Ethical Hacking: Buffer Overflows

What Are Buffer Overflows?

James D. Murray, CISSP C|EH

@jdmurray| www.TechExams.net/blogs/jdmurray

This is part of the Ethical Hacking series, see below URL for whole series

http://blog.pluralsight.com/learning-path-ethical-hacking

How Well Do You Speak "Computer?"

How are computer programs created?

What is inside of a running computer program?

An IT course, not a computer science course

Basics about programming and programs

Have some programming skills?

C, C++, or assembly language is great!

Buffer Overflow

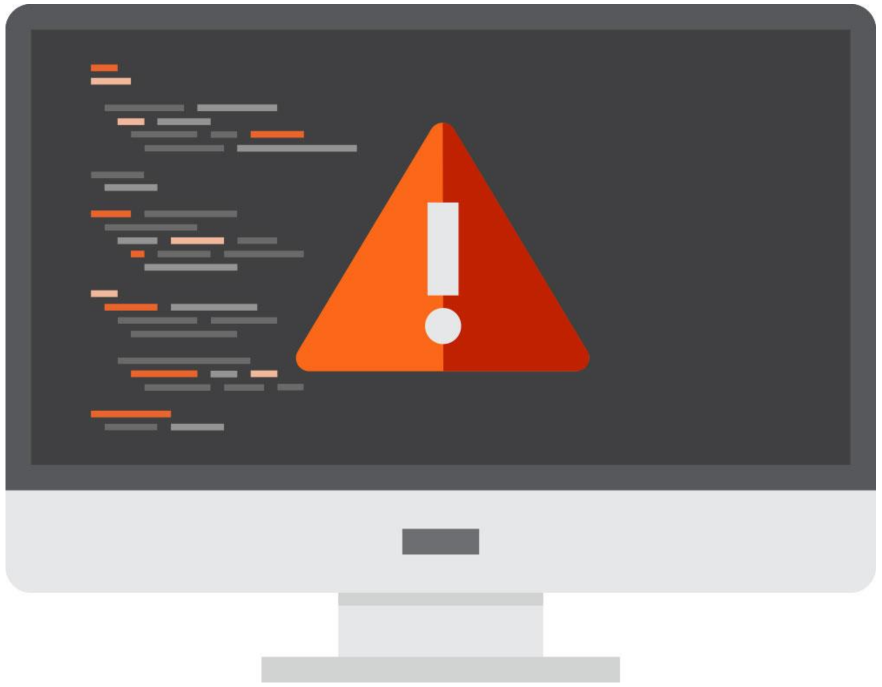
A condition in which a running program attempts to write data outside of a temporary data storage area (known as a buffer) and into other areas of program memory not intended to store this data. Also called a buffer overrun.

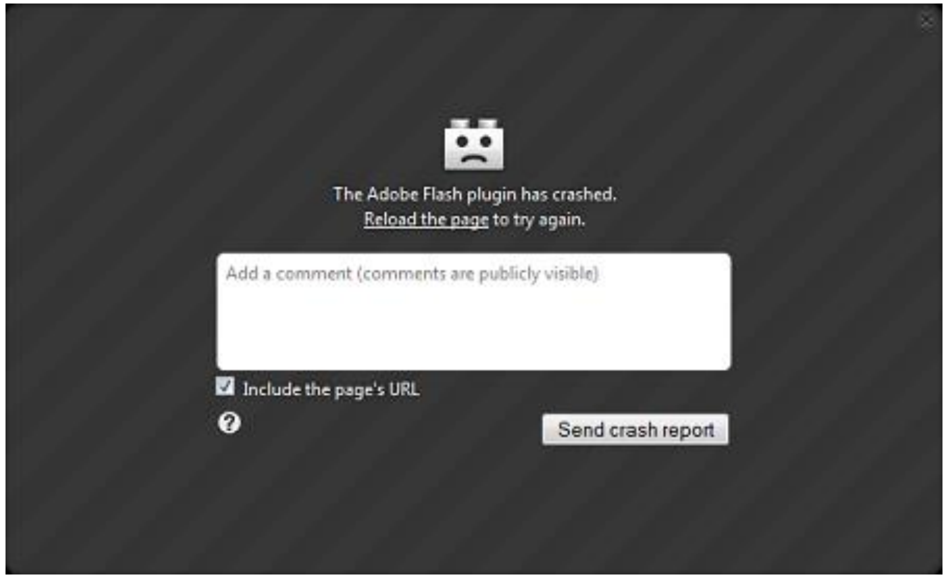
What Is a “Buffer?”

- Areas of memory in a running computer program
- Use to temporarily store data for use by the program
- Stored data is for input, processing, or output
- Buffers can exist for a very short or very long time
- Hundreds or thousands of buffers in a program
- Memory buffers are found in all programs

Why Do Buffers Overflow?

What Happens When a Buffer Overflows?




The Adobe Flash plugin has crashed.
Reload the page to try again.

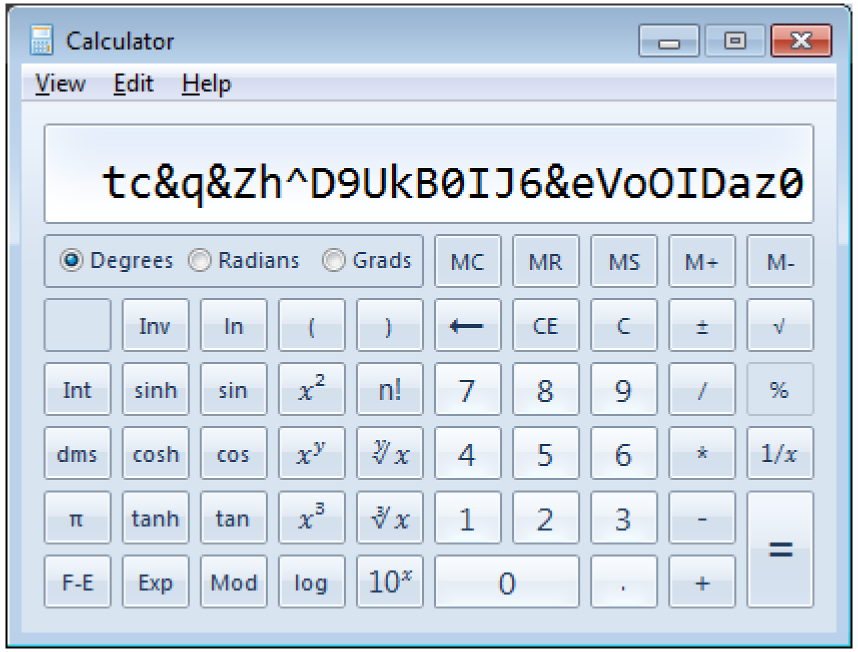
Add a comment (comments are publicly visible)

✓ Include the page's URL

Send crash report

Program instability

Abnormal termination


Calculator
View Edit Help
Degrees Radians Grads
MC MR MS M+ M-
Inv ln ( ) ← CE C ± √
Int sinh sin x^2 n! 7 8 9 / %
dms cosh cos x^y $\sqrt[y]{x}$ 4 5 6 * 1/x
π tanh tan x^3 $\sqrt[3]{x}$ 1 2 3 - =
F-E Exp Mod log 10^x 0 . +

```
tc&q&Zh^D9UkB0IJ6&eVoOIDaz0
```

Information corruption

Arbitrary code execution

Nothing at all

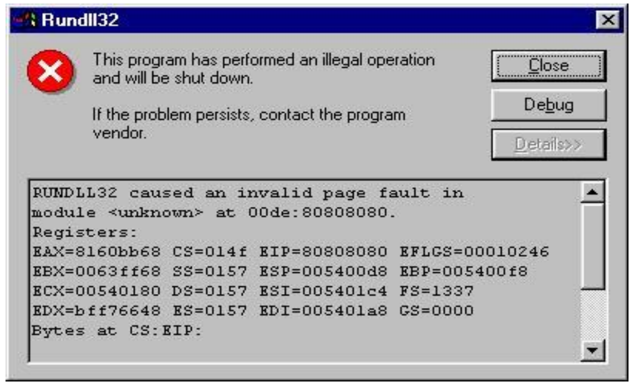
What Can You Do with a Buffer Overflow?

- Illicit program execution
- Command & control of computer
- Illicit network access by attacker
- Pivoting to other network hosts

What Can You Do with a Buffer Overflow?

Data exfiltration

Information corruption



This program has performed an illegal operation and will be shut down.

If the problem persists, contact the program vendor.

```
RUNDLL32 caused an invalid page fault in
module <unknown> at 00de:80808080.
Registers:
EAX=8160bb68 CS=014f EIP=80808080 EFLGS=00010246
EBX=0063ff68 SS=0157 ESP=005400d8 EBP=005400f8
ECX=00540180 DS=0157 ESI=005401c4 FS=1337
EDX=bff76648 ES=0157 EDI=005401a8 GS=0000
Bytes at CS:EIP:
```

Program or OS crash
(denial of service)

How You Do Keep Buffers from Overflowing?

Reactive

- Detect overflow conditions as they happen…
- …and minimize their effects

Proactive

- Prevent overflow conditions from happening…
- …which is the best solution

The Responsibility for Preventing Buffer Overflows

Software Programmers	Write code that prevents buffer overflows	Fix buffer management problems as they are found
System Administrators	System builds and configurations to minimize overflows	Security software to detect and mitigate overflows

Why Do Buffers Overflow?

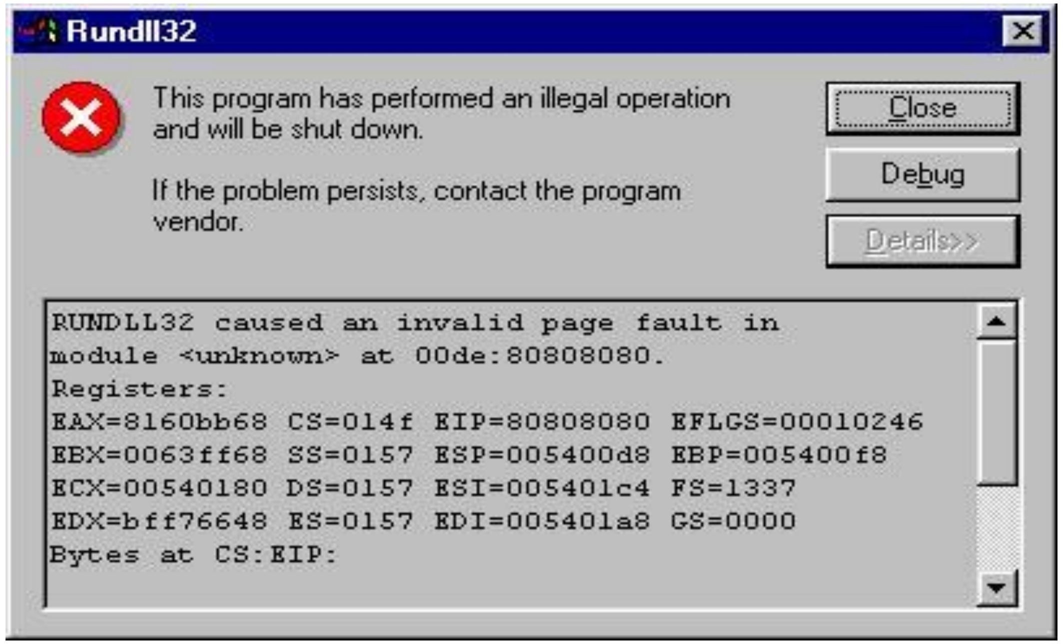
Common and long-lived software vulnerability

Common software bug

Easy to mistakenly create

Most are easy to find and fix

What Does a Buffer Overflow Look Like?



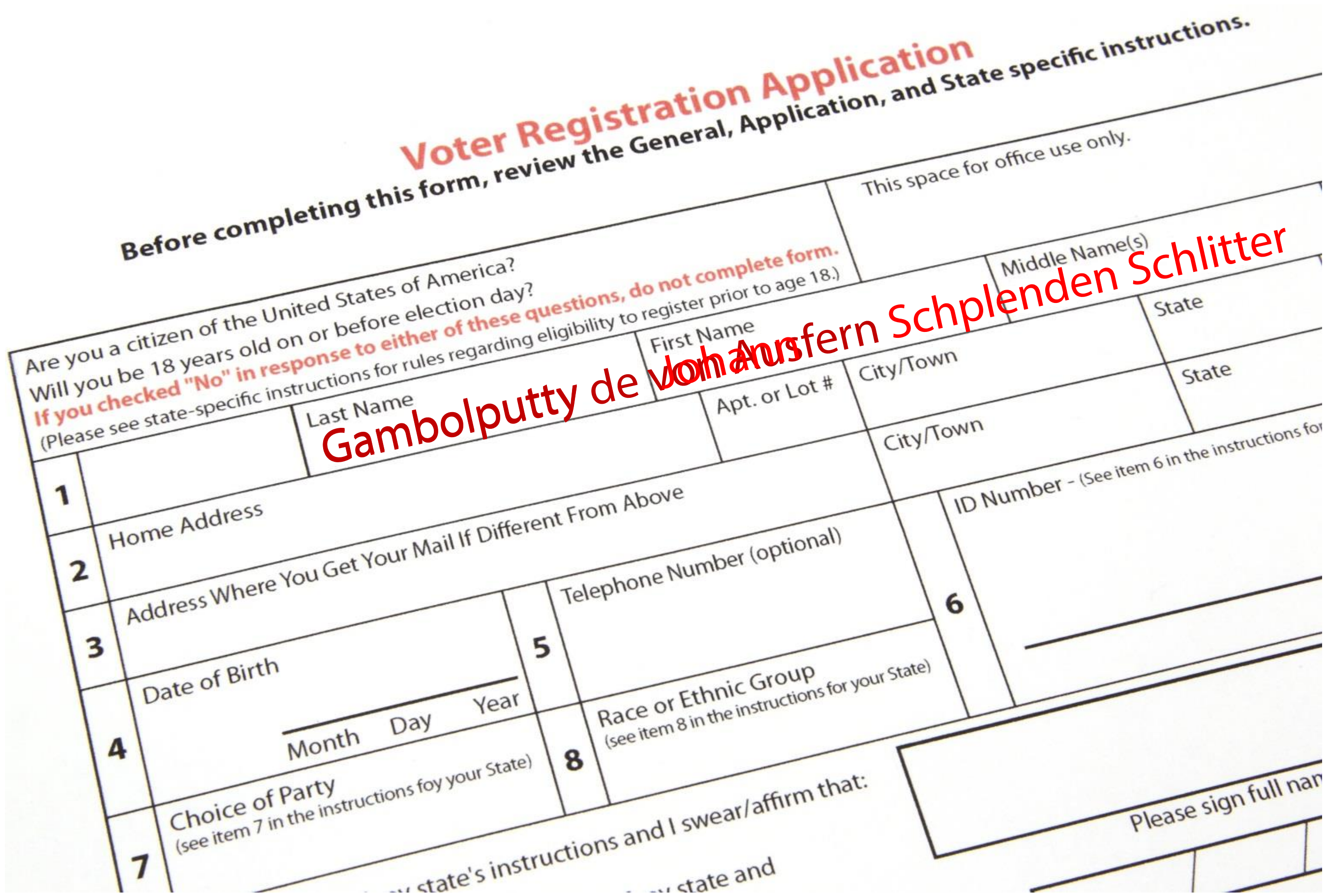
This program has performed an illegal operation and will be shut down.

If the problem persists, contact the program vendor.

```
RUNDLL32 caused an invalid page fault in
module <unknown> at 00de:80808080.
Registers:
EAX=8160bb68 CS=014f EIP=80808080 EFLGS=00010246
EBX=0063ff68 SS=0157 ESP=005400d8 EBP=005400f8
ECX=00540180 DS=0157 ESI=005401c4 FS=1337
EDX=bff76648 ES=0157 EDI=005401a8 GS=0000
Bytes at CS:EIP:
```

What Does a Buffer Overflow Look Like?

What Does a Buffer Overflow Look Like?



Voter Registration Application

Before completing this form, review the General, Application, and State specific instructions.

This space for office use only.

Are you a citizen of the United States of America?

Will you be 18 years old on or before election day?

If you checked "No" in response to either of these questions, do not complete form.

(Please see state-specific instructions for rules regarding eligibility to register prior to age 18.)

1	Last Name: Gambolputty de von Ausfern Schplenden Schlitter	First Name: Johann	Middle Name(s)
2	Home Address	Apt. or Lot #	City/Town / State
3	Address Where You Get Your Mail If Different From Above		City/Town / State
4	Date of Birth: Month Day Year	5 Telephone Number (optional)	6 ID Number - (See item 6 in the instructions for
7	Choice of Party (see item 7 in the instructions foy your State)	8 Race or Ethnic Group (see item 8 in the instructions for your State)	

y state's instructions and I swear/affirm that:

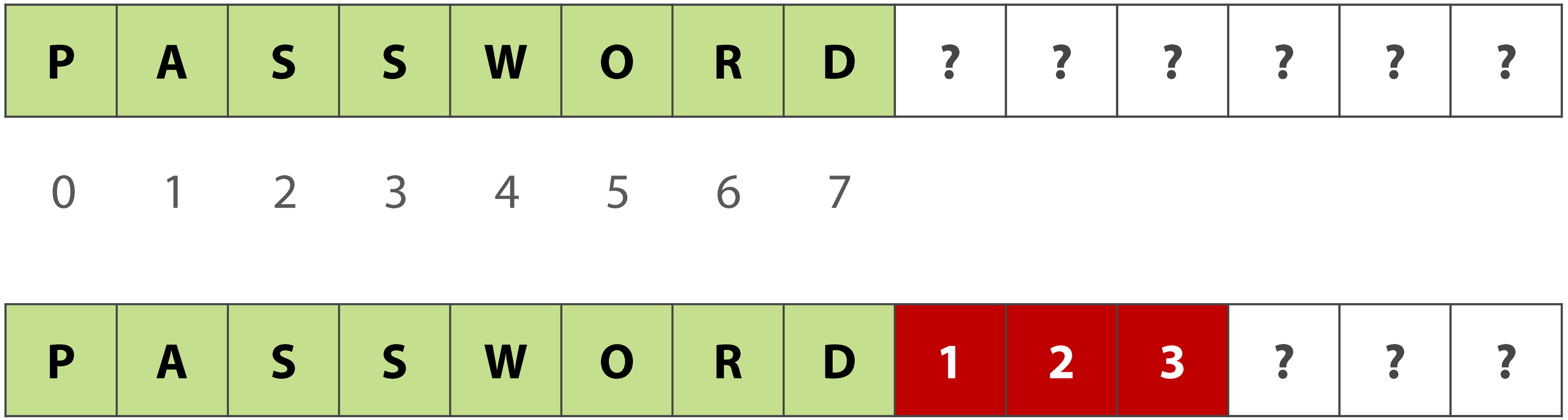
y state and

Please sign full nar

The World of Buffers

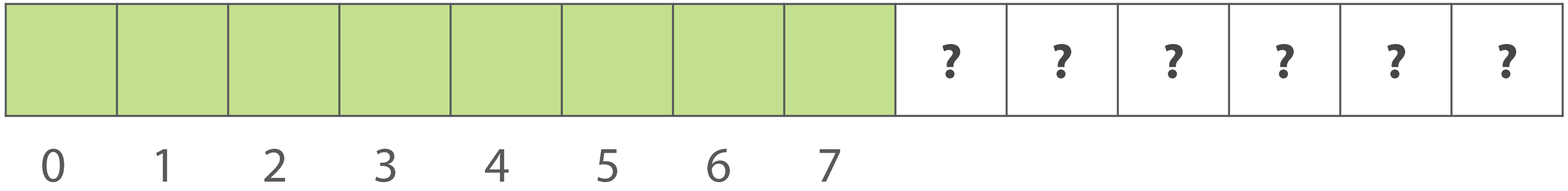
A	A	A	l	e	t	m	e	i	n	\0	1	2	3
A	5	C	A	P	C	H	A	215	s	e	c	r	e
t	.	k	e	y	s	0	0	0	0	0	4325	2342	344
1	2	3	-	4	5	-	6	7	8	9	\0	đ	€
ℓ	Σ	Ω	Π	п	a	p	o	л	b	#	#	#	#

Inside Buffers

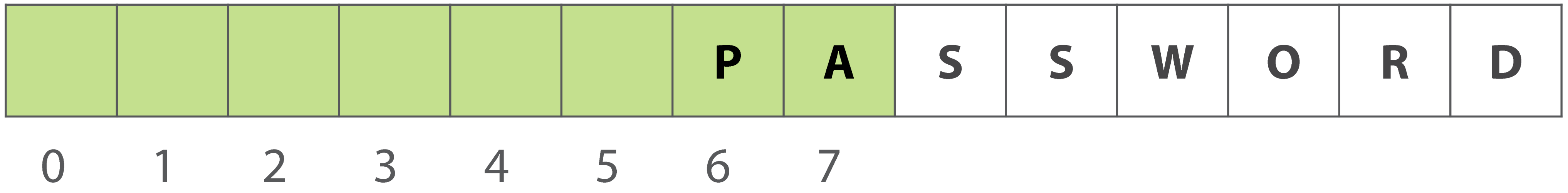


Overflow or Overrun?

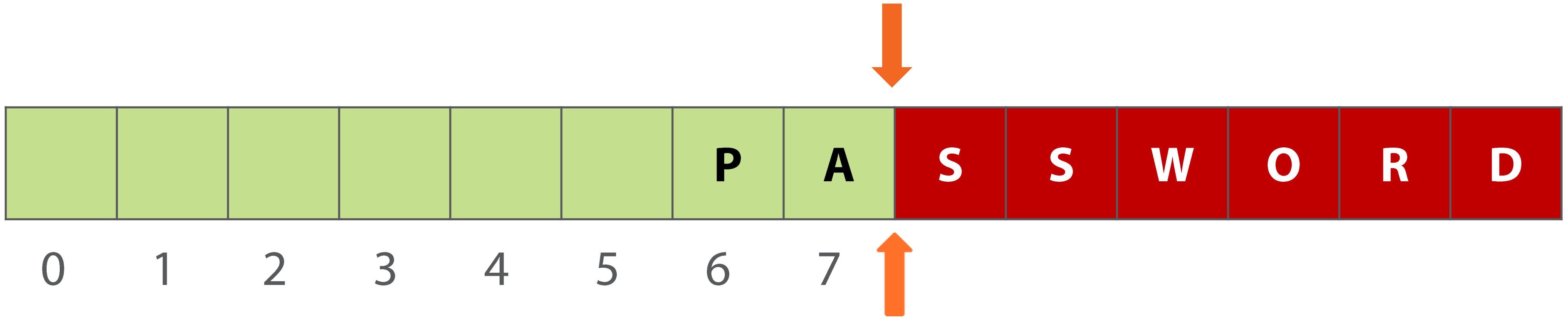
Underflows or Underruns



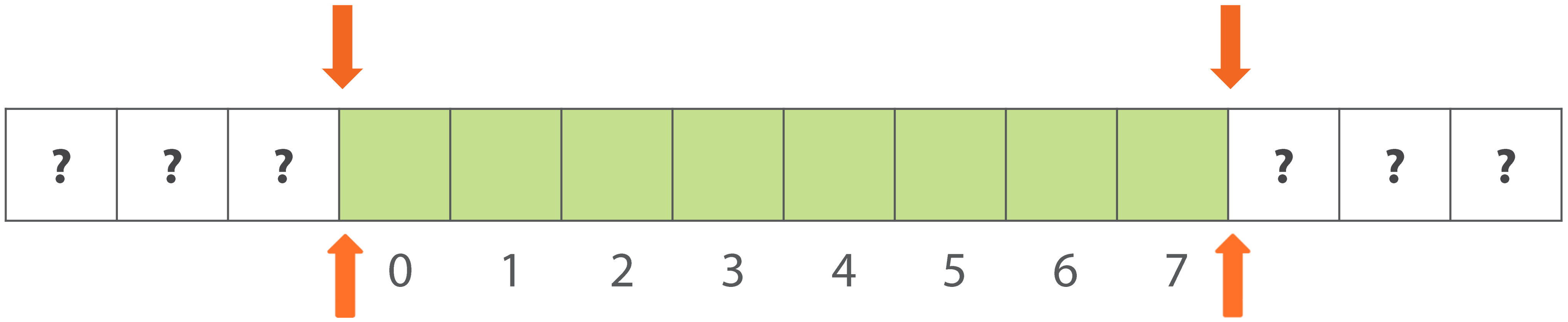
Underflows or Underruns



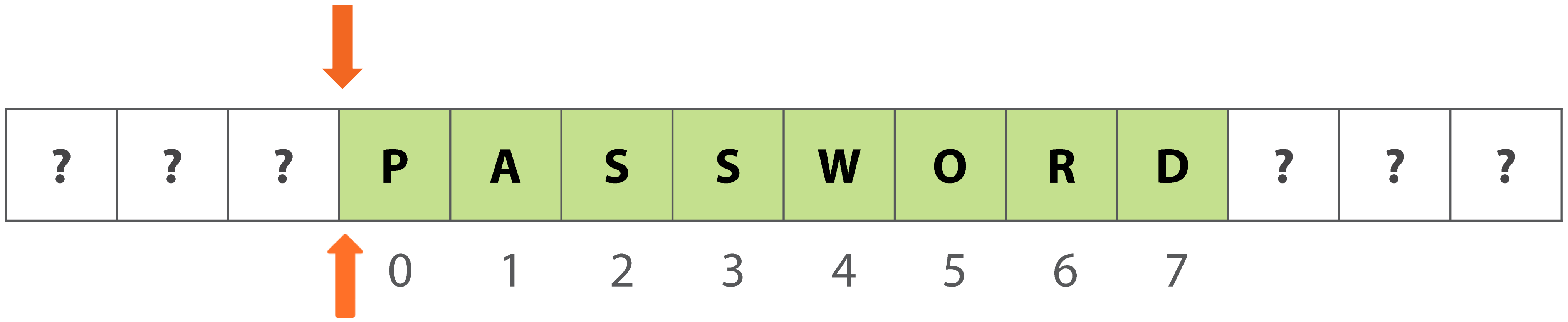
Underflows or Underruns



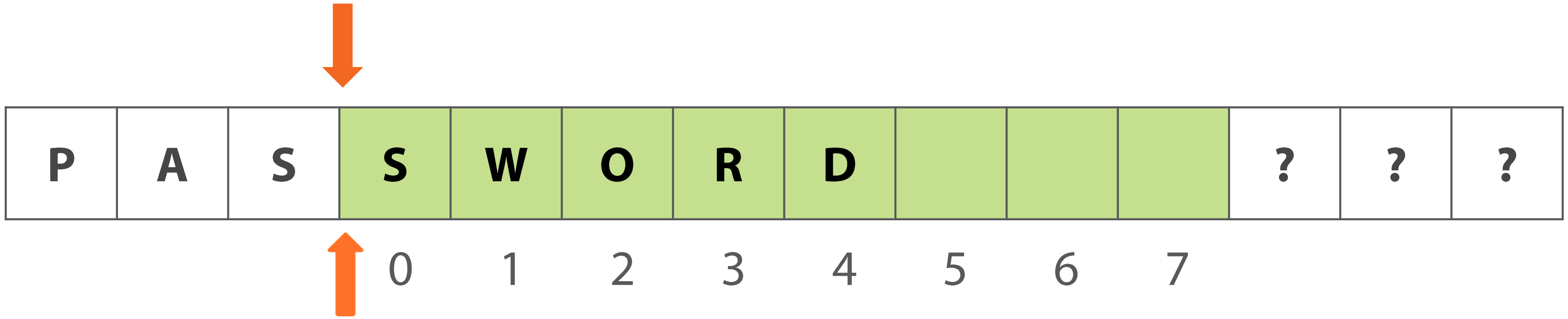
Underflows or Underruns



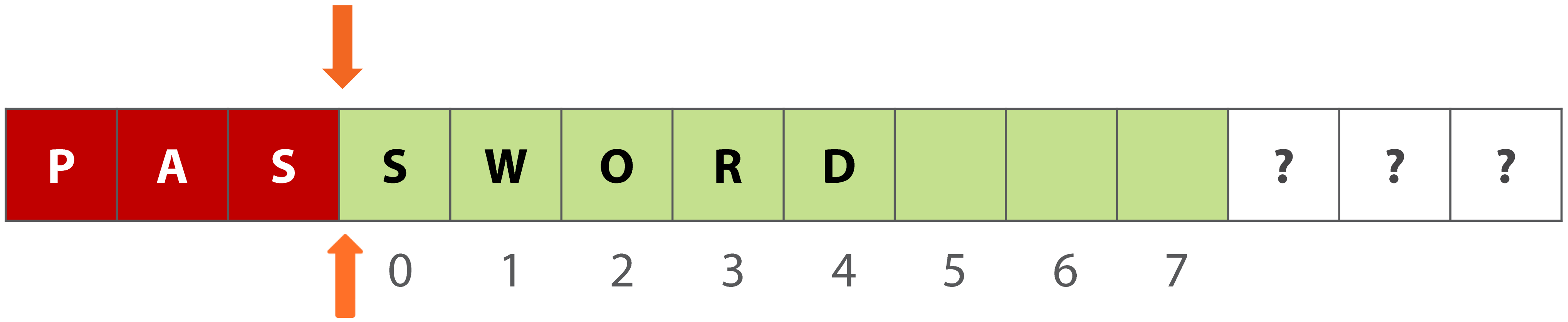
Underflows or Underruns



Underflows or Underruns



Underflows or Underruns



Writing Flows and Reading Runs

Buffers are always writeable

Buffers overflow by writing data

Reading buffers can exceed memory boundaries too

Reading can overrun or underrun a buffer

Check if an exploit reads from or writes to a buffer

Reading past a buffer can find interesting data

Integer Overflows

Integer values are stored in fixed-sized areas of memory

-32,768 to 32,767

0 to 255

255 + 1 = 0

Unexpected data values

Unintended program logic flow

One overflow condition may lead to another

What Happens After a Buffer Overflows?

Denial of Service

A condition in which programs, systems, or networks are prevented from providing information processing and transfer services at an acceptable level of performance. A DoS condition is a purposeful and often malicious action.

Local Denial of Service

- Physical access to the system
- Unplugging power cord or network cables
- Local administrator log in
- Stop services or power-down system

Remote Denial of Service

- Network access to system
- Flood of network traffic
- Hammering server with legitimate requests
- Sending bad input to exploit possible vulnerabilities—including buffer overflows

Accidental Denial?

DoS attacks are intentional and malicious

Non-malicious Denial of Service

DoS as a defensive reaction to illicit activity

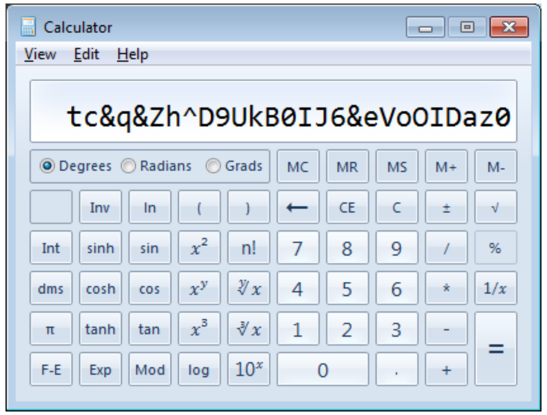
Accidental DoS?

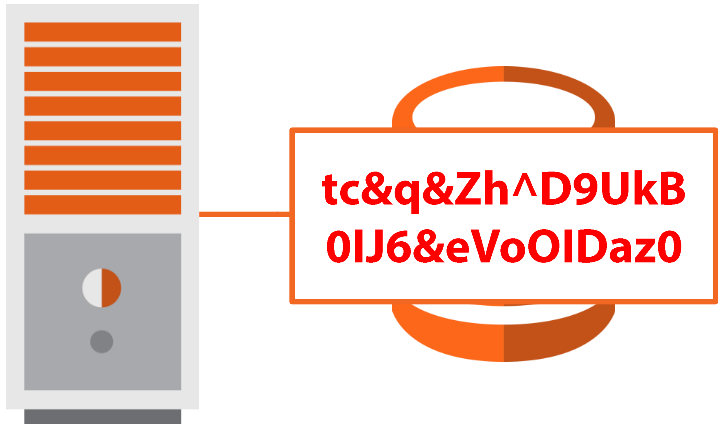
Failures
or
Outages

DoS was not an intentional result

Information Corruption

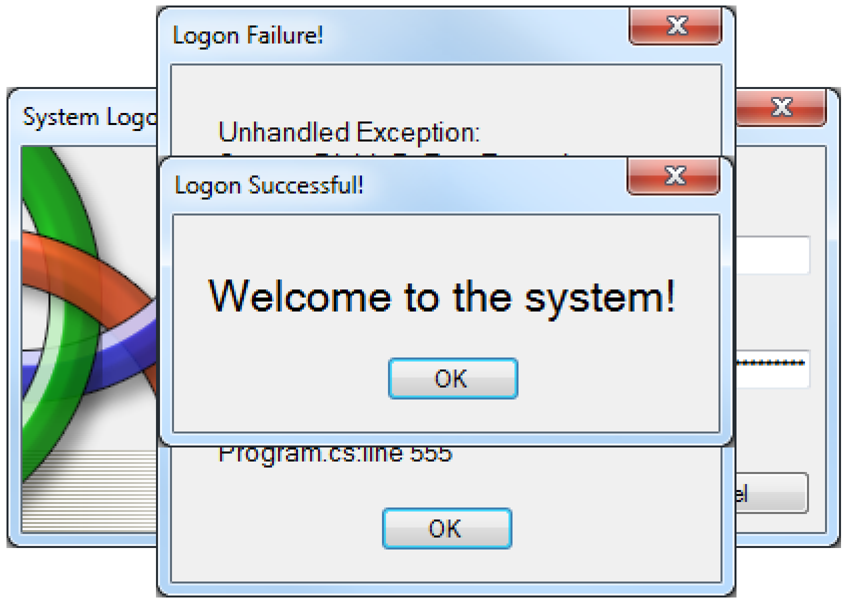
tc&q&Zh^D9UkB
0IJ6&eVoOIDaz0


tc&q&Zh^D9UkB0IJ6&eVoOIDaz0
Calculator
View Edit Help
Degrees Radians Grads MC MR MS M+ M-
Inv ln ( ) ← CE C ± √
Int sinh sin x^2 n! 7 8 9 / %
dms cosh cos x^y $\sqrt[y]{x}$ 4 5 6 * 1/x
π tanh tan x^3 $\sqrt[3]{x}$ 1 2 3 - =
F-E Exp Mod log 10^x 0 . +


tc&q&Zh^D9UkB
0IJ6&eVoOIDaz0

Changes in Program Flow

- Data controls the logical flow of program operation.
- Bad input data can make a program behave in unexpected ways.
- Buffer overflows may change specific aspects of a program’s behavior.
- Behavior changes may help defeat security features.


System Logo

Logon Failure!

Unhandled Exception:

Program.cs:line 555

Logon Successful!

Welcome to the system!

Arbitrary Code Execution

- The data overflowing a buffer can be an executable program.
- Code injection inserts code into a computing environment.
- The system administrator would not want this program to run.
- A buffer overflow can both load and run a malicious program.
- Any type of program the attacker wants to run on the vulnerable system is "arbitrary code."
- The arbitrary code must be compatible with the OS and CPU of the vulnerable system.

A buffer overflow in the FunGame application before version 2.3.4 allows remote attackers to cause a denial of service (application crash), or possibly execute arbitrary code via a specially-crafted input file.

Elevated Privileges

- Privileges determine what a program can access and do.
- Operating at a higher than normal privilege level
- Attackers desire to run their arbitrary code at an elevated privilege level.
- Buffer overflows can allow programs to be run at a higher privilege level
- Programs running with higher privileges have more capabilities:
  - Open network ports
  - Start command shells
  - Reconfigure system
  - Add user accounts

MyTaskList version 1.2.3 contains an input-handling flaw that may allow remote attackers to execute arbitrary code with elevated privileges.

Command & Control

C&C

C2

Military – to exercise command authority

Cybersecurity – to gain and maintain control over computers

C&C used by Malware and botnets

BoF exploits to install and run C&C Malware

C&C of computers is a goal of many cyber attacks

As if That's Not Enough…

- Denial of Service (DoS)
- Information Corruption
- Change in Program Flow
- Arbitrary Code Execution
- Elevated Privileges
- Command and Control (C&C, C2)
- Operational instability
- Abnormal termination
- Nothing at all

How Do You Keep Buffers from Overflowing?

```
public static void main (String[] args)
{
    BufferedReader file_reader = new BufferedReader (
    String text;
    while (!(text=file_reader.readLine(file_contents))
    int a;
    for (int i=0;z[i]!='\0';i++)
    a++;
    for (int j=0;x[j]!='\0';j++)
    {
        z[a+j]=x[j];
    }
```

Mitigation

To minimize the harmful impact of a threat, either before or after the threat occurs.

Safeguards and Countermeasures

- Safeguard
  - Proactive
  - Prevents a threat from occurring

Safeguards and Countermeasures

- Countermeasure
  - Reactive
  - Reacts to a threat to minimize the damage
- Technical and administrative

Safeguards Against Buffer Overflows

Programmers,

- ✓ write safer code!
- ✓ fix your code!
- ✓ have your code tested!

System Administrators,

- ✓ find vulnerable programs
- ✓ patch vulnerable programs
- ✓ remove vulnerable programs
- ✓ don't disable and forget programs

Users,

- ✓ learn about software security issues
- ✓ do not use unknown or untested software
- ✓ do not trust unverified software distributers

Countermeasures Against Buffer Overflows

Programmers,

- ✓ verify data in memory
- ✓ use BoF detection features
- ✓ log all errors related to memory management

System Administrators,

- ✓ use modern hardware and OS
- ✓ enable anti-BoF features
- ✓ install security apps
- ✓ monitor systems for errors related to BoF

Users,

- ✓ do not install unknown programs
- ✓ do not visit potentially unsafe Web sites
- ✓ keep all program patches up to date
- ✓ backup your data

Summary

- ✓Buffers are reserved areas of program memory
- ✓Buffers are used for data storage
- ✓Buffers are adjacent in memory
- ✓Reads and write operations must stay within a buffer's memory boundaries
- ✓Overflow, underflow, overrun, underrun
- ✓Buffers overflow because of poorly written software code

Summary

✓A vulnerability is a potential security risk

✓Programs can crash, become unstable, leak information, be forced to run other programs

✓Malware uses overflows for denial of service, elevated privileges, arbitrary code execution, command & control

✓Integer overflows are value rollovers that can cause buffer overflows and vice versa

Summary

- ✓Write safe and secure code
- ✓Fix legacy code
- ✓Use software tools security features
- ✓Patch or uninstall vulnerable programs
- ✓Use modern hardware and OS
- ✓Do not install and use untrusted software
- ✓Backup your data and test restoration

Simple can be harder than complex: You have to work hard to get your thinking clean to make it simple. But it’s worth it in the end because once you get there, you can move mountains.

— Steve Jobs

Next Up:

Inside Buffer Overflows