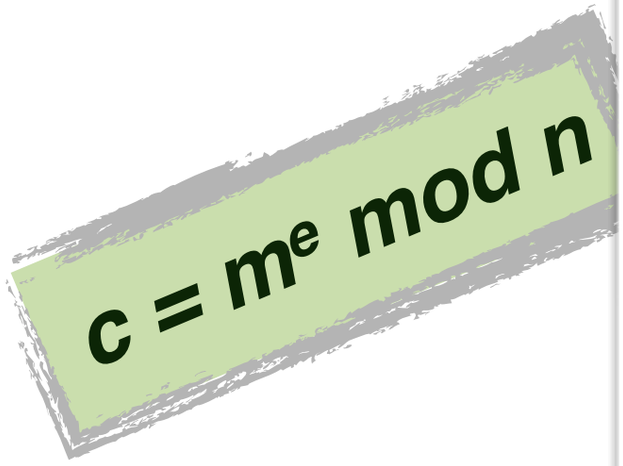
# CS5438
# Security and Privacy: Practice and Case Studies





## The Security Landscape

Instructors: Ari Juels and Vitaly Shmatikov
Spring 2016

# Course goal

- **Think adversarially! Adopt the "adversarial mindset."**
  - Ideally, you'll come out thinking like a criminal mastermind, but behaving like a gentlewoman / gentleman.
    - (We've all got something to learn about both!)

# Course goal

- More concretely, given a startup idea, system architecture, news article, etc., you should understand:
    1. Potential security and privacy vulnerabilities and attacks, i.e., how things might break
    2. The implications and cost of security and privacy failures
    3. Roughly what tools, techniques, and principles to use for defense
- This means a lifetime of learning!
    - Security is challenging, particularly if you're the defender.
    - Security is always an arms race. The specifics change.

# What’s an adversarial mindset?

And how boarding passes are like cookies.

“Security requires a particular mindset. Security professionals -- at least the good ones -- see the world differently. They can't walk into a store without noticing how they might shoplift…They can't vote without trying to figure out how to vote twice. They just can't help it.”

–Bruce Schneier (2008)

# The adversarial mindset: Four key questions

1. **Security goal:** What policy or good state is meant to be enforced?
2. **Adversarial model:** Who is the adversary? What is the adversary's space of possible actions?
3. **Mechanisms:** Are the right security mechanisms in place to achieve the security goal given the adversarial model?
4. **Incentives:** Will human factors and economics favor or disfavor the security goal?

# Four key security goals

**Confidentiality:** Data not leaked

**Integrity**: Data or resource not tampered with

**Availability**: Data or resource accessible when needed

**Authenticity**: Correct belief in data or resource origin

(CIA + Authenticity)

# In twenty years…

September 8, 2035

Dear Prof. Jules [sp?],

You asked us to
write to tell you if
we still
remember those two
slides of yours.

I do. They were RED!

POST CARD


Sincerely yours,

A former student,
now rich entrepreneur.

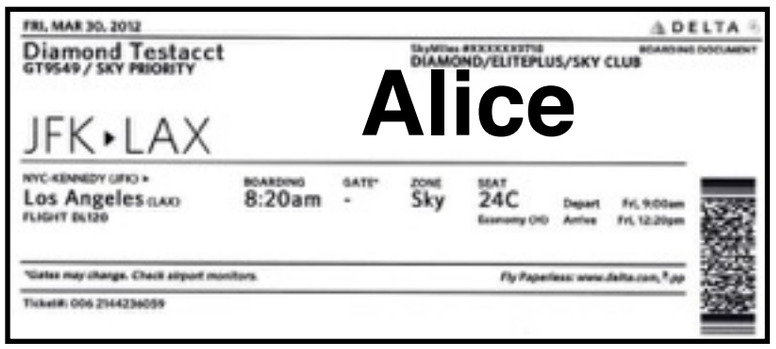
P.S. ฿100,000 check in
the mail!

# You can apply the adversarial mindset everywhere

- Card readers for this building
  - Can cards be skimmed / cloned?
- The vending machines here on the 3rd floor
  - How does the serviceperson get access?
- Your MTA card
  - Can the magstripe be hacked?
- Beam robots
  - How are they secured? What would be the consequences of a compromise?

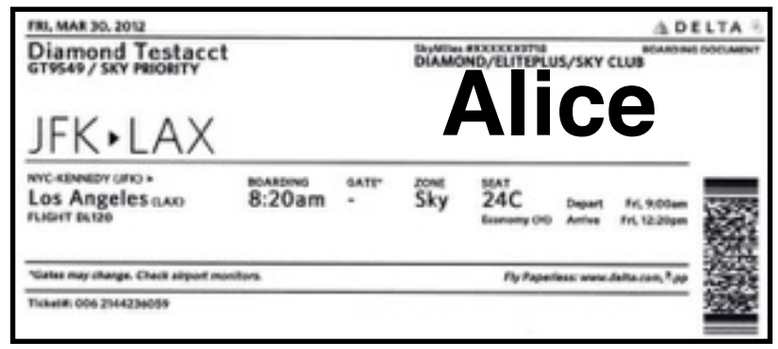
# Example:
# Air travel

## Step 1: Home




## Step 2: Security


## Step 3: Gate



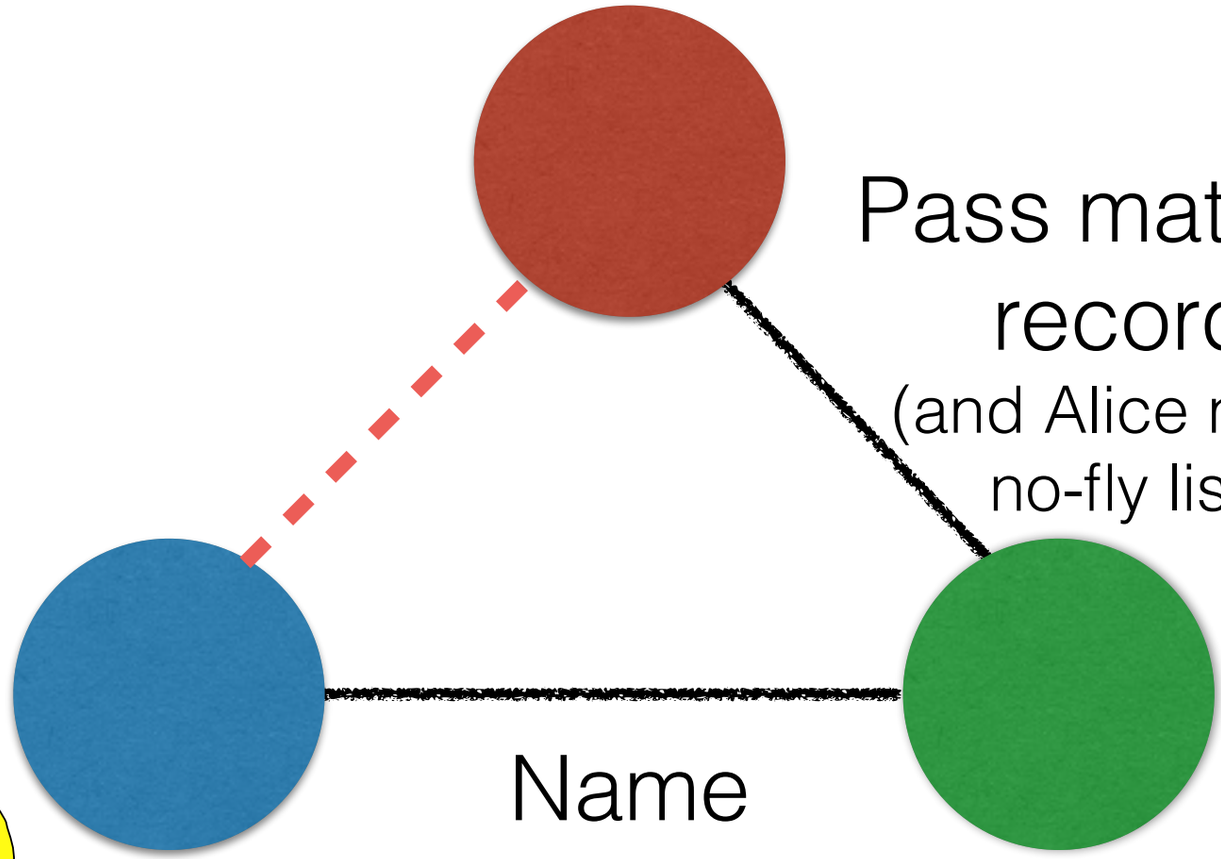
# What's the **security goal** for passport / ID checking?

- Ensure that passengers are correctly identified.
- Ensure that passengers on no-fly lists can be identified before they board.

# What's happening?

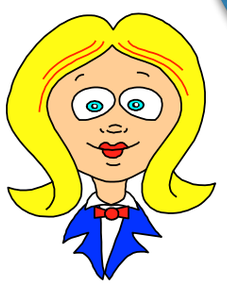
Flight record

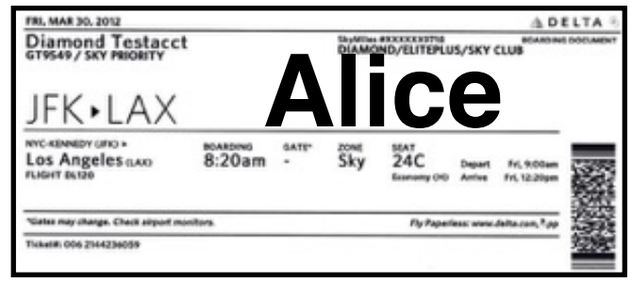
**Alice: JFK to LAX**



Pass matches record!
(and Alice not on no-fly list.)

Name matches!

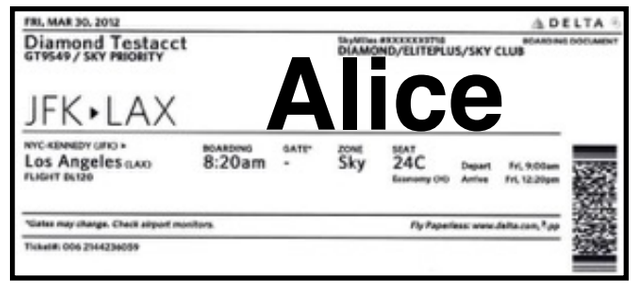





# (Evil) Eve wants to get on a plane without detection (she's on a no-fly list)

Eve

1. She steals a credit card (e.g., Alice's), buys a ticket in Alice's name, and prints a boarding pass for Alice.




2. She also forges a boarding pass with name of Eve.

# Eve can impersonate Alice!

Flight record

**Alice: JFK to LAX**

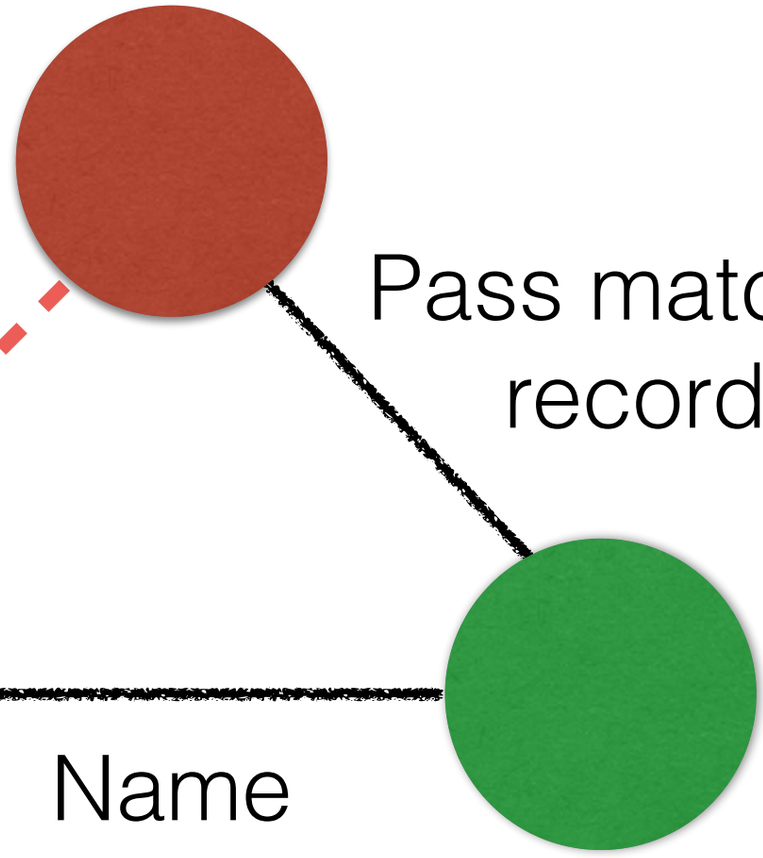
Pass matches record!

Name matches!


# There's no record of Eve boarding!

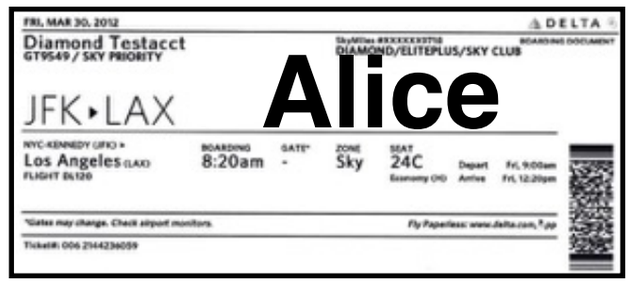
Flight record

**Alice: JFK to LAX**



Pass matches record!

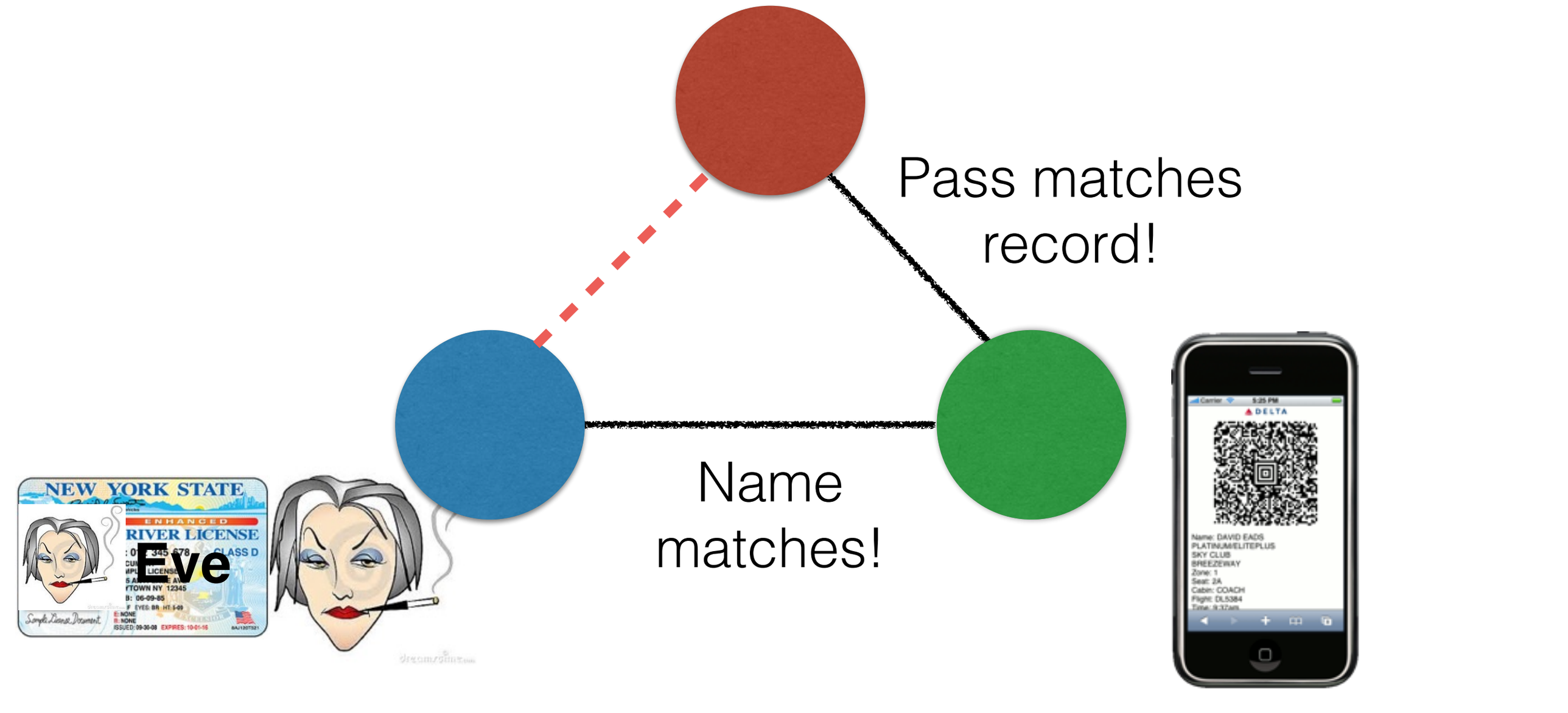
Name matches!



# Mobile boarding passes no better

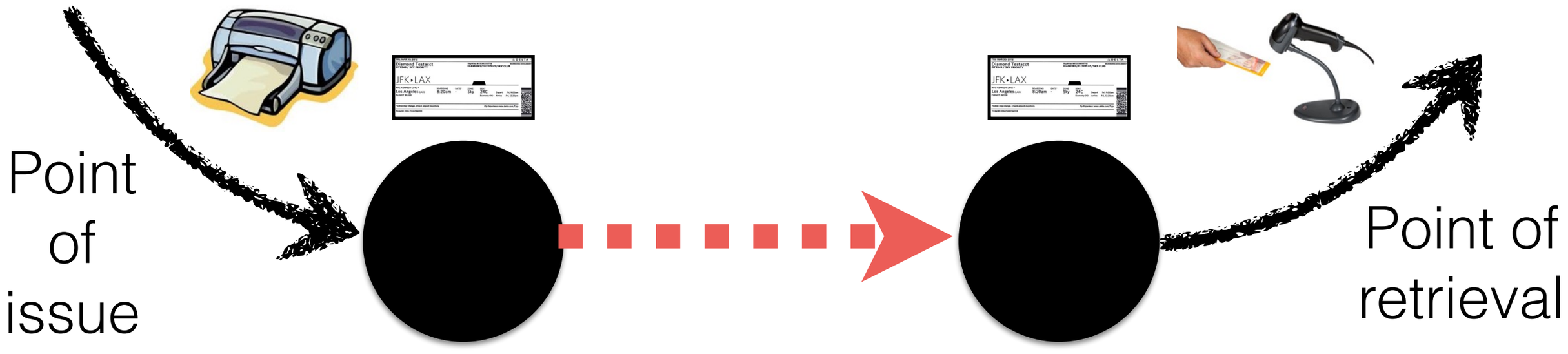
Flight record

**Alice: JFK to LAX**



# Where's the mistake?

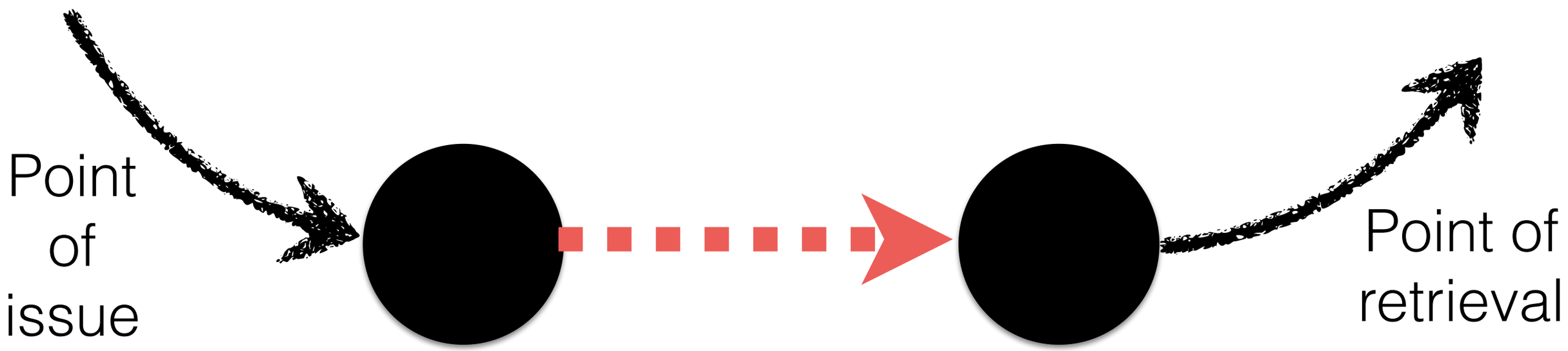
- The **adversarial model** should include boarding pass tampering, but doesn't.
- Assumption: pass that's *issued* is pass that's *presented*
- The boarding pass lacks **integrity**… anyone can modify it. Today's boarding-pass checks are an ineffective security **mechanism**.



# The adversarial model used to be different

- Alaska Airlines introduced home-printable boarding passes in 1999.
- Before that time, boarding passes were printed on special card stock.
- Security mechanism to protect integrity—passes were harder to modify


# Integrity forgotten in adversarial model in many, many other places



# Such as cookies

- Remember that a cookie is a piece of information (state) stored on a client's browser.
- It saves the trouble of a server storing state locally.
- E.g., user is shopping at an e-commerce site.

# Simple cookies lack integrity

- Clients can *tamper with* cookies ("cookie poisoning").

  E.g., Edit Cookies, Cookies Manager+ Firefox extension

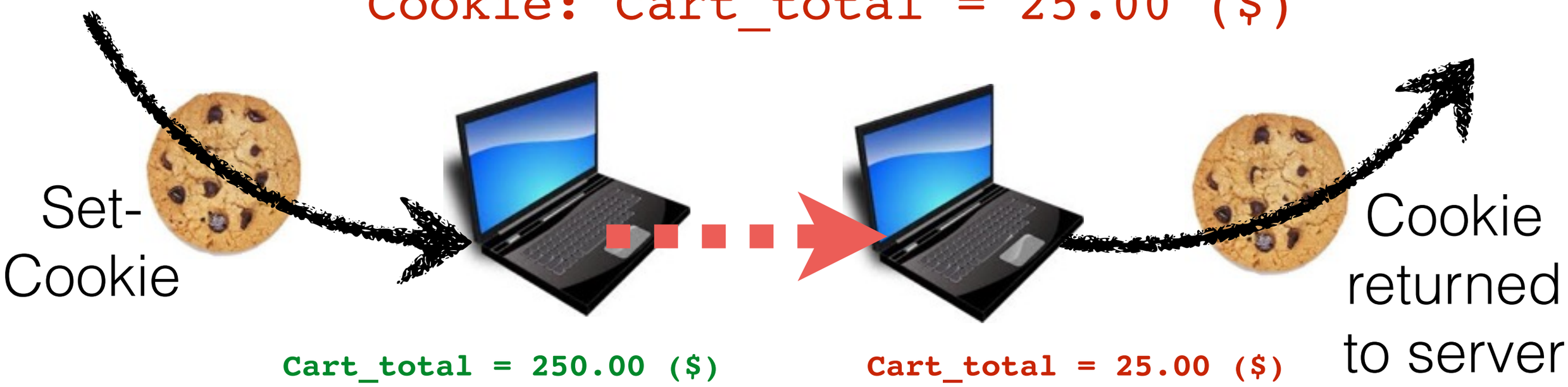
- Example:

  E-commerce site executes

```
Set-Cookie: Cart_total = 250.00 ($)
```

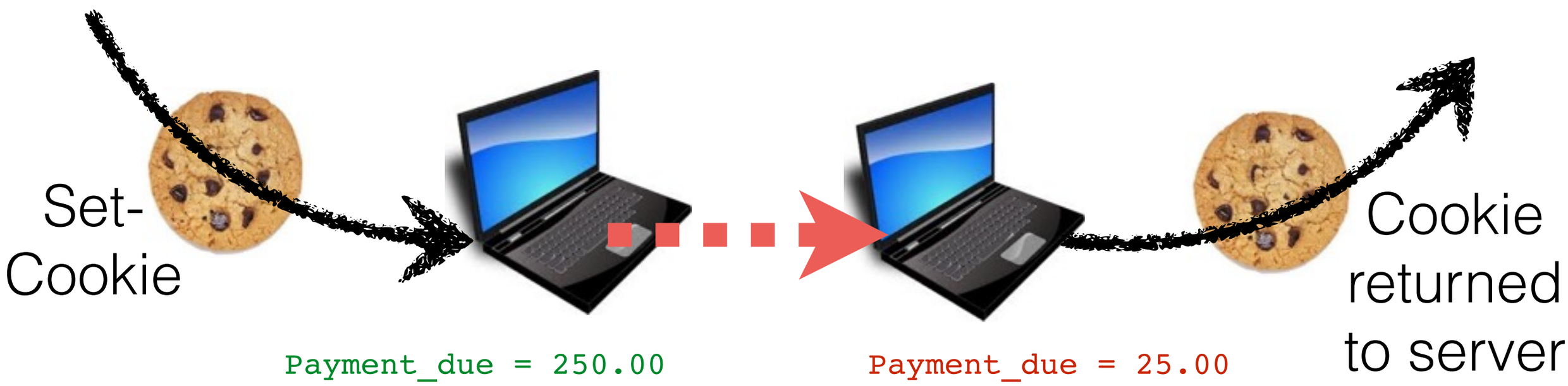
Before paying, user substitutes

```
Cookie: Cart_total = 25.00 ($)
```



# Cookies

Later in the course, we'll talk about how to address these problems using cryptography, a powerful security **mechanism**.



# Who is the adversary?

It depends on who you are

# Kevin “Condor” Mitnik


- **Targets:** LA bus system; corporate systems
- **Made off with:**
  - 1 year prison, 3 years parole
  - Book deals
  - Lucrative consulting career

See http://en.wikipedia.org/wiki/Kevin_Mitnick

# Russian Business Network


- St. Petersburg-based cybercrime organization
- Started as ISP hosting malware, spammers, phishing sites
- Alleged operation of "Storm" botnet
- Allegedly involved in (cyberwarfare) DoS attacks against Estonia (2007)

See http://en.wikipedia.org/wiki/Russian_Business_Network

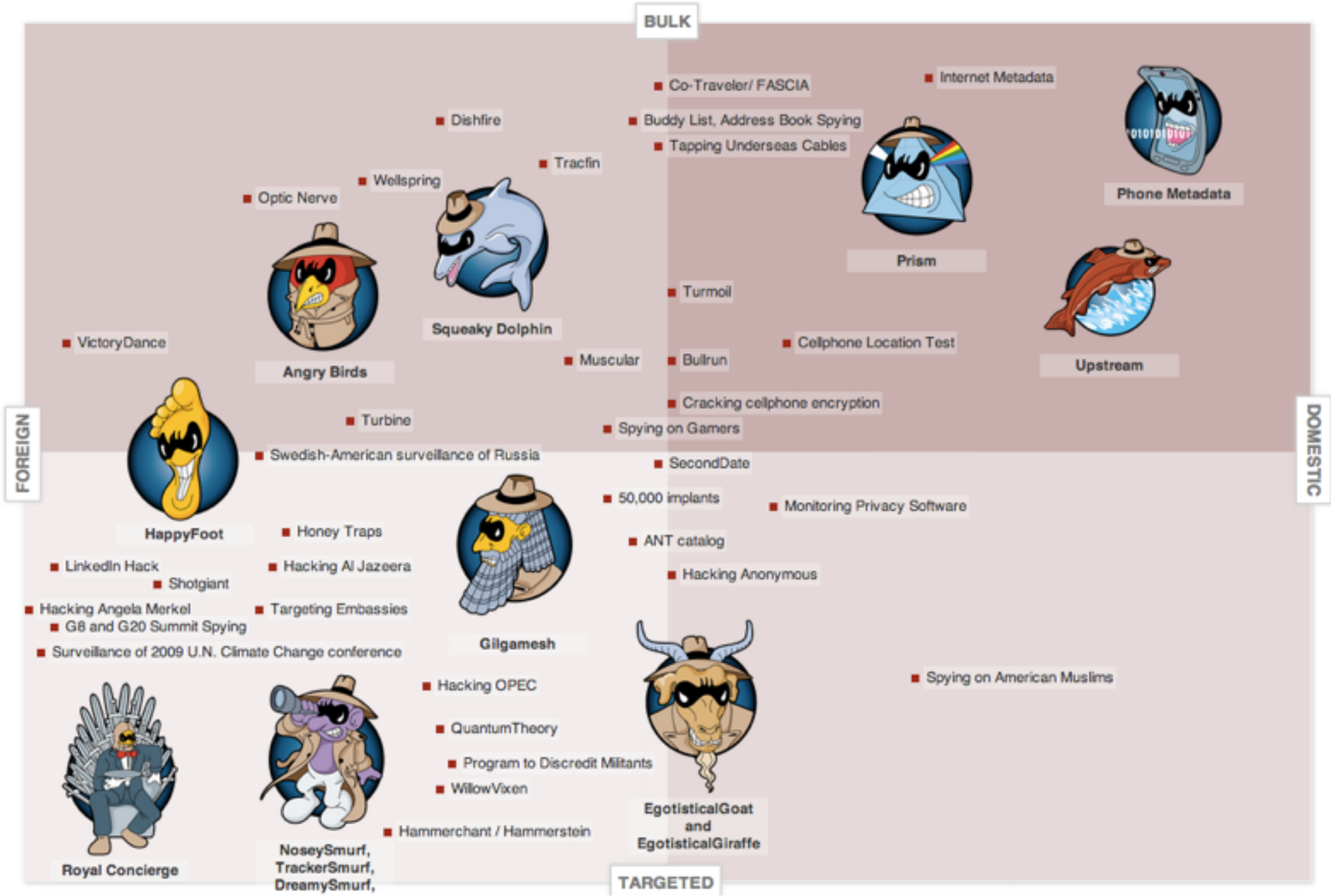
# People's Liberation Army and Chinese Government


- **Targets:**
  - U.S. companies, government
  - Dissidents
- **Makes off with:**
  - Intellectual property, military secrets
  - Strong censorship (Great Firewall of China)

See http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China; http://en.wikipedia.org/wiki/People's_Liberation_Army

# U.S. National Security Agency

**Targets:**




Source: http://projects.propublica.org/nsa-grid/

**Makes off with:** Not quite everything

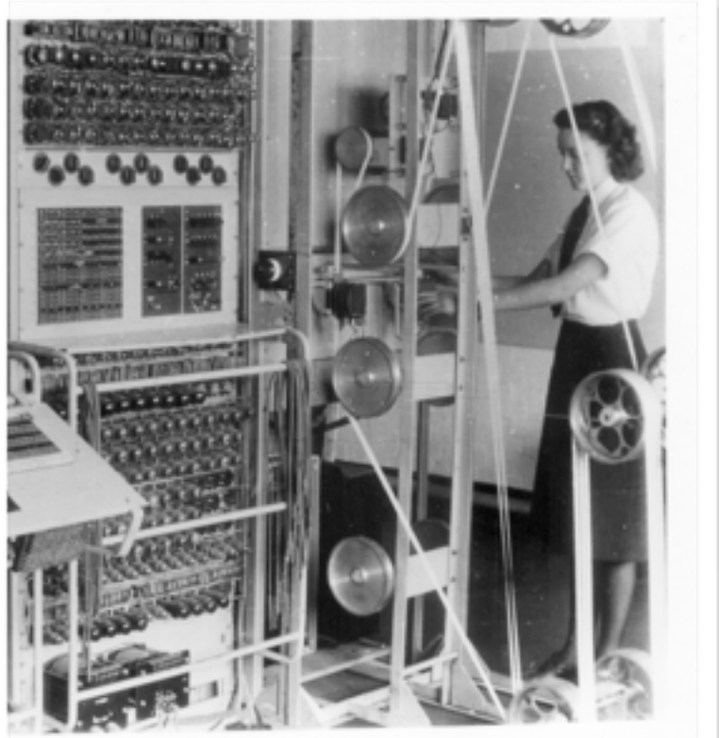
# U.S. National Security Agency


Source: http://projects.propublica.org/nsa-grid/

**(Has its own adversaries to contend with…)**

# But adversaries and systems change

- Thinking adversarially means thinking broadly.
  - Who knew that cookies were like boarding passes!
- Security and privacy aren't just about bits and bytes. Principles are deep and pervasive…



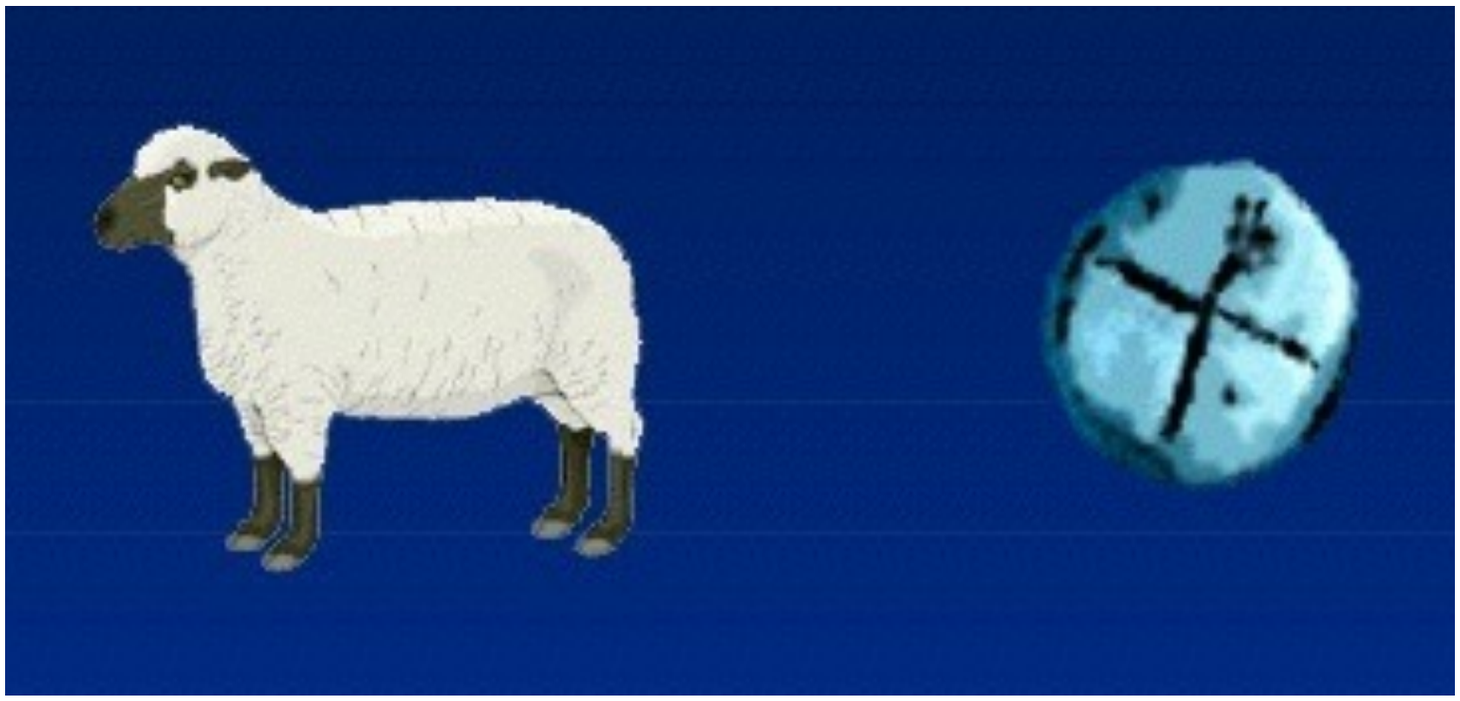
# A (Short) History of the World in Three Information Security Technologies

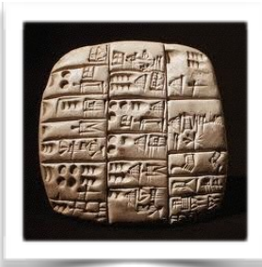
# The lost sheep problem

- Neolithic Middle East shortly after invention of agriculture (8000 B.C.E. or so), surplus food was produced.
- It was held in communal warehouses, flocks, etc.
- Suppose you deposited some sheep in the communal herd.
- **Security goal:** You don't want anyone to forget your sheep —or falsely claim you didn't deposit them.

# A solution

- To keep track of goods, clay accountancy tokens were used.
- Here's a token good for one sheep…

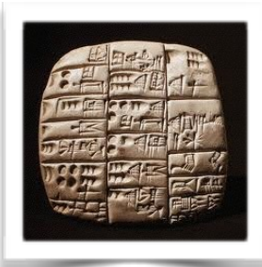




# Which led to… *writing*

- Eventually, it was necessary to consider an **adversarial model** that included *tampering* with or *stealing* tokens.
  - Especially for shipped goods.
- Eventually tokens were sealed in a clay envelope. (A security **mechanism** that preserved *integrity*.)
- If in doubt, envelope could be broken open…
- To avoid breaking envelope, signs impressed on surface: 3D representations went 2D.
  - (Middle 4th millennium B.C.E.)

Globular envelope with a cluster of accountancy tokens, Uruk period, from Susa. Louvre Museum. Source: Marie-Lan Nguyen (2009).

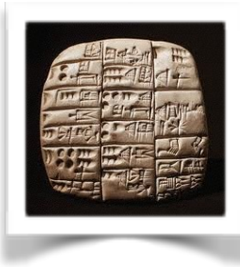


# Which led to… *writing*

- It's hypothesized that these impressions were the *first form of writing*.

- Process of breaking open the envelope to verify tokens was a very early security protocol!

Globular envelope with a cluster of accountancy tokens, Uruk period, from Susa. Louvre Museum. Source: Marie-Lan Nguyen (2009).



# Eventually signs migrated to tablets and stories were told…

"He who saw all, who was the foundation of the land,

"who knew (everything), was wise in all matters.

"Gilgamesh, who saw all, who was the foundation of the land…

An infosec problem gave birth to writing…

# Money

- Accountancy tokens had to be kept in a trustworthy place to prevent tampering, etc.
  - E.g., in a temple, clay envelope on shipping route
- How to make accountancy tokens completely portable?
  - E.g., for trade?

# Money

- What are the **security goals**?
  - Tokens can be created only by a trusted authority.
  - **Authenticity** verifiable by anyone, i.e., tokens are valid creations of the authority.
- What's the **adversarial model**?
  - Forgers can try to create and/or modify tokens away from observation.
- Unfortunately, clay tokens aren't too hard to forge…

# Money

- In the mid 7th century B.C.E., in Lydia and Ionia (modern Turkey), the first *coins* were struck.
- Coinage usually relies on two things:

1. Make tokens out of a scarce resource.

   Electrum (gold and silver)

2. Apply a sign / signature to tokens that's hard to duplicate.

   Drew on skills of gem-engravers

3. (Death penalty for forgers didn't hurt.)

- This solution (minus 3.) lasted for many centuries… until 1964 in U.S.

Alyattes Trite (Lydia 1/3 stater). 6th-5th century B.C.E. Image Courtesy of CNG: www.cngcoins.com.

Intaglio depicting goddess Demeter. 1st cent. B.C.E. Private collection.

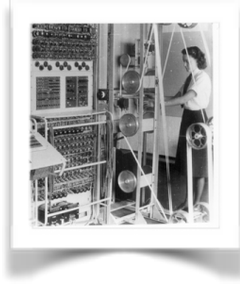
# 2600+ years later…

## Same principles!

1. Scarce resource: computation
2. Hard-to-forge data: cryptography

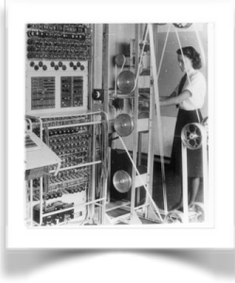
We'll talk about Bitcoin later in the course…


**Bitcoin**



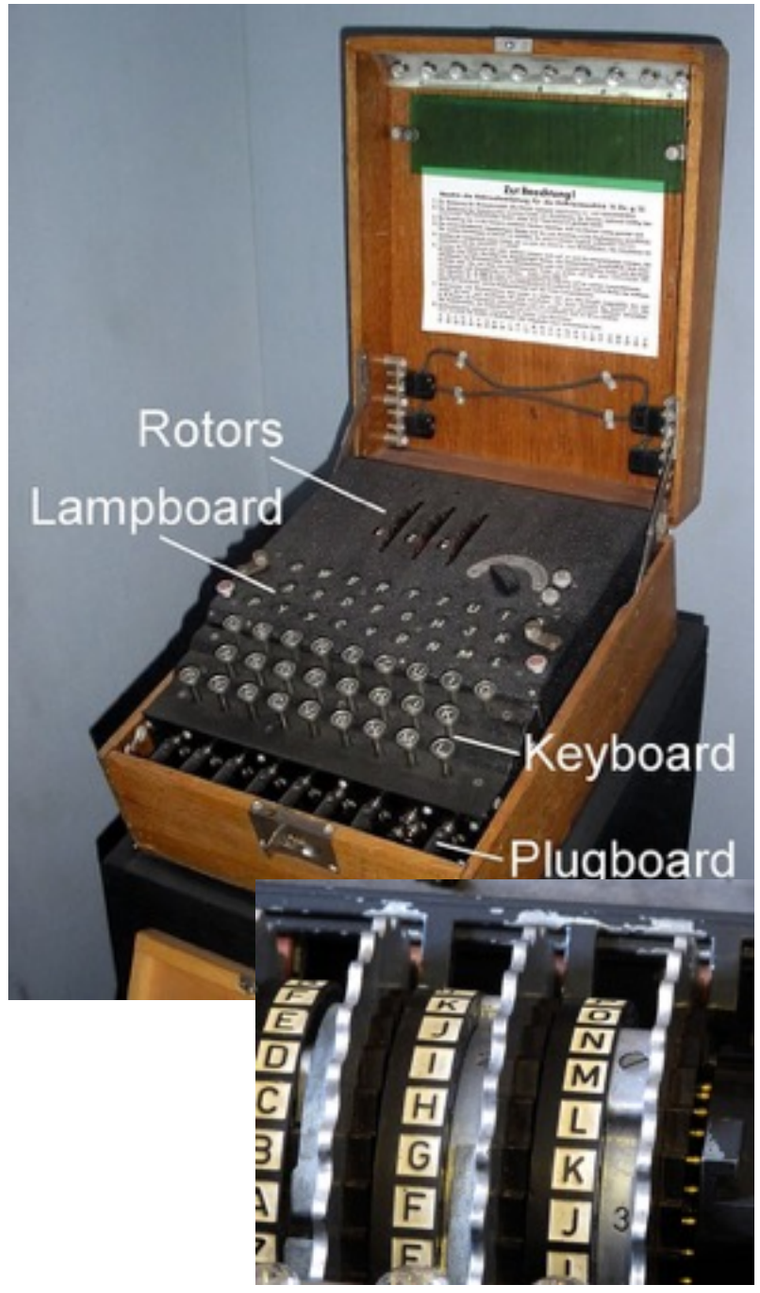
# The modern computer

- In early history, people communicated at a distance via letters, messengers.. eventually telegraph
- Radio communication grew in the early 20th century; very convenient, but…
- Everyone could hear and eavesdrop on your transmissions!
  - Radio changed the **adversarial model**!
- Especially during wartime, encryption became important.
- WWI hand ciphers gave way in WWII to cipher machines…



# Enciphering machines

- During WWII, the Germans used machines in the Enigma family.
- These machines enciphered using electromechanical rotors.
- The Enigmas had many possible settings…
- An Allied cryptanalyst faced in practice an estimated $10^{23}$ possible settings.
  - That's a hundred thousand billion billion!

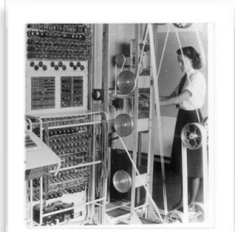



*German Enigma machine*

# How were these broken?

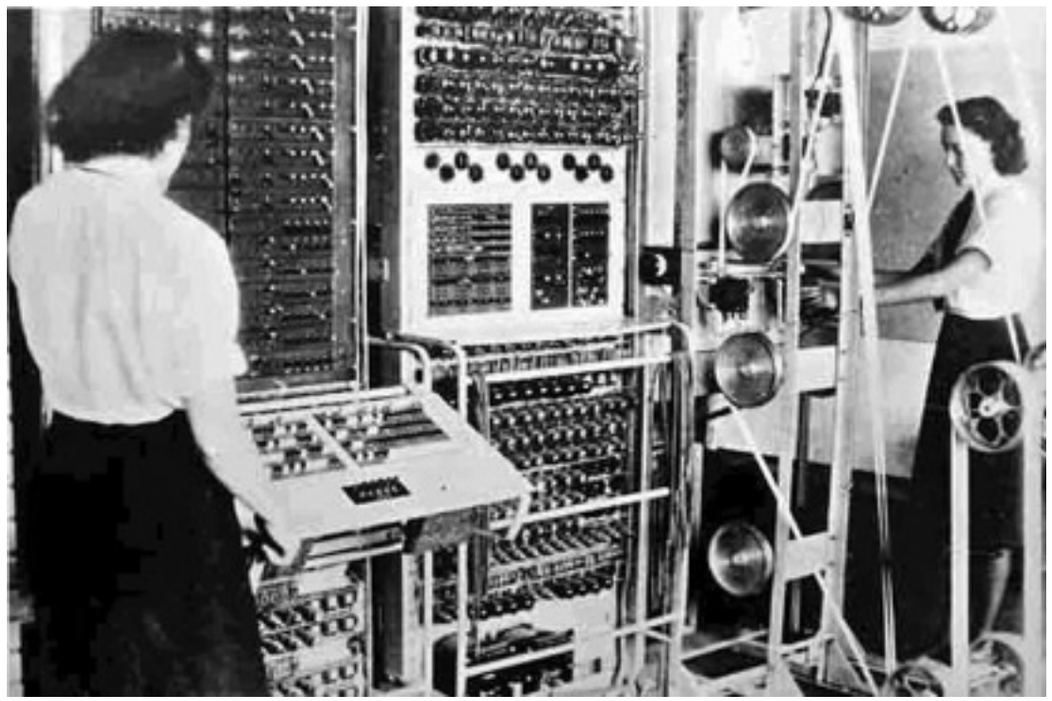
- “Bombes” were developed by British cryptologists to simulate Engima behavior.
  - Initial design by **Alan Turing**
  - A kind of proto-computer
- Bombes explored Enigma daily settings (the set and positions of rotors, the key, and the plugboard wirings).
- They enabled effective breaks of Enigma-encoded messages: yielded part of the ULTRA intelligence that played an enormous part in Allied victories.

Bombe reconstruction at Bletchley Park



# Colossus

- Another component of ULTRA was the Colossus machine.
  - Used to attack the Lorenz SZ40/42 in-line cipher machine, not Enigma.
- It was the world's first programmable electronic digital computing machine.
- **Codebreaking—infosec again—was intimately bound up in the birth of the programmable digital computer.**



A Colossus Mark 2 computer being operated by Dorothy Du Boisson and Elsie Booker (1944-5) [U.K. National Archives, FO850/234]

# And information security today?

Ripped from the headlines…

# Drumbeat of major national and international problems

The New York Times

By DAVID E. SANGER and JULIE HIRSCHFELD DAVIS JUNE 4, 2015

## *Hacking Linked to China Exposes Millions of U.S. Workers*

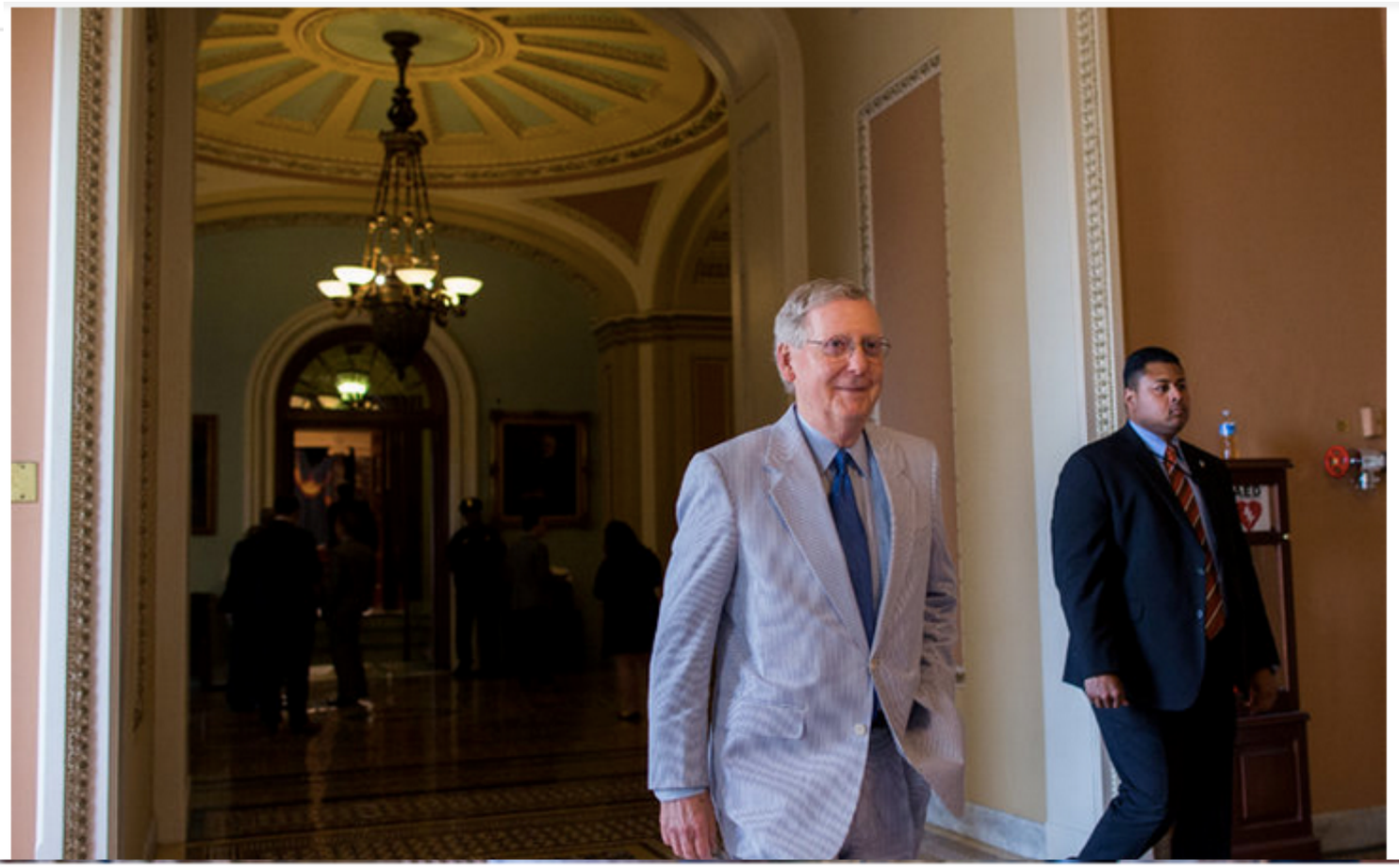
- Attack on U.S. federal systems started in 2014, detected in April 2015
- Initially reported to have affected four million current and former government workers
  - Later 18 million…
- Birth dates, Social Security numbers, previous addresses, and security clearances
  - Also fingerprints…
  - What would be the impact on secret agents?
- *Second break-in in less than a year*

# Thankfully, Congress took immediate action…

The New York Times

## Senate Rejects Measure to Strengthen Cybersecurity

By JENNIFER STEINHAUER JUNE 11, 2015



Senator Mitch McConnell, the majority leader, took part in a celebration of seersucker fabric on Thursday, but lamented the chamber's failure to pass cybersecurity legislation. Zach Gibson/The New York Times

# Problems won't go away

The New York Times

By THE ASSOCIATED PRESS JUNE 8, 2015, 10:32 A.M. E.D.T.

## *Obama: Cyberattack Attempts Against US Will Accelerate*

Obama is addressing cybersecurity following a massive hack of U.S. government employees' personnel files, described as the most significant cyberattack in U.S. history.

# Not confined to attacks on U.S.

The Opinion Pages | OP-ED CONTRIBUTOR

## Edward Snowden: The World Says No to Surveillance

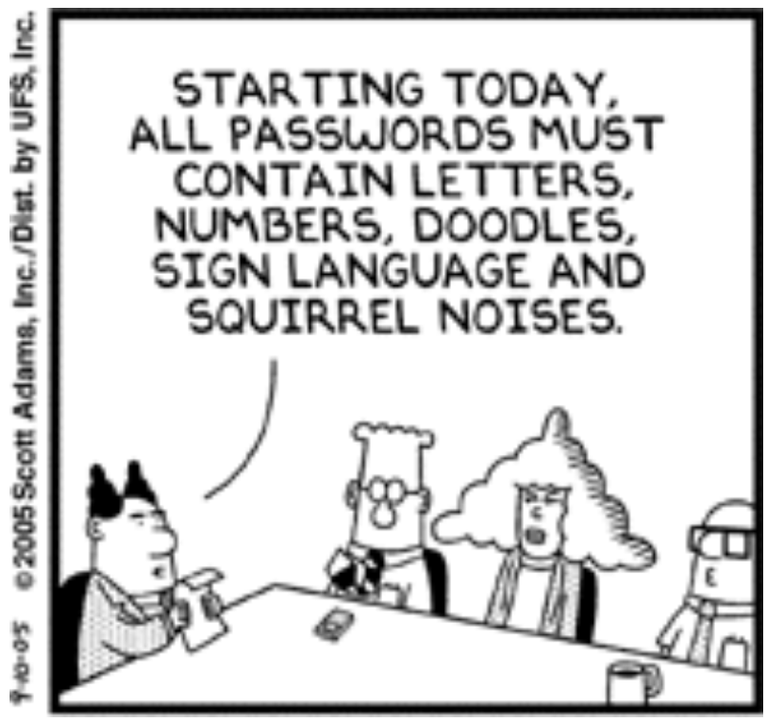
By EDWARD J. SNOWDEN JUNE 4, 2015

At the turning of the millennium, few imagined that citizens of developed democracies would soon be required to defend the concept of an open society against their own leaders.

# Security pervades daily life

- Passwords most visible example

**Breaking news!**




eWEEK

By Robert Lemos | Posted 2013-04-25

**Consumers Unhappy, Frustrated With Password Security**

**Nearly half of all consumers distrust online sites that rely on passwords for security and will abort transactions when they forget their passwords, according to a Ponemon Institute survey.**

# On the horizon…

CSO

By Taylor Armerding
CSO | Oct 9, 2013 8:00 AM PT

## The 'autonomous,' hackable car

the obvious question: If the best security available can't protect your smartphone, how is it going to protect you in your car?

What risks come if hacking is successful?

Self-driving cars are being worked on by Google and other technology companies. Photograph: Handout/Reuters

# Even more so in the future

## FBI warns driverless cars could be used as 'lethal weapons'

Internal report sees benefits for road safety, but warns that autonomy will create greater potential for criminal 'multitasking'

theguardian
Winner of the Pulitzer prize 2014

Self-driving cars are being worked on by Google and other technology companies. Photograph: Handout/Reuters

# Risk missed by media:
# Boring car chase scenes

# Ethics and the Law

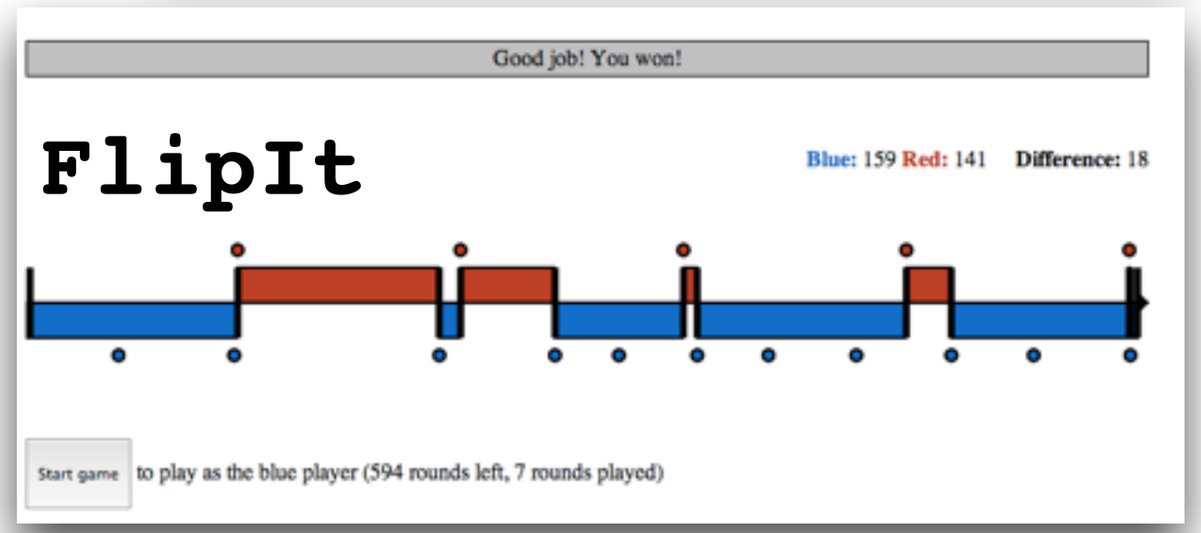
Behaving like a gentlewoman / gentleman

# Security is like a game

- It involves a pair of opponents, often a defender and attacker.
- They engage according to a set of rules, with a wide field of play.
- Breaking the rules is allowed.
- There are many ways to play and plenty of room for different skills:
  - Human factors
  - Mathematics
  - Bug finding
- It can be a lot of fun!

**Ctrl-Alt-Hack**


**http://www.controlalthack.com/**




**http://alannochenson.com/fliplt_demo/**

# There are several types of players

- **Black hat**: malicious hacker or criminal
- **Grey hat**: amoral hacker, sometimes criminal
- **White hat**: ethical hacker working within legal or ethical framework

# Question

Suppose you discovered the boarding pass vulnerability. What would be the right way to try to use your knowledge?

(a) Contact the TSA and report the problem.

(b) Publish an article on it.

(c) Create a web site that enables people to forge boarding passes easily.

(d) Sell it.

# Ethics

***Responsible disclosure*** means informing potential victims so they can fix a vulnerability before publication. The process is:

- Inform the vendor.
- Agree on a period of time to resolve / patch the problem. (E.g., CERT / CC gives vendors 45 days.)
- Disclose vulnerability publicly, so that affected parties are informed and the community learns.

# Example

- Bono et al. (2005) broke RFID device (TI DST) used in millions of automobiles and payment devices
- Stole our own car and stole gas using our own payment device
- Notified vendor
- Disclosed later in academic paper (USENIX)
  - Withheld critical implementation details
  - Gave enough detail to: (1) Give credible proof of vulnerability; (2) Offer knowledge on how to avoid it in future

"Stealing" car

"Stealing" gas

# Some guidelines

- Exploiting software vulnerabilities is unethical and illegal.
- Even exploration can be, as can unauthorized access to computer systems.
  - Computer Fraud and Abuse Act (CFAA)
- Violating others' privacy can also be illegal—and is certainly unethical.
- ***If in doubt, don't do it. (Ask!)***

# Takeaways

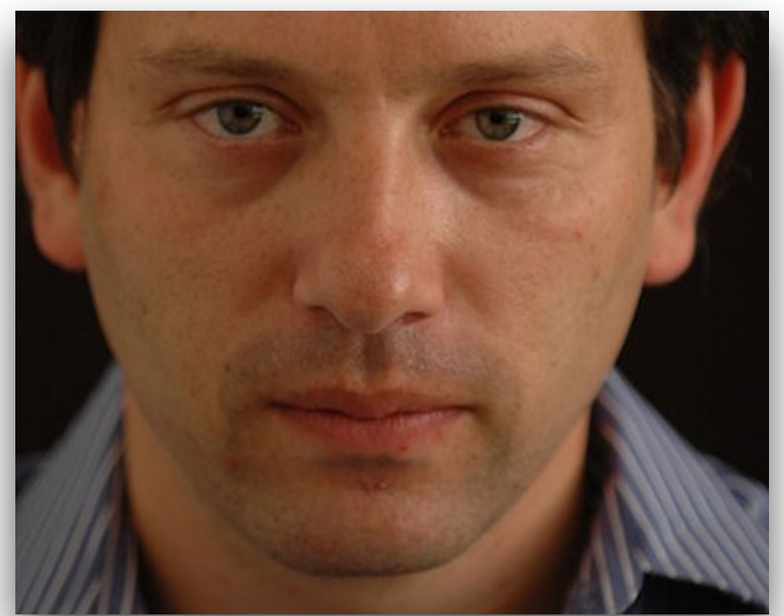
- Embrace the adversarial mindset. (Remember the two red slides!)
  - Four key questions: security goal, adversarial model, mechanisms, and incentives
  - Four key security goals: CIA + authenticity
- Take a broad view of security and privacy.
  - Not only about today's adversaries or system ABC v1.23.
  - About pervasive principles and societal impact.
- Behave like a gentlewoman / gentleman.
  - Be a white hat.
  - **If in doubt, don't do it. (Ask!)**

# Security, Privacy, and Crypto at Cornell Tech

Ari Juels

Rafael Pass

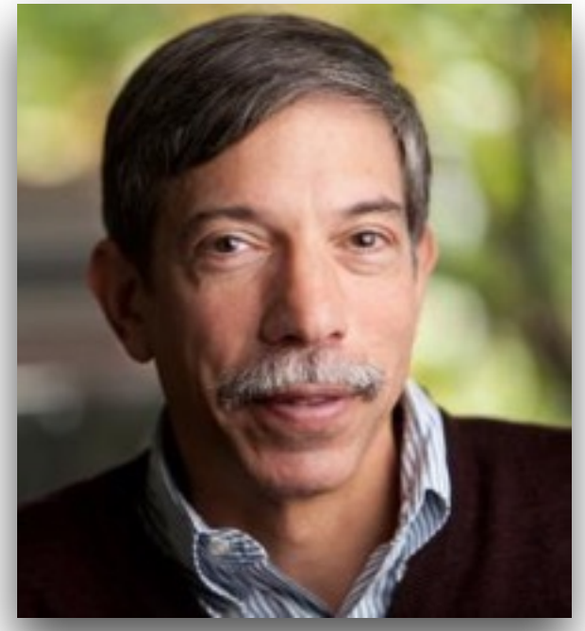
Tom Ristenpart



Vitaly Shmatikov

# Security, Privacy, and Crypto at Cornell (Ithaca)

Andrew Myers



Fred Schneider

Greg Morrisett
(CIS Dean)

Elaine Shi

Gün Sirer

# Course website

- http://www.cs.cornell.edu/~shmat/courses/cs5438/
- Google <- "Vitaly Shmatikov"