This World of Ours

JAMES MICKENS

James Mickens is a researcher in the Distributed Systems group at Microsoft's Redmond lab. His current research focuses on web applications, with an emphasis on the design of JavaScript frameworks that allow developers to diagnose and fix bugs in widely deployed web applications. James also works on fast, scalable storage systems for datacenters. James received his PhD in computer science from the University of Michigan, and a bachelor's degree in computer science from Georgia Tech. mickens@microsoft.com

Sometimes, when I check my work email, I'll find a message that says "Talk Announcement: Vertex-based Elliptic Cryptography on N-way Bojangle Spaces." I'll look at the abstract for the talk, and it will say something like this: "It is well-known that five-way secret sharing has been illegal since the Protestant Reformation [Luther1517]. However, using recent advances in polynomial-time Bojangle projections, we demonstrate how a set of peers who are frenemies can exchange up to five snide remarks that are robust to Bojangle-chosen plaintext attacks." I feel like these emails start in the middle of a tragic but unlikely-to-be-interesting opera. Why, exactly, have we been thrust into an elliptical world? Who, exactly, is Bojangle, and why do we care about the text that he chooses? If we care about him because he has abducted our families, can I at least exchange messages with those family members, and if so, do those messages have to be snide? Researchers who work on problems like these remind me of my friends who train for triathlons. When I encounter such a friend, I say, "In the normal universe, when are you ever going to be chased by someone into a lake, and then onto a bike, and then onto a road where you can't drive a car, but you *can* run in a wetsuit? Will that ever happen? If so, instead of training for such an event, perhaps a better activity is to discover why a madman is forcing people to swim, then bike, and then run." My friend will generally reply, "Triathlons are good exercise," and I'll say, "That's true, assuming that you've made a series of bad life decisions that result in you being hunted by an amphibious Ronald McDonald." My friend will say, "How do you know that it's Ronald McDonald who's chasing me?", and I'll say "OPEN YOUR EYES WHO ELSE COULD IT BE?", and then my friend will stop talking to me about triathlons, and I will be okay with this outcome.

In general, I think that security researchers have a problem with public relations. Security people are like smarmy teenagers who listen to goth music: they are full of morbid and detailed monologues about the pervasive catastrophes that surround us, but they are much less interested in the practical topic of what people should do before we're inevitably killed by ravens or a shortage of black mascara. It's like, websites are amazing BUT DON'T CLICK ON THAT LINK, and your phone can run all of these amazing apps BUT MANY OF YOUR APPS ARE EVIL, and if you order a Russian bride on Craigslist YOU MAY GET A CONFUSED FILIPINO MAN WHO DOES NOT LIKE BEING SHIPPED IN A BOX. It's not clear what else there is to do with computers besides click on things, run applications, and fill spiritual voids using destitute mail-ordered foreigners. If the security people are correct, then the only provably safe activity is to stare at a horseshoe whose integrity has

been verified by a quorum of Rivest, Shamir, and Adleman. Somehow, I am not excited to live in the manner of a Pilgrim who magically has access to 3-choose-2 {Rivest, Shamir, Adleman}, mainly because, if I were a bored Pilgrim who possessed a kidnapping time machine, I would kidnap Samuel L. Jackson or Robocop, not mathematical wizards from the future who would taunt me with their knowledge of prime numbers and how "Breaking Bad" ends.

The only thing that I've ever wanted for Christmas is an automated way to generate strong yet memorable passwords. Unfortunately, large swaths of the security community are fixated on avant garde horrors such as the fact that, during solar eclipses, pacemakers can be remotely controlled with a garage door opener and a Pringles can. It's definitely unfortunate that Pringles cans are the gateway to an obscure set of Sith-like powers that can be used against the 0.002% of the population that has both a pacemaker and bitter enemies in the electronics hobbyist community. However, if someone is motivated enough to kill you by focusing electromagnetic energy through a Pringles can, you probably did something to deserve that. I am not saying that I want you dead, but I am saying that you may have to die so that researchers who study per-photon HMACs for pacemaker transmitters can instead work on making it easier for people to generate good passwords. "But James," you protest, "there are many best practices for choosing passwords!" Yes, I am aware of the "use a vivid image" technique, and if I lived in a sensory deprivation tank and I had never used the Internet, I could easily remember a password phrase like "Gigantic Martian Insect Party." Unfortunately, I *have* used the Internet, and this means that I have seen, heard, and occasionally paid money for every thing that could ever be imagined. I have seen a video called "Gigantic Martian Insect Party," and I have seen another video called "Gigantic Martian Insect Party 2: Don't Tell Mom," and I hated both videos, but this did not stop me from directing the sequel "Gigantic Martian Insect Party Into Darkness." Thus, it is extremely difficult for me to generate a memorable image that can distinguish itself from the seething ocean of absurdities that I store as a result of consuming 31 hours of media in each 24-hour period.

So, coming up with a memorable image is difficult, and to make things worse, the security people tell me that I need *different* passwords for *different* web sites. Now I'm expected to remember both "Gigantic Martian Insect Party" *and* "Structurally Unsound Yeti Tote-bag," and I have to somehow recall which phrase is associated with my banking web site, and which one is associated with some other site that doesn't involve extraterrestrial insects or Yeti accoutrements. This is uncivilized and I demand more from life. Thus, when security researchers tell me that they're not working on passwords, it's like physicists from World War II telling me that they're not working on radar or nuclear bombs, but instead they're unravelling the mystery of how bumblebees fly. It's like, you are so close, and yet so far. You almost get it, but that's worse than not getting it at all.

My point is that security people need to get their priorities straight. The "threat model" section of a security paper resembles the script for a telenovela that was written by a paranoid schizophrenic: there are elaborate narratives and grand conspiracy theories, and there are heroes and villains with fantastic (yet oddly constrained) powers that necessitate a grinding battle of emotional and technical attrition. In the real world, threat models are much simpler (see Figure 1). Basically, you're either dealing with Mossad or not-Mossad. If your adversary is not-Mossad, then you'll probably be fine if you pick a good password and don't respond to emails from ChEaPestPAiNPi11s@virus-basket.biz.ru. If your adversary *is* the Mossad, YOU'RE GONNA DIE AND THERE'S NOTHING THAT YOU CAN DO ABOUT IT. The Mossad is not intimidated by the fact that you employ https://. If the Mossad wants your data, they're going to use a drone to replace your cellphone with a piece of uranium that's shaped like a cellphone, and when you die of tumors filled with tumors, they're going to hold a press conference and say "It wasn't us" as they wear t-shirts that say "IT WAS DEFINITELY US," and then they're going to buy all of your stuff at your estate sale so that they can directly look at the photos of your vacation instead of reading your insipid emails about them. In summary, https:// and two dollars will get you a bus ticket to nowhere. Also, SANTA CLAUS ISN'T REAL. When it rains, it pours.

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

This World of Ours

The Mossad/not-Mossad duality is just one of the truths that security researchers try to hide from you. The security community employs a variety of misdirections and soothing words to obscure the ultimate nature of reality; in this regard, they resemble used car salesmen and Girl Scouts (whose "cookie sales" are merely shell companies for the Yakuza). When you read a security paper, there's often a sentence near the beginning that says "assume that a public key cryptosystem exists." The authors intend for you to read this sentence in a breezy, carefree way, as if establishing a scalable key infrastructure is a weekend project, akin to organizing a walk-in closet or taming a chinchilla. Given such a public key infrastructure, the authors propose all kinds of entertaining, Ferris Bueller-like things that you can do, like taking hashes of keys, and arranging keys into fanciful tree-like structures, and determining which users are bad so that their keys can be destroyed, or revoked, or mixed with concrete and rendered inert. To better describe the Mendelian genetics of keys, the authors will define kinky, unnatural operators for the keys, operators that are described as unholy by the Book of Leviticus and the state of Alabama, and whose definitions require you to parse opaque, subscript-based sentences like "Let K_R ₩ K_T represent the semi-Kasparov foo-dongle operation in a bipartite XY_{abc} space, such that the modulus is spilt but a new key is not made."

This Caligula-style key party sounds like great fun, but constructing a public key infrastructure is incredibly difficult in practice. When someone says "assume that a public key cryptosystem exists," this is roughly equivalent to saying "assume that you could clone dinosaurs, and that you could fill a park with these dinosaurs, and that you could get a ticket to this 'Jurassic Park,' and that you could stroll throughout this park without getting eaten, clawed, or otherwise quantum entangled with a macroscopic dinosaur particle." With public key cryptography, there's a horrible, fundamental challenge of finding somebody, *anybody*, to establish and maintain the infrastructure. For example, you could enlist a well-known technology company to do it, but this would offend the refined aesthetics of the vaguely Marxist but comfortably bourgeoisie hacker community who wants everything to be decentralized and who non-ironically believes that Tor is used for things besides drug deals and kidnapping plots. Alternatively, the public key infrastructure could use a decentralized "web-of-trust" model; in this architecture, individuals make their own keys and certify the keys of trusted associates, creating chains of attestation. "Chains of Attestation" is a great name for a heavy metal band, but it is less practical in the real, non-Ozzy-Ozbourne-based world, since I don't just need a chain of attestation between me and some unknown, filthy stranger —I also need a chain of attestation *for each link in that chain*. This recursive attestation eventually leads to fractals and H.P. Lovecraft-style madness. Web-of-trust cryptosystems also result in the generation of emails with incredibly short bodies (e.g., "R U gonna be at the gym 2nite?!?!?!?") and multi-kilobyte PGP key attachments, leading to a packet framing overhead of 98.5%. PGP enthusiasts are like your friend with the ethno-literature degree whose multi-paragraph email signature has fourteen Buddhist quotes about wisdom and mankind's relationship to trees. It's like, I GET IT. You care deeply about the things that you care about. Please leave me alone so that I can ponder the inevitability of death.

Even worse than the PGP acolytes are the folks who claim that we can use online social networks to bootstrap a key infrastructure. Sadly, the people in an online social network are the same confused, ill-equipped blunderhats who inhabit the physical world. Thus, social network people are the same people who install desktop search toolbars, and who try to click on the monkey to win an iPad, and who are willing to at least entertain the notion that buying a fortune-telling app for any more money than "no money" is a good idea. These are not the best people in the history of people, yet somehow, I am supposed to stitch these clowns into a rich cryptographic tapestry that supports key revocation and verifiable audit trails. One time, I was on a plane, and a man asked me why his laptop wasn't working, and I tried to hit the power button, and I noticed that the power button was sticky, and I said, hey, why is the power button sticky, and he said, oh, IT'S BECAUSE I SPILLED AN ENTIRE SODA ONTO IT BUT THAT'S NOT A PROBLEM RIGHT? I don't think that this dude is ready to orchestrate cryptographic operations on 2048-bit integers.

Another myth spread by security researchers is that the planet Earth contains more than six programmers who can correctly use security labels and information flow control (IFC). This belief requires one to assume that, even though the most popular variable names are "thing" and "thing2," programmers will magically become disciplined software architects when confronted with a Dungeons-and-Dragons-style type system that requires variables to be annotated with rich biographical data and a list of vulnerabilities to output sinks. People feel genuine anxiety when asked if they want large fries for just 50 cents more, so I doubt that unfathomable lattice-based calculus is going to be a hit with the youths. I mean, yes, I understand how one can use labels to write a secure version of HelloWorld(), but once my program gets bigger than ten functions, my desire to think about combinatorial label flows will decrease and be replaced by an urgent desire to DECLASSIFY() so that I can go home and stop worrying about morally troubling phrases like "taint explosion" that are typically associated with the diaper industry and FEMA. I realize that, in an ideal world, I would recycle my trash, and contribute 10% of my income to charity, and willingly accept the cognitive overhead of fine-grained security labels. However, pragmatists understand that

This World of Ours

I will spend the bulk of my disposable income on comic books, and instead of recycling, I will throw all of my trash into New Jersey, where it will self-organize into elaborate "Matrix"-like simulations of the seagull world, simulations that consist solely of choking-hazard-sized particles and seagull-shaped objects that are not seagulls and that will not respond to seagull mating rituals by producing new seagull children. This is definitely a problem, but problem identification is what makes science fun, and now we know that we need to send SWAT teams into New Jersey to disarm a trash-based cellular automaton that threatens the seagull way of life. Similarly, we know that IFC research should not focus on what would happen if I somehow used seventeen types of labels to describe three types of variables. Instead, IFC research should focus on what will happen when I definitely give all my variables The God Label so that my program compiles and I can return to my loved ones. [Incidentally, I think that "The God Label" was an important plot device in the sixth "Dune" novel, but I stopped reading that series after the fifth book and my seven-hundredth time reading a speech that started "WHOEVER CONTROLS THE SPICE CONTROLS THE (SOME THING WHICH IS NOT THE SPICE)." Also note that if a police officer ever tries to give you a speeding ticket, do *not* tell him that you are the Kwisatz Haderach and You Can See Where No Bene Gesserit Can See and you cannot see a speeding ticket. This defense will not hold up in court, and the only "spice" that you will find in prison is made of mouthwash and fermented oranges.]

The worst part about growing up is that the world becomes more constrained. As a child, it seems completely reasonable to build a spaceship out of bed sheets, firecrackers, and lawn furniture; as you get older, you realize that the S.S. Improbable will not take you to space, but instead a lonely killing field of fire, Child Protective Services, and awkward local news interviews, not necessarily in that order, but with everything showing up eventually. Security research is the continual process of discovering that your spaceship is a deathtrap. However, as John F. Kennedy once said, "SCREW IT WE'RE GOING TO THE MOON." I cannot live my life in fear because someone named PhreakusMaximus at DefConHat 2014 showed that you can induce peanut allergies at a distance using an SMS message and a lock of your victim's hair. If that's how it is, I accept it and move on. Thinking about security is like thinking about where to ride your motorcycle: the safe places are no fun, and the fun places are not safe. I shall ride wherever my spirit takes me, and I shall find my Gigantic Martian Insect Party, and I will, uh, probably be rent asunder by huge cryptozoological mandibles, but I will die like Thomas Jefferson: free, defiant, and without a security label.

Why Join USENIX?

OPEN ACCESS

We support members' professional and technical development through many ongoing activities, including:

- Open access to research presented at our events
- Workshops on hot topics
- Conferences presenting the latest in research and practice
- LISA: The USENIX Special Interest Group for Sysadmins
- *;login:*, the magazine of USENIX
- Student outreach

Your membership dollars go towards programs including:

- Open access policy: All conference papers and videos are immediately free to everyone upon publication
- Student program, including grants for conference attendance
- Good Works program

Helping our many communities share, develop, and adopt ground-breaking ideas in advanced technology

Join us at www.usenix.org

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION