University of Dayton
Department of Computer Science

CPS 475/575
Secure Application Development

Lecture 6 – Secure Client Socket Programming in C

Phu Phung
1/30/2020

Buffer Overflows vs. Format String Vulnerabilities

	Buffer Overflow	*Format String*
public since	mid 1980's	June 1999
danger realized	1990's	June 2000
number of exploits	a few thousand	a few dozen
considered as	security threat	programming bug
techniques	evolved and advanced	basic techniques
visibility	sometimes very difficult to spot	easy to find