Privacy at the communication layer

The Parrot is Dead: Observing Unobservable Network Communications
Houmansadr, Brubaker, and Shmatikov 2013

CS-721

Carmela Troncoso
http://carmelatroncoso.com/


gifbin.com

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

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)

Finding the flow: fingerprinting

Destination:

IP addresses, hosts, ports,... Tor (or other anon comm)

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)

Finding the flow: fingerprinting

Destination:

IP addresses, hosts, ports,... Tor (or other anon comm)

Content:

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

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)

Finding the flow: fingerprinting

Destination:

IP addresses, hosts, ports,... Tor (or other anon comm)

Content:

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

Flow properties:

length, inter-arrival times, bursts, Obfuscation, mimic

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)

Finding the flow: fingerprinting

Destination:
IP addresses, hosts, ports,... Tor (or other anon comm)

Content:
protocol-strings, keywords, domains, http hosts,... Encryption

Flow properties:
length, inter-arrival times, bursts, Obfuscation, mimic

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)

Cover your ACKs

Exploit Mismatches cover vs. anti- censorship protocol

Even if one just substitutes content...

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Cover your ACKs

Exploit Mismatches cover vs. anti- censorship protocol

Even if one just substitutes content...

Architectural mismatches: P2P as cover for client-server

Channel mismatches: different reliability needs (UDP vs. TCP)

Content mismatches: VoIP vs. modem

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Cover your ACKs

Exploit Mismatches cover vs. anti- censorship protocol

Even if one just substitutes content...

Architectural mismatches: P2P as cover for client-server

Channel mismatches: different reliability needs (UDP vs. TCP)

Content mismatches: VoIP vs. modem

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Cover your acks: Architecture mismatch

SkypeMorph: *"The Skype system is peer to peer with sporadic short lived connections made between unique clients, while the client-proxy model in Tor sees long lived connections between many clients and a single proxy."*

FreeWave: *uses Skype supernodes as proxys. Skype does NOT do that (only as fallback)."*

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Cover your acks: Error Tolerance

FreeWave: modem to "create" VoIP.

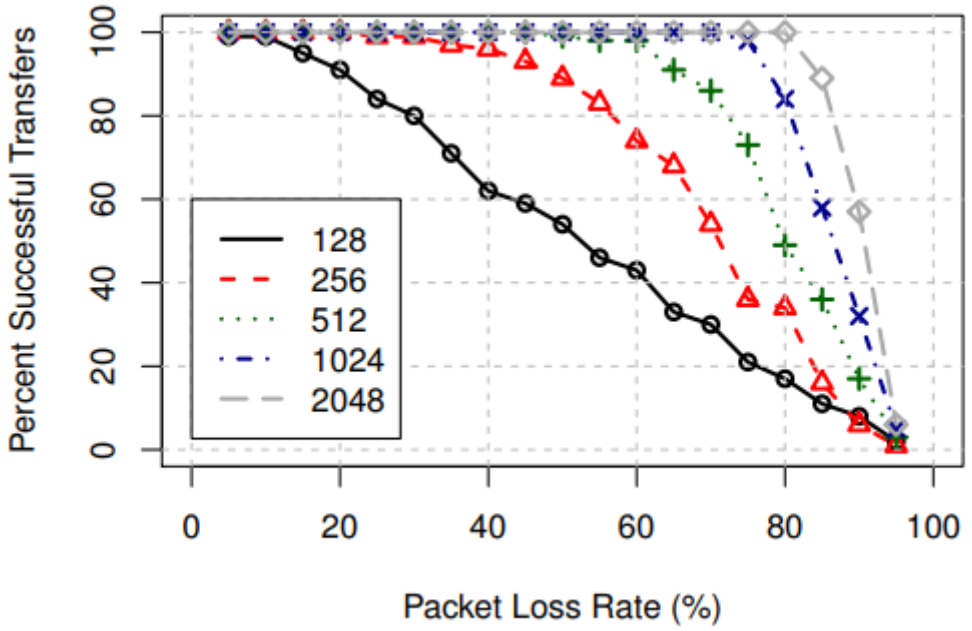
Transmits a preamble to find the message –> desynchronizing = censoring

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Cover your ACKs: Error Tolerance

FreeWave: modem to "create" VoIP.

Transmits a preamble to find the message -> desynchronizing = censoring



John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Cover your ACKs: Error Tolerance

SkypeMorph: ACKs at application level to compensate UDP.
drop ACKs = low throughput = censoring

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Cover your ACKs: Error Tolerance

SkypeMorph: ACKs at application level to compensate UDP.

drop ACKs = low throughput = censoring

Hurdle: identify Acks

Probabilistic analysis

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

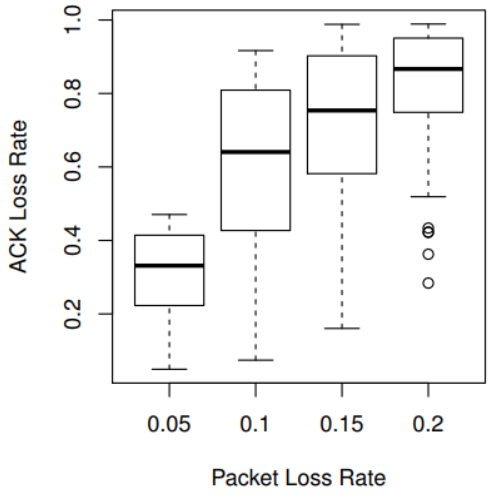
Cover your acks: Error Tolerance

SkypeMorph: ACKs at application level to compensate UDP.

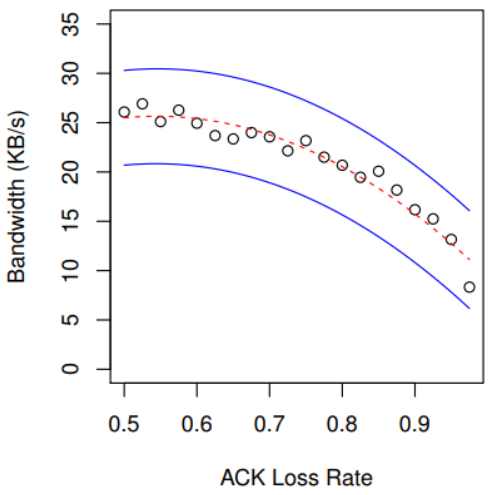
drop ACKs = low throughput = censoring

Hurdle: identify Acks

Probabilistic analysis



(a) Packet vs ACK Loss Rate



(b) ACK Loss Rate vs Bandwidth

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Cover your acks: Error Tolerance

Channel mismatches: different reliability needs

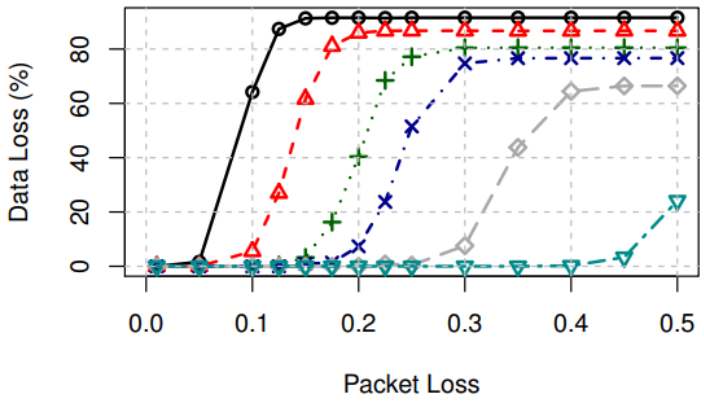
CensorSpoof: Reed-Solomon encoding to account for packet loss.
drop packets = loss data = censoring

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

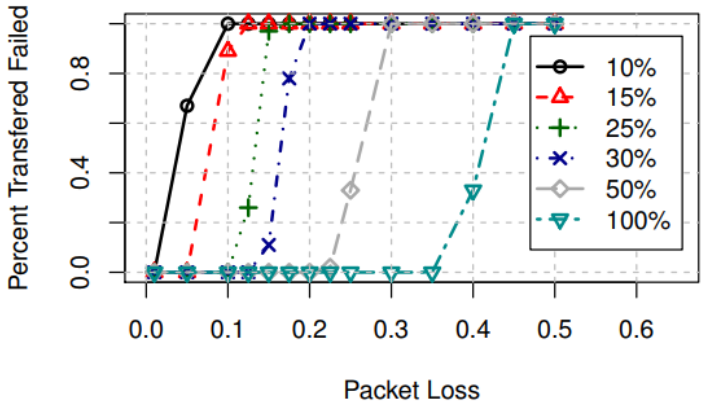
Cover your ACKs: Error Tolerance

Channel mismatches: different reliability needs

CensorSpoof: Reed-Solomon encoding to account for packet loss.
drop packets = loss data = censoring



(a) Percent Data Loss



(b) Percent Transfered Failed

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Cover your acks: Content

FreeWave: modem over VoIP

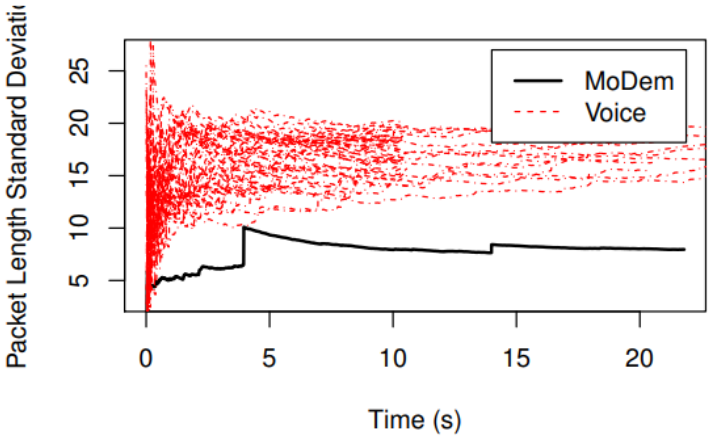
!= characteristics = flow identification

John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

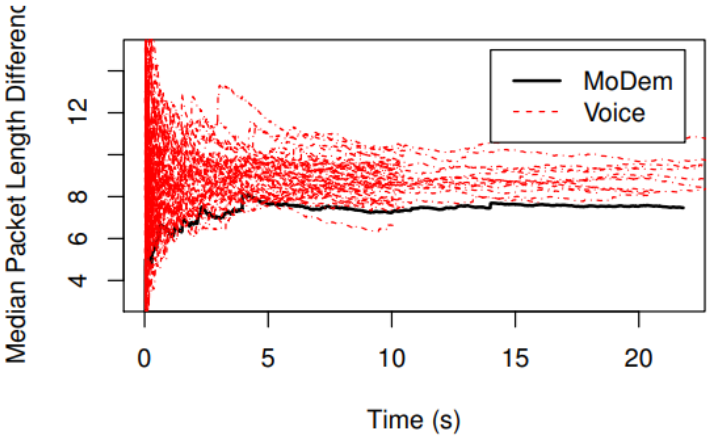
Cover your ACKs: Content

FreeWave: modem over VoIP

!= characteristics = flow identification



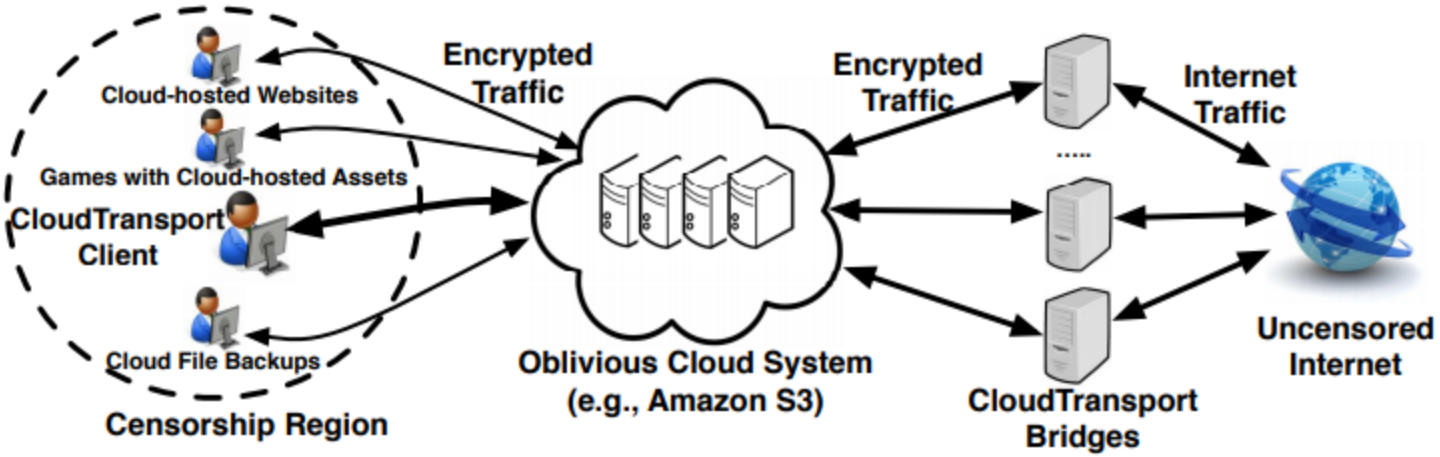
(a) Packet length standard deviation over time



(b) Average Packet Differences Over Time

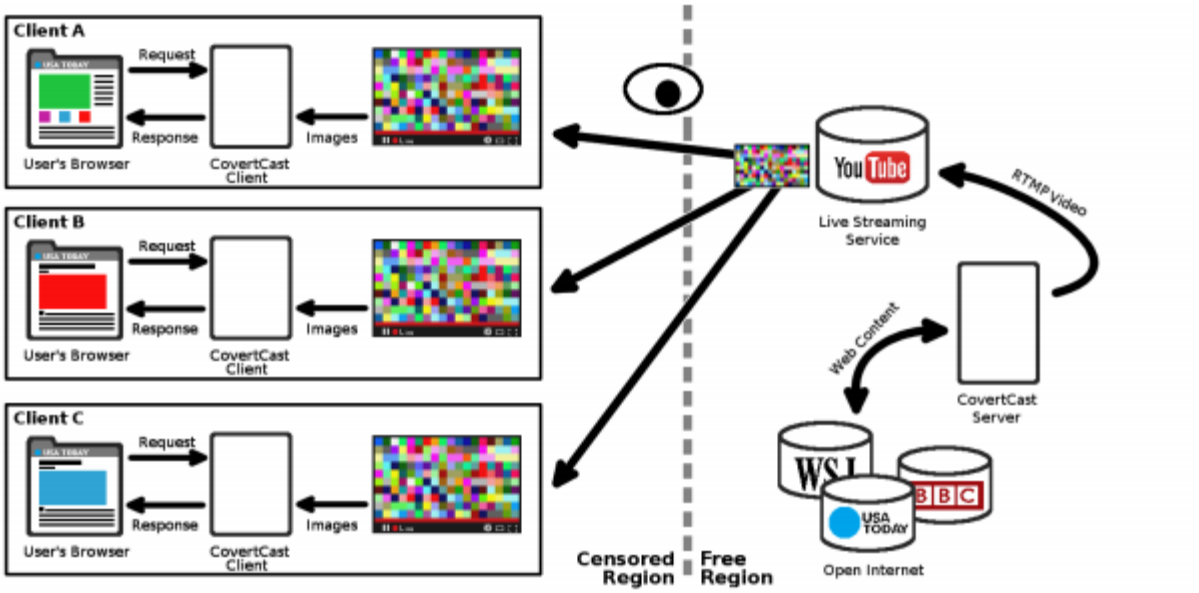
John Geddes, Maxfield Schuchard, and Nicholas Hopper.
Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention (CCS 2013)

Following recommendation Hide-not-mimic CloudTransport



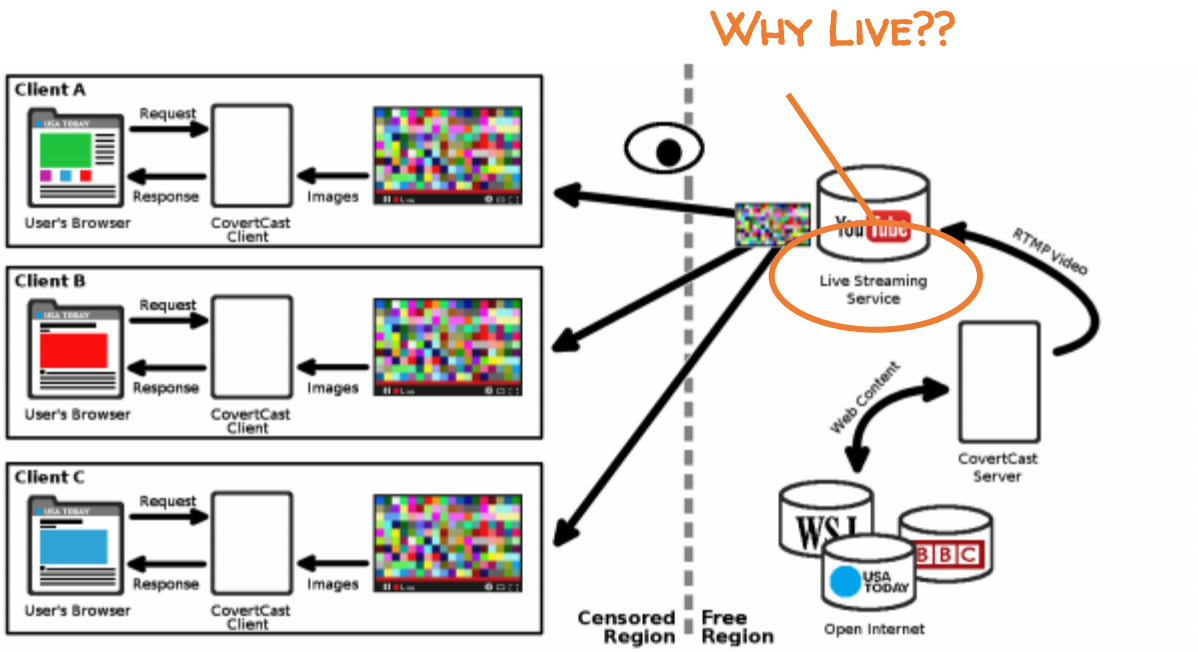
Chad Brubaker, Amir Houmansadr, and Vitaly Shmatikov
CloudTransport: Using Cloud Storage for Censorship-Resistant Networking (PETS 2014)

Following recommendation Hide-not-mimic CovertCast



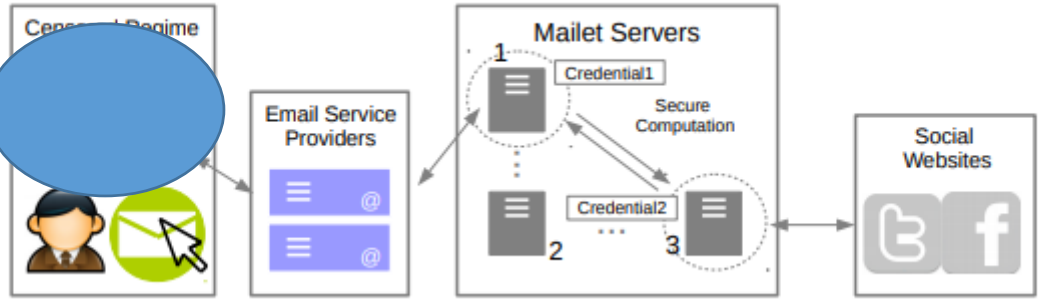
Richard McPherson, Amir Houmansadr, and Vitaly Shmatikov
CovertCast: Using Live Streaming to Evade Internet Censorship (PoPETS 2016)

Following recommendation Hide-not-mimic CovertCast



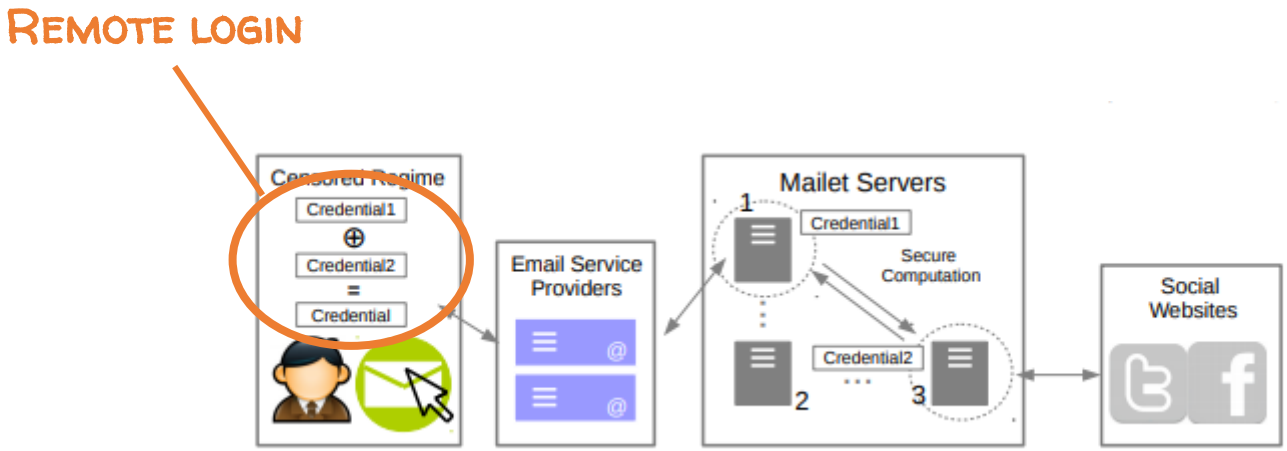
Richard McPherson, Amir Houmansadr, and Vitaly Shmatikov
CovertCast: Using Live Streaming to Evade Internet Censorship (PoPETS 2016)

Following recommendation Hide-not-mimic Mailet



Shuai Li* and Nicholas Hopper
Instant Social Networking under Censorship (PoPETS 2016)

Following recommendation Hide-not-mimic Mailet



Shuai Li* and Nicholas Hopper
Instant Social Networking under Censorship (PoPETS 2016)

Takeaways

- Mimic is difficult (to the point of impossible)
- If you cannot mimic, hide on it
  - Still some problems...
- Several systems that attempt to do so
  - Extremely complex backends
  - Targets of an attack?

FINDING THE FLOW: FINGERPRINTING

FLOW PROPERTIES:

length, inter-arrival times, bursts,

OBFUSCATION, MIMIC

FINDING THE FLOW: FINGERPRINTING

FLOW PROPERTIES:

length, inter-arrival times, bursts,

OBFUSCATION, MIMIC

OBFUSCATION, DOES IT WORK?

Finding the flow: fingerprinting

Flow properties:
length, inter-arrival times, bursts,

Obfuscation, mimic

Obfuscation, does it work?

Next week

Seeing Through Network-Protocol Obfuscation
Wang, Dyer, Akella, Ristenpart, and Shrimpton.