MOSAICS
2020
INDUSTRY
DAY

RunSafe SECURITY

RunSafe Security BLUF

1. RunSafe is about attack prevention, based on experience as attackers for USG.

2. RunSafe's Alkemist® immunizes software at run-time without software developer friction, reducing the attack surface and increasing mission success of weapon systems, Enterprise IT, and OT devices.

3. Alkemist randomizes where in memory functions and basic blocks are loaded. Alkemist implementation makes each instance of software functionally identical but logically unique, meaning attackers can't locate vulnerabilities.

RunSafe SECURITY

Vulnerabilities Exist in Compiled Code

Scanning and patching alone means your defenses have a severe gap.

40% of CVEs in Compiled Code Are Memory Related (1,2)

- Their CVSS rating is higher than non-memory CVEs
- The likelihood of having a public exploit script is higher

Static Testing Does Not Flag Memory CVE's (1)

- 2.5% Linux Memory CVEs were found during static testing
- The CVEs that were found, took a median of 567 days to get fixed

Patching Is Painful for Everyone and Too Slow

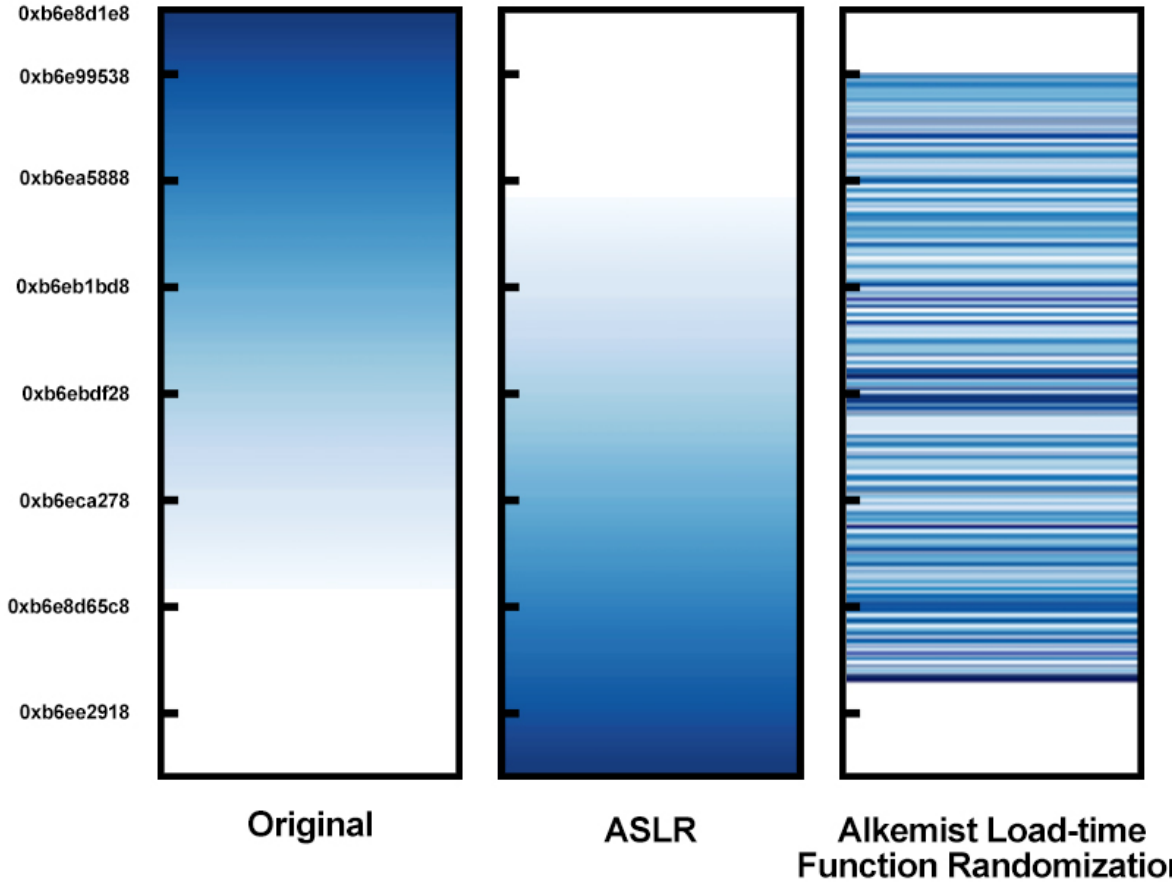
- Disruptive to your developers and your operators/customers
- Reactive to known vulnerabilities only

(1): Unpublished study led by Dr. Laurie Williams, North Carolina State University 2020
(2): MITRE Sep-2019 report: "Top 25 Most Dangerous Software Errors"

MOSAICS
2020
INDUSTRY
DAY

RunSafe SECURITY

Change the Memory; Cripple the Attack



Alkemist's transformation method delivers real time protections to dramatically enhance security.

How Alkemist Works

- Vulnerable to Zero-Day Attacks

✓ Protections applied directly to device code

✓ Passively Blocks Zero-Day Exploits (memory corruption)

Alkemist is seamlessly integrated into the software development life cycle.

MOSAICS

2020 INDUSTRY DAY

RunSafe SECURITY

RunSafe Fits OT Environment

1. Legacy Device Friendly
    a) Do not need source code
    b) Do not need additional compute resources

2. Smooths Patch Cycle
    a) Provides protection before patching possible
    b) Addresses unknown vulnerabilities

3. Cyber Expertise Not Required
    a) Automated tool
    b) Widely applicable

MOSAICS
2020
INDUSTRY
DAY

RunSafe SECURITY

Alkemist Success Stories

VERTIV

Avocent Core Insight™
Embedded Management Systems
(Based on OpenBMC)

- Significant Constraints
  - Ultra Low RAM
  - Ultra Slow Processor
  - Over 1,150 binaries
- Performance Preserved
  - Functionality not impacted
  - Zero runtime impact

TRL: 9

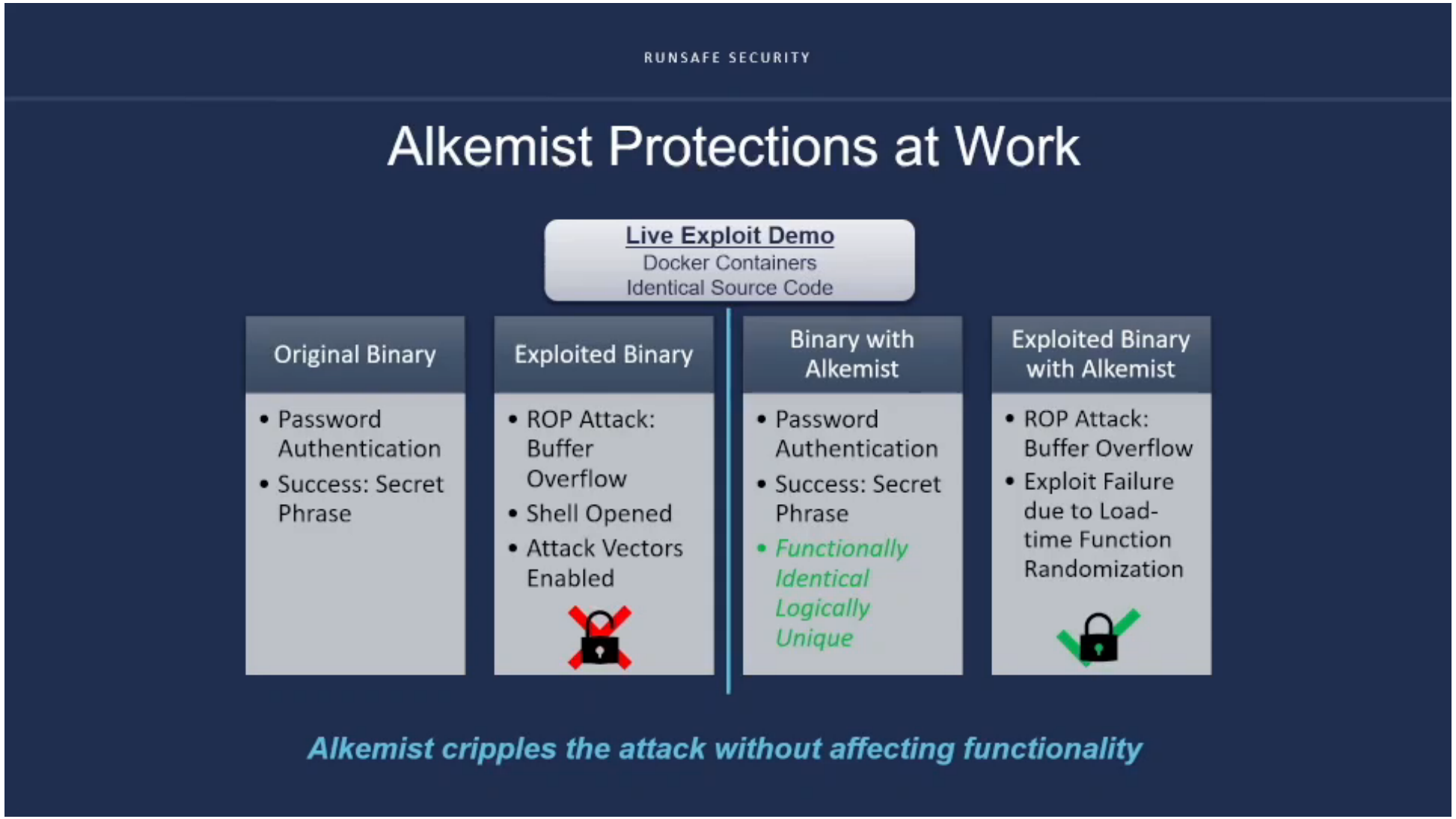
NAVAIR

Cyber Warfare Directorate

- Operational engine, CH-53K (King Stallion) and comm'l, e.g. dual use
- Harden GE38 FADEC (full authority digital engine control)
  - Key Attack Surface
  - 70% of functions transformed; Over 2^{32} possible unique binaries
- GE high-fidelity testing shows no change to performance and functionality

TRL: 6

Exploit Demonstration – Embedded Video



MOSAICS
2020
INDUSTRY
DAY

RunSafe SECURITY

Thank You

Dave Salwen
VP Federal
RunSafe Security, Inc.
202.486.7298
dave@runsafesecurity.com