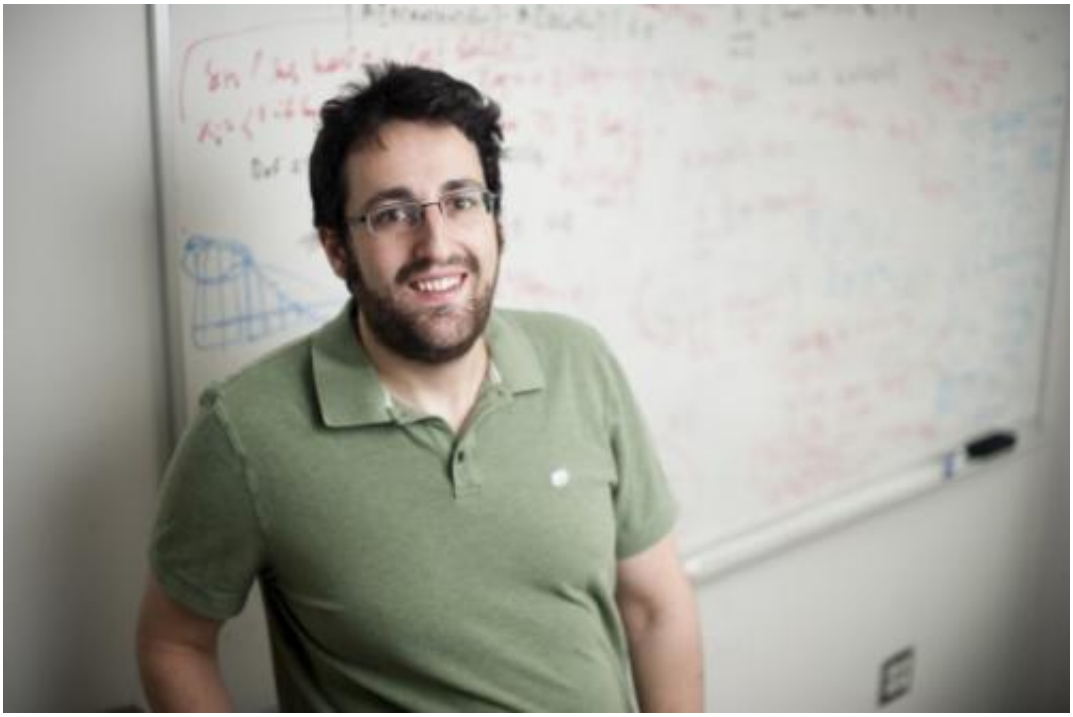
Sinister code-breakers, beware

January 24 2013, by Matt Collette



The research of Daniel Wichs, a new assistant professor in the College of Computer and Information Science, focuses on how cryptography can continue protecting personal data in an evolving digital age. Credit: Brooks Canaday.

In the early– to mid-20th century, governments commonly used cryptography to encrypt top-secret messages or military communications. But now that the computer and Internet age has evolved to a point where smartphones and tablets are readily available at our fingertips, its use has become much more widespread to meet the challenges of the 21st century, according to Daniel Wichs, a newly appointed assistant professor in

the College of Computer and Information Science.

"Cryptography is being used every day, but people probably don't even notice it," Wichs said. "Whether you're using Gmail or logging on to a site from your mobile phone, cryptography is there making sure others aren't able to see the data you're sending and receiving."

His interest in the field of cryptography blossomed as an undergraduate studying mathematics and computer science at Stanford University. The subject, he said, allowed him to apply complex mathematics with seemingly scant practical applications to solve real-world computer science problems related to security.

Wichs earned his doctorate from New York University in 2011 and later served as a Josef Raviv Memorial Postdoctoral Fellow at IBM before arriving at Northeastern this fall.

Wichs has noticed major changes in the field within the last few years. The massive expansion of cryptography work, for example, means researchers have to be much more focused on how outside forces, like hackers or foreign governments, try to break through encrypted systems or exploit unknown weaknesses.

In particular, his work focuses in part on what are called "side-channel attacks," in which third parties try to learn about an encrypted system by measuring information like how long a computer process takes or how much electricity is used by a given calculation.

"You can learn a lot of information just from these seemingly-meaningless details, so cryptography systems are starting to take them into account too by securing not just the data but also the computing system itself," Wichs said.

He noted that he is fascinated with cryptography because it merges theory and practical applications in ways that are seldom found in many fields of research.

"It's a really cool set of problems you're facing," he said. "How do you make sure data—which is a key part of nearly every component of our lives today—is secured?"

But perhaps the most important thing about cryptography research, Wichs said, is that the more time professionals spend working to protect critical data and systems, the less time the public should spend worrying about personal information breaches.

"If cryptographers do their job, you don't have to think about it all that much," Wichs said. "It's our goal to make sure these critical standards and protocols are in place."

Provided by Northeastern University