Privacy
Computer Security
Peter Reiher
March 4, 2021

Privacy

- Data privacy issues
- Network privacy issues
- Some privacy solutions

What Is Privacy?

- The ability to keep certain information secret
- Usually one's own information
- But also information that is "in your custody"
- Includes ongoing information about what you're doing

Privacy and Computers

- Much sensitive information currently kept on computers
  - Which are increasingly networked
- Often stored in large databases
  - Huge repositories of privacy time bombs
- We don't know where our information is

Privacy and Our Network Operations

- Lots of stuff goes on over the Internet
  - Banking and other commerce
  - Health care
  - Romance and sex
  - Family issues
  - Personal identity information
- We used to regard this stuff as private
  - Is it private any more?

Threat to Computer Privacy

- Cleartext transmission of data
- Poor security allows remote users to access our data
- Sites we visit save information on us
  - Multiple sites can combine information
- Governmental snooping
- Location privacy
- Insider threats in various places

Some Specific Privacy Problems

- Poorly secured databases that are remotely accessible
  - Or are stored on hackable computers
- Data mining by companies we interact with
- Eavesdropping on network communications by governments
- Insiders improperly accessing information
- Cell phone/mobile computer-based location tracking

Do Users Care About Privacy?

- Evidence suggests yes, but . . .
- Not necessarily in the way researchers think
  - E.g., data suggests teenagers aren't worried about privacy from hackers
  - They worry about privacy from their parents
- One must consider the actual privacy goals of users in protecting privacy

Data Privacy Issues

- My data is stored somewhere
  - Can I control who can use it/see it?
- Can I even know who's got it?
- How do I protect a set of private data?
  - While still allowing some use?
- Will data mining divulge data "through the back door"?

Privacy of Personal Data

- Who owns data about you?
- What if it's really personal data?
  - Social security number, DoB, your DNA record?
- What if it's data someone gathered about you?
  - Your Google history or shopping records
  - Does it matter how they got it?

Protecting Data Sets

- If my company has (legitimately) a bunch of personal data,
- What can I/should I do to protect it?
  - Given that I probably also need to use it?
- If I fail, how do I know that?
  - And what remedies do I have?

Options for Protecting Data

- Careful system design
- Limited access to the database
  - Networked or otherwise
- Full logging and careful auditing
- Store only encrypted data
  - But what about when it must be used?
  - Key issues

Data Mining and Privacy

- Data mining allows users to extract models from databases
  - Based on aggregated information
- Often data mining allowed when direct extraction isn't
- Unless handled carefully, attackers can use mining to deduce record values

An Example of the Problem

- Netflix released a large database of user rankings of films
  - Anonymized, but each user had one random identity
- Clever researchers correlated the database with IMDB rankings
  - Which weren't anonymized
  - Allowed them to match IMDB names to Netflix random identities

Insider Threats and Privacy

- Often insiders need access to private data
  - Under some circumstances
- But they might abuse that access
- How can we determine when they misbehave?
- What can we do?

Local Examples

- Over 120 UCLA medical center employees improperly viewed celebrities' medical records
  - Between 2004-2006
- Two accidental postings of private UCLA medical data in 2011
- UCLA is far from the only offender

Encryption and Privacy

- Properly encrypted data can only be read by those who have the key
  - In most cases
  - And assuming proper cryptography is hazardous
- So why isn't keeping data encrypted the privacy solution?

Problems With Data Encryption for Privacy

- Who's got the key?
- How well have they protected the key?
- If I'm not storing my data, how sure am I that encryption was applied?
- How can the data be used when encrypted?
  - If I decrypt for use, what then?

One Major Case

- Yahoo lost 450,000 user IDs and passwords in July 2012
  - The passwords weren't encrypted
  - Much less salted
- Password file clearly wasn't well protected, either
- Who else is storing your personal data unencrypted?

Network Privacy

- Mostly issues of preserving privacy of data flowing through network
- Start with encryption
  - With good encryption, data values not readable
- So what's the problem?

Traffic Analysis Problems

- Sometimes desirable to hide that you're talking to someone else
- That can be deduced even if the data itself cannot
- How can you hide that?
  - In the Internet of today?

A Cautionary Example

- VoIP traffic is commonly encrypted
- Researchers recently showed that they could understand what was being said
  - Despite the encryption
  - Without breaking the encryption
  - Without obtaining the key

How Did They Do That?

- Lots of sophisticated data analysis based on understanding human speech
  - And how the application worked
- In essence, use size of encrypted packets and interarrival time
  - With enough analysis, got conversation about half right
- Where else might similar techniques work on encrypted data?

Location Privacy

- Mobile devices often communicate while on the move
- Often providing information about their location
  - Perhaps detailed information
  - Maybe just hints
- This can be used to track our movements

Cellphones and Location

- Provider knows what cell tower you're using
- With some effort, can pinpoint you more accurately
- In US, law enforcement can get that information just by asking
  - Except in California

Other Electronic Communications and Location

- Easy to localize user based on hearing 802.11 wireless signals
- Many devices contain GPS nowadays
  - Often possible to get the GPS coordinates from that device
  - Did that app ask to see your GPS info?
- Bugging a car with a GPS receiver not allowed without warrant
  - For now . . .

Implications of Location Privacy Problems

- Anyone with access to location data can know where we go
- Allowing government surveillance
- Or a private detective following your moves
- Or a maniac stalker figuring out where to ambush you . . .

Why Isn't the Internet Private?

- All messages tagged with sender's IP address
- With sufficient legal authority, there are reliable mappings of IP to machine
  - ISP can do it without that authority
- Doesn't indicate who was using the machine
  - But owner is generally liable
  - Or at least gets the visit from the cops

Privacy and Cryptocurrency

- Theoretically, cryptocurrency offers private financial transactions
- But cryptocurrency is based on a public distributed ledger
  - All transactions are logged there
  - Not by name, but by an identifier
- The identifier can often be tied to a person

A Recent Example

- A child pornography ring using cryptocurrency recently (2019) busted
- Authorities traced whose cryptocurrency wallets were using it
- Then got identity information from the companies that handled the wallets
- Leading back to actual people

Web Privacy

- Where we visit with our browsers reveals a lot about us
- Advertisers and other merchants really want that information
- Maybe we don't want to give it to them
  - Or to others
- But there are many technologies to allow tracking
  - Even to sites the tracker doesn't control

Do Not Track

- Wouldn't it be nice if we could ensure that web sites don't track us?
- Enter the Do Not Track standard
- A configurable option in your web browser
- Which, by enabling, you might think prevents you from being tracked

The Problems With Do Not Track

- First, it's voluntary
  - Web server is supposed to honor it
  - But will they?
- Second, and worse, it doesn't mean what you think it means
  - Based on current definitions of the option

What Do Not Track Really Means

- What it really means is "I'll track you anyway"
- "But I won't provide you anything helpful based on the tracking"
- So they know what you're doing
  - And they do whatever they want with that data
- But you don't see targeted ads
- So what's the point of Do Not Track?
  - A good question

Some Privacy Solutions

- The Scott McNealy solution
  - "Get over it."
- Data encryption for privacy
- Anonymizers
- Onion routing
- Privacy-preserving data mining
- Preserving location privacy

Data Encryption for Privacy

- Store private data in encrypted form
- If the encrypted version is divulged, attacker might not be able to use it
  - Assuming strong crypto
  - And careful key management
- Particularly important for data on devices that are easily stolen
  - Portable computers, smart phones, flash drives

A Fundamental Issue

- Entities usually keep sensitive data because they want to process it
- They can't process encrypted data
- So they can usually decrypt it
- If the attacker can get the decrypted version, you lose
- Limits the benefit of crypto for privacy

Full Disk Encryption

- A useful solution for data on portable computers
  - Some laws regard such encrypted data as “safe”
- But only if key not available to a thief
  - So where did you get that key?

Anonymizers

- Network sites that accept requests of various kinds from outsiders
- Then submit those requests
  - Under their own or fake identity
- Responses returned to the original requestor
- A NAT box is a poor man's anonymizer

The Problem With Anonymizers

- The entity running it knows who's who
- Either can use that information himself
- Or can be fooled/compelled/hacked to divulge it to others
- Generally not a reliable source of real anonymity

An Early Example

- A remailer service in Finland
- Concealed the actual email address of the sender
  - By receiving the mail and resending it under its own address
- Court order required owner of service to provide a real address
  - After which he shut down the service

Onion Routing

- Meant to handle issue of people knowing who you're talking to
- Basic idea is to conceal sources and destinations
- By sending lots of crypo-protected packets between lots of places
- Each packet goes through multiple hops

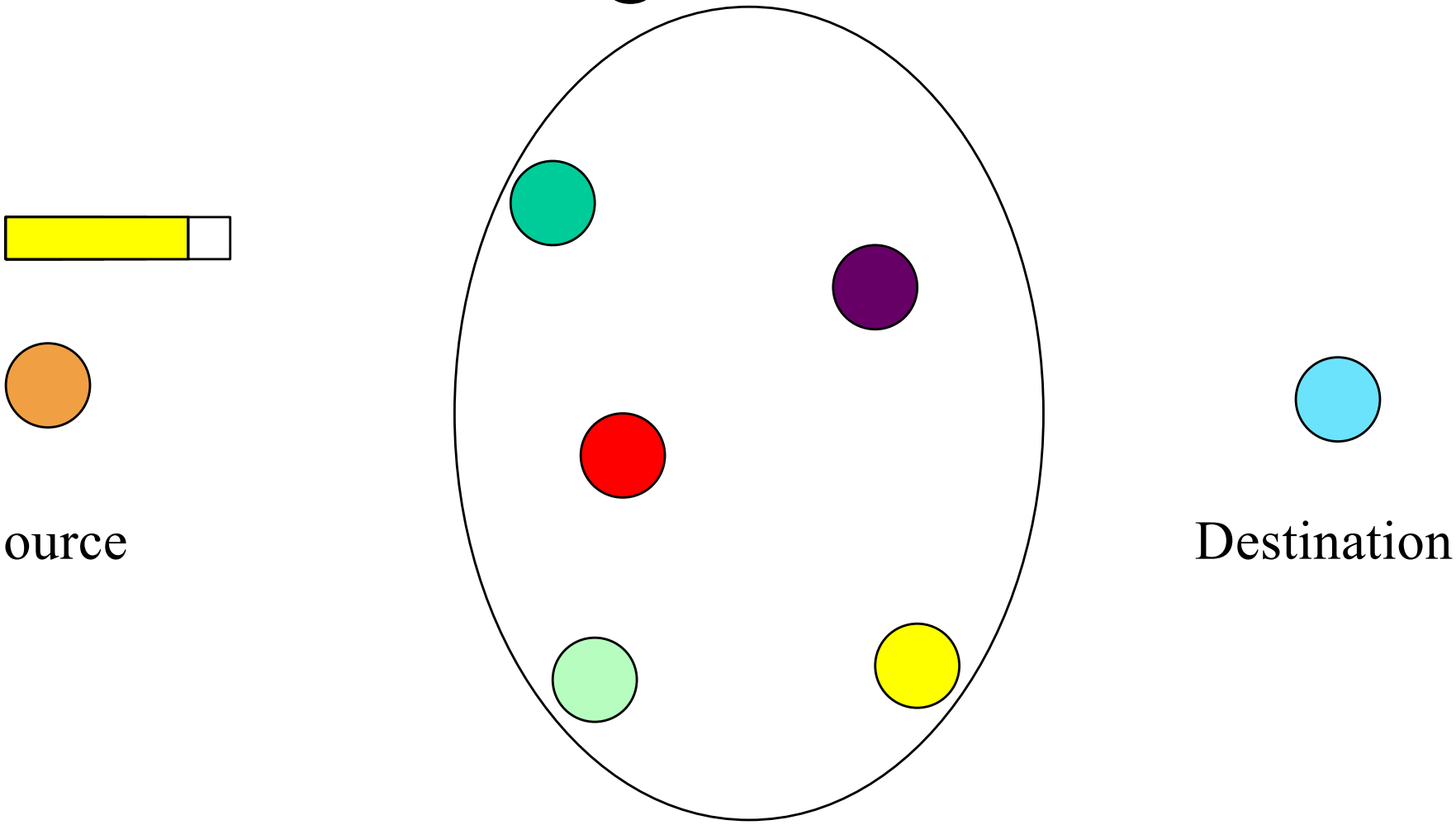
A Little More Detail

- A group of nodes agree to be onion routers
- Users obtain crypto keys for those nodes
- Plan is that many users send many packets through the onion routers
  - Concealing who's really talking

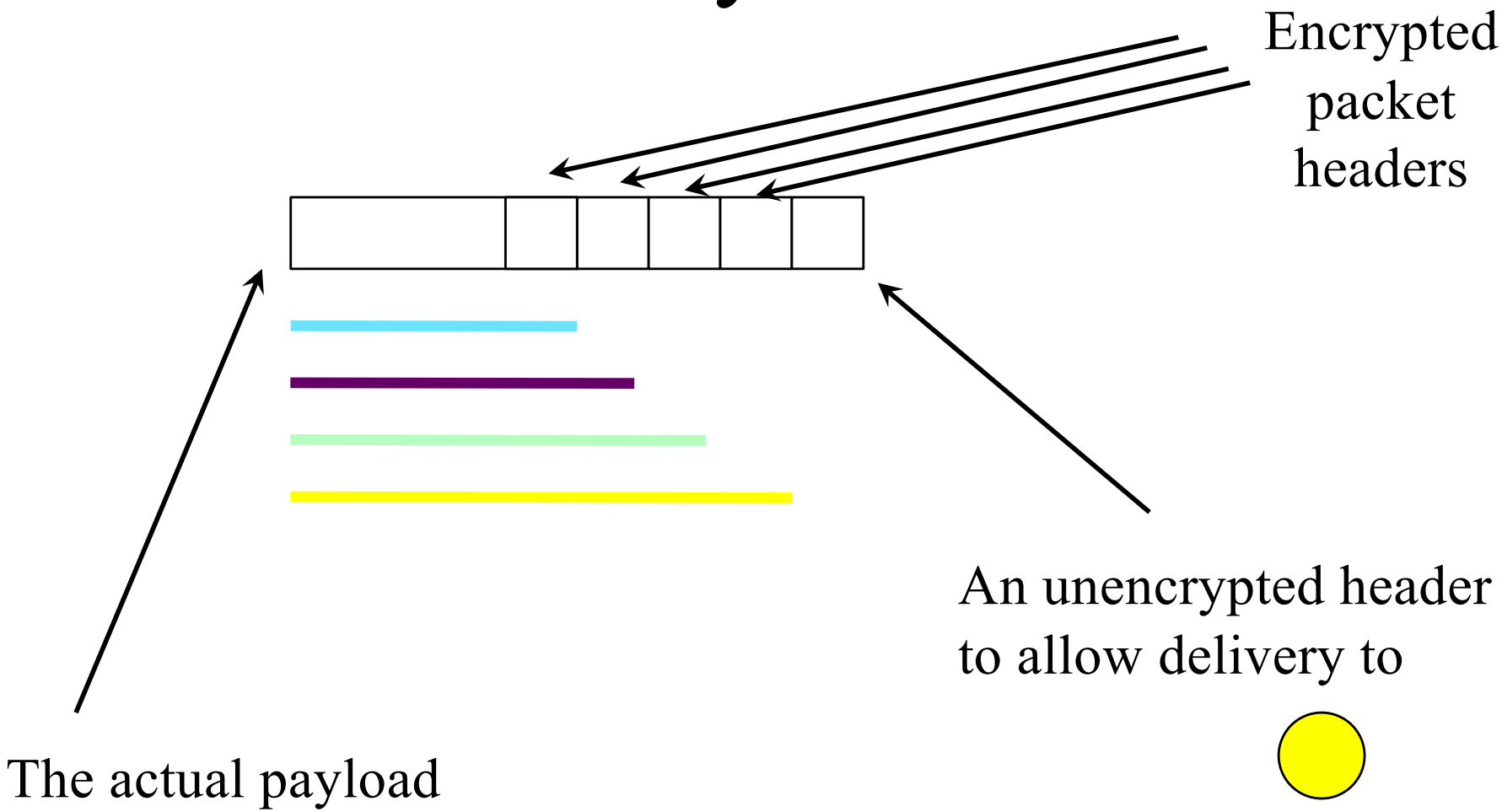
Sending an Onion-Routed Packet

- Encrypt the packet using the destination's key
- Wrap that with another packet to another router
  - Encrypted with that router's key
- Iterate a bunch of times

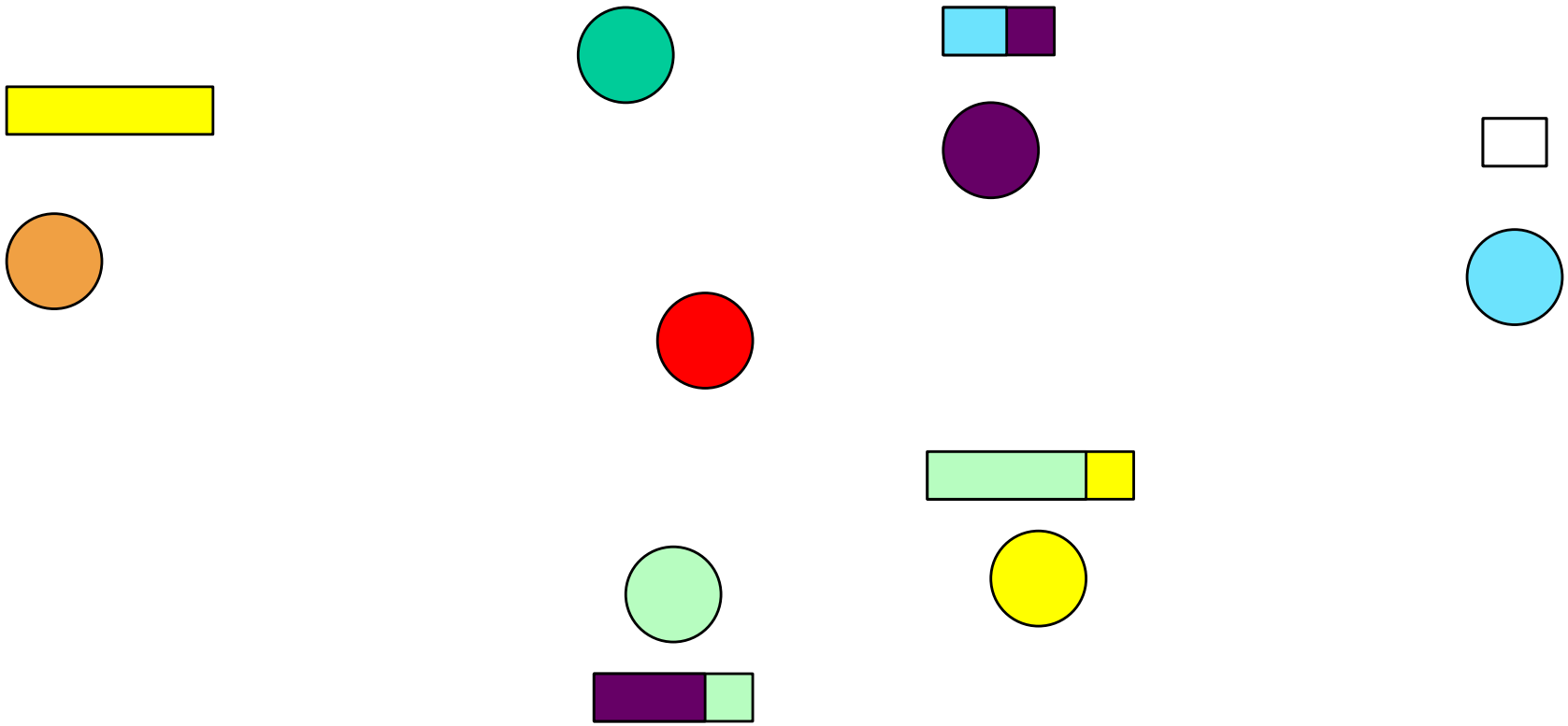
In Diagram Form



What's Really in the Packet



Delivering the Message



What's Been Achieved?

- Nobody improper read the message
- Nobody knows who sent the message
  - Except the receiver
- Nobody knows who received the message
  - Except the sender
- Assuming you got it all right

Issues for Onion Routing

- Proper use of keys
- Traffic analysis
- Overheads
  - Multiple hops
  - Multiple encryptions

Tor

- The most popular onion routing system
- Widely available on the Internet
- Using some of the original onion routing software
  - Significantly altered to handle various security problems
- Usable today, if you want to
- IETF is investigating standard for Tor

Why Hasn't Tor Solved This Privacy Problem?

- First, the limitations of onion routing
- Plus usability issues
  - Tor's as good as it gets, but isn't that easy to use
- Can't help if a national government disapproves
  - China and other nations have prohibited Tor's use

Can't I Surreptitiously Run Tor?

- Can't I get around government restrictions by just not telling them?
- No
  - Tor routers must know each others' identities
  - Traffic behavior of Tor routers "glows in the dark"
  - Tor developers keep trying

Another Problem With Tor

- What if a Tor router is compromised?
- Worse, what if many of them are?
- In particular, if your entry point to Tor is compromised, you lose all privacy
- An approach commonly used by sophisticated opponents (like the NSA)

Recent VPN Compromise

- Several commercial VPNs have had security compromises lately (2019)
  - NordVPN, TorGuard, VikingVPN
- All lost some crypto keys
- Not clear how much (and whose) data that exposed

Privacy and End-to-End Cryptography

- Privacy advocates usually recommend end-to-end crypto
- From the device you're actually using to the device you're talking to
- Don't rely purely on stuff like VPNs and commercial services promising crypto
- Of course, if an end point is compromised . . .

Privacy-Preserving Data Mining

- Allow users access to aggregate statistics
- But don't allow them to deduce individual statistics
- How to stop that?

Approaches to Privacy for Data Mining

- Perturbation
  - Add noise to sensitive value
- Blocking
  - Don't let aggregate query see sensitive value
- Sampling
  - Randomly sample only part of data

The NSA and Privacy

- 2013 revelations about NSA spying programs changed conversation on privacy
- The NSA is more heavily involved in surveillance than previously believed
- What are they doing and what does that mean for privacy?

Conclusion

- Privacy is a difficult problem in computer systems
- Good tools are lacking
  - Or are expensive/cumbersome
- Hard to get cooperation of others
- Probably an area where legal assistance is required