The Future of Cybersecurity

by Jim Routh

Cybersecurity has evolved into something every person has to confront in daily life. The explosive growth of constantly-connected devices influences our human experience in ways that were once unimaginable and confirms that cyber security is becoming a part of the value proposition for goods and services.

The cars we buy today have more engineering hours dedicated to developing software than bending sheet metal, leading to cultural challenges we expect to face with driverless automobiles.

A new market for digital personal assistants has emerged overnight (Apple Siri, Amazon Echo, Google Home) that combines voice recognition, access to online content and search algorithms designed to make our pursuit of instant information easier and woven into the fabric of our home lives.

Our homes are now secured by many forms of digital surveillance that protect against intruders, set the appropriate temperature control, ensure the doors are locked or adjust the sprinkler schedule—all remotely, using network connectivity.

Our refrigerators are becoming food inventory management systems automatically replenished and fulfilled online with goods delivered to our doorsteps. Our home procurement system is online and shared with family members using a variety of platforms, including Amazon Prime, which offers both free shipping on products and digital content, as well as the ability to recall every purchase made at any point in time.

As consumers, we are marching into a realm where the purchases we make, the content we consume, the queries we make and the friendships we forge online create ‘digital exhaust’ that is highly valued by hackers and marketers alike. Some of that digital exhaust includes our site credentials and our social security numbers.

In 2014, Yahoo leaked 500 million email IDs and passwords. LinkedIn leaked 167 million account credentials this year. Tens of millions of credentials were stolen from Gmail and Microsoft, reportedly by a Russian hacker who claims to have 1.17 billion records in total.

Today, criminal syndicates can purchase your name, date of birth and SSN for $7 and then use this information to take over your online accounts. Anyone with an email account knows well that the majority of messages are from aggressive marketers (SPAM) or criminals using phishing messages to capture sensitive information—and that's even after the SPAM filters are applied. We are being dragged into a new digital reality where the trade-off decisions of privacy vs. convenience will be a constant part of the new value system for products and services.

The technology capability across devices and platforms is well ahead of our preferred thresholds for privacy. In some cases (Galaxy 7) we are reminded of the hazards of mobile technology advancement every time we board a plane the result of the continuing struggle of mobile device manufacturers to squeeze more functionality out of cell phone batteries. The concentration of technology in our daily lives is increasing exponentially, taking over conventionally nonthreatening devices, products, and services, and forcing us to confront the challenges of information protection.

Some of us will resist the urge to participate in the digital environment while others will dive in and embrace new capabilities with little concern over our personal behavioral data. Most of us will attempt to make educated and well-informed decisions on the purchase of technology-enabled products and services, attempting to reach an appropriate balance of confidence and concern. In all cases, our privacy is and will continue to be impacted based on our consumption decisions as more and more software is written to gather behavioral data. This will make products better in many cases and security better in some cases, but expand the range of personal digital exhaust available in all cases.

Given the evolution of consumer technology, I believe there are three characteristics of cyber security of the future that are certain:

1. Software is more important than hardware
2. Patterns of behavior detected will both improve and protect the consumer experience
3. It's all about four letters: MATH

The key to providing consumers with a safe digital experience is to design and imbed security into resilient software when the software is written. As the number of devices within the Internet of Things (IOT) grows, the reliance on resilient software also grows. This means software development practices need to emphasize resiliency and security features need to be part of the end product recognizable by the consumer.

The only model for security in the IOT world that has any chance of success is a model where consumers demand device options that are more resilient and protective of their privacy and, of course, are willing to pay for it. Developing resilient software actually costs less than writing exploitable software with security defects, as long as consumers expect that the software is supposed to be resilient and accept it as part of the value proposition. Adding security features to products does add cost to the development process in most cases and, once again, the consumer has to decide to pay for the added features. The growth in IOT has more security implications for software than hardware design.

It turns out that all of us have unique patterns of behavior when using connected devices that are easily measured and attributed to us. Many of these discernable patterns use relatively benign information to determine if the user of a device at a precise moment in time is the same user of that device previously. For example, let's say that you and I both use an iPhone to interact with a social network daily. Any mobile application on our iPhone is allowed to use certain attributes of both the device and the software on the device to determine if we are who we were the last time we used the iPhone. The device has several mobile applications that are easily discernable. Your iPhone may have lots of applications related to dining, cooking, or other apps a "foodie" couldn't do without, while my iPhone may have apps to take a picture of a wine label and tell me what the rating of a specific wine is or an app to manage the inventory in my collection. So the way the iPhone is configured may change as apps are loaded to it, but the type of applications and how frequently they are used represents a pattern that can be used to authenticate that you are using you iPhone and I am using mine based on the device itself.

Combine this with data from each of our accelerometers (the gyroscope software that changes the orientation of the screen from portrait to landscape) that can recognize the unique way we walk, and it turns out the data on usage patterns is highly indicative of who we are. This capability is fostering a new generation of authentication capability that is no longer binary (user id and password) and instead is unique to our behavior. This both improves the user experience (no more passwords) while also improving the risk management capability (no more compromised passwords used by fraudsters).

That brings me to the third point: the future of cyber security is all about math. I really wish I knew this decades ago when I was an undergraduate choosing a major, because I avoided math like the plague and my passion was history. More specifically, it's all about algorithms that interpret data patterns and draw conclusions. It's one reason that Aetna has a chief security data scientist and it's also why Aetna has designed a next generation authentication capability for web and mobile applications that uses rules applied to data (often called machine learning) to authenticate users, eliminating the need for passwords.

Writing and deploying algorithms that parse large data sets and derive results that confirm behavioral patterns represents technology that has been used for years in the banking industry. It is now being applied to improve the consumer digital experience and cyber security capabilities.

This represents the future of cyber security and in many ways the future of consumer privacy as well. Today's consumers make choices on features, functions and privacy protection; tomorrow's consumers of health products and services will choose features based on convenience and information protection as part of the value proposition. Aetna is offering consumers both a better consumer experience that also offers them better protection of their information.

The future of cyber security is all about math applied to data. Ironically, math in the form of cryptology has been a part of human history for thousands of years. History has shown us that cryptanalysis (studying ways to break crypto code) always wins out eventually, making advancement in techniques for protecting information inevitable.

If you want to make sure that your kids are well equipped to flourish in the new markets they will encounter after graduation, encourage them to study math and statistics or data science. The consumers of the future will be grateful for their investment in relevant skills. If they listen to you and study data science, then make sure you tell them to considering joining Aetna where they can make the world a healthier place, using their highly-valued skills embracing the future of cyber security.

About the Author

Jim Routh is the chief security officer and leads the Global Security function for Aetna. He is the chairman of the National Health ISAC and a former board member of the FS-ISAC. Prior to joining Aetna in May 2013, Jim was global head of Application & Mobile Security for JP Morgan Chase. Additionally, he is the former CISO for KPMG, DTCC and American Express, and has over 30 years of experience in information technology and information security with global financial service firms. Jim was the Information Security Executive of the Year winner for the Northeast in 2007, and in 2014 was named the Information Security Executive of the Year in North America for Health Care, 2016 Security Alliance Innovation award winner and ISE Luminary Leadership award winner in 2016.