Fundamentals of Computer Security

Fall 2022

Radu Sion

Intro

Paranoia

Thanks to Ari Juels for parts of this deck!

A Message From Our Sponsors

- **Fundamentals**
  - System/Network Security, crypto
- **How** do things work
- **Why**
- How to **design** secure stuff

What we are **not**

- How to **install** XXX
- **Command line options** of XXX
- Latest **iexplorer buffer overflow bug**
- Latest McAfee/XXX **products**
- Network **administration**
- How to break your friend’s email account

What do we want?

- Doing things reliably …
- But isn't this what computing is all about?

- Doing things reliably …
- … in the presence of bad actors …
- … that want to mess with your system

- You can do cybersecurity in any area – this is fun
- Not unlike dentistry you always have stuff to do
- You can work in cybersec AND non-cybersec stuff

How?

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

Goals

- 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
- The course is about security design *concepts* or *principles*, not specific systems/software (although we'll explore those a bit too).
  - Security is always an arms race. The specifics change.

Paranoia

"Security requires a **particular mindset**. Security professionals […] 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)

Key Questions

1. **Security goal:** What policy (good state) is 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?

“Traditional” Security Goals

1. **Confidentiality:** Data not leaked
2. **Integrity:** Data or resource not tampered with
3. **Availability:** Data or resource accessible when needed
4. **Authenticity:** Correct belief in data or resource origin

“CIA + Authenticity”

But real life is much more complex.

Meaningful goals/policies can be arbitrarily complex.

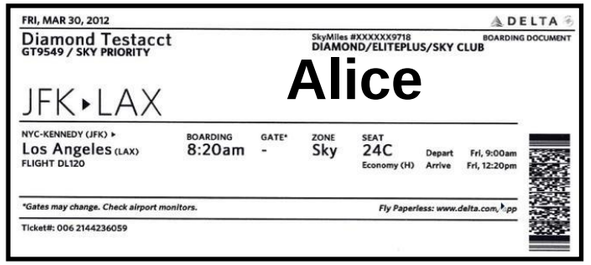
Sometimes they may not even mention “security”.

You can apply the adversarial mindset everywhere

- Card readers for this building
  - Can cards be skimmed / cloned?
- Your MTA card
  - Can the magstripe be hacked?
- Beam robots
  - How are they secured? What would be the consequences of a compromise?

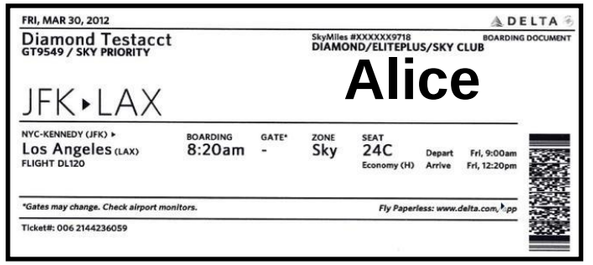
Example:
Air travel

Step 1: Home



Step 2: Security (Offline!!!)

Step 3: Gate



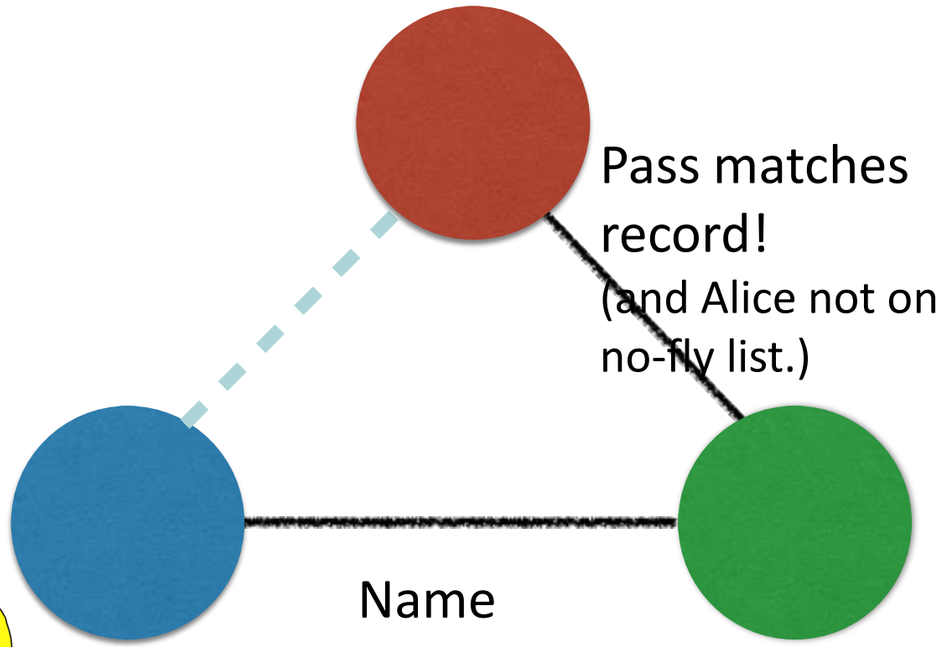
What's the **security goal** for passport / ID checking?

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

What's happening?

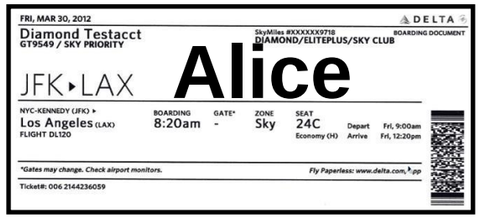
Flight record

Alice: JFK to LAX



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

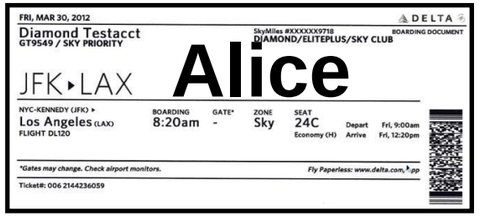
Name matches!



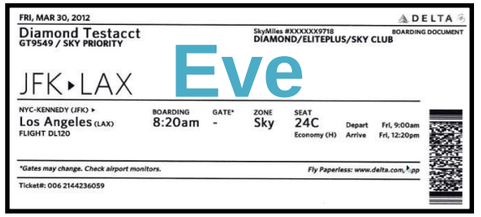
(Evil) Eve wants to get on a plane without detection (she's on a no-fly list)

Eve

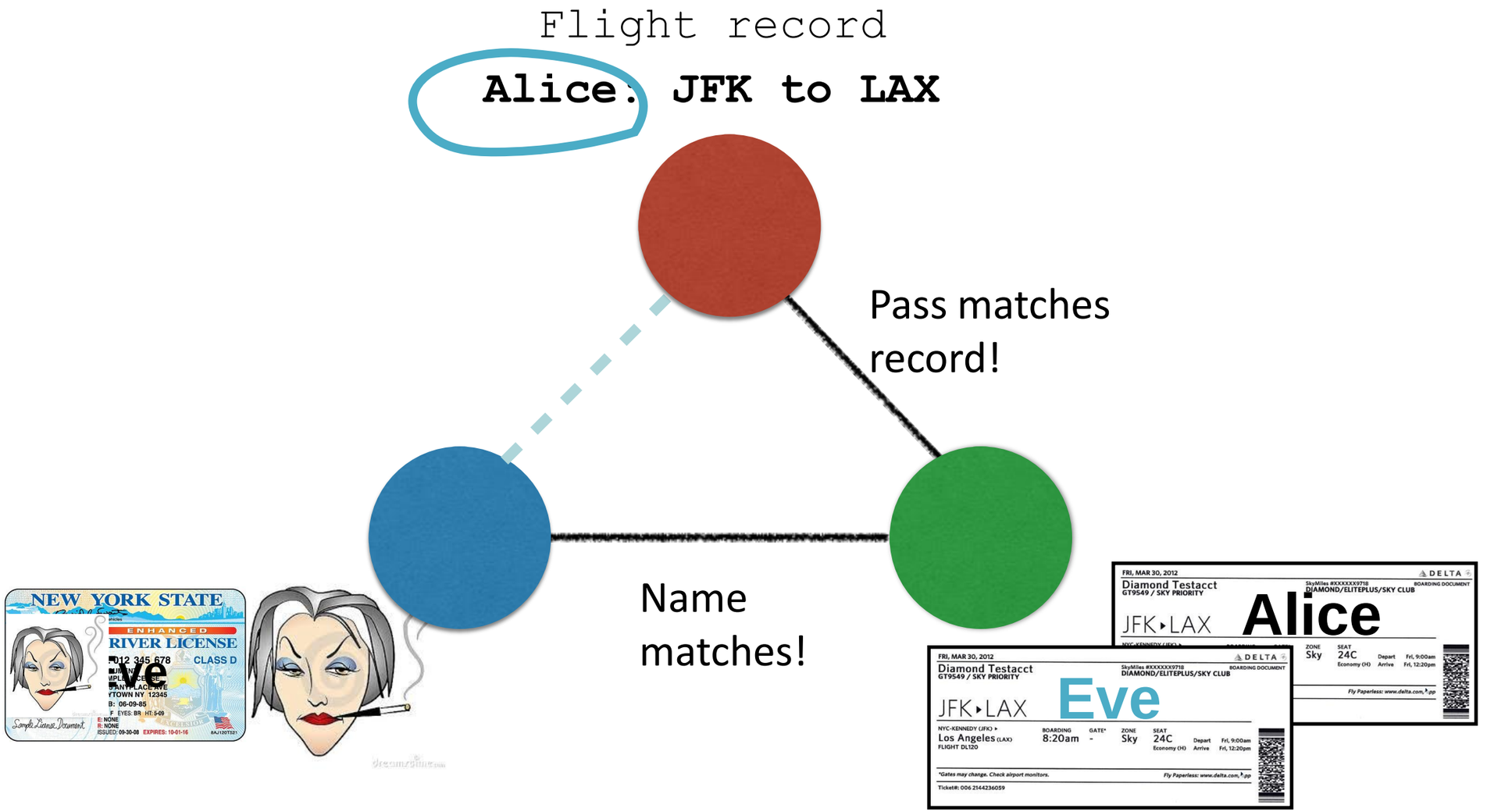
1. She steals a credit card (e.g., Alice's), buys a ticket in Alice's name, and prints a boarding pass for Alice.



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



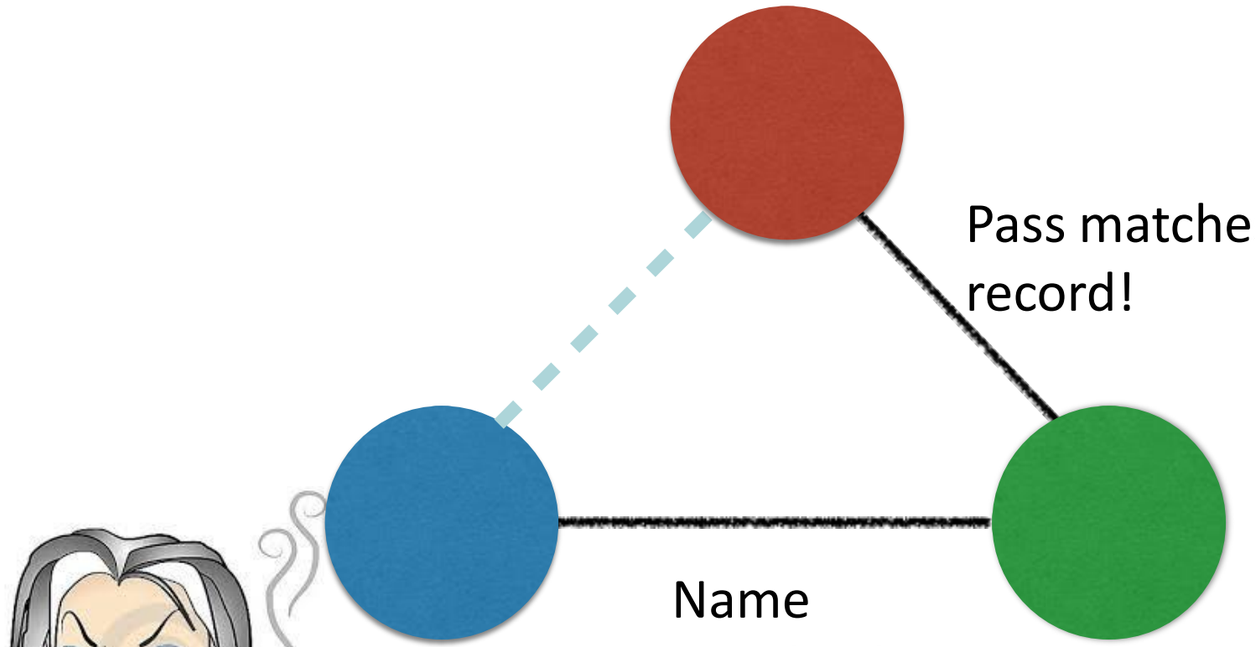
Eve can impersonate Alice!



There’s no record of Eve boarding!

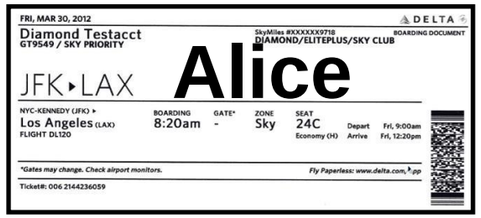
Flight record

Alice: JFK to LAX



Pass matches record!

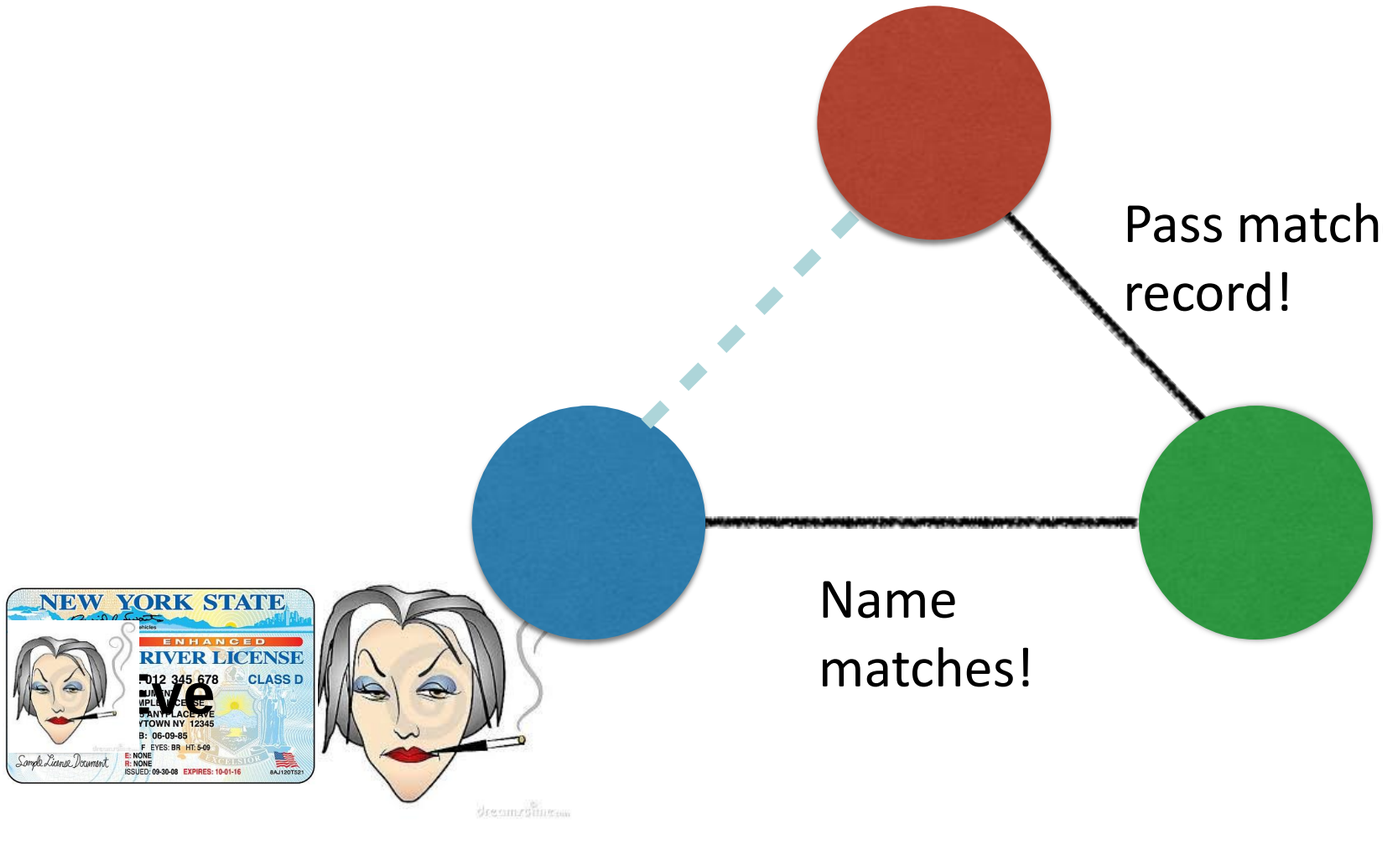
Name matches!



Mobile boarding passes no better

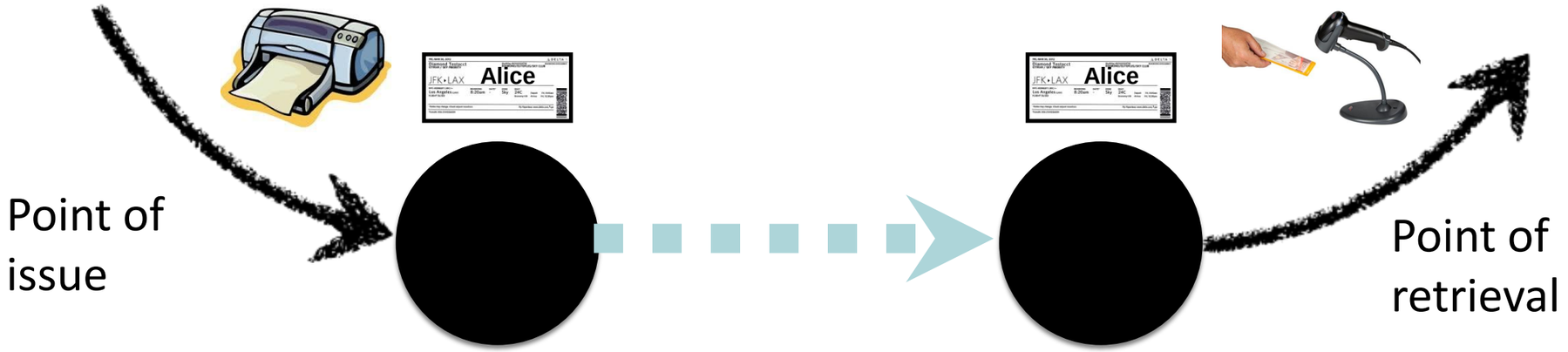
Flight record

Alice: JFK to LAX



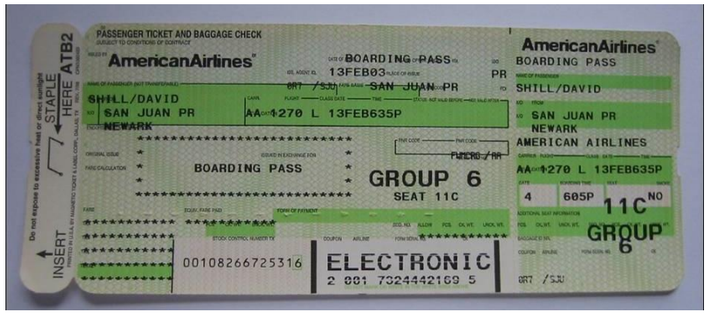
Where’s the mistake?

- 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**.

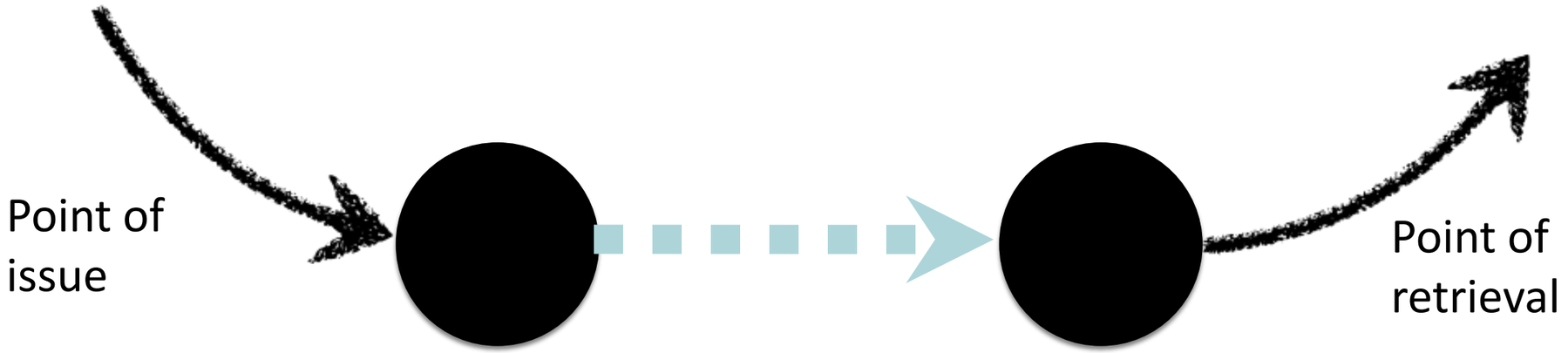


The adversarial model used to be different

- 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 Firefox extension

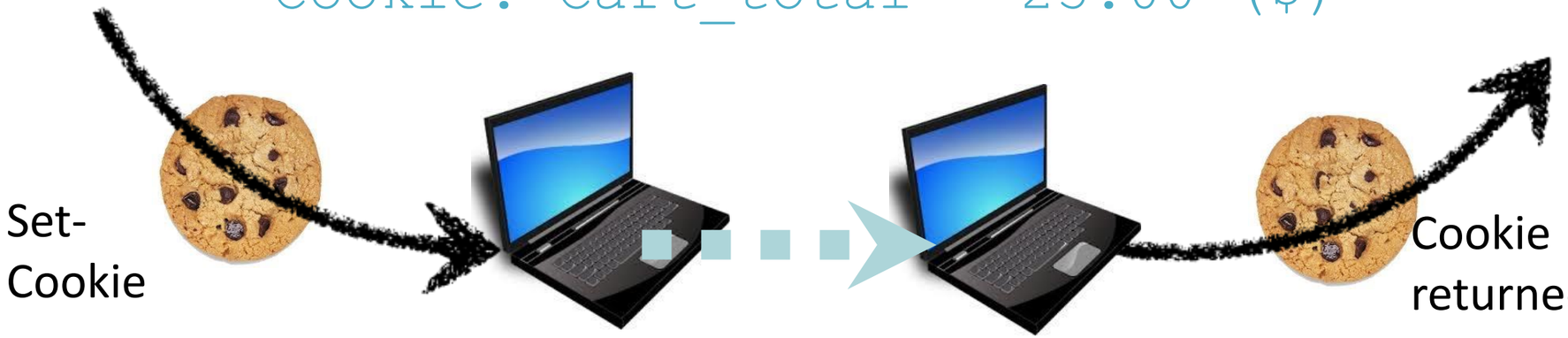
- Example:

  E-commerce site executes

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

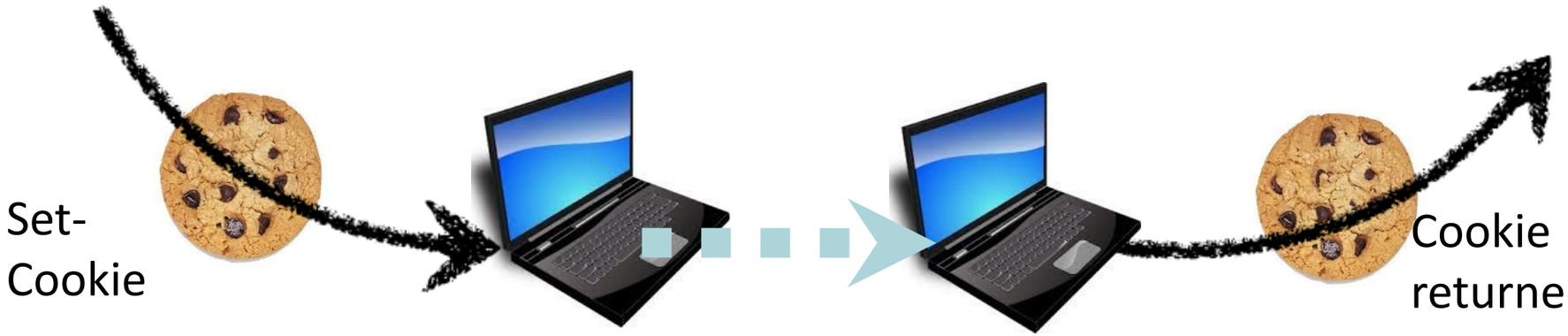
  Before paying, user substitutes

  ```
  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

Mobile-Number Thieves

SEARCH

The New York Times

GIFT T

y Thieves Hijack one Accounts to Go Virtual Currency

New Scrutiny for In-House Financial Court as Banker Faces Ban

BREAKINGVIEWS
Fine Print in Sempra's Energy Deal Bears a Close Examination

WHITE COLLAR WATCH
Insider Trading Case to Be a Test of the Role of Friendship

PAID POST: CON EDISON
5 Technologies That Represent the Future of Energy

conEdison

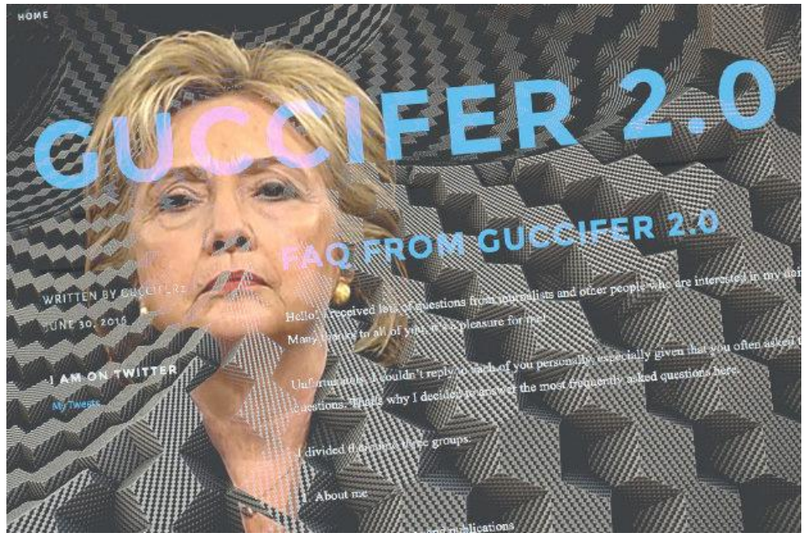
Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency

By NATHANIEL POPPER AUG. 21, 2017

- **Targets:** Mobile numbers of cryptocurrency holders
- **Made off with:**
  - Bitcoin!

Today's NYT

Guccifer 2.0



- **Targets:** The DNC computer network
- **Made off with:**
  - Confidential DNC documents
- Linked by U.S. intelligence to Russian intelligence services
- Involved in broad effort to swing U.S. election

https://en.wikipedia.org/wiki/Guccifer_2.0

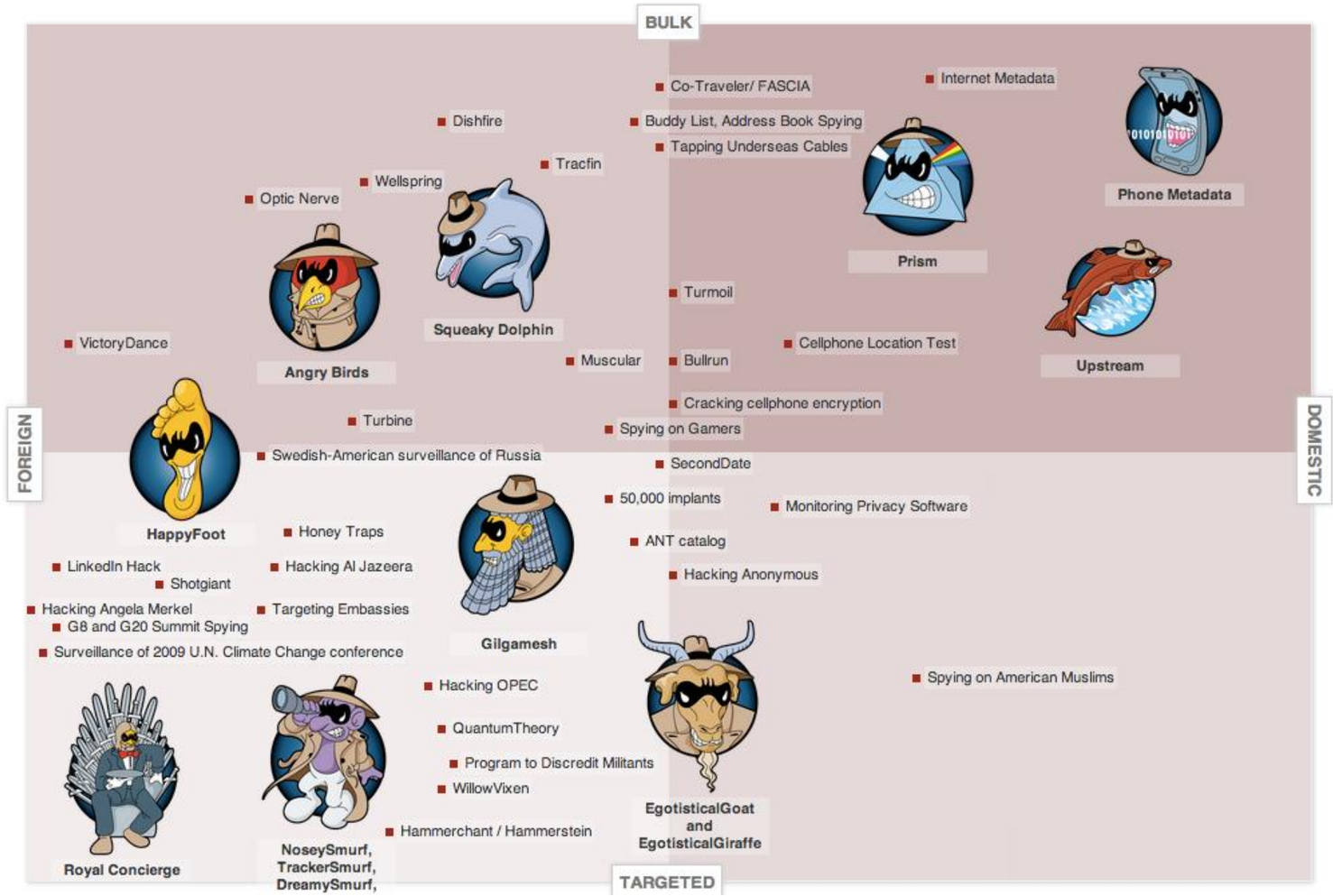
People’s Liberation Army and Chinese Government

- **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:



Makes off with: Not quite everything

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

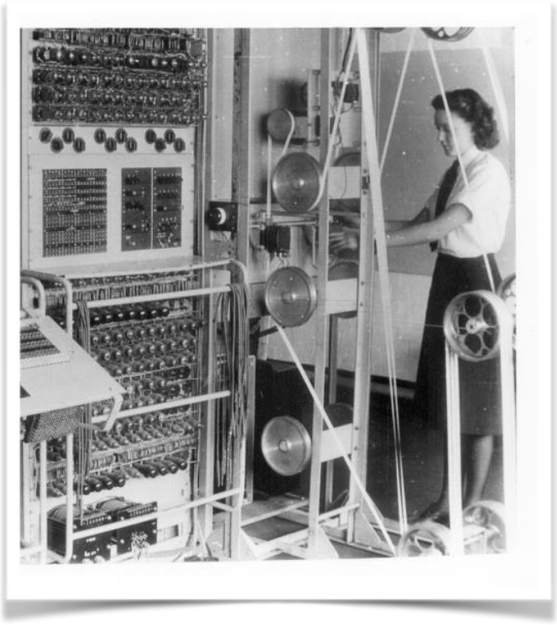
U.S. National Security Agency

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.

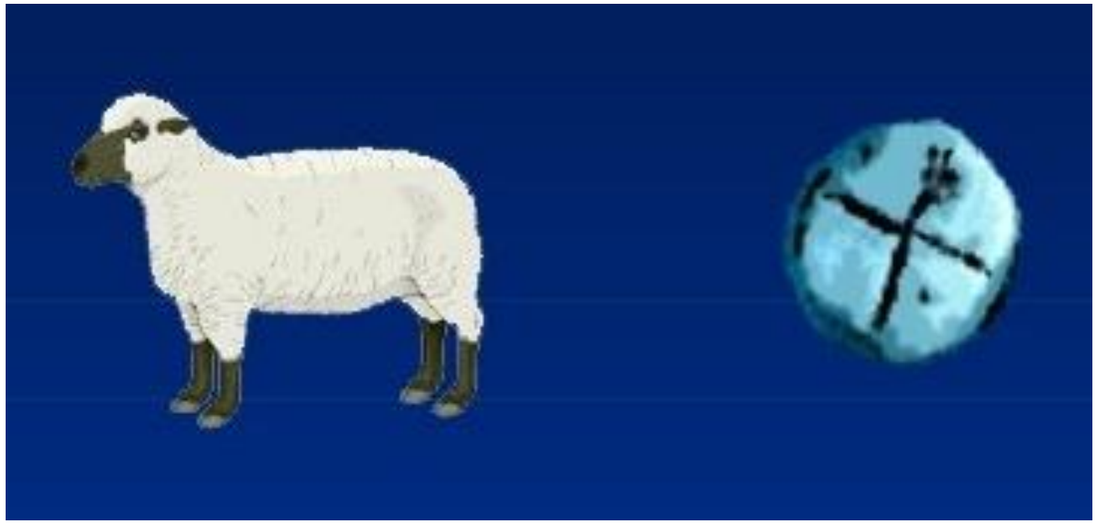
Suppose you deposited some sheep in the communal herd.

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…



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 may talk about Bitcoin later in the course…

Bitcoin

Cybersec @ Stony Brook

Amir

Michalis

Nick

Omkant

Radu

Sekar

Scott

Ground Rules

- Dates are listed online now
- Zero tolerance to academic dishonesty
- Informal class, ask questions anytime
- **Read your assigned readings !**
- There may be quizzes
- Call me Radu
- Questions: office hours, or email to schedule appt.
- Email: cse331@zxr.io
- Have fun !

Evaluation

- Homeworks (0-10%)
- Midterm (30-40%)
- Activity and pop quizzes (0-10%)
- Final (40-50%)
- Course website: **check link in your email**