Format of this Document

1. **Topic Label**
   1. ***Document Title***
      1. Document Bibliography
      2. Organization/Country affiliation/Sponsors
      3. Document Zotero Unique Key
      4. Summary of Ethical issues (implicit or explicit)
      5. Summary of Ethical argument, if any (implicit or explicit)

**Note 1:** Since documents were clustered according to both their closest and second closest topic, a few appear in multiple topics. This did not substantially reduce the number of unique docs/topic, however.

**Note 2:** Documents were selected according to the algorithm given in topic\_doc\_selector.py, with priority following the order: ethics/grey union, ethics+grey intersection, ethics, grey. First, all documents from a category were used if there were <=20. Otherwise, the set was narrowed to documents that fell under both the ethics and grey classifications (and changed to “only ethics” and then to “only grey,” respectively, if this set was still >20 documents; this situation never occurred, however). If this set was <10, however, documents belonging to that category were added in a pseudorandom order first from the ethics group, then the grey one, until 15 documents were collected. 15 was the actual desired upper limit given resources available, but 20 was permitted only if it encompassed all documents of interest, because the value of reading all documents in a set was judged to be greater than the time it would take to read those extra documents.

**Note 3:** We generally skimmed most papers, thoroughly reading only certain sections that were likely to contain relevant discussion. Most important discussion was in the abstract, introduction, methodology, data sources, and discussion sections, which we read or skimmed thoroughly. The background and analysis sections typically were not informative because they usually discussed isolated calculations with no externalities in themselves, or others’ work. We also performed extensive keyword searches on documents to try to find discussion we might have otherwise overlooked.

**Note 4**: Although many papers addressed ethics in a specific section, even these papers often discussed throughout the paper measures they took to reduce externalities caused by their work. It therefore proved very valuable to also read methodology and data collection sections of papers; proper future analyses of papers should aim to review as much of the experimental part of the paper as possible.

**Note 5:** Avoided reading papers that specifically referenced or included a citation for Encore or the Internet Census in their bodies (part of Zmap, and two papers from ACM’s NS-Ethics workshop - **Ethical Concerns for Censorship Measurement** and **Submission Summary ACM SigComm2015**)  
). Encore is interesting because it was published after the Menlo Report, NS-Ethics, and CREDS. Although it was eventually condemned, it still seems to have passed through peer review (and IRB approval) before reaching that point, so unless its condemning principles have been embedded without reference in normal research papers from before or after its publication, we have little reason to believe its ethics will certainly be covered by our research, unless our methodology has some merit for issue discovery. For both condemned papers, in any case, since we track references for rules, we can determine what kinds of papers revealed applicable rules (e.g. papers from ethics conferences, grey-area papers, ethics-only papers, papers from certain years or topics, etc.)

**Note 6:** The Zmap paper (Durumeric ‘13) was assigned to the web security paper, but because there were a number of usenix papers in that category, it was not one of the randomly chosen papers; However, because 3 other papers referred readers to Zmap for ethical discussion, we felt our analysis of those papers’ ethical arguments would be incomplete without including Zmap itself, especially considering it was only excluded by random chance. (to preserve the integrity of our experiment, we did not read the related works section at the end that mentioned the Internet Census).

1. **Vulnerabilities Topic (more specifically, usually local, or one-off, analyses, on or offline)**

*Observations of research conducted and ethical practices from this topic*

* Some countries seemed to have different standards than others. E.g. Luxembourg and Germany did not mention IRBs. Papers came from USA, UK, Hong Kong, China, and Europe
* One paper (Luxembourg) apparently identified and controlled Botnet C&C servers, and manipulated Tor
* Typically propose defenses/mitigations, usually enough to solve the problem if implemented (but they often simply express a desire for the problem to be solved). Occasionally a paper that is unsure of the best fix will still perform & discuss experiments evaluating attacks/mitigations
* Often disclose vulnerabilities to vendors and get in touch with them before publishing
  + usually are well on their way to resolving the problem, or have already resolved it, by the time they submit their paper for publication
* Only obtain IRB approval for explicit human subjects testing (e.g. mechanical turk or physical laboratory studies)
* Typically do not give links to exploit code, etc. (but one paper did) – but typically include great detail about how the attacks are conducted (either theoretically or with pseudocode)
* One paper put malware on the Apple Store for their own devices to download (but removed it once that was finished)
* Researchers sometimes launched remote attacks on devices they own/control, whether physical or cloud computing (e.g. AWS)
* Usually work with open source code
* Sometimes reverse engineer open source code or open access code (and also Apple’s programs – not sure what Apple’s policy on that is)
* Did dynamic analysis, but only on a benign program (to find vulnerabilities)
* Justify disclosing vulnerabilities as raising awareness
* Maybe only one paper used databases of personal information, but that paper:
  + Used data collected with users’ explicitly informed opt-in consent (e.g. they chose to sign up for this research study, they knew that it would be shared online for research and treated confidentially; which data would be collected: and usually mentioned that this data would be used for uniqueness identification research).
  + Also used pseudo-anonymized data (personal identifiers were removed or hashed, and application names were hashed), and removed unnecessary data like timestamps
  + Obtained the data directly from the collectors, and signed research agreements stipulating things like that they cannot ‘use the dataset to deanonymize the users in the database,’ or that they can do their study of uniqueness.
* **Two papers (from CREDS) were dedicated to ethical security research (see the first two papers), and include potentially valuable pointers to additional research topics**
  1. ***Ethical issues in online trust***
     1. Wilton, Robert. “Ethical Issues in Online Trust.” *CREDS*. N.p., 2014. Web. 29 June 2017.
     2. ISOC/United States
     3. 3ZPVV72B
     4. Ethical content: E
     5. Ethical issues and frameworks
        1. 4 (overlapping) problem areas in online trust
           + The principle of “no surprises”

Difference between “legal” and “legitimate”

Holding data vs using data

Necessary and proportionate

Notice, consent, transparency, accountability

“Do unto others...”, fairness, power asymmetry (e.g. service provider vs user)

* + - * + Ethical dilution

“Harm” is a poorly defined metric

Harms are often separate from their source (externalities)

Passive data collection, tagging, facial recognition, inference, etc., needs to be considered (e.g. in terms of consent, intent, etc.) vs active disclosure

Vagueness re: chilling effects, definitions (e.g. data subject/controller/processor/PII) – doesn’t understand ‘custodian’ or ‘inference data’

Dispersed data results in diluted responsibility, diligence, and redress

* + - * + Multiple stakeholders

Online, most things are mediated/relationships (and asymmetric)

Caused partly by “remote trust” problem, mostly by power/mass/money

Multi-stakeholder models are actually bad b/c of conflicting interests (comparable to pure democracy, which is bad – e.g. the U.S. is a republic)

Question: can ethics bridge cultures, etc.? (e.g. may need local Japan ethics)

* + - * + Multiple contexts

Read about Helen Nissenbaum (contextual integrity) since it is influential

“big data” age focuses on repurposing database

Context, risk, technology, laws, and opinions can change in the future!

Healthcare data offers good case studies in public good vs individual, anonymization reliability, DNA, and behavior (there’s also a USENIX paper on DNA research)

* + - 1. 3 standard ethical models
         * What happens when they’re tested, e.g. vs personal data processing?
         * Consequential

Depends on accurate risk assessment (a huge problem currently, and the reason cyber insurance is hand-wavy), utility/public good calculations; and is fraught with skepticism

‘Privacy Impacting Information’ (vs PII) might be a useful concept

* + - * + Rule-based

depends on theoretical virtue/duty: currently too constrained by PII: depends on enforcement: compliance is often not enough, realistically

* + - * + Justice-based

fairness and legitimacy, openness and transparency, accountability/redress

‘Balance’ is often a zero-sum framing of the problem, though

Needs enforcement, but leads to behavioral enforcement (not technological, which is arguably a good thing)

But, again, is often contextual and cultural

* + - 1. Final thoughts: All models problematic, but Justice/legislation/policy may be good
         * Can we frame a problem statement for cyber-security research ethics?
         * Can we extend that to the general case?
         * Who is the audience?
         * What would deliverables look like?
         * What is a successful outcome?
  1. ***A Case Study in Malware Research Ethics Education***
     1. Sullins, John. “Case Study in Developing Malware Ethics Education.” *Cyber-Security Research Ethics Dialog & Strategy Workshop II*. San José: N.p., 2014. Web. 29 June 2017.
     2. Sonoma/United States
     3. UWSH887R
     4. Ethical content: E
     5. Malware ethics research issues - distinct from medical/computer ethics
        1. Actually, not all malware is unethical – some of it is brilliant
        2. Thinking like a hacker can create new hackers
        3. Human subjects IRB problems/informed consent (vis a vis hackers/victims), communicating dangerous findings, synthesizing/acting on data – ‘do no additional harm’ is not enough! - and not being able to get informed consent is not a good enough response (at least, we need some ethical justification)
        4. Malware research usually contradicts ACM code of ethics?
        5. Communicating results of malware research may enable cyber-crime, and we cannot rely on self-censorship – but academic freedom is important to balance
        6. It may be dangerous to get funding from certain organizations (e.g. government, military) that make disclosure of malware research privileged to those organizations
        7. Basically a pointer to another paper we did not include: <http://www.ieee-security.org/TC/SPW2014/papers/5103a001.PDF>
     6. Class curriculum
        1. Personal codes of ethics are more important than standards? - Ethical motivations and justification should be a part of all malware research (i.e. it should be a motivator, not a process)
        2. Topics of interest: Utilitarianism, Deontology, Human rights, unified common goods (James Moor), virtue ethics, information ethics, CIA, professionalism, personal encryption/data-level security – ethical or not?, cyberwarfare
  2. ***What the App Is That? Deception and Countermeasures in the Android User Interface***
     1. Bianchi, A. et al. “What the App Is That? Deception and Countermeasures in the Android User Interface.” *2015 IEEE Symposium on Security and Privacy*. N.p., 2015. 931–948. *IEEE Xplore*. Web.
     2. UC Santa Barbara/United States
     3. 7GEKJC5V
     4. Ethical content: C
     5. Ethical Issues
        1. Almost no ethical content. Studied techniques for mounting GUI deception attacks in Android apps, using static analysis. Source code was placed on Github.
     6. Ethical Arguments
        1. Android is open-source
        2. Obtained IRB approval for recruiting Mechanical Turk workers to guess whether an Android device was infected
        3. They also notified Google’s Security Team of vulnerabilities; and a review was in progress at the time of the writing (i.e. they disclosed on Github before hearing back from the review?)
  3. ***Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization***
     1. Biryukov, A., I. Pustogarov, and R. P. Weinmann. “Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization.” *2013 IEEE Symposium on Security and Privacy*. N.p., 2013. 80–94. *IEEE Xplore*. Web.
     2. University of Luxembourg/Luxembourg
     3. AF8UQV9I
     4. Ethical Issues
     5. Ethical content: E
        1. They launched a real attack on Tor, and collected the descriptors for nearly all hidden services on Tor, and apparently controlled part of the Silk Road and DuckDuckGo; and they found botnet C&C addresses. From these they collected (1) The number of requests for the hidden service descriptor per day and (2) the rate of requests over the course of a day.
     6. Ethical Arguments
        1. The deemed ‘experiments on the live Tor network that did not **intentionally** cause degradation of the network and its services to be worthwhile and necessary’ (emphasis added), because hidden services had theretofore not been well studied.
        2. They did not fully disclose the attacks, Tor is open source, and they proposed patches – though they said that the Tor hidden service model needs an overhaul
        3. They did not disclose information about guard nodes, and **discarded data** after the experiments.
        4. No mention of IRB
  4. ***Off-Path TCP Exploits: Global Rate Limit Considered Dangerous***
     1. Cao, Yue et al. “Off-Path TCP Exploits: Global Rate Limit Considered Dangerous.” N.p., 2016. Print.
     2. University of California/United States/Army
     3. EDJPA2U6
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Summary of research: Discover a vulnerability that ‘allows a blind off-path attacker to infer if any two arbitrary hosts on the Internet are communicating using a TCP connection,’ terminate connections and inject traffic.
        2. The victim servers they attacked (resetting SSH) were an Amazon EC2 instances owned by them, and were located in various different geographic locations, worldwide
        3. Reset a Tor connection: Their own entry relay established connections with an arbitrary middle relay (anywhere in the world).
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Propose changes to the TCP spec/implementation (but had not proposed the defenses to the Linux community of of the writing), and did not link to any attack code
        2. Regarding Tor, ‘For ethical reasons, we do not perform attacks against arbitrary relay nodes that are not connected to our node.’ But I don’t know enough about Tor to understand the difference between iv.b and v.b.
  5. ***Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization***
     1. Snow, K. Z. et al. “Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization.” *2013 IEEE Symposium on Security and Privacy*. N.p., 2013. 574–588. *IEEE Xplore*. Web.
     2. United States/Germany
     3. ETII5WQP
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Develop an exploit that can be widely deployed. Describe how to create it in great detail.
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Do not provide source code for their particular exploit
        2. Suggest some (non-comprehensive) mitigations
        3. Explicitly, regarding ethics, say: ‘we believe that **shedding light on fundamental weaknesses** in current ways of thinking about exploit mitigation **outweighs the potential downside** of helping the next generation of hackers. If history serves any lesson it is that **attackers will adapt and so must we** in order to stay one step ahead. It is our hope that this work will inspire those more clever than ourselves to design more comprehensive defenses.’
  6. ***Privacy Wedges: Area-Based Audience Selection for Social Network Posts***
     1. Raber, Frederic, Alexander De Luca, and Moritz Graus. “Privacy Wedges: Area-Based Audience Selection for Social Network Posts.” *WPI@ SOUPS*. N.p., 2016. *Google Scholar*. Web. 30 June 2017.
     2. Germany
     3. F2MGACS2
     4. Ethical content: N
     5. Summary of Ethical issues (implicit or explicit)
        1. Note: this paper seems to be unrelated to vulnerabilities
        2. Details hiding information from others on social networks, but does not address the potential of this for creating echo chambers of communication
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. No discussion of ethics
        2. Implies that users should be allowed to easily limit their posts on social media sites like Facebook to specific people (and in particular, should be allowed to do so on all websites that use real identities)
        3. No discussion of IRB process for their testing of human subjects, or the data they collected (e.g. demographics)
  7. ***SandScout: Automatic Detection of Flaws in IOS Sandbox Profiles***
     1. Deshotels, Luke et al. “SandScout: Automatic Detection of Flaws in IOS Sandbox Profiles.” ACM Press, 2016. 704–716. *CrossRef*. Web. 29 June 2017.
     2. U.S./Romania/Germany
     3. GTZ9GJGX
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Decompiled Apple firmware for the purposes of finding vulnerabilities/attacking
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Mentioned that firmware is freely available, but did not mention Apple’s policies on decompilation
        2. Before submitting the paper, the researchers reported all vulnerabilities to, and began working with, Apple, to resolve the attacks.
  8. ***Call Me Back!: Attacks on System Server and System Apps in Android through Synchronous Callback***
     1. Wang, Kai, Yuqing Zhang, and Peng Liu. “Call Me Back!: Attacks on System Server and System Apps in Android through Synchronous Callback.” ACM Press, 2016. 92–103. *CrossRef*. Web. 29 June 2017.
     2. China/U.S.
     3. JQPZ4W83
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Using static analysis, discovered vulnerabilities in Android code affecting over 1 billion devices
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Android is open source
        2. Informed Google of their findings prior to publication: and included fix suggestions
  9. ***Near-Optimal Fingerprinting with Constraints***
     1. Gábor György Gulyás, Gergely Acs, and Claude Castelluccia. “Near-Optimal Fingerprinting with Constraints.” *Proceedings on Privacy Enhancing Technologies* 2016.4 (2016): n. pag. *CrossRef*. Web. 30 June 2017.
     2. France
     3. KTIKM87V
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Used 3 real-world datasets to try to re-identify users with an optimal algorithm they theoretically devised that optimizes a) minimizing the number of data attributes needed and b) maximizes the number of individuals re-identified.
        2. In 3 separate studies, used smartphone apps installed, cell phone towers activated, and browser fonts installed, as their data attributes.
        3. No mention of an IRB was given
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Used data collected with users’ explicitly informed consent (e.g. that it would be shared online for research, treated confidentially; which data would be collected: and usually mentioned that this data would be used for uniqueness identification research).
        2. Also used pseudo-anonymized data (personal identifiers were removed or hashed, and application names were hashed), and removed unnecessary data like timestamps
        3. Obtained the data directly from the collectors, and signed research agreements stipulating things like that they cannot ‘use the dataset to deanonymize the users in the database,’ or that they can do their study of uniqueness.
  10. ***Don’t Interrupt Me While I Type: Inferring Text Entered Through Gesture Typing on Android Keyboards***
      1. Simon, Laurent, Wenduan Xu, and Ross Anderson. “Don’t Interrupt Me While I Type: Inferring Text Entered Through Gesture Typing on Android Keyboards.” *Proceedings on Privacy Enhancing Technologies* 2016.3 (2016): 136–154. *DeGruyter*. Web.
      2. University of Cambridge/England/UK
      3. MW3588DS
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. Developed a malicious Android app to monitor keyboard input
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Explicitly addressed the ethics of their app, saying that it only monitored another ‘victim app’ that the researchers created (i.e. it did not monitor the system or all of participants’ keyboard input). This seems a little confusing, though, since they said that the typing information can be accessed system-wide.
         2. Proposed and assessed mitigations
         3. The researchers ‘responsibly disclosed’ their findings to Google prior to publication
  11. ***On the Practical (In-)Security of 64-Bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN***
      1. Bhargavan, Karthikeyan, and Ga?tan Leurent. “On the Practical (In-)Security of 64-Bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN.” ACM Press, 2016. 456–467. *CrossRef*. Web. 29 June 2017.
      2. France
      3. P534F2JG
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Set up two physical machines, and attacked one with the other, over OpenVPN and over HTTPS.
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. On their servers, used Firefox, nginx, Linux, and BasicAuth (all open source, I believe)
         2. Proposed mitigations
         3. The researchers ‘responsibly disclosed’ their findings prior to publication, to organizations like Akamai, Microsoft, Apple, Mozilla, OpenSSL, and OpenVPN, and received their responses before publishing/saw the results of the organizations’ responses (i.e. recommending clients not use 3DES)
         4. State that their attacks were both already (theoretically) known and that their goal in experimenting/publishing is to raise awareness: ‘Like many recent attacks on TLS, ...the underlying principles behind our attacks **were well known** to cryptographers. **Our goal is to raise awareness** among practitioners about the vulnerabilities of short block ciphers and on safe ways of using them.’
         5. Included a link for more details about countermeasures (not attacks): [http://sweet32.info](http://sweet32.info/)
  12. ***Breaking Web Applications Built On Top of Encrypted Data***
      1. Grubbs, Paul et al. “Breaking Web Applications Built On Top of Encrypted Data.” ACM Press, 2016. 1353–1364. *CrossRef*. Web. 29 June 2017.
      2. Cornell/USA/Microsoft
      3. WIZXW8DZ
      4. Ethical content: N
      5. Summary of Ethical issues (implicit or explicit)
         1. Analyzed applications that deal with medical data, exposing vulnerabilities in them
         2. Do not offer a good solution/fix/mitigation to their problem; though they do discuss that this appears to be a fundamental problem with the type of system they studied
         3. Do not discuss disclosing or pushing, etc., their results to the authors/maintainers of the programs they assessed
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Analyzed open source projects (Mylar, kChat, etc.)
         2. It sounds like they created/forked their own versions of open source apps on Github
  13. ***Jekyll on iOS: When Benign Apps Become Evil***
      1. Wang, Tielei et al. “Jekyll on IOS: When Benign Apps Become Evil.” N.p., 2013. Print.
      2. Georgia Tech/USA
      3. X7QZS7BR
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Put a malicious app on the Apple store (I believe another paper in this Vulnerabilities Topic put a malicious app on an app store and then took it down after a controlled group of phones had downloaded it – and they made sure nobody else had downloaded it – though if someone else had downloaded it, I don’t know what they would have done...I just can’t remember which paper it was...it could have been this one, actually)
         2. Remotely launched attacks on their own devices
         3. Proposed “a dynamic analysis technique to discover the private APIs used to post tweets, send email, and send SMS without user’s consent on iOS”
         4. Implicitly acknowledge the resources security researcher provide to hackers: “**If new vulnerabilities** in Mobile Safari **are disclosed by other researchers** in the future, **we can** simply **take advantage of these** new vulnerabilities to launch similar powerful attacks.”
         5. Developed a dynamic analysis tool to find a vulnerability in Twitter’s public (or private?) API – but did not disclose the vulnerability to Twitter?
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. “Following the ethical hacking practice, we immediately removed the app from App Store once a group of experiment devices of our control had downloaded it. The download statistic provided by Apple later confirmed that the app had never been downloaded by any other users.”
         2. Discussed countermeasures to secure against Jekyll apps
         3. Disclosed their attack to Apple prior to publication and began correspondence
         4. Note (with references) that “Discovering software vulnerabilities using static analysis alone is fundamentally an undecidable problem… . Dynamic analysis based vulnerability detection approaches can also be easily defeated,” although this does not seem to be a comment on their own use of dynamic analysis (which was done on benign software, anyway)
  14. ***No Pardon for the Interruption: New Inference Attacks on Android Through Interrupt Timing Analysis***
      1. Diao, W. et al. “No Pardon for the Interruption: New Inference Attacks on Android Through Interrupt Timing Analysis.” *2016 IEEE Symposium on Security and Privacy (SP)*. N.p., 2016. 414–432. *IEEE Xplore*. Web.
      2. Hong Kong
      3. XIIWZRN3
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. Perform small user studies (2-5 participants) involving Android unlock passwords, and apparently report the passwords used commonly (by their participants?) in an Appendix
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Obtained IRB approval for human subjects testing
         2. Propose defenses

1. **Online Measurement Topic (includes vulnerability research, but usually large scale)**

*Observations of research conducted and ethical practices from this topic*

* Researchers, Universities, Contributors, and Funding came from the U.S.A., Canada, China, Israel, Korea, Saudi Arabia
* Research and possible grey areas remaining:
  + Some created spam honeypots
  + dynamically executed malware and related content (e.g. malicious website javascript)
  + Buying criminal services
  + Controlled a botnet
  + Obtaining identifers, contact info, PII about assumed criminals
  + Website ToS may violate user agency (e.g. Facebook lets you share your friends pictures) but researchers treated ToS higher than possible ethics
  + At least one study ignored robots.txt
  + **Justified descriptions of attacks by saying it will help researchers, and trying to validate that it has not helped criminals** (though the latter was rare – and I haven’t seen a paper about how it has helped researchers...maybe a useful thing would be an analysis tracking citations of papers which disclose attacks/vulnerabilities (rather than just give the gist), to try to assess how much they are actually used...perhaps compared to other types of security papers)...certainly, responsible disclosure is useful...but maybe better ways exist of disseminating mitigation information to directly impacted vendors (as well as other vendors who potentially have or will create software with similar problems)
  + falsely advertising (though adhered to ToS and had a policy to fulfill ad claims)
  + Interacted w/ hackers/spammers (e.g. sent a bait to collect their IP address) – hack back?
  + Mention real email addresses of people (probably spammers) in papers
  + Consenting participants’ data was not always deleted, though it was kept confidential
* Explicit ethical practices:
  + Used publicly available data instead of scraping sites (though some of those sites may be questionably legal depending on the country), or did studies on various sites, queried once – but there were web scrapers too (lots of them)
  + Tried to minimize data collected
  + Tried to collect aggregate and/or anonymous data/not store identities
  + Responsible disclosure (even when stumbling upon relevant info, e.g. spammer emails – sending them to organizations after verifying them somehow)
  + Adhered to website ToS (treated this as paramount) or EULA
  + Got IRB approvals (treated this as a pass)
  + Obtained informed consent (data type, amount, use)
  + Securely transmitted data
  + Sometimes securely stored data
  + Deleted data from system when not needed (as in, immediately)
  + Were conscious that their intervention might change things on remote servers
  + When created sites in the wild (e.g. honeypots), carefully avoided problems that could arise if ‘real people’/innocent victims interacted; had protocols for this
  + Did not reveal participant information to third parties (e.g. to other participants)
  + Sometimes did not even reveal participant information to researchers (e.g. location, IPs)
  + Researched laws on things like downloading pictures (apparently that can be illegal)
  + Non-researchers affiliated with projects signed NDAs and deleted data
  + If deceiving people, debriefed them
  + passively collected information when possible
  + Suggested ways of taking down botnets without collateral damage
  + Some think the ACM code of ethics is a good starting point
  + Some might argue that maintaining human agency is even more important than utility/efficiency
  + Responsible disclosure
  1. ***Lurking Malice in the Cloud: Understanding and Detecting Cloud Repository as a Malicious Service***
     1. Liao, Xiaojing et al. “Lurking Malice in the Cloud: Understanding and Detecting Cloud Repository as a Malicious Service.” ACM Press, 2016. 1541–1552. *CrossRef*. Web. 29 June 2017.
     2. United States
     3. 4F4MQBZW
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Used Common Crawl, which has questionable legal status in Europe due to potential copyright infringement on websites it scrapes
        2. Actually scraped thousands of real websites, probably including some against their robots.txt agreements (claimed to scrape the Alexa 3000) using a firefox addon they developed
        3. Created a spam honeypot
        4. Provided (in the paper) links to apparently malicious domains
        5. found and exploited a vulnerability on websites, accessing some information about the websites
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Using common crawl for web scraping avoids unnecessary traffic to the real website
        2. Reported findings to websites, and awaited feedback from at least some of them before publishing
        3. May have only had to visit each website once/the main page, so that might not really be ‘crawling’
        4. Justified exploiting the vulnerability by saying: our **scanner was designed to minimize the privacy impacts** on vulnerable repositories: specifically, it **only tried** out the functionality like **file listing, uploading and downloading**. The **impact** of such operations are very much in line with those of running online web testing tools.... Most importantly, we did this with the full **intention to protect** such repositories from future exploits, and also carefully **avoided changing** any existing content there and **deleted from our system** all the files downloaded. Further, we have already **contacted** the major **vendors**
        5. In sum, they only did what was necessary (in their minds) to protect the repositories (though maybe I disagree); they claim their impact was not excessive: they did not change anything; they deleted files; the files were probably unimportant; and they responsibly disclosed the vulnerabilities (and apparently the vendors were grateful)
  2. ***Portrait of a Privacy Invasion***
     1. Shoshitaishvili, Yan, Christopher Kruegel, and Giovanni Vigna. “Portrait of a Privacy Invasion.” *Proceedings on Privacy Enhancing Technologies* 2015.1 (2015): 41–60. *DeGruyter*. Web.
     2. US/Austria
     3. 8G22E35G
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Created a machine learning program that detects romantic relationships based on pictures.
        2. Collected two corpora of pictures: one of celebrities collected via paparazzi, etc.; and one of facebook users obtained via the consent of only a very small fraction of people owning or in the pictures
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Obtained consent from users to use both their and their friends’ photographs
        2. Identified a facebook setting that allows you to give applications access to your friends’ pictures (which seems surprisingly invasive, as they comment)
        3. Obtained IRB approval
        4. Suggested a few mitigations and myriad other applications, both good and bad
        5. Edited excerpt: “Volunteers were **informed** about the **type** and **amount** accessed, and the **purpose**. Use of the friends’ data is **covered under the privacy policy** that they agreed to upon joining Facebook. **Photographs were discarded** after face detection. The ages of users are retrieved only to understand the demographics of the dataset, and the statuses of users are **retrieved** during each experiment **and discarded** after being used for training and cross-validation. All data transmission took place over **SSL-protected** channels. Other than the data of which users appear in which photographs and Creepic’s predictions, **no privacy-sensitive data was** ever **stored**. Even the photograph metadata and **Creepic’s predictions are purged** after every experiment is concluded, and C**reepic’s predictions are never explicitly revealed** to the volunteers, to preserve the privacy of their Facebook friends.”
        6. In sum, riding off of other privacy policies makes this allowed; and type/amount/purpose of data (i.e. informed) consent was obtained. Also, data was never unnecessarily stored (even if it would’ve been useful for some other research), and it was securely transmitted.
        7. Computed biases in their datasets, and found that it was slightly age-biased, but they didn’t do anything about that bias, since that was unrelated to the goal of their research (and it had no real effect, since it’s not like you need a representative sample in order to demonstrate the feasibility of a privacy invasion, since invading thousands of people’s privacy is enough of a demonstration)
  3. ***The Ever-Changing Labyrinth: A Large-Scale Analysis of Wildcard DNS Powered Blackhat SEO***
     1. Du Hao Yang, Kun et al. “The Ever-Changing Labyrinth: A Large-Scale Analysis of Wildcard DNS Powered Blackhat SEO.” N.p., 2016. Print.
     2. China/Hong Kong/Baidu
     3. 9TPBV29Q
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. infiltrated and purchased spider pool (蜘蛛池) service
        2. created a web crawler and DNS scanner
        3. reached out to an owner of a spider pool in operation and purchased SEO service to promote a site created by them
        4. Scanned domains both in and not in the spider pool (e.g. .gov and .edu)
        5. extracted contact information of criminals
        6. Exposed many links to criminal websites
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. The fake website’s webpages were modified to ensure there was no input box that accidentally accepts user’s sensitive information
        2. Filtered out site logs that do not belong to search crawlers
        3. Disclosed findings to Baidu and Google and started working with Baidu
        4. support of the criminal organization was only $8 and was for a short period
        5. Proposed a few mitigations
        6. Minimized pollution of search engine results
  4. ***Topics of Controversy: An Empirical Analysis of Web Censorship Lists***
     1. Weinberg, Zachary et al. “Topics of Controversy: An Empirical Analysis of Web Censorship Lists.” *Proceedings on Privacy Enhancing Technologies* 2017.1 (2016): 42–61. *DeGruyter*. Web.
     2. Carnegie Mellon/Australia
     3. 677WRHRN
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Created a massive web scraper to identify the topics of websites that are censored versus the rest of the Internet (using LDA)
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. **Our collector ignores robots.txt, because a human-driven browser would do the same.** Instead, we avoid disruptive effects on websites by randomizing the order of page loads, so that no website sees a large number of accesses in a short time. Also, we do not traverse any outbound hyperlinks from any page, which reduces the odds of modifying sites by accessing them. For legal reasons, our collector does not load images and videos, nor does it record how the pages would be rendered. While HTML sources are safe, there exist images that are illegal to possess, even unintentionally, in the USA.
        2. In sum, ignores robots.txt files, but tries to minimize site disruption/modification, and tried to avoid breaking laws about image processing
        3. Commented on the English-bias of Common Crawl
  5. ***Hunting the Red Fox Online: Understanding and Detection of Mass Redirect-Script Injections***
     1. Li, Z. et al. “Hunting the Red Fox Online: Understanding and Detection of Mass Redirect-Script Injections.” *2014 IEEE Symposium on Security and Privacy*. N.p., 2014. 3–18. *IEEE Xplore*. Web.
     2. USA/RSA/Microsoft/Saudi Arabia
     3. BV2ZQT3F
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Via a firefox extension, collected data via **web crawling** the top 1 million Alexa websites as well as sites deemed vulnerable by a virus scan
        2. **Executed all dynamic content** found on all webpages, expecting and **knowing** much of it to be **malicious** (in particular, looking for javascript redirects)
        3. Dumped all HTML/JS files found into a database, but apparently **retained the data**
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Did not notify discovered compromised sites because it was infeasible, but verified that all of them should have already been notified, by their presence on other lists
        2. Justifies **dynamically running the code** by simply saying that approach works much **more effectively**..., as new redirections and new web content are increasingly generated through execution of dynamic content such as scripts’
  6. ***To Befriend Or Not? A Model of Friend Request Acceptance on Facebook***
     1. Rashtian, Hootan, Yazan Boshmaf, Pooya Jaferian, and Konstantin Beznosov. “To Befriend Or Not? A Model of Friend Request Acceptance on Facebook.” In *Symposium on Usable Privacy and Security (SOUPS)*, 285–300. New York: Springer Pub. Co., 2014. <http://public.eblib.com/choice/publicfullrecord.aspx?p=423411>.
     2. Canada
     3. CPK73GW9
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Conducted an in-person and a mechanical turk user study
        2. Recruited participants on Craigslist and Kijiji, and deceived them
        3. Created a fake Facebook account (which I think is against the ToS)
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Received approval for their studies from their university research ethics board
        2. Recruited a somewhat unaffiliated mediator to aid in the recruiting of subjects. The recruiter followed a strict protocol, signed an NDA, and promptly delete all communications data
        3. Debriefed the participants after the study concluded
  7. ***You Are a Game Bot!: Uncovering Game Bots in MMORPGs via Self-Similarity in the Wild***
     1. Lee, Eunjo et al. “You Are a Game Bot!: Uncovering Game Bots in MMORPGs via Self-Similarity in the Wild.” Internet Society, 2016. *CrossRef*. Web. 30 June 2017.
     2. Korea
     3. IVZZ9K2B
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Worked with game companies to perform measurements on users, although the scope of these measurements may or may not be clearly communicated when the players consent to them (since consent via EULA, ToS, etc. is controversial)
        2. Identified robots playing MMORPGs, which has the potential for finding false positives and subsequently banning innocent players, which could be illegal
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Discussed reducing false positives by being conservative with estimates, such as looking at shared IP addresses, or payment history
        2. IRB/ethical committees approved the research
        3. Players signed a EULA when installing the game client, and only anonymous statistical data was collected, apparently, and only for this purpose, it sounds like
  8. ***All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records***
     1. Liu, Daiping, Shuai Hao, and Haining Wang. “All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records.” ACM Press, 2016. 1414–1425. *CrossRef*. Web. 29 June 2017.
     2. USA
     3. N726QEZ3
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Perform DNS and IP queries against a large number of websites
        2. Proposed new attacks
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “We **did not conduct any adversarial** activities against the scrutinized domains or the visitors to the Dares we successfully identified. We also checked with our institution’s **IRB** and confirmed that we **do not need** to obtain its **approval**. All examples presented in this paper have either been **corrected** **or defensively exploited** by us. We have **sent notifications** to all affected domains”
        2. In sum, they notified domains of the vulnerability, but they may or may not have also exploited it somehow
        3. Proposed mitigations to discovered attacks
  9. ***SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets***
     1. Rossow, C. et al. “SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets.” *2013 IEEE Symposium on Security and Privacy*. N.p., 2013. 97–111. *IEEE Xplore*. Web.
     2. Germany/The Netherlands/Crowdstrike
     3. S5WZ7R6P
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Create a model to analyze the resilience of P2P botnets/analyze them
        2. Apply crawling, injection, and disruption to real world botnets
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “attacks like **sinkholing involve unsolicited communication with infected hosts**, which could be considered unethical by some. Proponents of such attacks might argue that **sinkholing does not cause additional harm**, as infected hosts already communicate with other bots. Another ethical concern is the level of **detail our work should reveal** to the public about botnet resilience. The concern is that botmasters could **use our insights to harden their botnet** designs. Therefore, we describe our results such that they **cannot be directly applied** by botmasters to harden their botnets. On a reassuring note, several detailed strategies for resilient P2P botnet designs have been publicly proposed, but we **do not know of any real botnets that make use of these** ideas [22, 31, 32, 10]. We believe that the potentialof our work **to assist security experts justifies its publication**. We hope that our insights will help avoid damage to innocent third parties caused by the **common takedown problems pointed out by Dittrich et al**. [6]. ...Moreover, we think there is a pressing need for debate to establish clear boundaries on how far authorities are allowed to go when disabling P2P botnets. We currently see several alternative mitigation possibilities which we believe are deserving of further analysis. First, it is sometimes **possible to disinfect bots remotely by exploiting vulnerabilities** in bot software. This strategy is **currently considered unethical** because it could cause **collateral damage** to the hosts being disinfected if executed without great care. Nevertheless, it is a method which **may need to be considered** if future P2P botnets become immune to more conventional countermeasures. A second vector for mitigating P2P botnets is to **impersonate the botmaster** by forging commands for the bots.... Finally, some botnets could be mitigated by **attacking their monetization models**. For example, Zeus gathers bankingcredentials, and its botmaster relies on the accuracy of the stolen data. Inserting large amounts of invalid banking data could render the botnet unprofitable for the botmaster. For spamming botnets, node enumeration could be used to create spam blacklists, reducing the botnets’ revenue.”
  10. ***Website-Targeted False Content Injection by Network Operators***
      1. Nakibly, Gabi, Jaime Schcolnik, and Yossi Rubin. “Website-Targeted False Content Injection by Network Operators.” N.p., 2016. Print.
      2. Israel
      3. T72HZ3PE
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Published malicious packet injection content
         2. During their experiments, the authors observed many occurrences of (possibly state-sponsored) censorship-aimed injections, but did not report on them in this paper.
         3. Eavesdropped on/captured Internet traffic to analyze it for injection attempts by ISPs
         4. Don’t specify if/when they deleted the traffic they stored
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Publish injection samples ‘to facilitate continued analysis of this practice by the security community’
         2. “The system stores only TCP sessions in which a packet race was detected. All other sessions are **only cached briefly** in the workers’ caches, after which they are **permanently erased**. Moreover, for each stored session, only the last 30 packets (at most) are saved. Earlier packets are dropped. This is in order to **store only those packets that are relevant** to the analysis of the injection events while minimizing the chance that user privacy will be breached. Indeed, during our analysis **no identifiable personal information was found** in the stored sessions.”
         3. “Throughout our research we were **supervised** by the networks’ administration teams, who **reviewed and approved the code** of the monitoring system **and procedures** for the analysis of the stored sessions. During the analysis the location and identity of users associated with IP addresses were **never disclosed** to us. Finally, we note that our monitoring system **passively collected** information; it never interfered or tampered in any way with the traffic.”
         4. In sum, the researchers minimized the information they collected, they collected the traffic passively, they promptly deleted information, and they were supervised/approved by a more objective party
         5. Proposed mitigations
  11. ***Scambaiter: Understanding Targeted Nigerian Scams on Craigslist***
      1. Park, Youngsam et al. “Scambaiter: Understanding Targeted Nigerian Scams on Craigslist.” *system* 1 (2014): 2. Print.
      2. United States
      3. URC2WAHD
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Created a honeypot falsely advertising goods for sale on Craigslist
         2. Automatically received and replied to scam emails
            + sent images leading back to their server through email (i.e. Interacted with scammers’ systems on their system)
         3. Collected IP addresses of scammers to explicitly confirm their geolocation
         4. Performed a variety of analyses on a massive resultant data set
         5. Will give the spam email addresses to webmail providers/corporations like PayPal (and included some in the paper)
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Carefully designed their advertisements to specifically not appeal to real buyers
         2. Since our experiment **ultimately deals with human subjects**, we put several controls in place to manage any **harm to the participants**. In addition, we went through the process of getting our experiment **approved by our institution**’s human subjects review process…. In order to prevent this unintentional “victimization”, we **consistently check** if there were any actual payments made by legitimate Craigslist users. If a payment was made by a legitimate user, the **victim would be provided with pertinent information** about our experiment, and the **item** would be shipped to them **or the refund** procedure would be initiated immediately. In addition, any **messages from this user would be purged** from our collected data. Note that **fortunately, we found no payment** made by any legitimate users during the entire experiment.”
         3. “Another issue concerns how we use the collected data that might contain private information about scammers. Throughout the experiment, we gathered messages that contain information such as shipping addresses and phone numbers which could potentially be used to identify scammers. **We limit the use of raw data** to email addresses, IPs, and text from messages that will **not clearly identify** the actual identity of the scammer. All other information is **only included in aggregate** to avoid revealing the identity of any scammers.”
         4. In sum, limited information collected and stored, and limited the amount labeled with identifiers. Also, had a policy for dealing with problems (e.g. legitimate users), and received approval for human subjects experimentation.
         5. “**adhered to Craigslist’s terms of use** regarding posting advertisements”
  12. ***Why ‘No Worse Off’ Is Worse Off***
      1. Aycock, John, and John Sullins. “Why ‘No Worse Off’ Is Worse Off.” N.p. Web. 29 June 2017.
      2. Canada/US (disclaimer: same author as Malware class)
      3. WD738EHK
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Deception studies without consent or debriefing have been done with IRB approval (e.g. fake phishing)
         2. Botnet studies
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. IRB-approved or legal don’t necessarily mean ethical
         2. in 2009, a botnet was controlled and PII was collected; IRB approval was subsequently obtained
         3. Minimization of harm is not the same as no harm (and therefore the harm might outweigh the benefits, or it might not be up to the researchers to decide that; or some other practice is better) – essentially, this is bad because it forces a utilitarian approach: this is bad because these things are hard to measure/researcher biased
         4. Also, some researchers can only justify ethics by stating hopes and beliefs of benefit
         5. ACM code of ethics is pretty good
         6. Agency is important to maintain (Robert agrees in theory)
         7. If understanding and controlling botnets (for example) is the goal, is that goal really necessary? Are research projects that can impact people really necessary? More importantly, is their necessity properly explained in both their proposals and their reporting (e.g. conference papers)?
         8. ‘computer ethics’ and ‘information ethics’ and deontology and Kant
         9. proposal: assess utility; respect rights regardless of utility; fulfill duties
         10. ‘it’s too hard’/’it’s inefficient’ can be a cop-out; best avoided via collaborative efforts
  13. ***Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware***
      1. Seth Hardy et al. “Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware.” N.p., San Diego. Print.
      2. United States/The Citizen Lab
      3. ZKTI9ZQK
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Participants’ identities and PII was collected
         2. Do not address the privacy of the targeted attackers
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. IRB approved…
         2. Participants PII were kept confidential (but still observed/not deleted?)
         3. Participants forwarded emails themselves to provide data (i.e. self-reporting/consent)
         4. Do not do anything except analyze email content (e.g. body, malware, headers)

1. ***Low Level Documents***
   1. ***Hacking Blind***
      1. Bittau, A., A. Belay, A. Mashtizadeh, D. Mazières, and D. Boneh. “Hacking Blind.” In *2014 IEEE Symposium on Security and Privacy*, 227–42, 2014. <https://doi.org/10.1109/SP.2014.22>.
      2. United States/Stanford University/DARPA
      3. 4ZJKXIU7
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. Created and released a tool, Braille, for automating vulnerability exploitation
         2. Discovered a vulnerability for a public/open source project (nginx)
         3. Gave all the theoretical details of how to create a new attack type
         4. Gave the source code of an already known vulnerability
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Used a toy closed-binary proprietary service with a stack vulnerability written by a colleague
         2. both the binary and source were kept secret.
         3. Did not test against real-world proprietary services
   2. ***Just-In-Time Code Reuse:  
      On the Effectiveness of Fine-Grained Address Space Layout Randomization***
      1. Snow, K. Z., F. Monrose, L. Davi, A. Dmitrienko, C. Liebchen, and A. R. Sadeghi. “Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization.” In *2013 IEEE Symposium on Security and Privacy*, 574–88, 2013. <https://doi.org/10.1109/SP.2013.45>.
      2. United States/Germany
      3. ETII5WQP (duplicate from another category)
      4. Ethical content: blah
      5. Summary of Ethical issues (implicit or explicit)
         1. Gave all the theoretical details of how to create a new attack type
         2. Implemented, but apparently did not release, a software framework for exploitation
         3. Include partial code snippets of an exploit on a CVE
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Underwent “much deliberation among the authors about ethical responsibilities”
         2. Believe that shedding light on fundamental weaknesses in current ways of thinking about exploit mitigation outweighs the potential downside of helping the next generation of hackers. If history serves any lesson it is that attackers will adapt and so must we in order to stay one step ahead. It is our hope that this work will inspire those more clever than ourselves to design more comprehensive defenses.
   3. ***Targeted Online Password Guessing: An Underestimated Threat***
      1. Wang, Ding, Zijian Zhang, Ping Wang, Jeff Yan, and Xinyi Huang. “Targeted Online Password Guessing: An Underestimated Threat,” 1242–54. ACM Press, 2016. <https://doi.org/10.1145/2976749.2978339>.
      2. China/UK
      3. M4XHWUUF
      4. Ethical content: N
      5. Summary of Ethical issues (implicit or explicit)
         1. Used 100 million publicly released passwords and other info such as SSNs that hackers/insiders leaked
         2. Showed the top 10 passwords for some services
         3. correlated or matched passwords from multiple accounts to the same persons
         4. Cracked leaked hashed passwords
         5. No IRB approval, etc.
         6. Gave no indication of whether they stored or deleted data collected long-term
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. The information was already apparently publicly available
         2. The passwords are, in a sense, common knowledge, and could be helpful for creating tools to inform people to change their passwords
         3. No actual discussion of ethics
         4. Did not release any data outside of their paper
   4. ***You Needn’t Build That: Reusable Ethics‐Compliance Infrastructure for Human Subjects Research***
      1. Schechter, Stuart, Christian Bravo-Lillo, Cormac Herley, Serge Egelman, and Janice Tsai. “You Needn’t Build That: Reusable Ethics-Compliance Infrastructure for Human Subjects Research.” Accessed June 29, 2017. <https://www.caida.org/workshops/creds/1305/slides/creds1305_sschechter.pdf>.
      2. USA/Microsoft
      3. N9K4XX29
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. N/A?
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Claim: Researchers rarely engage in science with the primary goal of minimizing the risk to participants. Ethics as a secondary task includes:
         2. Anticipating harms or reactions
         3. Writing consent forms
         4. Investigating whether any participant felt harmed as a result of being part of a study
         5. Determining how well disclosures (e.g., post‐ deception) ameliorate concerns or feelings of harms
         6. Q: Can we make the most ethical path the easiest?
         7. Solutions: 1) Surrogate participants are asked how they would react to an  
            hypothetically‐posed experiment
         8. Surrogate participants are asked how they would react to an  
            hypothetically‐posed experiment (i.e., submit description of your planned experiment, receive surrogates’ responses, see how your experiment ranks against other experiments (some classic, some planned)).
         9. Solutions: 2) Consent‐form building tools (split into small pages to make material easier to digest, paired with questions about key facts to disclose)
         10. Solutions: 3) Post‐debriefing measures of harm, e.g. Please complete the following sentence: If someone I cared about was considering participating in this experiment, I would… “discourage/encourage them”
   5. ***Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge***
      1. Reaves, Bradley, Ethan Shernan, Adam Bates, Henry Carter, and Patrick Traynor. “Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge,” 2015.
      2. United States
      3. NP87CEMI
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. N/A set up simboxes to receive traffic?
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Used pre-existing public data and their own cellular base station
         2. Legal and privacy concerns prevented them from receiving simbox audio from mobile operators (since the audio would be from callers who could not give their consent for such use), so they didn’t do that
         3. Also did not use simboxes internationally, which would have been illegal
   6. ***Learning Assigned Secrets for Unlocking Mobile Devices*** 
      1. Schechter, Stuart, and Joseph Bonneau. “Learning Assigned Secrets for Unlocking Mobile Devices.” In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 277–295. USENIX Association, 2015. <https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schechter.pdf>.
      2. Microsoft/EFF/Stanford
      3. PNNA6APD
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Collected what were likely user’s real pins
         2. Gave no indication of whether they stored or deleted data collected
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Collected users’ pins with their informed consent
         2. Emphasis added:
         3. “...[R]evealed that the PIN was a component of our  
            study. We used the study sign-up process to **inform participants** about the research in place of a standard informed  
            consent form. We did not volunteer to participants that we  
            would later give them the opportunity to participate in a  
            follow-up study.  
            Unlike our prior work, we **informed participants in advance that we would pay for each attention game they played**  
            even if they did not complete all 50—though we did provide  
            a significant bonus to those who completed the study. This  
            is more **consistent with ethical guidelines that participants  
            should know they may leave an experiment at any time without penalty**.  
            We paid participants at a rate designed to ensure they  
            received at least the highest minimum wage in the US. We  
            identified that this was research being performed by Microsoft Research. We responded to workers’ requests quickly  
            and, where terms of service allowed, monitored worker forums to identify any participant concerns we might address.  
            Our study was **approved by Microsoft Research’s institutional review system**. The second author, who was not  
            employed by Microsoft Research, contributed after the last  
            participant had already been recruited and **was not involved**  
            in the conduct of the experiments or analysis of raw data.”
   7. ***Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network*** 
      1. Moreno-Sanchez, Pedro, Muhammad Bilal Zafar, and Aniket Kate. “Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network.” *Proceedings on Privacy Enhancing Technologies* 2016, no. 4 (January 1, 2016). <https://doi.org/10.1515/popets-2016-0049>.
      2. USA/Germany
      3. ME96ZDMA
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. deanonymized Ripple transactions/wallets: specifically, they linked Ripple/Ripple and Ripple/Bitcoin wallets together.
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. used publicly available data
         2. Used gateways services that are well known in the Ripple community and publicly advertised in their websites.
   8. ***A Large-Scale Empirical Analysis of Chinese Web Passwords*** 
      1. Zhigong Li, Weili Han, and Wenyuan Xu. “A Large-Scale Empirical Analysis of Chinese Web Passwords,” San Diego.
      2. China
      3. PQN2U3QV
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. Used publicly leaked password databases amount to 100 million passwords
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. “never utilized the leaked passwords for reasons other than understanding the overall statistical observation of passwords. “
   9. ***Should I Protect You? Understanding Developers’ Behavior to Privacy-Preserving APIs*** 
      1. Jain, Shubham, and Janne Lindqvist. “Should I Protect You? Understanding Developers’ Behavior to Privacy-Preserving APIs.” Internet Society, 2014. <https://doi.org/10.14722/usec.2014.23045>.
      2. USA
      3. PS6NPT4X
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. had students participate in a study, but didn’t obtain any kind of approval from a review board, or mention paying them; and didn’t discuss ethics regarding recruiting
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. participants were referred to by code names (anonymous participation)
   10. ***Know Thy Neighbor: Crypto Library Detection in Cloud***
       1. Irazoqui, Gorka, Mehmet Sinan IncI, Thomas Eisenbarth, and Berk Sunar. “Know Thy Neighbor: Crypto Library Detection in Cloud.” *Proceedings on Privacy Enhancing Technologies* 2015, no. 1 (2015): 25–40. <https://doi.org/10.1515/popets-2015-0003>.
       2. USA
       3. PXJSFTFZ
       4. Ethical content: N
       5. Summary of Ethical issues (implicit or explicit)
          1. Created an attack to detect what cryptographic library was being used on their own virtual machines? Or discovered a vulnerability?
       6. Summary of Ethical argument, if any (implicit or explicit)
          1. Proposed mitigations
   11. ***ByteWeight: Learning to Recognize Functions in Binary Code***
       1. Tiffany Bao, Jonathan Burket, Maverick Woo, Rafael Turner, and David Brumley. “BYTEWEIGHT: Learning to Recognize Functions in Binary Code,” San Diego.
       2. USA
       3. RTJV4MJJ
       4. Ethical content: C
       5. Summary of Ethical issues (implicit or explicit)
          1. N/A? - Created a tool for identifying functions in binaries
       6. Summary of Ethical argument, if any (implicit or explicit)
          1. They only reverse engineered open-source projects (probably to allow for ground-truth)
          2. Malicious or obfuscated binaries were out of scope
   12. ***Generic Attacks on Secure Outsourced Databases***
       1. Kellaris, Georgios, George Kollios, Kobbi Nissim, and Adam O’Neill. “Generic Attacks on Secure Outsourced Databases,” 1329–40. ACM Press, 2016. <https://doi.org/10.1145/2976749.2978386>.
       2. USA
       3. W3MZKITE
       4. Ethical content: C
       5. Summary of Ethical issues (implicit or explicit)
          1. None: Attacked a database containing datasets of hospital patients to recover records, but see below.
       6. Summary of Ethical argument, if any (implicit or explicit)
          1. Set up the servers and attacks on their own systems, and used a public use dataset (which is likely anonymized)
   13. ***Helping Johnny to Analyze Malware: A Usability-Optimized Decompiler and Malware Analysis User Study***
       1. Yakdan, K., S. Dechand, E. Gerhards-Padilla, and M. Smith. “Helping Johnny to Analyze Malware: A Usability-Optimized Decompiler and Malware Analysis User Study.” In *2016 IEEE Symposium on Security and Privacy (SP)*, 158–77, 2016. <https://doi.org/10.1109/SP.2016.18>.
       2. Germany
       3. **XBBPRKI2**
       4. **Ethical content: C**
       5. Summary of Ethical issues (implicit or explicit)
          1. decompiled malware for limited academic analysis
          2. Some malware comes with a license or has presumed copyright if it has none
       6. Summary of Ethical argument, if any (implicit or explicit)
          1. Obtained malware samples from legitimate malware analysts, who presumably would have obtained them via public means, e.g. typical malware distribution/infection channels.
          2. Didn’t use/reverse the full code
          3. But this seems totally ethical; therefore, reverse engineering pure malware should probably be ethical
          4. https://www.eff.org/issues/coders/reverse-engineering-faq#faq2
   14. ***Towards Automatic Software Lineage Inference***
       1. Jiyong Jang, Maverick Woo, and David Brumley. “Towards Automatic Software Lineage Inference,” Washington.
       2. USA/Lockheed Martin/DARPA
       3. Z57NCKD6
       4. Ethical content: C
       5. Summary of Ethical issues (implicit or explicit)
          1. Performed dynamic analysis on software, including malware
          2. disassembled malware as well as other software (to identify basic blocks)
       6. Summary of Ethical argument, if any (implicit or explicit)
          1. Analyzed open source “goodware” and used malware from a DARPA project (which may or may not have had source code – they had ground truth in terms of lineage, but that’s different from source code)
          2. downloaded only released versions of a program meant to be distributed to end users (but I think this is talking about versioning rather than copyright)
2. **Personal Information**

Keyword searches: user, inform, PII, ethic, data, personal, subject, delete, crim, moral, legal, safe, harm, remove, clean, scrape, malicious, malware, reverse, autono, medica, sample, equal, diverse, attack, vuln, report, disclos, notif, access, solution, code, program, script, sensitive, fair, crypt, save, record

* 1. ***Measuring the Practical Impact of DNSSEC Deployment*** 
     1. Wilson Lian, Eric Rescorla, Hovav Shacham, and Stefan Savage. “Measuring the Practical Impact of DNSSEC Deployment.” USENIX, Washington, D.C. <https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/lian>.
     2. USA
     3. 2XRQTI5X
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. recruited participants to a browser-based study via online ads
        2. “because our measurements were sensitive to the reliability of the participants’ Internet connections, we configured our ad campaign to target desktop operating systems, to the exclusion of mobile users”
        3. Did measurements on users who clicked on an ad…but didn’t describe what the ad looked like or if they informed users
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “Our experiment runs automatically without user interaction and is intended to measure the behavior and properties of **hosts** along the paths from users to our servers rather than the **users** themselves. We worked with...Human Research Protections Program...exempt from IRB review.”
        2. “In order to minimize sampling bias, our ad campaign did not target any particular keywords or countries. “
        3. “induces participants’ browsers to load 1×1- pixel images (“test resources”) from various domains.”
  2. ***Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways*** 
     1. Reaves, B., N. Scaife, D. Tian, L. Blue, P. Traynor, and K. R. B. Butler. “Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways.” In *2016 IEEE Symposium on Security and Privacy (SP)*, 339–56, 2016. <https://doi.org/10.1109/SP.2016.28>.
     2. USA
     3. 7NRRQ5GZ
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. “Our analysis tracks over 400 phone numbers in 28 countries over the course of 14 months, resulting in a dataset of 386,327 messages”
        2. We cluster and characterize the lifetime, volume and content of the traffic seen in SMS gateways.
        3. Determined whether a message was of a strictly personal nature (even though they didn’t analyze the messages further), e.g. contained credit card numbers (found many) and identification numbers like SSNs (found none), using a combination of automatic and manual inspection.
        4. May or may not have deleted sensitive data after the fact
        5. May or may not have read sensitive data on purpose (e.g. “to determine its sensitive nature”). Depending on what the data is, this might not be good enough.
        6. May or may not have attempted to contact services or operators to notify them of their findings.
        7. Did not discuss solutions?
        8. Discovered financial information, login information, password reset links, contact information, and content from sensitive applications
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. these messages are known by the recipient to be publicly available
        2. Most messages were related to account creation/recovery, or one-time passwords
        3. “because it is clear that all messages sent to these gateways are public, and their use is strictly ”opt-in”, users have no reasonable expectation of privacy in the collection and analysis of this data.”
        4. “Although we study bulk institutional messages, we do not analyze further those messages determined to be of a strictly personal nature. While those messages may have a research value, we deliberately avoid these messages to prevent further propagating this data.”
        5. “when personally identifying information (PII) or account credentials are sent to a gateway (whether or not all parties are aware), the compromise of that information is immediate and irrevocable.” “Except perhaps by the gateway itself; however, it is clear from our data that gateways are not taking steps to prevent PII exposure” “Because we do not make our data available to others, this study does not change — in severity or duration — the harm done by the existence and use of the gateway.” “Furthermore, while in Section V-A we describe a host of sensitive information found in the dataset, we do not publish, use, or otherwise take advantage of this information. In particular, we especially do not attempt to **access** accounts owned by gateway users or operators.”
        6. “Our data augmentation is sufficiently course-grained that [only one] individual user of a gateway [was] identified through our additional data. Geographic information not already disclosed in text messages was limited to country-scale records in the case of gateway users and cityscale in the case of gateway numbers (which in any case do not likely correlate with the location of the gateway operator).”
        7. “Overall, our hope is this study would raise awareness of the risks of sending sensitive information over insecure media and prevent future harm.”
        8. We do not attempt to deanonymize, track, or identify any users.
  3. ***Authentication Using Pulse-Response Biometrics***
     1. Rasmussen, Kasper Bonne, Marc Roeschlin, Ivan Martinovic, and Gene Tsudik. “Authentication Using Pulse- Response Biometrics.” In *The Network and Distributed System Security Symposium (NDSS)*, 2014. <https://ora.ox.ac.uk/objects/uuid:e7b4a968-24c0-43b7-8d11-0634e9112641>.
     2. USA/UK
     3. 782ZUEDW
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Collected pulse-response biometric information by subjecting subjects to low-voltage electrical pulses
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Used a pilot study to determine the minimum current and voltage users were subjected to, which was well below safe levels used in commercial devices
        2. “All subjects were given detailed information about the nature of the experiment beforehand and all were given the opportunity to opt out [presumably in the middle of the experiment]. None expressed any discomfort or, in fact, any perception of the current during the experiments.”
        3. Thoroughly considered safety and ethics
  4. ***Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems***
     1. Shaik, Altaf, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems.” Internet Society, 2016. <https://doi.org/10.14722/ndss.2016.23236>.
     2. Germany/Finland
     3. F6TXQ8RE
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. created and executed “the first practical attacks” attacks on (LTE) mobile devices to leak their [coarse] location and/or deny them service that they believe all LTE devices on the market are vulnerable to
        2. Investigated and discovered vulnerabilities in LTE
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “We reported our attacks to the manufacturers and carriers concerned as well as to the standardization body (3GPP). Remedial actions are under way while writing”
        2. “Our reports were acknowledged by all vendors and network operators we  
           contacted. For those vendors who have a standard responsible disclosure process in place, we followed the process.”
        3. “Two of them have already released patches. Two of three operators have fixed the configuration issues in their networks. 3GPP has initiated several updates to the LTE specifications to address the issues we raised.”
        4. “Specification of a large system like LTE is a complex endeavor involving many trade-offs among conflicting requirements. Rather than merely report on LTE vulnerabilities and attacks, we also discuss possible considerations that may have led to the vulnerabilities in the first place. Based on this we suggest some general guidelines for future standardization as well as specific fixes for our attacks.”
        5. Purchased/acquired legitimate open-source-based hardware/software to do their experiments
        6. “In addition, we modified the telephony protocol dissector available in Wireshark to decode all messages exchanged between the rogue eNodeB and UE. These modifications are submitted to the Wireshark project and are being merged into the mainstream application”
        7. “We carried out most of the active attacks in a Faraday cage to avoid affecting other UEs. For attacks in real LTE networks, we took care not to interrupt normal service to other UEs in the testing zone.”
        8. thoroughly discuss the details of the vulnerabilities they found, and solutions
  5. ***Survey on the Fate of Digital Footprints after Death***
     1. Grimm, Carsten, and Sonia Chiasson. “Survey on the Fate of Digital Footprints after Death.” Internet Society, 2014. <https://doi.org/10.14722/usec.2014.23049>.
     2. Germany/Canada
     3. IRWTE8QZ
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. “It remains an open question whether...the topic of the survey is considered taboo in these countries”
        2. conducted a survey about digital death, but this isn’t much different from any other survey…
        3. Discussed in detail the general results of their survey
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “Due to its sensitive nature, all sections are optional and only shown when participants agree to share their experiences.”
        2. “participants are shown the consent form informing them about the purpose of the study and their rights.”
        3. “The survey collects no sensitive information and participants remain anonymous.”
        4. “Participants can withdraw from the survey at any time and can always opt to skip a question should they feel uncomfortable answering it.”
        5. “The study design was reviewed and approved by the Research Ethics Board of Carleton University.”
        6. “We asked three colleagues to review the instructions, the consent form and the questionnaire for clarity and appropriateness of language. Two of these colleagues were native English speakers.”
  6. ***Conducting Ethical yet Realistic Usable Security Studies***
     1. Margulies, Ronen, and Amir Herzberg. “Conducting Ethical yet Realistic Usable Security Studies.” Accessed June 29, 2017. <https://www.caida.org/workshops/creds/1305/slides/creds1305_rmargulies.pdf>.
     2. Israel
     3. JI76RMFJ
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. N/A...pretty short presentation
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Introduced an outline of a design for user studies, although it seems focused on one particular type of study...but basically “Awareness + Long‐Term” makes things Realistic and apparently Ethical…
        2. Use a positive reward instead of using real sensitive accounts…
  7. ***Ethics in Security Research: Which Lines Should Not Be Crossed?***
     1. Schrittwieser, Sebastian, Martin Mulazzani, and Edgar Weippl. “Ethics in Security Research: Which Lines Should Not Be Crossed?” Accessed June 29, 2017. <https://www.caida.org/workshops/creds/1305/slides/creds1305_sschrittwieser.pdf>.
     2. Austria
     3. MNZEKKR8
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Discussed a number of papers/issues. Those are detailed below. All of these papers were published prior to the Menlo Report, and thus were not included in the papers we collected or analyzed.
        2. Case 1: “Watching without helping, even though the researchers knew which computers were infected and simply watched without taking actions; Victims were only informed after the experiments”
        3. Case 2: “Intercepting a “legal botnet” ([SETI@home](mailto:SETI@home)) would be unethical; Is a similar activity ethical simply because it is aimed at “bad” people?; No argument of self-defense can be made! “some [...] contents have already been widely and publicly documented. Consequently, we cannot create any new harm simply through association with these entities or repeating these findings””...is what everyone says
        4. Case 3: ““we believe that realistic experiments are the only way to reliably estimate success rates of attacks in the real-world” Does not solve the ethical dilemma!”
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “InfoSec research community is well aware of ethical questions within their field
        2. However, even the most fundamental ethical principles are difficult to fulfill
        3. Things are changing fast in information technology. Threat of guidelines that do not reflect the actual technological environment?”
  8. ***Understanding Saudis’ Privacy Concerns When Using WhatsApp*** 
     1. Rashidi, Yasmeen, Kami Vaniea, and L. Jean Camp. “Understanding Saudis’ Privacy Concerns When Using WhatsApp.” In *Proceedings of the Workshop on Usable Security (USEC’16)*, 2016. <http://www.vaniea.com/papers/usec2016.pdf>.
     2. USA/Scotland/Saudia Arabia
     3. N9RBFQA2
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Discussed in detail the general results of their survey
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “Participants did not receive any compensation. The participants were informed that we are studying WhatsApp privacy settings and the work was approved by our IRB.”
  9. ***Towards a Model on the Factors Influencing Social App Users’ Valuation of Interdependent Privacy*** 
     1. Pu, Yu, and Jens Grossklags. “Towards a Model on the Factors Influencing Social App Users’ Valuation of Interdependent Privacy.” *Proceedings on Privacy Enhancing Technologies* 2016, no. 2 (2015): 61–81. <https://doi.org/10.1515/popets-2016-0005>.
     2. USA
     3. N55ZZ2AT
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. N/A?
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “We paid $0.50 and $1.00 to each participant in the screening task and the app ranking task, respectively. Our study followed a protocol reviewed and approved by our university’s IRB.”
  10. ***Cross-Device Tracking: Measurement and Disclosures***
      1. Brookman, Justin, Phoebe Rouge, Aaron Alva, and Christina Yeung. “Cross-Device Tracking: Measurement and Disclosures.” *Proceedings on Privacy Enhancing Technologies* 2017, no. 2 (2017): 133–148. <https://doi.org/10.1515/popets-2017-0020>.
      2. USA FTC
      3. S6JCEB73
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Browsed (or crawled, or at least navigated to) the Alexa top 20 websites
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. The Alexa top 100 probably expect a ton of traffic, so it doesn’t degrade their service to scrape them.
         2. Might not have actually crawled the sights – just literally browsed to them 4 times?
         3. Used an open source program developed by a reputable research university to conduct the study
         4. Used their own accounts...even though they were fake? What about Facebook? It’s against their ToS, but that just means your fake account, if discovered, might be deleted…
         5. Since they used OpenWPM, I’m not sure how it worked, but worst case scenario is it scraped; best case is it just saved some stuff already saved in the browser.
  11. ***CrossFire: An Analysis of Firefox Extension-Reuse Vulnerabilities***
      1. Salih Buyukkayhan, Ahmet, Kaan Onarlioglu, William Robertson, and Engin Kirda. “CrossFire: An Analysis of Firefox Extension-Reuse Vulnerabilities.” Internet Society, 2016. <https://doi.org/10.14722/ndss.2016.23149>.
      2. USA
      3. SF8F8GUA
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. “identify a novel extension-reuse vulnerability that allows adversaries to launch stealthy attacks against users.”
         2. Introduce a tool that automatically detects the vulnerability and produces proof-of-concept exploits
         3. included snippets of exploit code in their paper that are apparently complete, even though they’re short?
         4. Submitted an extension containing an exploit to the Mozilla Add-ons repository
         5. Didn’t report vulnerabilities to extension maintainers or Firefox? But apparently fixing them is hard?
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Used a harmless URL in their extension, but since it is still a real attack, they took other precautions:
         2. “We have never publicly advertised our extension, and we  
            took it down from the repository promptly after receiving the  
            acceptance notification. We did not record or otherwise track  
            any activity on the sample domain that might have taken place  
            during the vetting of our extension. Finally, we performed  
            this case study only once to avoid unnecessarily burdening  
            the extension reviewers. “
         3. gave references to two other papers that did similar things recently (one of which I already analyzed: Jekyll on iOS)
         4. Gave the theoretical details of the vulnerability, etc.
         5. Opted for the highest level of review scrutiny of their extension when submitting it
  12. ***Ad Injection at Scale: Assessing Deceptive Advertisement Modifications***
      1. Thomas, K., E. Bursztein, C. Grier, G. Ho, N. Jagpal, A. Kapravelos, D. Mccoy, et al. “Ad Injection at Scale: Assessing Deceptive Advertisement Modifications.” In *2015 IEEE Symposium on Security and Privacy*, 151–67, 2015. <https://doi.org/10.1109/SP.2015.17>.
      2. USA/Spain/Google/Databricks
      3. TV67W4J5
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Scanned/scraped websites, collecting telemetry data for over 1 million page views
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. “contacted the Chrome Web Store and the advertisers targeted  
            by ad injectors to alert each of the deceptive practices involved.” “reported these to the Chrome Web Store, who confirmed  
            they violated the Web Store’s policies around deceptive ad  
            injection1 and subsequently disabled the extensions” “Our techniques for catching these extensions are now used by Google to scan new and updated extensions.”
         2. “Our data collection technique is analogous to Content Security Policies, which modern browsers use to report client-side telemetry of page integrity to website  
            operators. Prior to deploying our system, Google’s internal  
            privacy review board (similar to an IRB) vetted and approved  
            our architecture and the data it collects. Part of the restrictions  
            placed on our system include never analyzing data in non- aggregate form; never tracking or analyzing the behavior of  
            individual users; never sharing raw data outside of Google; and  
            setting a short lifetime on the data collected after which only  
            aggregates could be stored. We also verified that our system  
            is compatible for all clients that we collect data from (e.g.,  
            there is no degradation in the client’s user experience due to  
            crashing) and that our system never interferes with ad injectors  
            or tampers with the client’s DOM, but only provides a passive  
            measure of ad injection in the wild.”
         3. “Furthermore, we only collect a relatively small sample of  
            clickchain data to minimize the ad revenue impact we have  
            on advertisers buying traffic from ad injectors. We make no  
            effort to obfuscate our IP address or evade any automated  
            clicking protections used by advertisers.”
  13. ***Would a privacy fundamentalist sell their DNA for $1000… if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences*** 
      1. Woodruff, Allison, Vasyl Pihur, Sunny Consolvo, Lauren Schmidt, Laura Brandimarte, and Alessandro Acquisti. “Would a Privacy Fundamentalist Sell Their DNA for $1000... If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences.” In *Symposium on Usable Privacy and Security (SOUPS)*, 4:2, 2014. <https://www.usenix.org/system/files/conference/soups2014/soups14-paper-woodruff.pdf>.
      2. USA/Google
      3. TV74XQ6P
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. surveyed people using Mechanical Turk and GCS, asking questions about their privacy opinions, personality, and reactions to select large companies
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. “was reviewed and approved by CMU’s IRB”
         2. Paid an average hourly compensation of 8.2, “roughly on par with the United States minimum wage and consistent with payment standards of the MTurk community.”
         3. With GCS, “Answers are anonymous and are not connected to personally identifiable information.”
  14. **An unattended study of users performing security critical tasks under adversarial noise**
      1. Kaczmarek, Tyler, Alfred Kobsa, Robert Sy, and Gene Tsudik. “An Unattended Study of Users Performing Security Critical Tasks under Adversarial Noise.” In *Proceedings of the NDSS Workshop on Useable Security*, 14, 2015. <https://pdfs.semanticscholar.org/47bf/ef22f3918641838e91d59b545c1c2ac6a032.pdf>.
      2. USA
      3. UD4IXXMW
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Subjected people to a variety of unexpected sounds
         2. Did not inform subjects of the true purpose/nature of the experiment?
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. “Experiments described in this paper were fully authorized by the Institutional Review Board (IRB) of our university, well ahead of the actual commencement of the study. The level of review was: Exempt, Category II.”
         2. Even the highest of the sounds were within the OSHA safe regulation levels
         3. We note that no sensitive data was harvested during the experiments and minimal identifying information was retained. In particular:  
            • As part of Bluetooth device pairing, participants were not asked to select any secret PINs or passwords. Instead, the 6-digit PIN was generated on the computer hidden from view and displayed on the Smartboard as well as their smartphone; they were then asked to compare the two PINs and confirm that they were identical.  
            • The hidden computer (iMac) used for pairing was periodically flushed of all collected device pairings.  
            • No names, addresses, phone numbers or other identifying information was collected from the participants.  
            • Although email addresses were solicited in order to deliver the participation reward, they were erased very soon thereafter.  
            • Video recordings of the experiments were (and still are) kept for study integrity purposes. However, we plan is to erase them before IRB expiration time.
  15. ***Over-The-Top Bypass: Study of a Recent Telephony Fraud***
      1. Sahin, Merve, and Aur?lien Francillon. “Over-The-Top Bypass: Study of a Recent Telephony Fraud,” 1106–17. ACM Press, 2016. <https://doi.org/10.1145/2976749.2978334>.
      2. France
      3. VQTTS8P2
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Calls a certain practice fraud, though some people might disagree
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Provided ample evidence and argument/justification for labeling the practice negatively
         2. Assessed the ethics and privacy implications of a variety of measurement techniques for their study, and then chose the most “ethical” one
         3. Used their own platform and phone numbers to measure phone calls
  16. ***Analyzing the Impact of Collection Methods and Demographics for Android’s Pattern Unlock***
      1. Aviv, Adam J., Justin Maguire, and Jeanne Luning Prak. “Analyzing the Impact of Collection Methods and Demographics for Android’s Pattern Unlock.” In *Proc. Workshop on Usable Security (USEC). Internet Society*, 2016. <https://www.internetsociety.org/sites/default/files/blogs-media/analyzing-the-impact-of-collections-methods-and-demographics-for-androids-pattern-unlock.pdf>.
      2. USA/Navy
      3. X5CPGFEV
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. Collected graphical password patterns from subjects on Mechanical Turk
         2. Collected information on handedness, gender, etc. about participants
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Gave an option to not enter a password but still receive compensation (by answering a series of questions)
         2. “Both studies were approved by our Institution Review Board and meet the ethical standards.”

1. **Security Behavior**

Keyword searches: user, inform, PII, ethic, data, personal, subject, delete, crim, moral, legal, safe, harm, remove, clean, scrape, malicious, malware, reverse, autono, medica, sample, equal, diverse, attack, vuln, report, disclos, notif, access, solution, code, program, script, sensitive, fair, crypt, save, record

* 1. ***SIBRA: Scalable Internet Bandwidth Reservation Architecture***
     1. Basescu, Cristina, Raphael M. Reischuk, Pawel Szalachowski, Adrian Perrig, Yao Zhang, Hsu-Chun Hsiao, Ayumu Kubota, and Jumpei Urakawa. “SIBRA: Scalable Internet Bandwidth Reservation Architecture.” Internet Society, 2016. <https://doi.org/10.14722/ndss.2016.23132>.
     2. China/Switzerland/Japan/Taiwan
     3. 4EFU9IQE
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Did a variety of experiments and implementations of network traffic studies
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Simulated their studies (e.g. an Internet-scale study using a “CAIDA dataset”) or conducted them on local devices
  2. ***Individual versus Organizational Computer Security and Privacy Concerns in Journalism***
     1. McGregor, Susan E., Franziska Roesner, and Kelly Caine. “Individual versus Organizational Computer Security and Privacy Concerns in Journalism.” *Proceedings on Privacy Enhancing Technologies* 2016, no. 4 (January 1, 2016). <https://doi.org/10.1515/popets-2016-0048>.
     2. USA
     3. 6FGUVS3V
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Interviewed journalists and journalistic media “organizational stakeholders”
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “entire protocol was IRB approved”
        2. Considered Menlo-report-type principles
        3. “made explicit efforts not to leave a digital trail that could later identify the participants we interviewed. When organizing interviews, we avoided corresponding directly with interview subjects via email in advance of the interview. Instead, the interviewer typically corresponded with an organizational leader who then suggested potential interviewees.”
        4. “were careful not to elicit any protected information which journalists would normally not share, such as details about specific stories or sources”
        5. “agreed not to publish organizations’ specific security protocols”
        6. “All participants agreed to being audio recorded during the interview and all participants answered all of the questions in the interview script”
  3. ***Neural Signatures of User-Centered Security: An fMRI Study of Phishing, and Malware Warnings***
     1. Neupane, Ajaya, Nitesh Saxena, Keya Kuruvilla, Michael Georgescu, and Rajesh K. Kana. “Neural Signatures of User-Centered Security: An FMRI Study of Phishing, and Malware Warnings.” In *NDSS*, 2014. <http://www.cis.uab.edu/saxena/docs/nskgk-ndss14.pdf>.
     2. USA
     3. 38TADPPB
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Performed brain-scans on users while they were presented with images of security-critical computer scenarios (but not actual scenarios)
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “Our study was approved by the Institutional Review Board (IRB) at our University. Care was taken to maximize the safety of the participants while being scanned by following standard practices. Their participation in the study was strictly voluntary. The participants signed an informed consent form prior to the study and were given the option to withdraw from the study at any point of time. Best practices were followed to protect the confidentiality and privacy of participants’ data acquired during the study by de-identifying the collected data.”
  4. ***Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia***
     1. Alghamdi, Deena, Ivan Flechais, and Marina Jirotka. “Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia.” In *SOUPS*, 297–308, 2015. [http://enigma.usenix.org/sites/default/files/soups15\_full\_proceedings.pdf#page=319](http://enigma.usenix.org/sites/default/files/soups15_full_proceedings.pdf" \l "page=319).
     2. UK
     3. 648WM8I9
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Conducted a survey over the phone (and saved phone numbers, perhaps?) with Saudis
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. IRB approved
        2. Adhered to the customs of the people they interviewed
  5. ***Unpacking security policy compliance: The motivators and barriers of employees’ security behaviors***
     1. Blythe, John M., Lynne M. Coventry, and Linda Little. “Unpacking Security Policy Compliance: The Motivators and Barriers of Employees’ Security Behaviors.” In *SOUPS*, 103–122, 2015. [https://www.usenix.org/sites/default/files/soups15\_full\_proceedings.pdf#page=125](https://www.usenix.org/sites/default/files/soups15_full_proceedings.pdf" \l "page=125).
     2. UK
     3. BWV5FJ8D
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Interviewed people about security behavior
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. The study received approval from the faculty ethics board
        2. Participants were interviewed individually, in a private room at their organization and upon arrival were asked to read an information sheet covering all aspects of the investigation, including the purpose of the study and what they were required to do. They then provided written informed consent. Upon study commencement, participants were first required to complete a demographic questionnaire.
        3. Upon completion of the study, participants were presented with a debrief sheet which fully explained the purpose of the investigation and re-emphasized participants right to withdraw their data. Participants were all entered into a prize draw to win a £50 Amazon voucher.
  6. ***PhishEye: Live Monitoring of Sandboxed Phishing Kits***
     1. Han, Xiao, Nizar Kheir, and Davide Balzarotti. “PhishEye: Live Monitoring of Sandboxed Phishing Kits,” 1402–13. ACM Press, 2016. <https://doi.org/10.1145/2976749.2978330>.
     2. France
     3. 8ZVHC4PI
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. “present a novel approach to sandbox live phishing kits that completely protects  
           the privacy of victims” but what about the privacy of everyone else?
        2. “perform a comprehensive real-world assessment of phishing attacks, their mechanisms, and the behavior of the criminals, their victims, and the security community involved in the process”
        3. monitored hundreds of phishing campaigns
        4. “researchers have never observed the way real victims interact with phishing kits because of obvious ethical reasons”
        5. “leverages a web honeypot to attract real attackers into installing phishing kits in a compromised web application”
        6. monitors hacker behavior
        7. roughly geolocated victims by IP address...i.e. people connecting to their server
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “a natural tension exists between conducting accurate, reproducible research and reducing the harm caused by the content that is being removed”
        2. “[There are two] main challenges that affect research on phishing attacks:  
           Should researchers notify affected parties in order to expedite take-down of phishing sites? Should researchers intervene to assist victims?”
        3. “As soon as *victims* are being enrolled into a honeypot experimental setup, ethical considerations cover all aspects related to the protection and perfect secrecy of user identities, as well as the secrecy of their credentials in case where they may be exposed during the attack” - possibly because victims didn’t break in, and breaking in = consent? So it’s okay to use honeypots on hackers?
        4. Ref: “T. Moore and R. Clayton. Ethical dilemmas in  
           take-down research. In Financial Cryptography and  
           Data Security. 2012”
        5. “our institution does not have an IRB, but we asked advice from the company legal department, and were granted permission”
        6. “We removed on a daily basis [non-phishing] malicious files including web shells, exploit kits, and drive-by download from the honeypot”
        7. “we were able to confirm that no user credentials were disclosed during our experiments”
        8. “To prevent sensitive data from being sent out of the user terminal, our system injects into all phishing pages a JavaScript component whose purpose is to replace any posted information with random data  
           before it is sent over the network. [If the visitor is not an attacker,] The injected code protects all potential *victims* as long as they have not explicitly deactivated JavaScript in their browsers. For those users who  
           may have deactivated JavaScript, our system also injects a  
           HTML noscript tag that redirects user to an error page so  
           that they would disconnect from the honeypot.”
        9. “One of the main goals of our system is to protect the users while being perfectly transparent for the attacker”
        10. “Our system allows only redirections to other pages hosted in our honeypot, and automatically intercepts and drops any other destination”
  7. ***Fixing Security Together: Leveraging trust relationships to improve security in organization***
     1. Kirlappos, Iacovos, and Martina Angela Sasse. “Fixing Security Together: Leveraging Trust Relationships to Improve Security in Organizations.” Internet Society, 2015. <https://doi.org/10.14722/usec.2015.23013>.
     2. UK
     3. ETMBS4J5
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. conducted a survey of a large number of persons at multinational organizations
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “The presence of organizations or institutions with  
           power to sanction untrustworthy behavior (e.g. ethics  
           committees or legislation) acts as a deterrent, usually depending  
           on the type, strictness and severity of punishment (e.g. the  
           threat of being excluded from a professional group).”
        2. “Participation was anonymous and participants were given an  
           informed consent form, assuring that they would not be  
           identified or followed up. After the interview, participants were  
           paid the equivalent of $40. We did not encourage participants  
           to tell us about security infractions, but simply asked about their  
           awareness of, and experience with, a set of corporate security  
           policies.”
  8. ***Social Engineering Attacks on Government Opponents: Target Perspectives***
     1. Marczak, William R., and Vern Paxson. “Social Engineering Attacks on Government Opponents: Target Perspectives.” *Proceedings on Privacy Enhancing Technologies* 2017, no. 2 (2017): 172–185. <https://doi.org/10.1515/popets-2017-0022>.
     2. USA/Canada
     3. FU5G7EMR
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. interviewed subjects from foreign countries
        2. examined interviewees computers and phones
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. “IRB-approved”
        2. “After concluding our intervention with a subject, we offered to  
           answer any additional subject questions, and provided  
           them with customized security advice (subjects were not  
           paid for their participation).”
        3. “We obtained verbal consent (in GCC countries) and  
           signed consent (in the US and UK) before proceeding.  
           Consent materials were available in both Arabic and  
           English.”
        4. Took measures to “reduce [their] susceptibility to remote tracking, and minimize the amount of information that authorities could recover if we were arrested”
        5. “implemented procedures to determine whether our electronic devices had been subject to surreptitious tampering”
        6. “All interviews in the GCC were conducted  
           at a place of the subject’s choosing, and we abided by all  
           conditions set by contacts”
        7. Performed various uses and examinations of interviewees devices at their request
  9. ***On the Mismanagement and Maliciousness of Networks***
     1. Zhang, Jing, Zakir Durumeric, Michael Bailey, Mingyan Liu, and Manish Karir. “On the Mismanagement and Maliciousness of Networks.” In *NDSS*, 2014. <http://www.internetsociety.org/sites/default/files/01_1_1.pdf>.
     2. USA/DHS
     3. FU5ZHCVN
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Performed an internet-wide analysis
        2. Posed the question, without attempting to address it (despite authoring the Menlo Report): Is it ethical to perform regular active scans of the Internet if it leads to a safer, more stable Internet?
        3. Used Zmap to scan SMTP servers, and may have conducted other scans too
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. For the majority of their analysis, used existing datasets or other projects that scan/listen to certain things on the Internet, in order to reduce their impact on networks
  10. ***EKHUNTER: A Counter-Offensive Toolkit for Exploit Kit Infiltration***
      1. Eshete, Birhanu, Abeer Alhuzali, Maliheh Monshizadeh, Phillip Porras, V.N. Venkatakrishnan, and Vinod Yegneswaran. “EKHunter: A Counter-Offensive Toolkit for Exploit Kit Infiltration.” Internet Society, 2015. <https://doi.org/10.14722/ndss.2015.23237>.
      2. USA
      3. GVFCNQP6
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. designed/developed a system that can exploit/compromise exploit kits and the identities of their operators…
         2. deployed exploit kits in a laboratory setting
         3. Reverse-engineered
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Mentioned that this should be used with appropriate legal authority or something
         2. Disclosed their exploit findings to law enforcement (i.e. they found vulnerabilities in malware, so the question is who to disclose to, if anyone)
         3. Refers the reader to past takedown operations involving law enforcement for guidance on the ethics of analyzing malware in the wild, e.g. blackbox pentesting exploit kits, etc.
         4. Basically say that the benefits of their findings outweigh the cost of publishing their tools – the ability to find vulnerabilities in hacker software > their ability to more effectively patch as a result of these findings…so that means that it’s not that vulnerability/exploit disclosure is ethical, but that the ethics depends on the target/intended beneficiary, since most readers aren’t malicious…? Like, it’s okay to publish vulnerabilities for regular users with the goal of patching, but what makes publishing them for malware is the exploitation...so they assume that the goals of users of your info are different...essentially assuming that somehow more good actors will combined produce more good than bad readers...really, a study on how many bad actors read these papers/how many readers are bad, and how many act on their knowledge, and how much the good community uses/benefits from it, would be good...it seems like we use security by obscurity to avoid publications being used by hackers...i.e. we assume since they’re long, academic, and not quickly searchable, hackers don’t use them...but if I were a hacker, I would probably use them. As a script kiddy, I’d probably find the quickest solution, but if I were a seasoned hacker, I’d use these papers. That means measuring this is going to be hard without just measuring traces of papers’ code, etc., in the wild.
         5. We believe that it is unlikely and overwhelmingly  
            difficult for developers of illegal blackhat tools to successfully  
            prosecute well-intentioned [researchers who reverse engineer their stuff], and the legal implications of reversing malware (at least in the US) are similar to EULA ones, which maybe are just civil liabilities?
  11. ***Privacy Challenges in the Quantified Self Movement – An EU Perspective***
      1. Leibenger, Dominik, Frederik Möllers, Anna Petrlic, Ronald Petrlic, and Christoph Sorge. “Privacy Challenges in the Quantified Self Movement – An EU Perspective.” *Proceedings on Privacy Enhancing Technologies* 2016, no. 4 (January 1, 2016). <https://doi.org/10.1515/popets-2016-0042>.
      2. Germany
      3. GWGIT9EM
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. surveyed users on an online platform re their opinions on the quantified self
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Gives insight on processing of personal data as relevant to the GDPR (which should prove useful for evaluating future papers)...but it only applies to the EU...and is sort of out of scope...also provides some info for US and Australian law.
         2. Summarizes that to process personal data in the EU, you need the subject’s unambiguous consent, a relevant legitimate interest or a contract with the subject, and not to contradict the subject’s rights (but they can still process anonymized data); whereas in the US, laws prohibit certain actions
  12. ***The Parrot is Dead: Observing Unobservable Network Communications***
      1. Houmansadr, A., C. Brubaker, and V. Shmatikov. “The Parrot Is Dead: Observing Unobservable Network Communications.” In *2013 IEEE Symposium on Security and Privacy*, 65–79, 2013. <https://doi.org/10.1109/SP.2013.14>.
      2. USA
      3. HCID86JC
      4. Ethical content: N
      5. Summary of Ethical issues (implicit or explicit)
         1. Find what amount to vulnerabilities (or just workarounds?) in censorship-evasion technology
         2. Provided details of attacks that censors can use, which could degrade Skype service somewhat for users
         3. Possibly performed real attacks between their own devices, but some of which necessarily used the real network, although it shouldn’t have affected other users
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Say that quality of service is not degraded that much (but this is to imply that state-level actors might use it, not that they did)
  13. ***Gracewipe: Secure and Verifiable Deletion under Coercion***
      1. Zhao, Lianying, and Mohammad Mannan. “Gracewipe: Secure and Verifiable Deletion under Coercion.” Internet Society, 2015. <https://doi.org/10.14722/ndss.2015.23258>.
      2. Canada
      3. IC5ZH4NM
      4. Ethical content: N
      5. Summary of Ethical issues (implicit or explicit)
         1. N/A?
      6. Summary of Ethical argument, if any (implicit or explicit)
  14. ***The Curious Case of the PDF Converter that Likes Mozart: Dissecting and Mitigating the Privacy Risk of Personal Cloud Apps***
      1. Harkous, Hamza, Rameez Rahman, Bojan Karlas, and Karl Aberer. “The Curious Case of the PDF Converter That Likes Mozart: Dissecting and Mitigating the Privacy Risk of Personal Cloud Apps.” *Proceedings on Privacy Enhancing Technologies* 2016, no. 4 (2016): 123–143. <https://doi.org/10.1515/popets-2016-0032>.
      2. Switzerland
      3. MGUH8D5E
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. built a web crawler that can retrieve the permissions from a large number of apps
         2. analyzed users’ Google Drive documents on their servers – requested/got permission for “full access” of their files
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. after generating the insights from  
            a user’s files, these files are deleted immediately from our  
            apps’ servers
         2. Had a displayed privacy policy
         3. only kept the “insights data presented to the user,” even though that seems pretty personal....
         4. Made it easy for the user to delete their “insights”
         5. Used HTTPS
         6. used MD5 to hash/anonymize emails (why only MD5?)
         7. never manually checked the database for users’ insights
         8. Used public domain images in their paper/fake data
         9. post(why?) IRB review “didn’t object to” publication
         10. For transparency, listed the components of their tool/analysis for users
         11. Users were informed about their stuff being outsourced to a third party
         12. Users were enrolled in a lucky draw for partcipation
         13. Made sure their users were informed about Google drive/had experience with it
  15. ***Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning***
      1. Almuhimedi, Hazim, Adrienne Porter Felt, Robert W. Reeder, and Sunny Consolvo. “Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning.” In *Symposium on Usable Privacy and Security (SOUPS)*, 4:2, 2014. <https://www.usenix.org/system/files/conference/soups2014/soups14-paper-almuhimedi.pdf>.
      2. USA/Google
      3. MJHA8W7S
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. recorded statistics of users’ browser activity
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Only the history status and decision are recorded; the URL  
            itself is not included in the statistics.
         2. reports are pseudonymous and cannot be traced
  16. ***CovertCast: Using Live Streaming to Evade Internet Censorship***
      1. McPherson, Richard, Amir Houmansadr, and Vitaly Shmatikov. “CovertCast: Using Live Streaming to Evade Internet Censorship.” *Proceedings on Privacy Enhancing Technologies* 2016, no. 3 (2016): 212–225. <https://doi.org/10.1515/popets-2016-0024>.
      2. USA/Google
      3. Q5BPUWKV
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. Uses screen scraping to stream popular websites’ content
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Potential collateral damage to services being used (e.g. youtube) (in order to target CovertCast?) are minimal and “more ethical” than not having a service that hides in another one...which might be true, but…
  17. ***Ethics of Internet Freedom Promotion***
      1. Corrigan-Gibbs, Henry, and Bryan Ford. “Ethics of Internet Freedom Promotion - Welcome to the World of Human Rights: Please Make Yourself Uncomfortable.” Accessed June 29, 2017. <https://www.caida.org/workshops/creds/1305/slides/creds1305_hcgibbs.pdf>.
      2. USA
      3. QKM5RX69
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. N/A
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. “Internet freedom orgs can draw ethical lessons  
            from human rights orgs” and suggested a few references
         2. “if an organization’s work has no measurable impact, then it is hard to argue that the work has an ethical basis.”
  18. ***Why Johnny Can’t Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems***
      1. Norcie, Greg, Jim Blythe, Kelly Caine, and L. Jean Camp. “Why Johnny Can’t Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems.” Internet Society, 2014. <https://doi.org/10.14722/usec.2014.23022>.
      2. USA
      3. R4CUUDWF
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. Studied users as they installed and used Tor in a lab environment and did a specified action with it (to test usability)
         2. Made recommendations somehow affecting Tor (had direct affiliation with the project)?
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. “Students were given lab credit for  
            participating in the study. Students who were not comfortable  
            participating in the study were given the option instead to write  
            a one-page essay on Tor’s basic functionality. The entire study  
            is IRB approved.”
         2. Subjects were transparently informed of the purpose of the study and what the researchers were looking for
  19. ***An Exploratory Ethnographic Study of Issues and Concerns with Whole Genome Sequencing***
      1. De Cristofaro, Emiliano. “An Exploratory Ethnographic Study of Issues and Concerns with Whole Genome Sequencing.” Internet Society, 2014. <https://doi.org/10.14722/usec.2014.23020>.
      2. UK
      3. UA3UNATA
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. Conducted experimental interviews with subjects on their opinions on privacy and ethics issues in genomic sequencing
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. IRB approved
  20. ***NoPhish App Evaluation: Lab and Retention Study***
      1. Canova, Gamze, Melanie Volkamer, Clemens Bergmann, and Benjamin Reinheimer. “NoPhish App Evaluation: Lab and Retention Study.” Internet Society, 2015. <https://doi.org/10.14722/usec.2015.23009>.
      2. Germany
      3. ZANPQTZ3
      4. Ethical content:
      5. Summary of Ethical issues (implicit or explicit)
         1. did a lab experiment and a follow-up retention study on phishing security knowledge
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Did not mention phishing in the recruitment to avoid having subjects prepare for the study
         2. Offered some food and random rewards for participants
         3. explained the purpose of the study at the start, and did not require participants to complete it
         4. subjects were given informed consent forms
         5. Subjects were informed that they couldn’t receive the reward if they left early

1. **(new) Cryptography**

Keyword searches: user, inform, PII, ethic, data, personal, subject, delete, crim, moral, legal, safe, harm, remove, clean, scrape, malicious, malware, reverse, autono, medica, sample, equal, diverse, attack, vuln, report, disclos, notif, access, solution, code, program, script, sensitive, fair, crypt, save, record

* 1. ***TLS in the Wild: An Internet-wide Analysis of TLS-based Protocols for Electronic Communication***
     1. Holz, Ralph, Johanna Amann, Olivier Mehani, Matthias Wachs, and Mohamed Ali Kaafar. “TLS in the Wild: An Internet-Wide Analysis of TLS-Based Protocols for Electronic Communication.” Internet Society, 2016. <https://doi.org/10.14722/ndss.2016.23055>.
     2. Australia/USA/Germany
     3. 2XCACQFQ
     4. Ethical content: E
     5. # of matching raw data nodes:
     6. Summary of Ethical issues (implicit or explicit)
        1. Performed Internet-wide active scans (zmap)
        2. observed passive traffic of users
        3. examined nine days of  
           traffic of the Internet uplink of the University of California at  
           Berkeley using Bro, collecting ~10,000,000 SSL/TLS connections
     7. Summary of Ethical argument, if any (implicit or explicit)
        1. The campus administration has approved this data collection
        2. the University IRB takes the position that IP addresses, which  
           were also recorded for this measurement, are not treated as  
           personally identifiable (although according to the GDPR it IS now PII…)
        3. For the SSL/TLS measurements, the information that we save is constrained to  
           information in the SSL/TLS handshake without analysing any  
           later connection payload data.
        4. For the capability measurements only automatic server capability replies were recorded, which do not contain any personally identifiable information
        5. We refrained from scanning at line speed to reduce our scans’ impact.
        6. used a blacklist of IP ranges generated during pastscans
  2. ***Linking Health Records for Federated Query Processing***
     1. Dewri, Rinku, Toan Ong, and Ramakrishna Thurimella. “Linking Health Records for Federated Query Processing.” *Proceedings on Privacy Enhancing Technologies* 2016, no. 3 (2016): 4–23. <https://doi.org/10.1515/popets-2016-0013>.
     2. USA
     3. IKJ7FXS7
     4. Ethical content: N
     5. Summary of Ethical issues (implicit or explicit)
        1. The data sets referred to in the subsequent sections  
           are derived from a North Carolina Voters Registration database obtained in 2012 (ncsbe.gov/ncsbe/datastatistics). This database contains 7,088,370 individual  
           records with demographic data. We use the name and  
           street address attributes in this study. The name attribute is a concatenation of the first name, the middle name, and the last name. Similarly, the street address is  
           composed of the house number, street direction, street  
           name, and the street type, concatenated in that order.  
           We standardized all records to use upper case characters, and removed any blank space appearing in a name or a street address. This database also reflects input  
           errors typically seen in the real world.
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Voter registration data is public record and available for researchers (usually for some fee)
  3. **Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple IMessage**
     1. Garman, Christina, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan. “Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple IMessage,” 2016.
     2. USA
     3. UI3DTACP
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. analyze the iMessage protocol
        2. derived a specification for iMessage by conducting a partial black-box reverse engineering of the protocol; extend a high-level protocol overview published by Apple and two existing partial reverse-engineering efforts
        3. uncovered several previously unreported vulnerabilities in the iMessage protocol
        4. identifed a practical adaptive chosen ciphertext attack on the iMessage encryption mechanism that allows us to retrospectively decrypt certain iMessage payloads and attachments
        5. One weakness we exploit has been identifed by the reverse engineering efforts in [34], while another is novel
        6. implemented a proof of concept
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Reported results to Apple in November, and waited until after March when substantial patches covering most of the repairs were shipped before publishing
        2. vulnerability was straightforward to repair
        3. provide mitigations
        4. tested exploit against their own test devices

1. **(New) Machine Learning**  
   Keyword searches: user, inform, PII, ethic, data, personal, subject, delete, crim, moral, legal, safe, harm, remove, clean, scrape, malicious, malware, reverse, autono, medica, sample, equal, diverse, attack, vuln, report, disclos, notif, access, solution, code, program, script, sensitive, fair, crypt, save, record
   1. **Blogs, Twitter Feeds, and Reddit Comments: Cross-Domain Authorship Attribution**
      1. Overdorf, Rebekah, and Rachel Greenstadt. “Blogs, Twitter Feeds, and Reddit Comments: Cross-Domain Authorship Attribution.” *Proceedings on Privacy Enhancing Technologies* 2016, no. 3 (2016): 155–171. <https://doi.org/10.1515/popets-2016-0021>.
      2. USA
      3. CESMCPP8
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. created a high-accuracy stylometry tool with applications to in-field accounts on blogs, twitter fields, and reddit comments
         2. collected publicly posted data on thousands of linked twitter/wordpress and twitter/reddit accounts
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. looked at a few case studies of instances  
            in which an account was initially created as an anonymous account, but the author later came forward and acknowledged the account
         2. consider cases in which the authors explicitly linked to their accounts in other domains
         3. (didn’t mention releasing their implementation; and also didn’t come up with the initial algorithm anyway)
   2. **Dynamic Cognitive Game Captcha Usability and Detection of Streaming-Based Farming**
      1. Mohamed, Manar, Song Gao, Nitesh Saxena, and Chengcui Zhang. “Dynamic Cognitive Game Captcha Usability and Detection of Streaming-Based Farming.” In *The Workshop on Usable Security (USEC), Co-Located with NDSS*, 2014. <https://www.cis.uab.edu/saxena/docs/mgsz-usec14.pdf>.
      2. USA
      3. QCBKT3A4
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Conducted 2 M turk user studies (one with 40, one with 80 users)
         2. design and evaluate a Stream Relay attack detection mechanism
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Due to the legal restrictions on attacking commercial DCG  
            CAPTCHAs, we proceeded to develop our own animationbased DCG prototypes for the purpose of our study
         2. The project was approved by our University’s Institutional Review Board
         3. paid $0.5 for efforts that took approximately ten minutes.
         4. The MTurk workers were subjected to a consent agreement,  
            and a demographics form before the experiment
   3. **Analyzing Unique Bid Auction Sites for Fun and Profit**
      1. Samorodnitzky, Ory, Eran Tromer, and Avishai Wool. *Analyzing Unique Bid Auction Sites for Fun and Profit*. Tel Aviv University, 2013. <http://www.cs.tau.ac.il/~tromer/papers/uniquebid.pdf>.
      2. Israel
      3. RBSKN3KS
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. extracted 105 auctions traces, containing every bid and its time
         2. used simplest of our strategies in an actual leading Highest Unique-Bid Auctions site
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. **Did not claim winnings**; ensures that the auction owner is not harmed financially (in fact it **increases the owner’s** **profits**)
         2. Conducting live experimentation with unique-bid auctions affects both the site owner and auction participants.
         3. experiments would not have caused the auction site an immediate monetary loss, since all our bids were **properly paid for**
         4. If there is any harm to the site, it is  
            **indirect**: an automated strategy with a high win probability  
            may undermine the **perception of fairness** of the auctions.
         5. We do acknowledge that our experiments did **harm** some of the auction **bidders**, by **lowering each individual’s chance of winning**; for a heavy bidder this could be quantified as monetary loss of a few pounds per auction.
         6. However, at the time we conducted out experiments at  
            the UK site (during July 2011), the site’s Terms of Service **(ToS) did not forbid** automated bidding. Only after our work (and perhaps in part because of our work), the **site actually changed the ToS** to include language that specifically forbids automated bidding. Hence, the site owner, and the other players, that should have read the ToS that was in force at the time, **could have anticipated that automated players may participate**. Therefore one can argue that they assumed the risk knowingly, or at least by default.
         7. approved by the Tel Aviv University ethics committee
   4. **Towards Detecting Anomalous User Behavior in Online Social Networks**
      1. Bimal Viswanath, M. Ahmad Bashir, Mark Crovella, Saikat Guha, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. “Towards Detecting Anomalous User Behavior in Online Social Networks,” San Diego.
      2. Germany/USA/India
      3. WR32NB34
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. using over two years of complete user behavior data from nearly 14K Facebook users, 92K Yelp users, and 100K Twitter users (all sampled uniformly at random)
         2. used Selenium to crawl the publicly visible data for these users, covering 2.16M publicly-visible likes and an additional 1.19M publicly-visible Timeline posts including messages, URLs, and photos. We acquired all activity data for these users from their join date until end of August 2013
         3. acquired traffic from multiple black-market services, identified compromised users,  
            and obtained users who are part of incentivized collusion networks
         4. apply our technique to detect anomalous ad clicks on the Facebook ad platform
         5. obtained 2,259 likes on three Facebook pages we created, obtaining a set of 2,210 users, at an average cost of around $25 for 1,000 likes
         6. crawled the user activity of the users we found through collusion networks.  
            We collected 359,848 likes and 186,474 Timeline posts
         7. installed the malware Febipos.A in a sandbox and deobfuscated / analyzed the code
         8. reverse-engineered protocol between the browser component and the CnC server
         9. used curl to semi-passively monitor the entire activity of the malware for August 21–30, 2013
         10. used Facebook’s graph search ([https://en.wikipedia.org/wiki/Facebook\_Graph\_Search#Privacy](https://en.wikipedia.org/wiki/Facebook_Graph_Search" \l "Privacy))
         11. We collected the publicly visible like and Timeline [34] activity of 13,991 users over the 26 month period ending in August 2013
         12. Used datasets from other papers: The Twitter dataset consists of a random sample of  
             100K out of the 19M Twitter users who joined before August 2009 [4]
         13. The Yelp dataset consists of all 92,725 Yelp reviewers in the San Francisco area [50] who joined before January 2010 and were active (wrote at least one review) between January 2010 and January 2012
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. all money we paid to acquire anomalous likes were exclusively for pages both controlled by us and setup for the sole purpose of conducting the experiments in this paper.
         2. For the malware analysis, we ensured that our sandbox prevented the malware from executing the CnC’s instructions.
         3. We did not seek or receive any account credentials of any Facebook user.
         4. Overall, we ensured that no other Facebook page or user was harmed or benefited as a result of this research experiment
         5. disclosed our findings to Facebook in March 2014, and included a preprint of this paper
         6. crawled the **publicly-visible user behavior** of the black-market users who liked our pages, and **publicly visible posts** yielding an additional 89,452 Timeline posts
2. **(New) Mobile and App Security**  
   Keyword searches: user, inform, PII, ethic, data, personal, subject, delete, crim, moral, legal, safe, harm, remove, clean, scrape, malicious, malware, reverse, autono, medica, sample, equal, diverse, attack, vuln, report, disclos, notif, access, solution, code, program, script, sensitive, fair, crypt, save, record
   1. **A Field Study of Run-Time Location Access Disclosures on Android Smartphones**
      1. Fu, Huiqing, Yulong Yang, Nileema Shingte, Janne Lindqvist, and Marco Gruteser. “A Field Study of Run-Time Location Access Disclosures on Android Smartphones.” Internet Society, 2014. <https://doi.org/10.14722/usec.2014.23044>.
      2. USA
      3. G4NCUJUV
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. Made an Android application to record the name of the installed applications that request current location, and the locations where they request it. The  
            app also records all installed applications, when the apps are installed or uninstalled, how long and when a given app is used, and when the phone is used.
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. those who were interested in participating in the study were required to be age 18 or over, own an Android phone and answer a short online entry survey. Participants were screened by the entry survey answers: they were qualified if they used location based apps in daily lives.
         2. We assigned randomly with a coin toss all participants prior to the appointment to either the No Disclosure group or the Disclosure group
         3. All participants were compensated with $25 gift certificates for participating for four weeks, and were included in a raffle for two $50 gift certificates
         4. study was approved by the Institutional Review Board (IRB) of Rutgers University
         5. Had participants sign a consent form, allowed them to opt out after signing, and explained the experiment to them beforehand
         6. The study consisted of four parts. All participants (1) went through an entry interview, (2) had the study app installed on their phones, (3) ran the app for about four weeks, and (4) participated in an exit interview and debriefing.
         7. The application does not record any additional pii (such as usernames).
         8. The exit interviews we conducted took a total of 7.5 hours for the  
            Disclosure group, and 4 hours for the No Disclosure group  
            (due to the smaller number of participants and fewer topics to  
            discuss)
   2. **Free for All! Assessing User Data Exposure to Advertising Libraries on Android**
      1. Demetriou, Soteris, Whitney Merrill, Wei Yang, Aston Zhang, and Carl A. Gunter. “Free for All! Assessing User Data Exposure to Advertising Libraries on Android.” Internet Society, 2016. <https://doi.org/10.14722/ndss.2016.23082>.
      2. USA
      3. Q2NZ5UX2
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. open sourced their code
         2. decompiled the 2700 apps we have collected from Google Play, into smali code
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. The protocol for all the parts of the study was approved by the Institutional Research Board (IRB) for our institution. All participants gave their informed consent. We required informed consent during both parts of the study, and participants could leave the study at any time. Participants were informed that the information collected in the survey and the information collected by the mobile app would be associated with one another
         2. Participants included individuals over the age of 18 willing  
            to participate in the survey and who owned an Android device
         3. Before taking the survey, participants were required  
            to give informed consent to the information collected in the survey
         4. In addition, our workers were not compensated until after the finished tasks were reviewed and approved by the survey conductors. Before taking the survey, participants were required to give informed consent to the information collected in the survey
   3. **Look before You Authorize: Using Eye-Tracking to Enforce User Attention towards Application Permissions**
      1. Javed, Yousra, and Mohamed Shehab. “Look before You Authorize: Using Eye-Tracking to Enforce User Attention towards Application Permissions.” *Proceedings on Privacy Enhancing Technologies* 2017, no. 2 (2017): 23–37. <https://doi.org/10.1515/popets-2017-0014>.
      2. USA
      3. QAZCAHD5
      4. Ethical content: C
      5. Summary of Ethical issues (implicit or explicit)
         1. analyzed the eye-gaze data of 16 participants on permission authorization dialog as they installed Facebook applications/connected them to their accounts
         2. A total of 105 participants completed the experiment
         3. We recruited our participants through Craigslist, and word of mouth
         4. We did not tell the participants that they were participating in a security/privacy related study
         5. Each participant completed a questionnaire at the end of the experiment
         6. The participants logged into their Facebook account
         7. Each participant completed a questionnaire at the end of the experiment
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. The experiments were approved by UNC Charlotte’s IRB
         2. paid each participant a $5 Starbucks gift card at the end of the study
         3. In order to maintain ecological validity, and more closely study participant behavior, some amount of deception was used.
         4. Participants also had the option of not installing an application (connecting it to Facebook)
         5. After the participants completed the questionnaire, we informed  
            them about the goal of our experiment/ debriefed them
   4. **Security Analysis of Emerging Smart Home Applications**
      1. Fernandes, E., J. Jung, and A. Prakash. “Security Analysis of Emerging Smart Home Applications.” In *2016 IEEE Symposium on Security and Privacy (SP)*, 636–54, 2016. <https://doi.org/10.1109/SP.2016.44>.
      2. USA
      3. QERTHZDV
      4. Ethical content: E
      5. Summary of Ethical issues (implicit or explicit)
         1. a static source code analysis of 499 SmartThings apps (called SmartApps) and 132 device handlers, and carefully crafted test cases that revealed many undocumented features of the platform
         2. exploited framework design flaws to construct four proof-of-concept attacks (some of which were done remotely)
         3. Open-sourced their analysis tools
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. conclude the paper with security lessons for the design of emerging smart home programming frameworks
         2. Upon completing the survey, compensated participants with a $10 gift card
         3. did not collect any private data except the email address for those  
            who would want to receive a gift card. The email address was  
            deleted after sending a gift card
         4. The survey was designed and conducted by researchers from our team who are at an institution that does not require review board approval (the other researchers were given restricted access to survey responses)
         5. We disclosed the vulnerabilities identified in this paper to  
            SmartThings on December 17, 2015. We received a response  
            on January 12, 2016 that their internal team will be looking  
            to strengthen their OAuth tokens by April 2016 based on  
            the backdoor pin code injection attack, and that other attack  
            vectors will be taken into consideration in future releases.  
            We also contacted the developer of the Android app that  
            had the OAuth client ID and secret present in bytecode.  
            The developer told us that he was in communication with  
            SmartThings to help address the problem. A possible approach  
            being considered was for a developer to provide a whitelist  
            of redirect URI possibilities for the OAuth flow to prevent  
            arbitrary redirection. The SmartThings security team sent us  
            a followup response on April 15, 2016.
3. **(new) Anonymity and Privacy**

Keyword searches: user, inform, PII, ethic, data, personal, subject, delete, crim, moral, legal, safe, harm, remove, clean, scrape, malicious, malware, reverse, autono, medica, sample, equal, diverse, attack, vuln, report, disclos, notif, access, solution, code, program, script, sensitive, fair, crypt, save, record

* 1. **Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem**
     1. Soska  Nicolas Christin, Kyle. “Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem,” 2015.
     2. USA
     3. 4ZFSJ3FE
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. methodology consists of 1) crawling  
           online anonymous marketplaces, and 2) parsing them
        2. scraped 35 different marketplaces a total of 1,908 times yielding a dataset of 3.2 TB in size. The total number of pages obtained from each scrape ranged from 27 to 331,691 pages and performing each scrape took anywhere from minutes up to five days
        3. In addition to being careful about what to request from  
           a marketplace, we obfuscate how we request content. For  
           each page request, the scraper randomly selects a Tor circuit out of 20 pre-built circuits. This strategy ensures that  
           the requests are being distributed over several rendezvous points in the Tor network. This helps prevent triggering anti-DDoS heuristics certain marketplaces use.5  
           This strategy also provides redundancy in the event that  
           one of the circuits being used becomes unreliable and  
           speeds up the time it takes to observe the entire site
        4. attempted to completely scrape websites
        5. We generally attempted a scrape for each marketplace once every two to three days unless the marketplace was either unavailable or the previous scrape had not yet completed
        6. Created accounts on these marketplaces
        7. Parsed scraped information into a database
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. manually identified sites that prohibit aggressive scraping (e.g., Agora) and  
           imposed appropriate rate limits
        2. We share much of the ethical concerns and views documented in previous work [13]. Our data collection, in particular, is massive, and could potentially put some  
           strain on the Tor network, not to mention marketplace  
           servers themselves. However, even though it is hard  
           to assess we believe that our measurements represent a  
           small fraction of all traffic that is going to online anonymous marketplaces. As discussed in Section 3 we are attempting to balance accuracy of the data collection with a light-weight enough crawling strategy to avoid detection  
           – or worse, impacting the very operations we are trying to  
           measure. In addition, we are contributing Tor relays with  
           long uptimes on very fast networks to “compensate” for  
           our own massive use of the network. Our work takes a  
           number of steps to remain neutral. We certainly do not  
           want to facilitate vendor or marketplace operator arrests.  
           This is not just an ethical question, but is also a scientific  
           one: our measurements, to be sound, should not impact  
           the subject(s) being measured [23].
        3. [13]: Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace
        4. [23]: The Heisenbot uncertainty problem: challenges in separating bots from chaff
  2. **Cloak and Swagger: Understanding Data Sensitivity through the Lens of User Anonymity**
     1. Peddinti, S. T., A. Korolova, E. Bursztein, and G. Sampemane. “Cloak and Swagger: Understanding Data Sensitivity through the Lens of User Anonymity.” In *2014 IEEE Symposium on Security and Privacy*, 493–508, 2014. <https://doi.org/10.1109/SP.2014.38>.
     2. USA
     3. 8V34HKZ3
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. crawled the Quora website using our own custom crawler  
           during the period of August - October, 2012.
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. We follow a similar approach as outlined in [42] for crawling Quora. Our  
           crawler observed the Quora’s robots.txt as well as rate-limited  
           our access. Furthermore, in order to limit the request load,  
           we only crawled the Quora question pages, and omitted all  
           other pages, such as answer pages, follower pages, activity  
           pages, views pages, and user profile pages. As a result, the  
           information we obtained about question followers is limited to  
           the followers listed at the bottom right of the Quora question  
           page (Figure 1), and does not include all question followers
  3. **Introducing Precautionary Behavior by Temporal Diversion of Voter Attention from Casting to Verifying Their Vote**
     1. Budurushi, Jurlind, Marcel Woide, and Melanie Volkamer. “Introducing Precautionary Behavior by Temporal Diversion of Voter Attention from Casting to Verifying Their Vote.” Internet Society, 2014. <https://doi.org/10.14722/usec.2014.23037>.
     2. Germany
     3. AHMPX5RX
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Deceived participants about the nature of their study
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Because of ethical concerns around manipulation, the study cannot be conducted during a legally binding election
        2. An alternative might be to simulate an election. However, in an election simulation voters are likely to select those candidates they would also select in a real election  
           which might lead to violation of vote secrecy. Thus, if a  
           participant identifies the manipulation, and reveals the name of the selected candidate that was replaced (due to manipulating the printout), we would violate vote secrecy. Therefore, the user study cannot simulate an election
        3. We are aware that related works, e.g. [5], [6] and [7], have simulated elections to evaluate whether voters verify or not the printouts
        4. At the end of the experiment participants were debriefed and asked to not talk about the experiment with other persons, in order to avoid biasing other potential participants
        5. An ethics commission at our university provides ethical requirements for research involving humans. These requirements were met; all participants read and confirmed the experimental guidelines, which stated that all data would be stored anonymously and serve only for the purpose of the experiment.
  4. **Safely Measuring Tor**
     1. Jansen, Rob, and Aaron Johnson. “Safely Measuring Tor,” 1553–67. ACM Press, 2016. <https://doi.org/10.1145/2976749.2978310>.
     2. USA
     3. PRAVDRJC
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. We build on this recent work to develop PrivCount, an efficient and flexible system for privacy-preserving measurement on Tor.
        2. develop an open-source tool implementing PrivCount that is robust,  
           secure, and particularly convenient to use for research on Tor
        3. use the PrivCount tool to perform a measurement study of Tor users and traffic with a scope similar to past work but with user privacy as a foremost consideration
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. PrivCount adds random noise to each counter in order to provide differential privacy to individual Tor user actions that contribute to its value.
        2. PrivCount protects bounded numbers of the following types of user actions in a given time period: (i) connection to a guard, (ii) using a guard from a distinct IP address, (iii) circuit creation, (iv) stream creation, (v) sending or receiving a byte of data
        3. We do note that differential privacy only provides privacy  
           for a limited amount of time and user activity, and an active user will eventually exceed that amount. Thus, as the number of measurement rounds increases, the chance of revealing something private about user activity increases
        4. Discuss additional privacy-preserving measures that could be added to their tool, and the limitations of their work
        5. Carefully considered the Tor Project’s safety guidelines when designing our measurements. We would highlight that we **practice data minimization by limiting the statistics we gather to just those needed** to understand the major features of client and exit traffic for purposes of modeling Tor (e.g. in Shadow [18]) and improving Tor’s performance. We also note that all of our **measurements are designed to preserve user privacy** and are safe to release publicly. Overall, measuring Tor while protecting users is a primary challenge addressed by this work.
        6. Because of the sensitivity of storing client IP addresses in memory, we **limit the amount of time over which we count per client statistics before clearing the map** to 20 minutes. This is **comparable to the default circuit lifetime** in Tor of 10 minutes, and we also note that the Tor Project takes a similar approach for maintaining statistics such as per-country user numbers but is currently storing client IP addresses over a much longer and **less-safe period of 24 hours**
  5. **On Realistically Attacking Tor with Website Fingerprinting**
     1. Wang, Tao, and Ian Goldberg. “On Realistically Attacking Tor with Website Fingerprinting.” *Proceedings on Privacy Enhancing Technologies* 2016, no. 4 (2016): 21–36. <https://doi.org/10.1515/popets-2016-0027>.
     2. Hong Kong/Canada
     3. SR8IF83U
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. Solves problems that prevented website fingerprinting (which allows a local, passive observer to determine a web-browsing client’s web activity over an encrypted channel) on Tor
        2. The code and data for our system is available for download
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. did not use cell sequences collected in the wild from real clients; it is necessary for us to obtain the client’s consent for such data collection
        2. **used preexisting data sets** from the Alexa top 5000 (1 instance per page), and a sensitive data set that “Contains 40 instances of 100 sensitive pages that are censored in individual ISPs of the United Kingdom, Saudi Arabia, or China”
        3. honest Tor exit nodes should not be examining the contents of the traffic passing through them
  6. **Website Fingerprinting at Internet Scale**
     1. Panchenko, Andriy, Fabian Lanze, Andreas Zinnen, Martin Henze, Jan Pennekamp, Klaus Wehrle, and Thomas Engel. “Website Fingerprinting at Internet Scale.” Internet Society, 2016. <https://doi.org/10.14722/ndss.2016.23477>.
     2. Luxembourg/Germany
     3. WFFE6CJY
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. we re-recorded the websites used in Wang et al with 100 instances each using our own approach. This allows us to extract all layers of data representation (i.e.,  
           also those where SENDME cells are included
        2. loaded the index page of each website in the Alexa Top list of the 20,000 most popular sites and followed a randomly chosen link on this page
        3. selected 20,000 English terms at random and entered them into Google Search, selecting pages from the results at random
        4. Used Twitter’s **API** to collect random tweets over 3 days
        5. operated a public Tor exit node and captured unencrypted HTTP requests from this exit node over a duration of one week (specifically extracted the HTTP referer element), collecting 211,148 unique web pages
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Used existing datasets (in addition to collecting new ones), all of which the authors claimed were inadequate for the task at hand
        2. We ensured that we never downloaded more than one instance of a single page through the same circuit
        3. The collection of URLs for the TOR-Exit dataset does not strictly follow the guidelines for ethical Tor research that were published after we finished our experiments. Still, we believe that it is important to know the degree of protection offered by the real Tor network. There can be no better evaluation than using those pages that are actually retrieved via Tor. While running our exit nodes, we made every effort to minimize any potential harm to the users and tried to examine all the risks that may exist. Our scripts **extracted and stored only the URLs** – without timestamps, traces or any other data. From these we **automatically removed all identifying information** such as a session identifier. Hence, with the information we stored there is only a minimal risk to harm the anonymity of Tor users. This complies with the recommendations for statistical analyses in the Tor network (except that we did not publicly discuss our algorithms before conducting the experiments). Furthermore, we **will not make this dataset** or parts of it **publicly available** before consulting the Tor research community and an appropriate ethics feedback panel such as the Ethics Feedback Panel for Networking and Security

1. **(new) Usable Security**

Keyword searches: user, inform, PII, ethic, data, personal, subject, delete, crim, moral, legal, safe, harm, remove, clean, scrape, malicious, malware, reverse, autono, medica, sample, equal, diverse, attack, vuln, report, disclos, notif, access, solution, code, program, script, sensitive, fair, crypt, save, record, consent, discard

* 1. **The Emperor’s New Password Manager: Security Analysis of Web-Based Password Managers**
     1. Li, Zhiwei, Warren He, Devdatta Akhawe, and Dawn Song. “The Emperor’s New Password Manager: Security Analysis of Web-Based Password Managers,” 2014.
     2. USA
     3. AE9TLB9B
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Identified severe vulnerabilties in every type of proprietary password manager
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. We experimentally verified all our attacks in an ethical manner. We reported all the attacks discussed below to the software vendors affected in the last week of August 2013. Four out of the five vendors responded within a week of our report, while one (NeedMyPassword) still has not responded to our report. Aside from linkability vulnerabilities and those found in NeedMyPassword, all other bugs that we describe in the paper have been fixed by vendors within days after disclosure. None of the password managers had a bug bounty program.
        2. One concern is how to ethically verify the My1login authorization flaw without sharing another user’s credential by mistake. We observed over multiple days that it is rare that any other user creates a new web card between 2am - 3am PST. We then verified this vulnerability one day between 2am and 3am without sharing another user’s credential by mistake.
        3. Assuming asset\_id started at 1, we can infer that  
           PasswordBox manages over 4 million assets, an assumption anyone can verify with the flaw we discuss next. (We did not, because of the obvious ethical concerns.)
  2. **Users Really Do Plug in USB Drives They Find**
     1. Tischer, M., Z. Durumeric, S. Foster, S. Duan, A. Mori, E. Bursztein, and M. Bailey. “Users Really Do Plug in USB Drives They Find.” In *2016 IEEE Symposium on Security and Privacy (SP)*, 306–19, 2016. <https://doi.org/10.1109/SP.2016.26>.
     2. USA
     3. F84G4WXA
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. dropped USBs all over campus, labeling some in such a way as to encourage students and faculty to pick them up and plug them in
        2. We collect browser information from  
           consenting participants using their user-agent strings
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. The HTML file also **explained** the study, allowed recipients to **withdraw**  
           from the experiment, and included a link to a follow-up survey.  
           We emphasize that we **do not automatically run *any* code** on  
           participants’ machines. As such, we may under count responses  
           if a user connected the drive, but did not open any of the HTML files.
        2. **IRB approval** for both the experiment and base line survey.
        3. We explicitly note that our experiment **employed a degree of deception**: we misrepresented the purpose of and content on the flash drives.
        4. Throughout the experiment, we **provided participants with contact information**  
           for both our team and the University of Illinois IRB.
        5. We **allowed participants to exclude themselves from the experiment** when  
           they clicked on any of the HTML files on the flash drives.
        6. We received no negative feedback from participants and as  
           we discuss in Section IV; several participants expressed their  
           appreciation for the research and asked about our results.
        7. To minimize the risk to participants’ computers, we **did not  
           automatically run any code** on participants’ systems and the  
           HTML files contained **no scripts**.
        8. We purchased the USB drives from a **reputable vendor** and **tested the drives** to ensure they did not present any unusual warnings on our test systems.
  3. **Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords**
     1. Blocki, Jeremiah, Saranga Komanduri, Lorrie Cranor, and Anupam Datta. “Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords.” Internet Society, 2015. <https://doi.org/10.14722/ndss.2015.23094>.
     2. USA
     3. ZGLABD7U
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. user study was conducted online using Amazon’s Mechanical Turk framework
        2. either collected email addresses or had a means to email (received email from participants occasionally)
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. IRB approval
        2. After the user has memorized a PAO story the computer stores the images of the story person and the scene, but discards the images of the secret action and object
        3. We randomly selected actions (e.g., swallowing) and  
           objects (e.g., bike) for each participant to memorize.
        4. We paid participants $0.50 for completing the memorization phase.
        5. To encourage participants to return we paid participants $0.75  
           for each rehearsal, whether or not they were able to remember the words.
  4. **The Effect of Social Influence on Security Sensitivity**
     1. Das, Sauvik, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. “The Effect of Social Influence on Security Sensitivity.” In *Proc. SOUPS*, Vol. 14, 2014. <https://www.usenix.org/system/files/conference/soups2014/soups14-paper-das.pdf>.
     2. USA
     3. ZQ9E7NAB
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. We constructed an IRB approved semi-structured interview protocol to probe participants about recent security related behavior changes and conversations.
        2. (1) mobile authentication, (2) application installation and  
           uninstallation, and (3) online privacy settings in social media
        3. (couldn’t the above be used for social engineering attacks if PII is obtained?)
        4. Ultimately, our interview lasted approximately 45 minutes
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. IRB approved
        2. We recorded and transcribed, with consent, each interview, and  
           used a qualitative data analysis program called Dedoose [37] to  
           analyze the anonymized transcripts
        3. We iteratively refined our protocol by piloting it with 5 people.  
           All interviewers participated in the pilots in order to mitigate  
           variation in delivery across interviewers and interview sessions.
        4. Interviewees were compensated $10 to participate
        5. Participants were required to own a smartphone running Android or iOS, be an active user of any social media service, and be at least 18 years old.
        6. We went through three rounds of recruitment to recruit a variety of occupations and ages across our sample. For example, in our first round of recruitment, we predominantly interviewed students in their mid-twenties. Thus, in subsequent recruitment rounds, we specifically recruited older non-students.
        7. We stopped recruiting additional participants once we believed we had sufficient diversity in occupation, age, and security proficiency to capture a large cross-section of experiences with security-related behavior change and communication. In our case, we appeared to reach this point after interviewing 19 participants—indeed, after the first 15, every additional participant echoed experiences very similar to those previously reported by others

1. **(new) Web Security**

Keyword searches: user, inform, PII, ethic, data, personal, subject, delete, crim, moral, legal, safe, harm, remove, clean, scrape, malicious, malware, reverse, autono, medica, sample, equal, diverse, attack, vuln, report, disclos, notif, access, solution, code, program, script, sensitive, fair, crypt, save, record, consent, discard, (new: limit, maxim, minim, citizenship)

* 1. **Traffic Monitoring Considered Reasonable**
     1. Allman, Mark. “Traffic Monitoring Considered Reasonable.” Accessed June 29, 2017. <https://www.caida.org/workshops/creds/1305/slides/creds1305_mallman.pdf>.
     2. USA
     3. F6RRAASV
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. ?
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Is there informed consent for your monitoring?  
           What are you capturing and what are you filtering? Privacy is a huge issue, I don't think you can publish without at least explaining your methods for protecting it
        2. Network traffic monitoring---broadly defined---fits  
           well within the networking and security research community's norms.
        3. The community has rough consensus and running code that traffic monitoring is reasonable (but doesn’t cite anything lol)
        4. Therefore, the presumption should be that investigations that observe it-situ activities should be considered well within the bounds of what the  
           community considers to be reasonable.
        5. We should start stating the norms that have developed organically
        6. But, how to do this authoritatively?
  2. **Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosquatting**
     1. Khan, M. T., X. Huo, Z. Li, and C. Kanich. “Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosquatting.” In *2015 IEEE Symposium on Security and Privacy*, 135–50, 2015. <https://doi.org/10.1109/SP.2015.16>.
     2. USA
     3. IFPSF5VP
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. collected a set of http and DNS requests for non-existent domains collected  
           at a passive tap on a large public U.S. university’s network
        2. The final dataset is an active web scrape of all domains in the suspected typo or suspected target sets, totaling 13.5K domains. This crawl uses a javascript-aware crawling mechanism that allows recording of redirections through multiple intermediary sites and final rendered web pages, including any javascript based redirection attempts. ...this dataset allows us to ... collect page content for clustering purposes
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. how cybercrime is perpetrated and the profits of the attackers, the harm experienced by humans is less well understood, and reducing this harm should be the ultimate goal of any security intervention
        2. *Intent inference* allows us to define a new metric for quantifying harm to users, develop a new methodology for identifying typosquatting domain names, and quantify the harm caused by various typosquatting perpetrators
        3. The HTTP portion of this dataset was anonymized pre-analysis to only  
           include a salted hash of source IP address
        4. DNS requests were collected between the local recursive resolver and the Internet  
           so individual clients’ identities are not divulged, and prior to  
           analysis they were filtered to only include “non-existent domain” results
        5. Network operations does not filter this traffic in any way between the university and the Internet. Because of the preanalysis anonymization of the data, the Institutional Review Board determined this research to not be human subjects research due to its lack of personally identifying information and purely passive collection.
        6. A subset of HTTP/HTTPS communications between internal machines at a  
           technology services enterprise and external web sites, containing timestamp, anonymized source address, and destination domain (exclusive of domains internal to the corporation), was used
        7. (For one task) our analysis code is exported to the enterprise and run on one  
           of its internal servers. Only the statistical result is returned  
           and no personally identifiable information is revealed in this process
        8. This equivalence also aids us in our goal of maintaining user  
           privacy: because any identifying factors about the user are  
           immaterial in the aggregate, we have no use for any personally  
           identifying information and thus user privacy is maintained
  3. **Analyzing the Great Firewall of China Over Space and Time**
     1. Ensafi, Roya, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall. “Analyzing the Great Firewall of China Over Space and Time.” *Proceedings on Privacy Enhancing Technologies* 2015, no. 1 (2015): 61–76. <https://doi.org/10.1515/popets-2015-0005>.
     2. USA
     3. U4VMQUWP
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. Spoof SYN requests from clients in China to Tor servers, resulting in SYN/ACKs being sent from the server to the client, and RSTs in response back to the server.
        2. First, our SYN backlog scans briefly fill a Tor relay’s backlog in order to be able to observe packet drops.
        3. Second, our idle scans create unsolicited traffic between a client and a server.
        4. Discover/utilize a side channel (part a below) without trying to fix it?
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Set up a web server on measurement machines whose index page informed visitors about our experiments. The page contained our contact information to provide alarmed network operators with an opportunity to contact us and opt out of our measurements.
        2. A full backlog can prevent a relay from accepting new TCP connections or cause the use of SYN cookies which can lead to reduced throughput. To prevent relays from using SYN cookies, **we adapted our scan parameters to minimize the risk of completely filling a relay’s SYN backlog**. SYN cookies typically do not support scaled flow control windows, which is why we made every effort to avoid them. In general, the rate at which we are sending SYN packets, without intention of completing a connection, is not enough to create a denial of-service condition on any modern network stack. Even a much higher rate of SYNs would probably not cause any issues with the service, but we kept our SYN rate as low as possible just to be conservative. For an interesting discussion about ethical issues related to port scans in general, we refer the reader to Durumeric et al. [16].
        3. This traffic—which can be observed by the censor—is only SYN/ACKs from the server to the client and RSTs from the client to the server. As a result, we are **not causing any meaningful communication other than background noise** as it is also caused by port scanning activity. While one may conceptualize the hybrid idle scan technique as providing the ability to conscript a client into performing tests for us, in reality the traffic between the server and the client is no different from if the server chose to send SYN/ACKs to the client. Thus, in terms of the traffic that the censor sees, the hybrid idle scan technique is **no different** from if Tor relay operators performed simple connectivity measurements by directly sending SYN/ACKs.
        4. Referred reader to ZMap
  4. **Identifying the Scan and Attack Infrastructures Behind Amplification DDoS Attacks**
     1. Krupp, Johannes, Michael Backes, and Christian Rossow. “Identifying the Scan and Attack Infrastructures Behind Amplification DDoS Attacks,” 1426–37. ACM Press, 2016. <https://doi.org/10.1145/2976749.2978293>.
     2. Germany
     3. UNXDTW3P
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. We present a novel honeypot-based technique, selective response, that enables us to assign a fingerprint to scanners during the reconnaissance for amplification DDoS attacks and give confidence guarantees for subsequent attribution.
        2. We evaluate our technique on a set of 1,531,852 attacks recorded by our honeypot, of which we can link 785,285 back to their corresponding scanner with a confidence of 99.9% or higher.
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. The data sets used in this paper were collected leveraging AmpPot [20], a honeypot for DDoS amplification, which works by emulating a server for vulnerable protocols and thereby becoming one of the amplifiers used in attacks. Deployment of such a honeypot pose a challenge from an ethical point of view: By design, an amplification honeypot will also act as an amplifier in an actual attack and thus send unwanted traffic towards DDoS victims. **We argue that the contribution towards attack traffic by our honeypot is negligible and only incurs minimal harm to the victim’s system.** We did not modify the thresholds chosen by the authors of AmpPot, by which the honeypot will answer at most three requests per attack. Although we deployed our honeypot to listen on 48 IPs, as discussed later, at most 24 of those IPs will send replies towards a victim’s system. Therefore, our honeypot will reply to at most 72 packets in total, i.e., a few kilobytes at most. Taking into account that these attacks usually flood a victim’s system with traffic in the order of several Gbit/s, we conclude that the contribution of our honeypot is negligible.
        2. In addition, we offered attack victims a method to opt out from our measurements. During the course of our experiments, we received three complaints that we immediately answered describing our experimental setup, but none of the complainers asked to opt out. We refer the interested reader to a more detailed ethical discussion in [20].
        3. (non-US) legislation and university system does not require nor offer IRB approvals
        4. Referred reader to: Kramer, L., Krupp, J., Makita, D., Nishizoe, T., ¨Koide, T., Yoshioka, K., and Rossow, C. Amppot: Monitoring and defending against amplification ddos attacks. In RAID ’15:
           + With AmpPot, we provide valuable insights into amplification attacks that otherwise could not be observed on such large scale. Unfortunately, we face a dilemma, as these insights can only be revealed if AmpPot participates in the attacks to some extent. To minimize the harm by AmpPot, **we have included a rate limiting mechanism. Still, this leaves a small number of attack packets**. Content-based classifiers to distinguish between scan and attack traffic are unfeasible, as attackers typically use the same kind of requests for both activities. Seeing this risk, we considered to clearly mark AmpPot’s responses as such, e.g., by embedding an info text explaining the traffic. However, first, this would enable attackers to trivially detect AmpPot deployments. Second, attack victims usually do not inspect the payload of each and every attack packet, but rely on flow-based information instead. Looking at the flows, however, would hide any note that we add to the responses. Summarizing, **we concluded that an effective rate-limiting module is the most reliable and practical option to prevent abuse of the honeypots**. Each AmpPot deployment can configure the rate-limiting thresholds on their own, possibly resorting to an overly conservative threshold (e.g., only a single request is answered per IP address and hour).
  5. **Cyberprobe: Towards Internet-Scale Active Detection of Malicious Servers**
     1. Nappa, Antonio, Zhaoyan Xu, M. Zubair Rafique, Juan Caballero, and Guofei Gu. “Cyberprobe: Towards Internet-Scale Active Detection of Malicious Servers.” In *In Proceedings of the 2014 Network and Distributed System Security Symposium (NDSS 2014)*, 1–15, 2014. <https://lirias.kuleuven.be/handle/123456789/538854>.
     2. USA/Spain
     3. W8BN2RG9
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. propose a novel active probing approach for detecting malicious servers and compromised hosts
        2. We have implemented our active probing approach in a tool called CyberProbe.
        3. We have used CyberProbe to identify 151 malicious servers and 7,881 P2P bots through 24 localized and Internet-wide scans
        4. Our active probing approach takes as input network traces  
           capturing traffic involving a few seed servers that belong to the [malware]  
           family of interest, often only one. CyberProbe replays previously observed requests to the seed servers. These requests come from valid interactions with the malicious servers [from infected hosts?] and thus are well-formed and inconspicuous. We obtain such requests by executing malware in a contained environment, by monitoring a honeyclient as it is exploited in a drive-by download, or from external analysis
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Internet scanning has been carried out many times for different research goals. Still, the unsolicited nature of the probes makes some targets consider it offensive.
        2. In this work, for good citizenship we limit each horizontal and UDP scanner  
           host to a maximum of 60,000 packets per second (26 Mbps),  
           and each appTCP scanner host to a rate of 400 connections per second.
        3. before probing a target, the horizontal and UDP scanners check if the target’s IP is in a whitelist of IP addresses to scan, otherwise they skip it. The whitelist is implemented using a 512 MB bit array, where each bit indicates if the corresponding IP address needs to be probed. This ensures that checks are done in O(1)
        4. For the appTCP scanner, which does not use an LCG, we simply  
           remove IP addresses that should not be probed from the input target list.
        5. We take ethical considerations seriously in our study.  
           For our horizontal scanning, we follow the recommendations  
           of prior work, notably those by Leonard and Loguinov [28]  
           who study how to perform maximally polite horizontal scans.  
           We adopt their proposals of **mixing the scanner IP addresses**,  
           setting up forward and backward **DNS records** for the scanners,  
           running a web server on the scanners with a **page explaining**  
           **that the probing is part of a research project**, and **removing**  
           from the scan whitelist the **ranges of owners that complain**  
           about our probing and are willing to share their IP ranges.  
           Overall, we have removed from the whitelist 106K IP addresses.
        6. In addition, we limit the probing rate of our horizontal scanners to 60,000pps, well below their maximum rate. We also manually vet the generated fingerprints before scanning to make sure they do not contain attacks and will not compromise any host. Furthermore, we work with our system administrators to minimize the impact on the local network (e.g., bypass the firewall / IDS) and to quickly answer any complaints.
        7. **No prior literature details how to perform application layer probing of malicious servers**. Our HTTP probing is not malicious, it **simply sends a request,** which we have manually vetted first, **and collects a response from a target server**. However, our requests mimic those of malicious families, and **often request inexistent resources** from web servers. Thus, they may be considered suspicious or malicious by server owners, or **may trigger IDSes** loosely configured to match traffic on both directions. Overall, out of 11 VMs that we use for HTTP probing, 2 of them got suspended for “malicious” behavior. We did not get a warning from those providers, but found out when trying to access the instances. In addition, we received 3 emails warning us that our VMs may have been compromised. The communications from the providers and those received by the system administrators of our institutions show that the majority of the complaints come from web honeypots that do not advertise their IP addresses and consider any received traffic malicious. A less frequent reason are owners thinking our scanner hosts have been infected or are attacking them. Similar to the horizontal scanning, **when the providers let us know their IP ranges, we avoid further probing**.
        8. Finally, it is worth noting that our scanning does not collect  
           and publicize any sensitive information on remote networks.
        9. Executing malware in a contained environment is a widely studied problem [22], [27], [57]. For active probing, the main goals are acquiring the malicious endpoints known to the malware sample (e.g., C&C servers and P2P peers) and collecting instances of the network traffic between the sample and the malicious endpoints. Since C&C servers are highly dynamic it is important to run the malware soon after collection to maximize the probability that at least one of the C&C servers is alive.
        10. We use **two containment policies for running the malware: endpoint failure and restricted access**. The endpoint failure policy **aborts any outgoing communication** from the malware by sending error responses to DNS requests, resets to SYN packets, and sinking outgoing UDP traffic. This policy is designed to trick the malware into revealing all endpoints it knows, as it tries to find a working endpoint. The restricted access policy **allows C&C traffic to and from the Internet, but blocks other malicious activities** such sending spam, launching attacks, or clickfraud. This policy also resets any connection with a payload larger than 4 KB to prevent the malware to download and install other executables.
        11. The malware is first run with the endpoint failure containment policy and a default configuration. If it fails to send any traffic, it is rerun with different configurations. For example, it is queued to be rerun on a different VM (e.g., on QEMU if originally run on VMWare) and for an extended period of time (e.g., doubling the execution timer). This helps to address malware samples that use evasion techniques for specific VM platforms, and to account for malware samples that may take longer to start its network communication.
        12. Making the probes identifiable to selected parties. Whenever we get a complaint on our probing we ask the reporters for the IP ranges they own and we remove them from the whitelist. However, **some reporters may not want to disclose their IP ranges**, e.g., if they run web honeypots whose addresses should remain secret. For those cases, we **could embed a secret in our probes and disclose it to selected parties**. For example, we could fix the secret used to compute the sequence number of our TCP probes and reveal it to reporters so that they can check if a received probe was sent by CyberProbe. Whenever the secret is updated we would need to notify all reporters.
  6. **Real-World Decision Making: Logging into Secure vs. Insecure Websites**
     1. Kelley, Timothy, and Bennett I. Bertenthal. *Real-World Decision Making: Logging into Secure vs. Insecure Websites*. USEC, 2016. <https://pdfs.semanticscholar.org/b4d4/0627fd913f9a056b1022b26761a1b215a665.pdf>.
     2. USA
     3. X7FQFEE7
     4. Ethical content: C
     5. Summary of Ethical issues (implicit or explicit)
        1. within-subjects two alternative forced choice paradigm on Amazon’s MT
        2. Participants were presented with simulated versions of real websites
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Internal Review Board (IRB) approval from Indiana University
        2. All websites were manipulated in a graphical editing program, and presented to participants in a popup window with disabled user interface chrome to minimize confusion between the proxy websites’ chrome and their actual browser chrome
        3. Participants were offered $2 to visit 16 websites, and an online survey was administered in the original study window after the login tasks were completed
  7. **Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse**
     1. Kurt Thomas, Damon McCoy, Chris Grier, Alek Kolcz, and Vern Paxson. “Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse.” In *Proceedings of the 22nd USENIX Security Symposium*. Washington, D.C., USA, 2013.
     2. USA
     3. ZRAC7H62
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. conducted a longitudinal study of these merchants and purchased a total of 121,027 fraudulent Twitter accounts on a bi-weekly basis over ten months from June, 2012 – April, 2013
        2. Investigated blackhat forums, etc. to participate in the underground market for Twitter accounts
        3. We conduct payments through multiple  
           identities tied to PayPal, WebMoney, and pre-paid credit cards
        4. Finally, we access all web content on a virtual machine through a network proxy.
        5. We find that merchants leverage thousands of compromised hosts, CAPTCHA solvers, and access to fraudulent email accounts
        6. A total of 10% of accounts in our dataset were logged into (either by the seller or a third party; it is not possible to distinguish the two) within a median of 3 days from our purchase. We find that 6% of all accounts go on to be resold in a median of 5 days from our purchase.
        7. merchants email confirm 77% of accounts we acquire, all of which they seeded with a unique email
        8. Merchants solved a CAPTCHA for 35% of the accounts we purchase; the remaining accounts were registered from fresh IPs that did not trigger throttling
        9. For two of the Fiverr sellers, buuman and smokinbluelady, the median CAPTCHA solution rate per IP is 100% and 67% respectively, which would indicate a human
        10. Immediately after Twitter suspended the last of the underground market’s accounts, we placed 16 new orders for accounts from the 10 merchants we suspected of controlling the largest stockpiles
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. Had the express permission of Twitter
        2. Our study is limited to Twitter, as we were unable to acquire permission to conduct our research from other companies we saw being abused.
        3. Our study hinges on infiltrating the market for fraudulent Twitter credentials where we interact with account merchants and potentially galvanize the abuse of Twitter. We do so with the express intent of understanding how sellers register accounts and to disrupt their future efforts, but that does not allay our legal or ethical obligations. Prior to conducting our study, we worked with Twitter and our institutions to set down guidelines for interacting with merchants.
        4. protect our identity from merchants by using a number of email and Skype pseudonyms
        5. With Twitter’s cooperation, disabled 95% of fraudulent accounts registered by the 27 merchants tracked, including those previously sold but not yet suspended for spam
        6. To minimize the risk posed to Twitter or its users by  
           our investigation of the account market, we follow a set  
           of policies set down by our institutions and Twitter, reproduced here to serve as a note of caution to other researchers conducting similar research.
        7. **Twitter & Users** Some of the account merchants we deal  
           with work in an on-demand fashion, where purchases we  
           place directly result in abusive registrations on Twitter  
           (e.g. harm) in violation of the site’s Terms of Services.  
           Even purchases from existing stockpiles might be misconstrued as galvanizing further abuse of Twitter. As such, we **directly contacted Twitter to receive permission** to conduct our study. In the process, we determined that  
           **any interactions with the underground market should not  
           result in harm to Twitter’s user base**. In particular, accounts we purchased **should** **never be used to tweet or form relationships while under our control**. Furthermore, **we take no special action to guarantee our accounts are  
           not suspended** (e.g disabled) by Twitter; our goal is to  
           **observe the natural registration process, not to interact  
           with or impede** Twitter’s service in any way.
        8. **Account Merchants** We **do not interact with merchants  
           anymore than necessary** to perform transactions. To this  
           end, we only purchased from merchants that advertise  
           their goods publicly and n**ever contact merchants outside  
           the web sites or forums** they provide to conduct a sale  
           (or to request replacement accounts in the event of a bad  
           batch). Our goal is not to study the merchants themselves  
           or to collect personal information on them; only to analyze the algorithms they use to generate accounts.
        9. **Sensitive User Data** Personal data logged by Twitter is  
           subject to a multitude of controls, while user names and  
           passwords sold by merchants also carry controls to prevent fraud, abuse, and unauthorized access. First, **we never log into accounts**; instead, we rely on Twitter to verify the authenticity of credentials we purchase. Furthermore, **all personal data such as IP addresses or activities tied to an account are never accessed outside of Twitter’s infrastructure**, requiring researchers involved in this  
           study to work on site at Twitter and to follow all relevant  
           Twitter security practices. This also serves to **remove  
           any risk in the event an account is compromised rather  
           than registered by an account merchant**, as no personal  
           data ever leaves Twitter. To our knowledge, we never  
           obtained credentials for compromised accounts.
  8. **ZMap: Fast Internet-Wide Scanning and Its Security Applications**
     1. Durumeric, Zakir, Eric Wustrow, and J. Alex Halderman. “ZMap: Fast Internet-Wide Scanning and Its Security Applications.” In *Proceedings of the 22nd USENIX Security Symposium*. Washington, D.C., USA, 2013.
     2. USA
     3. JA8WXYD2
     4. Ethical content: E
     5. Summary of Ethical issues (implicit or explicit)
        1. ZMap forgoes any per-connection state
        2. selects addresses according to a random permutation
        3. targets are randomly ordered and widely dispersed
        4. attempt to send probes as quickly as the source’s NIC can support, skipping the  
           TCP/IP stack and generating Ethernet frames directly
        5. No retransmission
        6. **High-speed vulnerability scanning, which could allow attackers to widely exploit vulnerabilities within hours of their discovery**
        7. released Zmap as an open source project that is documented and packaged for real world use. It is available at <https://zmap.io/>
        8. Described their test/development environment thoroughly
        9. compared ZMap’s results to Nmap
        10. experimented by sending TCP SYN packets to random 1% samples of the IPv4 address space on port 443 at varying scan rates. We conducted 10 trials at each  
            of 16 scan rates ranging from 1,000 to 1.4 M packets per second
        11. performed this experiment by sending 1, 2, 5, 8, 10, 15, 20, and 25 SYN packets to random 1% samples of the IPv4 address space on port 443 and recording the number of distinct hosts that sent SYN-ACK responses in each scan
        12. The advent of comprehensive high-speed scanning raises  
            potential new privacy threats, such as the **possibility of  
            tracking user devices between IP addresses**
        13. **Could help botnet operators**, etc. to send two-way anonymous communication to destination hosts
        14. any interaction with remote systems might cause operational problems
     6. Summary of Ethical argument, if any (implicit or explicit)
        1. If ZMap simply probed every IPv4 address in numerical  
           order, it would risk overloading destination networks with scan traffic
        2. We send packets at the Ethernet layer in order to cache  
           packet values and reduce unnecessary kernel overhead
        3. no TCP session is established in the kernel
        4. Certain address ranges need to be excluded for performance reasons (e.g., skipping IANA reserved allocations [16]) and others to honor requests  
           from their owners to discontinue scanning
        5. note that ZMap’s performance on other source networks may be worse than reported here due to local congestion
        6. worked with senior colleagues and our local network  
           administrators to consider the ethical implications
        7. impossible to request permission in advance from the owners of all these systems
        8. no IP-level equivalent of the HTTP robots exclusion standard
        9. even if they scan at full gigabit speed, traffic volumes should be negligible for destinations
        10. Recommendations:
            + 1. Coordinate closely with local network admins to  
              reduce risks and handle inquiries.  
              2. Verify that scans will not overwhelm the local network or upstream provider.  
              3. Signal the benign nature of the scans in web pages  
              and DNS entries of the source addresses.  
              4. Clearly explain the purpose and scope of the scans  
              in all communications.  
              5. Provide a simple means of opting out, and honor  
              requests promptly.  
              6. Conduct scans no larger or more frequent than is  
              necessary for research objectives.  
              7. Spread scan traffic over time or source addresses  
              when feasible

1. NS-Ethics papers
   1. **Addressing Ethical Considerations in Network Measurement Papers: Abstract**
      1. Partridge, Craig, and Mark Allman. “Addressing Ethical Considerations in Network Measurement Papers: Abstract,” 33–33. ACM Press, 2015. <https://doi.org/10.1145/2793013.2793014>.
      2. USA
      3. V7QHHQ39
      4. Ethical content:
      5. Summary of Ethical issues (implicit or explicit)
         1. explore the benefits of requiring measurement papers to include  
            an ethical considerations section
         2. We focus our attention on what  
            specific questions such a section should answer
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. The issue of how to expose ethical issues raised by rejected papers  
            remains
         2. Cite: our community does not have a set of shared ethical norms
   2. **Cyber Research Ethics Decision Support (CREDS) Tool**
      1. Kenneally, Erin, and Marina Fomenkov. “Cyber Research Ethics Decision Support (CREDS) Tool,” 21–21. ACM Press, 2015. <https://doi.org/10.1145/2793013.2793017>.
      2. USA
      3. 3UKPMKQN
      4. Ethical content:
      5. Summary of Ethical issues (implicit or explicit)
         1. This effort is motivated to operationalize a  
            decision support methodology, conceptual framework, and  
            an interactive online tool to identify, reason, and manage  
            ethical and legal issues related to cyber-based research  
            (e.g., network and system security)
         2. functional goals include: estimating and  
            communicating ethical risk; identifying potential impacts of  
            technology; and measuring and improving judgment and  
            reasoning
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. The methodology involves deriving principles  
            and practices from established law, ethics and best  
            practices, and then using that output to drive the underlying  
            logic of the tool
         2. The CREDS tool is intended to be a  
            resource for the entire community to engage repeatable and  
            transparent decision making
   3. **Does the Internet Deserve Everybody?**
      1. Elkhatib, Yehia, Gareth Tyson, and Arjuna Sathiaseelan. “Does the Internet Deserve Everybody?,” 5–8. ACM Press, 2015. <https://doi.org/10.1145/2793013.2793018>.
      2. UK
      3. FW3V98W4
      4. Ethical content:
      5. Summary of Ethical issues (implicit or explicit)
         1. explore whether initiatives to improve Internet connectivity in developing regions are always ethical
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. The following questions should clearly be answered to the public (transparency):
            * Who are the stakeholders involved, both internally and  
              externally? What is the exact role of each of the stakeholders?
            * What is the management timeline; i.e. what are the  
              targets for the different phases of the project (e.g.  
              foundation, pilot, public launch, etc.)? And who is managing these?
            * Who are the decision makers in the initiative? How  
              much control do they have? Who are they answerable  
              to? What are the mechanisms for members of the local community to participate in the decision making process?
         2. Should analyse the effect on the local community:  
            • How does the initiative empower the people?  
            • What sort of business/social links are expected to be built and with whom? What is the expected effect on the political structure?  
            • How would the initiative affect the dynamics of the local community?  
            • How do we enable successful adoption?
         3. It is a responsibility to ensure that new users introduced to the Internet are properly educated about the means and potential risks of it
         4. Summary: In what directions will the ICT be  
            improved? Who are the local and outside stakeholders that  
            will be involved both in the planning, actuation, and follow  
            up development stages? What are the socio-economic repercussions of the said development? What political obstacles,  
            if any would need to be overcome and how?
   4. **Ethical Challenges in Collaborative Storytelling**
      1. Mu, Mu, Mark Rouncefield, Yehia Elkhatib, Steven Simpson, Jacco Taal, and Nicholas Race. “Ethical Challenges in Collaborative Storytelling,” 29–32. ACM Press, 2015. <https://doi.org/10.1145/2793013.2793019>.
      2. UK/The Netherlands
      3. PSURBT62
      4. Ethical content:
      5. Summary of Ethical issues (implicit or explicit)
         1. ethical challenges involved in the handling of experimental data from people posting stories on a dedicated website (how is this different from youtube? Don’t people consent to having people watch their videos…?)
         2. Conventionally:
            * one or multiple investigators lead the test procedures or user interviews, and the user responses or any material generated from the interviews are  
              strictly **anonymized**, securely **stored**, and **selectively** made **accessible** to  
              a few named researchers. **Only relevant elements** or  
              **abstracted information** from an experiment are made  
              available for the research activities
         3. UK Data Protection Act:
            * used fairly and lawfully.
            * used for limited, specifically stated purposes
            * used in a way that is adequate, relevant and not excessive.
            * accurate.
            * kept for no longer than is absolutely necessary.
            * handled according to people’s data protection rights.
            * kept safe and secure.
            * not transferred outside the UK without adequate protection
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. It is not feasible to completely anonymize user content of  
            this nature (but then...why don’t you censor things manually? Too much stuff?)
         2. Any conversations that are supposedly private or off record are in fact on-record   
            (I guess, but I’m not sure what this means/how it’s different from online forums or private messaging on youtube…unless I’m misunderstanding what you mean by “on-record”)
         3. User data must be open for collaborative storytelling
         4. geographical constraints on the access of user data are not applicable
         5. Cite: while current computer  
            ethics guidelines may prove suitable for dealing with existing  
            and well recognized moral issues, there remains some  
            concern over computer-related practices that are not (yet)  
            morally controversial, that are what Brey terms ‘morally  
            opaque’ [Brey2000], either because they are unfamiliar or  
            because they are not recognized as moral issues but,  
            nevertheless, seem to have some (possible future) moral  
            import
         6. Cite (or cite Langdon Winner...): it is necessary for the  
            researchers to address the wider implications of technological  
            innovations [Stahl2014]
         7. We employed a new design in video authoring that allows editing using a manifest, a lightweight text-based document that describes the internal structure of audio-visual content. This design allows the content to be effectively decoupled from dependent stories, and hence problematic content could be easily retired from the system.
         8. Should any participant not wish to have any of his/her content publicly accessible or used by other participants, corresponding content will be removed upon request
         9. The form also ensures participant’s rights to withdraw from  
            the pilot and decline to answer any questions
         10. user’s responses to the interview will be completely anonymized where appropriate. Only cursory information about the identity (e.g., gender) will be used
         11. It specifies that user involvement in this study will require recording audio-visual content and that the content, along with any associated metadata (e.g.,  
             geo-location) for the study, will be uploaded to the storytelling platform and be publicly accessible for research related to the topic of community storytelling
         12. responsible design: the use of reflective practice; an emphasis on user participation and dialogue as an aspect of inclusion; a concern with values in design and deployment and an awareness of the possibility of unintended consequences in deployment and evaluation
   5. **Ethical Challenges in the MOSAIC 2B Project**
      1. Galati, Adriano, Stefan Mangold, Melani Prinsloo, Luis Almeida, and Danie Behr. “Ethical Challenges in the MOSAIC 2B Project,” 9–12. ACM Press, 2015. <https://doi.org/10.1145/2793013.2793020>.
      2. Switzerland/South Africa/Portugal
      3. PWWFEC7Z
      4. Ethical content:
      5. Summary of Ethical issues (implicit or explicit)
         1. Considering the ethical implications of using incentives
         2. These incentives include equipment (cinema-in-a-backpack), a competition among the micro-entrepreneurs offering additional equipment as prizes as well as business and technical training.
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. In [17], Grant and Sugarman show that, for the most part, the use of incentives to recruit and retain research subjects is **harmless**. They do however go further to identify instances in which incentives become problematic. These instances include cases where the subject is in a **dependency relationship** with the researcher, where the **risks are particularly high**, where the research is **degrading**, where the participant will only consent if the incentive is relatively large because the **participants’ actual aversion to the study is strong and where the aversion is a principled one**.
         2. The promise of equipment in exchange for participation may well have influenced their decision to participate. This ethical risk was however mitigated with the use of **pre-project introduction interviews** where the team merely interviewed the micro-entrepreneurs enquiring about their vision for their business and their openness to explore new opportunities without any mention of equipment. All the micro-entrepreneurs who received the offer to participate in the cinema-in-a-backpack project declared, voluntarily, in the pre-interview that they are looking for ways in which to grow their enterprises through technology-based offerings
         3. Consent from participants was obtained first and foremost  
            through the SLA. It became again necessary to re**assure** participants  
            through the project coordinator, and in one instance from a senior manager, that data would be anonymised and that responses would, at all times, be untraceable back to the individual. It was also necessary to ensure that informed and written consent was received from all participants regarding use of photographs and video recordings.
         4. All micro-entrepreneurs have **access to a copy of the final report** to verify that their identities, with relation to personal information, have indeed been protected
         5. In the light of the nature of delay-tolerant networks, some form of authentication and access control to the network itself is provided. Users need credentials to be able to access the network. Besides, the DTN network protocol allows encryption of data. Care has also been taken to separate data of the participant’s activity from transactional and statistical data.
         6. Besides his/her own activity, a microentrepreneur can access global aggregated analytics without violating the privacy of all of the other participants
         7. expectations must be managed with care (apparently this is related to no harm?)
   6. **Ethical Concerns for Censorship Measurement**
      1. Jones, Ben, Roya Ensafi, Nick Feamster, Vern Paxson, and Nick Weaver. “Ethical Concerns for Censorship Measurement,” 17–19. ACM Press, 2015. <https://doi.org/10.1145/2793013.2793015>.
      2. USA
      3. KXV2V2Q2
      4. Ethical content:
      5. Summary of Ethical issues (implicit or explicit)
         1. DIDN’T READ BECAUSE OF MENTION OF ENCORE
      6. Summary of Ethical argument, if any (implicit or explicit)
   7. **Forgive Us Our SYNs: Technical and Ethical Considerations for Measuring Internet Filtering**
      1. “Forgive Us Our SYNs: Technical and Ethical Considerations for Measuring Internet Filtering - Semantic Scholar.” Accessed September 15, 2017. [/paper/Forgive-Us-our-SYNs-Technical-and-Ethical-Consider-Crandall-Crete-Nishihata/103615db909248e4a8c04e5862182f500922e4a2](https://doi.org//paper/Forgive-Us-our-SYNs-Technical-and-Ethical-Consider-Crandall-Crete-Nishihata/103615db909248e4a8c04e5862182f500922e4a2).
      2. USA/Canada
      3. 27KVH8KZ
      4. Ethical content:
      5. Summary of Ethical issues (implicit or explicit)
         1. It is impractical to obtain prior informed consent for network  
            side channel experiments.
         2. IPID: Approx. 1% of IPv4 address space has global IPIDs; difcult to apply in IPv6 because the fragment ID is only included in fragments
         3. SYN backlog: Every machine on the Internet with an open port (i.e., every server) has a SYN backlog; SYN backlogs vary from OS to OS; relatively noise-free signal compared to IPID side channel
         4. Fragment cache: Virtually no noise; fragment cache implementations vary widely
         5. ICMP rate limits: Not well studied; may be relatively low noise
         6. Is it necessary for the measurement machine IP address to appear in traffic logs for both the server and the client?
         7. What is the proper level of risk with respect to denial of service?
         8. What kind of machine should the client be? What if client is associated w/ a person?
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. IPID: Requires a relatively low rate of packets (e.g., 5 per second); measurement machine must communicate directly with client
         2. SYN backlog: Some OSes do not properly protect themselves against DoS; requires a relatively low rate of packets (e.g., 5 per second); measurement machine must communicate directly with server.
         3. Fragment cache: Some fragment cache implementations do not protect properly against DoS; packet rates depend on fragment cache size
         4. ICMP rate limits: Can be elicited from gateway routers for IP addresses where no machine exists; may be possible to use at very low packet rates (e.g., 5 per second).
         5. Cite: ethical gray areas
         6. Cite: Nonetheless grey areas and knowledge gaps persist due in part to lack of shared community values and insufficient subject matter expertise on institutional review boards [12]
         7. Side channel experiments are interventions into an environment, and to be done responsibly research risk has to reduced to a minimum.
         8. Client-side network measurement is implemented by installing software on a volunteer’s computer in the target country. The HTTP GET requests the client initiates are done without any obfuscation or anonymization as the intent is to collect responses from the network that are representative of the average user experience. If the users’ network is being monitored requests to potentially sensitive URLs can be discovered, which puts them at risk.
         9. measurements do not harm or disrupt the networks under investigation
         10. In over 10 years the ONI never experienced a user being arrested, apprehended, pressured, or intimidated by authorities for their participation in the project.
         11. The project protocol has been reviewed and approved by an REB
         12. Need to assess varying levels of risk and communicate them to users; We are restricting our study to countries that present the medium research risk level
         13. of the side channels discussed above only the hybrid idle scan and the fragment cache side channel have the property that the measurement machine communicates with both the server and the client during measurements. For the other side channels, the measurement machine could be made to send packets to both the client and server but this may make it much easier for censors to block measurements
         14. Acceptable packet rates (for avoiding DoS) depend on the packet type
         15. An idea (that has been mentioned by a number of colleagues) is to traceroute to a given client and then fnd a router near the client that can be used as the client instead, e.g., a router with a global IPID can be used as a client in the hybrid idle scan. This mitigation is what is done in the Censored Planet project [2].
         16. Another possibility is to use something like the ICMP rate limitation side channel, where the “client” can be an IP address that is unresponsive (i.e., no client exists at that IP address) and the side channel is actually being measured on its gateway router.
         17. Yet another possibility is to use servers as clients, on the theory that web servers cannot be tied to one person as clients. For noisy side channels such as the IPID or hybrid idle scan, this may not be practical because servers typically have a high amount of IPID noise.
         18. Another possible mitigation is to perform measurements for entire /24s at once, so that no individual can be associated with the measurements incorrectly. Any side channel measurement can be performed in this way, but this technique will be more eﬀective if a large fraction of the /24 meets the requirements of the measurement.
   8. **High Fidelity, High Risk, High Reward: Using High-Fidelity Networking Data in Ethically Sound Research**
      1. Khan, Mohammad Taha, and Chris Kanich. “High Fidelity, High Risk, High Reward: Using High-Fidelity Networking Data in Ethically Sound Research,” 23–26. ACM Press, 2015. <https://doi.org/10.1145/2793013.2793024>.
      2. USA
      3. M3653E9T
      4. Ethical content:
      5. Summary of Ethical issues (implicit or explicit)
         1. Network taps have the capability to observe every bit going in/out of an organization
         2. Network taps’ existence might create chilling effects on organizations
      6. Summary of Ethical argument, if any (implicit or explicit)
         1. Cite: In this work we apply these guidelines to the use of high fidelity data obtained from network taps. (i.e. they applied general guidelines to specific instances)
         2. Middleware Data and Reports: This category includes data logs generally obtained from proxies, firewalls, and filtering products…. This **homogeneity**, along with the fact that many if not all devices and software are **owned and controlled by the enterprise**, place research using this data on slightly stronger ethical footing. However, one must still consider employees as stakeholders in this case, and research should be done in such a way to minimize harm wherever possible.
         3. Individuals who are the subjects under consideration within the tap data should have  
            informed consent of participating in the research as well as the option to opt out.
         4. While researchers may explore multiple directions, the essential goal should be the welfare of the community. The overall scope of benefits and risks should be identified to provide a balanced methodology.
         5. Tap data generally contains a diverse group of subjects. All research should be performed in an unbiased manner. In cases where specific cliques are under consideration, the rationale should be explicitly mentioned.
         6. Cite: Allman and Paxson [1] Results generated from network tap data should be in an aggregated format to reduce the sensitivity while elucidating a  
            specific trend. Another important aspect is the anonymization of the dataset to rule out “any” possible affiliation with the providing entity as a means to minimize risk.
         7. As a part of performing cybercrime research, the stakeholders should be kept up to date with all insights, specifically the ones that might pose serious harm to the enterprise
         8. Subjects of research should have the option to opt-in for data collection when they start using a network service.