Toward a “Periodic Table” of Bugs
or
How Can I Really Tell What’s Wrong With My Code?

Paul E. Black, Irena Bojanova, Yaacov Yesha, Yan Wu

NIST, BGSU

12 August 2015

Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor does it imply that the products are necessarily the best available for the purpose.

Outline

- **The “Science” of Weaknesses**
- **Our Nomenclature**
- **Examples of Applying Our Approach**
- **Using This Work**

NIST National Institute of Standards and Technology • U.S. Department of Commerce

Precise Medical Vocabulary

- Medical professionals have terms to precisely name muscles, bones, organs, conditions, diseases, and so forth.

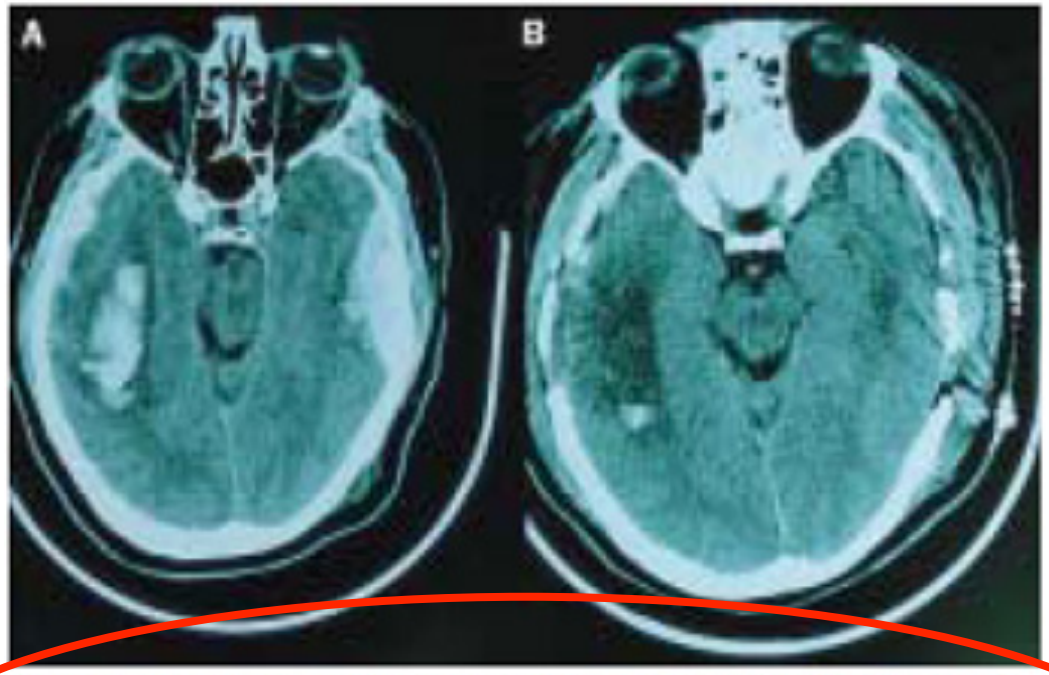


Figure 2: **Computed tomography of a comatose patient with a left temporal epidural haematoma, right parenchymal temporal lobe haematoma, and a right convexity subdural haematoma before and after craniotomy and evacuation of haematomas**

Common Nomenclature

Common Weakness Enumeration (CWE)

- A "dictionary" of every *class* of bug or flaw in software
- More than 600 distinct classes, e.g., buffer overflow, directory traversal, OS injection, race condition, cross-site scripting, hard-coded password, and insecure random numbers

http://cwe.mitre.org/

Common Vulnerability Enumeration (CVE)

- A list of *instances* of security vulnerabilities in software
- More than 9000 CVEs were assigned in 2014
  Heartbleed is CVE-2014-0160
- NIST's National Vulnerability Database (NVD) has fixes, severity ratings, etc. for CVEs

https://cve.mitre.org/

Common Weakness Enumeration (CWE) is a Mess

- **CWE is widely used - by far the best dictionary of software weaknesses. Many tools, projects, etc. are based on CWE.**
- **But definitions are imprecise and inconsistent.**
- **CWEs are "coarse grained": they bundle lots of stuff, like consequences and likely attacks.**
- **The coverage is uneven, with some combinations well represented and others not represented at all.**
- **No mobile weaknesses, eg., battery drain, physical sensors (GPS, gyro, microphone, hi-res camera), unencrypted wireless communication, etc.**

Definitions are Imprecise

- **CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer:**

  "The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer."

  - ***Note that "read from or write to a memory location" is not tied to the buffer!***

NIST National Institute of Standards and Technology • U.S. Department of Commerce

Overflow Has Gaps in Coverage

- **CWE-124: Buffer Underwrite (’Buffer Underflow') and CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vs.**
- **CWE-121: Stack-based Buffer Overflow and CWE-122: Heap-based Buffer Overflow**

- **CWE-127: Buffer Under-read and CWE-126: Buffer Over-read**
- ***but no read-stack and read-heap versions*.**

… and a buncha' others, too

- **CWE-123: Write-what-where Condition**
- **CWE-125: Out-of-bounds Read**
- **CWE-787: Out-of-bounds Write**
- **CWE-786: Access of Memory Location Before Start of Buffer**
- **CWE-788: Access of Memory Location After End of Buffer**
- **CWE-805: Buffer Access with Incorrect Length Value**
- **CWE-823: Use of Out-of-range Pointer Offset**

Path Traversal is too Detailed

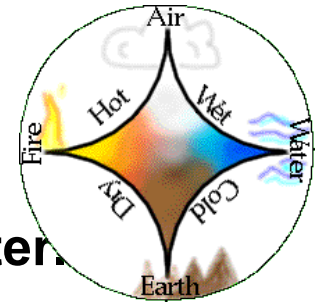
- **CWE-23: Relative Path Traversal**
- **CWE-24: Path Traversal: '../filedir'**
- **CWE-25: Path Traversal: '/../filedir'**
- **CWE-26: Path Traversal: '/dir/../filename'**
- **CWE-27: Path Traversal: 'dir/../../filename'**
- **CWE-28: Path Traversal: '..\filedir'**
- **CWE-29: Path Traversal: '\..\filename'**
- **CWE-30: Path Traversal: '\dir\..\filename'**
- **CWE-31: Path Traversal: 'dir\..\..\filename'**
- **CWE-32: Path Traversal: '...' (Triple Dot)**
- **CWE-33: Path Traversal: '....' (Multiple Dot)**
- **CWE-34: Path Traversal: '..../'**
- **CWE-35: Path Traversal: '.../.../'**

Other Bug Descriptions Have Problems, Too.

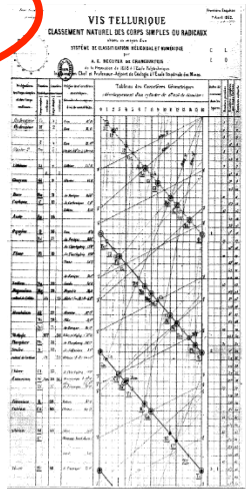
- **Software Fault Patterns (SFP)**
  - **“factor” weaknesses into parameters, but**
  - **don’t include upstream causes or consequences,**
  - **and are based solely on CWEs.**
- **Semantic Templates**
  - **collect CWEs into four general areas**
    - **Software-fault**
    - **Weakness**
    - **Resource/Location**
    - **Consequences**
  - **but are guides to aid human comprehension.**

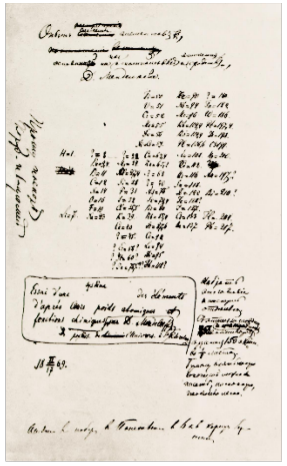
We don’t (yet) know the best structure for bug descriptions.

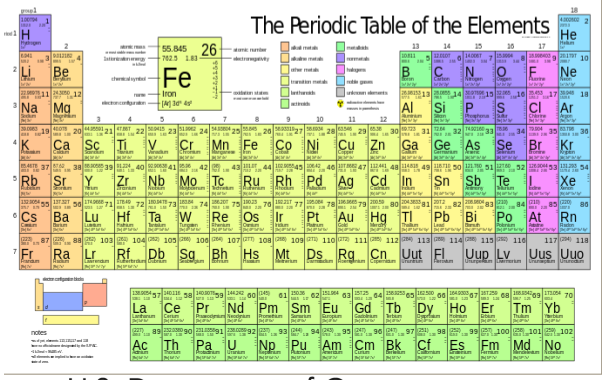
Periodic Table Took Centuries



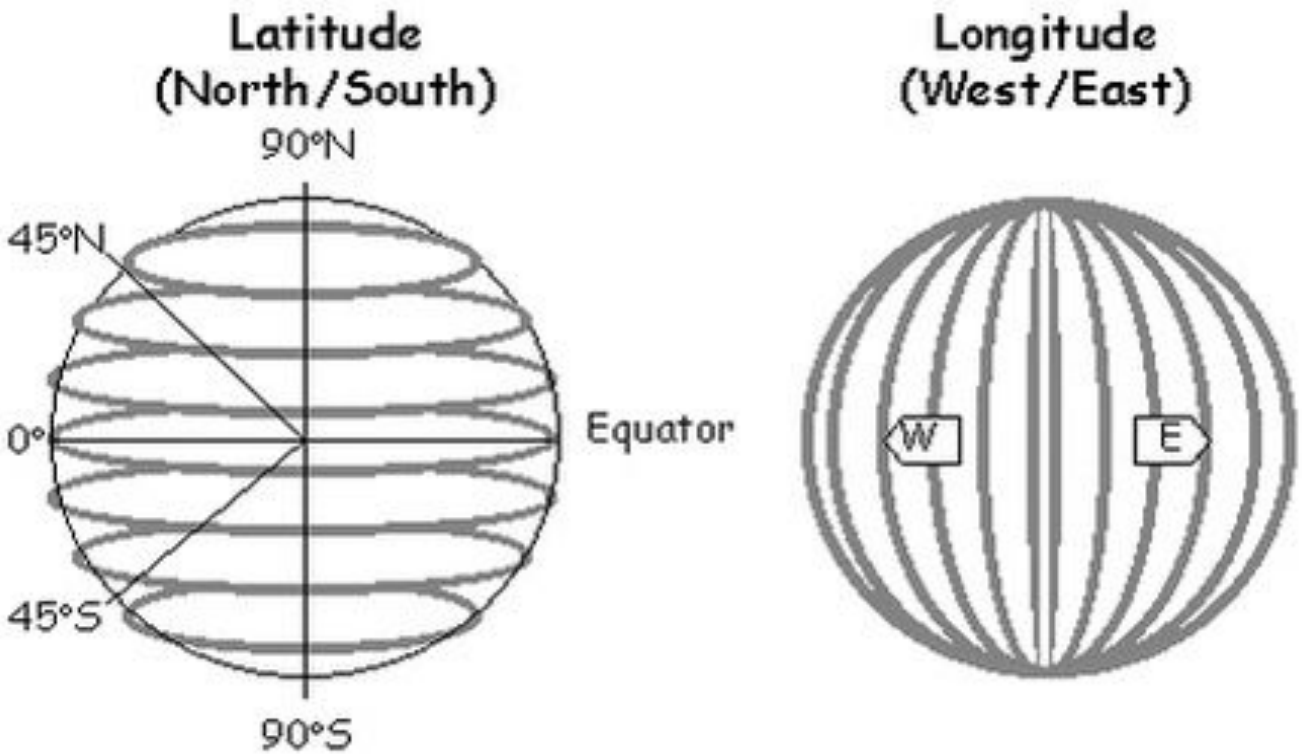
- Greeks used the terms *element* and *atom*.
- Aristotle: everything is a mix of Earth, Fire, Air, or Water.
- Alchemists in the Middle Ages cataloged materials like alcohol, sulfur, mercury, and salt.
- Lavoisier listed 33 elements and distinguished metals and non-metals.
  - including oxygen, nitrogen, hydrogen, phosphorus, mercury, zinc, sulfur, *light*, and *caloric*.
- Dalton realized "atoms of same element are identical in all respects, particularly weight."
- Mendeleev's table embodied centuries of knowledge that reflects atomic structure and forecast properties of missing elements.





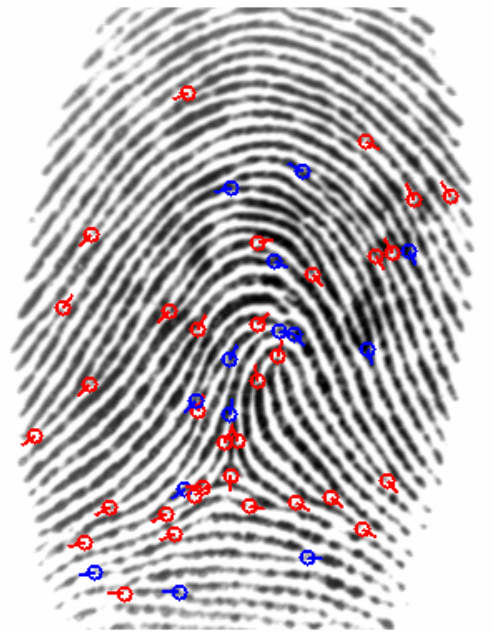


Specify Terrestrial Location with Latitude, Longitude, and Elevation

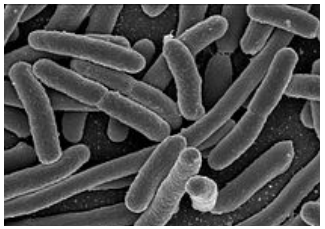


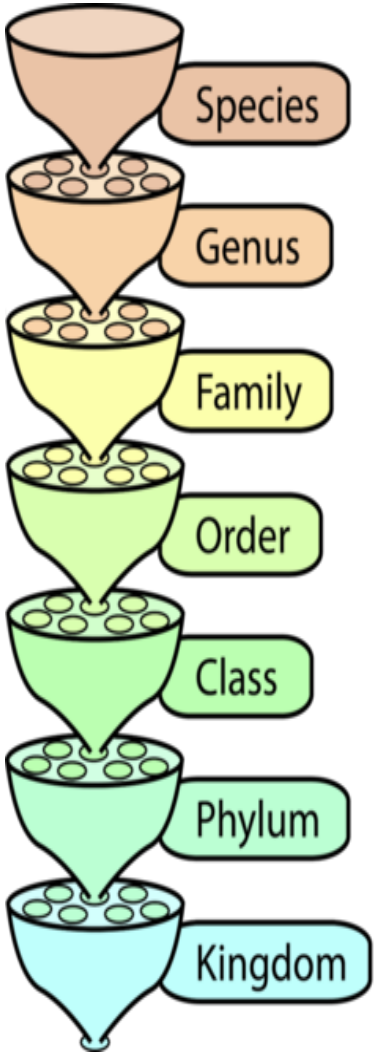
Fingerprints

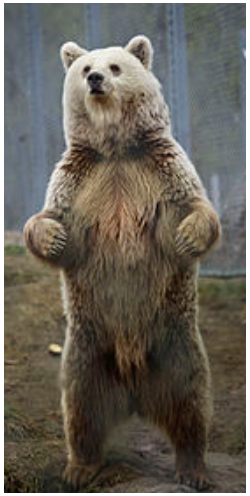
- **Classified as loop, whorl, or arch.**
- **Retrieved by minutia**

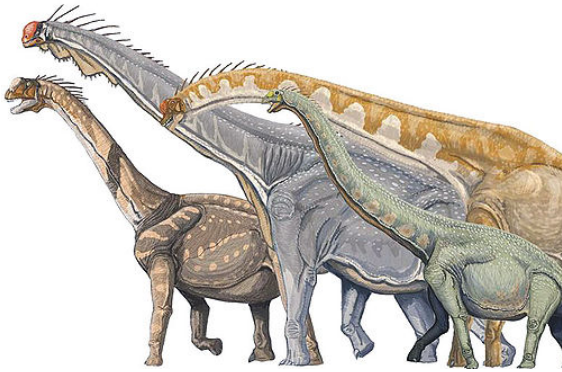


Linnaeus' Taxonomy Categorizes Living Things into a Hierarchy.



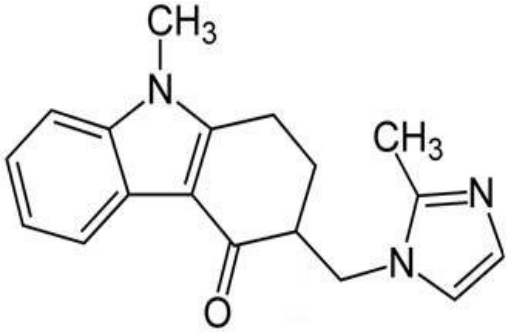






Chemists Have Detailed Systems to Describe Molecules

Zofran ODT is: $C_{18}H_{19}N_3O$



(±) 1, 2, 3, 9-tetrahydro-9-methyl-3-[(2-methyl-1H-imidazol-1-yl)methyl]-4H-carbazol-4-one

Integers Have Prime Factors

$$6 = 2 \times 3$$

$$70 = 2 \times 5 \times 7$$

$$43{,}747{,}298{,}756 = 2 \times 2 \times 7 \times 641 \times 1471 \times 1657$$

Our vision is to have
a precise descriptive language for bugs
organized in a “natural” way.

(e.g., vocabulary, grammar, ontology, etc. whatever best fits the information)

Outline

- The "Science" of Weaknesses
- **Our Nomenclature**
- Examples of Applying Our Approach
- Using This

We Start With Buffer Overflow

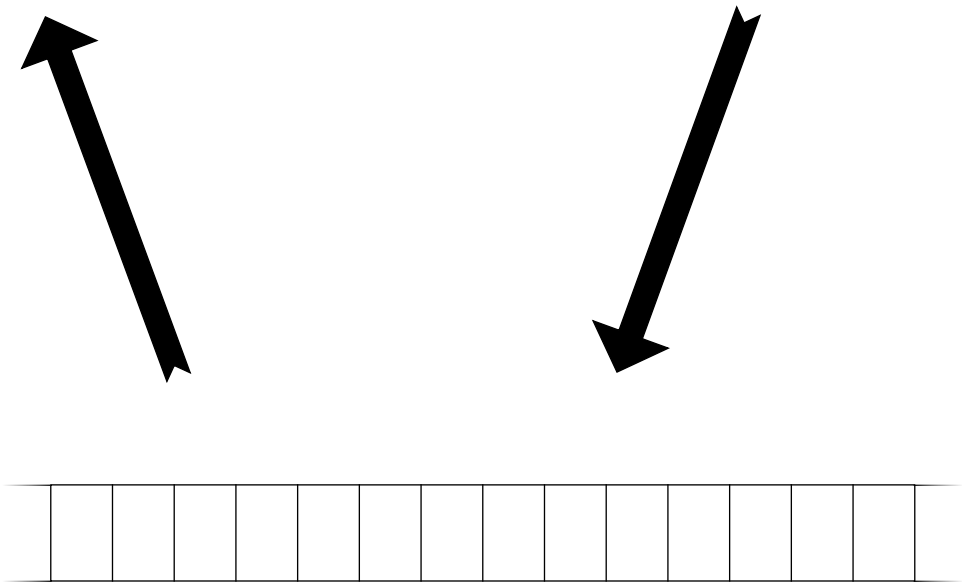
- **Our Definition:**
  The software can access through a buffer a memory location that is not allocated to that buffer.

- **Clearer than CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer: "The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer."**

Buffer Overflow: Attributes

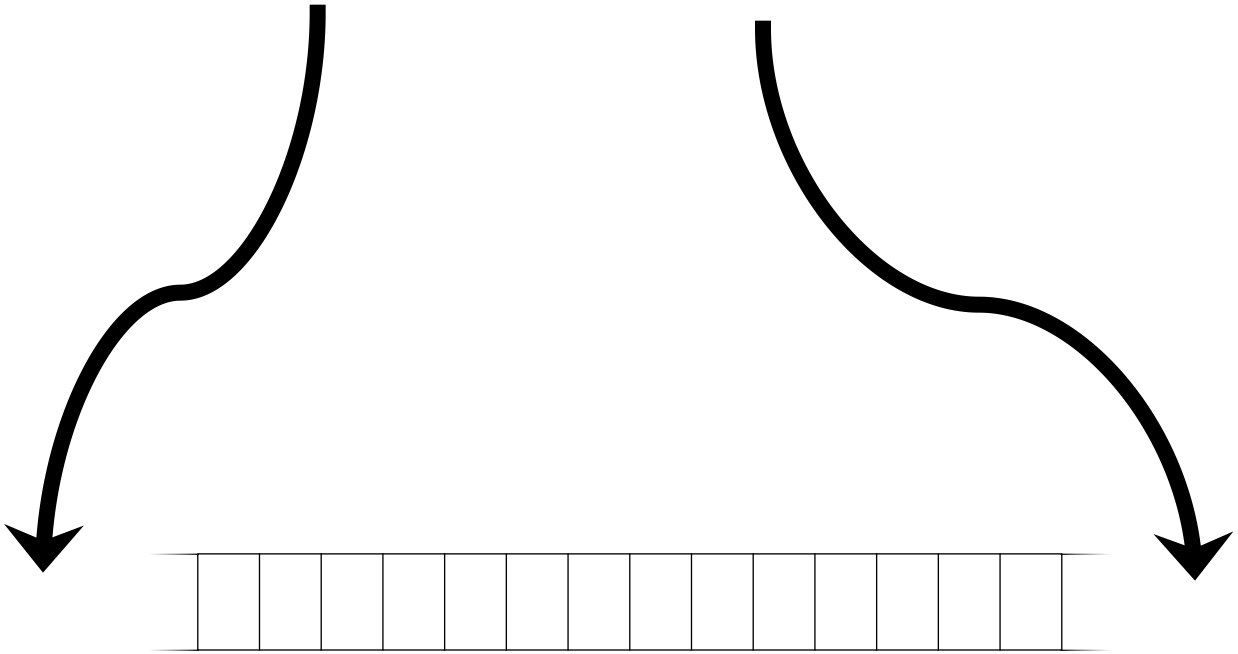
Buffer Overflow: Attributes

- **Access:**
  - **Read, Write.**



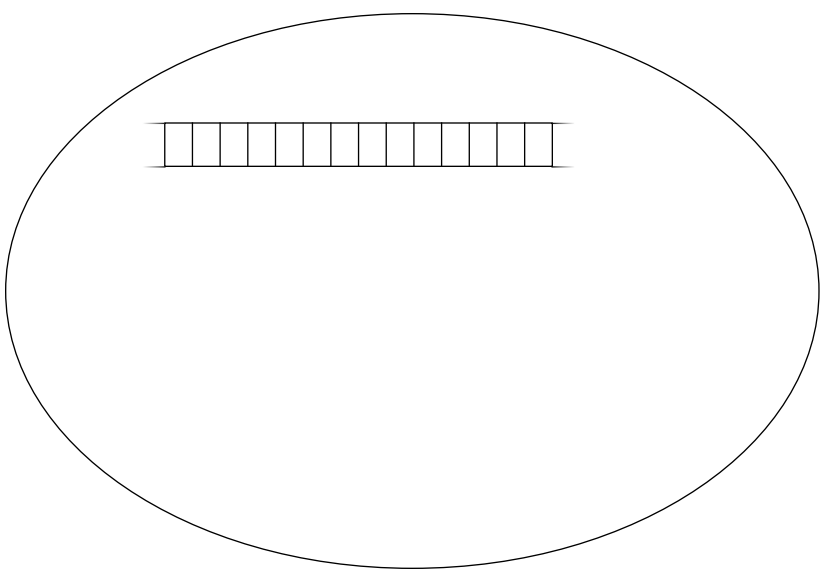
Buffer Overflow: Attributes

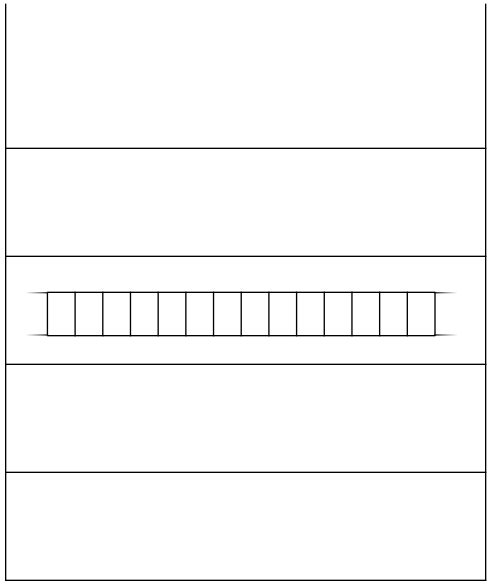
- **Access:**
  - **Read, Write.**
- **Side:**
  - **Below (before, under, or lower), Above (after, over, or upper).**



Buffer Overflow: Attributes

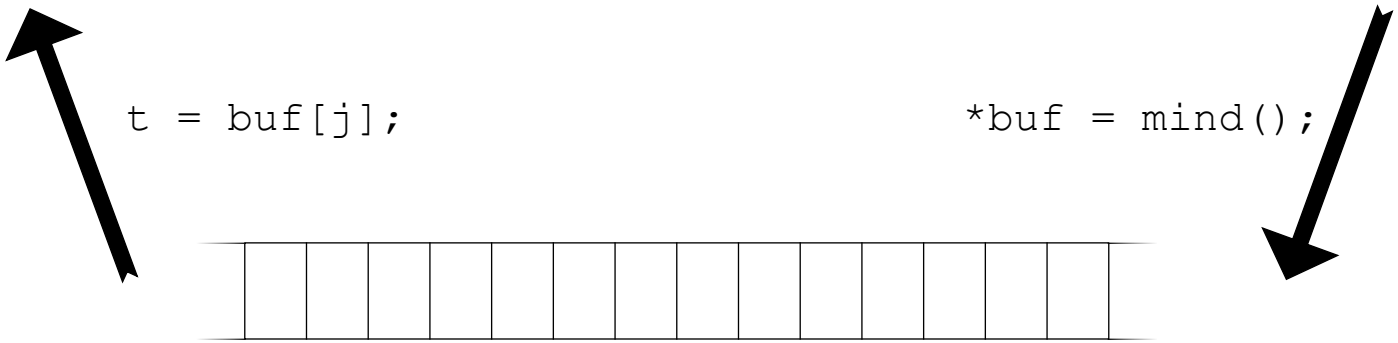
- **Access:**
  - **Read, Write.**
- **Side:**
  - **Below (before, under, or lower), Above (after, over, or upper).**
- **Segment (memory area):**
  - **Heap, Stack, BSS (uninitialized data), Data (initialized), Code (text).**





Buffer Overflow: Attributes

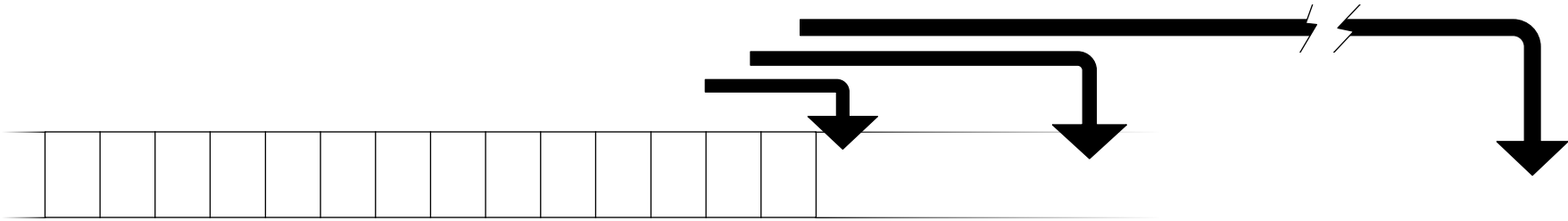
- **Access:**
  - **Read, Write.**
- **Side:**
  - **Below (before, under, or lower), Above (after, over, or upper).**
- **Segment (memory area):**
  - **Heap, Stack, BSS (uninitialized data), Data (initialized), Code (text).**
- **Method:**
  - **Indexed, (bare) Pointer.**



NIST National Institute of Standards and Technology • U.S. Department of Commerce

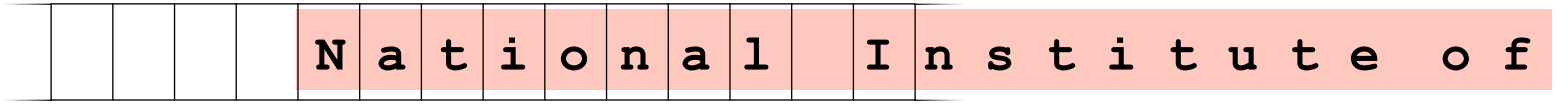
Buffer Overflow: Attributes

- **Access:**
  - **Read, Write.**
- **Side:**
  - **Below (before, under, or lower), Above (after, over, or upper).**
- **Segment (memory area):**
  - **Heap, Stack, BSS (uninitialized data), Data (initialized), Code (text).**
- **Method:**
  - **Indexed, (bare) Pointer.**
- **Magnitude (how far outside):**
  - **Minimal (just barely outside), Moderate, Far (e.g. 4000).**

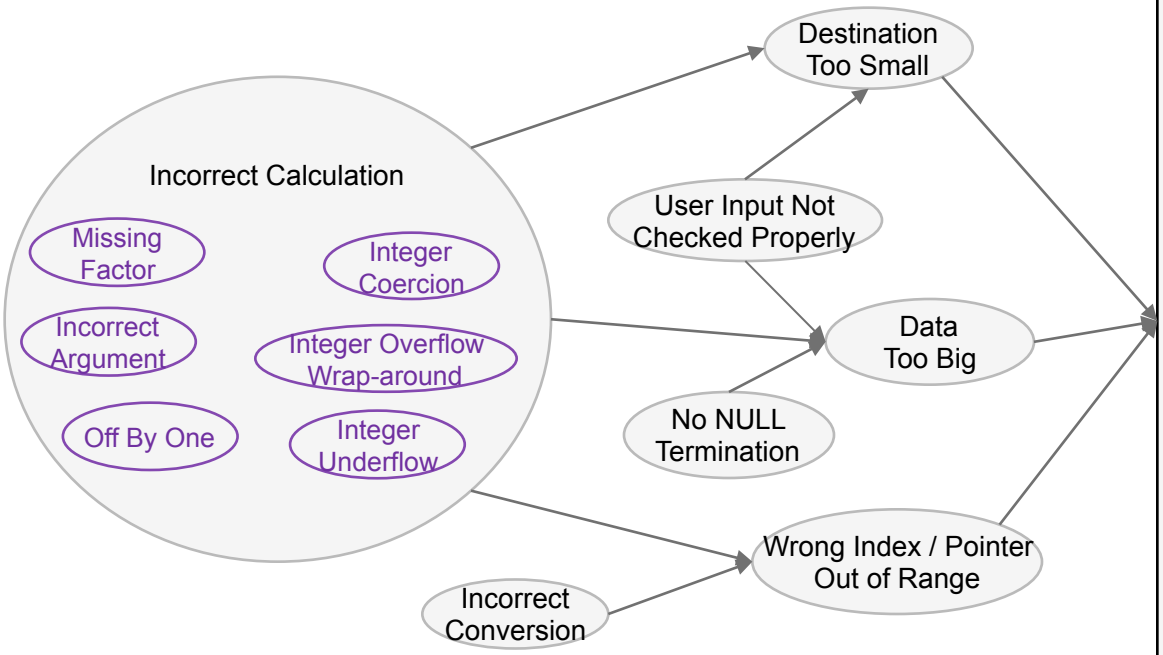


Buffer Overflow: Attributes

- **Access:**
  - **Read, Write.**
- **Side:**
  - **Below (before, under, or lower), Above (after, over, or upper).**
- **Segment (memory area):**
  - **Heap, Stack, BSS (uninitialized data), Data (initialized), Code (text).**
- **Method:**
  - **Indexed, (bare) Pointer.**
- **Magnitude (how far outside):**
  - **Minimal (just barely outside), Moderate, Far (e.g. 4000).**
- **Data Size (how much is outside):**
  - **Minimal, Some (e.g. half dozen), Gazillion.**



Buffer Overflow: Causes



Buffer Overflow

Attributes:

- Access:
  - ✓ *Read*, *Write*.
- Side:
  - ✓ *Below* (before or under), *Above* (after or over)
- Segment (memory area):
  - ✓ *Heap*, *Stack*, *BSS*, *Data* (initialized), *Code* (text)
- Method:
  - ✓ *Indexed*, (bare) *Pointer*.
- Magnitude (how far outside):
  - ✓ *Minimal* (just barely), *Moderate*, *Far* (e.g. 4000).
- Data Size (how much data) :
  - ✓ *Minimal*, *Some*, *Gazillion*.

The graph of causes shows:

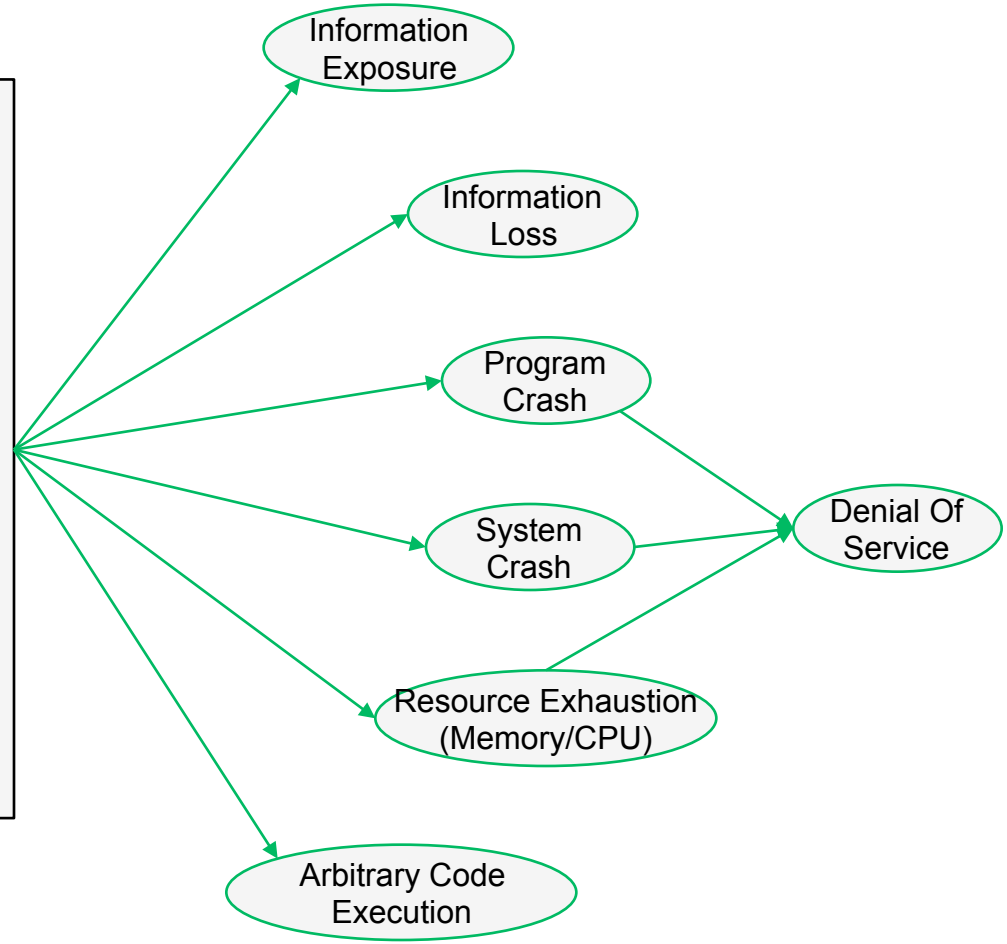
- ➢ There are only 3 proximate causes of buffer overflows:
  - Destination is too small
  - Data is too big
  - Wrong index / pointer out of range.
- ➢ Those 3 have preceding causes that may lead to them.

Buffer Overflow: Consequences

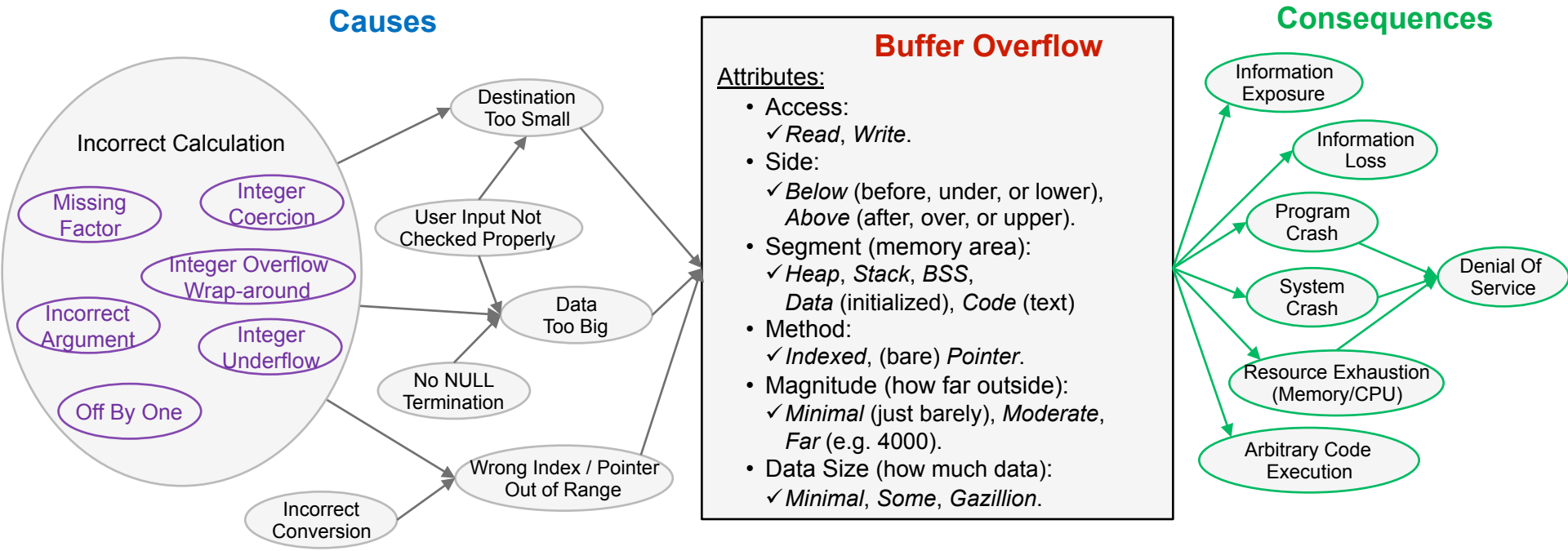
Buffer Overflow

Attributes:

- Access:
  - ✓ *Read*, *Write*.
- Side:
  - ✓ *Below* (before, under, or lower), *Above* (after, over, or upper).
- Segment (memory area):
  - ✓ *Heap*, *Stack*, *BSS* (uninitialized data), *Data* (initialized), *Code* (text)
- Method:
  - ✓ *Indexed*, (bare) *Pointer*.
- Magnitude (how far outside):
  - ✓ *Minimal* (just barely), *Moderate*, *Far* (e.g. 4000).
- Data Size (how much data) :
  - ✓ *Minimal*, *Some*, *Gazillion*.



Buffer Overflow: Causes, Attributes, and Consequences



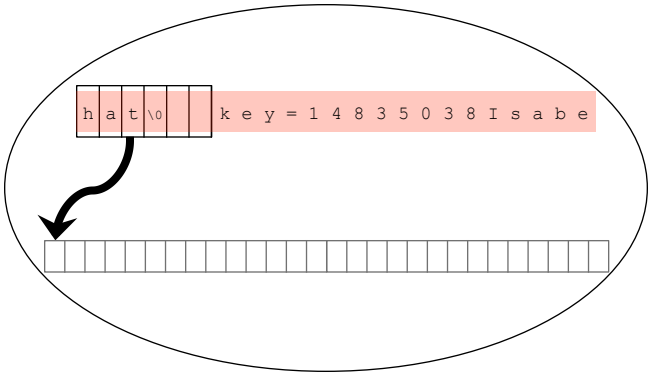
The graph of causes shows:

- There are only 3 proximate causes of buffer overflows:
  - Destination is too small
  - Data is too big
  - Wrong index / pointer out of range.
- Those 3 have preceding causes that may lead to them.

Outline

- The “Science” of Weaknesses
- Our Nomenclature
- **Examples of Applying Our Approach**
- Using This

Example 1: Heartbleed CVE-2014-0160

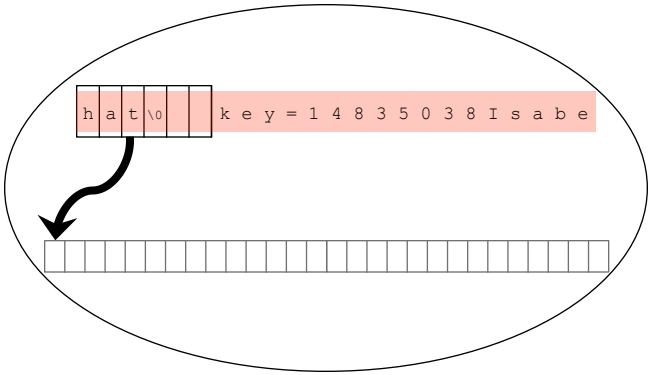


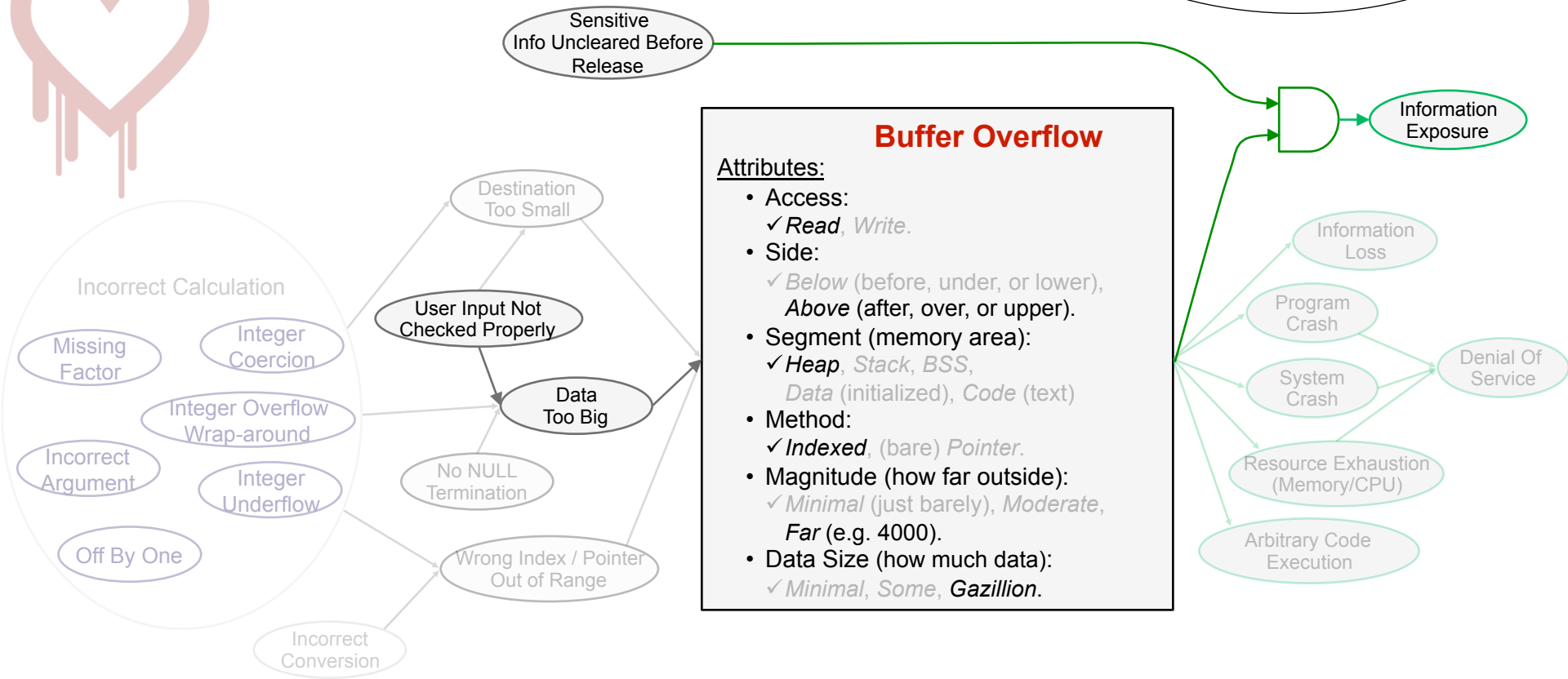
Heartbleed buffer overflow is:

- **caused by *Data Too Big***
- **because of *User Input not Checked Properly***
- **where there was a *Read* that was *After* the end, *Far* outside**
- **reading a *Gazillion* bytes**
- **from a buffer in the *Heap***
- **that may be exploited for *Information Exposure***
- **when enabled by *Sensitive Information Uncleared Before Release (CWE-226)*.**

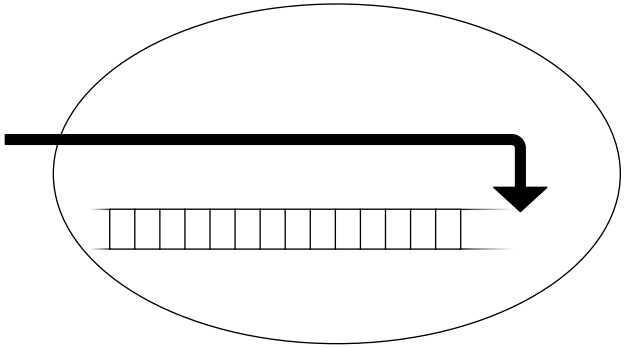
The (1) TLS and (2) DTLS implementations … do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, …

Example 1: Heartbleed CVE-2014-0160





Example 2: Ghost CVE-2015-0235

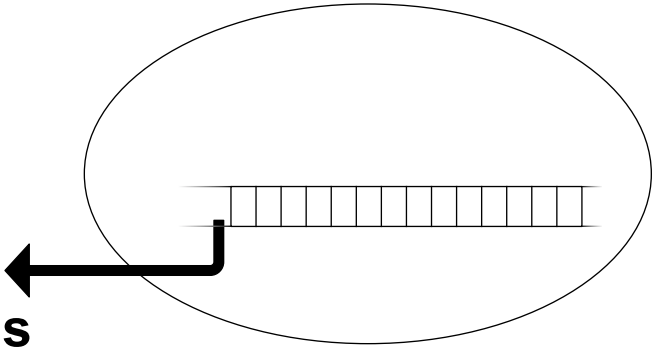


Ghost — gethostbyname buffer overflow is

- **caused by a *Destination Too Small***
- **because of an *Incorrect Calculation*, specifically *Missing Factor*,**
- **where there was a *Write* that was *After* the end by a *Moderate* number of bytes**
- **of a buffer in the *Heap***
- **that may be exploited for *Arbitrary Code Execution*.**

Heap-based buffer overflow in the __nss_hostname_digits_dots function … allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST."

Example 3: Chrome CVE-2010-1773



Chrome WebCore — render buffer overflow is

- **caused by a *Wrong Index***
- **because of an *Incorrect Calculation*, specifically *Off by One*,**
- **where there was a *Read* that was *Below* the start by a *Minimal* amount**
- **of a buffer in the *Heap***
- **that leads to use of *User Input Not Checked Properly***
- **that may be exploited for *Information Exposure*, *Arbitrary Code Execution*, or *Program Crash* leading to *Denial of Service.***

Off-by-one error in the toAlphabetic function …, allows remote attackers to obtain sensitive information, cause a denial of service (memory corruption and application crash), or possibly execute arbitrary code via vectors related to list markers for HTML lists, …

Example 4: cppCheck Warning Classes

CppCheck is a static analysis tool. Table 1 provides descriptions of the buffer overflow parts of its warning classes.

Warning \ Attribute:	Access	Side	Indexed	Size	Magnitude
Array Index Out Of Bounds	-	-	Yes	-	-
Buffer Access Out Of Bounds	-	-	-	-	-
Out Of Bounds	-	-	-	-	-
Negative Index	-	Below	Yes	-	-
Insecure Cmd Line Args	Write	Above	-	-	-
Write Outside Buffer Size	Write	-	-	-	-
Invalid Scanf	Write	Above	-	Varies	Moderately outside

NIST National Institute of Standards and Technology • U.S. Department of Commerce

Example 5: Refactoring CWEs

Applying our definition and attributes, Buffer Overflow CWEs can be categorized as follows.

Table 2. Buffer Overflow CWEs Organized by Attribute.

	before	after	either end	stack	heap
read	127	126	125		
write	124	120	123, 787	121	122
either r/w	786	788			

Focus On: Injection

- **CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): The software constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.**

  → "Using input", "intended command", and "correctly neutralizing" are imprecise. Our definition precisely defines "using input" and "intended command". We do not include "correctly neutralizing", because it simply means that intended OS command cannot be modified.

Injection: Causes, Attributes, and Consequences

Causes

Input Not Checked Properly
- Permissive Whitelist
- Incomplete Blacklist

Input Not Sanitized Properly
- Failure to Remove Offending Characters
- Failure to Reject Input Altogether
- Failure to "Escape" Offending Characters

Injection

Attributes:
- Language/Resource:
  - ✓ *SQL query, Regular expression, Bash shell command (OS injection), XML/Xpath, http, C printf format string, PHP (eval), file path,* etc.
- Special Element:
  - ✓ *Quotes (' or ") – enclosing query strings, Line delimiter (CRLF) – separating headers, Angle brackets and ampersand (< or > or &) – web scripting elements, ".." and "/" – path traversal, etc.*

Consequences

- Mask Legitimate Commands or Information → Loss of Confidentiality/ Authentication/ Authorization/ Integrity → Information Exposure; Information Loss
- Add additional command → Computer Worm Propagation → Denial Of Service
- Add additional command → Arbitrary Code Execution → Denial Of Service
- Complete Host Takeover → Arbitrary Code Execution
- Denial Of Access

Examples of immediate consequences:
- Add Additional Command – turn "touch file" into "touch file; rm /etc/passwd".
- Mask Legitimate Commands or Information – turn "WHERE login == 'name' " into "WHERE login == 'name' && 1=1 --'r' " so that the check for password is skipped.

Example 1: Yoggie Pico

CVE-2007-3572

Yoggie Pico and Pico Pro — remote take over is

- **caused by *Input Not Checked Properly***
- **specifically *Incomplete Blacklist*,**
- **where injection was through a *shell command***
- **using a *back tick (`)* special element**
- **to *Add Command* that adds a user-chosen root password to /etc/shadow allowing *Arbitrary Code Execution.***

Incomplete blacklist vulnerability in cgi-bin/runDiagnostics.cgi in the web interface on the Yoggie Pico and Pico Pro allows remote attackers to execute arbitrary commands via shell metacharacters in the param parameter, as demonstrated by URL encoded "`" (backtick) characters (%60 sequences).

Outline

- The "Science" of Weaknesses
- Our Nomenclature
- Examples of Applying Our Approach
- **Using This**

Migrating From CWEs

- **Add descriptions in our notation to CWEs.**
- **Tool makers describe their classes with it. CVEs and others describe bugs with it.**
- **They will say "This is like CWE-121, but has *read* access", people will just use our notation. *(CWE descriptions serve as prototypes.)***

Next Steps

- **Apply our technique to more examples**
- **Work out another weakness class:**
  - **Authentication Attempts (CWE-307)**
- **Define more "vocabulary" – add terms, more formal, refine**
- **Elaborate causes and consequences.**

Focus On: Authentication

- **CWE-307: Improper Restriction of Excessive Authentication Attempts:**
  The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.

- **→ "Multiple" and "short" are vague. Our definition recognizes that CWE-307 actually represents a set of weaknesses, each of which satisfies particular institution-specific definitions of "multiple" and "short".**

- ***<u>Our Definition</u>*: The software does not limit the number of failed authentication attempts or allows more than a specified number of failed authentication**

Some Benefits Are:

- **Help programmers write better code, because they understand more clearly.**
- **Better train computer scientists and cybersecurity workers.**
- **More precisely explain vulnerabilities (e.g. Heartbleed, Shellshock, or Ghost).**
- **Develop new techniques to mitigate or prevent vulnerabilities.**
- **More precisely describe the classes of bugs that tools cover (e.g. buffer overflow, hard-coded password, or SQL injection)**
- **Improve existing classifications.**

Thanks!

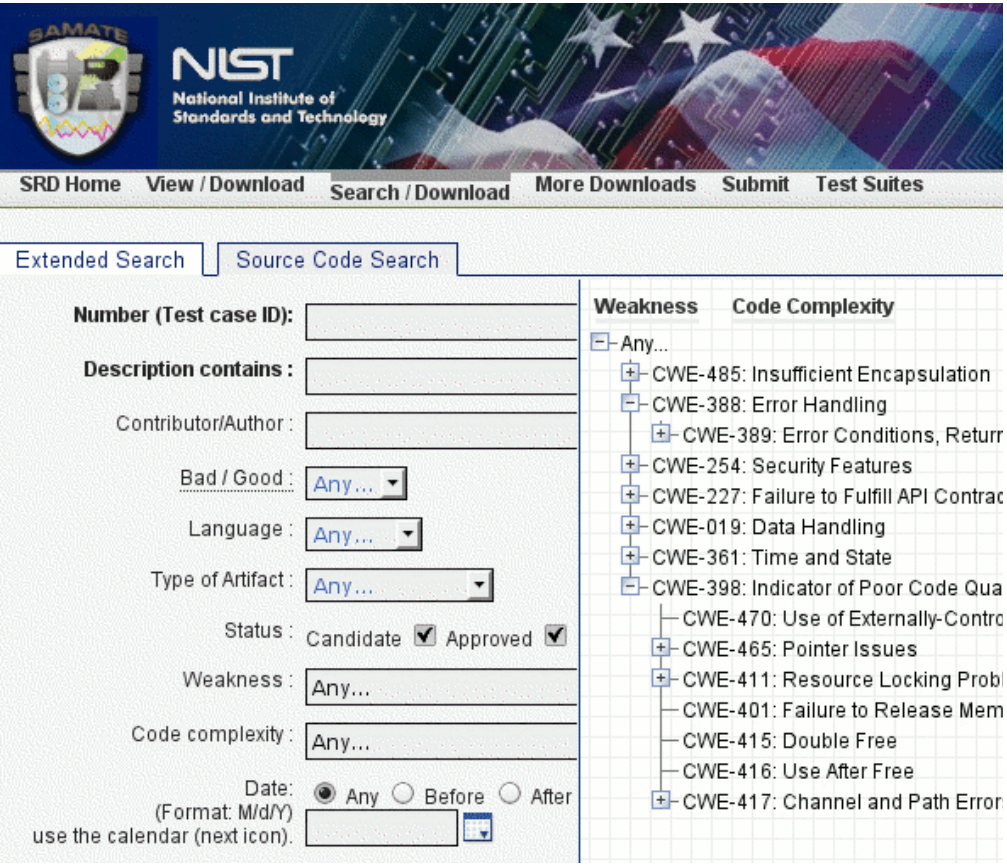
Society has 3 options:

- **Learn how to make software that works**
- **Limit size or authority of software**
- **Accept failing software**

extra slides

ADDITIONAL SLIDES

Software Assurance Reference Dataset (SARD)



Need:

- **Suites of programs with known bugs to calibrate software assurance tools**

Objective:

- **Collect and develop sets of programs with known bugs in various languages, with bugs of various classes, and bugs woven into various code structures**

http://samate.nist.gov/SARD/

Software Assurance Reference Dataset (SARD)

- **Over 140 000 cases in C, C++, Java, C#, and PHP**
- **Contributions also from Fortify, Defence R&D Canada, Klocwork, Kratkiewicz, MIT Lincoln Laboratory, Secure Software, Praxis, etc.**
- **NSA Juliet 1.0 and 1.2 - over 80 000 small, synthetic test cases in C, C++, and Java covering 150 bug classes**
- **IARPA STONESOUP - 15 000 cases based on 12 web apps with injected bug from 25 classes**
- **2000 PHP cases developed at TELECOM Nancy**
- **Users can search and download by language, weakness, size, content, etc.**