Ethical Considerations in Network Security and Network Measurement Research

Exploration and Confusion from a PH.D. Student

Yiming Zhang NISL@Tsinghua University 2021.06.06

Experience Must Be Bought



Important Dates

Considering the challenges we all face at this time, the TPC chairs have decided to extend the paper registration and submission deadline by one week. Please note the changed dates. Beyond this, if you are an author who has been directly affected by the disease, please do not hesitate to contact the chairs directly at imc2020pcchairs@sigcomm.org.

Paper registration (with abstract)	Tuesday May 19, 2020 May 26, 2020 at 11:59PM PDT (UTC-7)
Paper submission	Tuesday May 26, 2020 June 2, 2020 at 11:59PM PDT (UTC-7)
Early reject notification	Friday July 10, 2020 Monday July 20, 2020
Notification	Wednesday August 12, 2020
Camera-ready due	Wednesday September 23, 2020
Conference	October 27 - 29, 2020

2020.05.26

One Paper submitted to IMC' 20

2020.08.12 Notification Date

Unexpectedly, instread of reviews, I received such an email...

Experience Must Be Bought

Detection and measurement of a new type of fraudulent cybercrime

Your IMC submission

Dear authors.

was flagged by the

IMC reviewers as requiring further consideration due to legal or ethical concerns.

An Ethics committee reviewed the work and concluded that your paper fails to meet the required ethical standard for human subject research for the following reasons:

1) Details of what users agree to when turning on

were not clear.

- 2) The paper says nothing about an IRB procedure for the researchers.
- There is no description of how the data was handled by the researchers.
- The reports on specific aspects of PII in the paper
 - , which significantly raises the bar in terms of user consent.

Given that none of these issues are addressed in the paper as required by the CFP, your paper has been rejected on ethical grounds.

Superficial Knowledge of Ethical Standards

What I know

- Existence of ethical standards
- Several typical requirements
- Need to write something in paper

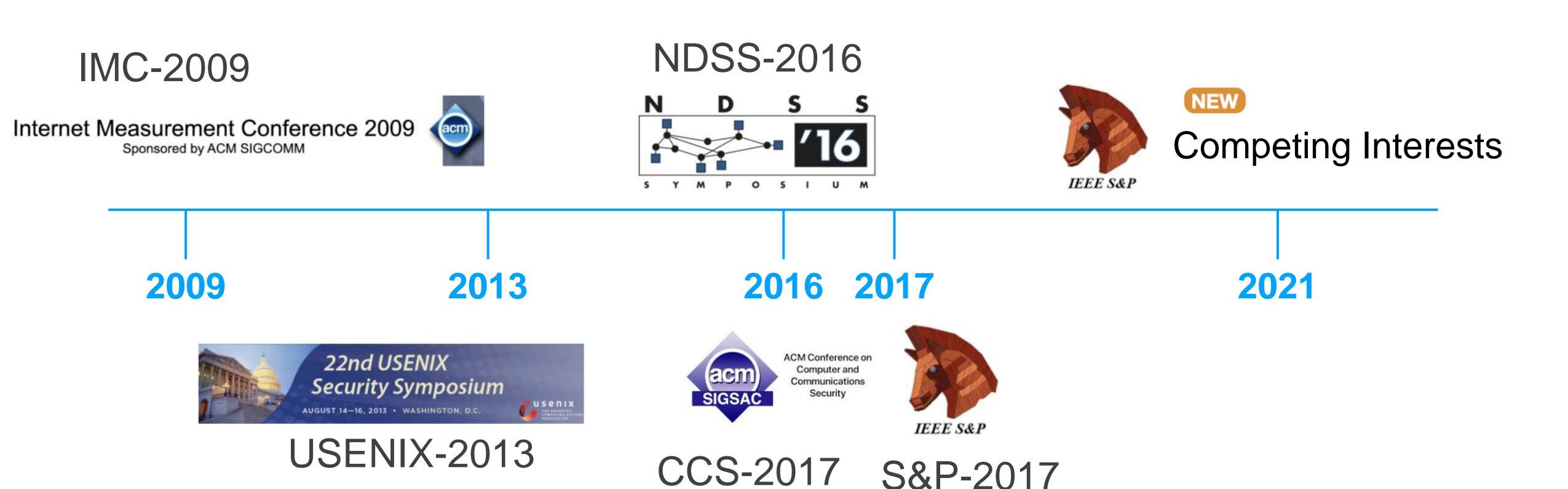
What I don't know

- Origin and evolution of specific claims
- Systematic ethical considerations
- How to organize a well writing

Survey: Ethics in Network Security/Measurement

- Requirement of ethical standards in CFP of major security conferences
 - S&P, NDSS, CCS, USENIX, IMC
- •Recognized papers/reports devoted to ethical issues
 - General standards of information technology
 - Network measurement
 - Censorship (measurement)
 - Data sharing
- How ethical issues are indicated in published studies in recent years
 - •Learn how to design experiment and write ethical consideration sections

Timeline: Ethics Requirement Changes in CFP



Ethical Standards in IMC

2009 CFP

Ethical standards for measurement must be considered by all IMC authors. In particular, authors must be aware of and conform to acceptable use policies for individual domains that are probed or monitored, data privacy and anonymity for all personally identifiable information, and etiquette for using shared measurement data (see Allman and Paxson, IMC '07). If applicable, authors are also urged to notify parties of security flaws in their products or services in advance of publication. Adherence to ethical standards for measurement will be a criteria for all submissions and violations will be grounds for rejection.

Key Points

- Must consider ethical standards for measurement
- Use policies, data privacy and anonymity, shared data, security flaw notifications
- Violations of ethical standards could be grounds for rejection

Ethical Standards in IMC

2021 CFP

Research involving experiments with human subjects or user data (e.g., network traffic, passwords, social network information) should adhere to community norms. Any work that raises potential ethics considerations should indicate this on the submission form. The basic principles of ethical research are outlined in the Belmont Report: (1) respect for persons (which may involve obtaining consent); (2) beneficence (a careful consideration of risks and benefits); and (3) justice (ensuring that parts of the population that bear the risks of the research also are poised to obtain some benefit from it).

Research involving human subjects must be approved by the researchers' respective Institutional Review Boards before the research takes place. Authors should indicate on the submission form whether the work involves human subjects, and, if so, if an IRB protocol has been approved for the research. We also expect that any research follows the practices and procedures of the institution(s) where the work is being carried out; for example, some universities require separate approval for the use of campus data. We expect researchers to abide by these protocols.

Some research does not involve human subjects yet nonetheless raises questions of ethics, which may be wide-ranging and not necessarily limited to direct effects. We encourage authors to be mindful of the ethics of the research that they undertake; these considerations are often not clear-cut, but often warrant thoughtful consideration. The program committee may raise concerns around the ethics of the work, and so we ask authors to outline these considerations explicitly in a separate appendix section (clearly marked with an appendix section heading "Ethics"), and when appropriate for context, in the body of the paper. The submission form will include a way to alert reviewers of this additional material.

Additionally, the program committee reserves the right to conduct additional evaluations and reviews of research ethics and reserves the right to independent judgment concerning the ethics of the conducted research.

Contact the program committee co-chairs at imc2021pcchairs@sigcomm.org if you have any questions.

Key Points

Basic Principle: Belmont Report

Human Subjects

Must approved by IRB

Other Ethical Issues

Outline in body/appendix

Clearly marked with "Ethics"

Ethical Standards in USENIX

2013 CFP

Key Points

IRB approval

Steps taken to mitigate ethical issues
Steps taken to deal with vulnerabilities
Steps taken to deal with sensitive data
Reject if insufficient

New in 2013: Papers that describe experiments on human subjects, or that analyze non-public data derived from human subjects (even anonymized data), should disclose whether an ethics review (e.g., IRB approval) was conducted and discuss steps taken to ensure that participants were treated ethically.

2021 CFP

Human Subjects and Ethical Considerations

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should:

- 1. Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (e.g., an IRB).
- Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

If the submission deals with vulnerabilities (e.g., software vulnerabilities in a given program or design weaknesses in a hardware system), the authors need to discuss in detail the steps they have already taken or plan to take to address these vulnerabilities (e.g., by disclosing vulnerabilities to the vendors). The same applies if the submission deals with personally identifiable information (PII) or other kinds of sensitive data. If a paper raises significant ethical and legal concerns, it might be rejected based on these concerns.

Ethical Standards in NDSS

2016 CFP

If a paper relates to human subjects, analyzes data derived from human subjects, may put humans at risk or might have other ethical or legal implications, authors should disclose if an ethics review (e.g., IRB approval) was conducted, and discuss in the paper how ethical and legal concerns were addressed. If the paper reports a potentially high-impact vulnerability the authors should discuss their plan for responsible disclosure. The chairs will contact the authors in case of major concerns. The Program Committee reserves the right to reject a submission if insufficient evidence was presented that ethical and legal concerns were appropriately addressed.

2021 CFP

If a paper relates to human subjects, analyzes data derived from human subjects, may put humans at risk, or might have other ethical implications or introduce legal issues of potential concern to the NDSS community, authors should disclose if an ethics review (e.g., IRB approval) was conducted, and discuss in the paper how ethical and legal concerns were addressed. If the paper reports a potentially high-impact vulnerability the authors should discuss their plan for responsible disclosure. The chairs will contact the authors in case of major concerns. The Program Committee reserves the right to reject a submission if insufficient evidence was presented that ethical or relevant legal concerns were appropriately addressed.

Key Points

IRB approval

Ethical and legal concerns

Responsible disclosure

Reject if insufficient

Ethical Standards in CCS

2017 CFP

Submissions will be evaluated based on their scientific merit, novelty, importance, presentation quality, and relevance to computer and communications security and privacy. If a paper includes work that raises ethical concerns it is up to the authors to convince the reviewers that appropriate practices were followed to minimize possible harm and that any harm caused by the work is greatly outweighed by its benefits. The review process will be carried out in two phases and authors will have an opportunity to provide a length-limited response to the first-phase reviews.

2021 CFP

All submitted papers will be evaluated based on their merits, particularly their importance to practical aspects of computer and communications security and privacy, novelty, quality of execution, and presentation. For papers that might raise ethical concerns, authors are expected to convince reviewers that proper procedures (such as IRB approval or responsible disclosure) have been followed, and due diligence has been made to minimize potential harm.

Key Points

Expected to provide ethics discussions (IRB, considerations)

Ethical Standards in S&P

Human Subjects and Ethical Considerations Start from 2017

Drawn from the USENIX Security 2016 CFP

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should:

- 1. Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (IRB) if applicable.
- 2. Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

If the submission deals with vulnerabilities (e.g., software vulnerabilities in a given program or design weaknesses in a hardware system), the authors need to discuss in detail the steps they have taken or plan to take to address these vulnerabilities (e.g., by disclosing vulnerabilities to the vendors). The same applies if the submission deals with personal identifiable information (PII) or other kinds of sensitive data. If a paper raises significant ethical and legal concerns, it might be rejected based on these concerns.

Authors seeking ways to reduce the ethical risks of their experiments may optionally consider reaching out to the Ethics Feedback Panel for Networking and Security. The panel's mission is to help researchers identify ethics-related risks, find prior research that provides precedent or data to inform ethical decision making, to suggest ways to improve experimental designs to reduce ethical risks, and provide any other information that may assist the researchers in meeting their ethical obligations. The best time to reach out to this panel is before conducting your experiments, but they may be able to assist if concerns arise during an experiment. Contact the program co-chairs if you have any questions.

Ethical Standards in S&P

Financial and Non-financial competing interests NEW

In the interests of transparency and to help readers form their own judgements of potential bias, the IEEE Symposium on Security & Privacy requires authors and PC members to declare any competing financial and/or non-financial interests in relation to the work described. Authors need to include a disclosure of relevant financial interests in the camera-ready versions of their papers. This includes not just the standard funding lines, but should also include disclosures of any financial interest related to the research described. For example, "Author X is on the Technical Advisory Board of the ByteCoin Foundation," or "Professor Y is the CTO of DoubleDefense, which specializes in malware analysis." More information regarding this policy is available here.

Ethical Considerations for Vulnerability Disclosure

Where research identifies a vulnerability (e.g., software vulnerabilities in a given program, design weaknesses in a hardware system, or any other kind of vulnerability in deployed systems), we expect that researchers act in a way that avoids gratuitous harm to affected users and, where possible, affirmatively protects those users. In nearly every case, disclosing the vulnerability to vendors of affected systems, and other stakeholders, will help protect users. It is the committee's sense that a disclosure window of 45 days https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy to 90 days https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html ahead of publication is consistent with authors' ethical obligations.

The version of the paper submitted for review must discuss in detail the steps the authors have taken or plan to take to address these vulnerabilities; but, consistent with the timelines above, the authors do not have to disclose vulnerabilities ahead of submission. If a paper raises significant ethical and/or legal concerns, it might be rejected based on these concerns. The PC chairs will be happy to consult with authors about how this policy applies to their submissions.

Ethical Considerations for Human Subjects Research

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should:

- 1. Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (IRB) if applicable.
- 2. Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

If a submission deals with any kind of personal identifiable information (PII) or other kinds of sensitive data, the version of the paper submitted for review must discuss in detail the steps the authors have taken to mitigate harms to the persons identified. If a paper raises significant ethical and/or legal concerns, it might be rejected based on these concerns. The PC chairs will be happy to consult with authors about how this policy applies to their submissions.

Ethical Standards in S&P

What's updated Detailed requirements for vulnerability disclosure

- A disclosure window of 45 days to 90 days ahead of publication
- Review version must discuss in details the steps authors taken to address the vulnerabilities
- Do not have to disclose vulnerabilities ahead of submission

What's NEW Financial and non-financial competing interests (required in camera-ready)

- To protect the objectivity, integrity and value of a publication, help readers form their own judgement of potential bias.
- Financial interests: funding, employment, personal financial interests, and etc. No threshold.
- Non-financial interests: unpaid membership of government or non-governmental organizations, acting as an expert witness, and etc.

e.g. Professor Y is the CTO of DoubleDefense, which specializes in malware analysis.

Ethical Standards in ...

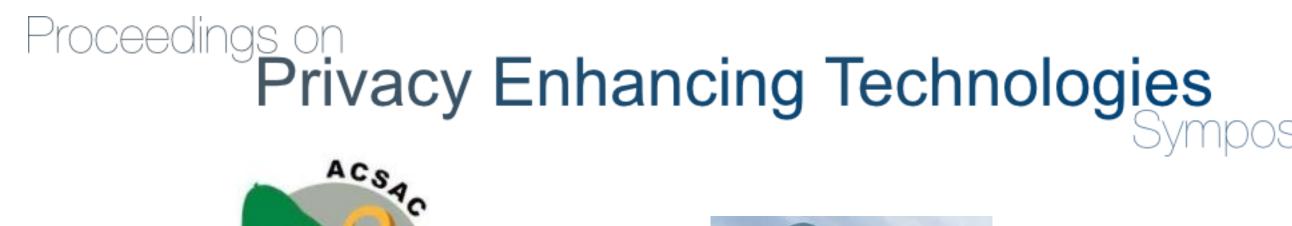






PETS





PAM



SOUPS



















EMNLP

Recognized Papers/Reports Devoted to Ethics

Topic	Paper/Report
	[1979] The Belmont Report
	[1989] RFC 1087
General	ACM Code of Ethics and Professional Conduct
General	[2012] The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research
	[2013] Applying Ethical Principles to Information and Communication Technology Research: A Companion to the Menlo Report
	[2013 Microsoft Tech.Rep] Common pitfalls in writing about security and privacy human subjects experiments and how to avoid them
Measurement Data Sharing	[IMC' 07] Issues and Etiquette Concerning Use of Shared Measurement Data
Network	[1991] RFC 1262
Measurement	[NS Ethics@SIGCOMM' 15] Addressing Ethical Consideration in Network Measurement Paper
	[NS Ethics@SIGCOMM' 15] Forgive us our SYNs: Technical and Ethical Considerations for Measuring Internet Filtering
Censorship Measurement	[NS Ethics@SIGCOMM' 15] Ethical Concerns for Censorship Measurement
Madaronia	[2015] No Encore for Encore? Ethical questions for web-based censorship measurement

The Belmont Report

#BELMONT REPORT

Ethical Principles and Guidelines for the Protection of Human Subjects of Research

The Belmont Report

Office of the Secretary

Ethical Principles and Guidelines for the Protection of Human Subjects of Research

The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research

April 18, 1979



AGENCY: Department of Health, Education, and Welfare.

ACTION: Notice of Report for Public Comment.

Issued on 1978.09.30

Summarized ethical principles and guidelines for research involving human beings

Three core principles:

- Respect for persons
- Beneficence
- Justice

The Menlo Report

The Menlo Report

Ethical Principles Guiding Information and Communication Technology Research

August 2012



Principle	Application
Respect for Persons	Participation as a research subject is voluntary, and follows from informed consents. Treat individuals as autonomous agents and respect their right to determine their own best interests; Respect individuals who are not targets of research yet are impacted; Individuals with diminished autonomy, who are incapable of deciding for themselves, are entitled to protection.
Beneficence	Do not harm; Maximize probable benefits and minimize probable harms; Systematically assess both risk of harm and benefit.
Justice	Each person deserves equal consideration in how to be treated, and the benefits of research should be fairly distributed according to individual need, effort, societal contribution, and merit; Selection of subjects should be fair, and burdens should be allocated equitably across impacted subjects.
Respect for Law and Public Interest	Engage in legal due diligence; Be transparent in methods and results; Be accountable for actions.

Proposed Guidelines for ethical assessment of ICT Research

- Michael Bailey, University of Michigan
- Aaron Burstein, University of California Berkeley
- KC Claffy, CAIDA, University of California San Diego
- Shari Clayman, DHS Science & Technology
- David Dittrich, Co-Lead Author, University of Washington
- John Heidemann,
 University of Southern California, ISI
- Erin Kenneally, CAIDA,
 University of California San Diego, Co-Lead Author
- Douglas Maughan, DHS Science & Technology
- Jenny McNeill, SRI International
- Peter Neumann, SRI International
- Charlotte Scheper, RTI International
- Lee Tien, Electronic Frontier Foundation
- Christos Papadopoulos, Colorado State University
- Wendy Visscher, RTI International
- Jody Westby, Global Cyber Risk, LLC

Authors and Working Group Participants

The Menlo Report

Guideline-1 Respect for person

- Paticipants must be voluntary
- Informed consent must be provided
 - State all the possible negative consequences
 - Do not induce users to participate with benefits
 - Need to be clear for all the details, easy to understand
 - Emphasize voluntary participation
 - Explain it well after the experiment if it had to deceive the users

Guideline-2 Beneficence

- Maximize the positive effects, minimize the negative effects
 - Take into account, all the negative effects, as far as possible
 - Development of corresponding mitigation
 - Need to inform all the affected parties
 - Consider the worst case scenario and prepare mitigations accordingly

The Menlo Report

Guideline-3 Justice

- Every person deserves equal consideration in how to be treated
- Selection of subjects should be fair
- The benefits and potential harms are the same for all

Guideline-4 Law and Public Interest

- Obey the law, do not compromise the public interest
- Be open about your methods and results
- Be accountable for your actions

^{*} Application details and case studies could be seen in: 2013 Companion to the Menlo Report.

Dataset Sharing

Motivation: Pose a set of reasonable, high-level considerations for sharing and using measurement data.

Data release considerations

Risk of information leakage

- 1. Full anonymization adapted to multiple scenarios
- 2. Detailed usage guidelines/policies
- 3. Interaction with users
- 4. Information of auxiliary dataset
- 5. Guidelines of how to cite/give acknowledgement

Issues and Etiquette Concerning Use of Shared Measurement Data

IMC 2007

Mark Allman ICSI Berkeley, CA, USA mallman@icir.org

Vern Paxson ICSI & LBNL Berkeley, CA, USA vern@icir.org

Data use considerations

Fully appreciate the difficulty of releasing data

- 1. Obey the access policies claimed by providers
- 2. Further anonymization before report results
- 3. Use purposed-provided data with caution
- 4. Be careful of de-anonymization
- 5. Notification and acknowledgement

Network Measurement

Background: Network measurement community is increasingly facing ethics issues and finding itself poorly prepared.

Addressing Ethical Considerations in Network Measurement Papers

NS Ethics @ SIGCOMM. 2015

Craig Partridge
Raytheon BBN Technologies
craig@aland.bbn.com

Mark Allman ICSI mallman@icir.org

Motivation: Propose measurement papers include an ethical consideration sections and give guidelines.

Scope: Ethics issues involving human beings

"Harm"

- Harm is generally spectural, consider the worst case
- Regardless whether the harm is direct or indirect
- Potential harm is to be discussed, even if not directly caused by the experiment

Network Measurement

Addressing Ethical Considerations in Network Measurement Papers

NS Ethics @ SIGCOMM. 2015

Craig Partridge
Raytheon BBN Technologies
craig@aland.bbn.com

Mark Allman ICSI mallman@icir.org

- Data collection (even passive-collected)
 - Public datasets collected in an unethical manner, e.g., compromise.
 - Non-public dataset collected in some form by researchers (more serious)
- Publish datasets
- Must be anonymized (anonymization != no-risk, e.g., de-anonymization technology)
- Do not require perfect solutions while at least, find mitigations

Basic questions authors should answer

- 1. Datasets directly collected by the authors: the ethics consideration & mitigation of data collection
- 2. Datasets not directly collected by the authors: if ethics has been discussed, give citation, otherwise provide ethical considerations both of the data collection and the data usage.
- 3. Can the data reveal private or confidential information of individuals? Provide mitigations.
- 4. Additional ethical issues specific to the work.

Censorship Measurement

- Ways of censorship measurement
 - Network channel measurement: e.g., ping, SYN
 - Client-side measurement
 - Deploy researchers with software
 - Deploy software to citizens
 - Co-opt existing deployed software
 - Ethical Issues of network channel measurement
 - Risk: Participation in the experiment is unlikely to be by prior consent
 - Mitigation: Minimize the rate of packets
 - Ethical Issues of client-side measurement
 - Risk: Users involved in the measurement may also be subject to scrutiny. (higher risk interest)
 - Mitigation: Evaluate "risk score" and restrict research to "medium" regions
 - Freedom on the Internet; Economist Democracy Index; Travel Advisory
 - e.g., US->Low risk, Pakistan->Medium risk, Syria->High risk

Open questions:

- What packet rates are acceptable?
- •Is it necessary for user consent?
- Proper level of risk with respect to DoS?

Learn From Published Big4 Papers

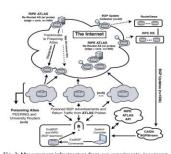
- How to write Ethics Considerations in an academic paper?
 - To facilitate the judgement of reviewers on whether it is compliant with ethical standards
 - To provide a sound reference for subsequent studies

IRB improved paper

Year	Oakland	USENIX	CCS	NDSS
2020	10	19	3	7
2019	8	12	11	10

10 well-written (just in my opinion) Big4 papers

Topic	Conference	Paper
	NDSS' 20	Withdrawing the BGP Re-Routing Curtain: Understanding the Security Impact of BGP
Internet Measurement	ND33 20	Poisoning via Real-World Measurements
	NDSS' 20	On Using Application-Layer Middlebox Protocols for Peeking Behind NAT Gateways
Concorchin	NDSS' 20	Decentralized Control: A Case Study of Russia
Censorship	NDSS' 20	Measuring the Deployment of Network Censorship Filters at Global Scale
Scam	Usenix' 19	The Art of The Scam: Demystifying Honeypots in Ethereum Smart Contracts
Scalli	Usenix' 19	Users Really Do Answer Telephone Scams
Privacy	S&P' 19	Characterizing Pixel Tracking through the Lens of Disposable Email Services
Mobile Security	S&P' 19	Automatic Uncovering of Hidden Behaviors From Input Validation in Mobile Apps
Web Security	NDSS' 19	TRANCO: A Research-Oriented Top Sites Ranking Hardened Against Manipulation
IOT Security	Usenix' 19	All Things Considered: An Analysis of IoT Devices on Home Networks



 $\{AS_{origin}, AS_{AV_1}, AS_{AV_2}, ..., AS_{AV_N}, \underbrace{AV_{origin}}_{For ROV}\}$ (1)

Data-Plane Infrastructure: We utilize RIPE Atlas [45] to

Hang Control plane have propagated successfully by the time or traceroutes, our experiments wait at least 2 minutes between measurements after each BGP advertisement, and in some cases 10 minutes if conducted via PEERING infrastructure.

IV. ETHICAL CONSIDERATIONS

study conducts active measurements of routing or on the live Internet. As a result, we took several

Significant care was taken to notify various groups of our

we can steer a remote AS onto and dive deepty into the properties of these alternative paths. This analysis includes quantifying the diversity of transit ASes along those alternative paths, computing weighted and unweighted minimum cuts of the topology based on AS properties, and exploring latency differences between alternative paths. We also attempt to reproduce past security research and build statistical models that represent how successfully an AS can conduct return path

BGP updates have propagated is due to the poisoning itself.

Algorithm: Recursive path steering algorithm

9 mapping.put(newPoisons, c
 10 if currentPath == ∅ then
 11 | disconnected = true;

ely, we could not find a publicly available data set

For proxy protocols, we limit our actions to connecting and in case of HTTP, performing single requests. In order to obtain evidence of misconfigurations, we had to target some non routable addresses. We deliberately chose two target addresses (localhost and "192.168.0.1") that were likely to provide u the confirmation without really trying to access any networker

A Educat Considerations

Considering that we are studying live systems on the Internet, we aim to prevent (or at least minimize) any potential harm on the target systems by avoiding changes to these systems. With all the following precautions in place, we try to balance between the benefits and the potential harm caused by our scanning, as discussed in the Menlo report [7]. We argue that the understanding of these phenomena outweigh the potential harms and now discuss in detail the steps we undertook to guide our measurements. Scanning approaches involving multiple application-layer requests have previously for example been used to detect TLS vulnerabilities [48]; All collected data is stored on secured servers, and only authorized persons have access to this data. We did not collect any kind of personal data; our university does not require an IRB approval for this type of network scans.

As UPnP is not designed to be accessible over the Internet, the mitigation would be patching these vulnerable devices. However, considering that UPnP/SSDP has been misused for amplification attacks for years, it is doubtful that the manufacturers are going to provide fixes for these CPE devices. Therefore, the average recommendation and industry best presented.

First of all, we utilize standard-conforming querying func-tionality whenever possible (e.g., UPnP IGD enumeration). Where it is unavoidable (e.g., understanding potential PCP vulnerabilities), we follow the corresponding RPC guidance. For example, RPC 6887 [71, Section 11.6] recommends using a short-lived forward for obtaining the external address for PCP and we craft our payloads accordingly. All requests we sent conform to the respective standards, and we did not try to misuse or exploit any vulnerability. We undertook several steps in order to make clear that Besides the protocols discussed in this paper, there are also other protocols for relaying traffic which could be susceptible for misuse. One example are Traversal Using Relay NAT (TURN) relays, which are mainly used for VoIP and WebRTC when no direct peer-to-peer connectivity is available. Case in point, it was recently reported that Cisco's Meeting Server acting as a TURN gateway is vulnerable for arbitrary TCP relaying [5]. However, based on our brief investigation, their relaying [3]. However, based on our orbeit investigation, tient population seems to be restricted to service providers and access to these servers requires authentication, i.e., there is no openly accessible TURN server population in the same sense as for proxies, so we omitted their analysis in this paper. For Internet proxies, there is also a recent IETF draft for a non-backwards compatible SOCKS5 [53] aimed for today's The reverse DNS record of the scanning host was set to indicate its use for research purposes. Furthermore, the whois information for its IP address contained our abuse e-mail address, which received mostly automated mails noting that our scans have been detected. We promptly responded to

protocol designs (e.g., extendability and reduction of initial round trips) with no public implementations yet.

While we cannot completely exclude the possibility that our organizational vantage points will be somehow penalized, we took several steps to reduce the potential risk. Because IRB considers remote measurement studies outside of their purview (as these studies did not involve human subjects or their personally identifiable data), we discussed the study's design with internal and external colleagues in our community. Like Quack, Hyperquack only establishes connections between our own measurement machine and organizational HTTP(S)

Moreover, we make it easy for anyone investigating of nanged traffic is part of a measurement research experime te set up WHOIS records and a web page served from p

We also follow the best practices set forth by the ZMap teasurement system [19] and limit the rate at which we HTTPs tests at different times so that servers used for both HTTP and HTTPS measurements do not receive simultane-ous requests. On average, our probes caused servers behind filter deployments to trigger the filter 99 times a day, and a maximum of 240 times a day. As a point of comparison, two-thirds of Top Million sites cause requests to Google servers, and one-third to Facebook servers, so filters that block these

The data collection phase aims to collect an extensive and diverse set of disrupted application-layer data—which and diverse set of instripact application-layer data—which
most likely contains many blockpages from different filters.
We achieved this by combining Quack, OONI and our new

To address both constraints, we use the following approach
for identifying organizational servers: Using the official list

Initial Domains(P) $\{P_2, ..., P_N\}$ Ethical Server T, T = T, T = T, T T, T = T, T = T, TStep 2: Test Domain Not Blocked Retry: GET_T(Domain) 2 CT Disrupted T GET_T(P) - CT

Fig. 4: HyperQuack pipeline: Given server, initial benign (sub)domains, and domain inputs, Hyperquack generates a canonical template CT, and then performs a set of trials, denoted get_t, to classify the test into possible output states. \circ

than 50 million active HTTP(S) web servers around the world with heterogeneous characteristics ranging from international CDNs to personal sites operated by individuals. We select servers from this pool with a focus on two properties: Location Diversity and Ethical Soundness. Location Diversity: Our desire for location diversity is a

Location Diversity: Our desire for location diversity is a property of the path as much as the remote vantage points. There are two important considerations on why the location of a server itself is not sufficient for our understanding of behavior. First, a subset of servers, including major CDNs, make use of anycasting. Anycasting describes the situation where an IP address is resolved to multiple physical hosts in different locations based upon the location of the client requesting content from the server [9]. This means that whil the IP address may have a point of presence in a desire

Ethical Soundness: Aligned with the ethical consideration we need to only use servers known to be organizational

7.3 Ethical Considerations

In general, honeypots have two participants, the creator of the honeypot, and the user whose funds are trapped by the honeypot. However, the ethical intentions of both particinake profit. In this case we clearly have a malicious in cious or benign. For example, if a user tries to intentio lly exploit a reentrancy vulnerability, then he or she need under the assumption that he or she is participating in a fair lottery. Thus, both honeypot creators and users cannot al-

8 Related Work

Honeypots are a new type of fraud that combine security issues with scams. They either rely on the blockchain itself or on related services such as Etherscan. With growing interes on related services such as Emerscan. With growing interest within the blockchain community, they have been discussed online [31, 32, 33] and collected within public user repositories [22, 45]. Frauds and security issues are nothing new within the blockchain scosystem. Blockchains have been used for money laundering [24] and been the target of several scams [42], including mining scams, wallet scams and Ponzi schemes, which are further discussed in [4, 43]. In particuar, smart contracts have been shown to contain security is-ues [2]. Although not performed directly on the blockchain, exchanges have also been the target of fraud [23]. Several different methods have been proposed to discover

fraud as well as security issues. Manual analysis is performed on publicly available source code to detect Ponz schemes [3]. [49] introduces ERAYS, a tool that aims to produce easy to analyse pseudocode from bytecode where the source code is not available. However, manual analysis is particularly laborious, especially considering the number of contracts on the blockchain. Machine learning has been used to detect Ponzi schemes [8] and to find vulnerabilities [36]. The latter relies on [27] to obtain a ground truth of vulnerable smart contracts for training their model. Fuzzing techniques have been employed to detect security vulnera-

events or function calls [17]. However, fuzzing often fail ties in smart contracts. [7] requires manual interaction, while [39] requires both the definition of violation and compliance patterns. [37] requires Solidity code and therefore cannot be used to analyse the large majority of the smart contract can, to some extent, be translated from source code or byte code into F* [5, 12] where the verification can more easily be performed. Other work operates on high-level source code available for Ethereum or Hyperledger [16], [13, 14] pro ivaliable for Ethereum or Hyperedger [10], [15, 14] pro-oses a formal definition of the EVM, that is extended in [1] owards more automated smart contract verification and the consideration of gas. Formal verification often requires (incomplete) translations into other languages or manual user nteraction (e.g.: [30]). Both of these reasons make formal verification unsuitable to be used on a large number of con tracts, as it is required in this work.

bilities in smart contracts [15] and in combination with sym-

bolic execution to discover issues related to the ordering of

Symbolic execution has been used on smart contracts to detect common [28, 25, 21, 38] vulnerabilities. This technique also allows to find specific kinds of misbehaving contracts [27]. It can further provide values that can serve to ger erate automated exploits that trigger vulnerabilities [18]. The ame technique is used in this paper. Symbolic execution has the advantage of being capable to reason about all possible execution paths and states in a smart contract. This allows for the implementation of precise heuristics while achieving a low false positive rate. Another advantage is that symbolic execution can be applied directly to bytecode, thus making it well suited for our purpose of analysing more than 2 million smart contracts for which source code is largely not avail able. The disadvantage is the large number of possible paths that need to be analysed. However, in the case of smart contracts this is not an issue, as most are not very complex and very short. Moreover, smart contract by grow arbitrarily large due to the gas limit enforced by the Ethereum blockchain.

To the best of the authors' knowledge, this paper is the first

In this work, we investigated an emerging new type of fraud in Ethereum: honeypots. We presented a taxonomy of hontools have their own methods to label a domain as being consent from the volunteers, who were rect "manipulated" or "blocked". Satellite creates an array of five metrics to compare the resolved IP against: Matching IP. Matching HTTP content hash, Matching TLS certificate, ASN, and AS Name. If a response fails all of the control metrics, it is classified as blocked. Quack first makes an HTTP-lookike request to port 7 of the Echo server with a benign omain (example.com). If the vantage point correctly echoes

IV. ETHICAL CONSIDERATIONS

cation with prominent activ

Our direct measurements involve sending requests for potentially censored content from vantage points inside Russia. This creates a potential risk to participants who own and control these vantage points. We consulted with our activist collaborators, who assured us that even if the anonymized vantage points, data centers, or ISPs are discovered, there has never been any punitive action on the part of the Russian revertment or others assist entities who do not comply with

We obtained our VPSes from commercial VPS platforms whose operators understand the risk in offering network an computing services. In collecting the data from our VPS platform, we did not subject anyone in Russia (or elsewhere to any more risk than they would already incur in the course of operating a VPS service;

organizational or ISP infrastructure. As in the c and residential probes, there is a possibility to operators of these remote vantage points at r is no documented case of such an operator be a crime due to any remote Internet measurem domain is hosted. We also set up reverse DNS records, WHOIS records, and a web page served from port 80 on each machine

The most recent sample of RUBL contains 132,798 unique domains and 324,695 unique IP addresses. It also contains a list of 39 subnets ranging from /24s to /16s. This section characterizes both the full RUBL blocklist and the final filtered

A. IPs and Subnets

As mentioned in Section III, we examined the responsiveness of the IPs on the blocklist. Only 121,025 IPs on the blocklist (37.3%) were reachable from our controls. Our control measurements were highly concordant; over 99% of IPs that were reachable at some control vantage point were reachable. at all control vantage points. The low rate of respons (37.3%) might be the artifact of our measurement, as the might be alive but not responding on port 80, such as proxies configured on custom ports.

Figure 2: Incoming call screen of different experiments.

whether the recipient was convinced by the scam (transcript in Appendix D.1) and, depending on how they responded, (2) or convinced them not to believe the scam (Appendix D.3). We recorded the participant's voice recording for the second question. After the second survey question, the autodialer system plays an ending message stating the researcher's contact

aler was configured to collect the following inputs from the ecipient: Continued, Entered SSN, Convinced, Unconvinced,

3.5 Ethics

These experiments were a deceptive study on involuntary participants, and therefore we deeply considered the ethical issues. To address the ethical issues inherent in our experiments, we carefully designed the experiments and worked vith our university's IRB, to not simply obtain approval but cause, to have scientifically valid results, we could not obtain nformed consent (this would bias the results of the study) and that the call was an actual scam call). To protect our partici-

The nature of this experiment, studying telephone phishing attacks, involves deception as well as involuntary participa-tion. Both aspects are critical to receiving scientifically valid esults-informing the participants of the study would sigificantly bias the results. However, the use of deception ca leading them to believe they fell victim to a scam. Therefore,

consisted of two questions: (1) a survey question that asked once throughout the entire study duration (to minimize the Before proceeding with the study, we also worked with our university's IT security group to provide them with in-formation that would help to alleviate the concerns of our participants. This IT security group at ASU is responsible for the security of all aspects of the university. We shared with the security group the experiment contact list, the experimental design, and the incoming phone numbers (that we used to send the calls) so that the help desk personnel could information (transcript in Appendix E). In summary, during each step of the procedure, the autodibe prepared to handle any requests and reports. In this way,

> In recording the results, we also strove to do so ethically and in accordance with established IRB protocols. One of the major safeguards is that we did not record the Social Security number. While a spammer would typically want the Social Security number, all that we record is the fact that they pressed any digit. In fact, we did not even ask for the full Social Security number, and we performed no analysis our data—participants may have felt safe to input only the last four of their Social Security number (when they would not input the full number) or they input fake last four digits of their Social Security number. Although these measures may iminish the strength of our data, we believe ethics is a mor important aspect of designing a telephone phishing study

We ran the previously described procedure using the 10 described experiments during a workweek in the late March of 2017, during core working hours of 10:00am-5:00pm each day. We used an Internet-hosted autodialer4 to automate the process of sending out the telephone calls to the 3,000 recipi-

Website	Claimed Time	Actual Time (Min., Avg., Max.)
guerrillamail.com	"1 hour"	1, 1, 1 (hour)
mailinator.com	"a few hours"	10.5, 12.6, 16.5 (hours)
temp-mail.org	"25 mins"	3, 3, 3 (hours)
maildrop.cc	"Dynamic"	1, 1, 1 (day)
mailnesia.com	"Dynamic"	12.6, 12.8, 13.1 (days)
mailfall.com	"25 mins"	30, 30, 30 (days)
mailsac.com	"Dynamic"	19.9, 20.3, 20.7 (days)

B. Disposable Email Dataset

al the second		DEE II. Statistics of the conceted datas			
nd the actual	Website	# Emails	Dispos. Address	Uniq. Sender Address (Domain)	Ms; Sen
	guerrillamail	1,098,875	1,138	410,457 (190,585)	1,0
, Avg., Max.)	mailinator	657,634	10,000	27,740 (16,342)	55,
ours)	temp-mail	198,041	5,758	1.748 (1.425)	13.
	maildrop	150,641	9,992	786 (613)	3,9
	mailnesia	106,850	9,983	1.738 (686)	4.9
avs)	mailfall	75,179	9,731	3,130 (288)	75,
	mailsac	45,324	9,987	11,469 (8,019)	45.3
ays)	Total	2,332,544	56,589	452,220 (210,373)	1,29

the meantime, we have a script that constantly monitors each tracking. However, given the data collection method, the inbox to record the message deletion time. In this way, we obtain 25 measurements for each disposable email service.

As shown in Table I, disposable email services often analysis results later. First, our dataset only covers the userdon't delete emails as quickly as promised. For example, mailfall.com claimed to delete emails in 25 minutes but in actuality, held all the emails for 30 days. Similarly oppular email addresses monitored, but is incomplete with temp-mail.org claimed to delete emails in 25 minutes but respect to all the available addresses. As such, any "volume" kept the emails for 3 hours. This could be an implementation metrics can only serve as a lower bound. Third, we don't claim He developers or a false advertisement by the service.

Many of the services claim that the expiration time is not fixed inbox". Intuitively, users (in theory) would use disposable (which depends on their available storage and email volume). email addresses differently relative to their personal email Based on Table I, we only need to apply the early-timeout for addresses. Instead, we argue the unique value of this dataset temp—mail and guerrillamail to discard lower-ranked usernames, using a timeout of 1 hour and 3 hours respectively.

B. Disposable Email Dataset
We applied the crawler to 7 disposable email services from
October 16, 2017 to January 16, 2018 for three months. In
total, we collected 2,332,544 email messages sent to montotal, we collected 2,332,544 email messages sent to monitored email addresses. Our crawler is implemented using Selenium [7] to control a headless browser to retrieve email content. The detailed statistics are summarized in Table II. For 5 of the disposable email services, we can cover all 10K

We are aware of the sensitivity of the dataset and have addresses and almost all of them have received at least one email. For the other 2 email services with very a short expiration time (temp-mail and guerrillamail), we focus on an abbreviated version of the popular usernames list. The number of emails per account has a highly skewed distribution. About 48% of disposable email addresses received only one email, and 5% of popular addresses received more than 100 carefully have controlled the crawling rate to minimize the impact on the respective services. For example, we enforce

emails each.
Each email message is characterized by an email title, email body, receiver address (disposable email address), and sender address. As shown in Table II, not all emails contain all the Users are typically informed that other users can also view the fields. 4 of the 7 disposable email services do not always emails sent to these addresses. (4) We have spent extensive keep the sender email addresses. Sometimes the disposable efforts on detecting and removing PII and personal email address in the first place. In total, there are 1,290,073 emails the opportunity to opt out. More specifically, we send out (55%) containing a sender address (with a total of 452,220 an email to each of the disposable email addresses in our unique sender addresses). These sender addresses correspond to 210,373 unique sender domain names. From the email body, we extracted 13,396,757 URLs (1,031,580 unique URLs after user

A. Ethical Considerations

e	# Emails	Dispos. Address	Uniq. Sender Address (Domain)	Msgs w/ Sender Address
lamail	1,098,875	1,138	410,457 (190,585)	1,091,230 (99%)
itor	657,634	10,000	27,740 (16,342)	55,611 (8%)
nail	198,041	5,758	1,748 (1,425)	13,846 (7%)
op	150,641	9,992	786 (613)	3,950 (3%)
sia	106,850	9,983	1,738 (686)	4.957 (5%)
1	75,179	9,731	3,130 (288)	75,164 (100%)
2	45,324	9,987	11,469 (8,019)	45,315 (100%)

Biases of the Dataset. This dataset provides a rare tracking from the perspective of online services (instead of

Defending against our Secret-uncovering Analysis. We have demonstrated that with INPUTSCOPE a variety of app secrets can be discovered. In certain cases, there may be a need to protect these secrets against our analysis. For instance, an app may consider its blacklist a secret, and developers

App may consider its blacklist a secret, and developers. cannot use the trusted server or TrustZone to perform the input hidden behaviors (or secrets) unknown to normal users in validations, e.g., client-side blacklist filtering is inevitable in Android mobile apps. validations, e.g., client-side blacklist filtering is inevitable in time-sensitive services such as live-streaming media. To defeat our analysis, there could be a number of possible avenues. For instance, an app can use obfuscation, or implement servers to thought of the possible avenues. For instance, an app can use obfuscation, or implements load the possible avenues. For example, AppsPlayground [31], SmartDroid [44], Dyndroid [26], and SMV-Hunters [34] are capable of exploring mobile app heavyors by recognizing UI elements and generations.

We have taken ethical considerations seriously in every step of our research. First, we only validated the vulnerabilities on our own accounts and our own smartphones (during our deep case studies), and we never try to compromise other users

themselves be bypassed with additional implementation effort.

can have severe consequences to either app users or devel-opers, and these apps need to be patched by app developers. o disclose vulnerabilities, and then we disclosed the details to

Static Taint Analysis. Our approach is based on static analysis tractocol [16], and SmartGen [45] focus more on the data LeakScope [46] extract hard-coded secret keys that are used

mobile app behaviors by recognizing UI elements and generating appropriate user input accordingly. However, this work generates input dynamically. In our work, we leverage static analysis and only focus on string related input generation.

classification to detect sensitive privacy data from user inpu Unlike leveraging UI text to detect malicious behaviors, o work focus on user input in general to recognize its hidden behaviors through carefully defined validation context that is

effect the OS or servers. Unlike these works that extract the events, permissions), INPUTSCOPE intends to uncover hidde behaviors are triggered by user input at the Java bytecode leve

Malware Detection. Prior efforts also focus on finding hidder

While input validation has been well studied in vulnerabil-While input validation has been well studied in vulnerability discovery, in this paper we have demonstrated that input
validation can also have another important application, namely
exposing input-triggered secrets such as backdoors (e.g., secret
access keys, master passwords, and secret privileged commands) and blacklists of unwanted items (e.g., censorship
keywords, cyber-bulling expressions, and weak passwords). To
understand the severity of such input validations in mobile apps
at scale, we developed a tool. INPUTS COPE. To automatically Input Validation. Input validation has been well studied in the and the content involved in the validation to automatically

Quantcast performs the check only once, the domain and the website also do not need to be sustained. Merely registering for tracking may even suffice to be ranked: over 2 000 domains are

2) Alternatives: Quantcast states that it also uses traffic data 2) Alternatives: Quanticast states that it also uses traffic data from 'ISPs and toolbar providers' [64]. ISPs sell traffic data to third parties [18], and Quanticast may be buying these services to generate the number of page visits and therefore the rank for non-quantified websites. However, we cannot determine which ISPs may be used. As for extensions, we were unable to discover any extensions reporting to a URL that was obviously related to Quanticast.

have a large impact on the reputation of the rankings as well as potentially affect third parties, we conduct an ethical review of Because of their commercial nature, the providers of popu-

r issue without any statement, and we received no response from Quantcast. None of our test domains were (retroactively) removed from any rankings after our notification.

VI. AN IMPROVED TOP WEBSITES RANKING As we showed the different methods used to generate

As we snowed, the directed metanos used to generate popularity rankings cause undesirable effects on their properties that can potentially sway the results and conclusions of studies In addition, we showed that researchers are prone to ignore or be unaware of these effects. We also proved that these rankings show several pitfalls that leave them vulnerable to leave seals a proposal configuration, further equipments publishing the proposal control of the prop large-scale manipulation, further reducing their reliability and suitability to research. Nevertheless, popularity rankings remain essential for large-scale empirical evaluations, so we propose improvements to existing rankings as well as a new ranking that has characteristics geared towards research.

Even though the methods for data collection and processing of the existing lists are usually unknown, our experiments

suggest that their providers employ little defense against large-scale manipulation. We outline techniques that the providers could use to make these lists more resilient to attacks. Detecting and deterring singular instances of fraud ensure and Quantcast rely on the reporting of page visits; within the realm of online advertising, techniques have been designed to subvert click inflation [2], [16], [51]. As we saw that not all

may imply that Alexa already employs some of these tactic To deter large-scale manipulation, ranking providers could employ tactics that increase the effort and resources required to affect many domains to prohibitive levels. This therefore avoids significant influence on research results, even if these tactics may not be sufficient to stop small-scale manipulation.

For a traffic reporting extension, the profile setup could interaction can be requested, and fraud detection as discussed earlier may be required. For providers that use both, the two metrics can be compared to detect anomalies where only one source reports significant traffic numbers, as we suspect such manipulation is already happening for Alexa Certif

Data could be filtered on the IP address from which it originates. Ignoring requests from ranges belonging to cloud providers or conversely requiring requests to come from ranges known to belong to Internet service providers (e.g. through its autonomous system) does not block a single user from reporting their traffic. However, using many IP addresses concurrently in the provider of the providers of the provider of the providers of the provider of the providers of permitted ranges. This technique is particularly useful for Umbrella's list; for the other lists, using many IP addresses is not strictly necessary for large-scale maning

period. Of the 500,716 homes scanned by WiFi Inspector on

2.5 Internet-Wide Scanning

We further augment the WiFi Inspector data with data colunderstand whether the vulnerabilities present on gateways (i.e., home routers) could be remotely exploitable. Similarly tion between Censys and Avast data for a 24-hour period on anuary 30, 2019 to control for potential DHCP churn. We also check whether devices that accept weak credentials for authentication present login interfaces on public IP addresses. We discuss the results in Section 4.

2.6 Ethical Considerations

WiFi Inspector collects data from inside users' homes. To ensure that this data is collected in line with user expecta-tions, we only collect statistics about homes where the user explicitly agreed to share data for research purposes. Thi ata sharing agreement is not hidden in a EULA, but out lined in simple English. We show the dialogue where user cknowledge this in Figure 1. We note that this is an explicit opt-out process. The data sharing agreement is the last mesage shown to the user before the main menu, meaning users o not need to wait and remember to turn off detraction

In order to keep up to date information on the devices in a home, WiFi Inspector runs periodic, automated scans of the local network. Automated scans do not perform any ulnerability testing or password weakness checks; they only identify devices through banners and MAC addresses. We limit our analysis to homes where a user explicitly manually initiated a network scan. To protect user privacy and minimize risk to users, Avast only shared aggregate data with our team. This data was aggregated by device manufacturer, region, and device type The smallest region contained over 100,000 homes. We never

the aggregates in this paper will be stored long term. is anonymized and no personally identifiable information i Inspector data satisfies personal data protection laws, such

lid not collect any additional data for this work, nor did the

Figure 2: Devices per Region—There is significant variance in device usage across regions. The largest presence is in North America, where homes have a median seven hosts.

require at least one computer and one router to be included ollected when explicitly necessary for the security function

Conversely, homes in South Asia have a median two hosts

It is vital that the security community understands the types of IoT devices that consumers install and their respective egional distributions given their increasing security and privacy implications. In this section, we provide one of first large-scale analyses of these devices based on scans from

The presence of IoT devices varies by region. For example, while more than 70% of homes in North America have an IoT device, fewer than 10% of homes in South Asia do (Figure 2). Media devices (i.e., smart TVs and streaming devices are the most common type of device in seven of the eleven regions, in terms of both presence in homes (2.5%-42.8%) nd total number of devices (16.6%-59.0%). Four regions differ: surveillance devices are most common in South and Southeast Asia, while work appliances are most common in East Asia and Sub-Saharan Africa. We show the most popular devices in each region in Table 4.

are strong correlations between regions for the types of deices that are popular.² In other words, the most popular types of devices are similar across regions. Still, certain pairs of regions differ. For example, homes in all Asian regions are east similar to homes in North America. On the other hand, nomes in geographically similar regions (e.g., South Asia and Southeastern Asia) are highly correlated, even when they dif-fer from the global distribution. The fact that distinct regions

²To quantify the preference for difference types of devices across regions

Space devoted to discussions related to ethical issues

Organization of Ethical Discussion Section

Point out the issues

Our experiment involves task1, task2,..., which may involve ethical questions Q1, Q2 and Q3...

Principles: citations

We followed report1, paper1. We designed the experiment according to report2, paper2.

Mitigations

We have done our best!

- Although we cannot rule out the possibility of xxx risk, we have taken xxx steps to reduce the possible risk.
- We try to balance between the benefits and the potential harm caused by our xxx...
- The nature of this experiment, studying xxx, involves xxx as inevitable ethical issues

Helpful third parties

- IRB. Work closely with IRB to design the study. Consulted with IRB.
- University's General Counsel. Consultations on specific legal issues.
- Experts and colleagues. Discuss how to design the experiment.
- University's IT security group, or other community responsible for security issues.

Key Points of Ethical Considerations

User Consent

Give snapshot/citation

- We only collected xxx where the user explanation agreed to xxxx policy.
- We've made user consent eye-catching, clear and easy to understand.

Please don't skip this

Nearly every software product you use collects information about you. Search engines, games, everything. We do the same. This allows us to provide better products and services for you. **But we promise to respect your privacy**. We also promise that we will never publish or share any of your personal information outside nor allow anyone else to use it to contact you for marketing purposes without your consent.

We do use the information that we collect to help us understand new and interesting trends. We may share this information with third parties outside

However, before we do that, we will remove anything that identifies you personally. For more information, read our Privacy Policy.

If after installing this product, you'd prefer not to participate in data sharing with and third parties, you can opt-out at any till by unchecking the 'participate in data-sharing' box in the settings.

Anonymization

- Protect identifiers, e.g., IP address, client-ID
- Remove sensitive information, e.g., PIIs

CONTINUE

Example of user consent snapshot

Data Usage

- All collected data is stored on secured servers, and only authorized persons have access to this data
- We keep the dataset strictly to ourselves.
- Inside the company, as intern.....

Solutions to Improve My Project

Main ethical-related content of the modifications:

- Details of data collection process
- Details of user consent
- Removed research content that may disclose private information
- Steps taken to mitigate the potential harm
 - 1. Access to data sets
 - 2. Remove of sensitive data (PII)
 - 3. Data usage & storage
- More comprehensive ethical discussion



Ethical discussion in

IMC' 20 submission



Ethical discussion in

ACSAC' 21 submission

Good Luck!

Unsolved Questions

• There are no IRBs in most of the domestic universities, except for medical departments.

学者呼吁: 国内高校也该建立伦理委员会了

这所"双一流"高校成立学术伦理委员会

2018-11-27 · 一读EDU

2019-12-17 22:38

中国人民大学学术伦理委员会工作会议暨学术边界与底线学术研讨会公告

2019/12/10

为推进一流大学建设,深入学习领会习近平总书记在全国教育大会上的重要讲话和中央全面深化改革委员会第九次会议精神,推动构建覆盖全面、导向明确、规范有序、协调一致的科技伦理治理体系,中国人民大学定于2019年12月11日在北京主办"中国人民大学学术伦理委员会工作会议暨学术边界与底线学术研讨会"。会议将邀请相关部委领导、高等教育研究专家、"双一流"建设高校相关部门负责人等作主题发言,会议规模100人左右。



Unsolved Questions

IRB REVIEW PROCESS



Berkeley Human Research Protection Program

IRB Decision is Required Prior to Contacting Participants or Collecting Data



清华大学医学伦理委员会

校内项目: 1500.00元/次 校外项目: 2500.00元/次

伦理审查委员会(Institutional Review Board, IRB)由来自社会科学各个领域的专家组成,根据国家的相关法律、法规和有关政策,对项目进行伦理审查、评价、指导,并依据伦理原则审查和监督涉及人体的研究活动,以保护受试者的权益和安全。各项研究工作需在获得IRB批准后方可执行,项目执行期间接受IRB的持续监督,定期向IRB报告进展,研究方案修改后及时向IRB报批。

2010年12月9日,清华大学医学伦理委员会(IRB)成立;2011年5月23日,清华大学IRB在美国卫生与公众服务部的人类研究保护办公室(OHRP)登记备案。清华大学IRB委员来自基础医学、临床医学、心理学、生物医学工程、法学等不同学科领域,并设有专职秘书一名。

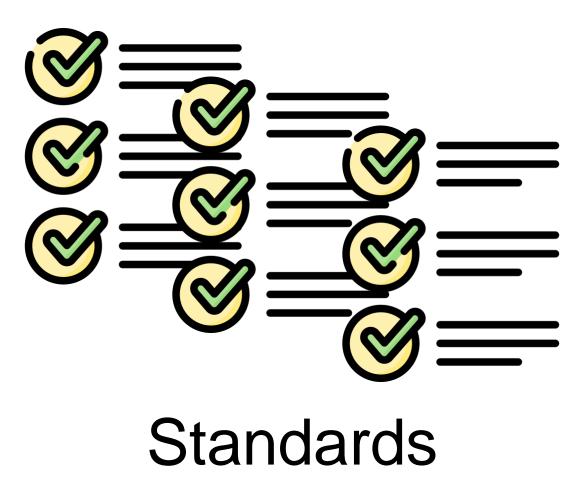
清华大学IRB的成立,将保证我校各项涉及人的生物医学研究均能遵循伦理学规范,最大程度的保护受试者的权利、利益和福祉。

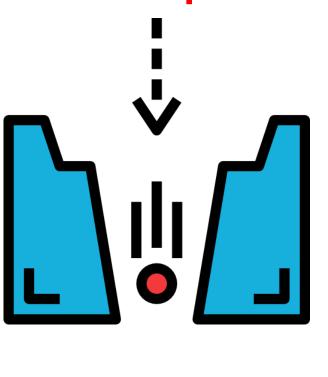
Temporary solutions:

- Apply reviews from the IRB of co-authors' universities
- Consult the legal department of the cooperating companies

Unsolved Questions

Lack of authoritative, systematic and practical guidance.







Huge Gap

How to address?







Summary

 We should get into the habit of considering and discussing ethical issues in our works.

- •The best time to think about ethics is before you start the research, followed by now.
- •There is a lot of work to be done on ethics compliance for the security community.

Ethical Considerations in Network Security and Network Measurement Research

Thanks.