Feb 4, 2005 -- Lecture 8

THE UNIVERSITY OF IOWA

22C:169 Computer Security

Douglas W. Jones

Department of Computer Science

Program Security

Is this program secure?

A simple question only if

program has no input or output

Threats:

From: the legitimate users
the illegetimate users
the developers
other programs it listens to

To: the program's own execution
any device the program controls
any stored data it manipulates
any other programs it talks to

IEEE Programming terminology:

Error

A mistake made by a programmer

Fault

Embedding of error in program

Failure

Manifestation of fault in behavior

Relative to spec assumed correct!

Security and Programming

Security error:

Failure to understand security problem

Security fault

Vulnerability created by security error

Security failure

Exploitation of security failure

Security Errors in Specification

1997, Microsoft Spec:

Visual Basic in all MS Office Apps

Assume

Correct implementation

Security fault

Opening any file in an Office App can have arbitrary side-effects

MS OFFICE VIRUSES

Security Errors in Specification

C Standard Library, ca 1973

```
char * gets( char * str );
```

Assume

Correct implementation

Fault

Buffer Overflow Errors

Used by many attackers

Security Errors in Specification?

Decision to use unsafe tools

- *C*
- *C++*
- *MS Office*

Banning such tools

- *can be materially improve security*
  - There is resistance to this
  - Some of it is very legitimate!

Security Errors in Implementation

Error

- *use of* **`gets()`** *(should use* **`fgets()`***)*
- *use of* **`strcat()`**   **`strncat()`**
- *failure to check parameter validity*

Security Errors in Use

Error

- *Reliance on insecure products*
- *Demanding features now, security later*
- *Failure to update in face of known bugs*

Marketplace Forces

- *Reinforce many of these behaviors*

Attacks from Developers

Frequently overlooked

How do you prevent

- *Backdoors*
- *Trojans*
- *Easter Eggs*

The threat from illicit users is familiar