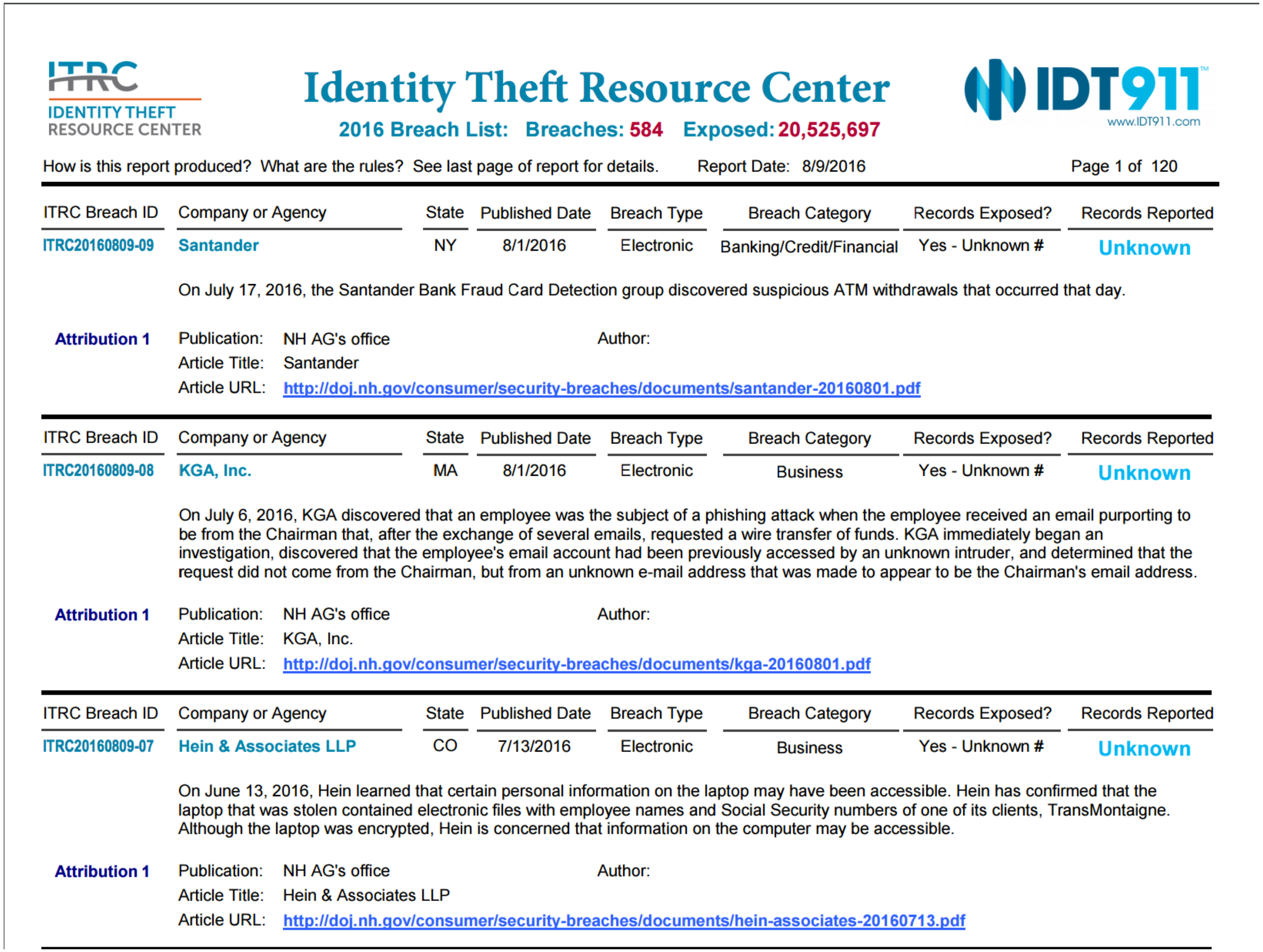
DATA BREACHES

Roadmap: Fall 2017

These Happen Quite a Bit



ITRC IDENTITY THEFT RESOURCE CENTER

Identity Theft Resource Center

2016 Breach List: Breaches: 584 Exposed: 20,525,697

IDT911 www.IDT911.com

How is this report produced? What are the rules? See last page of report for details. Report Date: 8/9/2016 Page 1 of 120

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-09	Santander	NY	8/1/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On July 17, 2016, the Santander Bank Fraud Card Detection group discovered suspicious ATM withdrawals that occurred that day.

Attribution 1
Publication: NH AG's office Author:
Article Title: Santander
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/santander-20160801.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-08	KGA, Inc.	MA	8/1/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 6, 2016, KGA discovered that an employee was the subject of a phishing attack when the employee received an email purporting to be from the Chairman that, after the exchange of several emails, requested a wire transfer of funds. KGA immediately began an investigation, discovered that the employee's email account had been previously accessed by an unknown intruder, and determined that the request did not come from the Chairman, but from an unknown e-mail address that was made to appear to be the Chairman's email address.

Attribution 1
Publication: NH AG's office Author:
Article Title: KGA, Inc.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/kga-20160801.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-07	Hein & Associates LLP	CO	7/13/2016	Electronic	Business	Yes - Unknown #	Unknown

On June 13, 2016, Hein learned that certain personal information on the laptop may have been accessible. Hein has confirmed that the laptop that was stolen contained electronic files with employee names and Social Security numbers of one of its clients, TransMontaigne. Although the laptop was encrypted, Hein is concerned that information on the computer may be accessible.

Attribution 1
Publication: NH AG's office Author:
Article Title: Hein & Associates LLP
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/hein-associates-20160713.pdf

Why Can’t We Stop These?

- Have we figured out yet how to stop home break-ins?
  - Not by a long shot. And houses have been around for thousands of years. Computers have only been widespread for perhaps 30 or so years
- What you can do: manage risk
  - The amount of security applied to a physical building is usually directly related to the value of the items being protected
    - E.g., Fort Knox versus my house
      - Of course, with my house I am not trying to protect against theft of my wife and children — different issue altogether

So, How Exactly Are Databases Hacked?

- Almost all “hacks” are the result of some kind of programming or system design error
- An example: phone phreaking — “stealing” long distance calls (basically making such calls for free)

A Digression into Breakfast Cereals

- 2600 Hz tone a form of *inband signaling*
- ***Beware allowing control information to come from data***
- (also illustrates security-by-obscurity)

So, How Exactly Are Databases Hacked?

- Computer systems are controlled by computer programs
  - Lists of instructions that describe what should happen under various conditions
    - Thousands of languages to do this (but that's another story)
  - These instructions can sometimes leave "vulnerabilities" that hackers exploit
    - Think of a building design that is generally solid, but such that if just the wrong thing happens, you've got a problem

So, How Exactly Are Databases Hacked?

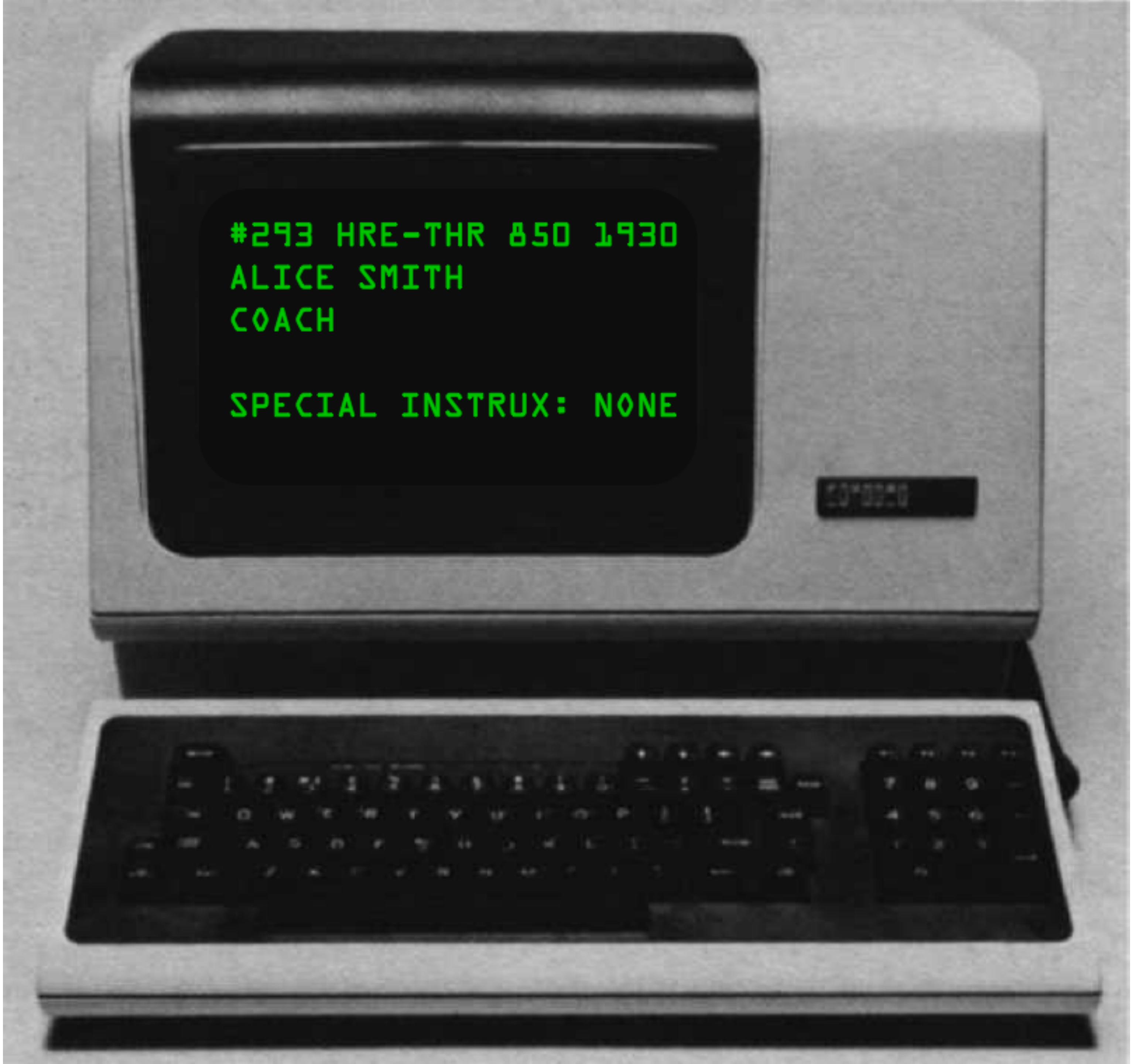
- Hacker Goal: find a way to get their instructions ("code") onto the target computer and then executed
  - Typically, these are instructions that tell the computer to let the attacker do whatever they want
    - This is called "code injection"
- So, how does one get instructions onto a computer system?
  - Often, by invitation
    - With an unexpected and unchecked reply

So, How Exactly Are Databases Hacked?

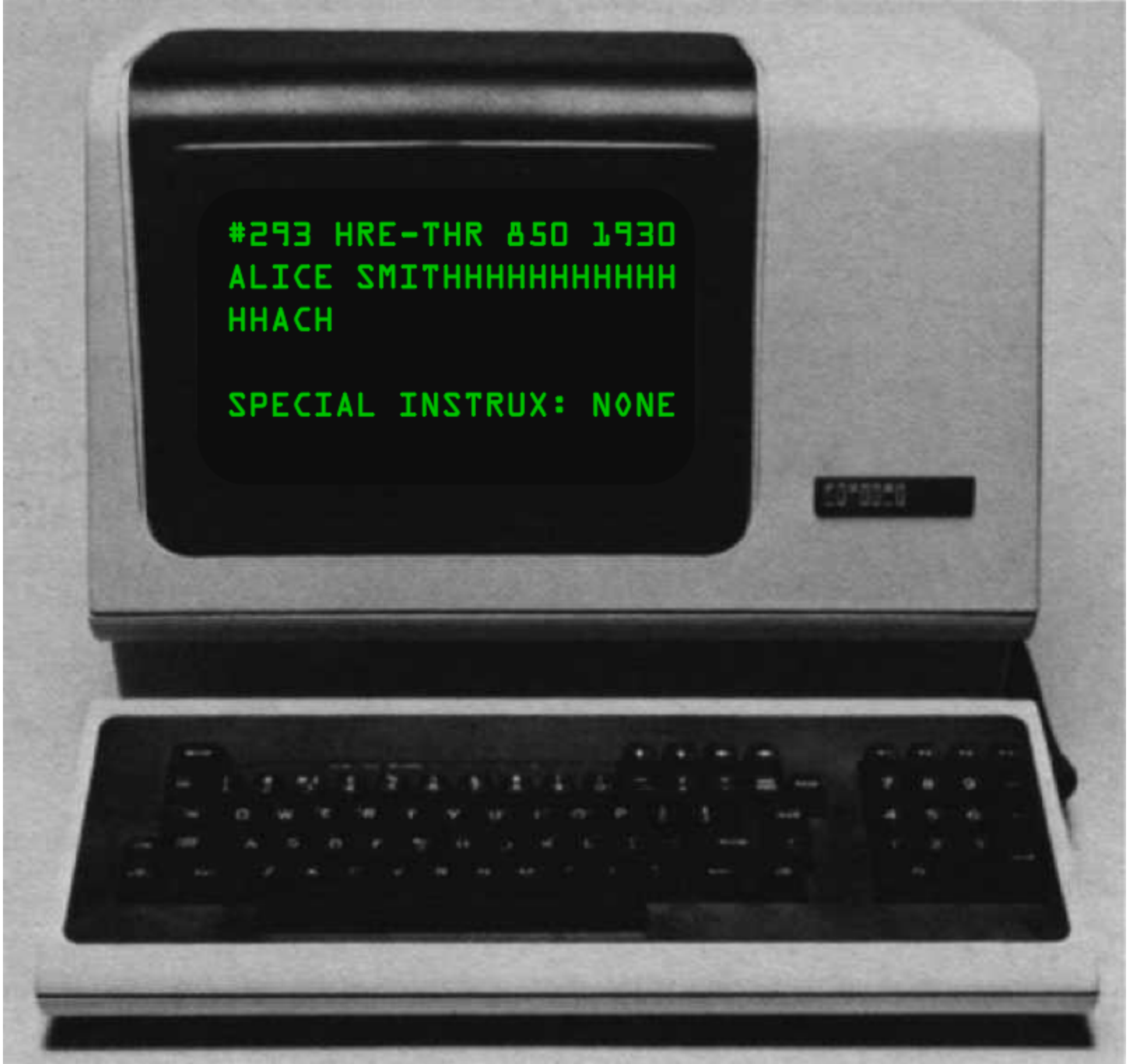
- So, how does one get instructions onto a computer system?
  - Often, by invitation
    - With an unexpected and unchecked reply
    - Physical world analogy: A person is invited to a posh event but shows up drunk and covered in mud
      - This is unexpected (did invite specifically prohibit this? Why would it?)
      - If unchecked (no security to keep person out?), a problem

So, How Exactly Are Databases Hacked?

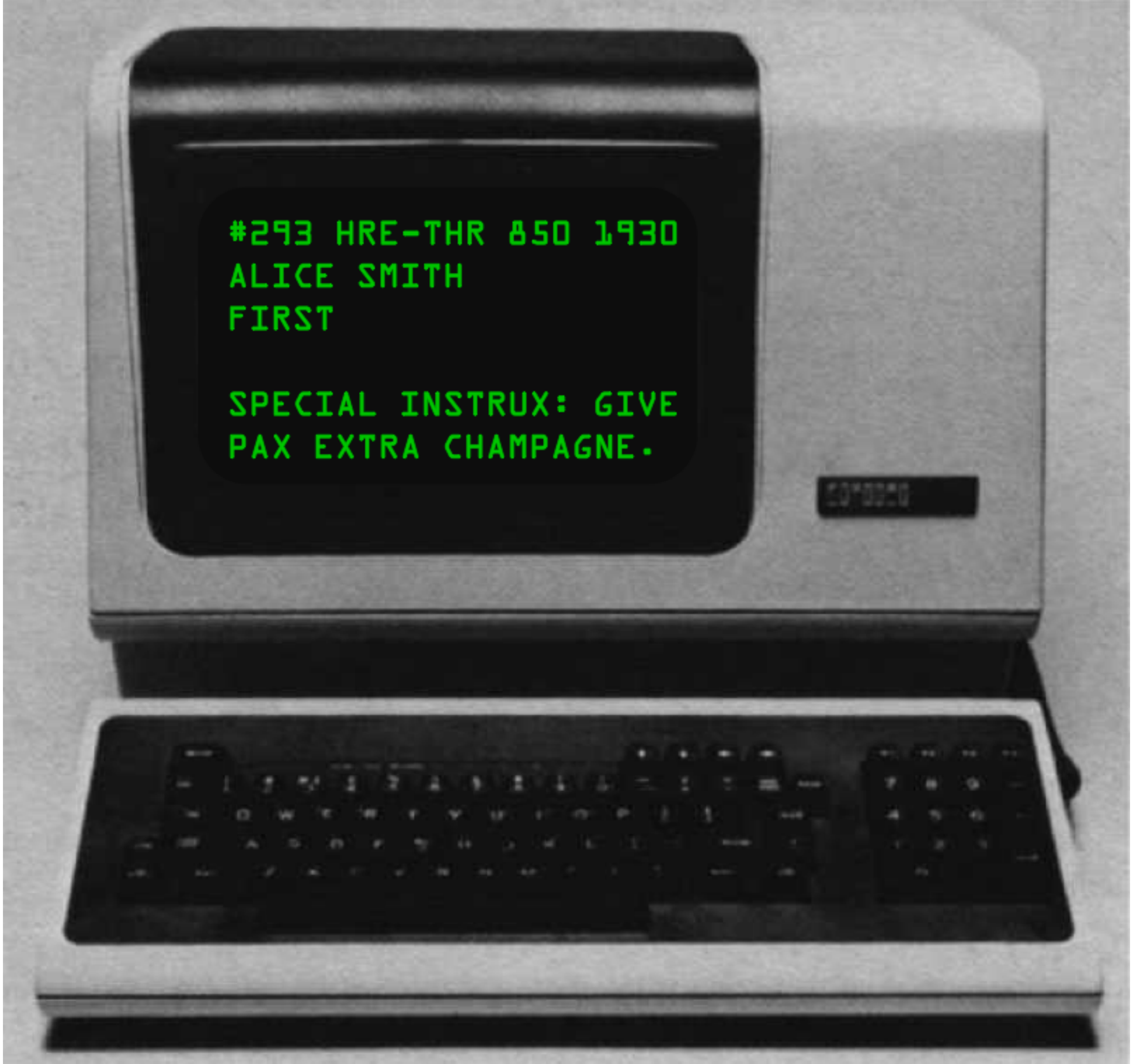
- These code vulnerabilities exist in application code (e.g., Word, Keynote, etc) as well as the code used by web sites
- Let’s look at a small example



```
#293 HRE-THR 850 1930
ALICE SMITH
COACH

SPECIAL INSTRUX: NONE
```



```
#293 HRE-THR 850 1930
ALICE SMITHHHHHHHHHHHH
HHACH

SPECIAL INSTRUX: NONE
```

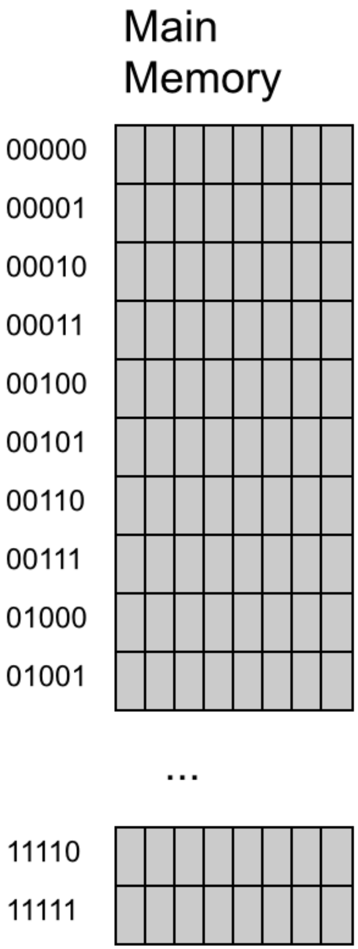


```
#293 HRE-THR 850 1930
ALICE SMITH
FIRST

SPECIAL INSTRUX: GIVE
PAX EXTRA CHAMPAGNE.
```

```
char name[20];
char instrux[80] = "none";

void vulnerable() {
  gets(name);
}
```

So What's Going On Here?

- Recall what memory looks like
  - Suppose `name` is stored at addresses 0 - 19 and `instrux` is stored at addresses 20 - 99
    - What happens if the user enters a name that is more than 20 characters long?



Another Attack: SQL Injection

- SQL: Structured Query Language
  - A widely used language used to facilitate the searching of databases
  - Fetch a set of records

    ```
    SELECT * FROM Person WHERE Username='smith'
    ```

  - Add data to the database

    ```
    INSERT INTO Person(username, balance) VALUES ('smith', 10)
    ```

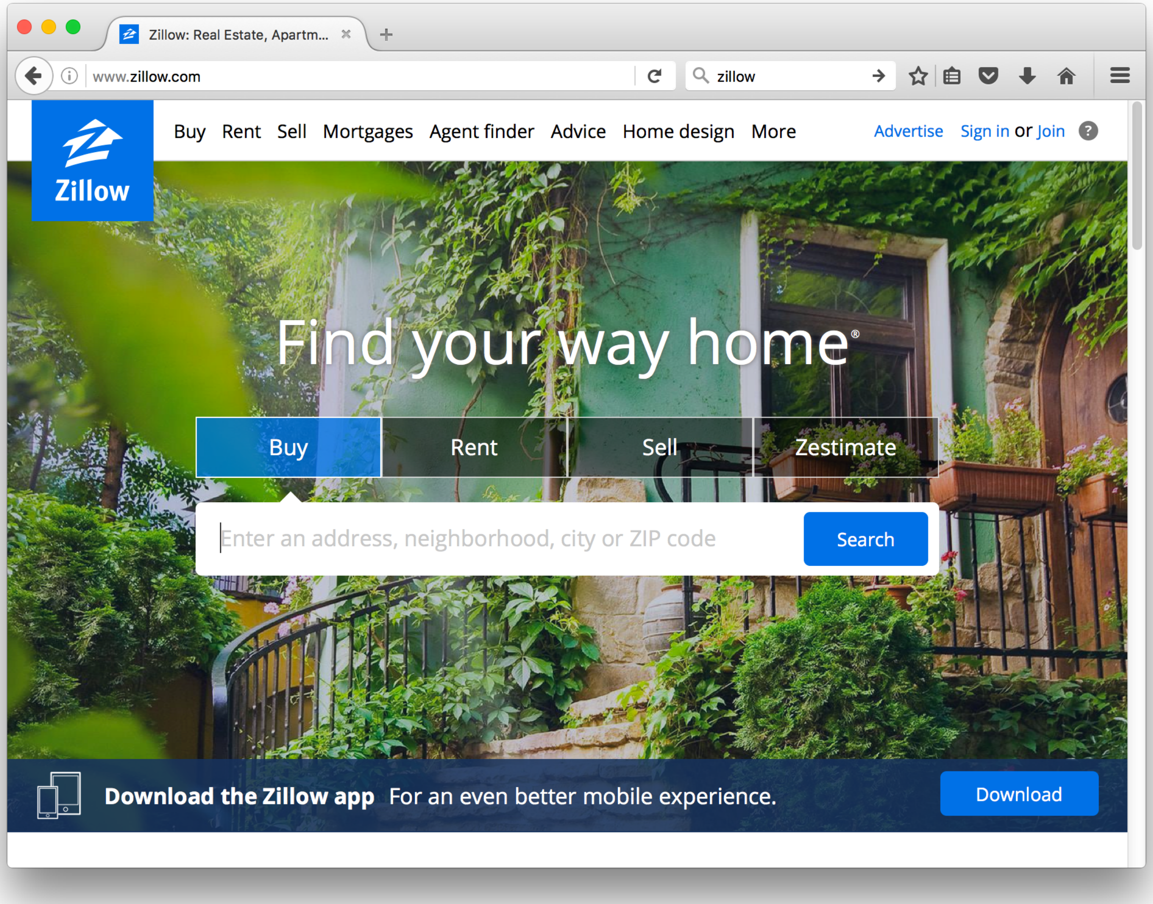
  - Modify data

    ```
    UPDATE Person SET Balance=42 WHERE Username='smith'
    ```

- Query syntax (mostly) independent of vendor

Another Attack: SQL Injection

- I’m coding a web page, and I want you to be able to search a related database



Another Attack: SQL Injection

- So I’m going to write a line of code that looks something like this:

```
SELECT PersonID FROM Person WHERE Balance
  < 100 AND Username='$recipient';
```

- In English: Whatever the user enters, call that $recipient. So please find me the ID numbers of all people in the database whose balance is less than 100, and whose username is what the user supplied in the web form.
  - Works fine if the user actually enters a username

Another Attack: SQL Injection

- So I’m going to write a line of code that looks something like this:

SELECT PersonID FROM Person WHERE Balance < 100 AND Username='$recipient';

- Doesn’t work so well if the user enters this:

foo' OR 1=1 —

- in which case the command becomes

SELECT PersonID FROM Person WHERE Balance < 100 AND Username=‘foo’ OR 1-1 —‘;

- Which says give me the ID of every entry in the database

Another Attack: SQL Injection

```
SELECT PersonID FROM Person WHERE Balance
   < 100 AND Username='$recipient';
```

- Doesn’t work so well if the user enters this:

```
foo'; DROP TABLE Person; --
```

- in which case the command becomes

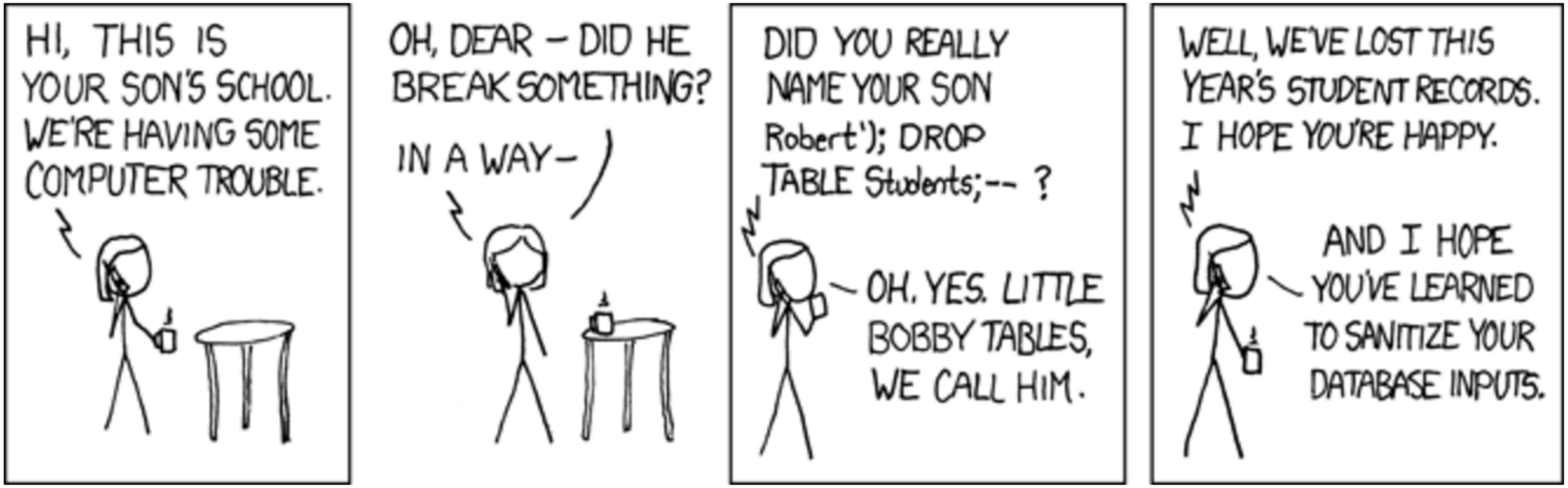
```
SELECT PersonID FROM Person WHERE Balance
   < 100 AND Username=‘foo’; DROP TABLE
   Person; —‘;
```

- Which says give me the ID of the entry with username foo, then delete the entire database

Another Attack: SQL Injection

- This is difficult to prevent, though there are various means of doing so
  - Input sanitization: make sure certain control characters are not contained in what the user entered
    - Difficult to do well
  - Structure code better so that the commands that are issued (e.g., DROP TABLE is a command) are not influenced in any way by what the user enters
    - Think of relation between this and Captain Crunch whistle!

Another Attack: SQL Injection


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Other Types of Web Attacks

- Cross-site scripting (XSS) attacks
  - Roughly, I trick your browser into thinking it’s receiving information from a safe site, when in fact it’s not
- Cross-site request forgery
  - A method by which I fool your browser into doing something for me (or allowing me to do it)
    - For example, transfer money from your bank account to mine

Other Types of Web Attacks

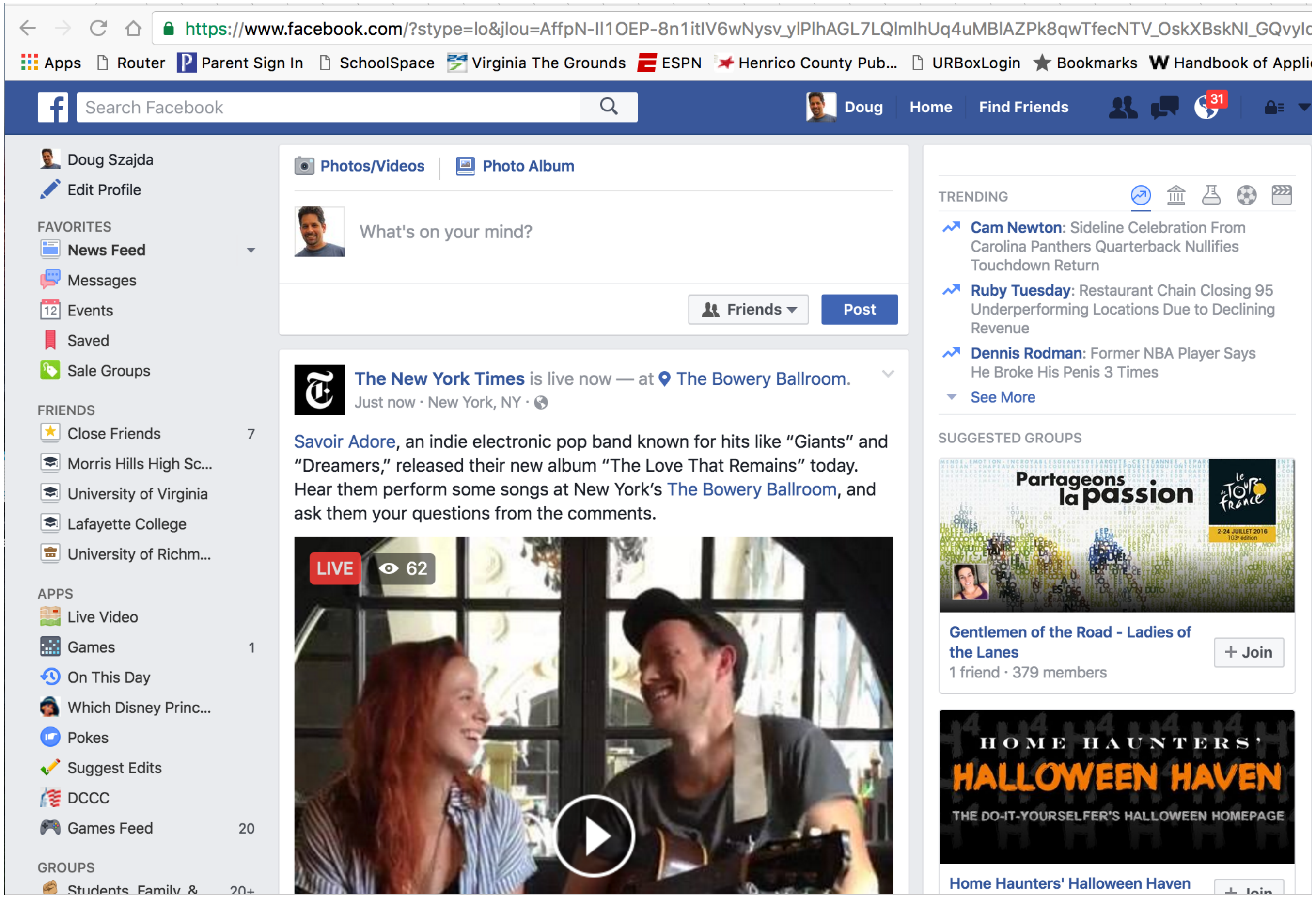
- Drive-by download
  - You visit my site, which uploads malware to your browser
    - And allows me to take over your machine
      - Usually without you knowing it
        - You very likely already have malware on your laptop
- Security folks used to say “practice safe computing”
  - Meaning: don’t visit sites likely to be distributing malware
  - These days, no such thing as “safe site”

What a Web Hacker Wants

- You to visit their site — because your browser will upload whatever the site tells it to
- How do I do this?
  - Advertise a site that shows something you would want(?) to see
    - E.g., pics of Michael Jackson in the morgue
    - Free games
    - Free adult pics
- But basically, I just need you to visit a site where I can place carefully crafted links
  - Can you think of such a site?

What a Web Hacker Wants

- Let’s see: lots of viewers, and user generated content…



The New York Times is live now — at The Bowery Ballroom.
Just now · New York, NY ·

Savoir Adore, an indie electronic pop band known for hits like “Giants” and “Dreamers,” released their new album “The Love That Remains” today. Hear them perform some songs at New York’s The Bowery Ballroom, and ask them your questions from the comments.

Cam Newton: Sideline Celebration From Carolina Panthers Quarterback Nullifies Touchdown Return

Ruby Tuesday: Restaurant Chain Closing 95 Underperforming Locations Due to Declining Revenue

Dennis Rodman: Former NBA Player Says He Broke His Penis 3 Times

See More

Gentlemen of the Road - Ladies of the Lanes
1 friend · 379 members

Home Haunters' Halloween Haven

Web Security is a Bit Off Topic

- But it should be something of which you are aware. It suffers from mission creep
  - Lots of things are done on the web now, none of which were intended when it was originally designed
    - Banking
    - Controlling appliances/home security/home heating systems
    - All sorts of commerce
    - Registering for classes

Web Security is a Bit Off Topic

- Some even want us to vote via the Internet
  - This is a very bad idea
  - Electronic voting systems of any kind, unless they are carefully designed and integrated with mechanisms for a paper audit trail, are in general not a good idea
  - Check it out: https://www.youtube.com/watch?v=aZws98jw67g