Google's Eric Grosse on security and innovation in the face of rising threats

At a February 3 Sandia/California Distinguished Lecture titled "Protecting the Cloud, Its Users, and Innovation," Dr. Eric Grosse, Google vice president of security and privacy engineering, shared Google's strategies for Internet security, its efforts to gain transparency on domestic surveillance, and how Sandia can help Google.

"In the old days, security came in three different grades: military, enterprise, and consumer," Grosse explained. "Security at the consumer level was not considered a major priority, but that's not the way it is today. The world has changed, and so have consumers. Gmail account owners include dissidents in countries with repressive governments – people who bravely put their lives on the line. They assume security people like me have done their job and are keeping their information safe. It's a tough standard to achieve, but it is where we are today."

He also spoke about another security issue: the U.S. government potentially abusing its domestic surveillance abilities. "There are valid law enforcement and national security reasons for this, but there is also a real risk for abuse," said Grosse. "I don't believe that abuse is happening today, but there are not a lot of checks and balances to provide reassurance. With other governments, we would certainly expect abuse to happen."

Working with industry partners, Google launched the Google Transparency Report [https://www.google.com/transparencyreport/], which details the number of government requests for user information and the number of accounts affected in six-month increments (read the Google blog post [http://googleblog.blogspot.com/2014/02/shedding-some-light-on-foreign.html]) dating back to 2009.

"Just today I am pleased to say we are now allowed to report on FISA [Foreign Intelligence Surveillance Act] requests," said Grosse. "I want this to be a real way that anyone on the outside can judge what is happening. The data shows that, at least for Google, there is not bulk surveillance through that legal channel. The number of accounts affected is modest – not as small as I would like, but not completely preposterous either."

Maintaining security is an ongoing battle

Turning to security at Google, Grosse said the company focuses much of its efforts on red teaming. "I don't mean a set team. We pluck out a couple of employees and give them a few weeks to break into a test Gmail account using any means they can imagine. There is a referee so they don't take down Google or get into real user data, but they are doing it on a live system like a military readiness exercise."

He described this approach as tremendously helpful, to the point where Google security feels it has an idea of how often adversaries break in based on the performance of the red teams. "Our people are amazingly talented and creative at breaking in. Some of the stories would make your skin crawl," he said. "I have a standing offer to other organizations – including yours – to do symmetric red teaming, where you try to break into us and we try to break into you."

Google also has a Vulnerability Reward Program [http://www.google.com/about/appsecurity/reward-program/], known as the "bug bounty." The company pays independent researchers when they find and report qualifying problems on Google-owned web services, including Google, YouTube, Blogger, and Chrome.

"There are people earning an annual income by reporting bugs to us," said Grosse. "That's embarrassing to me because my team works really hard not to have any bugs. We have even tried to hire some of these people to come work for us."

Passwords are dead

Losing data through a loss of credentials is one of the biggest security problems on the Internet today, even bigger than malware, according to Grosse. "We've put a lot of effort into authentication issues," he said. "Sites are getting knocked over and losing their password databases."

To demonstrate the damage that hackers can do, he cited examples of James Fallow [http://www.theatlantic.com/magazine/archive/2011/11/hacked/308673/], who wrote an article in the *Atlantic* about his wife's Gmail account being hacked in 2011; Josh Bryant [http://hackticool.com/post/75171875746], who evaded an attempt to steal his @JB Twitter handle; and Naoki Hiroshima [https://medium.com/cyber-security/24eb09e026dd], who was blackmailed into giving up his @N Twitter handle.

"We have to declare that passwords are dead," Grosse said. "We're past incremental changes. It's time to make a big leap forward. At Google, we think public encryption is the way to go. Our goal is to have a public key smartcard so malware cannot steal the secret key credential from it. The idea is not that malware on the device can't misbehave because there is nothing to stop that. If the malware can act as you on the device, then the malware can misbehave. But at least once you close the lid, you have stopped the threat."

Grosse also strongly encouraged everyone in attendance to turn on two-step verification [http://www.google.com/landing/2step/] for critical accounts like email and banking and to add a phone number and backup email address to the recovery systems for these accounts. "If all we know is your password and that is the only relationship between you and Google, we don't have enough information to know if it is really you trying to recover your password or someone pretending to be you," he said. "This is a bad way to be."

In closing, Grosse made a request of Sandia – secure the grid. "We worry about mitigating all these different risks, but one big risk we can't mitigate is somebody cutting off the supply of electricity," he said. "I was surprised to learn at Google that we count our data centers in terms of the number of megawatts because megawatts are that hard to get locally. So, I really need you to help the power companies secure the grid. It's really important."

###


The world has changed and so must we…