CS 161: Computer Security

http://inst.eecs.berkeley.edu/~cs161/

January 16, 2017

Prof. Raluca Ada Popa

ROOM
FIRE
CODE

And a team of a talented TAs

Keyhan Vakil

Won Park

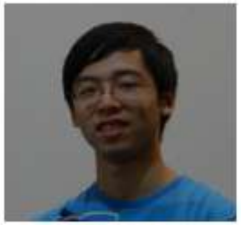
Aditya Chopra

Karthik Shanmugam

Brian Kim

Joanna Yang

Alex Zhang



Richard Hu

Kevyn

Michael McCoyd

Cameron Rasmussen

Mor Nitesh

Head TAs:
Keyhan and
Won

…and talented readers

- Jianan Lu
- Kijung Kim
- Katharine Jiang
- Kate Xu
- Denis Li
- Audrey Ku
- Kevin Ma
- David Niu
- Billy Zhao
- Anusha Syed
- Riku Miyao

What is Computer Security?

- Detects or prevents unwanted use of computer systems or data

Why security?

Obama unveils cybersecurity proposals: 'Cyber threats are urgent and growing danger'

Why should you care?

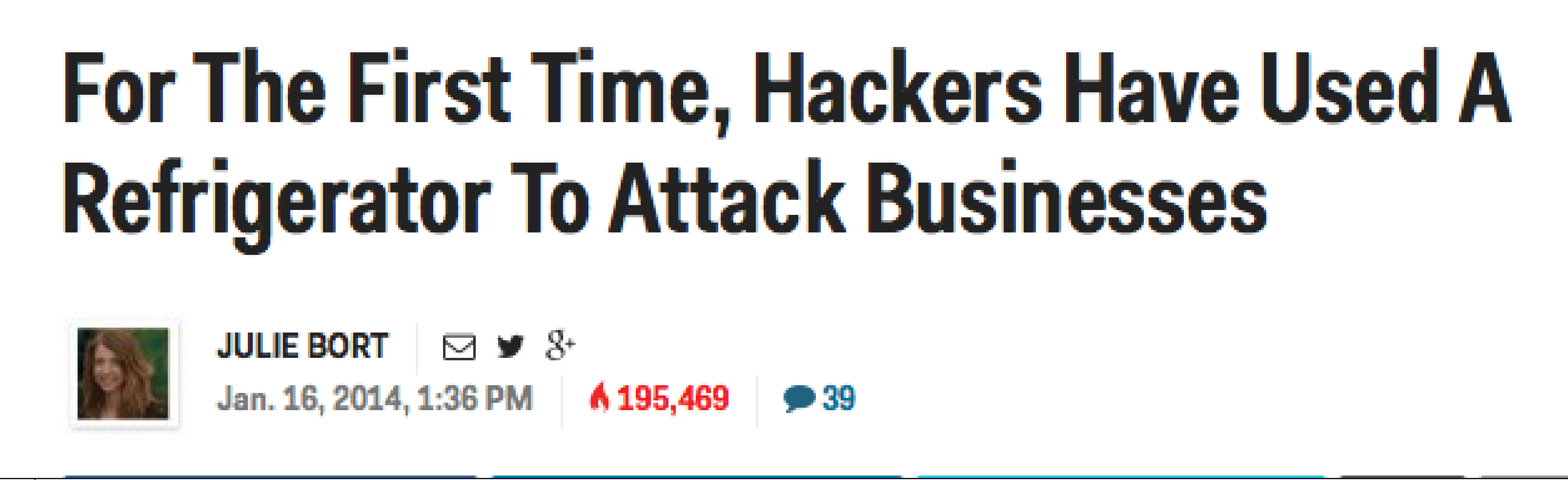
- Impacts everyone’s day-to-day life
  - Millions of compromised computers, millions of stolen passwords, stolen money

It is important for our …

- physical safety and safety of our possessions
- confidentiality of data/ privacy
- functionality

Safety

Adversaries can affect our safety by tampering with pacemakers, planes, cars



For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

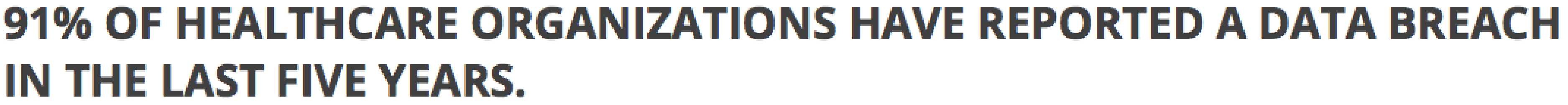
JULIE BORT

Jan. 16, 2014, 1:36 PM | 195,469 | 39

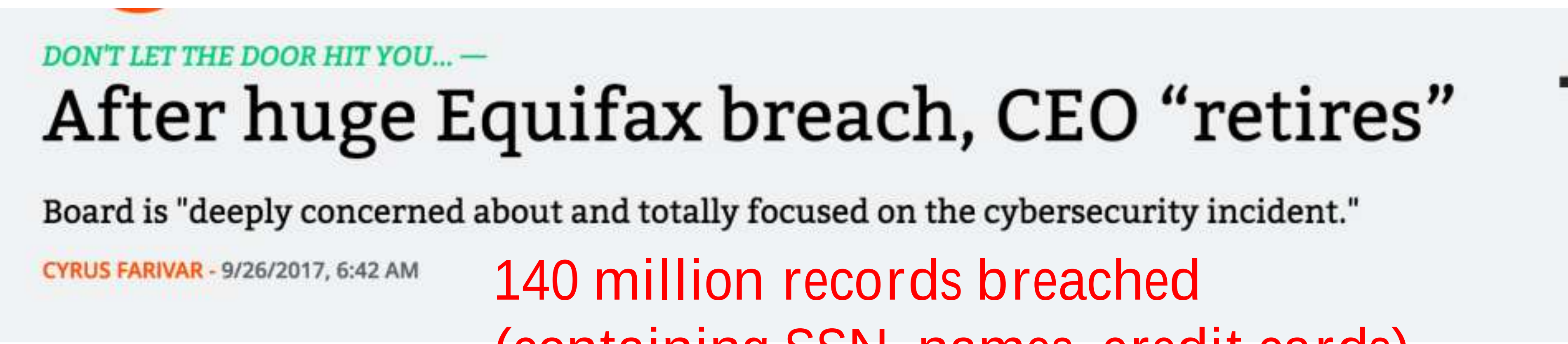
FBI probe of alleged plane hack sparks worries over flight safety

Privacy/confidentiality

- Adversaries get access to medical, financial, personal user data, or sensitive corporate data



91% OF HEALTHCARE ORGANIZATIONS HAVE REPORTED A DATA BREACH IN THE LAST FIVE YEARS.



DON'T LET THE DOOR HIT YOU... —

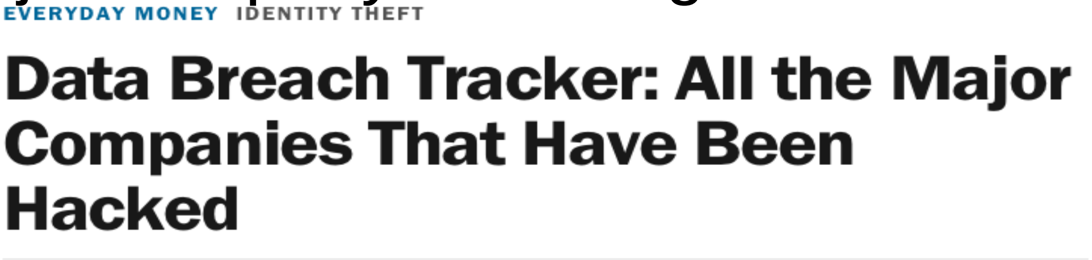
After huge Equifax breach, CEO "retires"

Board is "deeply concerned about and totally focused on the cybersecurity incident."

CYRUS FARIVAR - 9/26/2017, 6:42 AM

140 million records breached
(containing SSN, names, credit cards)

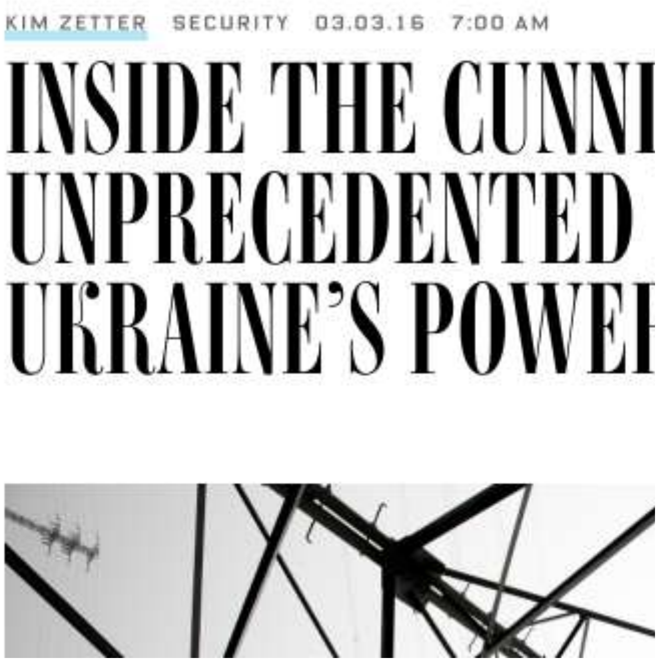
- Pretty much any major company collecting user data has been hacked



EVERYDAY MONEY IDENTITY THEFT

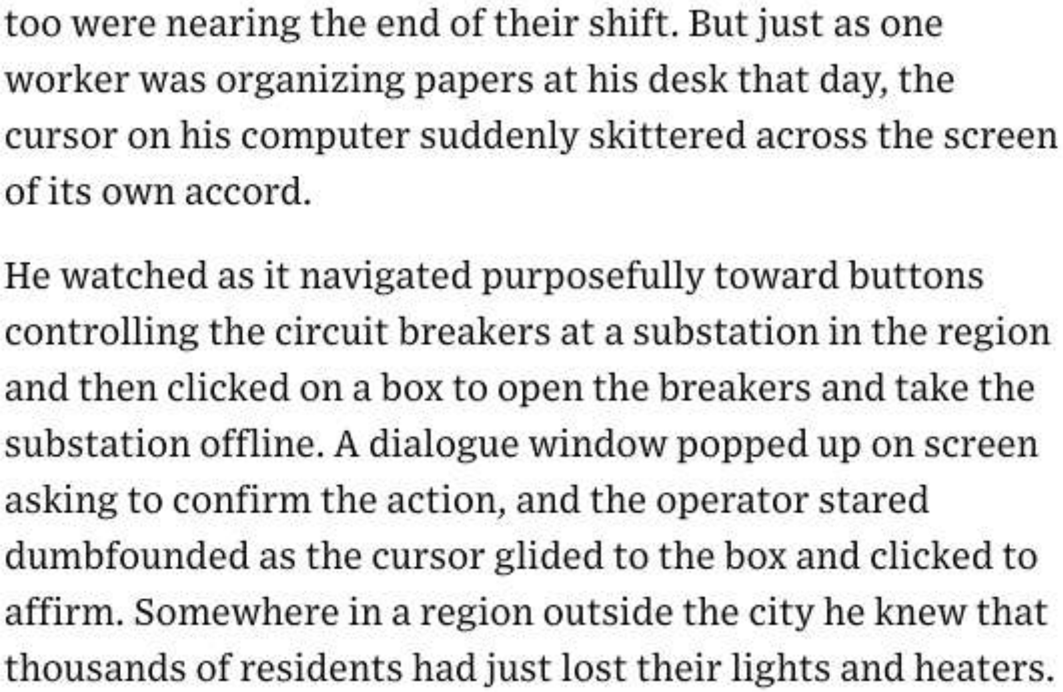
Data Breach Tracker: All the Major Companies That Have Been Hacked

Can affect a country’s economy



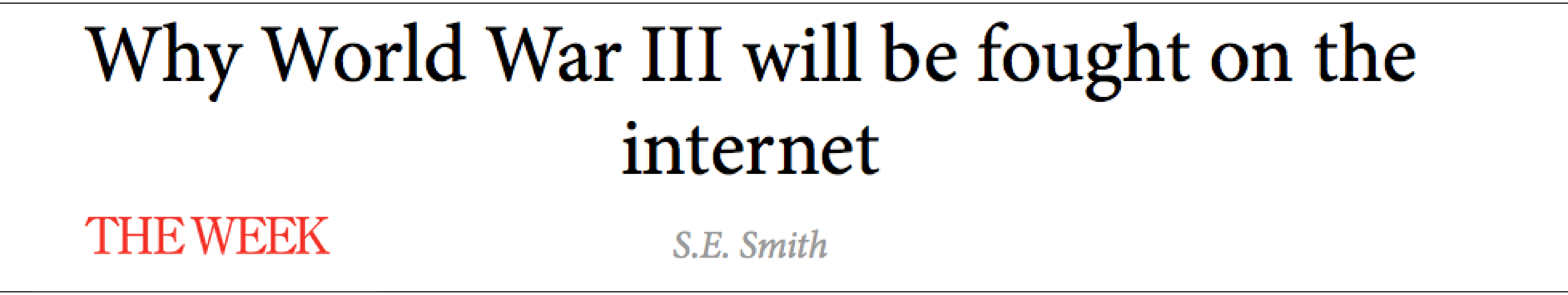
KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNI
UNPRECEDENTED
UKRAINE’S POWE



too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord.

He watched as it navigated purposefully toward buttons controlling the circuit breakers at a substation in the region and then clicked on a box to open the breakers and take the substation offline. A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the box and clicked to affirm. Somewhere in a region outside the city he knew that thousands of residents had just lost their lights and heaters.



Why World War III will be fought on the internet

THE WEEK

S.E. Smith

Learn About Security

Make a Difference

Computer security is not only important but it is …

FUN!

- You are playing a game: can you stop the attacker?
- Beautiful blend of analytical thinking (math) and engineering (build systems)

Computer security is varied

It has room for many skills

- Cryptography
- Network security
- Operating systems security
- Web security
- Database security
- Distributed systems security
- Machine learning and security
- Security usability

Big challenge: many of you **don't yet have** the expertise in those areas

Provides a glimpse of these disciplines

Tell us what concepts you need more background in

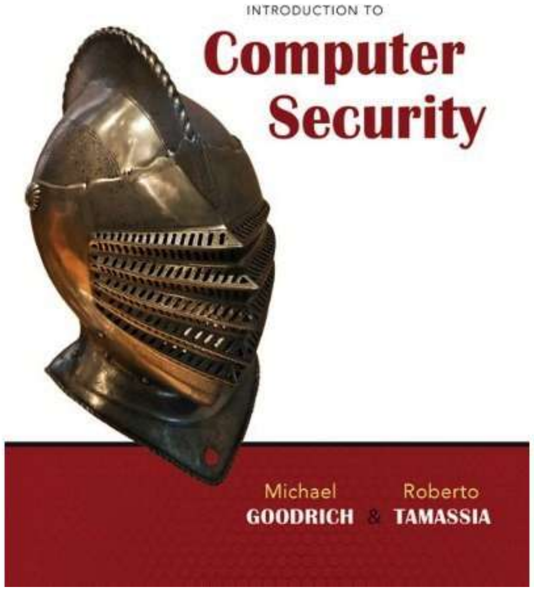
Logistics

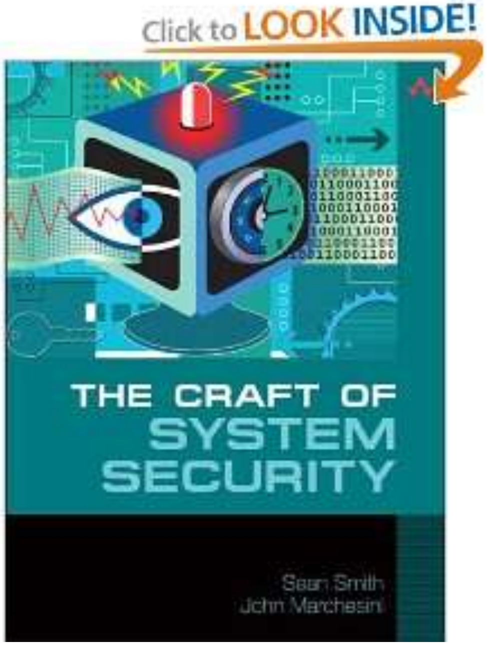
Course Structure

- Absorb material presented in lectures and section
  - Lecture will be webcasted
- 3 course projects (24% total)
  - Done individually or in small groups
- ~4 homeworks (16% total)
  - Done individually
- Two midterms (30%)
- A comprehensive final exam (30%)

Textbooks

- No required textbook. If you want extra reading:
- *Optional*: *Introduction to Computer Security*, Goodrich & Tamassia
- *Optional*: The Craft of System Security, Smith & Marchesini





Class Policies

- Late homework: no credit
- Late project: -10% if < 24 hrs, -20% < 48 hrs, -40% < 72 hrs, **no credit** ≥ 72 hrs
- Never read or share solutions, code, etc. with someone else, nor read past materials: work on your own (unless assignment states otherwise).
- If lecture materials available prior to lecture, *don't use to answer questions* during class
- Participate in Piazza
  - Send course-related questions/comments, or ask in office hours. No email please: it doesn't scale.

Ethics

- Do not cheat, it’s bad for you and others
- We will be looking for plagiarism, both manually and using advanced software; we can identify copy even if not exact, including from old material or submissions
- We will apply severe penalties including reporting to Student Conduct office

THREAT MODELS

Threat models

- Cannot protect against all possible attackers
- High-level goal is risk management
  - Much of the effort concerns *raising the bar* and *trading off resources*
    - How to prudently spend your time & money?
- Key notion of threat model: what you are defending against
  - Determines which defenses are worthwhile

Threats have evolved…

- 1990’s: bragging rights
- late 2000’s: financially motivated
  - Spam, pharmaceuticals, credit card theft, identity theft

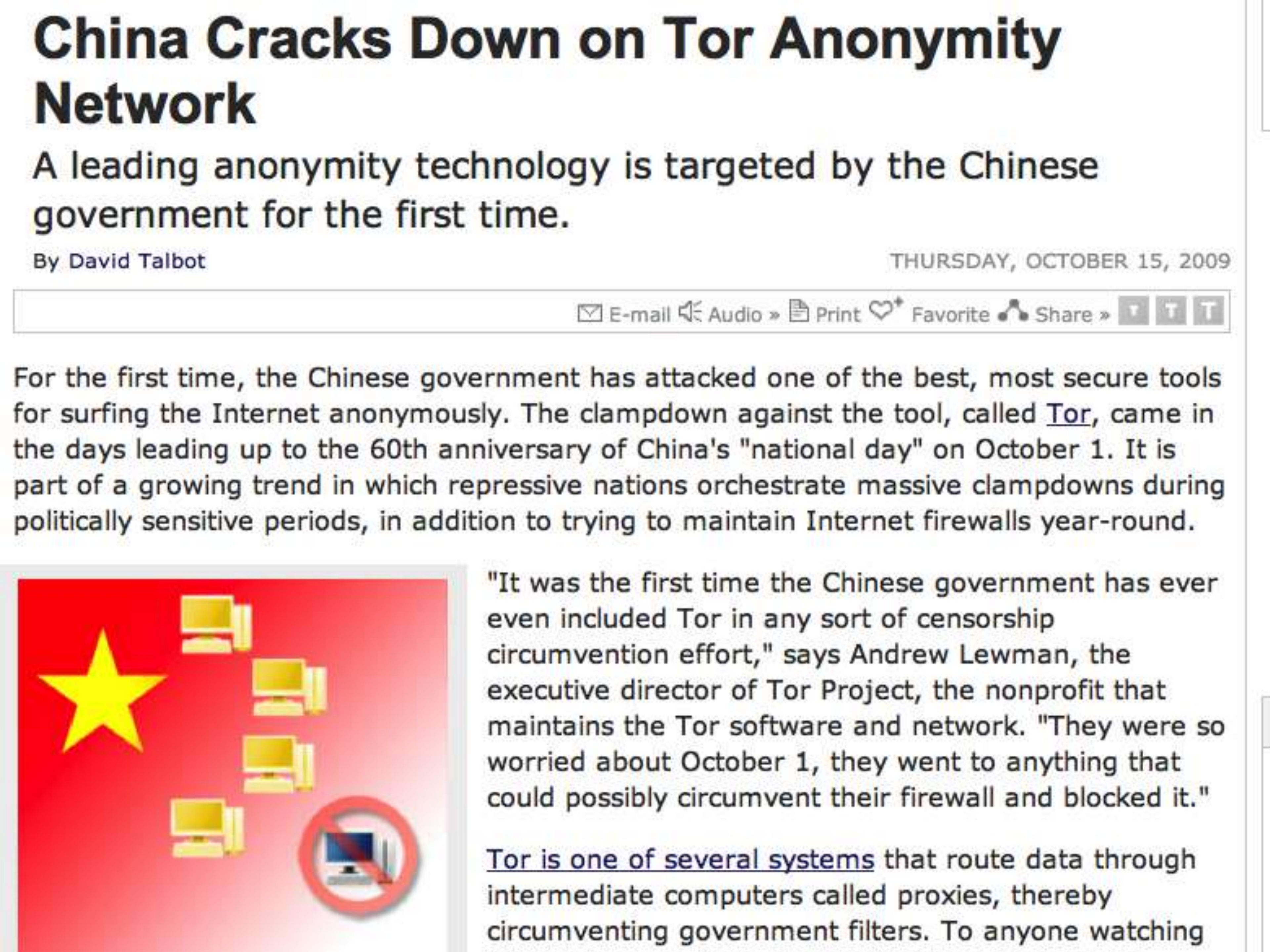
Threats have evolved…

- Attackers have become more sophisticated; arms race between attackers and defenders fuels rapid innovation in malware
  - but not all security is an arms race, there are definite solutions to certain settings

- Many attacks aim for profit and are facilitated by a well-developed “underground economy”

Threats have evolved…

- 1990’s: bragging rights
- late 2000’s: financially motivated
  - Spam, pharmaceuticals, credit card theft, click fraud
- 2010’s: politically motivated
  - Government actors: Stuxnet, Flame, Aurora, Sony
  - Private activism: Anonymous, Wikileaks



China Cracks Down on Tor Anonymity Network

A leading anonymity technology is targeted by the Chinese government for the first time.

By David Talbot

THURSDAY, OCTOBER 15, 2009

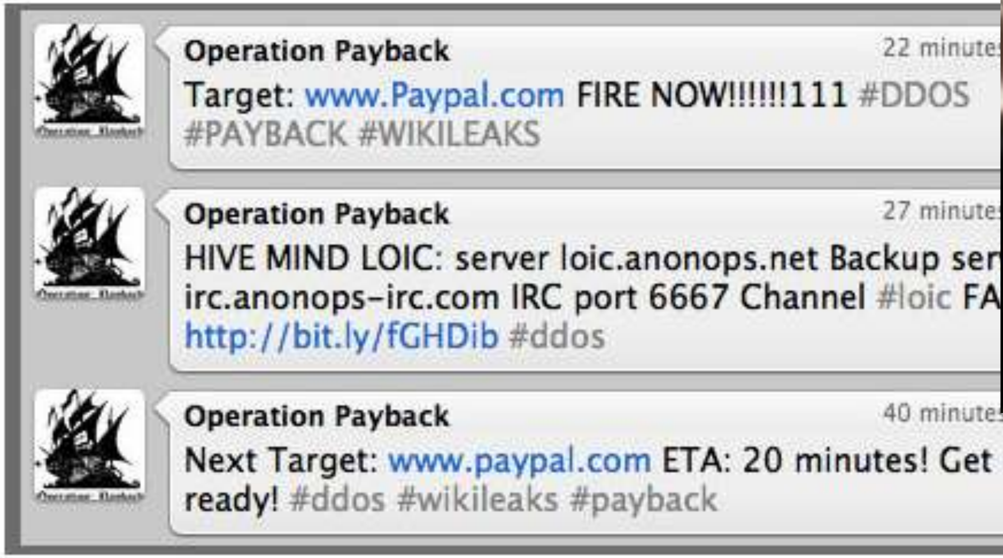
For the first time, the Chinese government has attacked one of the best, most secure tools for surfing the Internet anonymously. The clampdown against the tool, called Tor, came in the days leading up to the 60th anniversary of China's "national day" on October 1. It is part of a growing trend in which repressive nations orchestrate massive clampdowns during politically sensitive periods, in addition to trying to maintain Internet firewalls year-round.

"It was the first time the Chinese government has ever even included Tor in any sort of censorship circumvention effort," says Andrew Lewman, the executive director of Tor Project, the nonprofit that maintains the Tor software and network. "They were so worried about October 1, they went to anything that could possibly circumvent their firewall and blocked it."

Tor is one of several systems that route data through intermediate computers called proxies, thereby circumventing government filters. To anyone watching

Continuing pro-Wikileaks DDOS actions, Anonymous takes down PayPal.com

Xeni Jardin at 7:10 PM Wednesday, Dec 8, 2010



Operation Payback 22 minutes

Target: www.Paypal.com FIRE NOW!!!!!!111 #DDOS #PAYBACK #WIKILEAKS

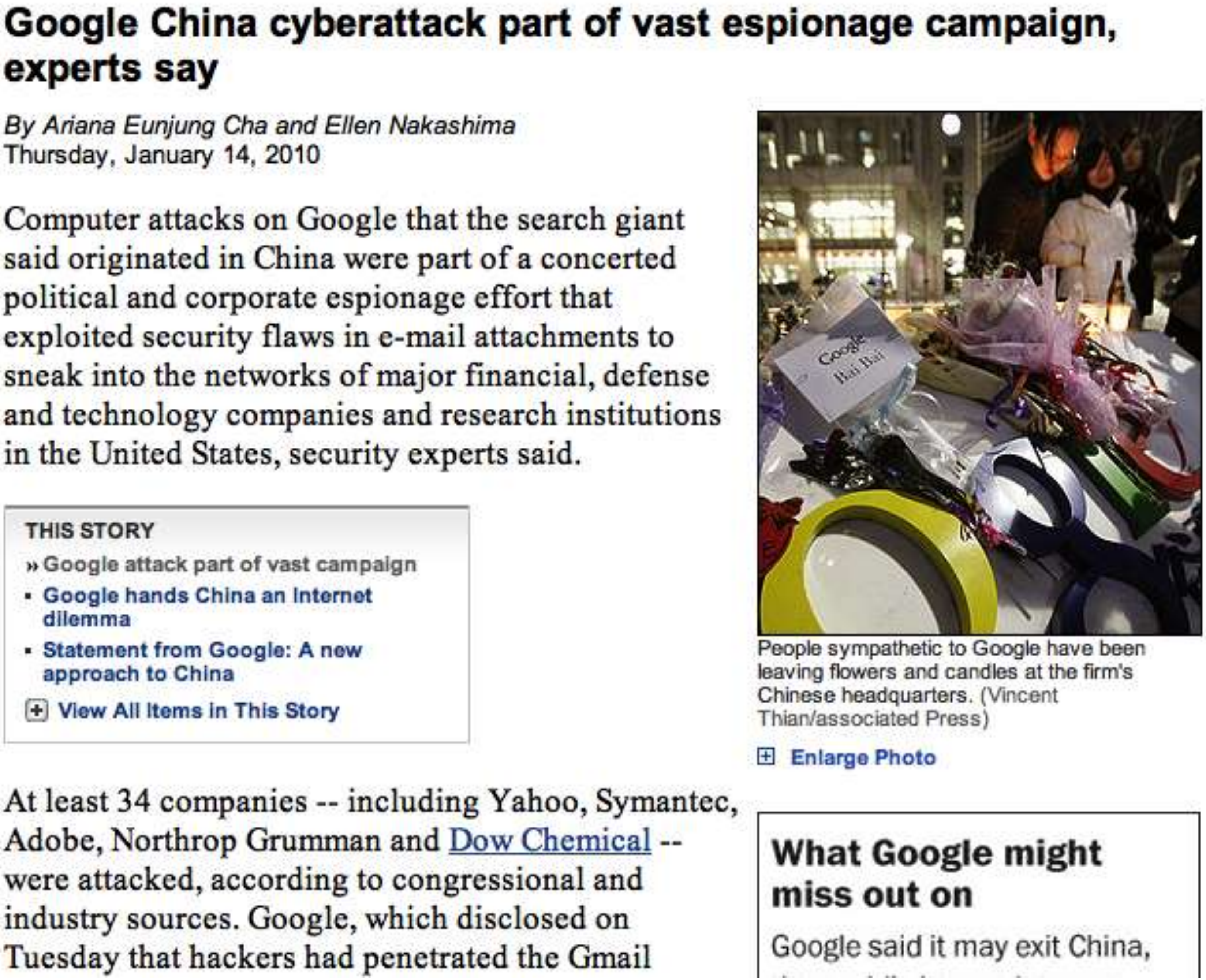
Operation Payback 27 minute

HIVE MIND LOIC: server loic.anonops.net Backup ser irc.anonops-irc.com IRC port 6667 Channel #loic FA http://bit.ly/fGHDib #ddos

Operation Payback 40 minutes ago

Next Target: www.paypal.com ETA: 20 minutes! Get ready! #ddos #wikileaks #payback

Third finance-related Anonymous "Operation Payback" takedown in a single day: PayPal.com is effectively offline, moments after the command was tweeted. At the time of this blog post, the PayPal *service* is still functioning, but the site's dead. Earlier today, Visa.com and Mastercard.com were taken offline by Anonymous DDOS attacks, along with other targets perceived as enemies of Wikileaks and of online free speech... including Twitter.com, for a while.



Google China cyberattack part of vast espionage campaign, experts say

By Ariana Eunjung Cha and Ellen Nakashima
Thursday, January 14, 2010

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States, security experts said.

THIS STORY

- » Google attack part of vast campaign
- Google hands China an Internet dilemma
- Statement from Google: A new approach to China

⊞ View All Items in This Story

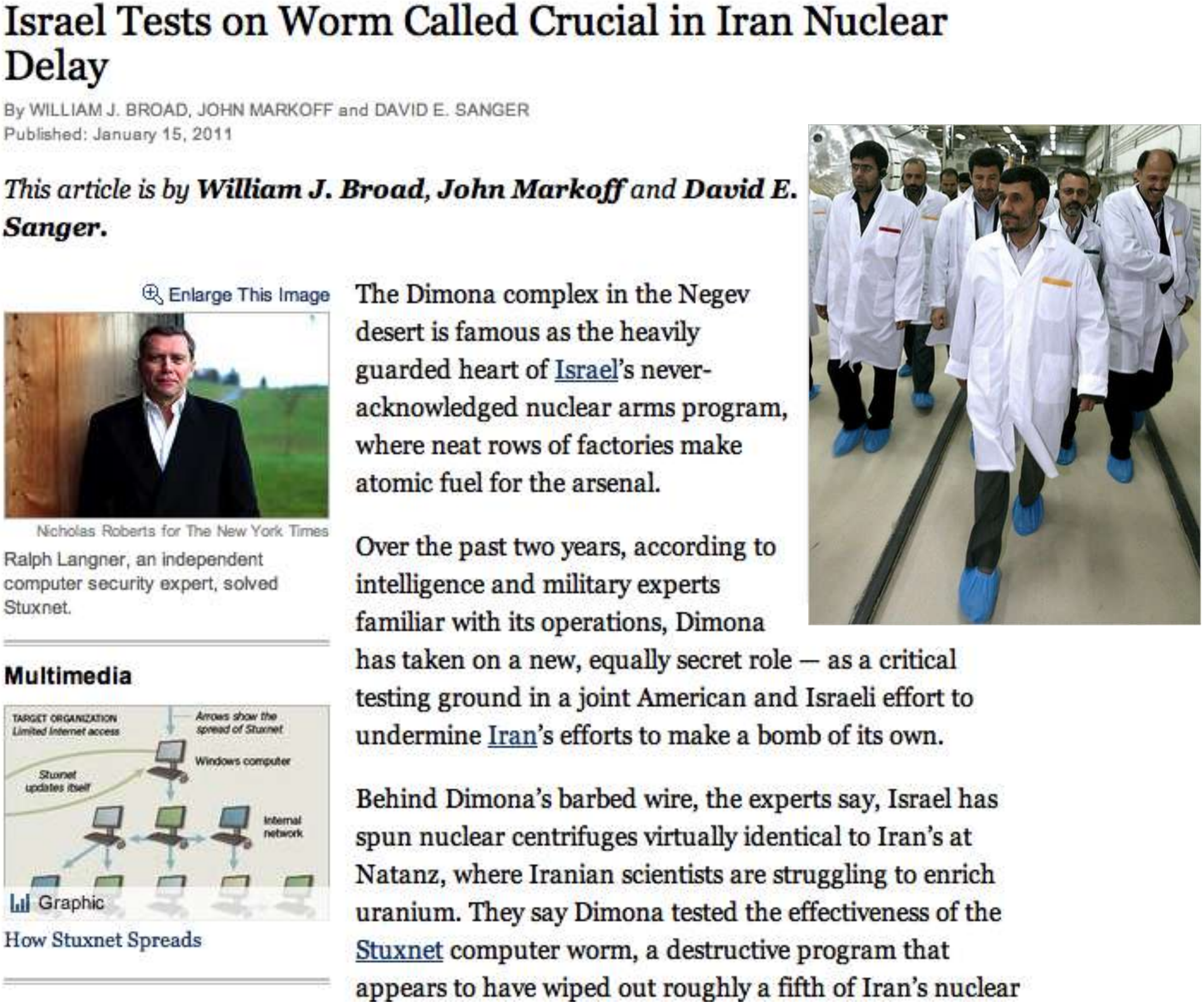
People sympathetic to Google have been leaving flowers and candles at the firm's Chinese headquarters. (Vincent Thian/associated Press)

⊞ Enlarge Photo

At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical -- were attacked, according to congressional and industry sources. Google, which disclosed on Tuesday that hackers had penetrated the Gmail

What Google might miss out on

Google said it may exit China,



Israel Tests on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER
Published: January 15, 2011

This article is by ***William J. Broad, John Markoff*** *and* ***David E. Sanger.***

Enlarge This Image

Nicholas Roberts for The New York Times

Ralph Langner, an independent computer security expert, solved Stuxnet.

Multimedia

Graphic

How Stuxnet Spreads

The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel's never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine Iran's efforts to make a bomb of its own.

Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the Stuxnet computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear

Lesson

- To protect computer systems, you must know your enemy

- Security is not about perfection: it’s about defenses that are good enough to stop the threats you’re likely to encounter

2 CLASSICAL EXPLOITS

Epic Hack: Internet worm

- The first Internet worm, Morris worm
- A grad student experimented (in the lab) with self-spreading malware
- It got out.

Epic Hack: Internet worm

- The first Internet worm
- A grad student experimented (in the lab) with self-spreading malware
- It got out
- And took down the Internet

Epic Hack: Internet worm

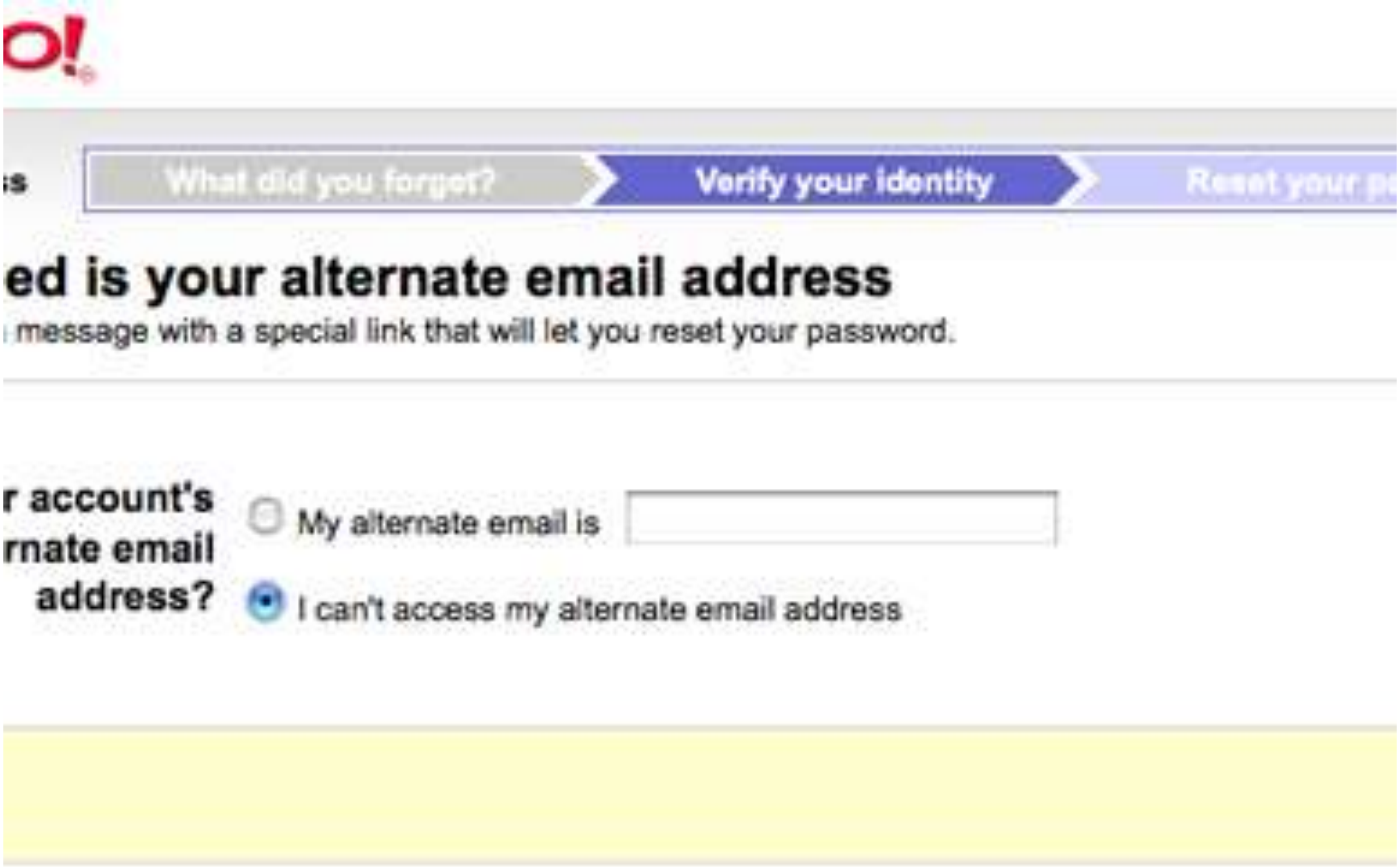
- The first Internet worm
- A grad student experimented (in the lab) with self-spreading malware
- It got out.
- And took down the Internet.

- There is a lesson here.

Epic Hack: Sarah Palin

- Guy wants to mess with Sarah Palin’s campaign
- Tries logging into her Yahoo Mail account, sees her security questions…

Epic Hack: Sarah Palin



ed is your alternate email address

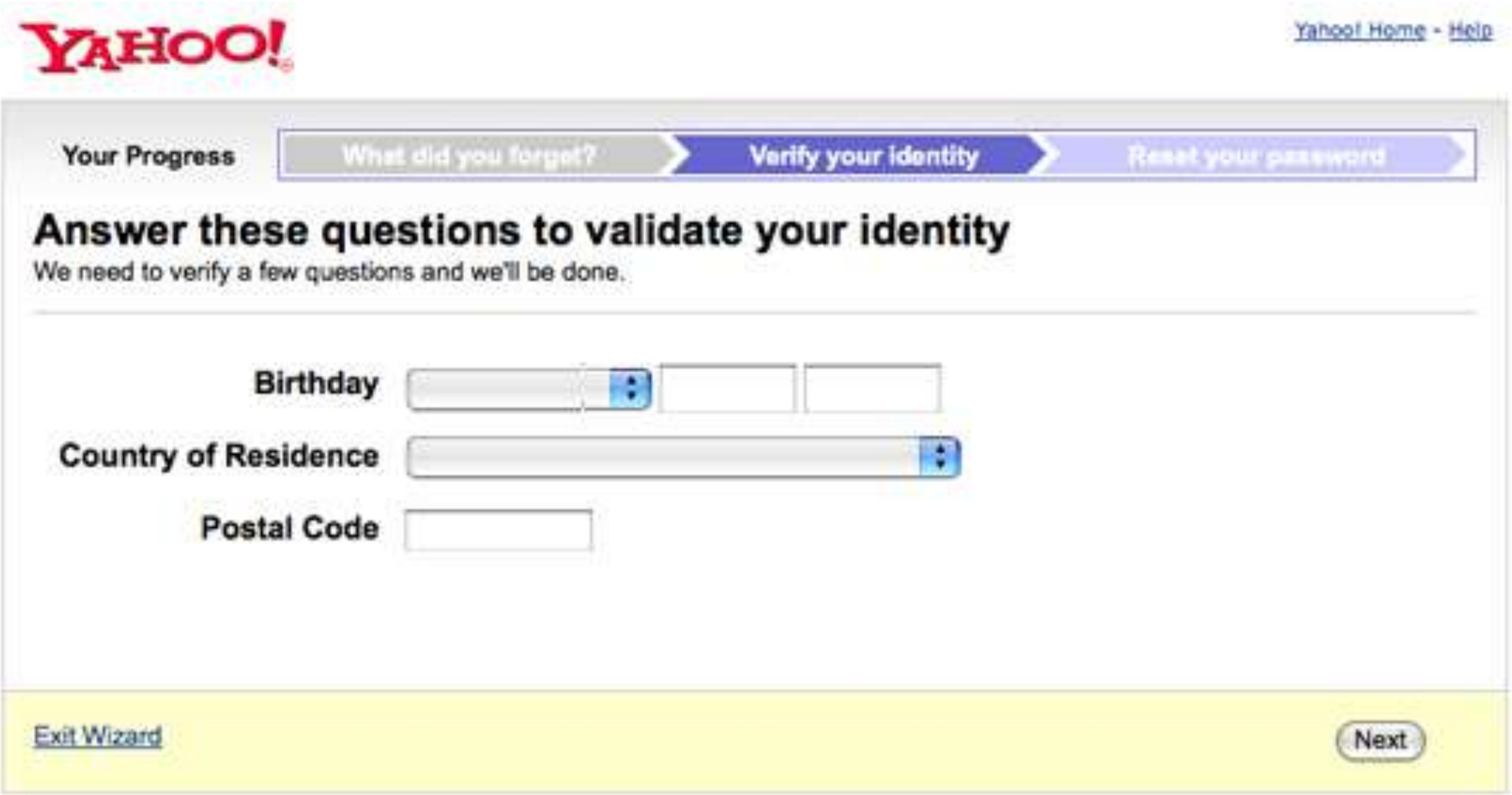
message with a special link that will let you reset your password.

r account's rnate email address?

○ My alternate email is

● I can't access my alternate email address

Epic Hack: Sarah Palin



YAHOO!

Yahoo! Home - Help

Your Progress: What did you forget? › Verify your identity › Reset your password

Answer these questions to validate your identity

We need to verify a few questions and we'll be done.

Birthday

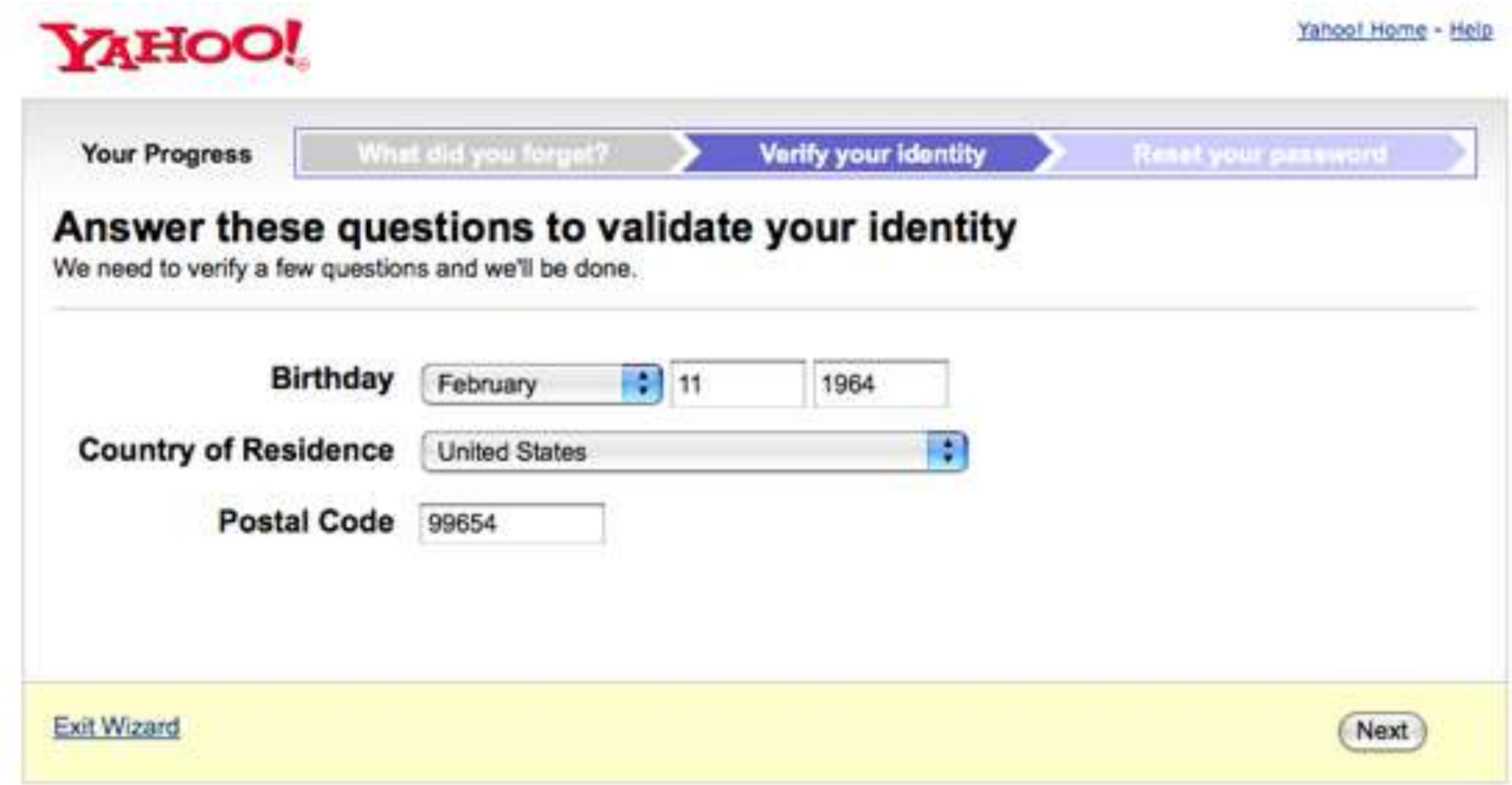
Country of Residence

Postal Code

Exit Wizard

Next

Epic Hack: Sarah Palin

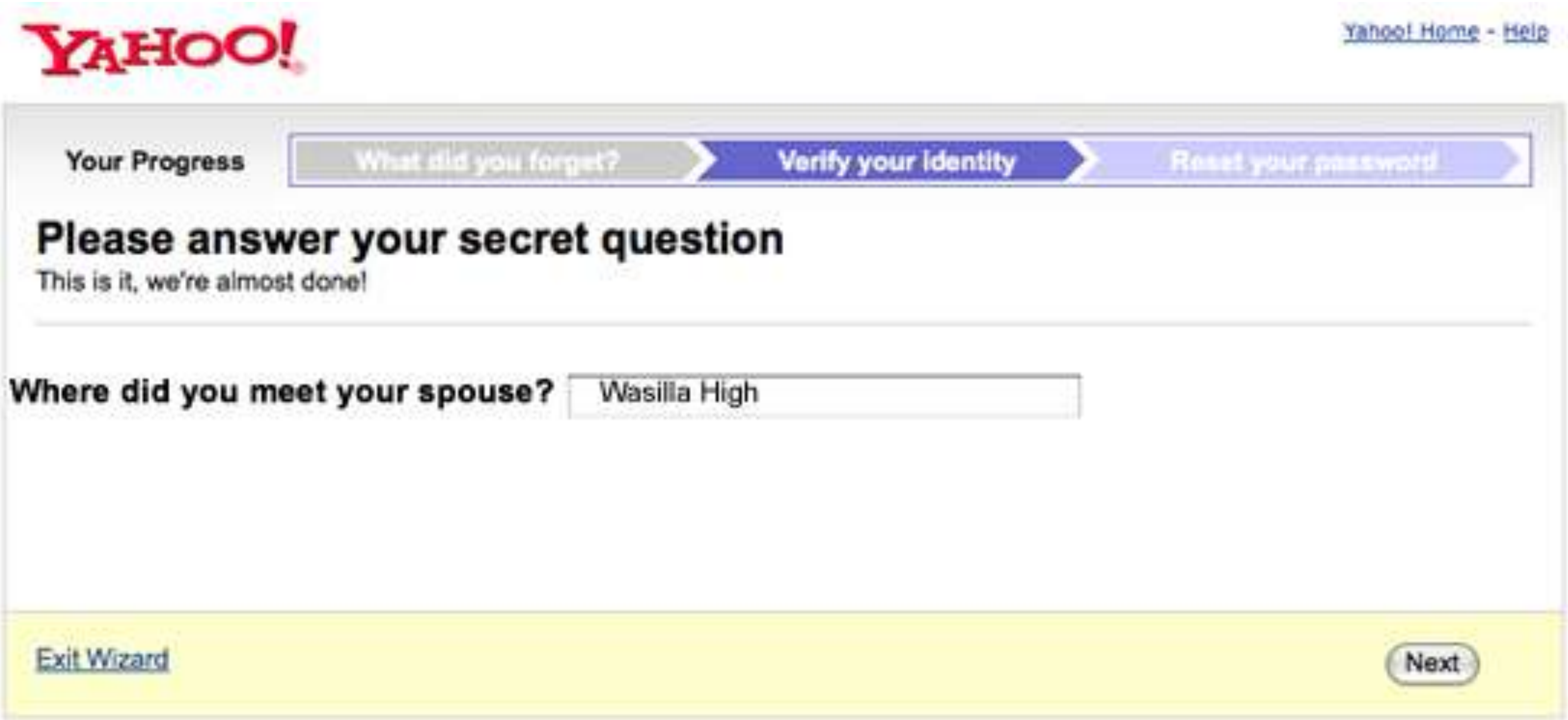


Answer these questions to validate your identity

We need to verify a few questions and we'll be done.

Birthday	February 11 1964
Country of Residence	United States
Postal Code	99654

Epic Hack: Sarah Palin

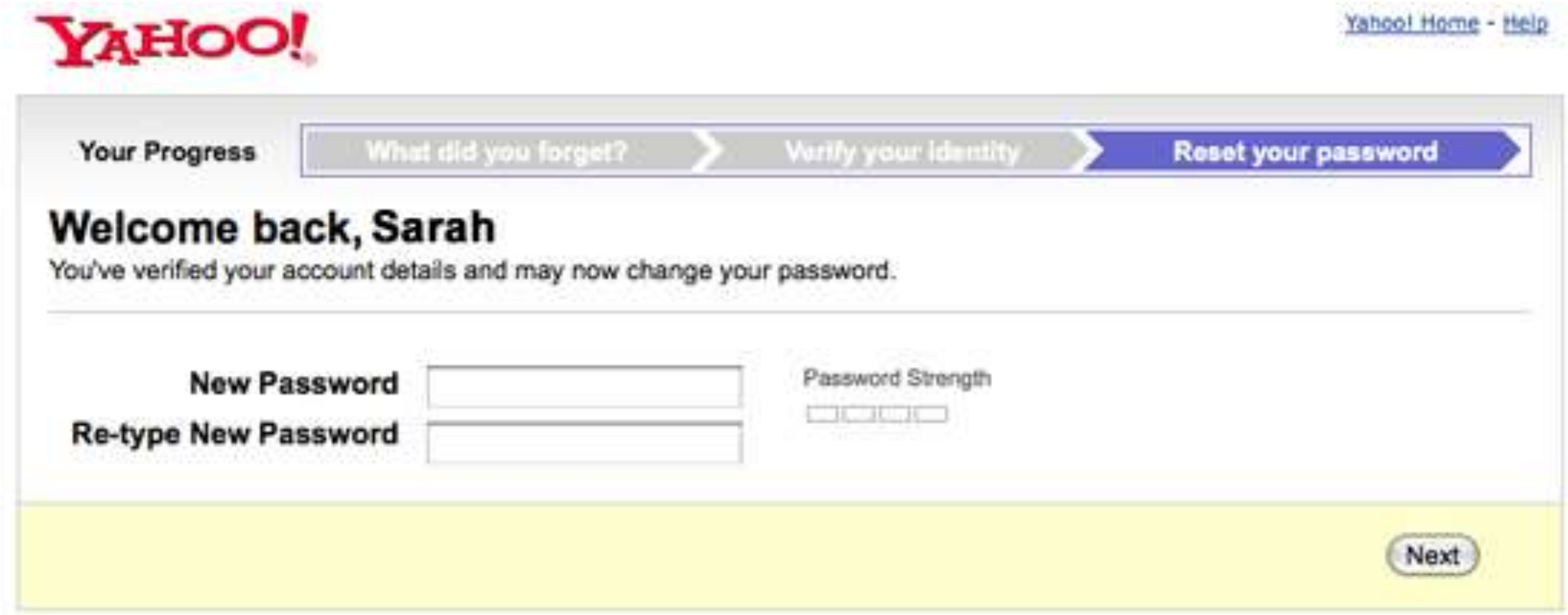


Please answer your secret question

This is it, we're almost done!

Where did you meet your spouse? Wasilla High

Epic Hack: Sarah Palin



Welcome back, Sarah

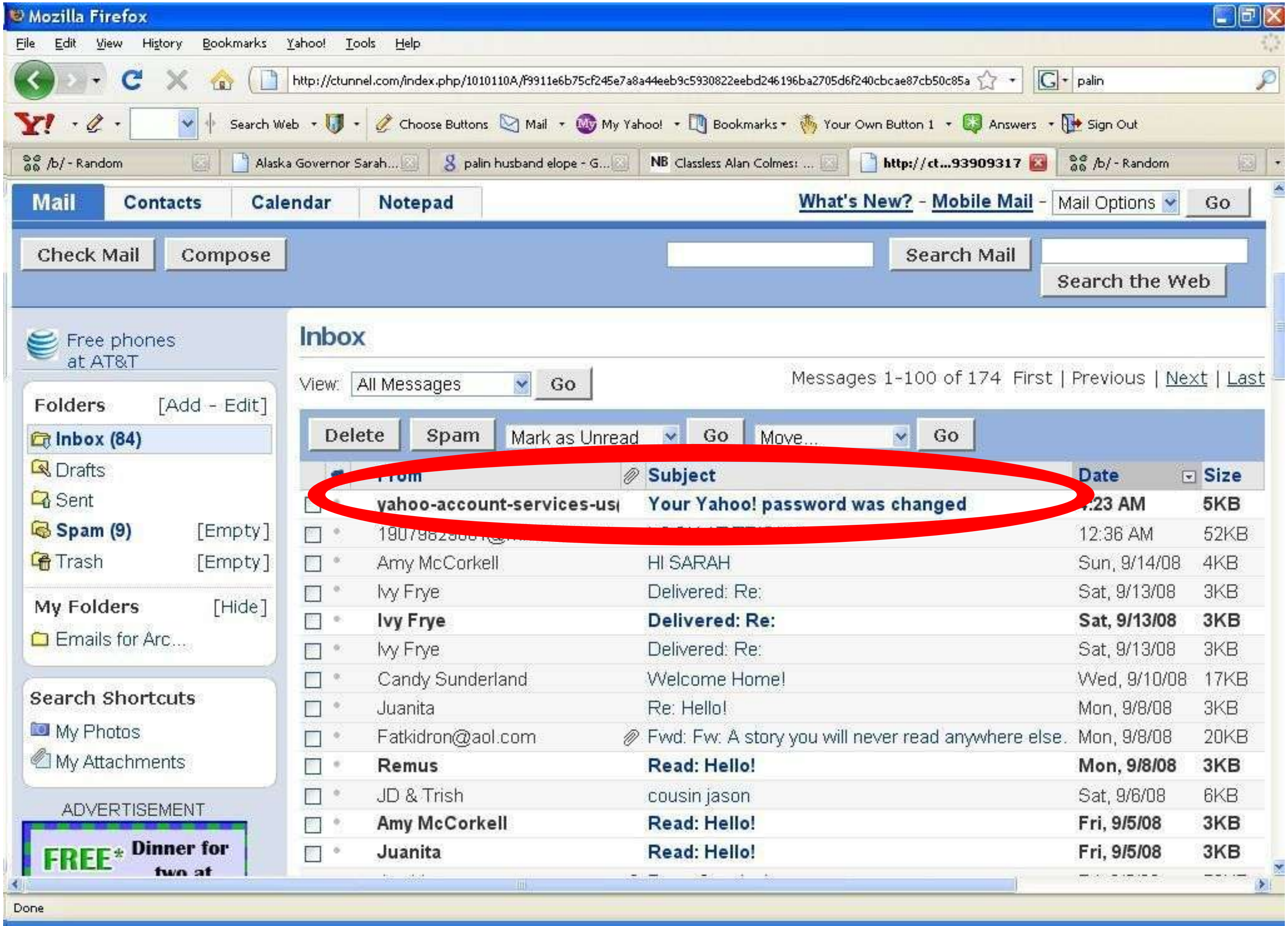
You've verified your account details and may now change your password.

New Password

Re-type New Password

Password Strength

Epic Hack: Sarah Palin



From	Subject	Date	Size
yahoo-account-services-us	Your Yahoo! password was changed	[illegible]:23 AM	5KB
1907982500[illegible]	[illegible]	12:36 AM	52KB
Amy McCorkell	HI SARAH	Sun, 9/14/08	4KB
Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
Ivy Frye	**Delivered: Re:**	**Sat, 9/13/08**	**3KB**
Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
Candy Sunderland	Welcome Home!	Wed, 9/10/08	17KB
Juanita	Re: Hello!	Mon, 9/8/08	3KB
Fatkidron@aol.com	Fwd: Fw: A story you will never read anywhere else.	Mon, 9/8/08	20KB
Remus	**Read: Hello!**	**Mon, 9/8/08**	**3KB**
JD & Trish	cousin jason	Sat, 9/6/08	6KB
Amy McCorkell	**Read: Hello!**	**Fri, 9/5/08**	**3KB**
Juanita	**Read: Hello!**	**Fri, 9/5/08**	**3KB**

Epic Hack: Sarah Palin

- Sentenced to 1 year in federal prison

Lesson: your system is only as secure as the weakest link.

Epic Hack: Sarah Palin

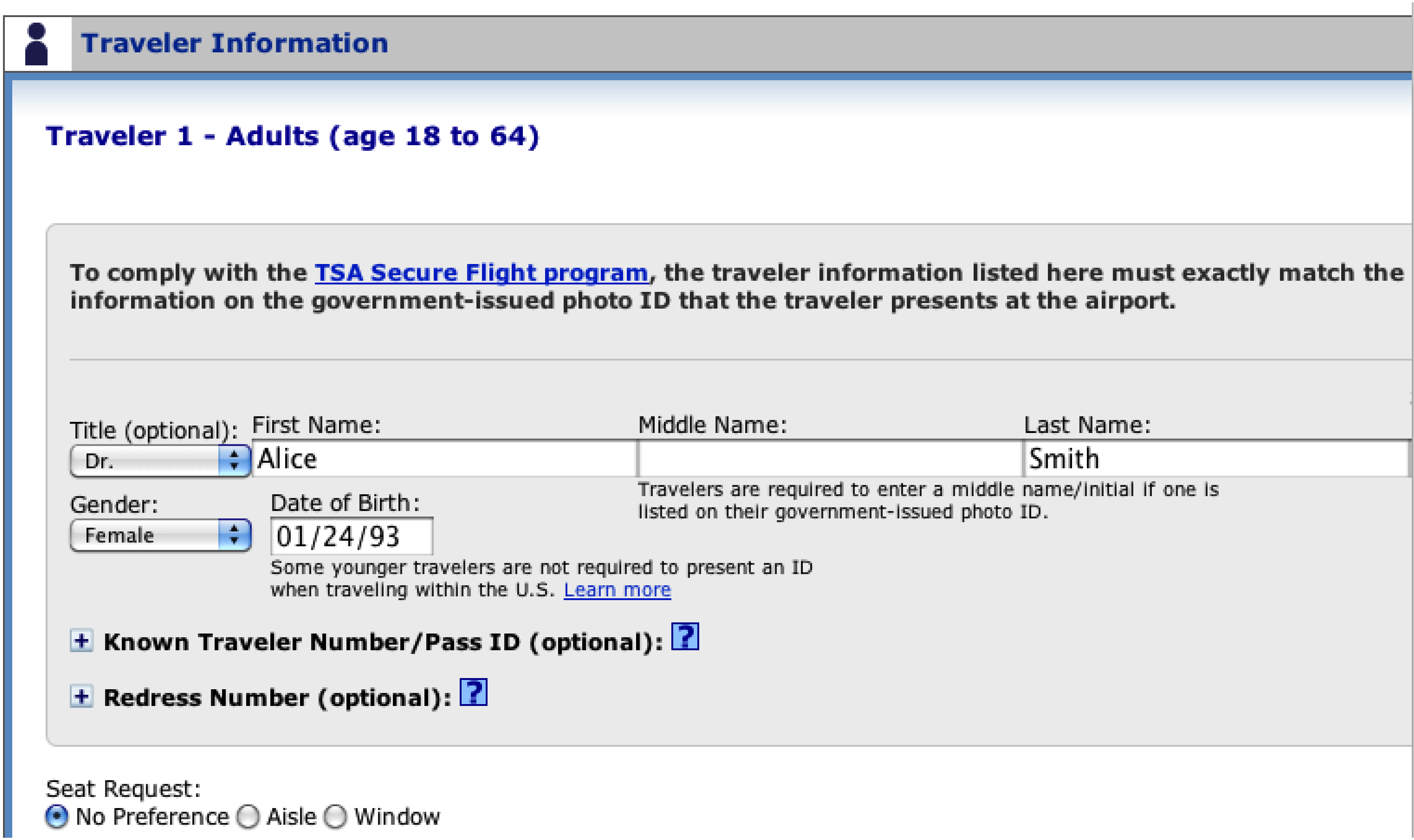
- Aftermath: in 2012, someone hacks Mitt Romney’s email account

Epic Hack: Sarah Palin

- Aftermath: in 2012, someone hacks Mitt Romney’s email account
- … by guessing the name of his pet dog

Lesson: old attacks remain relevant

Memory safety



Traveler Information

Traveler 1 - Adults (age 18 to 64)

To comply with the TSA Secure Flight program, the traveler information listed here must exactly match the information on the government-issued photo ID that the traveler presents at the airport.

Title (optional): Dr.

First Name: Alice

Middle Name:

Last Name: Smith

Travelers are required to enter a middle name/initial if one is listed on their government-issued photo ID.

Gender: Female

Date of Birth: 01/24/93

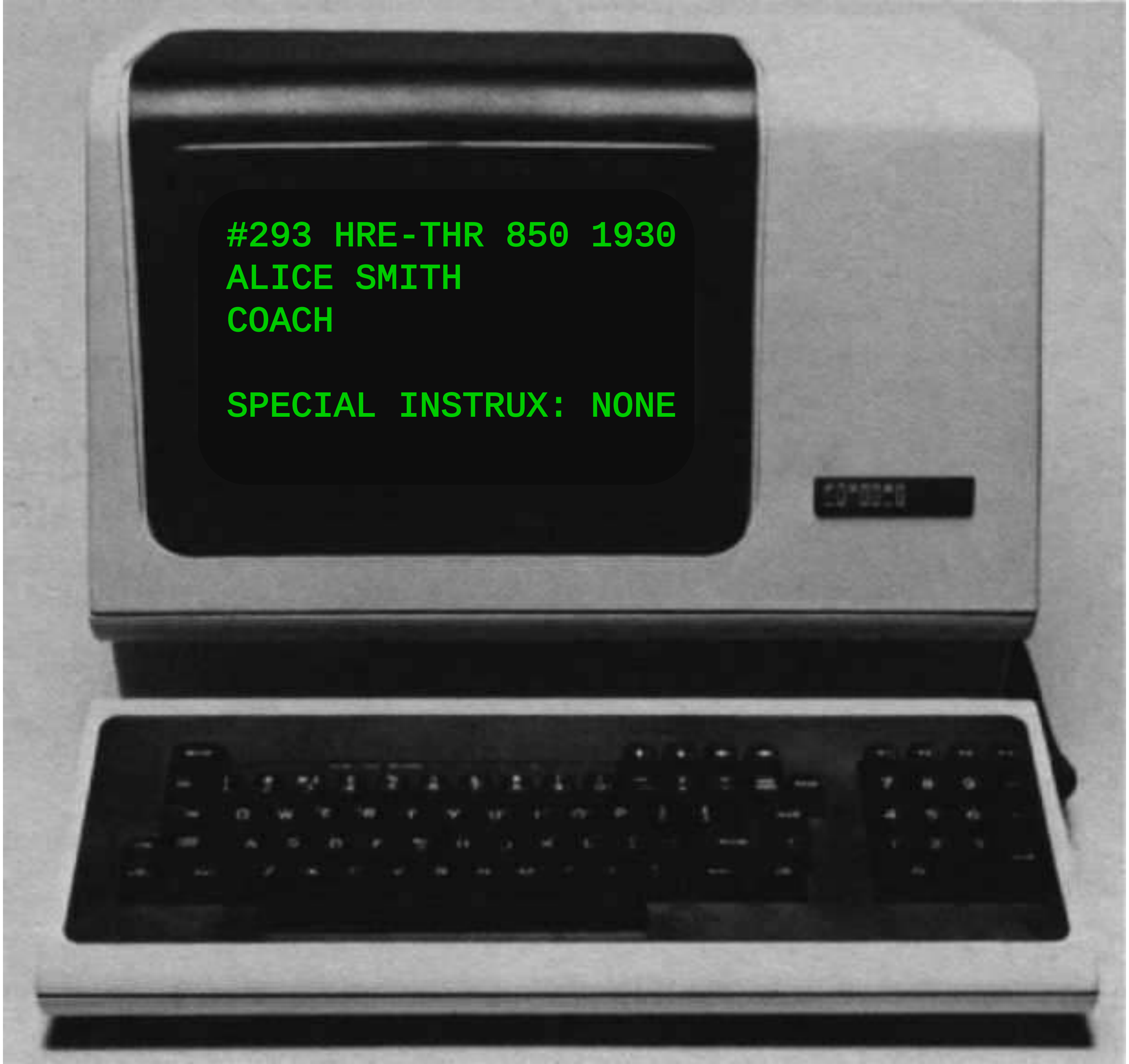
Some younger travelers are not required to present an ID when traveling within the U.S. Learn more

+ Known Traveler Number/Pass ID (optional): ?

+ Redress Number (optional): ?

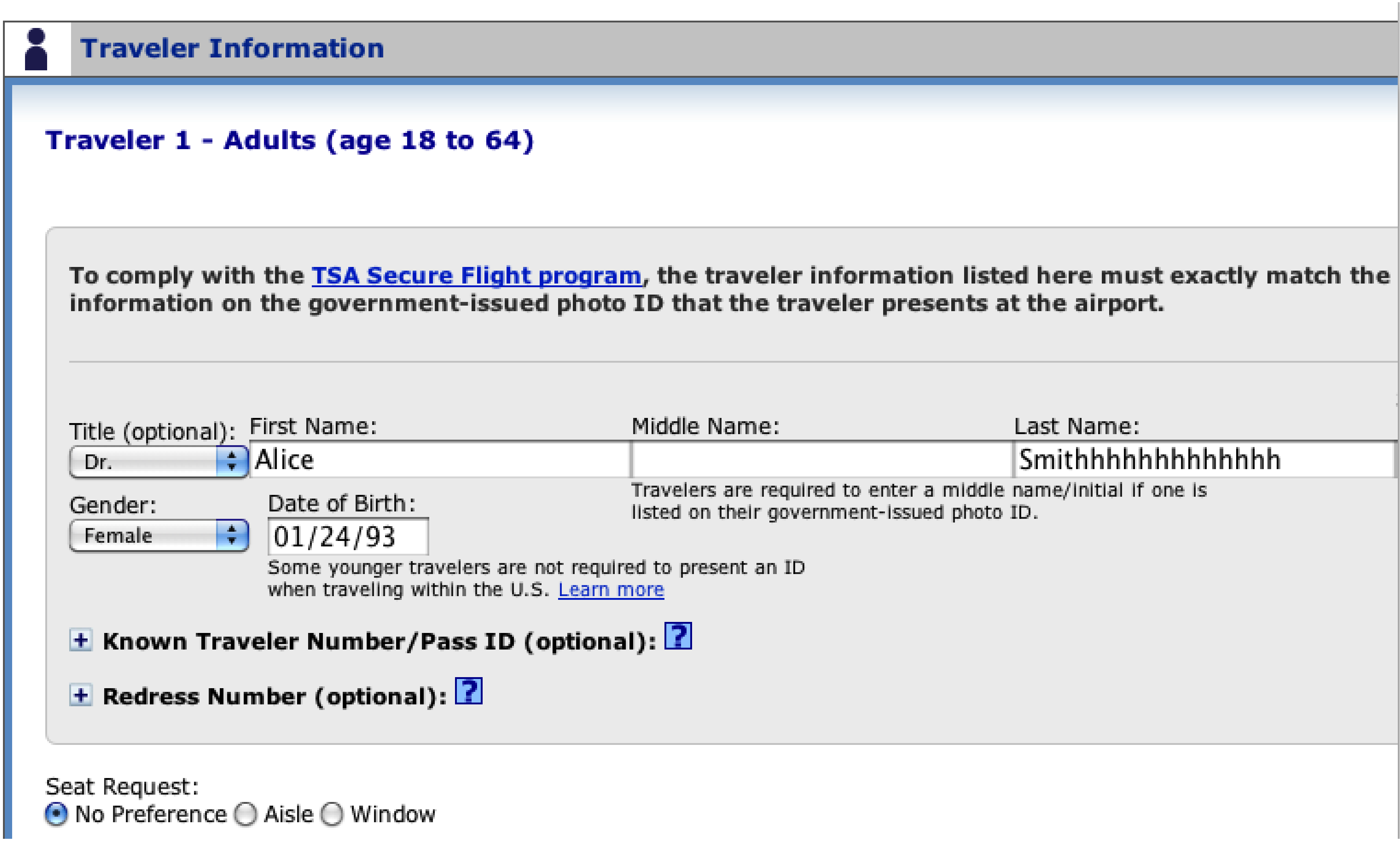
Seat Request:

● No Preference ○ Aisle ○ Window



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

SPECIAL INSTRUX: NONE
```



Traveler Information

Traveler 1 - Adults (age 18 to 64)

To comply with the TSA Secure Flight program, the traveler information listed here must exactly match the information on the government-issued photo ID that the traveler presents at the airport.

Title (optional): Dr.

First Name: Alice

Middle Name:

Last Name: Smithhhhhhhhhhhh

Travelers are required to enter a middle name/initial if one is listed on their government-issued photo ID.

Gender: Female

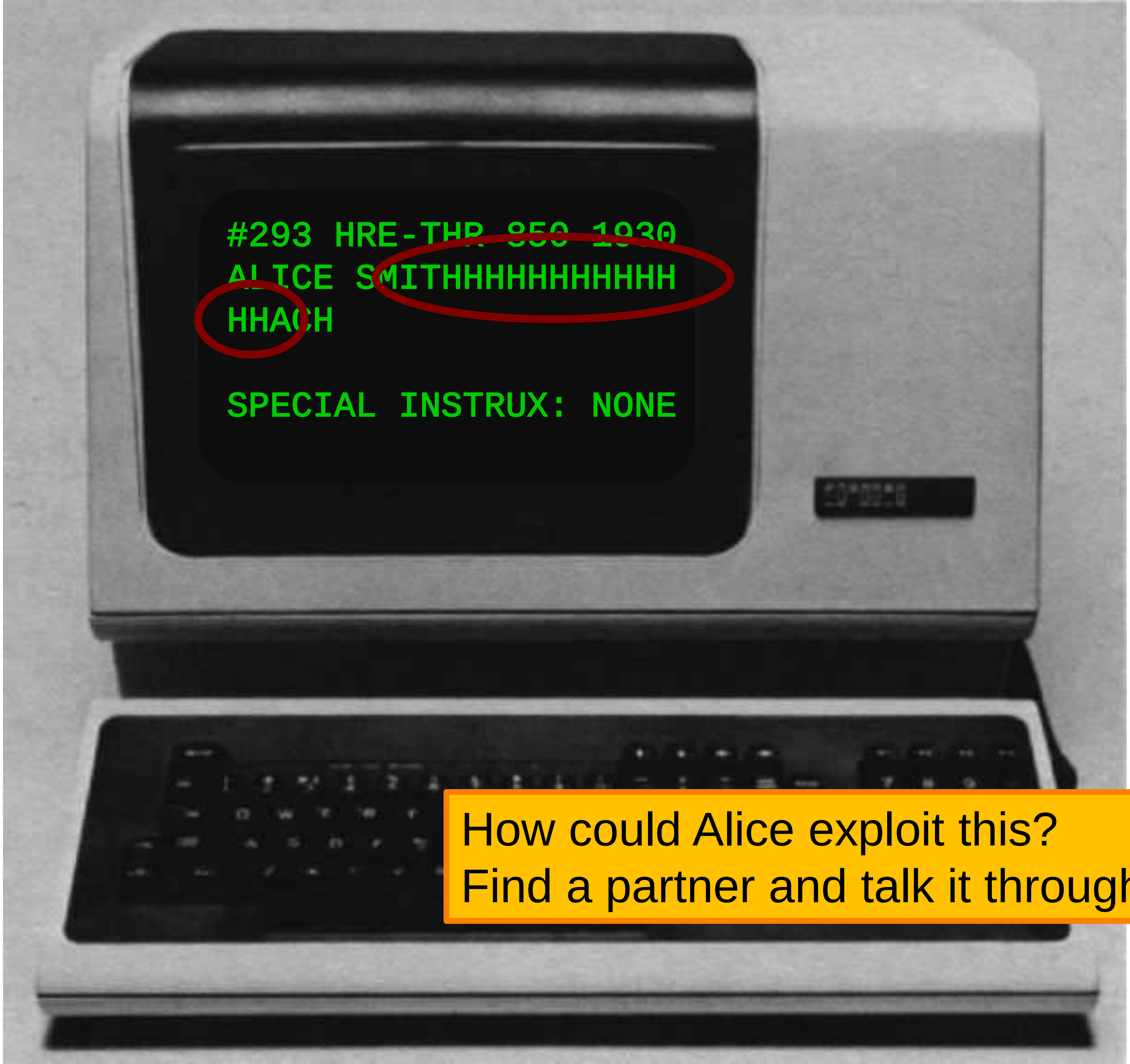
Date of Birth: 01/24/93

Some younger travelers are not required to present an ID when traveling within the U.S. Learn more

+ Known Traveler Number/Pass ID (optional): ?

+ Redress Number (optional): ?

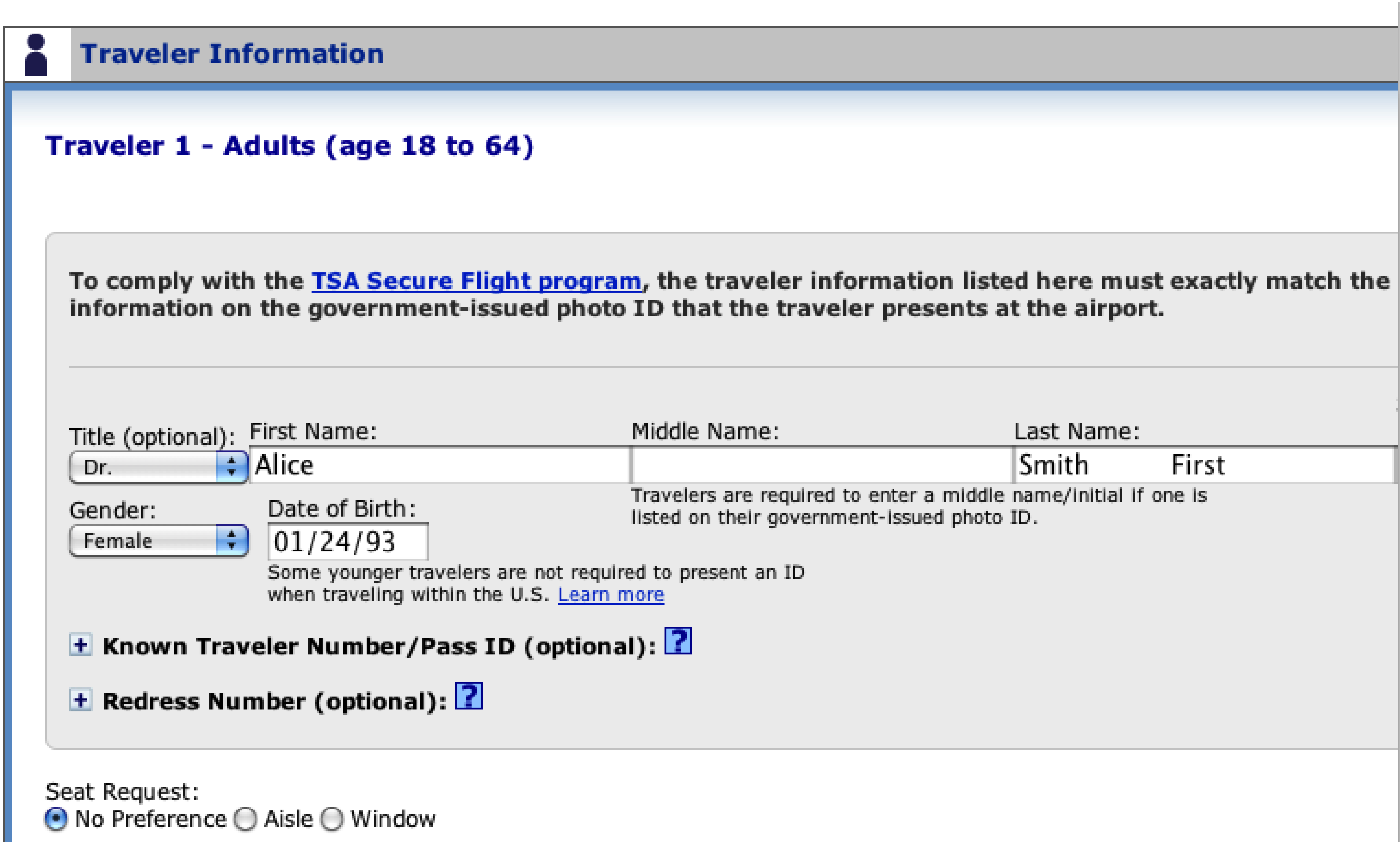
Seat Request:
● No Preference ○ Aisle ○ Window



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

SPECIAL INSTRUX: NONE
```

How could Alice exploit this?
Find a partner and talk it through.



Traveler Information

Traveler 1 - Adults (age 18 to 64)

To comply with the TSA Secure Flight program, the traveler information listed here must exactly match the information on the government-issued photo ID that the traveler presents at the airport.

Title (optional): Dr.

First Name: Alice

Middle Name:

Last Name: Smith First

Travelers are required to enter a middle name/initial if one is listed on their government-issued photo ID.

Gender: Female

Date of Birth: 01/24/93

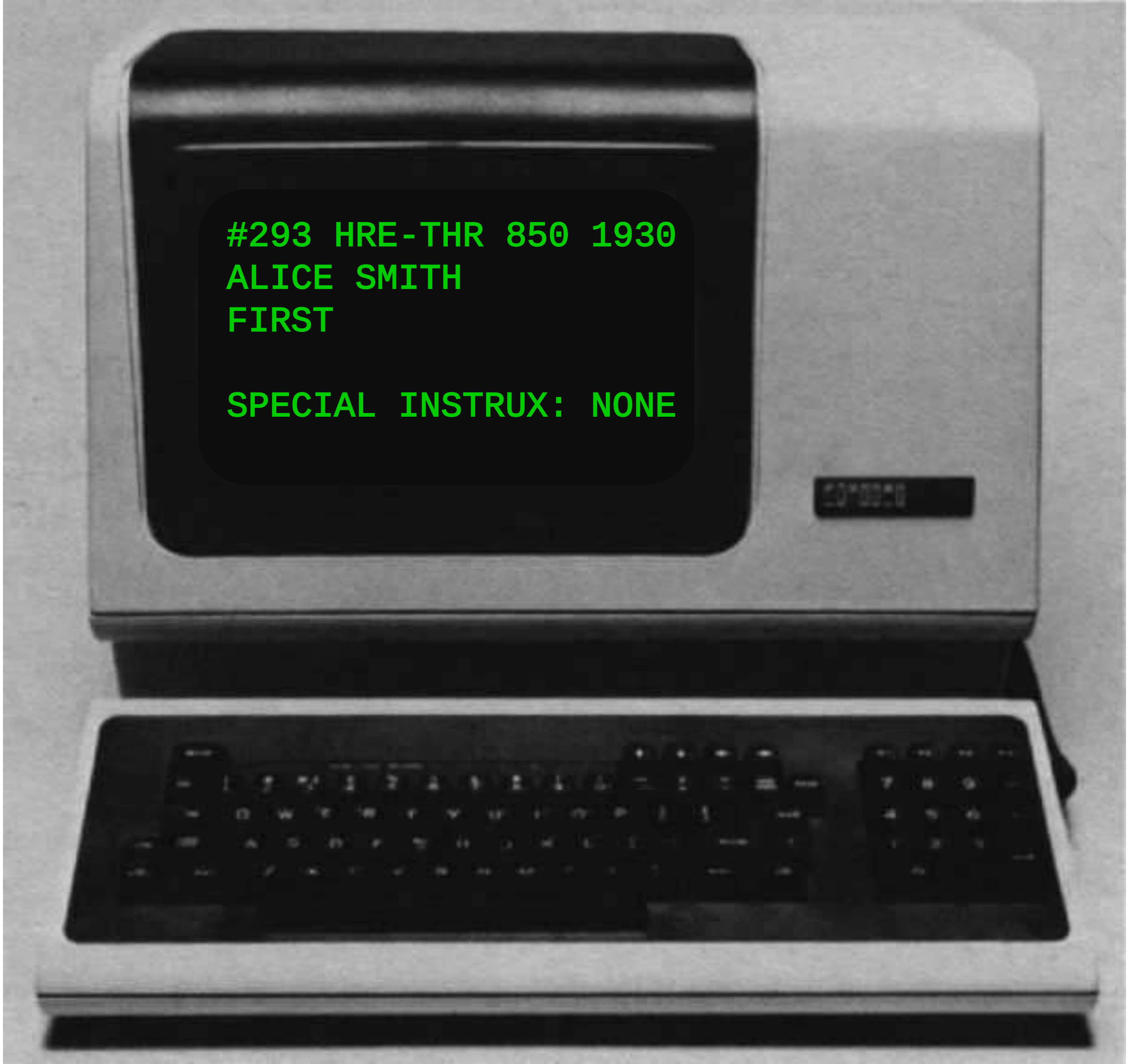
Some younger travelers are not required to present an ID when traveling within the U.S. Learn more

+ Known Traveler Number/Pass ID (optional): ?

+ Redress Number (optional): ?

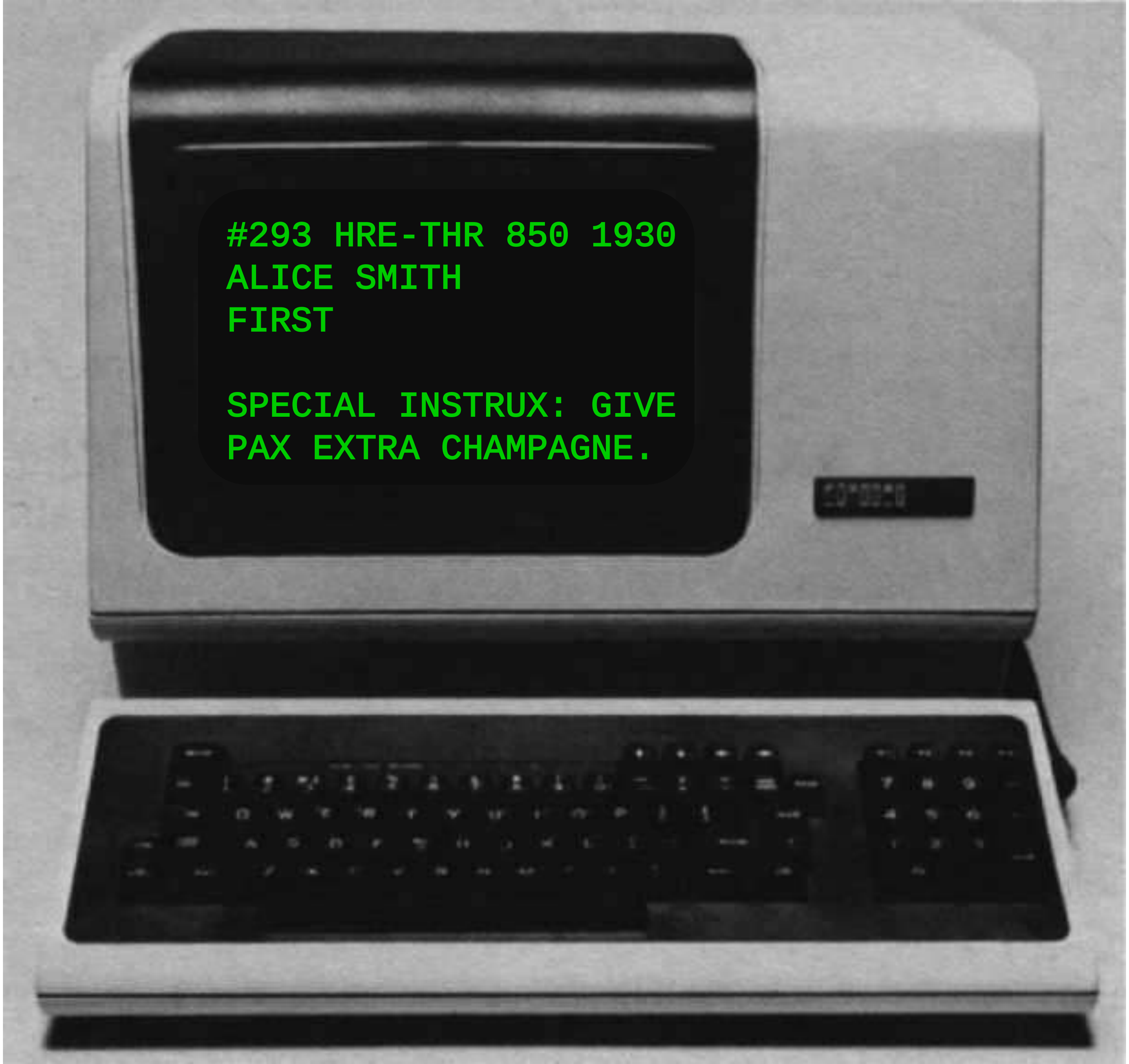
Seat Request:

● No Preference ○ Aisle ○ Window



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

SPECIAL INSTRUX: NONE
```



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

SPECIAL INSTRUX: GIVE
PAX EXTRA CHAMPAGNE.
```

```
char name[20];

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

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

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

Memory unsafe code

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

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

Reading data in name past 20 characters starts overlapping instrux because name and instrux are stored next to each other in memory

```
char line[512];
char command[] = "/usr/bin/finger";

void main() {
  ...
  gets(line);
  ...
  execv(command, ...);
}
```

```
char name[20];
int (*fnptr)();

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

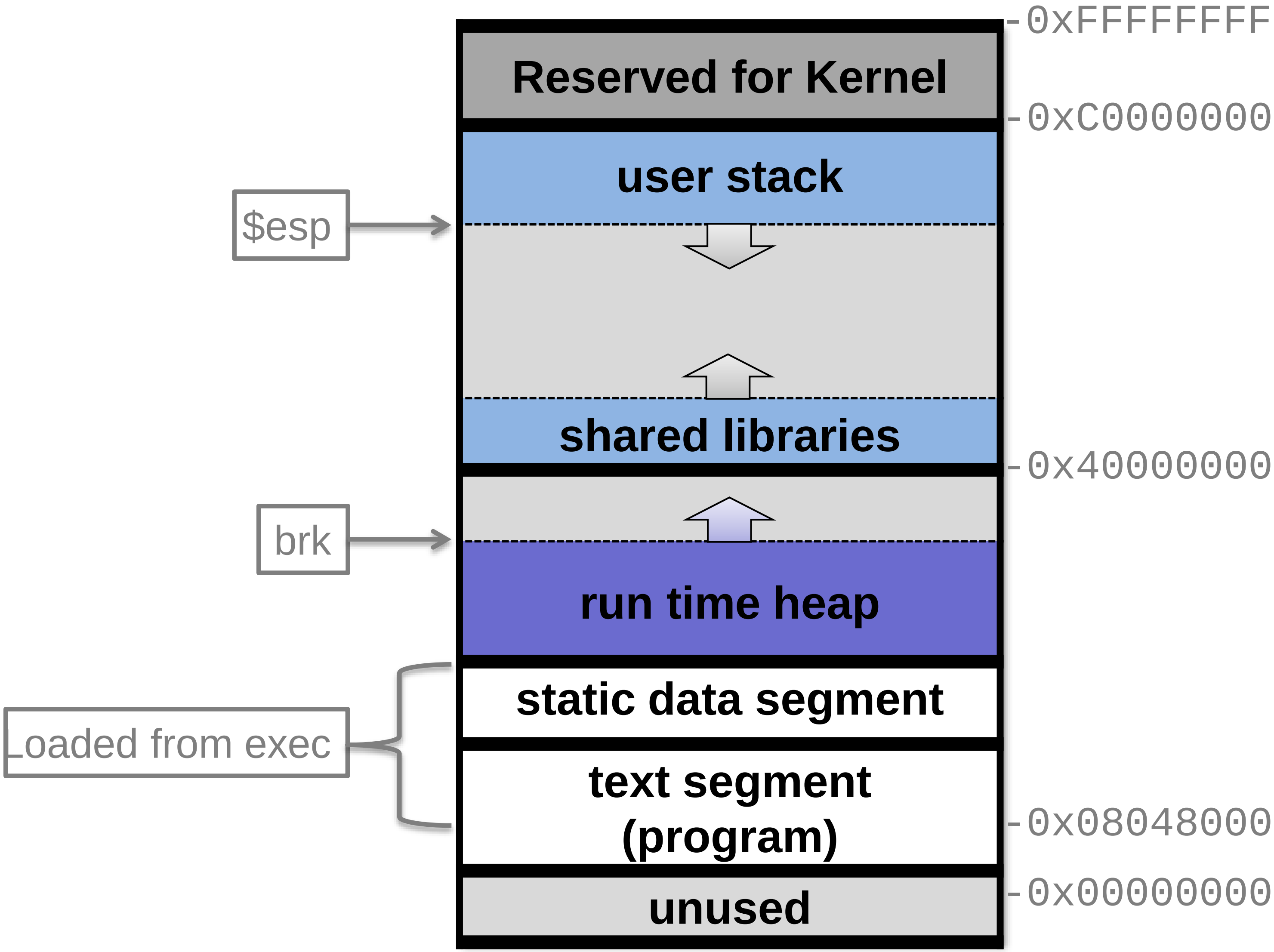
```
char name[20];
int  seatinfirstclass = 0;

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

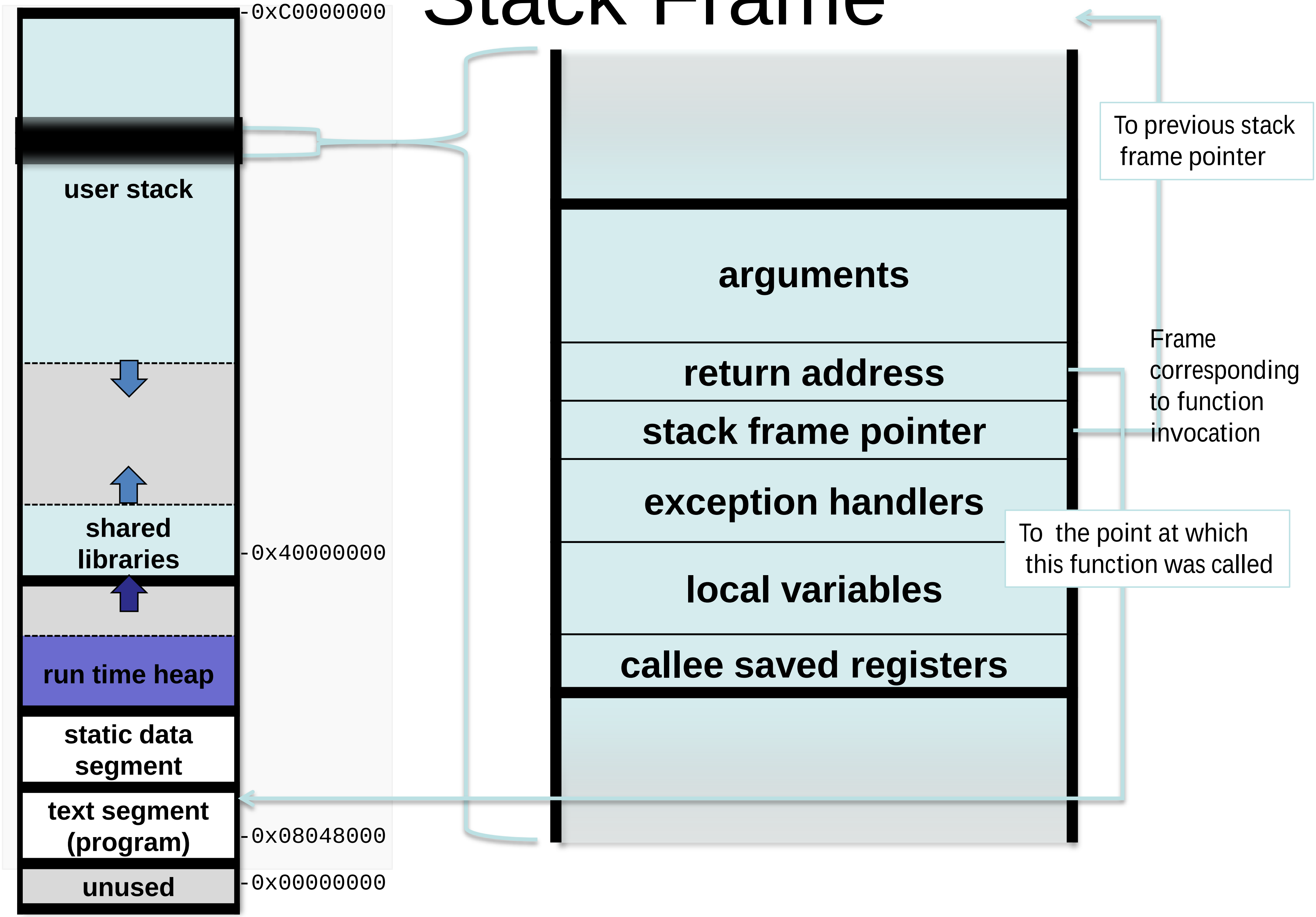
```
char name[20];
int  authenticated = 0;

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

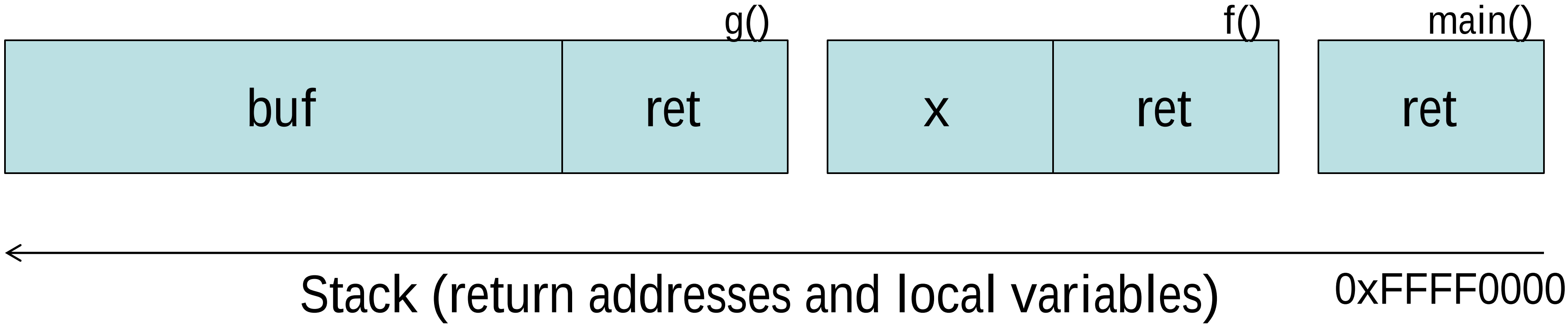
Linux (32-bit) process memory layout



Stack Frame


0xC0000000
user stack
shared libraries
0x40000000
run time heap
static data segment
text segment (program)
0x08048000
unused
0x00000000
arguments
return address
stack frame pointer
exception handlers
local variables
callee saved registers
To previous stack frame pointer
Frame corresponding to function invocation
To the point at which this function was called

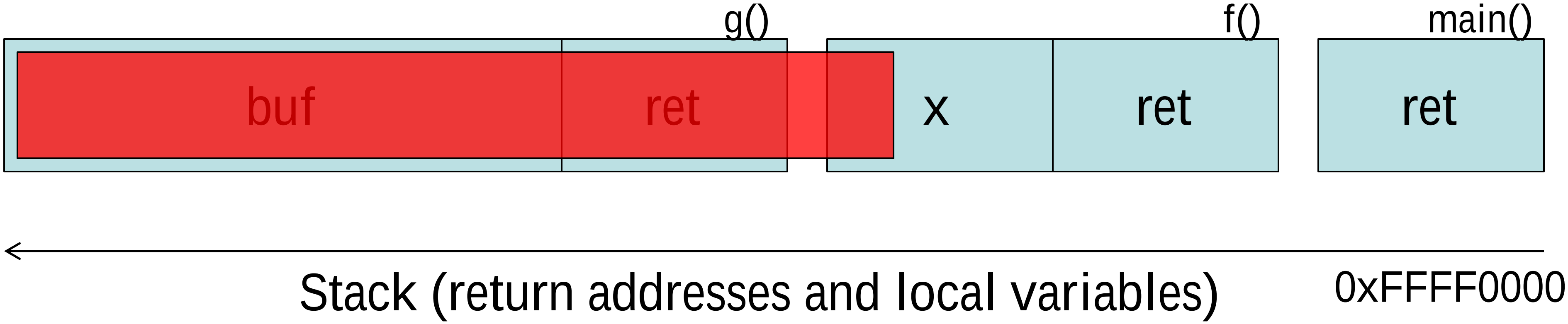
Code Injection



```
main() {
  f();
}
```

```
f() {
  int x;
  g();
}
```

```
g() {
  char buf[80];
  gets(buf);
}
```



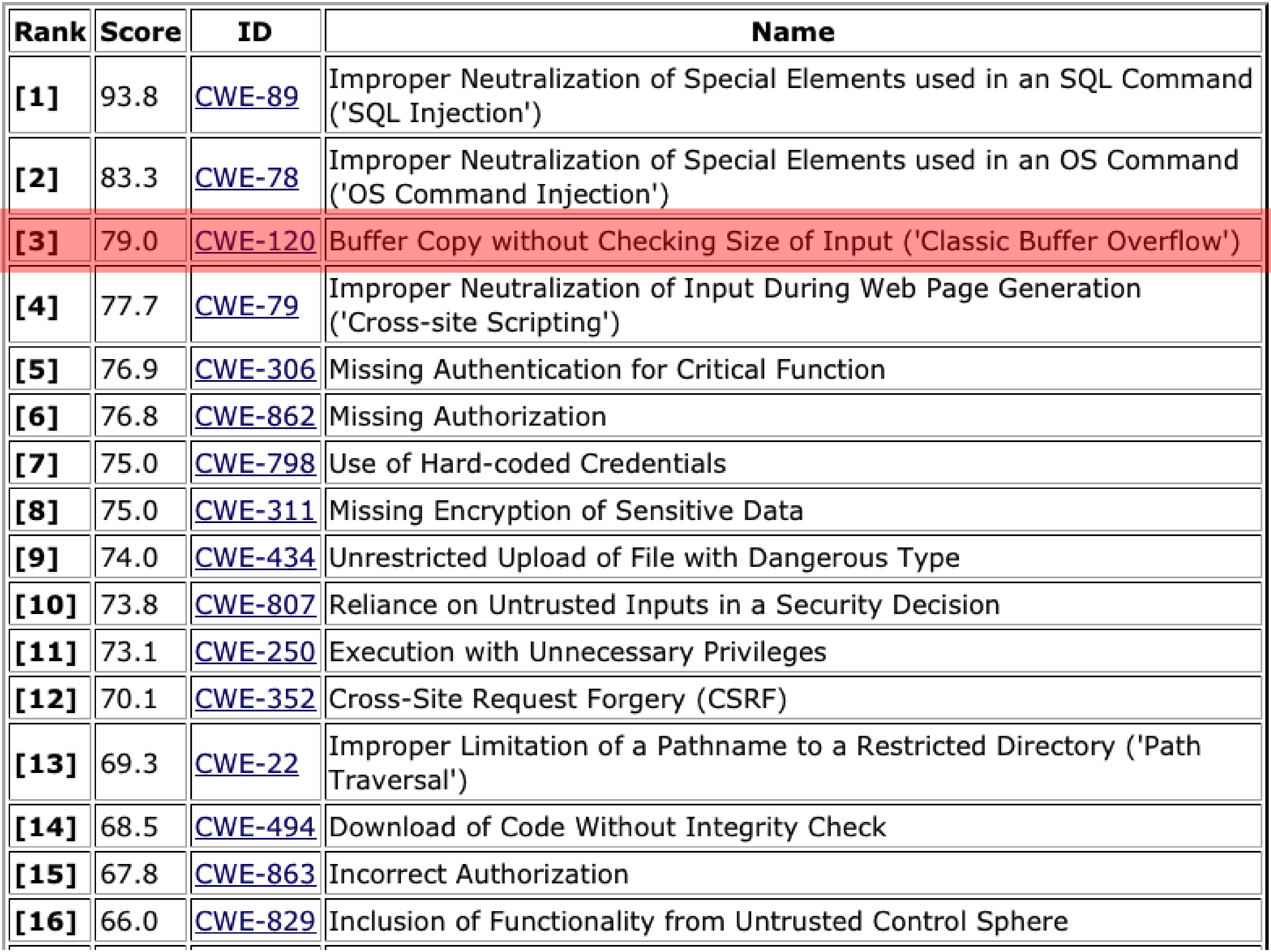
```
main() {
  f();
}
```

```
f() {
  int x;
  g();
}
```

```
g() {
  char buf[80];
  gets(buf);
}
```

Basic Stack Exploit

- Overwriting the return address allows an attacker to redirect the flow of program control.
- Instead of crashing, this can allow *arbitrary* code to be executed.
- Example: attacker chooses malicious code he wants executed ("shellcode"), compiles to bytes, includes this in the input to the program so it will get stored in memory somewhere, then overwrites return address to point to it.



Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	79.0	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75.0	CWE-798	Use of Hard-coded Credentials
[8]	75.0	CWE-311	Missing Encryption of Sensitive Data
[9]	74.0	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66.0	CWE-829	Inclusion of Functionality from Untrusted Control Sphere

```
void vulnerable() {
  char buf[64];
  ...
  gets(buf);
  ...
}
```

```
void safe() {
  char buf[64];
  ...
  fgets(buf, 64, stdin);
  ...
}
```

```
void safer() {
  char buf[64];
  ...
  fgets(buf, sizeof buf, stdin);
  ...
}
```

```
void vulnerable(int len, char *data) {
  char buf[64];
  if (len > 64)
    return;
  memcpy(buf, data, len);
}
```

```
memcpy(void *dst, const void *src, size_t n);
```

Attack: attacker supplies negative len, which becomes large value when cast to size_t

Fix:

```
void safe(size_t len, char *data) {
  char buf[64];
  if (len > 64)
    return;
  memcpy(buf, data, len);
}
```

```
void f(size_t len, char *data) {
  char *buf = malloc(len+2);
  if (buf == NULL) return;
  memcpy(buf, data, len);
  buf[len] = '\n';
  buf[len+1] = '\0';
}
```

Is it safe? Talk to your partner.

Vulnerable!

If `len` = `0xffffffff`, *allocates only 1 byte*

Broward Vote-Counting Blunder Changes Amendment Result

POSTED: 1:34 pm EST November 4, 2004

BROWARD COUNTY, Fla. -- The Broward County Elections Department has egg on its face today after a computer glitch misreported a key amendment race, according to WPLG-TV in Miami.

Amendment 4, which would allow Miami-Dade and Broward counties to hold a future election to decide if slot machines should be allowed at racetracks, was thought to be tied. But now that a computer glitch for machines counting absentee ballots has been exposed, it turns out the amendment passed.

Broward County Mayor Ilene Lieberman says voting counting error is an "embarrassing mistake."

"The software is not geared to count more than 32,000 votes in a precinct. So what happens when it gets to 32,000 is the software starts counting backward," said Broward County Mayor Ilene Lieberman.

That means that Amendment 4 passed in Broward County by more than 240,000 votes rather than the 166,000-vote margin reported Wednesday night. That increase changes the overall statewide results in what had been a neck-and-neck race, one for which recounts had been going on today. But with news of Broward's error, it's clear amendment 4 passed.