resource can communicate only though a single trusted path (no backdoors)
- Separation kernel
  - Security through isolation
- Verified parser
  - Eliminate 80% of data ingest vulnerabilities

Formal methods at Amazon Web Services (AWS)

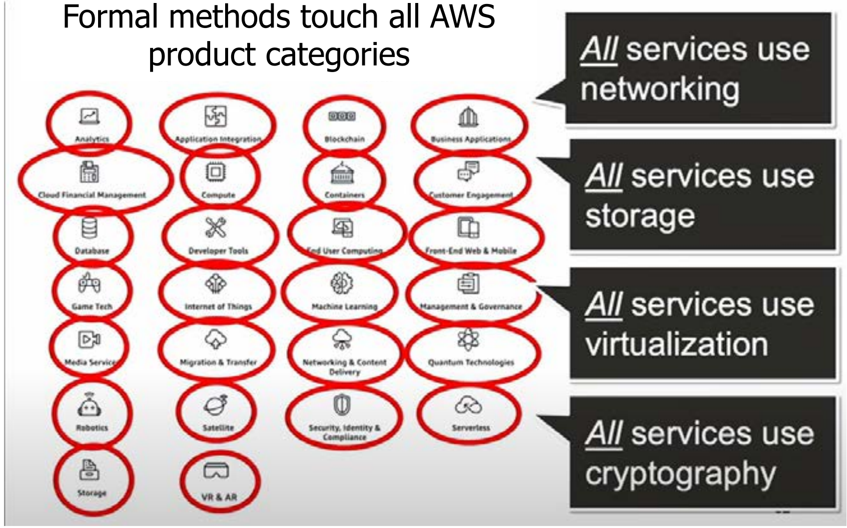
An unexpected discovery – Formal methods makes systems more efficient and easier to maintain

Lessons learned

- Formally verified code is often more performant than the unverified code it replaces
  - Runs faster
  - Faster to deploy
  - Easier to update, modify, and operate
- Convincing managers to invest in security is hard, but to invest in performance is easier

Any good software will evolve. Its proof needs evolve automatically as well, e.g., PROVERS – *Byron Cook, AWS*

Formal methods touch all AWS product categories



AWS uses formal methods tools pioneered by I2O

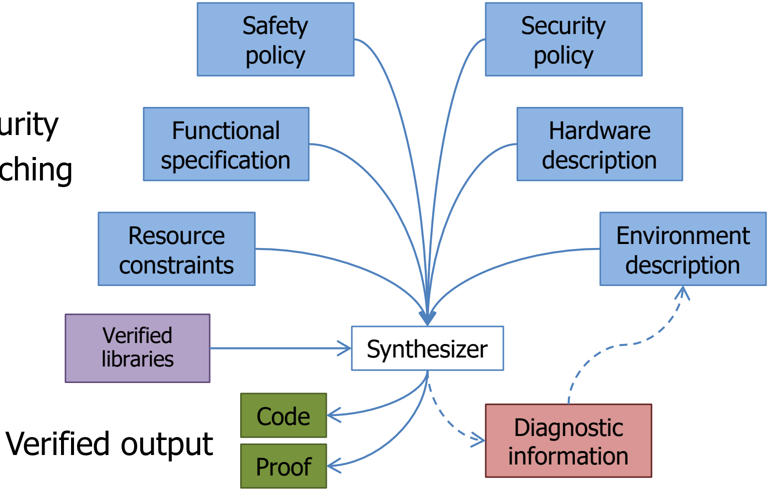
https://aws.amazon.com/blogs/security/an-unexpected-discovery-automated-reasoning-often-makes-systems-more-efficient-and-easier-to-maintain/

Wide spectrum of formal methods

- Architectural analysis
- Assured parsing
- Encryption best practices
- Memory safety
- Hardware support for security
- Metadata for fast bug patching

Formal methods allow you to answer:

What CAN the system do?
What WILL the system do?
What can the system NEVER DO?



Systems can be automatically correct by construction throughout their lifecycle, including maintenance

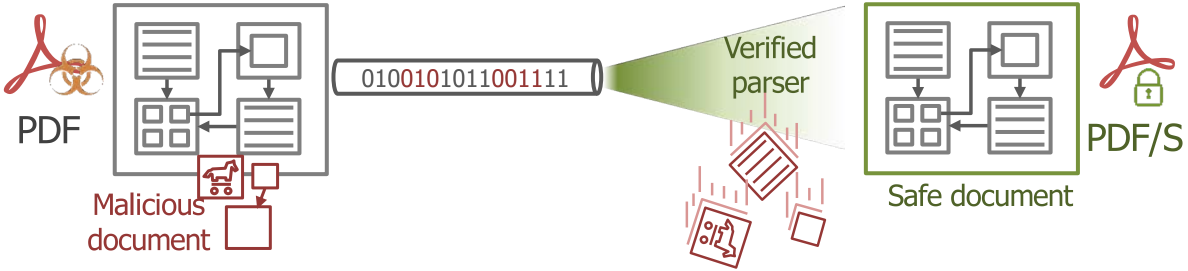
Two things you can do right away

1. Use automated verified parsers for safe data ingest. Never hand craft a parser.
2. Use RUST for memory safety. Rust is actually a theorem prover that tricks programmers into doing proofs of memory safety.

https://www.theregister.com/2025/01/07/interview_with_aws_byron_cook/

Automating verified parsers

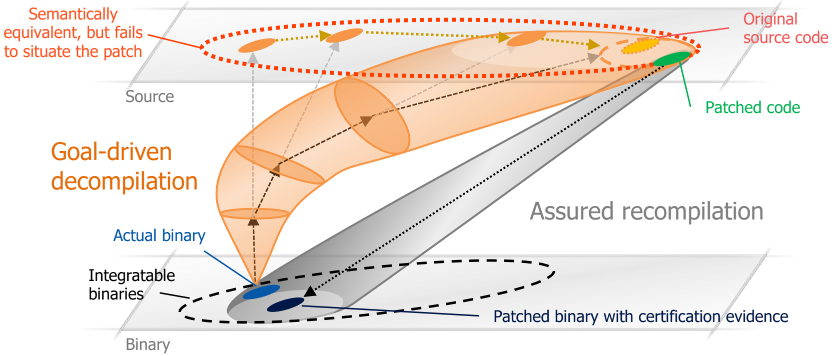
Safe Documents (SafeDocs)



Safe data ingest

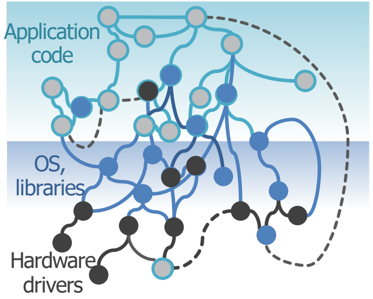
Patching with guarantees

Assured Micropatching (AMP)


Semantically equivalent, but fails to situate the patch
Original source code
Source
Patched code
Goal-driven decompilation
Assured recompilation
Actual binary
Integratable binaries
Patched binary with certification evidence
Binary

Targeted security patches with strong guarantees

Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS)



Legacy code base

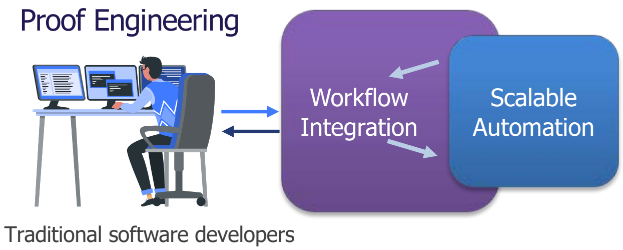
1. *Untangle*
2. *Separate*
3. *Recover abstractions*
4. *Re-implement*
5. *Flatten and verify*

Piece-by-piece replacement of legacy code with verified code

Distribution Statement A: Approved for Public Release, Distribution Unlimited.

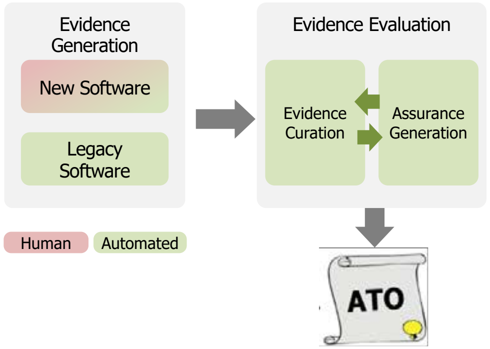
Automating the assurance pipeline

Pipelined Reasoning Of Verifiers Enabling Robust Systems (PROVERS)



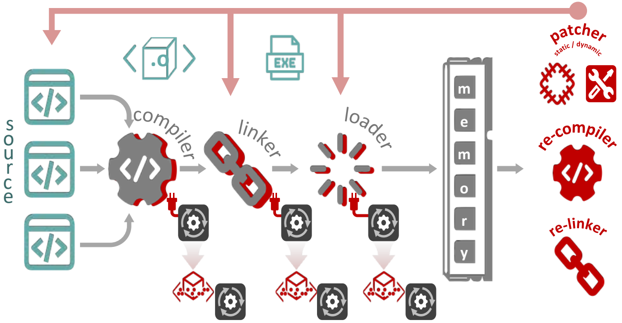
Build formal methods tools for traditional software developers

Automated Rapid Certification of Software (ARCOS)



Evidence-based software assurance

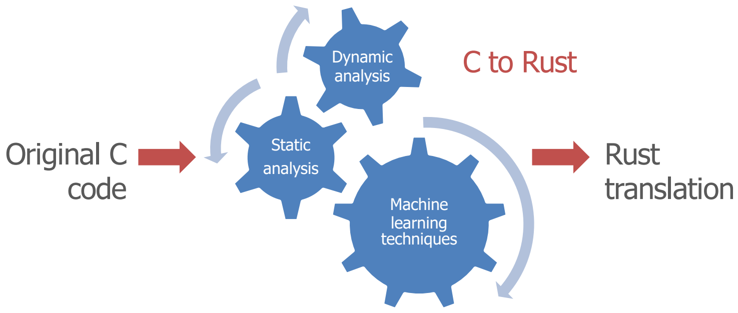
Enhanced SBOM for Optimized Software Sustainment (E-BOSS)



Build trusted software to improve security in open source software

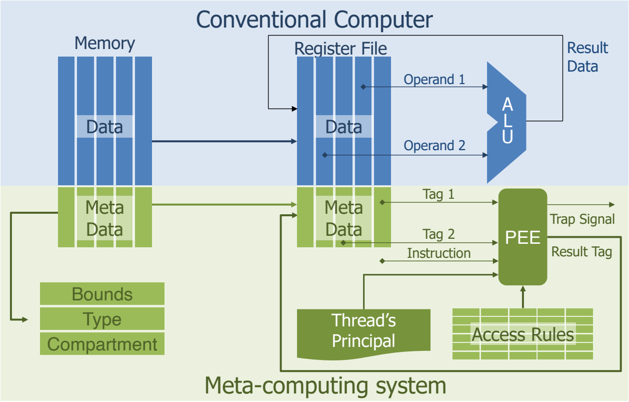
Memory safety and compartmentalization

TRanslating All C TO Rust (TRACTOR)



Eliminate software memory safety vulnerabilities

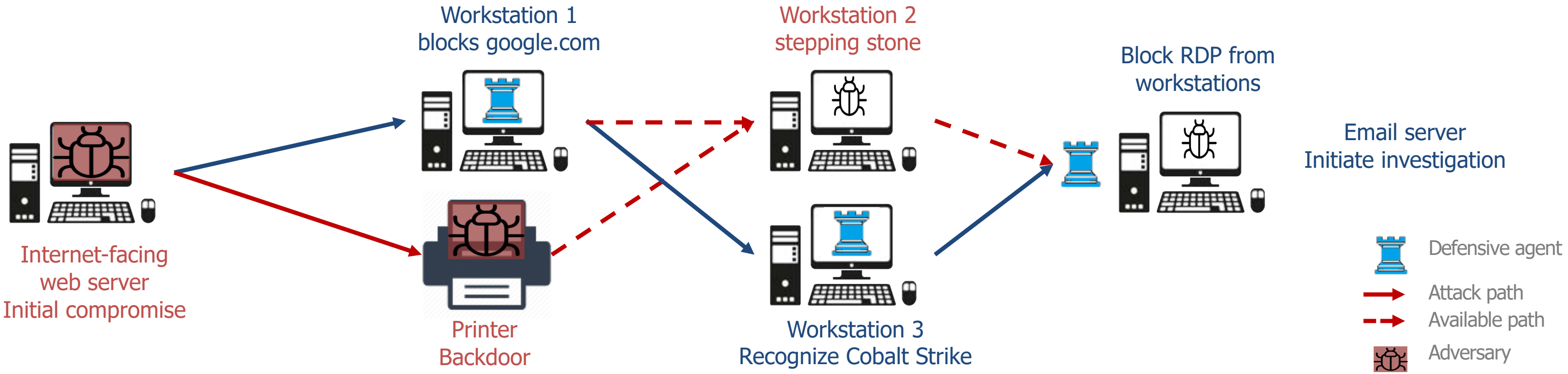
Compartmentalization and Privilege Management (CPM)



Automatically compartmentalize large legacy software systems

AI-enabled cyber agents

Develop an AI-toolkit to instantiate realistic network environments and train cyber agents to enable resilient network operations against advanced persistent threats (APTs)



Cyber Agents for Security Testing and Learning Environments (CASTLE)

Approach

- Purple team: Build open, evolving, and adversarial RL environments resembling actual networks
- Blue team: Enable resilient network workflows vs. APT threats via trained agents
- Red team: Mimic APTs with representative threats to support blue agent training

Automatically find and fix software vulnerabilities

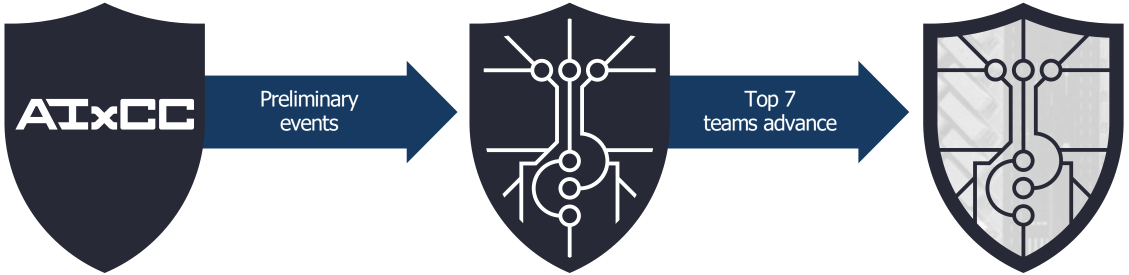
AI Cyber Challenge

Inter-agency collaboration between DARPA and the Advanced Research Projects Agency for Health (ARPA-H)

Announced
August 2023

Semifinals completed
11 Aug 2024

Finals to be held
Aug 2025



OPEN TRACK AND SMALL BUSINESS TRACK SUBMISSIONS

SEMIFINALS
Top 7 teams $2 million each

FINALS
1st: $4 Million
2nd: $3 Million
3rd: $1.5 Million

ANTHROPIC   OpenAI   Google   Microsoft   THE LINUX FOUNDATION   OpenSSF OPEN SOURCE SECURITY FOUNDATION

Industry Collaborators

Automatically find and fix software vulnerabilities

AI Cyber Challenge

Semifinals completed
11 Aug 2024

Finals to be held Aug 2025

- **42** teams competed
- **5** challenge projects (Linux Kernel, Jenkins, Nginx, SQLite3, and Apache Tika)
- **22** unique synthetic vulnerabilities discovered by competitor Cyber Reasoning Systems (CRS)
- **15** vulnerabilities patched by competitor CRSs
- **1** real-world zero-day vulnerability discovered and responsibly disclosed

We live in “interesting” AI times

OpenAI

ChatGPT: Optimizing Language Models for Dialogue

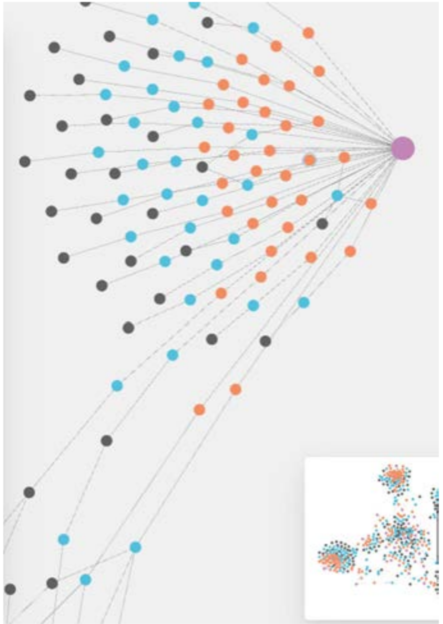
We’ve trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer followup questions, admit its mistakes, challenge incorrect premises, and reject inappropriate equests. ChatGPT is a sibling model to InstructGPT, which is d to follow an instruction in a prompt and provide a onse.

Leon Neal/Getty Images

- AI will make cyber attacks easier
- AI will make defending systems easier
- How will the balance of power shift?

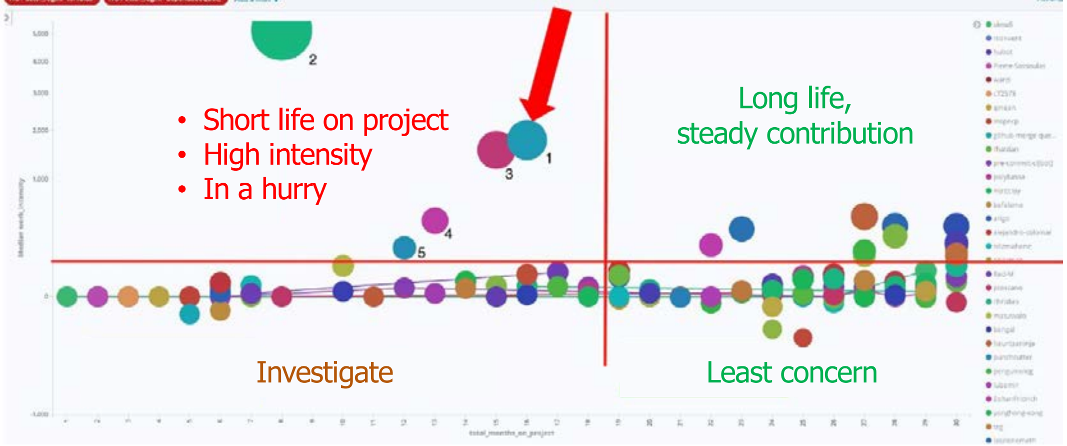
Detect and mitigate open source sabotage

Situational awareness of critical shared areas of the software supply chain



Graph view providing understanding of technology contributors including organizations and their collaborations

Infiltrator pattern scan



- Short life on project
- High intensity
- In a hurry

Long life,
steady contribution

Investigate

Least concern

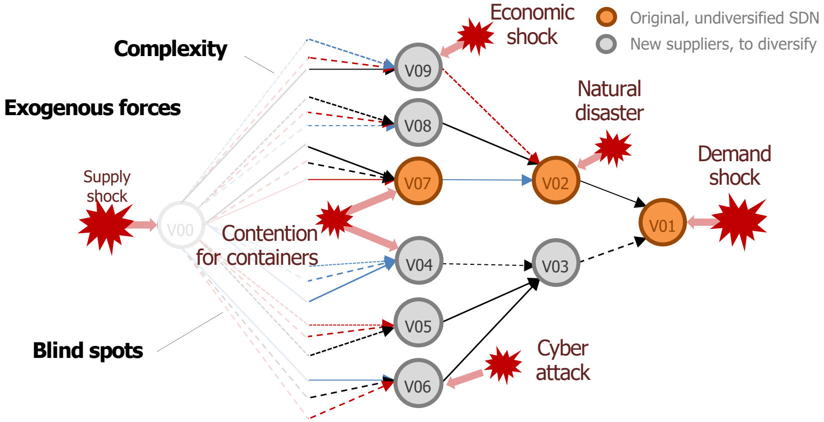
Pattern scan identifies XZ project where a backdoor introduced by Jia Tan (JiaT75) infiltrator – discovered in Mar 2024

SocialCyber: Hybrid AI to Protect Integrity of Open Source Code

Distribution Statement A: Approved for Public Release, Distribution Unlimited.

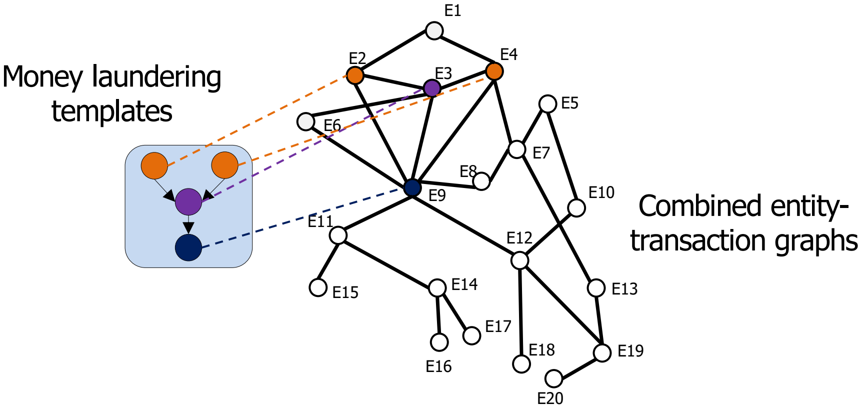
Resilient, anticipatory, and adaptive networks

Resilient Supply-and-Demand Networks (RSDN)



Supply and demand network (SDN) risk and resilience

Anticipatory and Adaptive Anti-money Laundering (A3ML)



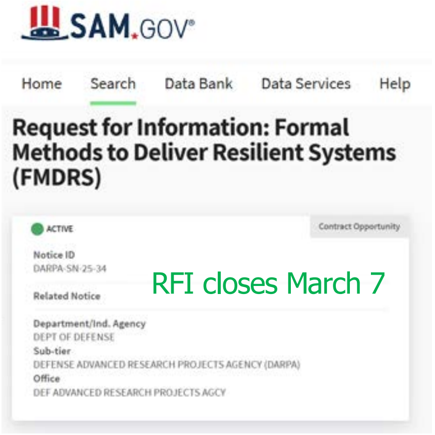
Money laundering templates
Combined entity-transaction graphs
E1
E2
E3
E4
E5
E6
E7
E8
E9
E10
E11
E12
E13
E14
E15
E16
E17
E18
E19
E20

Detect robust and resilient hidden networks

Transition plan to industry

Develop a framework for broad adoption of high-assurance software standards, methods, and tools

- Convened round table discussions with Defense Industrial Base
- Formed partnership with USD(R&E), USD (A&S), DOT&E
  - Conduct cyber resiliency capstone pilot projects
  - Issue a Best Practices Guide for successful cyber resiliency systems and platforms
  - Develop various sustainment models and mechanisms
- Incentivize proposers to incorporate resilient software requirements into proposals
  - Issued RFI for DARPA Guide to Formal Methods to Deliver Resilient Systems for Proposals
- Hold a formal methods colloquium June 17, 2025



SAM.GOV®

Home Search Data Bank Data Services Help

Request for Information: Formal Methods to Deliver Resilient Systems (FMDRS)

● ACTIVE

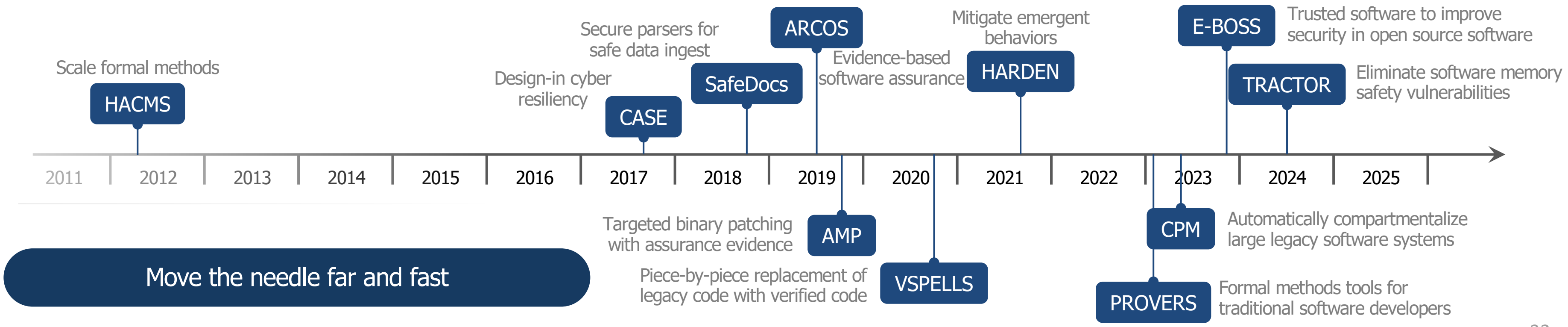
Contract Opportunity

Notice ID
DARPA-SN-25-34

Related Notice

Department/Ind. Agency
DEPT OF DEFENSE
Sub-tier
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)
Office
DEF ADVANCED RESEARCH PROJECTS AGCY

RFI closes March 7



HACMS: Scale formal methods

CASE: Design-in cyber resiliency

SafeDocs: Secure parsers for safe data ingest

ARCOS: Evidence-based software assurance

AMP: Targeted binary patching with assurance evidence

VSPELLS: Piece-by-piece replacement of legacy code with verified code

HARDEN: Mitigate emergent behaviors

PROVERS: Formal methods tools for traditional software developers

CPM: Automatically compartmentalize large legacy software systems

E-BOSS: Trusted software to improve security in open source software

TRACTOR: Eliminate software memory safety vulnerabilities

Move the needle far and fast

www.darpa.mil

Imagine a world without software vulnerabilities

- Eliminate the acceptance of vulnerable software within the DoD as an unavoidable risk
- Rapidly secure the software for critical systems within the DoD
- Implement a rapid artifact-based ATO process to keep frontline systems secure
- Create the critical mass of formal methods service companies, tools, and training

Working with DARPA

- Become a Program Manager

- Respond to a solicitation:
  - Program-specific Broad Agency Announcements (BAAs) released throughout the year
  - Office-wide BAAs for one or two years with general tech-office scope
  - Research announcements for grants or cooperative agreements
  - Funding durations and amounts vary based on objectives
  - Concept studies can be 6 to 12 months
  - Program and study funding amounts are based on proposed research level of effort

- Leverage DARPAConnect's resources

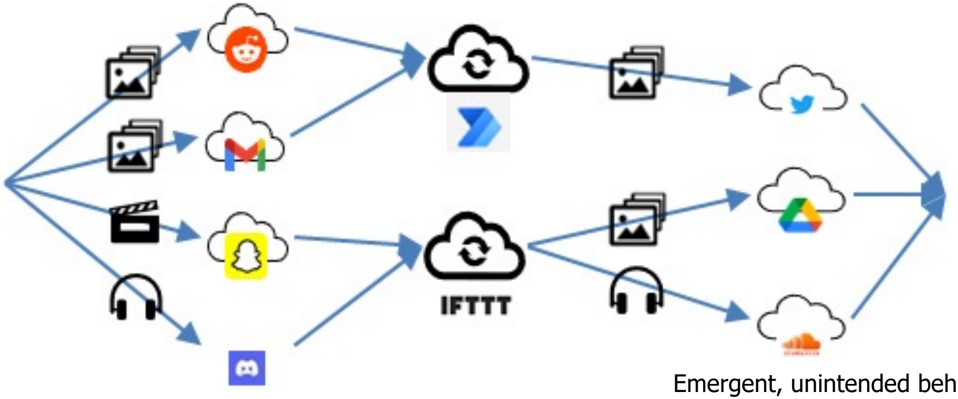
- Sign up for I2O's mailing list: sign up at darpa.mil/i2o

- Attend I2O Resilient Systems Colloquium, June 17, 2025

DARPAConnect.us

Deploy and detect robust and resilient hidden networks

Provably Weird Network Deployment and Detection (PWND2)



Emergent, unintended behavior at specific network entities can evade adversary detection and defenses

Resilient communications