Traffic Analysis
high latency anonymous communications

Carmela Troncoso*
IMDEA Software Institute

*Thanks to George Danezis for sharing slides
Privacy in electronic communications

Alice

A Network

Bob
Dear Dr. Bob,
Can we change my chemo appointment?

A.
Dear Dr. Bob,
Can we change my chemo appointment?

A
Privacy in electronic communications

Dear Dr. Bob,
Can we change my chemo appointment?

A

A Network
Dear Dr. Bob,
Can we change my chemo appointment?

A.

A Network
Dear Dr. Bob,
Can we change my chemo appointment?

A Network

Intelligence agencies
Your Parents
Your Children
The Boss
SysAdmins
Alice
Bob
ISPs
Privacy in electronic communications

Intelligence agencies

Your Parents

Your Children

SysAdmins

The Boss

Anybody curious

ISPs

Alice

A Network

Dear Dr. Bob, Can we change my chemo appointment? A.

Bob
Privacy in electronic communications

Intelligence agencies
Your Parents
Your Children
The Boss
Anybody curious
SysAdmins

Dear Dr. Bob,
Can we change my chemo appointment?

A

A Network

Alice
Bob

ISPs
Privacy in electronic communications

Dear Dr. Bob,
Can we change my chemo appointment?
A.
But we can encrypt! What is the problem?

Dear Dr. Bob,
Can we change my chemo appointment?

A

Alice

Bob

A Network
But we can encrypt! What is the problem?
But we can encrypt! What is the problem?
But we can encrypt! What is the problem?

A Network

<table>
<thead>
<tr>
<th>PREAMBLE</th>
<th>DESTINATION ADDRESS</th>
<th>SOURCE ADDRESS</th>
<th>LENGTH/ETHTYPE</th>
<th>DATA</th>
<th>PCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Bytes</td>
<td>6 Bytes</td>
<td>6 Bytes</td>
<td>2 Bytes</td>
<td>Variable 46-1500 Bytes</td>
<td>4 Bytes</td>
</tr>
</tbody>
</table>

ETHERNET
(IEEE 802.3, 1997)
But we can encrypt! What is the problem?

A Network

<table>
<thead>
<tr>
<th>PREAMBLE</th>
<th>DESTINATION ADDRESS</th>
<th>SOURCE ADDRESS</th>
<th>LENGTH/ETYPE</th>
<th>DATA</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Bytes</td>
<td>6 Bytes</td>
<td>6 Bytes</td>
<td>2 Bytes</td>
<td>Variable 46-1500 Bytes</td>
<td>4 Bytes</td>
</tr>
</tbody>
</table>

Ethernet
(IEEE 802.3, 1997)
But we can encrypt! What is the problem?

A Network

Alice

Bob

<table>
<thead>
<tr>
<th>PREAMBLE</th>
<th>DESTINATION ADDRESS</th>
<th>SOURCE ADDRESS</th>
<th>LENGTH/ETYPE</th>
<th>DATA</th>
<th>PCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Bytes</td>
<td>6 Bytes</td>
<td>6 Bytes</td>
<td>2 Bytes</td>
<td>Variable 46-1500 Bytes</td>
<td>4 Bytes</td>
</tr>
</tbody>
</table>

ETHERNET
(IEEE 802.3, 1997)
But we can encrypt! What is the problem?

A Network

SAME for TCP, SMTP, IRC, HTTP, ...

Ethernet
(IEEE 802.3, 1997)

IPv4 Header
(RFC 791, 1981)

Weak Identifier
But we can encrypt! What is the problem?
OMG!! The problem is Traffic Analysis!!

A Network

ETHERNET (IEEE 802.3, 1997)

IPV4 HEADER (RFC 791, 1981)

SAME for TCP, SMTP, IRC, HTTP, ...
Traffic WHAT?

Wikipedia: traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication.

Making use of "just" traffic data of a communication (aka metadata) to extract information (as opposed to analyzing content or perform cryptanalysis).
Traffic WHAT?

WIREPEDIA: traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. Making use of “just” traffic data of a communication (aka metadata) to extract information (as opposed to analyzing content or perform cryptanalysis).

- Identities of communicating parties
- Timing, frequency, duration
- Location
- Volume
- Device
Traffic WHAT?

Wikipedia: traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication.

Making use of "just" traffic data of a communication (aka metadata) to extract information (as opposed to analyzing content or perform cryptanalysis)

Military Roots

- M. Herman: "These non-textual techniques can establish TARGETS' LOCATIONS, order-of-battle and MOVEMENT. Even when messages are not being deciphered, traffic analysis of the target's Command, Control, Communications and intelligence system and its patterns of behavior provides indications of his INTENTIONS and STATES OF MIND."

- WWI: British troops finding German boats.

- WWII: assessing size of German Air Force, fingerprinting of transmitters or operators (localization of troops).

Herman, Michael. Intelligence power in peace and war. Cambridge University Press, 1996.
http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded
Traffic WHAT?

Wikipedia: traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication

Making use of “just” traffic data of a communication (aka metadata) to extract information
(as opposed to analyzing content or perform cryptanalysis)

Military Roots

- M. Herman: “These non-textual techniques can establish targets’ locations, order-of-battle and movement. Even when messages are not being deciphered, traffic analysis of the target’s Command, Control, Communications and intelligence system and its patterns of behavior provides indications of his intentions and states of mind.”

- WWI: British troops finding German boats.

- WWII: assessing size of German Air Force, fingerprinting of transmitters or operators (localization of troops).

Nowadays

- Diffie & Landau: “Traffic analysis, not cryptanalysis, is the backbone of communications intelligence.”

- Stewart Baker (NSA): “metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.”

- Tempora, MUSCULAR → XkeyScore, PRISM

- Also “good” uses: recommendations, location-based services,

Herman, Michael. Intelligence power in peace and war. Cambridge University Press, 1996.
http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded
Actually, any **Meta Data** is sensitive!!
Actually, any **Meta Data** is sensitive!!
Actually, any **Meta Data** is sensitive!!
Actually, any **meta data** is sensitive!!
Actually, any **Meta Data** is sensitive!!

Dr. Bob
Oncologist

Alice

Cold

Cancer

0x37FD00
0x39FD10

0x54E100
0x61AB10
Actually, any **Meta Data** is sensitive!!
Actually, any **Meta Data** is sensitive!!
Actually, any **Meta Data** is sensitive!!
We need to protect the communication layer!

Anonymous communications

- **General applications**
  - Freedom of speech
  - Profiling / price discrimination
  - Spam avoidance
  - Investigation / market research
  - Censorship resistance

- **Specialized applications**
  - Electronic voting
  - Auctions / bidding / stock market
  - Incident reporting
  - Witness protection / whistle blowing
  - Showing anonymous credentials!

Anonymity is important to:

- the people who run some of the funniest parody Twitter accounts, such as @FeministHulk (SMASH THE PATRIARCHY) or @BFGlobalPr during the Deepwater Horizon aftermath. San Francisco would not be better off if we knew who was behind @KartheFog, the most charming personification of a major city's climate phenomenon.
- the young LGBTQ youth seeking advice online about coming out to their parents.
- the marijuana grower who needs to ask questions on an online message board about lamps and fertilizer or complying with state law, without publicly admitting to committing a federal offense.
- the medical patient seeking advice from other patients in coping with a chronic disease, whether it's alopecia, irritable bowel syndrome, cancer or a sexually transmitted infection.
- the online dater, who wants to meet new people but only reveal her identities after she's determined that potential dates are not creeps.
- the business that wants no-pulled-punches feedback from its customers.
- the World of Warcraft player, or any other MMOG gamer, who only wants to engage with other players in character.
- artists. Anonymity is integral to the work of The Yes Men, Bankay and Keizer.
- the low-income neighborhood resident who wants to comment on an article about gang violence in her community, without incurring retribution in the form of spray paint and broken windows.
- the boyfriend who doesn't want his girlfriend to know he's posing questions on a forum about how to pick out a wedding ring and propose. On the other end: Anonymity is important to anyone seeking advice about divorce attorneys online.
- the youth from an orthodox religion who secretly posts reviews on hip hop albums or R-rated movies.
- the young, pregnant woman who is seeking out advice on reproductive health services.
- the person seeking mental health support from an online community. There's a reason that support groups so often end their names with "Anonymous."
- the job seeker, in pursuit of cover letter and resume advice in a business blogger's comments, who doesn't want his current employer to know he is looking for work.
- many people's sexual lives, whether they're discussing online erotica or arranging kink meet-ups.
- Political Gabfest listeners. Each week, the hosts encourage listeners to post comments. Of the 262 largely positive customer reviews on iTunes, only a handful see value in using their real names.

https://www.eff.org/deeplinks/2013/10/online-anonymity-not-only-trolls-and-political-dissidents
http://geekfeminism.wikia.com/wiki/Who_is harmed_by_a_%22Real_Names%22_policy%3F
Anonymous communications: abstract model

- IDs
- Timing
- Volume
- Length

Senders

Anonymous communication system

Receivers

- Bitwiseunlinkability
  - Crypto to make inputs and outputs bit patterns different

- (Re)packetizing + (Re)schedule
  - Destroy patterns (traffic analysis resistance)
Anonymous communications: abstract model

- Bitwise unlinkability
  - Crypto to make inputs and outputs bit patterns different

- (re)packetizing + (re)schedule + (re)routing,
  - Destroy patterns (traffic analysis resistance)
  - Load balancing
  - Distribute trust
Anonymous communications: abstract model

- Bitwise unlinkability
  - Crypto to make inputs and outputs bit patterns different

- (re)packetizing + (re)schedule + (re)routing,
  - Destroy patterns (traffic analysis resistance)
  - Load balancing
  - Distribute trust
In theory should work, but in practice...

- **IDs**
- **Timing**
- **Volume**
- **Length**

...  

**Senders**  

**Receivers**

- **Bitwise unlinkability**
  - Crypto to make inputs and outputs bit patterns different

- **(Re)packetizing + (Re)schedule + (Re)routing**,  
  - Destroy patterns (traffic analysis resistance)  
  - Load balancing  
  - Distribute trust
In theory should work, but in practice...

- **Bitwise unlinkability**
  - Crypto to make inputs and outputs bit patterns different

- **(Re)packetizing + (Re)schedule + (Re)routing**
  - Destroy patterns (traffic analysis resistance)
  - Load balancing
  - Distribute trust

**Receivers**

IDs
Timing
Volume
Length
...

**Senders**

Bandwidth
Delay
Churn
Intrinsic network differences
Trust?
### STILL VULNERABLE TO TRAFFIC ANALYSIS

<table>
<thead>
<tr>
<th>Find profiles and communication patterns</th>
<th>Device identification / location</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistent relationships show up</td>
<td>hosts' hardware particular characteristics</td>
</tr>
<tr>
<td>Trace traffic based on patterns</td>
<td>Identify users based on choices</td>
</tr>
<tr>
<td>number of packets, delays, ... differ per flow</td>
<td>not everybody can choose everything</td>
</tr>
<tr>
<td>Identify traffic based on their patterns (e.g., website fingerprinting)</td>
<td>Recover content</td>
</tr>
<tr>
<td>same traffic always looks similar</td>
<td>timing and length of packets</td>
</tr>
<tr>
<td>Users' past history</td>
<td>Trace packets based on routing algorithms</td>
</tr>
<tr>
<td>timing correlated to caches</td>
<td>not all routes are possible</td>
</tr>
</tbody>
</table>

... Many, many, many, many, many, many more....

---

Murdoch, Steven J. "Hot or not: Revealing hidden services by their clock skew." CCS, 2006.
... STILL VULNERABLE TO TRAFFIC ANALYSIS

**Find profiles and communication patterns**
persistent relationships show up

**Trace traffic based on patterns**
number of packets, delays, ... differ per flow

**Identify traffic based on their patterns**
(e.g., website fingerprinting)
same traffic always looks similar

**Users' past history**
timing correlated to caches

**Device identification / location**
hosts' hardware particular characteristics

**Identify users based on choices**
not everybody can choose everything

**Trace packets based on routing algorithms**
not all routes are possible

**Recover content**
timing and length of packets

---

Murdoch, Steven J. "Hot or not: Revealing hidden services by their clock skew." CCS, 2006.
... STILL VULNERABLE TO TRAFFIC ANALYSIS

Find profiles and communication patterns
persistent relationships show up

Device identification / location
hosts' hardware particular characteristics

Trace traffic based on patterns
number of packets, delays, ... differ per flow

Identify users based on choices
not everybody can choose everything

Identify traffic based on their patterns
(e.g., website fingerprinting)
same traffic always looks similar

Recover content
timing and length of packets

Trace packets based on routing algorithms
not all routes are possible

Users' past history
timing correlated to caches

Many, many, many, many, many more....

Murdoch, Steven J. "Hot or not: Revealing hidden services by their clock skew." CCS, 2006.
Where do messages go?

Threshold mix: collects $t$ messages, and outputs them changing their appearance and in a random order.
**Where do messages go?**

- **Threshold mix**: collects $t$ messages, and outputs them changing their appearance and in a random order.
Threshold mix: collects $t$ messages, and outputs them changing their appearance and in a random order.
Threshold mix: collects $t$ messages, and outputs them changing their appearance and in a random order.
Where do messages go?

Threshold mix: collects t messages, and outputs them changing their appearance and in a random order.
Where do messages go?

**Threshold mix**: collects $t$ messages, and outputs them changing their appearance and in a random order.
Threshold mix: collects $t$ messages, and outputs them changing their appearance and in a random order.
WHERE DO MESSAGES GO?
not everything is possible (e.g., max 2 hops)

Threshold mix: collects t messages, and outputs them changing their appearance and in a random order

Danezis, George. "Mix-Networks with Restricted Routes". PETS 2003
**Where do messages go?**
not everything is possible (e.g., max 2 hops)

**Threshold mix**: collects $t$ messages, and outputs them changing their appearance and in a random order.

Danezis, George. "Mix-Networks with Restricted Routes". PETS 2003
**Where do messages go?**
not everything is possible (e.g., max 2 hops)

**Threshold mix:** collects $t$ messages, and outputs them changing their appearance and in a random order.

Danezis, George. "Mix-Networks with Restricted Routes". PETS 2003
Where do messages go?
not everything is possible (e.g., ⬆ does not know M2)

**Threshold mix**: collects $t$ messages, and outputs them changing their appearance and in a random order.

Where do messages go?
not everything is possible (e.g., does not know M2)

Threshold mix: collects t messages, and outputs them changing their appearance and in a random order

Non trivial given observation!!

A “large” trace 😂

Senders

Mixes (Threshold = 3)

Receivers
Redefining the problem

Given what we see (Observation) and the system operation (Constraints)

Probability of mixes “Hidden State”?
(or Probability of each possible path?)
Redefining the problem

Given what we see (Observation) and the system operation (Constraints)
Probability of mixes “Hidden State”?
(or Probability of each possible path?)

\[
Pr[HS|O,C] = \frac{Pr[O|HS,C] \cdot Pr[HS|C]}{\sum_{HS} Pr[HS,O|C]}
\]
Redefining the problem

Given what we see (Observation) and the system operation (Constraints)

Probability of mixes “Hidden State”? 
(or Probability of each possible path?)

\[ Pr[HS|O,C] = \frac{Pr[O|HS,C] \cdot Pr[HS|C]}{\sum_{HS} Pr[HS,O|C]} \]
**Redefining the Problem**

Given what we see (**Observation**) and the system operation (**Constraints**)

Probability of mixes “**Hidden State**”?  
(or Probability of each possible path?)

\[ Pr[HS|O,C] = \frac{Pr[O|HS,C] \cdot Pr[HS|C]}{\sum_{HS} Pr[HS,O|C]} = \frac{Pr[O|HS,C] \cdot K}{Z} = \frac{Pr[Paths|C] \cdot K}{Z} \]
Redefining the problem

Given what we see (Observation) and the system operation (Constraints)
Probability of mixes “Hidden State”? (or Probability of each possible path?)

\[
Pr[HS|O,C] = \frac{Pr[O|HS,C] \cdot Pr[HS|C]}{\sum_{HS} Pr[HS,O|C]} = \frac{Pr[O|HS,C] \cdot K}{Z} = \frac{Pr[Paths|C] \cdot K}{Z}
\]
Redefining the problem

Given what we see (Observation) and the system operation (Constraints)
Probability of mixes “Hidden State”?
(or Probability of each possible path?)

\[
Pr[ \text{HS} \mid O, C] = \frac{\Pr[O \mid \text{HS}, C] \cdot \Pr[\text{HS} \mid C]}{\sum_{\text{HS}} \Pr[\text{HS}, O \mid C]} = \frac{\Pr[O \mid \text{HS}, C] \cdot K}{Z} = \frac{\Pr[\text{Paths} \mid C] \cdot K}{Z}
\]

We usually care about marginal probabilities, not all (Pr[\text{\rightarrow} \mid O, C]) ← SAMPLING!!

Takeaways attacks on routes

➢ Traffic analysis is non trivial when there are constraints

➢ Traffic analysis as inference problem: systematic!
  ➢ Probabilistic model: can incorporate most attacks
    ➢ Can integrate knowledge on path probability computation
    ➢ More constraints → less anonymity but more complexity
    ➢ Combines well with other inferences: e.g., long-term attacks (in a minute)

➢ Sampling methods to extract marginal probabilities
Finding persistent communications

Disclosure Attacks

In reality...

Alice has few friends with whom she communicates often
Alice is not always online (at least not active)

Can Sauron learn Alice's friends?
Finding persistent communications
Disclosure Attacks

In reality...

Alice has few friends with whom she communicates often
Alice is not always online (at least not active)

Can Sauron learn Alice's friends?
Finding persistent communications
Disclosure Attacks

In reality...

Alice has few friends with whom she communicates often
Alice is not always online (at least not active)

Setting

1- Sees Alice sending a single message to the system
2- Anonymity set size = $K$
3- Perfect!
As time goes by and Alice sends more messages...
Let's “do” the math

Approach 1: Statistical Disclosure Attack

- Alice’s friends will be in the sets more often than random receivers. How often?
  Expected number of messages per receiver after $t$ rounds:
  - $\mu_{\text{other}} = \frac{1}{N} \cdot (K-1) \cdot t$
  - $\mu_{\text{Alice}} = \frac{1}{M} \cdot t + \mu_{\text{other}}$

- Just count the number of messages per receiver when Alice is sending!
  - $\mu_{\text{Alice}} > \mu_{\text{other}}$

Mathewson, Nick, and Roger Dingledine. "Practical traffic analysis: Extending and resisting statistical disclosure." PETS, 2004
Let's “do” the math

**Approach 1: Statistical Disclosure Attack**

- Alice’s friends will be in the sets more often than random receivers. How often?
  - Expected number of messages per receiver after $t$ rounds:
    - $\mu_{\text{other}} = \frac{1}{N} \cdot (K-1) \cdot t$
    - $\mu_{\text{Alice}} = \frac{1}{M} \cdot t + \mu_{\text{other}}$
  - Just count the number of messages per receiver when Alice is sending!
    - $\mu_{\text{Alice}} > \mu_{\text{other}}$

<table>
<thead>
<tr>
<th>Round</th>
<th>Receivers</th>
<th>SDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[15, 13, 14, 5, 9]</td>
<td>[13, 15, 18]</td>
</tr>
<tr>
<td>2</td>
<td>[19, 10, 17, 13, 8]</td>
<td>[13, 17, 19]</td>
</tr>
<tr>
<td>3</td>
<td>[0, 7, 0, 13, 5]</td>
<td>[0, 5, 13]</td>
</tr>
<tr>
<td>4</td>
<td>[16, 18, 6, 13, 10]</td>
<td>[5, 10, 13]</td>
</tr>
<tr>
<td>5</td>
<td>[1, 17, 1, 13, 6]</td>
<td>[10, 13, 17]</td>
</tr>
<tr>
<td>6</td>
<td>[18, 15, 17, 13, 17]</td>
<td>[13, 17, 18]</td>
</tr>
<tr>
<td>7</td>
<td>[0, 13, 11, 8, 4]</td>
<td>[0, 13, 17]</td>
</tr>
<tr>
<td>8</td>
<td>[15, 18, 0, 8, 12]</td>
<td>[0, 13, 17]</td>
</tr>
<tr>
<td>9</td>
<td>[15, 18, 15, 19, 14]</td>
<td>[13, 15, 18]</td>
</tr>
<tr>
<td>10</td>
<td>[0, 12, 4, 2, 8]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>11</td>
<td>[9, 13, 14, 19, 15]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>12</td>
<td>[13, 6, 2, 16, 0]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>13</td>
<td>[1, 0, 3, 5, 1]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>14</td>
<td>[17, 10, 14, 11, 19]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>15</td>
<td>[12, 14, 17, 13, 0]</td>
<td>[0, 13, 17]</td>
</tr>
<tr>
<td>16</td>
<td>[18, 19, 19, 8, 11]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>17</td>
<td>[4, 1, 19, 0, 19]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>18</td>
<td>[0, 6, 1, 18, 3]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>19</td>
<td>[5, 1, 14, 0, 5]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>20</td>
<td>[17, 18, 2, 4, 13]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>21</td>
<td>[8, 10, 1, 18, 13]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>22</td>
<td>[14, 4, 13, 12, 4]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>23</td>
<td>[19, 13, 3, 17, 12]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>24</td>
<td>[8, 18, 0, 10, 18]</td>
<td>[0, 13, 18]</td>
</tr>
</tbody>
</table>

Mathewson, Nick, and Roger Dingledine. "Practical traffic analysis: Extending and resisting statistical disclosure." PETS, 2004
Let's “do” the math

Approach 1: Statistical Disclosure Attack

- Alice’s friends will be in the sets more often than random receivers. How often?
  Expected number of messages per receiver after t rounds:
  - $\mu_{\text{other}} = (1 / N) \cdot (K-1) \cdot t$
  - $\mu_{\text{Alice}} = (1 / M) \cdot t + \mu_{\text{other}}$

- Just count the number of messages per receiver when Alice is sending!
  - $\mu_{\text{Alice}} > \mu_{\text{other}}$

<table>
<thead>
<tr>
<th>Round</th>
<th>Receivers</th>
<th>SDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[15, 13, 14, 5, 9]</td>
<td>[13, 15, 18]</td>
</tr>
<tr>
<td>2</td>
<td>[19, 10, 17, 13, 8]</td>
<td>[13, 17, 19]</td>
</tr>
<tr>
<td>3</td>
<td>[0, 7, 0, 13, 5]</td>
<td>[0, 5, 13]</td>
</tr>
<tr>
<td>4</td>
<td>[16, 18, 6, 13, 10]</td>
<td>[10, 13, 17]</td>
</tr>
<tr>
<td>5</td>
<td>[1, 17, 1, 13, 6]</td>
<td>[13, 17, 18]</td>
</tr>
<tr>
<td>6</td>
<td>[18, 15, 17, 13, 17]</td>
<td>[13, 17, 18]</td>
</tr>
<tr>
<td>7</td>
<td>[0, 13, 11, 8, 4]</td>
<td>[0, 13, 17]</td>
</tr>
<tr>
<td>8</td>
<td>[15, 18, 0, 8, 12]</td>
<td>[0, 13, 17]</td>
</tr>
<tr>
<td>9</td>
<td>[15, 18, 15, 19, 14]</td>
<td>[13, 15, 18]</td>
</tr>
<tr>
<td>10</td>
<td>[0, 12, 4, 2, 8]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>11</td>
<td>[9, 13, 14, 19, 15]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>12</td>
<td>[13, 6, 2, 16, 0]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>13</td>
<td>[1, 0, 3, 5, 1]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>14</td>
<td>[17, 10, 14, 11, 19]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>15</td>
<td>[12, 14, 17, 13, 0]</td>
<td>[0, 13, 17]</td>
</tr>
<tr>
<td>16</td>
<td>[18, 19, 19, 8, 11]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>17</td>
<td>[4, 1, 19, 0, 19]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>18</td>
<td>[0, 6, 1, 18, 3]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>19</td>
<td>[5, 1, 14, 0, 5]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>20</td>
<td>[17, 18, 2, 4, 13]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>21</td>
<td>[8, 10, 1, 18, 13]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>22</td>
<td>[14, 4, 13, 12, 4]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>23</td>
<td>[19, 13, 3, 17, 12]</td>
<td>[0, 13, 19]</td>
</tr>
<tr>
<td>24</td>
<td>[8, 18, 0, 10, 18]</td>
<td>[0, 13, 18]</td>
</tr>
</tbody>
</table>

Mathewson, Nick, and Roger Dingledine. "Practical traffic analysis: Extending and resisting statistical disclosure." PETS, 2004
**Approach 1: Statistical Disclosure Attack**

- Alice’s friends will be in the sets more often than random receivers. How often?
  
  Expected number of messages per receiver after $t$ rounds:
  
  - $\mu_{\text{other}} = (1 / N) \cdot (K-1) \cdot t$
  - $\mu_{\text{Alice}} = (1 / M) \cdot t + \mu_{\text{other}}$

- Just count the number of messages per receiver when Alice is sending!
  - $\mu_{\text{Alice}} > \mu_{\text{other}}$

<table>
<thead>
<tr>
<th>Round</th>
<th>Receivers</th>
<th>SDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[15, 13, 14, 5, 9]</td>
<td>[13, 14, 15]</td>
</tr>
<tr>
<td>2</td>
<td>[19, 10, 17, 13, 8]</td>
<td>[0, 5, 13]</td>
</tr>
<tr>
<td>3</td>
<td>[0, 7, 0, 13, 5]</td>
<td>[0, 13, 17]</td>
</tr>
<tr>
<td>4</td>
<td>[16, 18, 6, 13, 10]</td>
<td>[5, 10, 13]</td>
</tr>
<tr>
<td>5</td>
<td>[1, 17, 1, 13, 6]</td>
<td>[10, 13, 17]</td>
</tr>
<tr>
<td>6</td>
<td>[18, 15, 17, 13, 17]</td>
<td>[13, 17, 18]</td>
</tr>
<tr>
<td>7</td>
<td>[0, 13, 11, 8, 4]</td>
<td>[0, 13, 17]</td>
</tr>
<tr>
<td>8</td>
<td>[15, 18, 0, 8, 12]</td>
<td>[0, 13, 17]</td>
</tr>
<tr>
<td>9</td>
<td>[15, 18, 15, 19, 14]</td>
<td>[13, 15, 18]</td>
</tr>
<tr>
<td>10</td>
<td>[0, 12, 4, 2, 8]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>11</td>
<td>[9, 13, 14, 19, 15]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>12</td>
<td>[13, 6, 2, 16, 0]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>13</td>
<td>[1, 0, 3, 5, 1]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>14</td>
<td>[17, 10, 14, 11, 19]</td>
<td>[0, 13, 15]</td>
</tr>
<tr>
<td>15</td>
<td>[12, 14, 17, 13, 0]</td>
<td>[0, 13, 17]</td>
</tr>
</tbody>
</table>

16 | [18, 19, 19, 8, 11] | [0, 13, 19] |

17 | [4, 1, 19, 0, 19] | [0, 13, 19] |
18 | [0, 6, 1, 18, 3] | [0, 13, 19] |
19 | [5, 1, 14, 0, 5] | [0, 13, 19] |
20 | [17, 18, 2, 4, 13] | [0, 13, 19] |
21 | [8, 10, 1, 18, 13] | [0, 13, 19] |
22 | [14, 4, 13, 12, 4] | [0, 13, 19] |
23 | [19, 13, 3, 17, 12] | [0, 13, 19] |
24 | [8, 18, 0, 10, 18] | [0, 13, 18] |

Mathewson, Nick, and Roger Dingledine. "Practical traffic analysis: Extending and resisting statistical disclosure." PETS, 2004
Let's “do” the math

Approach 2: Least Squares Disclosure Attack

- Maximum likelihood approach: solve a Least Squares minimizing mean squared error between real and estimated profiles

\( P_{\text{a} \rightarrow \text{b}} \) = probability that \( \text{a} \) sends a message to \( \text{b} \)

\( x^r = \text{vector of n# of messages sent round } r \ (x^r_{1} = 1) \)

\( y^r = \text{vector of n# of messages received round } r \ (y^r_{2} = 2) \)

\( H = [x^1, x^2, x^3, ..., ] \)


Perez-Gonzalez, Fernando, Carmela Troncoso, and Simon Oya. "A least squares approach to the static traffic analysis of high-latency anonymous communication systems." TIFS 2014
**Approach 2: Least Squares Disclosure Attack**

- Maximum likelihood approach: solve a Least Squares minimizing mean squared error between real and estimated profiles

\[
\hat{p} = \arg \min_p \| y - Hp \|
\]

\[
p_{i,j} \leq 1
\]

\[
\sum_i p_{i,j} = 1
\]

\[
\hat{p} = (H^T H)^{-1} H^T y
\]
**Let’s “do” the math**

**Approach 2: Least Squares Disclosure Attack**

- Maximum likelihood approach: solve a Least Squares minimizing mean squared error between real and estimated profiles

\[
\hat{p} = \arg \min_p \| y - Hp \| \\
\sum_i p_{i,j} \leq 1 \\
\sum_i p_{i,j} = 1
\]

\[
\hat{p} = (H^TH)^{-1}H^Ty
\]

- Analytical expressions that describe the evolution of the profiling error

\[
MSE = \| p - \hat{p} \|^2 = \frac{1}{t} \left( N - 1 + \frac{1}{k} \right) \left( N - \sum f_i^2 / f_i^2N \right)
\]


Perez-Gonzalez, Fernando, Carmela Troncoso, and Simon Oya. "A least squares approach to the static traffic analysis of high-latency anonymous communication systems." TIFS 2014
Let's "do" the math

Approach 2: Least Squares Disclosure Attack

- Maximum likelihood approach: solve a Least Squares minimizing mean squared error between real and estimated profiles

$$\hat{p} = \arg \min_p \| y - Hp \|$$

$$\sum_i p_{i,j} = 1, \quad p_{i,j} \leq 1$$

$$\hat{p} = (H^T H)^{-1} H^T y$$

- Analytical expressions that describe the evolution of the profiling error

$$MSE = \| p - \hat{p} \|^2 = \frac{1}{t} \left( N - 1 + \frac{1}{k} \right) \left( N - \sum_i \frac{f_i^2}{f^2 N} \right)$$


Pérez-Gonzalez, Fernando, Carmela Troncoso, and Simon Oya. "A least squares approach to the static traffic analysis of high-latency anonymous communication systems." TIFS 2014
Let's “do” the math

Approach 3: Disclosure attack as an inference problem

➢ What we are looking for: Pr[ρAlice, ρOthers, M | O, M, Ψ]
➢ More concretely, marginal probabilities & distributions
  ➢ Pr[Alice→Bob] – Are Alice and Bob friends?
  ➢ Mx – Who is talking to whom at round x?
  ➢ Solve through sampling!

Profiles: Pr[ρAlice, ρOthers | M, O, M, Ψ, K]
  (Direct sampling by sampling Dirichlet dist.)
Mappings: Pr[M | ρAlice, ρOthers, O, M, Ψ, K]
  (Direct sampling of the matching link by link)

**Persistent patterns Takeaways**

- Near-perfect anonymity is not perfect enough!
  - High level patterns cannot be hidden for ever
  - Unobservability / maximal anonymity is needed

- Three approaches to the problem (actually I skipped the seminal work)

<table>
<thead>
<tr>
<th>SDA</th>
<th>LSDA</th>
<th>Bayesian Inference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Flexible</td>
<td>Flexible</td>
</tr>
<tr>
<td>Fast!</td>
<td>Fast!</td>
<td>“expensive”</td>
</tr>
<tr>
<td>Best result not guaranteed</td>
<td>Optimal result (MSE)</td>
<td>Distribution</td>
</tr>
<tr>
<td>Only that one</td>
<td>But only that one</td>
<td>Many quantities</td>
</tr>
<tr>
<td></td>
<td>Error prediction</td>
<td>Confidence intervals</td>
</tr>
<tr>
<td></td>
<td>Design tool!</td>
<td>Not best solution</td>
</tr>
</tbody>
</table>

---

ARE WE DOOMED? - CHALLENGES

➢ **Countermeasures** – Systematic design?

➢ Delay: plain batching does not seem the best
  ➢ Pool mixes
  ➢ Attacks can be adapted to account for more complex delay patterns

➢ Dummy traffic: include “fake packets” to disorient the adversary
  ➢ How do we make them indistinguishable?
  ➢ Who decides about them?

➢ Weaker protections suffice for other adversary models
  ➢ e.g. Tor partial adversary

➢ **Privacy metric**, what is the goal?

➢ **Modeling adversarial knowledge**
Summary

➢ The Lord of The Rings is a great timeless book

➢ Crypto protects data, but does not always protect privacy

➢ Traffic analysis is the art of exploiting meta-data to extract information

➢ Traffic analysis can exploit a gazillion features: protecting efficiently is difficult!
   ➢ Recovering persistent patterns, tracing messages in restricted routes

➢ Design privacy-preserving systems is far from trivial
THANKS!

Any questions?

More about privacy:
https://www.petsymposium.org/
http://www.degruyter.com/view/j/popets

17th Privacy Enhancing Technologies Symposium
July 18–21, 2017
Minneapolis, MN, USA

2018 Barcelona! Deadlines: 31 Aug, 30 Nov, 28 Feb

carmela.troncoso@imdea.org
https://software.imdea.org/~carmela.troncoso/
(these slides will be there soon)