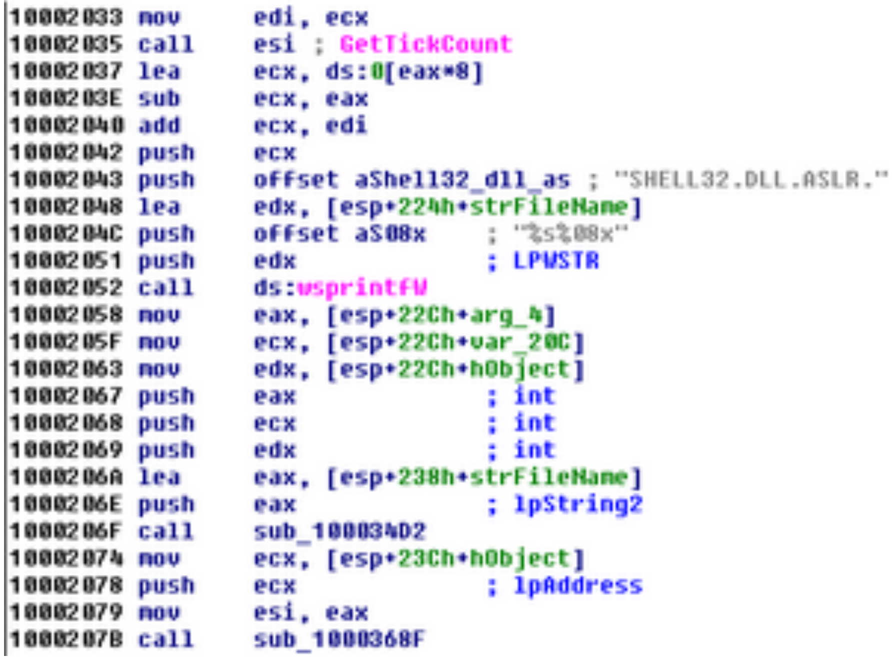
CS 5430

Introduction to Security

Prof. Clarkson
Spring 2017

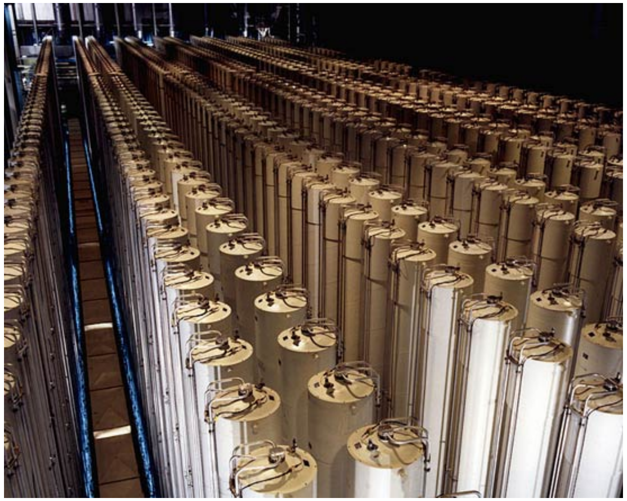
```
static report_breakin(arg1, arg2)       /* 0x2494 */
{
    int s;
    struct sockaddr_in sin;
    char msg;

    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" */
```

November 2, 1988



```
10002033 mov     edi, ecx
10002035 call    esi ; GetTickCount
10002037 lea     ecx, ds:0[eax*8]
1000203E sub     ecx, eax
10002040 add     ecx, edi
10002042 push    ecx
10002043 push    offset aShell32_dll_as ; "SHELL32.DLL.ASLR."
10002048 lea     edx, [esp+224h+strFileName]
1000204C push    offset aS08x     ; "%s%08x"
10002051 push    edx              ; LPWSTR
10002052 call    ds:wsprintfW
10002058 mov     eax, [esp+22Ch+arg_4]
1000205F mov     ecx, [esp+22Ch+var_20C]
10002063 mov     edx, [esp+22Ch+hObject]
10002067 push    eax              ; int
10002068 push    ecx              ; int
10002069 push    edx              ; int
1000206A lea     eax, [esp+238h+strFileName]
1000206E push    eax              ; lpString2
1000206F call    sub_100034D2
10002074 mov     ecx, [esp+23Ch+hObject]
10002078 push    ecx              ; lpAddress
10002079 mov     esi, eax
1000207B call    sub_1000368F
```

June 1, 2012



INTERESTING

HARD

Today

FUN

IMPORTANT

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 typically formulated in terms of three *aspects* of security...

CIA

CIA

Confidentiality

Integrity

Availability

Aspects of security

- **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

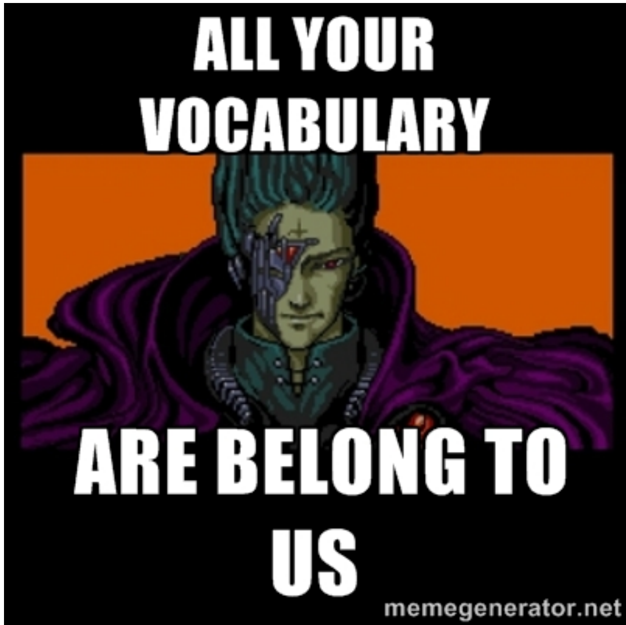
i.e., which principals are allowed to learn what

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 policies

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 policies

Examples:

- Output is correct according to (mathematical) specification
- No exceptions thrown
- 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 policies

Examples:

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

Aspects of security

- 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 POLICIES

Ex 1

- **Attack:** John copies Mary's homework

- What is a **policy** this attack would violate?

- Which **aspect** of security does that policy address?

Advice (for now) on policies

- Make them specific
- Make them about one aspect
- Make them about assets and principals

(L4 will return to these ideas in great depth)

Ex 2

- **Attack:** Paul causes Linda's system to freeze

- **Policy?**

- **Aspect?**

Ex 3

- **Attack:** Carol changes the amount of Angelo's check from $100 to $1000

- **Policy**?

- **Aspect?**

More exercises

(see notes for today)

LOGISTICS

Course website

http://www.cs.cornell.edu/courses/cs5430/2017sp/

- 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

Course staff

TAs:

- **CS 5430:** Elisavet "Eliza" Kozyri
- **CS 5431:** Eleanor Birrell
  – both ABD PhD students working on security

Consultants: Paul Chesnais, Matthew Li, Justin Lu, Gur-Eyal Sela

– undergrads who took this class before and did well

Office hours

- My office hours will be posted on Piazza next week
- Rest of staff's hours are in a Google calendar on course website

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:** MW 10:10-11:25, Phillips 203
  - no 5430 lectures on Fridays :)
  - sorry, I won't approve the overlap with CS 5152
- **5431:** F 10:10-11:25, Hollister 314

Communication

- **Preferred means:** talk to us in person during office hours or (me) after class
- Piazza is available
- If you must send email to me, send to cs5430-profs-L@list.cornell.edu, not directly to my Cornell address
  - Best used for conveying information that needs no response
  - Assume that responses will take about 5 days
  - I.e., always faster to talk to me in person

Piazza

- Once upon a time, there were office hours...
- Fall 2016: CS 3110
  - 305 students
  - 2,719 Piazza posts
    - a lot of junk
    - a lot of disappointment
  - 1,082 contributions made by me
  - **this is not sustainable**
- Alternatives:
  - I could shut off Piazza and return to only office hours
  - I could leave Piazza on with no instructor involvement
  - We can all try to make Piazza useful and viable again...

Piazza

- Full policy and rationale on course website (required reading)
- Summary:
  1. Piazza is a giant office hour we're all attending
  2. You must all commit to asking only smart questions [guide to smart questions]
  3. Replies on Piazza are *pro bono*

Piazza and anonymity

- Anonymous posts disabled this semester
  - A consequence of "giant office hour"
  - I believe we need social accountability for asking smart questions
- This is indeed a tradeoff! I welcome your discussion throughout semester
- Intent is not to be needlessly restrictive but to make Piazza useful and viable

Upcoming events

- [Wed-Thu pm] Drop by my office (Gates 461) in the afternoon if you need something immediately
- [Fri] First practicum meeting; please try to hold questions about 5431 until then
- [next Wed] First assignment out; regular office hours start

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