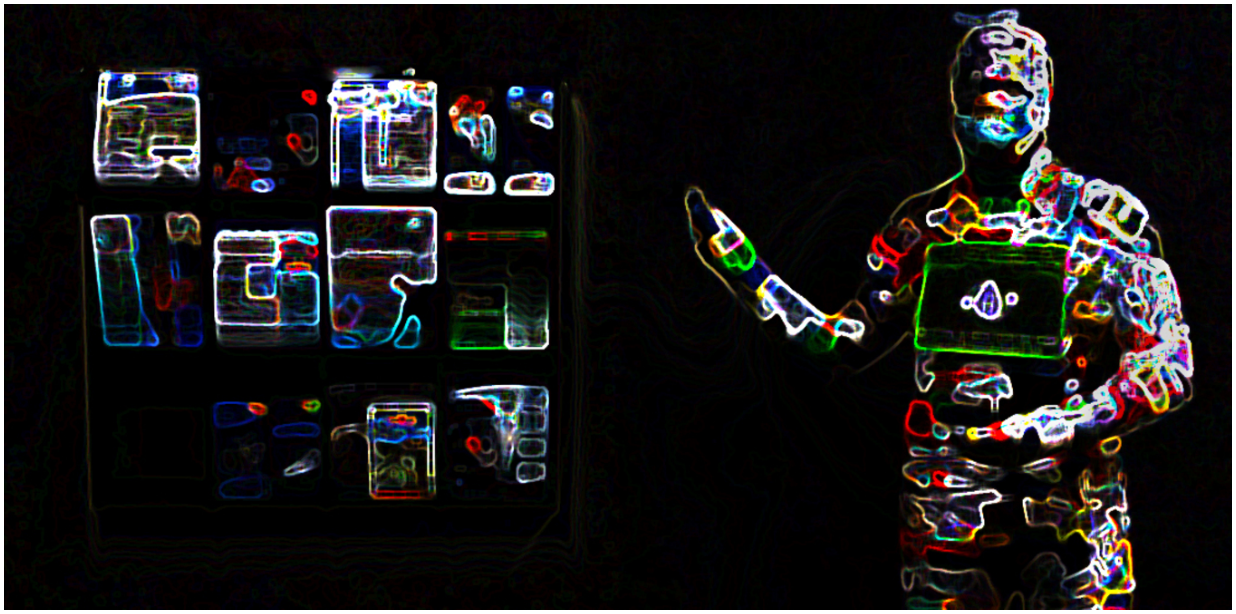
It's the year 2020...how's your cybersecurity?

April 29 2016, by Steven Weber, And Betsy Cooper, University Of California, Berkeley



If we’re super-wired in the future, will we also be super-vulnerable? Credit: keoni101/flickr, CC BY-SA

What if, in 2020, wearable devices did not care about how many steps you took, and instead were concerned with your real-time emotional state? With networked devices tracking hormone levels, heart rates, facial expressions, voice tone and more, the Internet could become a vast system of "emotion readers," touching the most intimate aspects of human psychology. What if these technologies allowed people's underlying mental, emotional and physical states to be tracked – and manipulated?

Whether for blackmail, "revenge porn" or other motives, cybercriminals and hostile governments in this world would find new ways to exploit data about emotion. The terms of cybersecurity would be redefined, as it became more important for people to manage and protect how their emotions and mindsets appeared to the monitors.

This is just one of several potential future cybersecurity scenarios dreamed up by a group of multidisciplinary experts recently. Here at the Center for Long-Term Cybersecurity, we asked them to think about what we could see happening in the near future of 2020. These are not predictions – it's impossible to make precise forecasts about such a complex set of issues. Rather, the scenarios paint a landscape of future possibilities, exploring how emerging and unknown forces could intersect to reshape the relationship between humans and technology – and what it means to be "secure."

And they raise pressing questions we should consider today as we lay the groundwork for a secure information technology environment in the future: how might individuals function in a world when they are no longer able to ignore the fact that literally everything they do online will likely be hacked or stolen? How could the proliferation of networked appliances, vehicles and devices transform what it means to have a "secure" society? What would be the consequences of almost unimaginably powerful algorithms predicting individual human behavior at the most granular scale?

Imagining scenarios

At the heart of our approach is scenario thinking, a proven methodology for identifying important driving forces and unexpected consequences that could shape the future. This approach often leads to more questions than answers, but what we identify can help guide us toward solutions as society and technology evolve.

In our scenario about emotion-sensing, for example, many questions arise:

- How might biosensing technologies evolve, and what would be the effect of having sensors tracking massive numbers of individuals' emotions and mental states?
- How will people respond when their most private and intimate experiences are understood by the Internet better than they themselves understand them?
- How might virtual reality, sentiment analysis, wearable devices and other "sensory" technologies intersect with domains such as marketing, politics and the workforce?
- What are the potential cybersecurity risks and benefits that could come with the proliferation of sensors capable of capturing and interpreting emotions?

Our broad interdisciplinary group of experts on computer science, political science, neuroscience and other areas came from universities, the private sector, nonprofits and governments. They helped us develop that scenario, and four others, for the year 2020.

Cybersecurity in hard economic times

For example, imagine that two decades after the first dot-com bust, the advertising-driven business model for major Internet companies has fallen apart. As overvalued web companies large and small collapse, criminals and companies alike race to gain ownership of underpriced but potentially valuable data assets. It's a "war for data" under some of the worst possible circumstances: financial stress and sometimes panic, ambiguous property rights, opaque markets and data trolls everywhere.

In this world, cybersecurity and data security become inextricably intertwined. There are two key assets that criminals exploit: the datasets themselves, which become the principal targets of attack; and the humans who work on them, as the collapse of the industry leaves unemployed data scientists seeking new jobs. The questions that arise are difficult:

How might cybercriminals adapt to a more open and raucous data market?If governments want to prevent certain datasets from having a "for-sale" sign attached to them, what kinds of options will they have?What new systems or standards could emerge to verify the legitimacy or provenance of data? What does "buyer beware" look like in a fast-moving market for data?What role should government play in making markets for data more efficient and secure?

What comes next?

This is just the beginning. In one of our other scenarios, we imagine that hackers have become so successful that the public's default expectation about Internet transactions flips from "we are basically safe" to "we are going to have our data stolen." Another looks at the potential of predictive algorithms: if those improve to be able to predict individual behavior, all sorts of new attacks might occur. Still another looks at the Internet of Things, suggesting that governments may lead the way in IoT adoption – and could become both more effective and more vulnerable as a result.

The world in 2020 could look very different from today. Our scenarios are designed to serve as a starting point for conversation and debate among academic researchers, industry practitioners, and government policymakers. We invite the public to join us as well; please read the full-text scenarios and engage with them on Twitter (@cltcberkeley). We look forward to building a better cybersecurity future with you.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation

Citation: It's the year 2020...how's your cybersecurity? (2016, April 29) retrieved 26 April 2024 from https://phys.org/news/2016-04-year-2020how-cybersecurity.html