PHYS.ORG

Computer security tools for journalists lacking in a post-Snowden world

July 22 2015

Edward Snowden's leak of classified documents to journalists around the world about massive government surveillance programs and threats to personal privacy ultimately resulted in a Pulitzer Prize for public service.

Though Snowden had no intention of hiding his identity, the disclosures also raised new questions about how effectively news organizations can protect anonymous sources and sensitive information in an era of constant data collection and tracking.

A new study by University of Washington and Columbia University researchers that will be presented next month at the 24th USENIX Security Symposium probed the computer security habits of 15 journalists across two continents and found a number of security weaknesses in their technological tools and ad-hoc workarounds.

Those included computer security tools that go unused because they introduce roadblocks to information gathering, inadequate solutions for basic tasks like transcribing interviews and failing to consider potential risks from cloud computing and other common practices.

"The way people try to bridge gaps can introduce security issues," said UW senior author Franziska Roesner, an assistant professor of computer science and engineering who focuses on computer security and privacy.

"If you use your iPhone to translate speech to text, for example, it sends that information to Apple. So if you record a sensitive conversation, you have to trust that Apple isn't colluding with an adversary or that Apple's security is good enough that your information is never going to be compromised."

News organizations' abilities to build trust with sources and gather sensitive information have been called into question by recent disclosures about surveillance: the U.S. Department of Justice's admission that it secretly obtained phone records from the Associated Press, Microsoft's admission that it read a blogger's personal Hotmail account to find a source of an internal leak and criminal investigations that have used email traces to identify and prosecute anonymous sources.

"Addressing many of the security issues journalists face will require new technical solutions, while many existing secure tools are incompatible with the journalistic process in one way or another," said lead author Susan McGregor, assistant professor at Columbia Journalism School and assistant director of the Tow Center for Digital Journalism.

"At the same time, there are clearly opportunities to build tools that really support journalists' workflow and build them in a secure way."

The researchers interviewed 15 working journalists from the U.S. and France about how they communicate with sources, what strategies they use to organize notes and protect sensitive information, and their use of existing information security tools. They found some reporters took steps to lessen certain types of security risks, but not others.

One journalist who went to great pains to protect the identity of sources by only meeting in person, for instance, used an iPad to photograph sensitive documents. Although roughly one-third of the reporters used encryption services to communicate with sources or protect their notes, a majority also used popular cloud services like Google Drive or Dropbox to store and share information.

That may be fine for the average user—or even most journalists—but anyone working with sensitive material ought to consider how much they trust that those servers will never be hacked, Roesner said.

"The flip side is that it's not just a matter of giving journalists information about the right tools to use—it's that the tools are often not usable," Roesner said. "They often fail because they're not designed for journalists."

For instance, the team found that reporters' number one goal—obtaining information—was often impeded by existing security tools that introduce roadblocks to communication. The communication methods that reporters used were driven by the preferences of sources, who have widely different experiences with and access to technology.

One open-source product that sought to let whistleblowers securely send documents to journalists was rarely used because it lacked the common mechanisms by which news organizations tend to authenticate a source's identity. Encryption tools that garble the content of an email or message unless someone knows the secure key can still leave behind traces of "metadata," which leak investigations or criminal prosecutions can use to prove a relationship between a reporter and a source existed.

One of the study's goals was to identify opportunities for the computer security community to better serve journalists, Roesner said. That might include building security applications into a wider content management tool that accomplishes other tasks that reporters would find helpful, such as transcribing interviews and tagging or organizing notes.

"Tools fail when the technical community has built the wrong thing," said Roesner. "We've been missing a deeper understanding of how journalists work and what kinds of security tools will and won't work for them."

More information: www.franziroesner.com/pdf/journalism-sec15.pdf

Provided by University of Washington

Citation: Computer security tools for journalists lacking in a post-Snowden world (2015, July 22) retrieved 5 May 2024 from https://phys.org/news/2015-07-tools-journalists-lacking-post-snowden-world.html