The Cybersecurity Readiness Podcast Series

Episode Title	Authenticate without Storing Credentials: MIT Scientist Cracks the Code
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Tina Srivastava, Ph.D., MIT Lecturer and Co-Founder of Badge Inc.
Summary Pitch	Despite companies' best efforts, stored access credentials inevitably get stolen or misused. Whether it is a disgruntled employee posting the data, an employee that makes an innocent mistake exposing that data, a company needing revenue selling the information, a criminal hacker group stealing the information, or a government-backed group stealing the information, etc. it is simply a matter of when not if that information will be stolen. "The only truly safe way to handle people's secrets is never to store them in the first place – what is not stored cannot be stolen," says Tina Srivastava, Ph.D., an MIT-trained rocket scientist and privacy expert, who has cracked the code on stored credentials She is the co-founder of Badge, a platform that allows users to enroll and authenticate on any device without storing Personally Identifiable Information (PII). In this episode, Tina and I discuss how the new technology works, its implications, and the steps organizations should take to ensure they are not storing user credentials.
Action Items and Discussion Highlights	▪ The number one cause of data breach is the theft of identity credentials."

	▪ "When the system is breached, or, in fact, handed over to an adversary, it just has public keys. And that's really a paradigm shift, there are no credentials, no private data. ▪ With the proposed solution, you can jump the identity S curve to cross domain digital identity -- because you are your key, you are your token, and that allows the user to be in control of their identity as they move across applications, across services and across providers. ▪ Evaluate the organization's current identity and access management practices, specifically whether user credentials are being stored, and consider transitioning to a credential-less authentication approach like Badge.
Time Stamps	00:02 – Introduction 03:20 – Guest's Professional Journey Highlights 04:15 – Framing the discussion 07:51 – Feasibility of authentication with storing credentials 13:19 – If personal credentials are not being stored then what do the hackers go away with after breaking into a system? 14:43 – New authentication method 16:28 -- What's the motivation for the perpetrators to break into systems, then, if they're not going to get anything valuable? If there's a mass adoption of this new authentication method, will security breach incidents greatly diminish? 17:42 -- What is it that your current methodology does not address and that still needs to be addressed in the years to come18:58 -- Is your platform open to individuals or it's exclusively for organizations?

	22:38 -- What should a CISO be doing next in terms of checking whether their current authentication system is following your approach, and if not, then what should be their next step? 25:10 -- What happens to multi-factor authentication? Do we not need it anymore? 26:02 – Final Thoughts
Memorable Tina Srivastava Quotes/Statements	"We looked into the cryptography and the math, and we found there was a 20-year open problem in cryptography in this field called fuzzy extraction – How do you extract a stable key or the same key every time? And this is really getting at this core question of identity credentials." "The number one cause of data breach is the theft of identity credentials." "When the system is breached, or, in fact, handed over to an adversary, it just has public keys. And that's really a paradigm shift, that there are no credentials, no private data." "This took a long time to get working. We spent several years in stealth mode working on the cryptography. And to give you some context, our first working implementation, it was secure, but it took 10 seconds for a single authentication. So, of course, that's not workable. It took years of hard work to get to where it is, which is just 22 milliseconds. Very much feels instant and undetectable for users." "Percentage of data breaches that are due to the theft of identity credentials is about 80%." "So with Badge, you can jump the identity S curve to cross domain digital identity, because you are your key, you are your token, and that

	allows the user to be in control of their identity as they move across applications, across services and across providers." "When we think about MFA, we often think about these push notifications to our phones paired with a password, and that is a very frustrating experience for users. We are talking about the complete elimination of that type of workflow. We're talking about a situation where you don't need to be redirected to some other phone or device in order to log in, you can just walk up to any system and derive your credentials and log in, and then when you leave, you leave no trace behind."