Influencing Mental Models of Security

Dr. Rick Wash, Department of Media and Information, Michigan State University, wash@msu.edu
Dr. Emilee Rader, Department of Media and Information, Michigan State University, emilee@msu.edu
Project URL: https://bitlab.cas.msu.edu/securitymodels

RESEARCH PROBLEM

Over 80 million households in the US have a computer in the home and an Internet connection. Home computer users have to make many security-sensitive decisions every day, such as "do I click on this suspicious link?" or "should I install this software update?"

People use mental models -- simplified understandings of socio-technical systems -- to make a wide variety of everyday computer security decisions. How do people learn these mental models? And how does this learning impact future security decisions?

APPROACH

To understand learning, we collected a corpus of materials that people can learn from, and then asked people for additional information about how they learned and what they learned.

To understand decision-making, we collected a wide variety of self-report data from users and compared it to log data from those users' computers. This allowed us to examine real-world decisions made after learning, and compare them with beliefs and knowledge of the users.

MAJOR FINDINGS

Current technologies make it difficult for **individuals** to learn about security:

- Automating the install of software updates makes it harder for people to learn how to make decisions about updates because there are fewer opportunities to learn [SOUPS 2014].
- More knowledge about security or technical issues is not associated with more secure behavior [SOUPS 2015].
- People can only accurately self-report security behaviors that are discrete and have visible outcomes [Under Review].

Many people learn about security from **other people:**

- People hear stories about security incidents informally from family and friends. These stories often contain lessons [SOUPS 2012].

> **Example story:** "My dad warned me that sometimes frauds will target university email addresses of students to trick them into giving up information about themselves. I made the mistake of offering up information even after this warning. It was from my 'bank' requesting that I verify my card information, otherwise my account will be suspended. Stupid me, I should have known that it was a trick. I had to end up canceling my card and getting a new one, freezing my accounts, etc. It was pretty embarrassing. I was a freshman though, and very dumb at the time. I quickly wisened up and have since never ever been a victim again. I won't be fooled twice." -- *User 6* from [SOUPS 2012]

- Traditional security education focuses on *how* to protect yourself, but stories from other people emphasize *who* is attacking and news stories discuss consequences of attacks [J. CyberSec 2015].

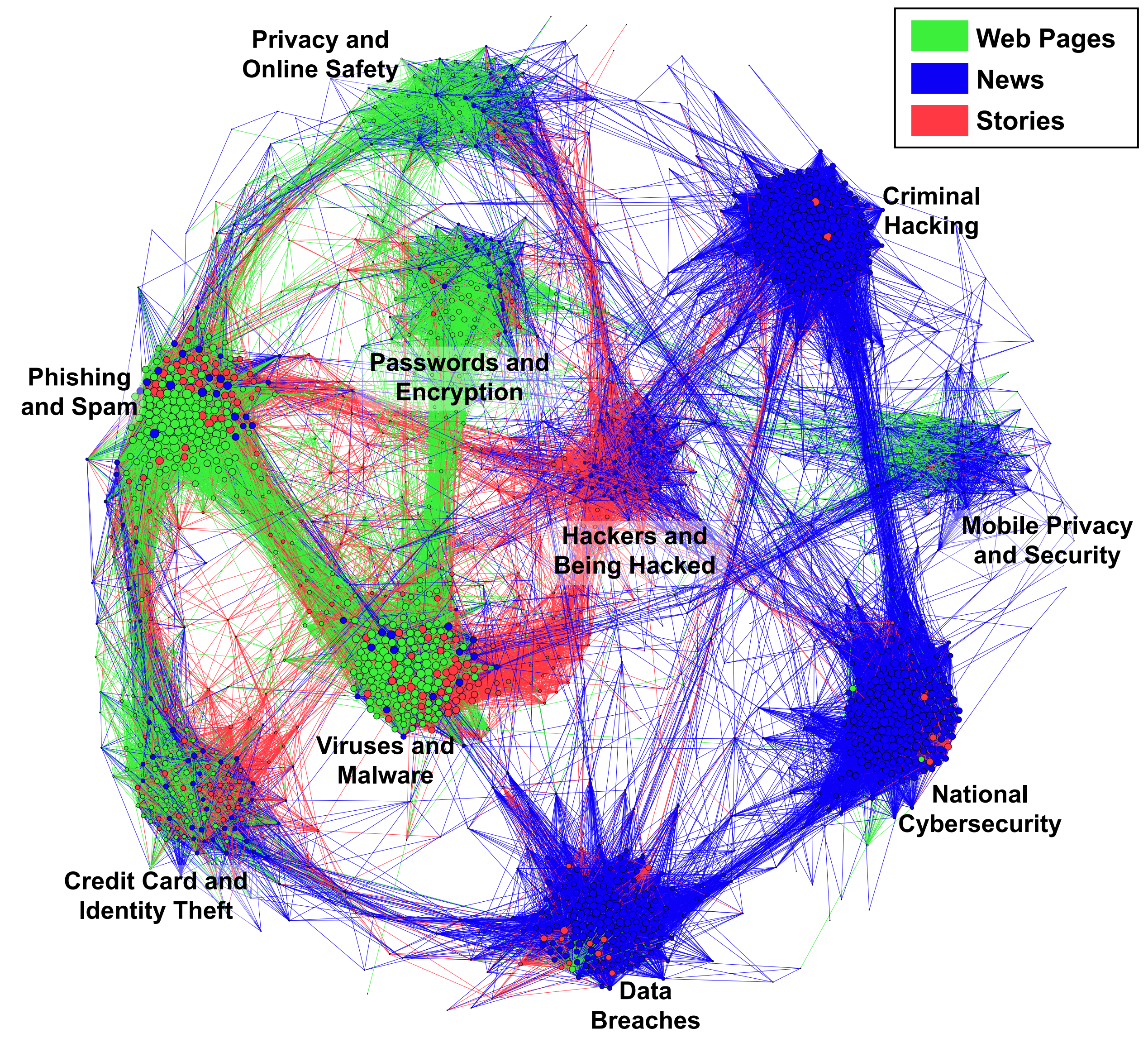

Figure 1: The document similarity graph, with clusters for each topic in security education web pages (green), news articles (blue), and interpersonal stories (red), collected in 2012. There is one node for each document in the dataset. Topics were identified using Latent Dirichlet Allocation (LDA). Larger nodes are connected to more other documents. Edges represent the Pearson correlation between the topic vectors for a pair of documents. The Hackers and Being Hacked topic is strongly connected to both Viruses and Malware and Phishing and Spam among the interpersonal stories. However, in both the web pages and the news articles, Hackers rarely co-occurs with either Viruses or Phishing. [J. CyberSec 2015]

People generalize security learning from one system to other, **technically unrelated** systems:

- Negative experiences with software updates create *spillover*, or a refusal to install even unrelated updates [CHI 2014].
- People re-use passwords they must enter frequently on many other websites, most likely because it is easiest to recall [SOUPS 2016].

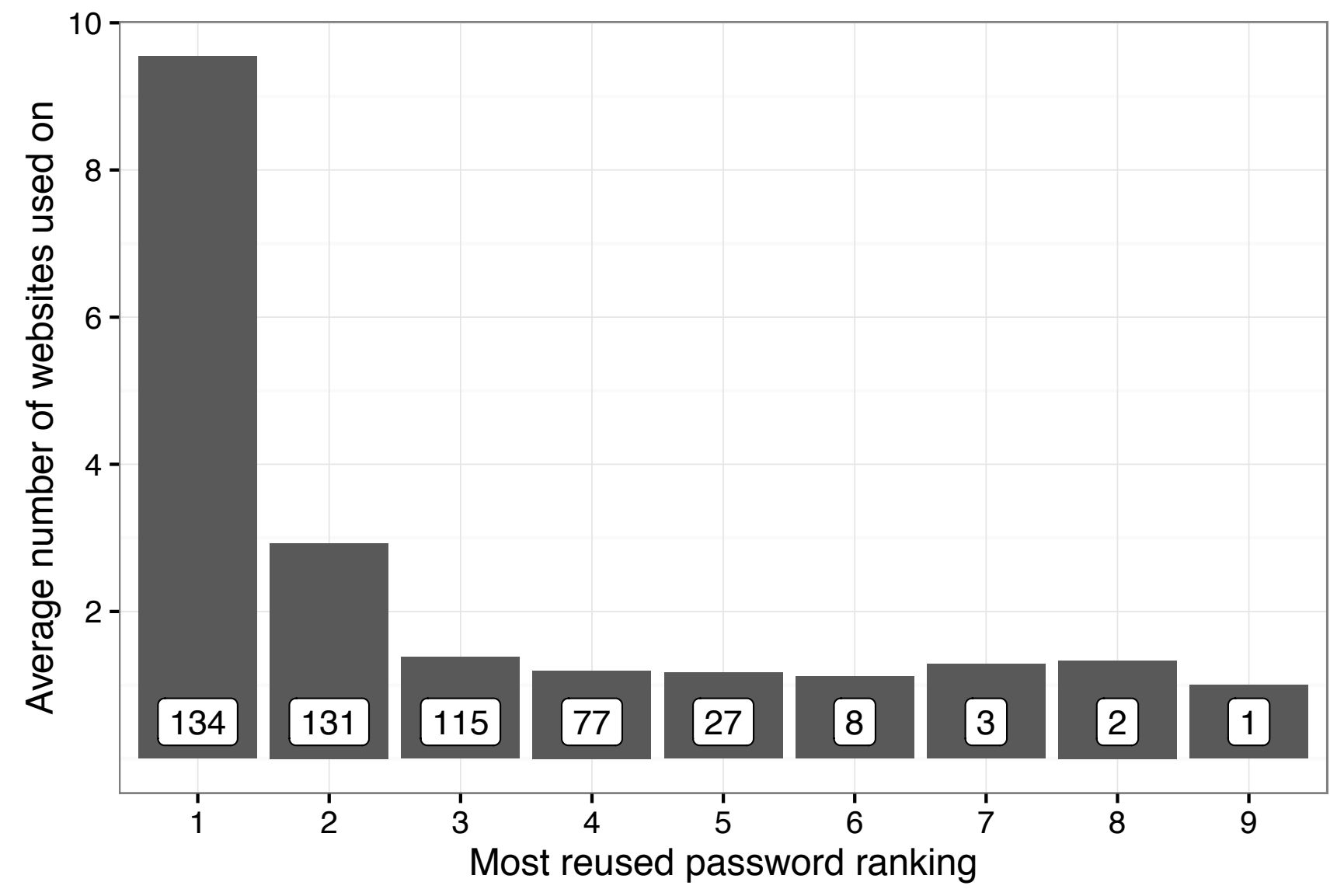

Figure 2: How often passwords were re-used. The leftmost bar shows the average for a subject's most re-used password; the second bar the second most re-used password; and so on. The number near the bottom of each bar shows the number of subjects with passwords at that rank. [SOUPS 2016]

Stories about security are an effective **alternative approach** for training end users:

- Stories, when presented by people similar to the user, are just as effective at preventing users from clicking on phishing links as advice from experts [In progress].

INTELLECTUAL MERIT

Learning about security is a social activity that involves hearing stories from friends and family and generalizing that knowledge across systems.

This learning creates two forms of socio-technical interdependence:

- What one person learns about security can spread to other people through stories.
- What one person learns from using one system can influence how they use other systems.

When done poorly, this interdependence spreads vulnerability through bad user decisions. If done well, this can enable systems to make the other systems around them more secure.

BROADER IMPACTS

- Trained 25 undergrads, 2 graduate students, and 1 postdoc in how to do interdisciplinary cybersecurity research.
- Over 50% of the team are women, and 3 research assistants are members of demographic groups that are underpresented in STEM research.
- Developed survey instruments and data collection code that has been made available to other researchers via the Open Science Framework (osf.io/r2mha/).
- Trained 2000 end users in phishing prevention.
- Spread knowledge about the challenges of protecting yourself online, and what can be done about it, to the general public through public speeches and news interviews.

REFERENCES

[SOUPS 2012] Rader, E., Wash, R., and Brooks, B. "Stories as Informal Lessons About Security".

[CHI 2014] Vaniea, K., Rader, E., and Wash, R. "Betrayed By Updates: How Negative Experiences Affect Future Security".

[SOUPS 2014] Wash, R., Rader, E., Vaniea, K, and Rizor, M. "Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences".

[SOUPS 2015] Wash R. and Rader, E. "Too Much Knowledge? Security Beliefs and Protective Behaviors Among US Internet Users".

[J. CyberSec 2015] Rader, E. and Wash, R. "Identifying Patterns in Informal Sources of Security Information".

[SOUPS 2016] Wash, R., Rader, E., Berman, R., and Wellmer, Z. "Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites".

[Under Review] Wash, R., Rader, E., and Fennell, C. "Can People Self-Report Security Accurately? Agreement Between Self-Report and Behavioral Measures".

This material is based upon work supported by the National Science Foundation under awards CNS-1116544 and CNS- 1115926.

MICHIGAN STATE
UNIVERSITY