Privacy at the communication layer

Telex : Anticensorship in the Network Infrastructure
Wustrow, Wolchock, Goldberg and Halderman 2011

CS-721

Carmela Troncoso
http://carmelatroncoso.com/

What we have seen so far

Previous papers where about anonymous communication:

Adversary's goal: find who is speaking to whom

Where are we

Previous papers where about anonymous communication:

Adversary's goal: find who is speaking to whom

routing strategies

- source-based
  - restricted (?)
  - unrestricted (?)
- per-hop (?)
- broadcast (?)

node selection

- central directory (?)
- P2P discovery (?)

Protecting content

- Layered encryption
  - circuit-based (?)
  - message based (?)

Where are we

Previous papers where about anonymous communication:

Adversary's goal: find who is speaking to whom

routing strategies

- source-based
  - restricted (Tor)
  - unrestricted (salsa)
- per-hop (Crowds)
- broadcast (DC-Nets)

node selection

- central directory (Tor, Crowds)
- P2P discovery (Salsa, Tarzan)

Protecting content

- Layered encryption
  - circuit-based (Tor)
  - message based (mixes)

+ ATTACKS!!

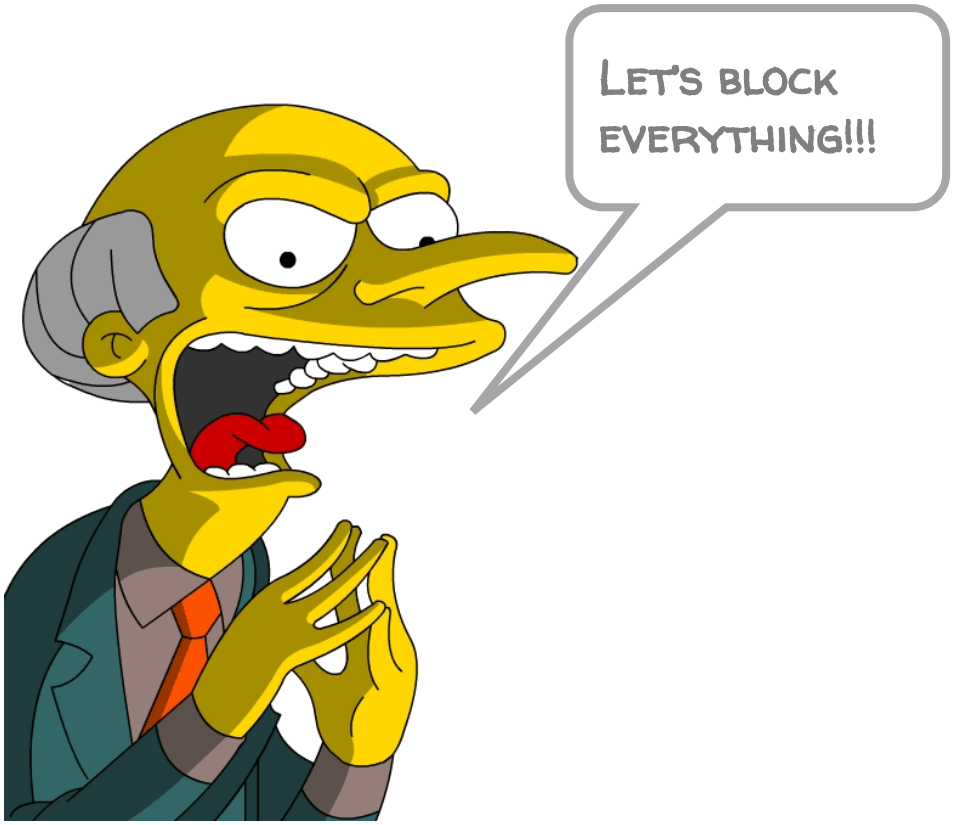
Beyond anonymity: Censorship prevention

Adversary's goal: prevent communication between two parties

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Beyond anonymity: Censorship prevention

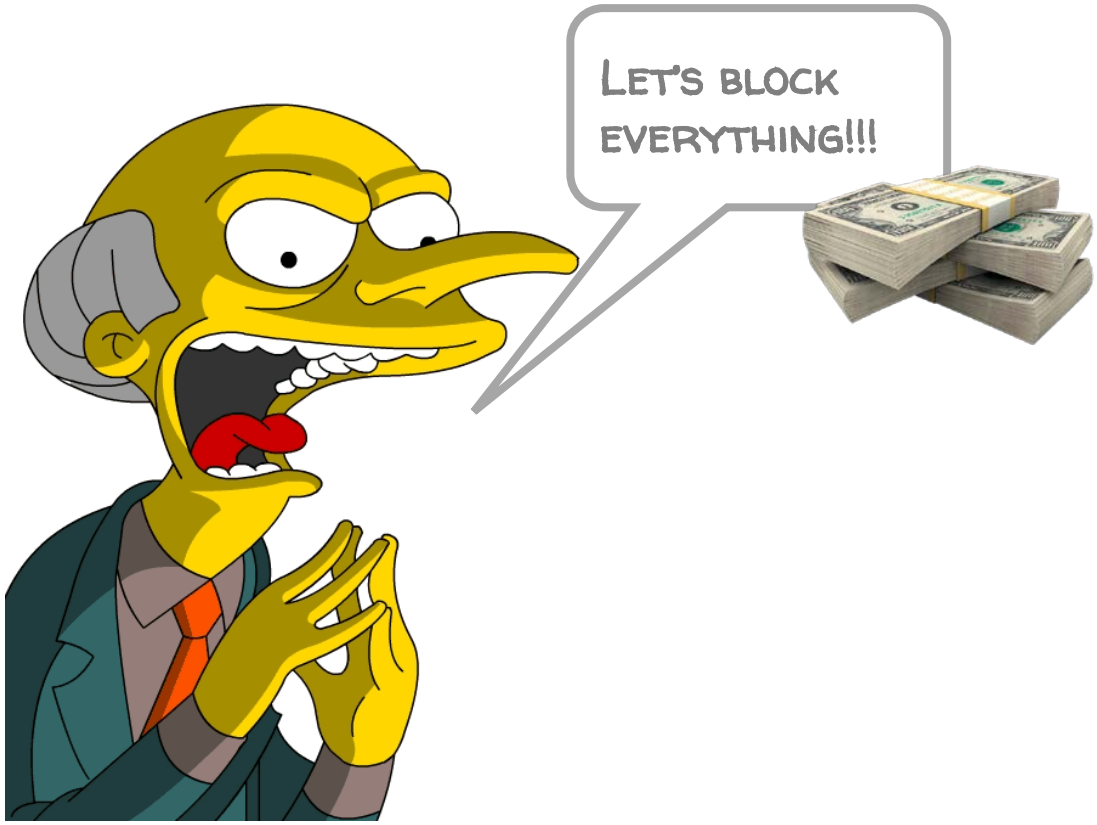
Adversary's goal: prevent communication between two parties



Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Beyond anonymity: Censorship prevention

Adversary's goal: prevent communication between two parties



Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Beyond anonymity: Censorship prevention

Adversary's goal: prevent communication between two parties

2-step process:


finding the flow: fingerprinting


prevent communication: direct censor

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

🔍 FINDING THE FLOW: FINGERPRINTING

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

FINDING THE FLOW: FINGERPRINTING

DESTINATION:

IP addresses, hosts, ports,...

CONTENT:

protocol-strings, keywords, domains, http hosts,...

FLOW PROPERTIES:

length, inter-arrival times, bursts,

PROTOCOL SEMANTICS:

protocol behavior (mostly active attacks)

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Prevent communication: direct censor

Block destination (Great Firewall China... rather soft)

Degrade performance:
disrupt brittle traffic, complicate access

Corrupt routing:
BGP hijacking (disconnect part of the network)
DNS manipulation (redirect to censor or blackhole)

Corrupt flow content:
HTTP 404 not found

Corrupt Protocol semantics:
Forged RST packets

User-side censorship: local software
Publisher-side censorship: automatic/manual deletion

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Censorship resistance systems

1. Communication establishment:
   Obtain credentials / server addresses
   Goal: easy for users but difficult to censor

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Censorship resistance systems

1. Communication establishment:
   Obtain credentials / server addresses
   Goal: easy for users but difficult to censor

- High churn: change continuously
- Rate limit: based on time (Tor bridges), based on "space" (partitioning), PoW (puzzle)
- Trust-based: social graph, previous behavior, token,...

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Censorship resistance systems

1. Communication establishment:
   Obtain credentials / server addresses
   Goal: easy for users but difficult to censor

- High churn: change continuously
- Rate limit: based on time (Tor bridges), based on "space" (partitioning), PoW (puzzle)
- Trust-based: social graph, previous behavior, token,...

Active probing resistance
- Obfuscate aliveness: only respond if correct sequence
- Obfuscate service: only respond "censorsh-language" if correct sequence

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Censorship resistance systems

2. Conversation:
   Actual communication
   Goal: Avoid prevention / modification

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Censorship resistance systems

2. Conversation:

   Actual communication

   Goal: Avoid prevention / modification

- Mimicry: look like whitelisted (or not blacklisted) ← increase cost of blocking
- Tunneling: tunnel traffic through unblocked application
- Covert channel: hide censored traffic on images, voice, emails,...

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Censorship resistance systems

2. Conversation:

   Actual communication

   Goal: Avoid prevention / modification

- Mimicry: look like whitelisted (or not blacklisted) ← increase cost of blocking
- Tunneling: tunnel traffic through unblocked application
- Covert channel: hide censored traffic on images, voice, emails,...

Destination obfuscation

- Proxy-based: Tor
- Decoy routing: Telex, Cirripede,...

Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg.
SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies (PoPETS 2016)

Routing attacks

1. Find all decoy routers
   - Public list (Telex)
   - Scan all ASes (Cirripede)

Max Schuchard, John Geddes, Christopher Thompson, and Nicholas Hopper.
Routing Around Decoys (CCS 2012)

Routing attacks

1. Find all decoy routers
   - Public list (Telex)
   - Scan all ASes (Cirripede)

} Tainted vs. Clean ASes

Max Schuchard, John Geddes, Christopher Thompson, and Nicholas Hopper.
Routing Around Decoys (CCS 2012)

Routing attacks

1. Find all decoy routers
   - Public list (Telex)
   - Scan all ASes (Cirripede)

   } Tainted vs. Clean ASes

2. Route over honest Ases

Max Schuchard, John Geddes, Christopher Thompson, and Nicholas Hopper.
Routing Around Decoys (CCS 2012)

Routing attacks

1. Find all decoy routers
   - Public list (Telex)
   - Scan all ASes (Cirripede)

   } Tainted vs. Clean ASes

2. Route over honest Ases

Find / Confirm decoys
- Reply TCP: through clean and tainted
- Reroute through the decoy: force dropping
- Flip tainted/non-tainted path: observe reaction

Max Schuchard, John Geddes, Christopher Thompson, and Nicholas Hopper.
Routing Around Decoys (CCS 2012)

Routing attacks

1. Find all decoy routers
   - Public list (Telex)
   - Scan all ASes (Cirripede)

   } Tainted vs. Clean ASes

2. Route over honest Ases

Find / Confirm decoys
- Reply TCP: through clean and tainted
- Reroute through the decoy: force dropping
- Flip tainted/non-tainted path: observe reaction

Timing also works! Time to NotBlocked != real timing.

Max Schuchard, John Geddes, Christopher Thompson, and Nicholas Hopper.
Routing Around Decoys (CCS 2012)

Not everything is lost

1. Find all decoy routers
   - Public list (Telex)
   - Scan all ASes (Cirripede)

   } Tainted vs. Clean ASes

2. Route over honest Ases

CRAZY EXPENSIVE!!

Find / Confirm decoys
- Reply TCP: through clean and tainted
- Reroute through the decoy: force dropping
- Flip tainted/non-tainted path: observe reaction

Timing also works! Time to NotBlocked != real timing.

Amir Houmansadr, Edmund L. Wong, and Vitaly Shmatikov.
No Direction Home: The True Cost of Routing Around Decoys (NDSS 2014)

Takeaways

- Anonymous communication techniques are also useful for censorship
- Censorship Resistance requires solving 2 aspects:
  - Establishing the connection
  - Exchange data
- We have seen DECOY ROUTING that does both:
  - Establish connection to a decoy (assumes decoy is known)
  - Have a conversation through the decoy
  - Attackable, but expensive

Mimicry, does it work?

Mimicry, does it work?

Next week

The Parrot is Dead: Observing Unobservable Network Communications
Amir Houmansadr, Chad Brubaker, and Vitaly Shmatikov