Where art thou, Eve?
Experiences laying traps for Internet eavesdroppers

Tavish Vaidya   Eric Burger   Micah Sherr   Clay Shields
Georgetown University

Abstract

This paper describes a set of experiments we conducted to answer the question: *just how prevalent is Internet interception?* That is, if we sent our most sensitive information (bank information, passwords, etc.) in the clear, should we expect to regret it?

For a little over a year, we sent different types of Internet traffic over unencrypted channels between multiple clients and servers located at geographically diverse locations around the globe. Our messages contained seemingly sensitive and valuable information, including login credentials for banking sites, password reset links, etc. In total, we found *no* instances in which our information was acted upon by an eavesdropper.

This paper details the numerous challenges—technical, legal, and ethical—of setting up and maintaining a year-long, large-scale honeytrap. We discuss some fundamental limitations of such an experiment, and argue why our results should not be misinterpreted to suggest that message encryption is gratuitous.

1 Introduction and Goals

It has recently become easier for Johnny to encrypt [23, 29]. Likely due to successful efforts such as the Let's Encrypt free certificate authority and the push for ubiquitous STARTTLS between mail transport agents, a significant portion of the Internet's traffic is now encrypted. To illustrate, as of early February 2017, according to Mozilla's Firefox Telemetry data, more than half of loaded web pages were retrieved using HTTPS [17]; Google reports that 87% and 82% of the respective outbound and inbound email transmissions to/from Gmail are encrypted [15]. This general trend towards normalizing encryption follows the conventional wisdom that potentially sensitive information should never be sent unencrypted on the Internet.

Perhaps surprisingly, there is little existing work that empirically measures the consequences of not following this advice. That is, if I don't encrypt, should I expect to regret it?

Clearly, performing traffic capture and analyzing plaintext is trivial, especially when the potential eavesdropper is advantageously positioned in the network to observe the communication. Moreover, weaknesses in the Internet's routing infrastructure [7, 14] allow eavesdropping even when the eavesdropper's network location does not naturally lend itself to interception. Hence, a *targeted* user who does not encrypt his communication is likely to be observed by the interested party.

We now know that the Internet is commonly subject to bulk surveillance by intelligence agencies. However, while there is still always the potential that recorded communication could later be recalled and used against the communicants, we were interested in the more immediate *and criminal* threat of illegal interception.

This work poses the question: *how dangerous is it for an untargeted ordinary user to communicate sensitive information on the Internet without encryption?* That is, if Johnny ignores the conventional wisdom and transmits sensitive information through unencrypted channels, should he expect to be harmed?

To answer these questions, we designed and performed a yearlong experiment in which we attempted to measure the degree to which users' unencrypted communications were both collected and acted upon. Conceptually, our experiments constituted an Internet-wide honeytrap in which we sent a moderately-sized volume of unencrypted messages between clients and servers located at geographically diverse locations. Our messages contained falsified login credentials and other sensitive information, sent only between accounts that we controlled (that is, we did not spam[1]), ensuring that in the absence of unauthorized interception no one should act on these bogus messages. Conversely, attempts to use the sensitive information, for example by logging into a site

[1] We consider the many ethical questions posed by our study later in the paper.

with the observed credentials, indicate both that the information was intercepted and that the interceptor acted upon the information. By monitoring whether our “bait” was used, we can empirically determine a lower bound for interception on the Internet.

The main contribution of this paper is a retrospective accounting of the significant challenges—technical, legal, ethical, and institutional—that we faced to both instantiate and maintain our honeytrap. Perhaps naïvely, at the onset of this project, we initially envisioned a simple experiment in which we would send and receive unencrypted messages to/from various location on the Internet. In actuality, even before we deployed our experimental apparatus, we encountered a number of interesting and challenging legal and ethical questions. In this paper, we describe our experiences with our institutional organizations and enumerate many of the hurdles we faced towards launching our experiment.

We additionally discuss what worked—and what did not—in constructing an Internet-wide honeytrap, and argue about the seemingly inherent difficulties of performing such an experiment.

2 An Experiment in Eavesdropping Detection

There is unfortunately little prior work that empirically measures both how often Internet interception occurs and whether such interception leads to tangible harm. (A discussion of the related work is provided in Section 4.) Towards advancing our understanding of Internet interception, we were interested in the following research questions:

1. How often does Internet interception occur?
2. Of the traffic that is intercepted, how often does the eavesdropper act upon the information in the intercepts?
3. Are certain types of messages (e.g., unencrypted emails that contained plaintext passwords vs. telnet login credentials) more likely to be intercepted and acted upon than others?
4. Where does interception most commonly occur—near the sender, receiver, or somewhere along the network path between the two?
5. Relatedly, are there areas of the Internet in which interception is a more common occurrence? That is, are there areas of the Internet that experience a higher frequency of eavesdropping?

2.1 Scope

Since interception can be a passive act that is difficult to detect, we dismissed the first goal and instead focused on interceptions that were acted upon.

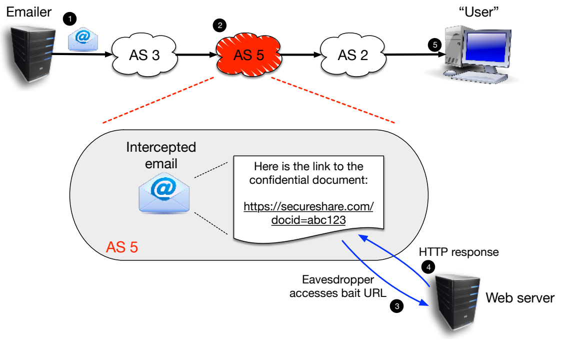

Emailer
1
AS 3
2
AS 5
AS 2
5
“User”
Intercepted email
Here is the link to the confidential document:
https://secureshare.com/docid=abc123
AS 5
HTTP response
4
Eavesdropper accesses bait URL
3
Web server

Figure 1: Workflow of our honeytrap using email (SMTP) bait.

Domain name
hasslefreetax.com
loanswithease.com
creditprocard.com
financialsindia.com
hastlefreetax.com
inyourffingface.com
mytaxeshelp.com
payroll-cheque.com
consultingforwealth.com

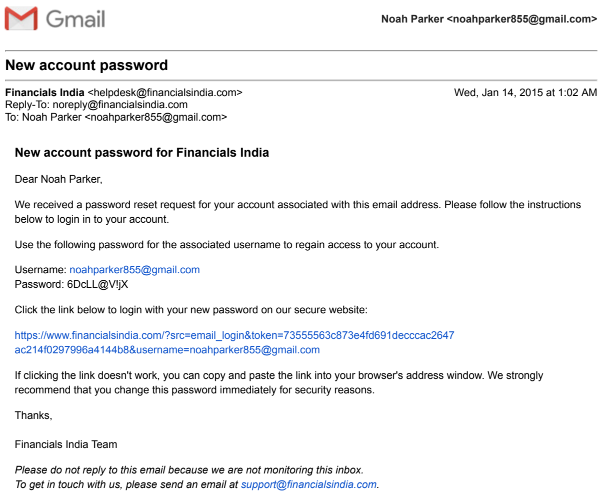
Table 1: Source domains of bait emails.

Consequently, a significant weakness of our study is that the prevalence of interception that is acted upon may be much smaller than that of traffic that is solely intercepted (and perhaps stored). The latter, for example, would include bulk surveillance operations whereas the former generally does not. While unauthorized interception is arguably always a violation of privacy[2], our interest primarily lied with the more tangible consequences of sending sensitive information in the clear. We were especially interested in cases in which an eavesdropper would attempt to use intercepted credentials or otherwise leverage its interception to further harm the user. The focus of this paper specifically targets *criminal activity*: the illegal interception of network traffic for criminal gain.

2.2 Baiting the Eavesdropper

Our high-level approach for measuring interception was to create a distributed infrastructure in which servers sent unencrypted messages to clients containing sensitive information. In particular, we transmitted—in the clear—login credentials and links to password reset pages and shared documents.

[2] In many countries, unauthorized interception of Internet traffic is a felony regardless of whether that information is later acted upon by the interceptor. In particular, unauthorized interception of electronic communication in the United States risks a five year prison term under the Electronic Communications Privacy Act [28]. Bates et al. [6] and Sherr et al. [24] provide fuller discussions of U.S. interception law from a computer science perspective.



Noah Parker <noahparker855@gmail.com>

New account password

Financials India <helpdesk@financialsindia.com> Wed, Jan 14, 2015 at 1:02 AM
Reply-To: noreply@financialsindia.com
To: Noah Parker <noahparker855@gmail.com>

New account password for Financials India

Dear Noah Parker,

We received a password reset request for your account associated with this email address. Please follow the instructions below to login in to your account.

Use the following password for the associated username to regain access to your account.

Username: noahparker855@gmail.com
Password: 6DcLL@V!jX

Click the link below to login with your new password on our secure website:

https://www.financialsindia.com/?src=email_login&token=73555563c873e4fd691decccac2647ac214f0297996a4144b8&username=noahparker855@gmail.com

If clicking the link doesn't work, you can copy and paste the link into your browser's address window. We strongly recommend that you change this password immediately for security reasons.

Thanks,

Financials India Team

Please do not reply to this email because we are not monitoring this inbox.
To get in touch with us, please send an email at support@financialsindia.com.

Figure 2: Example bait email.

Email Service Provider	No. Accounts
gmail.com	14
outlook.com	11
gmx.com	8
mail.com	7
hotmail.com	5
inbox.com	4
yahoo.com	3
aim.com	1
accountant.com	1
yandex.com	1
australiamail.com	1
planetmail.com	1
usa.com	1

Table 2: Distribution of recipient email addresses, by email service provider.

Figure 1 provides an overview of our distributed honeytrap. We operated email servers on five virtual private servers (VPSes) purchased from commercial web hosting providers in geographically and administratively distinct areas of the Internet: on the east and west coasts of the U.S., and in Russia, Brazil, and the Netherlands. We registered one or more domains for each email server (see Table 1) and sent emails from those domains to a fixed set of email addresses (step ❶ in Figure 1). In total, we used 58 email accounts which resided on popular free email services (e.g., Gmail, Hotmail, Yahoo, and Inbox; see Table 2) and on our own private email server hosted at our university.[3]

We anticipated that an eavesdropper positioned somewhere along the path traversed by a transmitted email would intercept the message (step ❷) and inspect its content, either manually or, more likely, through automated techniques.

The emails were constructed such that each contained information that we believed would interest an eavesdropper. The emails also contained a unique, trackable identifier. For example, some emails appeared to contain "download links" to files stored on a file sharing service, while others contained links to reset passwords. An example bait email is presented in Figure 2. To appear legitimate, each email was signed with a valid DKIM signature and contained a valid SPF record for the server that sent the email.

As shown in Table 1, we chose domains that implied (falsely) that the emails originated from a financial institution (e.g., loanswithease.com, hasslefreetax.com, financialsindia.com). Our hypothesis was that accounts that were seemingly associated with financial institutions would be especially valuable to the (criminal) eavesdropper.

An eavesdropper that accessed the "bait" URLs in the email (step ❸) would send its request to a web server that we hosted that would, in turn, log the request and transmit a seemingly valid response (step ❹). Except for creditprocard.com[4], each website operated over HTTPS using a genuine domain validated (DV) TLS certificate, issued by a popular commercial certificate authority. To avoid capturing any actual person's credentials, the webpages themselves showed only a "down for maintainence" message and did not collect login information. We relied on the unique URLs in the emails to verify that an eavesdropper acted upon an intercepted email.

Finally, to verify that our email apparatus was operating correctly, we confirmed that emails were received by the intended email account (step ❺).

In summary, we transmit information in the clear that we hope will pique the interests of an eavesdropper. If the eavesdropper attempts to use the information in the intercepted email—either by using the credentials in the email to log into a site (under our control) or by clicking on a link (hosted by a web server under our control)—then we detect such actions and conclude that interception occurred.

2.3 Growing our Trap

An early concern with our initial experimental setup was that it implicitly assumed that an eavesdropper who intercepts potentially hundreds of millions of emails would nevertheless select, examine, and act upon our bait emails. Given the prevalence of email spam [16] and—worse—phishing emails [4] that appear similar in struc-

[3] We emphasize that we operated these email addresses and that all email involved in this project originated from machines that we controlled and were addressed to our own email addresses. In short, we talked to ourselves and attempted to determine whether anyone illegally listened in.

[4] We were initially denied a DV TLS certificate for this domain. We suspect that the CA maintained a list of suspicious terms for domain names that could indicate fraud, and that some portion of creditprocard.com matched this list. The CA asked us to first to show the content being served on creditprocard.com. Since we did not serve any content, we did not pursue this further.

ture and content to our bait emails, we looked for other methods of enticing the eavesdropper.

In particular, we focused on unencrypted protocols that carry login credentials. Figure 3 shows our Post Office Protocol (POP)-based honeytrap. Here, we automate email clients regularly fetching their email via the POP protocol from our email server. To achieve greater network diversity, we use a VPN service to effectively distribute the clients' network locations (step ❶). The locations of the 802 VPN endpoints used in our study are plotted in Figure 5. Importantly, our automated clients use plaintext authentication when fetching their email over POP (step ❷), and hence an eavesdropper trivially learns these clients' login credentials by observing the traffic (step ❸).

In comparison to our vanilla email honeytrap, this bait has the advantage that POP is very often used insecurely (at least when not tunneled over TLS). Thus, rather than scanning through potentially hundreds of millions of emails, an eavesdropper could easily filter for unencrypted POP exchanges to steal users' credentials (step ❹). To detect such instances, we record unauthorized attempts (i.e., those not made by us) to log into to the email server.

In a similar vein, we conducted a parallel honeytrap in which automated clients, connected via a VPN (see Figure 4, step ❶), use telnet to log into one of our servers (step ❷). We believed that telnet was a particularly attractive target for an eavesdropper, since its use is almost always insecure and exposes login credentials. That is, we intuited that a resourceful eavesdropper would hone in on telnet connections since these are likely to yield login credentials (step ❸). To determine whether our telnet credentials were intercepted and acted upon (step ❹), we carefully monitored the logs of our telnet servers.

2.4 Experimental Results and Findings

We operated our honeytrap from May 2014 until June 2015. During the first half of the study, we sent 4,182 bait emails. In the experiment's latter half, we transmitted unencrypted credentials via 351,360 POP fetches and 184,456 telnet logins.

While the quantity of bait emails may at first blush seem relatively small given the long duration of the study, we purposefully chose a "bait rate" that we believed would not raise suspicion. Specifically, we ensured that each of our 58 email addresses received no more than one password reset email from a given website in a two day span. This was done to reduce the chances of being labeled as spam and to more closely mimic what we perceived as realistic behavior. For similar reasons, POP fetches occurred only every 45 minutes, per client, and telnet connections occurred every 10 to 20 minutes.

Findings: In total, we did not find a single instance in which active interception occurred. The URLs listed in our bait emails were never accessed. Nor did anyone attempt to log in with the credentials that were sent in the clear through either POP fetches or telnet logins. This indicates that either no interception occurred within the time period of our study; that our traffic was intercepted but was uninteresting to the eavesdropper; or that the interception was purely passive.

3 Challenges

In what follows, we present a retrospective analysis of our experiment. In particular, we describe the myriad technical challenges of performing a large-scale, longterm study of Internet eavesdropping (Section 3.1), many of which likely contributed to our negative results. We also identify some of the ethical and legal challenges of our experiment and describe our approach at navigating these issues in partnership with our institution's Office of General Counsel and Social and Behavioral Sciences Institutional Review Board (Section 3.2).

3.1 Technical and Design Challenges

In general, we found that operating an effective large, longterm honeytrap is far more difficult than we anticipated.

Ensuring adequate coverage of the Internet: It is very likely that our honeytrap infrastructure was inadequately small. In total, we had 802 VPN endpoints and only six server locations. In contrast, there are nearly 55,000 ASes on the Internet [8]. While our bait traffic likely passed through the largest transit networks (e.g., Level 3, Cogent, Telia, etc.), we conjecture that the illegal interception and acting upon of intercepted content is more likely to occur at the Internet's edges, where we have especially limited coverage.

Several factors made it difficult to scale up our infrastructure:

- Each VPS service provider had its own unique interface. Installing our virtual machine images was a very manual process, and was made more complicated by the sometimes subtle quirks of the different hosting providers. Deploying a number of instances at a single provider was far more tractable, but we avoided such replication since it would not contribute to achieving greater network diversity.
- We were limited by the small set of languages spoken by the authors. While many hosting sites had English translations, many did not.
- We were advised by our General Counsel's Office against purchasing services in certain countries.

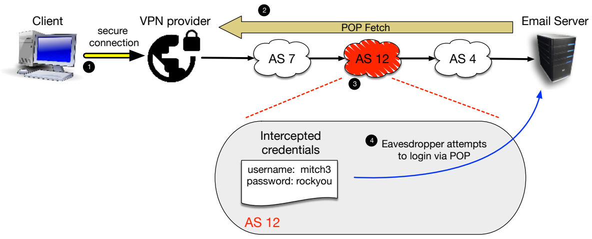


Figure 3: Workflow of our honeytrap using email-fetching (POP) bait.

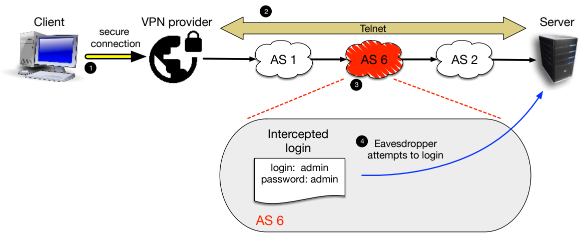


Figure 4: Workflow of our honeytrap using telnet bait.

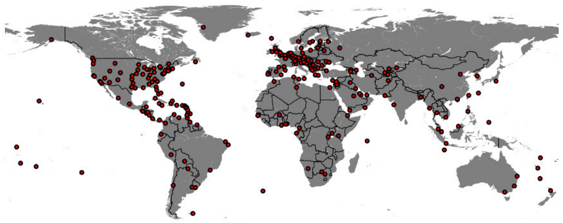


Figure 5: Locations of VPN endpoints used for POP and telnet bait experiments.

United States law also forbids us from contracting services in certain locations. In general, however, we did not find such restrictions especially onerous, since the number of such locations is relatively small.

- Scaling to thousands or tens of thousands of geographically distributed hosted servers is expensive and would cost at least tens of thousands of dollars per month. The administrative overhead of managing this many bills would quickly overwhelm our departmental administrators.
- Finally, each hosted server requires its own domain name and certificate. While our partnership with a major CA eliminated the cost of obtaining certificates[5], crafting hostnames that might attract the attention of eavesdroppers (see Table 1) is a manual exercise requiring quite a bit of creativity, and does not easily scale.

Luring the eavesdropper: Our most significant technical difficulty was the creation of bait that is sufficiently attractive that it lures an eavesdropper into taking some observable action.

Our initial experimental design included only email-based bait. It quickly became apparent that no one was falling for our traps.

A likely contributing factor to the absence of click-throughs was that we relied only on made-up sites and domain names. We suspect that eavesdroppers are either unwilling or unable to comb through potentially enormous email interception logs to determine which domains appear most useful.

An obvious mitigation strategy is to avoid fictitious sites and instead mimic legitimate businesses. Mimicking legitimate sites could potentially significantly increase the value of our bait emails. In particular, eavesdroppers may filter for emails that, because they are sent from selected financial institutions, could yield information useful for fraud or theft. For example, we posit that an intelligent eavesdropper may search for intercepted emails from, say, `support@bankofamerica.com` that also contain the phrase “password reset link”. Although we very briefly considered forging messages from actual businesses, we quickly abandoned such an approach as it crossed ethical and legal lines we wished to avoid.[6]

An interesting extension of our experiment—and one that raises even more daunting legal and ethical questions—is to communicate *real* account information via unencrypted channels. If, for example, we created a bank account with $10 in it and regularly transmitted the username and password associated with that account in unencrypted emails, would our money disappear?

A potentially[7] less legally thorny approach is to communicate Bitcoin wallets in the clear. Here, an eavesdropper has a tangible incentive for acting upon the interception—it can easily steal the money associated with the wallet. Transmitting Bitcoin wallets avoids having to spoof an actual bank. However, as is also the case with the $10 left in a bank account, such experimentation inherently rewards criminal behavior with money.

For practical, legal, and ethical reasons, we decided against such extensions and instead restricted ourselves to sending content only from made-up institutions.

We were more surprised that our POP and telnet-based baits were ignored. In particular, since “high-value” network devices such as routers, switches, and PDUs often

[5] We began this project before Let’s Encrypt began publicly issuing certificates. However, using a Let’s Encrypt certificate would not lend credibility to a site purportedly run by a financial services firm.

[6] This does raise the interesting legal question as to whether messages sent and received by the same party constitute *communication*. That is, is it legal to forge messages from a bank if the sender sends such messages only to himself? The context of our experiment raises a compounding issue: does the forger incur additional legal risk if the purpose of the self-directed communication was to bait other parties (albeit criminal parties) to read the forgeries?

[7] We emphasize that the authors have no formal legal training.

use telnet, we anticipated that telnet sessions would be extremely attractive to an eavesdropper. Either this assumption is incorrect (that is, we overvalued telnet credentials) or, as discussed above, our coverage of the Internet was inadequate.

3.2 Legal and Ethical Challenges

Like other research attempting to understand the criminal element, we are operating at the edge of ethics. In this section, we describe our ethical dilemmas and experiences with our general counsel's office and IRB.

Since we were not trying to examine the motivations, characteristics, or identities of the criminal element, our IRB very quickly determined this project was not human subjects research. Clearly we agreed with this determination.

However, there were some issues that nagged at us. For example, what if we had detected interception of our emails? If this had occurred, our experimental setup would have recorded the IP addresses of the eavesdroppers (assuming they did not conceal their network location through Tor [11] or some other anonymity service), since our web, telnet, and POP servers logged the origin of received requests.[8] The issue here is in many countries, unauthorized interception is illegal [28]. Many countries, including the United States and almost all European nations, have legal means to compel people who have information relevant to a crime to produce that information. As such, if we had detected interception and the relevant authorities found out we had evidence and they had jurisdiction, we could have been compelled to divulge the detected IP addresses. Depending on the country, that could result in arrest or worse for the perpetrator.

What was not clear was whether we were trying to deceive criminals as individuals. If so, this project may have slipped into the human subjects research area. It was our expectation that much of the interception and notification machinery of the criminal element would be automated. However, in parts of the world where labor is inexpensive, criminal gangs might have been using people to intercept mail.

We had the expectation of humans triggering the interception detection, either by clicking through on a link of a password reset email or using telnet or POP credentials. One of the driving factors for presenting an "Under Construction" webpage was to not unnecessarily deceive the person doing the interception.

We figured we could not outright impersonate an existing financial institution. However, we did have some interest by some financial institutions to participate. When we discussed the research plan with our general counsel (GC), they emphatically confirmed our initial suspicion that impersonating, even to a lesser extent (e.g., calling our site the "Bank of Froo" to impersonate the "Bank of Foo"), could be a violation of U.S. law.

We believe our GC's office did a good job considering U.S. law when approving the project and setting limitations on the parameters of our emails and impersonation. However, in retrospect we might have been well served to consider the laws applicable to our project in other jurisdictions. Here the obvious relevant jurisdictions are the locations of the retrieving mail server and the hosting mail repository.

An even more complex question is do countries that are simply transiting our traffic have jurisdiction? Clearly, the interpretation of the United States government is they do, more especially if both ends of the communication are outside the United States.[9]

4 Related Work

Honeypots have long been used both to carry out security research and to protect networks and detect potential attacks [1, 2, 9, 10, 19, 21, 26]. In prior work, honeypots lure attackers, but rely on the adversary to discover the (mimicked) service(s) themselves. In contrast, we proactively bait an adversary by sending login credentials in the clear.

The prevalence of unauthorized traffic interception has also been studied by Ballani et al. [5]. There, the authors focus on indirectly observing interception of traffic by detecting BGP traffic hijacking attempts. They did not employ any bait content for gathering direct evidence of any interception.

There has been a large body of existing work that examines criminal behavior on the Internet. Of particular note, Ramachandran and Feamster [22] and Anderson et al. [3] investigate spam campaigns and their infrastructure by performing network level measurements and evaluating the data collected by following the spam links. Levchenko et al. [18] present a detailed study of email spam and quantify the various resources necessary to monetize spam. Several others have studied the infrastructure of botnets and their command-and-control mechanisms by collecting data from passive interaction or active control of the botnet [20, 25, 27, 30]. To the best of our knowledge, we are the first to attempt to detect instances of illegal interception by baiting the eavesdropper into performing an observable action.

[8] Here, it is worth emphasizing that our logging was quite typical. For example, web servers routinely log the IP addresses of the requesting clients.

[9] *See* for example Executive Order 12333 with respect to the NSA's authority to intercept traffic of foreign sourced and sinked traffic of foreign persons that happen to transit the United States.

Arguably, more attention has recently been paid to the ethics of computer security research. For example, program committees (including that of USENIX Security) have fairly recently begun requiring authors to discuss in their submissions how they approach responsible disclosure and human subjects research, when applicable. This has, in part, been influenced by previous calls to develop a computer security ethics community [12] and the formation of ethics panels [13] that help provide guidance to security researchers to assess and minimize ethics-related risks. We believe these are positive steps towards making computer security a more mature and responsible discipline. We described our own ethical dilemmas and the mechanisms through which we sought guidance in Section 3.2.

5 Discussion and Conclusion

None of our bait was taken and acted upon by an eavesdropper. It is difficult to determine why that is. It might be that there is too much traffic for an eavesdropper to attempt to determine, on the fly, whether a particular message would be valuable unless it matches a known-valuable format or address. Our traffic thus might simply have gone unnoticed, while some other traffic from a known bank (for example) would have been targeted. Given the size and diversity of Internet endpoints, it is clearly possible that we were not using an ISP or path where general eavesdropping was taking place and a wider study would have shown where it was actually occurring. It might be that eavesdroppers are cautious not to attack traffic that might reveal their presence and some portion of our experimental setup raised too many red flags—perhaps because the domains did not look completely established or were relatively newly registered.

Or maybe there just are not many eavesdroppers at all. It could be that other forms of illicit activity are more profitable and that the time and effort required to filter Internet traffic looking for unencrypted valuables is not worth the time, when encryption is increasingly common and spear phishing and ransomware pay more handsomely.

We might have done better had we not come up against the limits of what we considered prudent and ethical. Sending email that appeared to be a real bank or that gave access to a real account might have elicited eavesdropper action. Sending a Bitcoin wallet might have been appealing as well, but as we described we opted not to provide eavesdroppers with funding.

Our experiments imply that sending unencrypted data may be less dangerous that expected. This, however, would be the wrong conclusion to draw. Should many parties omit encrypting or otherwise protecting valuable data in transit, interception might become more valuable and worth an attacker's effort. While one might hope that their traffic goes unnoticed, hope provides little protection. Encryption does.

Acknowledgments

This work is partially supported through the Security and Software Engineering Research Center (S^2ERC) and through S^2ERC industry affiliates. The S^2ERC at Georgetown University is supported by the National Science Foundation under Grant No. 1362046. However, no NSF or other Federal funds were used for this work. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation, S^2ERC, or the industry affiliates of S^2ERC.

References

[1] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis. A multifaceted approach to understanding the botnet phenomenon. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, pages 41–52. ACM, 2006.

[2] K. G. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. P. Markatos, and A. D. Keromytis. Detecting targeted attacks using shadow honeypots. In *Usenix Security*, 2005.

[3] D. S. Anderson, C. Fleizach, S. Savage, and G. M. Voelker. Spamscatter: Characterizing internet scam hosting infrastructure. In *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, 2007.

[4] Anti-Phishing Working Group (APWG). Phishing Activity Trends Report. 4th Quarter 2016. Available at http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf.

[5] H. Ballani, P. Francis, and X. Zhang. A study of prefix hijacking and interception in the internet. In *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, SIGCOMM '07, 2007.

[6] A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. In *Network and Distributed System Security Symposium (NDSS)*, February 2012.

[7] K. Butler, T. Farley, P. McDaniel, and J. Rexford. A Survey of BGP Security Issues and Solutions. *Proceedings of the IEEE*, 98(1):100 –122, January 2010.

[8] Center for Applied Internet Data Analysis (CAIDA). AS Ranking. Available at http://as-rank.caida.org/.

[9] D. Dagon, X. Qin, G. Gu, W. Lee, J. Grizzard, J. Levine, and H. Owen. Honeystat: Local worm detection using honeypots. In *International Workshop on Recent Advances in Intrusion Detection*, pages 39–58. Springer, 2004.

[10] E. De Cristofaro, A. Friedman, G. Jourjon, M. A. Kaafar, and M. Z. Shafiq. Paying for likes?: Understanding facebook like fraud using honeypots. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 129–136. ACM, 2014.

[11] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In *USENIX Security Symposium (USENIX)*, August 2004.

[12] D. Dittrich, M. Bailey, and S. Dietrich. Building an active computer security ethics community. *IEEE Security Privacy*, 2011.

[13] Ethics Feedback Panel. Ethics Feedback Panel for Networking and Security. Available at https://www.ethicalresearch.org/efp/netsec/. Retrieved 1 April, 2017.

[14] S. Goldberg. Why is it Taking so Long to Secure Internet Routing? *Communications of the ACM*, 57(10):56–63, 2014.

[15] Google. Email Encryption in Transit. Available at https://www.google.com/transparencyreport/saferemail/. Retrieved 20 March, 2017.

[16] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. Spamalytics: An Empirical Analysis of Spam Marketing Conversion. In *ACM Conference on Computer and Communications Security (CCS)*, 2008.

[17] LetsEncrypt. Percentage of Web Pages Loaded by Firefox Using HTTPS. Available at https://letsencrypt.org/stats/. Retrieved 20 March, 2017.

[18] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, et al. Click trajectories: End-to-end analysis of the spam value chain. In *Security and Privacy (SP), 2011 IEEE Symposium on*. IEEE.

[19] J. G. Levine, J. B. Grizzard, and H. L. Owen. Using honeynets to protect large enterprise networks. *IEEE Security Privacy*, Nov 2004.

[20] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang. Botnet: Classification, attacks, detection, tracing, and preventive measures. In *Proceedings of the 2009 Fourth International Conference on Innovative Computing, Information and Control*, 2009.

[21] N. Provos et al. A virtual honeypot framework. In *USENIX Security Symposium*, volume 173, pages 1–14, 2004.

[22] A. Ramachandran and N. Feamster. Understanding the network-level behavior of spammers. In *ACM SIGCOMM Computer Communication Review*, 2006.

[23] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland. Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software. In *Symposium On Usable Privacy and Security*, 2006.

[24] M. Sherr, G. Shah, E. Cronin, S. Clark, and M. Blaze. Can They Hear Me Now?: A Security Analysis of Law Enforcement Wiretaps. In *ACM Conference on Computer and Communications Security (CCS)*, November 2009.

[25] S. S. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles. Botnets: A survey. *Computer Networks*, 2013. Botnet Activity: Analysis, Detection and Shutdown.

[26] L. Spitzner. The honeynet project: Trapping the hackers. *IEEE Security and Privacy*.

[27] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna. Your botnet is my botnet: Analysis of a botnet takeover. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 2009.

[28] United States Congress. Omnibus Crime Control and Safe Streets Act of 1968: Title III. Pub. L. No. 90-351, 82 Stat. 197, USA, 1968. (codified as amended in 18 U.S.C. Sect. 2510-2522).

[29] A. Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium (USENIX)*, 1999.

[30] L. Zhuang, J. Dunagan, D. R. Simon, H. J. Wang, I. Osipkov, and J. D. Tygar. Characterizing botnets from email spam records. *LEET*, 2008.