

Lecture Notes – Computer Security

Author: Dr. Aaron Striegel
University of Notre Dame striegel@nd.edu

Topic: Program Security

Trapdoor

Entry point into a module Hooks/API
Unit vs. integration testing
 Stub/driver
 Debug commands
Error Checking
 Defensive programming
 Case, if
 No default
 This will never happen
 Undefined opcodes – HW
Salami Attack
 Think superman
 Rectify an error
 \$0.01 error on bank statement
 Cause: Accept some small error as unavoidable

Covert Channels

Bypass confidentiality requirement
 Extract data clandestinely
Human example
 Location of pencil, tap on desk, blink
Draw fig
 User -> Svc Program -> Data
 |
 Spy
Insignificant changes to a report / item
 ps
 Report -> Total or Totals (1 bit channel)
 OS items
Storage channel
 Presence/absence of objects
 File lock channel
 Create -> time synchronization
 1 bit -> seems slow
 1 bit / ms 1 kb / sec
 2 days -> entire book
Timing channel
 Use / not use computing time

Identifying Covert Channels

Shared Resource Matrix

Identify all resources, who can use them

Build a matrix

	Svc Process	Spy Process
Lock	R,M	R,M
Data	R	

Potential for info flow

M	R
R	Yields R