Software catches vulnerabilities on websites before they're exploited

September 17 2014, by Rob Matheson

Tinfoil's co-founders, Michael Borohovski ’09 and Ainsley Braun ’10. Credit: Courtesy of Tinfoil

Hacking is often done with malicious intent. But the two MIT alumni who co-founded fast-growing startup Tinfoil Security have shown that hacking can be put to good use: improving security.

Through Tinfoil, Michael Borohovski '09 and Ainsley Braun '10 have

commercialized scanning software that uses hacking tricks to find vulnerabilities in websites and alert developers and engineers who can quickly fix problems before sites go live.

Thousands of startups and small businesses, as well as several large enterprises, are now using the software. And around 75 percent of websites scanned have some form of vulnerability, Braun says. Indeed, a ticker on Tinfoil's website shows that the software has caught more than 450,000 vulnerabilities so far.

"Our No. 1 goal is making sure we're securing the Internet," says Braun, Tinfoil's CEO and a graduate of MIT's brain and cognitive sciences program.

While at MIT, Braun and Borohovski ran with a group of computer-savvy students who extensively researched security issues, inside and outside the classroom. For his part, Borohovski, a lifelong hacker, took many classes on security and wrote his senior thesis on the topic of Web security.

Tinfoil started as an enterprise, however, when Braun and Borohovski reconnected in Washington after graduating, while working separate security gigs. As a hobby, they caught vulnerabilities in websites that required their personal information, and then notified site administrators.

"We'd get emails back saying they'd fixed the vulnerability. But we could exploit it again," Braun says. "Eventually, we'd just walk them through how to fix it."

When job offers started pouring in, the duo saw potential. "We said, 'If people want to hire us to do this, then there's a need,'" says Borohovski, Tinfoil's chief technology officer, who helped build the firm's software.

Returning to Boston, Braun and Borohovski founded Tinfoil, with the help of MIT's Venture Mentoring Service, to launch the product. The startup has grown rapidly ever since: Recently, it partnered with CloudFlare, adding to a list of partnerships with Heroku, Rackspace, and others.

Finding vulnerabilities

Much like Google, the Tinfoil software works by crawling websites. "But instead of looking for text and images, we're looking for anywhere we can inject code to exploit vulnerabilities," Braun says.

The software uses techniques identical to those used by external hackers, says Borohovski, who studied computer science and engineering at MIT. "We don't have access to source code or anything that an external hacker wouldn't have access to. We just systematically go through every possible entry point and attempt to see if there's a vulnerability," he says.

Currently, the software has tactics to identify about 50 vulnerabilities, including the Open Web Application Security Project's list of the top 10 Web app risks. For each vulnerability discovered, the software can conduct anywhere from 10 to hundreds of tests. The Tinfoil team—now five employees—constantly updates the software as new risks and attacks are discovered.

One of the most common risks, for instance, is insecure cookies (data containing personal information). If someone logs on to a website through, say, a public Wi-Fi spot, it's possible for a hacker to steal an insecure cookie and pretend to be the user. Another popular vulnerability is one that allows hackers to inject arbitrary code into a website to wreak havoc.

On the user end, the developer sees a description of such

vulnerabilities—including its location and impact on the website—and step-by-step instructions on how to fix the vulnerability (by patches or other means), tailored to specific programming languages.

Although vulnerability-scanning software has been available since the early 2000s, Tinfoil's software is novel in that it's geared more toward developers, who are able to fix vulnerabilities as part of their workflow, Borohovski says.

"Any large enterprise has maybe 1,000 developers and a much smaller security team—maybe a dozen, or 100 for really large places," he says. While these developers have tests for some functional bugs, "there isn't anything that's part of that process for security scanning. We fit in there."

This is especially important in today's world, Braun adds, as websites make constant changes. Every tweaked line of code opens the risk of new vulnerabilities—and security teams may have trouble keeping up. "We can put some of that work on the developers," she says.

Rolling out Tinfoil

Tinfoil launched in Boston in 2011. Winning the $100,000 MassChallenge startup competition grand prize later that year helped the firm relocate to Palo Alto, Calif. But while here, Borohovski and Braun received guidance from the MIT Venture Mentoring Service (VMS) that played an integral part in Tinfoil's history; even today, Tinfoil still reaches out to the VMS for guidance.

Primarily, Braun says, the VMS helped them wade through the logistical intricacies of building a startup: creating a business plan, finding funding, hiring a lawyer, and more. (Braun's mother, Lucille, a financial advisor, is a mentor for VMS, but didn't serve on Tinfoil's mentor team.)

"Before we launched a startup, we had a boss and structure. But then we had to do everything, like design a website, advertise, marketing and sales, business strategy, hiring, engineering," Braun says. "The VMS helped us prioritize. They gave us homework and milestones we had to accomplish, so we held ourselves accountable."

For Borohovski, MIT played an earlier role in his path to security entrepreneurship. "It was where some of the Web-security seeds got planted," he says: At the Institute, he organized student teams for computer hacking competitions and took classes on the topic, including 6.857 (Computer and Network Security).

Additionally, he found encouragement in risk-taking and innovating for real-world applications. "The energy at MIT is all about building stuff," he says. "Everywhere I went, there were people working on things, and I couldn't stop being curious about them. I haven't been able to find that intensive building mindset anywhere else."

Pride in his alma mater is one reason why two of Tinfoil's other engineers are MIT alumni: Ben Sedat '09 and Angel Irizarry '09. They had co-written a paper on securing authentication cookies with Borohovski—which later became Borohovski and Sedat's senior thesis—and are now helping build the company. "Eighty percent of our company is MIT alumni," Borohovski says. "I guess we're trying to recreate our own little MIT here."

Provided by Massachusetts Institute of Technology