

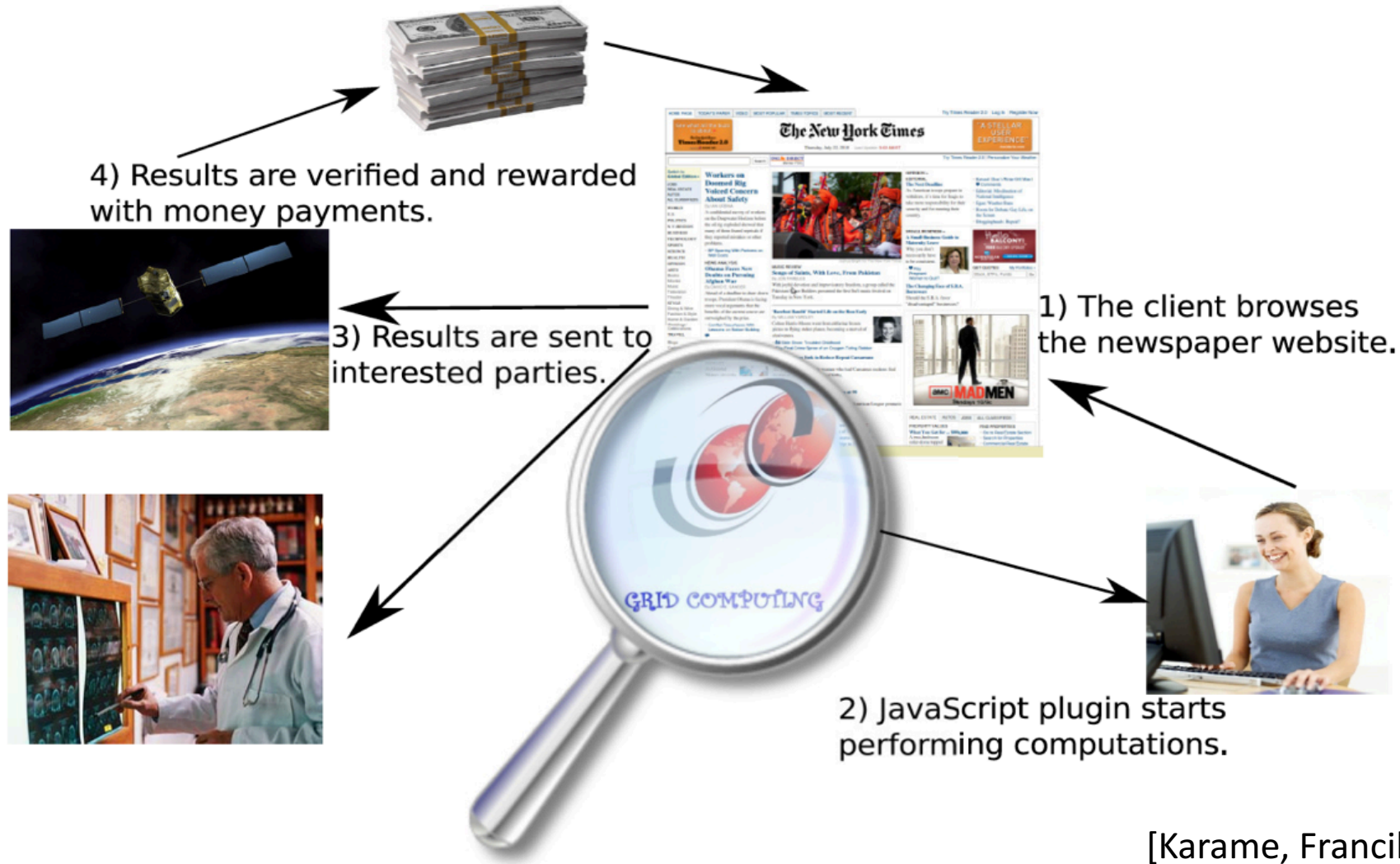
# CoverUp: Privacy Through “Forced” Participation in Anonymous Communication Networks

Srdjan Čapkun

[joint work with David Sommer, Aritra Dhar, Luka Malisa  
Esfandiar Mohammadi, Daniel Ronzani]

Practically *anyone* can run code on your machine, open connections, download / upload data ...

# Micropayments



# Motivation: Participation

- Strong anonymity
  - Hide which users are connected to whom
  - Limits surveillance and censorship
- Two problems:
  - **Low number of connected users reduces privacy guarantees**
  - **Bootstrapping: low participation -> reduces privacy -> low participation ...**
- Participation alone raises suspicion
  - Establishment of communication => Intention of communication



# Motivation: Deniability

- Deniability
  - Accessing classified or leaked documents
  - Information related to specific medical conditions
  - ...
- Why is it important?
  - Freedom of speech
  - Whistleblowers
  - Open journalism
  - Democracy in general 😊



# User Profiling ...

REUTERS


White House says Trump to sign broadband privacy repeal

TECHNOLOGY NEWS | Thu Mar 30, 2017 | 7:38am EDT

## White House says Trump to sign broadband privacy repeal

LIVE COVERAGE  
THE FIRST **100** DAYS

REUTERS TV  
Congress turns back the clock on internet privacy

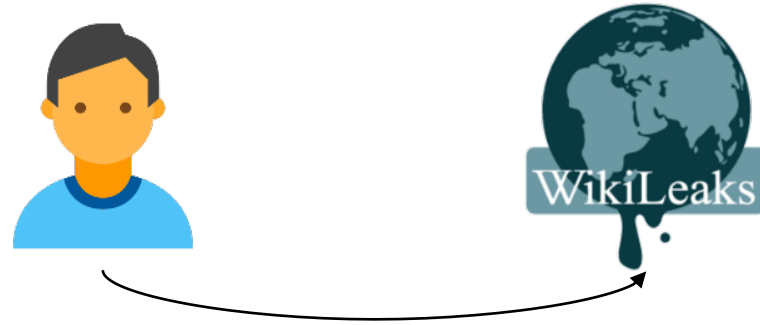


CONGRESS TURNS BACK THE CLOCK ON INTERNET PRIVACY

0:12 / 13:18

# Were you Ever Afraid to ...

- ... download something that is readily available?



- Maybe someone is watching?

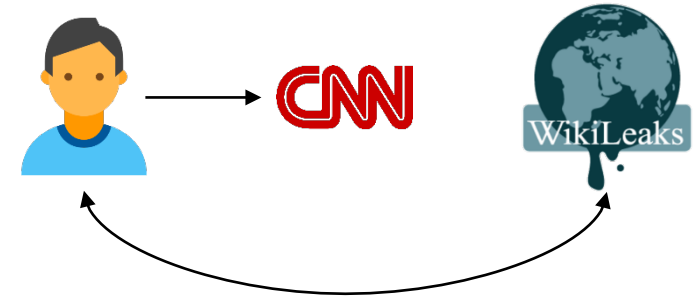
# Forced Participation?

- “Forced” participation?

- Involving unaware/involuntary users
- Enlarged anonymity set:

**Hard to determine if one is forced or willing participant**

- E.g., all the users of CNN → potential users of WikiLeaks



Some past works: ConScript, AdLeaks (focus on upload of content)

Our focus:

**Anonymous feed and chat**

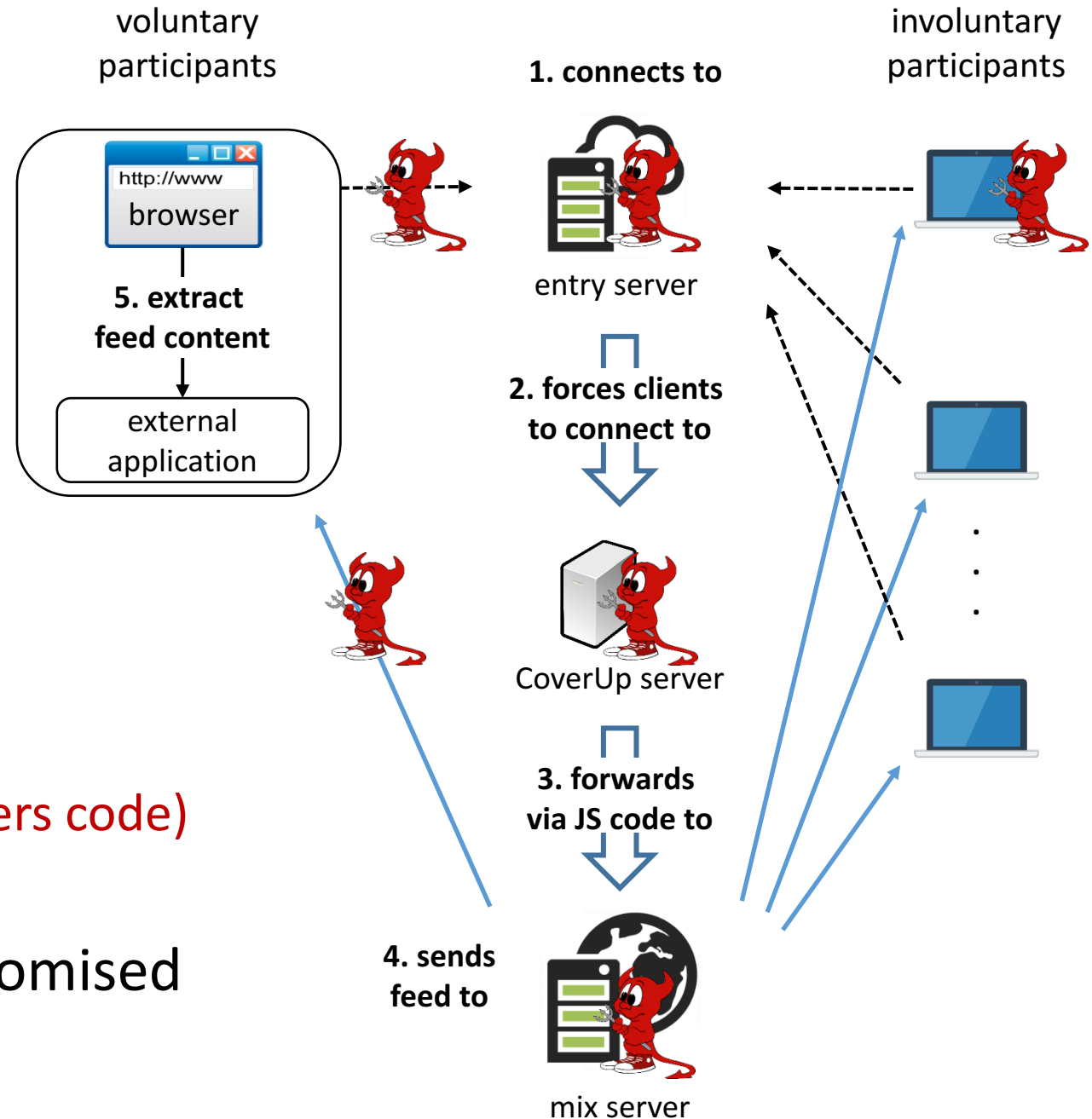


# Contributions

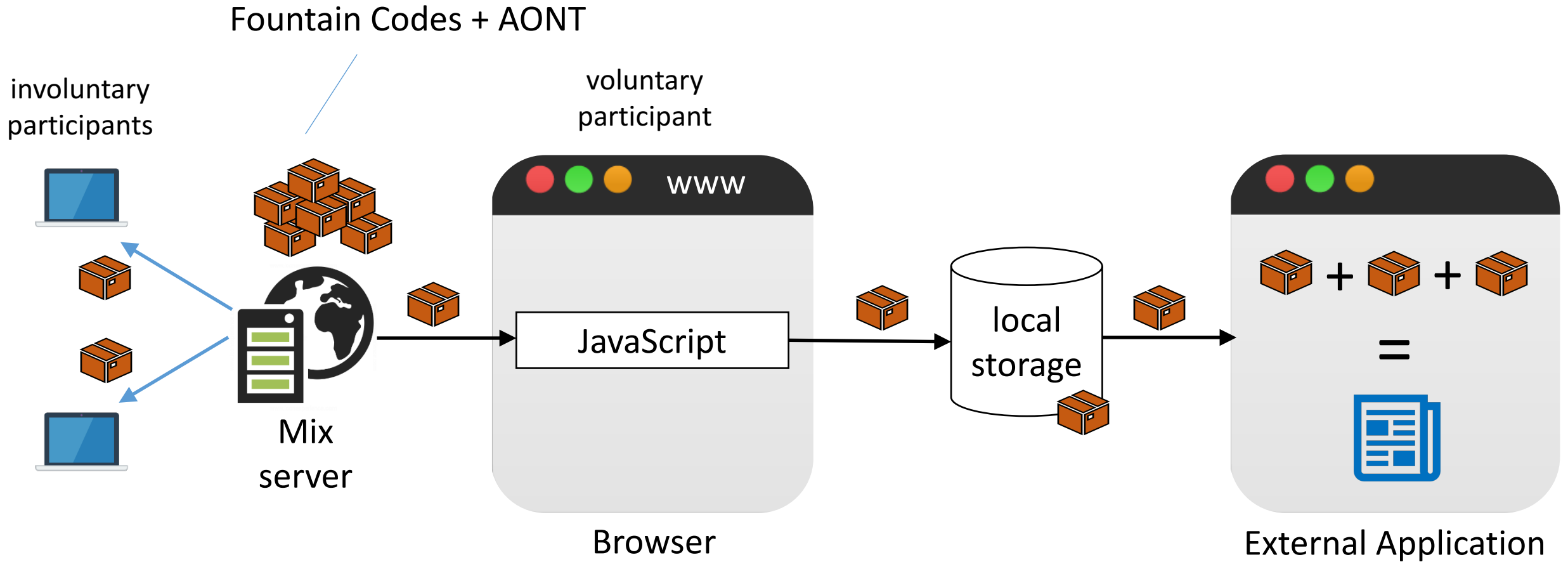
- Uses “forced participation”
  - Unidirectional channel to deliver broadcast (Feed)
  - Bidirectional channel to implement secure chat protocol
- Previous Work
  - ConScript, AdLeaks, New covert channels in HTTP
- Working Prototype
- Detailed attacker model
  - Analysis of the attacker’s capabilities
  - Analysis of privacy leakage and mitigation techniques
- Quantitative privacy metric

# CoverUp: Feed

- Attacker controls:
  - Network (monitor/drop/fake)
  - Entry (CNN) and CoverUp server (delivers code)
  - Mix server (delivers feed)
- Voluntary user's machine not compromised

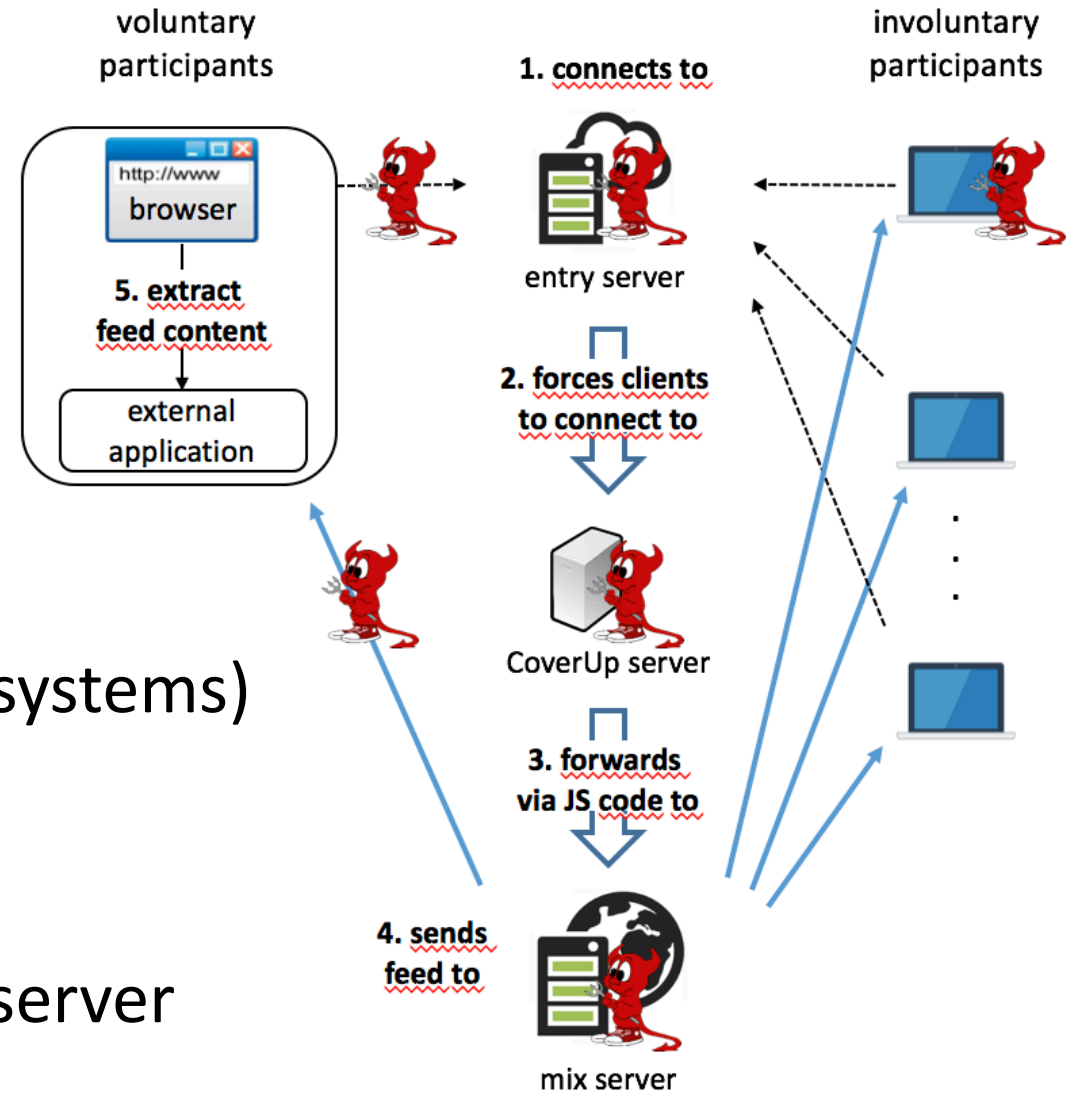


# CoverUp: Feed



# CoverUp: Feed

- Voluntary and Involuntary users are **indistinguishable!**
- Even to a very strong adversary (full control of network and CoverUp systems)
- Anonymity set size = visitors of entry server



# CoverUp: Feed

- Major news sites
- University sites
- ...



# CoverUp: Limiting Profiling by ISPs

## Internet Noise

On March 29th [congress passed a law](#) that makes it legal for your Internet Service Providers (ISP) to track and sell your personal activity online. This means that things you search for, buy, read, and say can be collected by corporations and used against you.

Click this button, and your browser will start passively loading random sites in browser tabs. Leave it running to fill their databases with noise. Just quit your browser when you're done.

Make some noise

STOP THE NOISE!

*This is an early stage and still evolving project. Please offer feedback [via twitter](#) and if something goes wrong let me know.*

---

**IMPORTANT: this button will make some noise as a form of digital protest. IT DOES NOT MAKE YOU SAFE.**

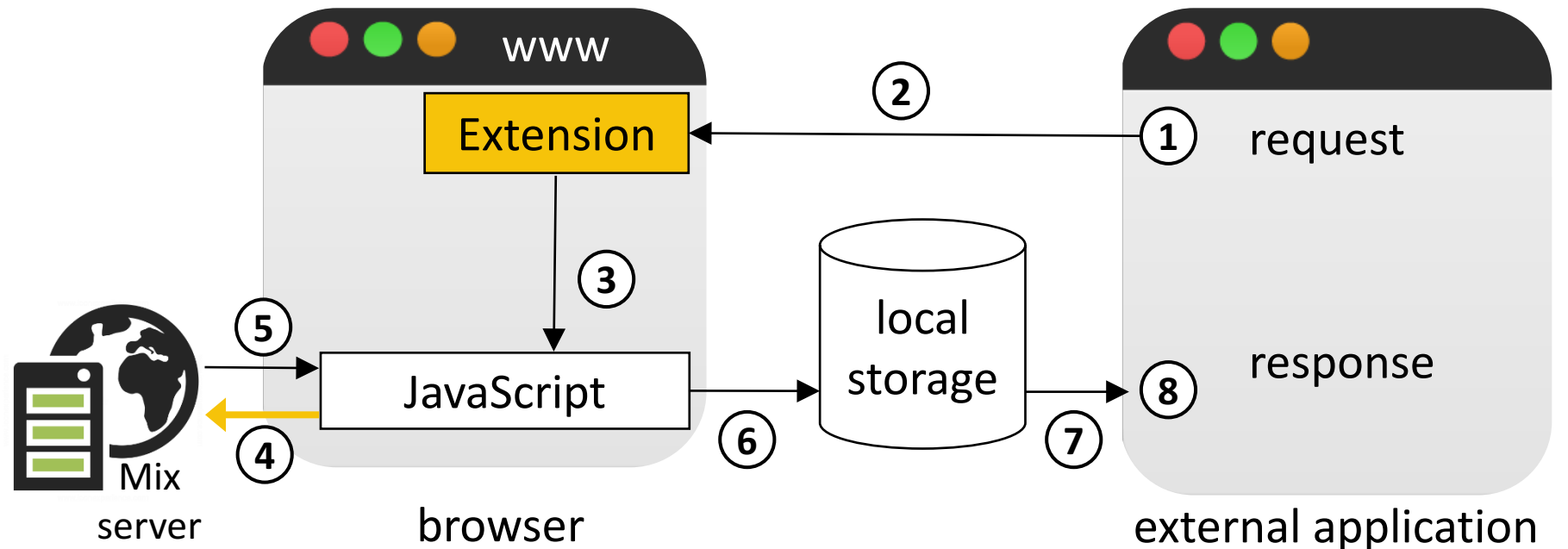
If you are genuinely interested in thwarting the tracking efforts of your ISP and advertisers you should:

1. Install [HTTPS Everywhere](#) to ensure your web activities are encrypted as often as possible.
2. [Donate to the EFF.](#)
3. Learn about [Tor](#).
4. Consider [using a VPN](#)
5. Install [Privacy Badger](#) to block spies and hidden trackers from sites you visit.

[https://slifty.github.io/internet\\_noise/index.html](https://slifty.github.io/internet_noise/index.html)

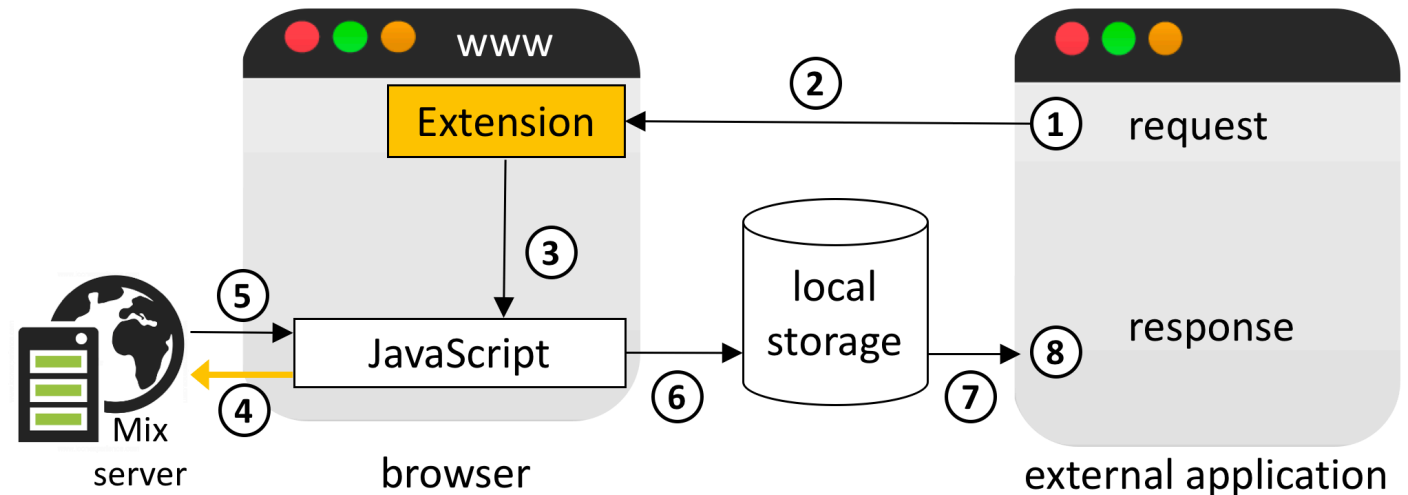
# CoverUp: Chat

- Enhances feed
  - Upstream channel to the mix server
  - Involves extension
  - Using TLS



# CoverUp: Chat

- General purpose bi-directional channel
  - Sandboxed iframe
  - Same-Origin-Policy
- Use case: chat
  - End-to-end encryption
- Mix
  - Chat relay
  - Constant time replay
- Trust assumption: mix is fully trusted



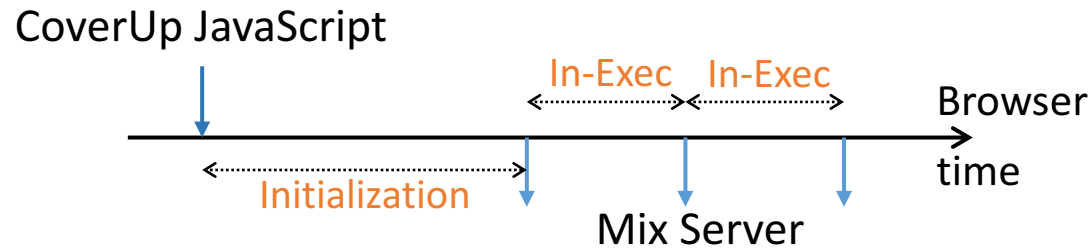


# Evaluating the Indistinguishability Assertion

- Protocol transcripts are indistinguishable
- What else can attacker do?
  - **Analyze user's entry server visiting pattern**
  - **Measure execution time by network timestamps**
- We analyze the **worst case**:
  - Precise knowledge of execution time distributions for voluntary and involuntary user.
  - No other processes running on the system (except the browser's

# CoverUp: Timing Leakage

- Two measurement scenarios:

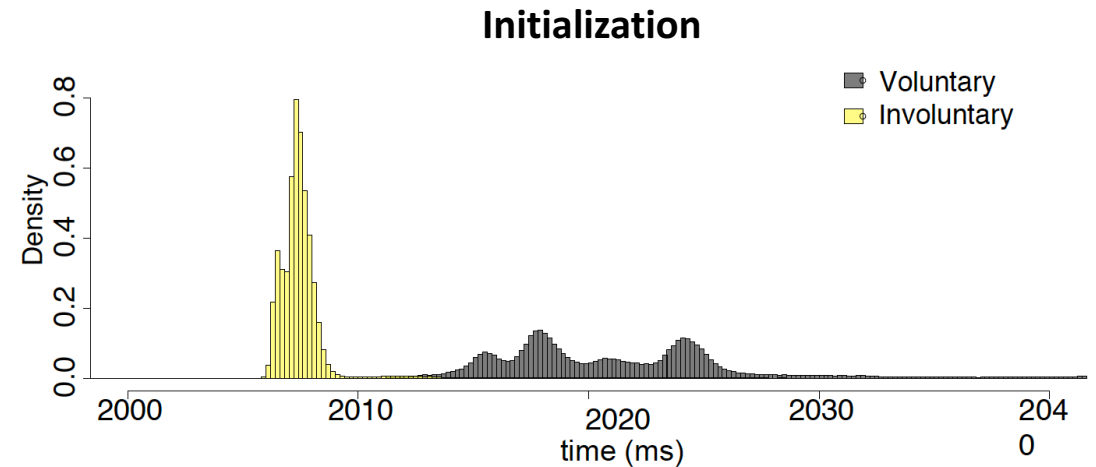
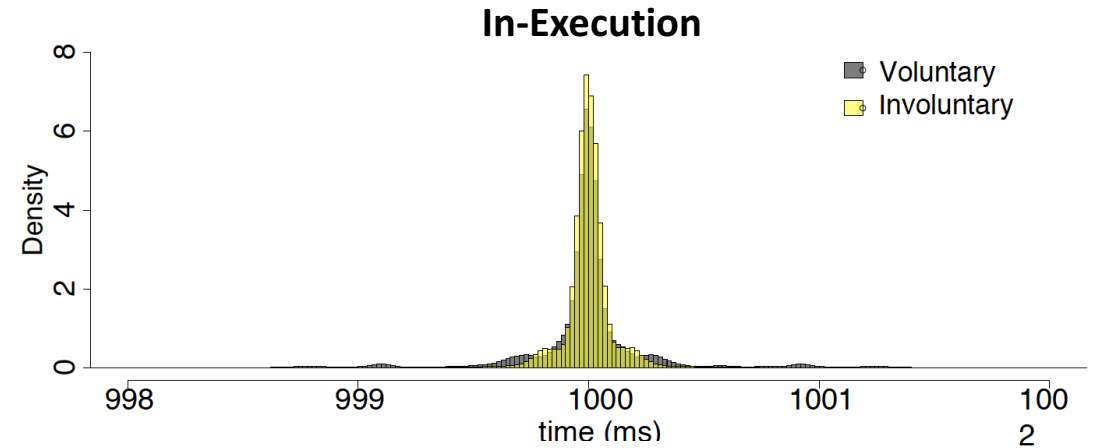


- Setup

- Server and client on same machine
- TCP timestamp on loop-back interface

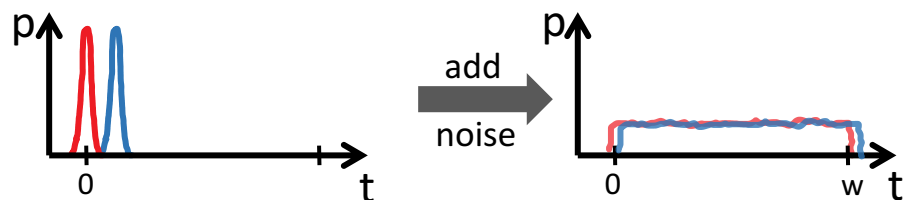
- Timing leakage

- Timestamp Frequency distribution

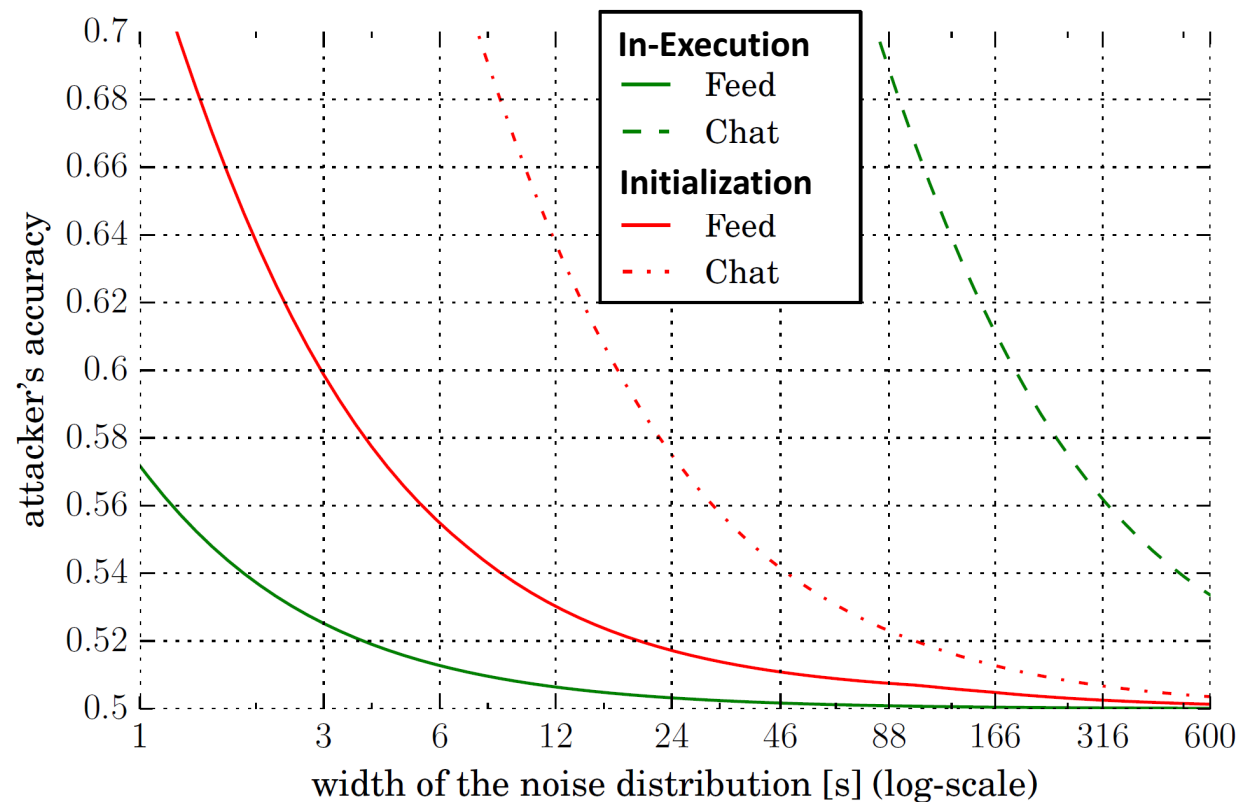


# CoverUp: Adding Noise

- Add uniform noise  $\in [0, width]$



- $accuracy := \frac{tp+tn}{tp+tn+fp+fn}$   
 $tp$  = true positive  
 $fn$  = false negative



Upper Privacy Bound

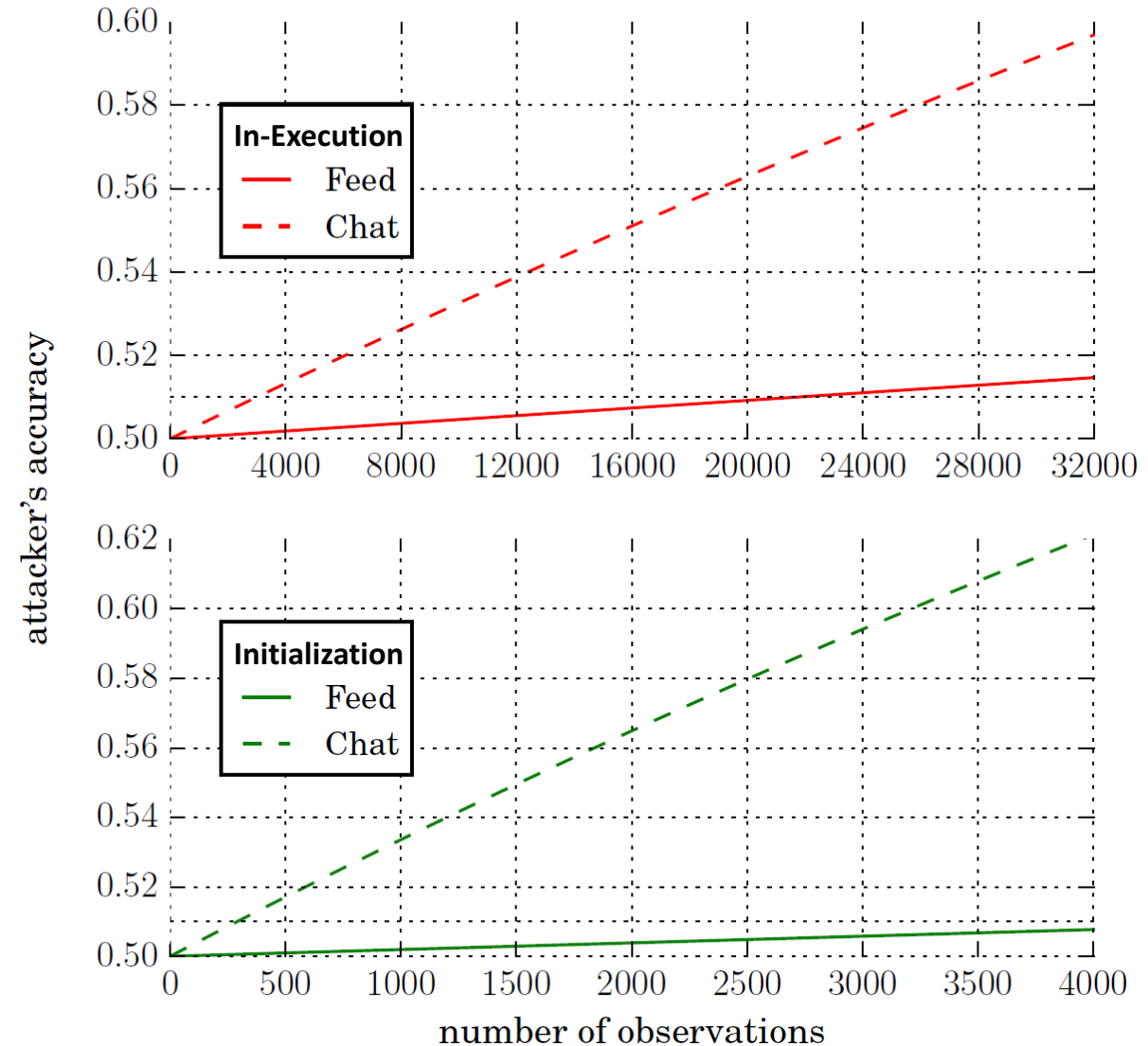
Sample size: 1K (Initialization), 10K (In-Execution)

# CoverUp: Privacy Budget (worst case)

Type	Width	AVG
Periodic	60s	30s
Loading feed	40s	20s
Loading chat	10min	5min

- Privacy Budget for Feed

- Invoke feed 4 times/day, 10min/stay\*
- 1k loading & 20k periodic observations/year
- Privacy budget: 1 year @ acc < 51%



\*Calculated over working days

# CoverUp: Performance

- Session time 10 minutes
- Performance
  - Packet size: 75 KB every 30s
  - Goodput: 20KBit/s
  - Decent enough for chat application
- Per user overhead with 10 connections/day
  - Around 165 MB/month

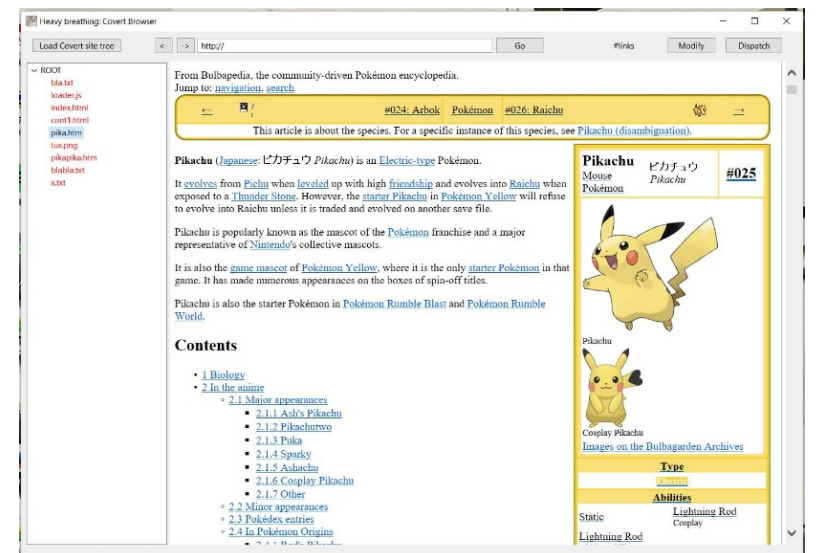
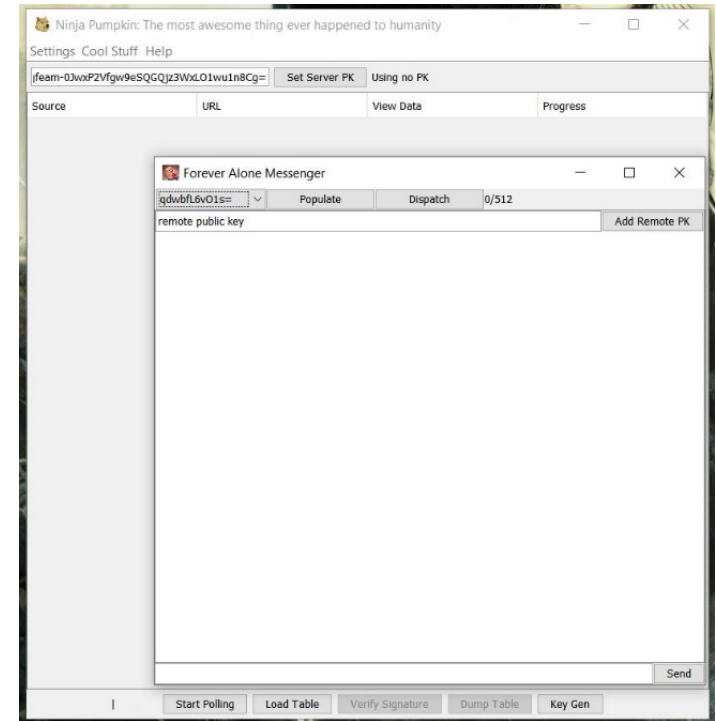
Country	Computer			Tablet			Phone		
	2016Q1	2015Q1	YoY	2016Q1	2015Q1	YoY	2016Q1	2015Q1	YoY
GLOBAL	9.4	8.8	7%	9.9	9.5	4%	7.5	8.2	-9%
USA	9.3	8.5	9%	9.6	9.0	7%	7.5	8.1	-7%
UK	10.3	10.2	1%	11.0	10.8	2%	7.5	8.2	-9%
GERMANY	9.3	9.2	1%	10.1	9.2	10%	7.8	8.5	-8%
FRANCE	8.7	7.9	10%	8.5	8.8	-3%	6.7	7.9	-15%
CANADA	10.0	8.2	22%	8.9	8.1	10%	7.8	7.8	0%

Reference: Demandware shopping index 2016Q1

# CoverUp: Implementation

- External application
  - Implemented in Java
  - Features: feed, chat and interactive browsing
  - Uses crypto APIs from whisper systems and JCA
- Browser extension
  - Firefox extension based on WebExtension API
- Mix and CoverUp server
  - Implemented using Java EE Servlet API
  - Hosted on Apache Tomcat webserver

Available for download and testing.



# Ethics?

- User could get informed about their participation
  - Option to opt out / opt it in a browser / on a page
- Users do not get harmed
  - Computational overhead negligible
  - Data overhead minimal ( 7.5MB / day )
- Advertisement networks / Tracking Services already execute code and 'store' data (temporarily) in browser cache

# Legal (Convention on Cybercrime (CCC))?

- **Illegal access** (article 2 CCC) penalizes the entering of a computer system. **However, download of the JavaScript from the CoverUp server is standard browser functionality** for communication. The same would happen if the entry server were financed by online advertising.
- **Data interference** (article 4 CCC) penalizes the damaging, deletion, deterioration, alteration or suppression of computer data “without right”. CoverUp does not damage, delete, deteriorate, or suppress data on the participant’s client. However, it does alter the data on the hard disk: on the one hand the webpage with the iframe uses disk space and thus modifies the participant’s data. **However the explanatory report to the Convention on Cybercrime foresees that the file causing data interference be “malicious”.** Code is malicious if it executes harmful functions or if the functions are undesirable.



# Legal (Convention on Cybercrime (CCC))?

- **Misuse of devices** (article 6 CCC) penalizes the production, making available, or distribution of a code designed or adapted primarily for the purpose of committing a cybercrime offense, or the possession of such a computer program.

One of the main questions relating to the misuse of devices is how to handle dual use devices (code). Dual use means in our case that the JavaScript code could be used to download legal content, e.g. political information, as well as illegal content, e.g. child pornography.

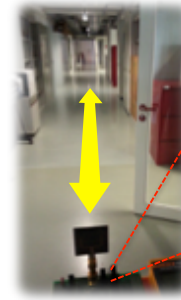
CoverUp was not produced for offensive purposes and makes sure that content is only available to voluntary users.

# Summary

- “Forced” participation
  - Increases anonymity set for any mix
  - Hides Intention
- Can this idea be generalized to other problems / properties?

# Other stuff that I like to do ...

- Secure and precise distance measurement
- GPS spoofing and spoofing detection
- Location-based Authentication
- Trusted computing (SGX, TrustZone, ...)
- ....



ANDY GREENBERG SECURITY 03.21.16 10:32 AM

## RADIO ATTACK LETS HACKERS STEAL 24 DIFFERENT CAR MODELS





### About ZISC

The world is undergoing a dramatic transformation. New information technologies emerge at rapid pace and these innovations have a significant impact on our social, political, and economic lives. The change does not come without risks. The goal of ZISC is to bring academia and industry together to solve the information security challenges of tomorrow. ZISC is an industry-funded research center of ETH Zurich where PhD students and senior researchers perform academic research under the supervision of ETH faculty members.

[Read More >](#)

