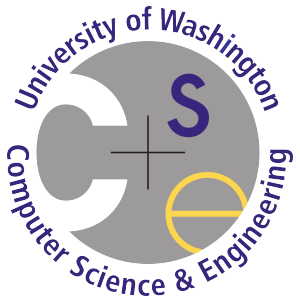
Investigating the Computer Security Needs and Practices of Journalists

USENIX Security 2015

Susan McGregor
Columbia Journalism School

Polina Charters, Tobin Holliday,
Franziska Roesner
University of Washington



Motivation: Securing Journalist-Source Communications

TECHNOLOGY

Hackers in China Attacked The Times for Last 4 Months

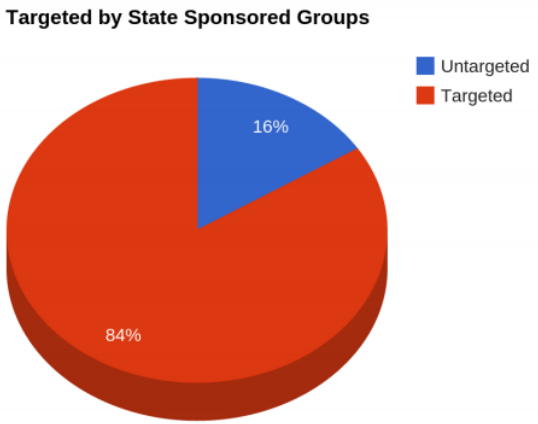
By NICOLE PERLROTH JAN. 30, 2013

Washington Post Joins List of News Media Hacked by the Chinese

By NICOLE PERLROTH FEB. 1, 2013

RANK*	NEWS SITE
1	nytimes.com
2	indiatimes.com
3	wsj.com
4	usatoday.com
5	washingtonpost.com
6	latimes.com
7	examiner.com
8	smh.com.au
9	sfgate.com
10	chron.com
11	thehindu.com
12	nypost.com
13	hindustantimes.com
14	eenadu.net
15	chicagotribune.com
16	hollywoodreporter.com
17	indianexpress.com
18	theglobeandmail.com
19	theage.com.au
20	manoramonline.com
21	amarujala.com
22	washingtontimes.com
23	thestar.com
24	dnaindia.com
25	nj.com

Top 25 New Sites



*From Alexa Top 25 New as of 03/23/2014 by @ashk4n

Huntley & Marquis-Boire, BlackHat Asia, 2014

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Motivation: Securing Journalist-Source Communications

POLITICS

C.I.A. Officer Is Found Guilty in Leak Tied to Times Reporter

Justice Dept. Investigated Fox Reporter Over Leak

By **BRIAN STELTER** and **MICHAEL D. SHEAR** MAY 20, 2013

Email

Share

GCHQ captured emails of journalists from top international media

- Snowden files reveal emails of BBC, NY Times and more
- Agency includes investigative journalists on 'threat' list
- Editors call on Cameron to act against snooping on media

"I don't want the government to force me to act like a spy. I'm not a spy; I'm a journalist... What are we supposed to do? Use multiple burners? No email? Dead drops? I don't want to do my job that way. You can't be a journalist and do your job that way."

— Adam Goldman

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Motivation: Securing Journalist-Source Communications

Despite these and other examples...

even investigative journalists rarely use secure communication tools.

GnuPG

Tor

SILENT CIRCLE

SECUREDROP

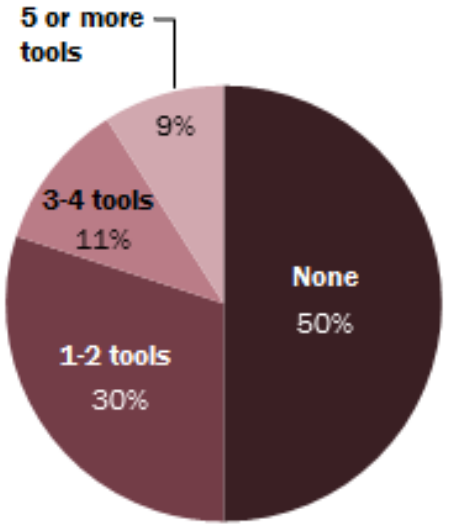
Wickr LEAVE NO TRACE™

LastPass ****

Mailvelope

Use of Digital Security Tools Varies

% of IRE journalists who use __ of the eight security tools asked about



PEW RESEARCH CENTER

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Why Not?!

Observation: The computer security community builds a lot of tools that might be useful for journalists, ***but we don't deeply understand the journalistic process!***

> "I report on unauthorized immigrants a great deal and have concerns about how to communicate with them without putting them at risk. That said, asking them to use encrypted methods of communication I think would create a greater sense of threat about talking to me and make it more difficult to report. Many are also not extremely computer-savvy. This is something I struggle with a great deal."

38% of IRE reporters have, in the past year, at least somewhat changed the way they communicate with sources. 4 of 10

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Our Work

Investigating the Computer Security Needs and Practices of Journalists

We are:
Experts from the journalism and computer security communities

Our subjects:
15 full-time journalists working at a range of news media organizations in the U.S. and France

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Study Design

Conduct **in-depth interviews with full-time journalists** at recognized media organizations operating across a range of media, including print, digital, broadcast and wire services

Interview questions focused on **"typical" workflows**, communications and information storage and retrieval.

Threat models were elicited through questions about risk and consequence of information exposure.

Qualitative data analysis: interviews were coded for themes by 2 independent coders.
(average inter-coder agreement by Cohen's kappa: 0.88)

Our Participants

15 journalists in the U.S. and France

- **Organizations** ranged from large multinational media outlets to smaller, more single-subject oriented outfits.

- Participants' beats ranged from government to city life, capturing a **range of risks and sensitivities.**
  - One participant reported having *only* his laptop stolen from his home while working on sensitive stories.
  - Another reported strange technical glitches when communicating by phone with sources overseas.
  - Others report being physically surveilled.

Findings

Research Questions

- **What are journalists':**
  - General practices?
  - Security concerns?
  - Defensive strategies?
  - Computer security needs?

Findings

General Practices

- Participants use a wide range of communication methods, usually whatever is **preferred by the source.**

> ***[The source] probably understand[s] the threat model they're under better than I would.*** *So, it brings up an interesting question: do you go with what they're comfortable with? Or do you say, alright, actually let me assess what's going on and get back to you with what would be appropriate. [...]* ***People's first impression is that they would go by what the source feels comfortable doing. As opposed to stepping in and being paternalistic about it.***

Findings

General Practices

- **Long-term sources are common**, and often connect journalists to new sources.
  - The "Snowden use case" is rare!
- **Audio recording and digital note-taking** were primary forms of interview documentation.
  - Many participants use **third-party cloud services**, but few voiced concern about possible security risks.

Findings

Security Concerns

- **Primary concerns:**
  - Negative effects on source
  - Loss of credibility if source information was exposed
  - Government identification of sources
  - Disciplinary actions (e.g., losing job)

- **Additional concerns (unexpected for us!):**
  - Loss of competitive advantage
  - Potential financial consequences

Findings

Security Strategies

- **Non-technical**
  - Example: Meeting with sources in person *(though often more for journalistic than security reasons!)*
  - Example: Using intermediaries or code names
- **Ad hoc**
  - Example: Asking a source to prove ownership of a Twitter account by posting a sentence provided by the journalist.

Findings

Security Strategies

- **Technical**
  - Most common:
    - Encrypted email/chat (especially within org.)
    - Encrypted files (e.g. FileVault)
  - Rarely used: Tor, VPN, other secure messaging apps
  - (More details in the paper!)

Findings

Security Strategies

- **Common reasons for using security tools:**
  - a source required them
  - explicit digital-security training

- Where participants *did* make efforts to protect information, they often succeeded in one area **but left it exposed in another.**
  - Example: meeting a source in person but bringing a phone and/or using it to record.

Findings

Obstacles to Better Security Practice

- Because journalists often defer to sources' preferences, **the digital divide is a significant barrier to better communication security.**

> *"Most of the [sensitive sources] I've worked with [are] also people who probably aren't very tech-savvy. Like, entry-level people in prisons, or something like that. So if they were really concerned about communication, I don't quite know what a secure, non-intimidatingly techy way would be. [...]* ***Some of them don't even necessarily have email addresses."***

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Findings

Obstacles to Better Security Practice

- Absence of **clear, authoritative indicators about the protections offered** by particular tools.

> *"A lot of services out there say they're secure, but having to know which ones are actually audited and approved by security professionals — **it takes a lot of work to find that out."***

- **Lack of institutional support** in the form of installed software, machine admin rights, or educational resources.

Recommendations

Insights for Tool Design

- **Why don't journalists use more technical security tools?**
- **It's not just usability** -- tools must be built with an understanding of the journalistic process!
  - For example, secure anonymous document drops are useful for sources like Snowden, but less so for the (more common) case of long-term sources that may not initially provide sensitive information.

Recommendations

Insights for Tool Design

- In the vast majority of cases, **journalists depend on knowing a source's identity.**

> ***"If I don't know who they are and can't check their background, I'm not going to use the information they give.*** *Anonymous sourcing is fine if I know who they are, and I've checked who they are, and my editor knows who they are, but they can't keep that from me and then expect me to use the information they provide."*

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Recommendations

Insights for Tool Design

- The technological requirements of secure communications **raise barriers to working with less-expert or lower-income sources**, who may be the most vulnerable.
- **Usability, stability, & reliability** remain ongoing issues, especially for organizations.

Recommendations

Opportunities for Future Research

- **Knowledge management** (e.g. storing, searching, syncing and tagging story-related media) remains a significant unmet need.
  - Ad-hoc solutions (e.g., third-party services) may introduce vulnerabilities.
- **Audio transcription** presents a particular bottleneck, as well as potential vulnerability.

Recommendations

Opportunities for Future Research

"There were different kinds of litigation software that I was familiar with as a lawyer, where, let's say, you have a massive case, where you have a document dump that has 15,000 documents. [...] There are programs that help you consolidate and put them into a secure database. So it's searchable [and provides a secure place where you can see everything related to a story at once]. ***I don't know of anything like that for journalism."***

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Recommendations

Opportunities for Future Research

- Exploring methods of **secure first-contact** and ways to **manage the tension between anonymity and authentication.**

> ***"The first contact is never or very rarely anonymous or protected.*** *If someone wants to give me some information and we don't already know each other, how would he do it? He could send me an email, yeah, okay — but then how could I be sure it's him? Unless he contacts me with his real identity first.* ***It's very difficult to have the first contact secure."***

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Recommendations

Opportunities for Future Research

- Effective **metadata protection** for digital communications and storage.
- **Deeper exploration** of the journalistic process and the needs of sources.
- Understanding of the **role of journalistic organizations** in influencing security practices.

Thank you!

Investigating the Computer Security Needs and Practices of Journalists

USENIX Security 2015

Susan McGregor
Columbia Journalism School

Polina Charters, Tobin Holliday,
Franziska Roesner
University of Washington

Findings

General practices

Tool/technology	Number of participants	Inter-coder agreement
Email (unencrypted)	15	1.00
Google Docs/Drive	8	1.00
Microsoft Word	8	1.00
SMS	8	1.00
Social media	7	1.00
Dropbox	4	1.00
Skype	4	1.00
Evernote	3	1.00
Text editor	2	1.00
Chat (unencrypted)	1	1.00
Scrivener	1	1.00

Findings

Security concerns

Category	Concern	No. of participants	Inter-coder agreement
Threats to sources	Discovery by government	6	0.88
	Disciplinary action (e.g., lost job)	6	0.88
	Reputation/personal consequences	6	0.88
	Generally vulnerable populations (e.g., abuse victims)	4	0.65
	Discovery by others wishing to reveal identity	3	0.80
	Physical danger	3	0.86
	Prison	2	1.00
Threats to journalists or organizations	Reputation consequences (incl. loss of source's trust)	9	0.89
	Being "scooped" (i.e., journalistic competition)	6	1.00
	False or misleading information from a source	4	0.36
	Physical threats (incl. theft)	2	0.50
	Financial consequences	1	1.00
Threats to others	Political / foreign relations consequences	1	0.50
	Other	1	1.00

University of Washington Computer Science & Engineering

Columbia Journalism School

TOW CENTER FOR DIGITAL JOURNALISM

Recommendations

Insights for Tool Design

Category	Reasons for not using security technology	No. of participants	Inter-coder agreement
Usability and adoption	Not enough people using it	5	0.79
	Digital divide: sources don't have/understand technology	4	0.86
	Security technology is too complicated	3	1.00
	Hard to evaluate credibility/security of a tool	2	0.50
Interference with journalism	Creates barrier to communication with sources	5	0.64
	Doesn't want to impose on sources	5	0.83
	Interferes with some other part of their work	3	1.00
Other	Work isn't sensitive enough / no one is looking	8	0.41
	Uses a non-technical strategy instead	6	0.70
	Insufficient support from organization	2	0.80
	Tool doesn't provide the needed defense	1	1.00