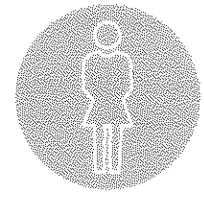
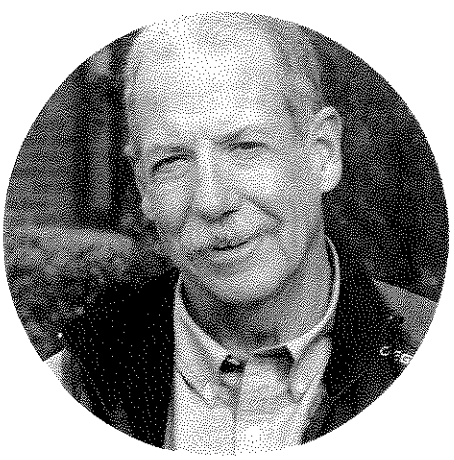
THE INTERNET OF THINGS



COMPUTERS CAN CONTROL EVERYTHING FROM THE THERMOSTAT TO THE FAMILY CAR—FOR BETTER OR WORSE

BY MATT COOPER



IMAGINE: IT'S A WINTER snowstorm and you're driving in the mountains, late at night. You approach a narrow bridge—is it safe to use? Is there ice on it? You can barely make out the other side—could something be coming the other way?

Fortunately, this is no ordinary bridge. It's a smart bridge. Sensors in the cement monitor cracks and stresses; they can send data to engineers via the wireless Internet. These sensors can detect ice on the bridge and communicate with your car, which has sensors of its own—if there's a hazard ahead, on the ground or in your path, you'll be instructed to slow down. Someday soon, maybe the car will even slow down for you.

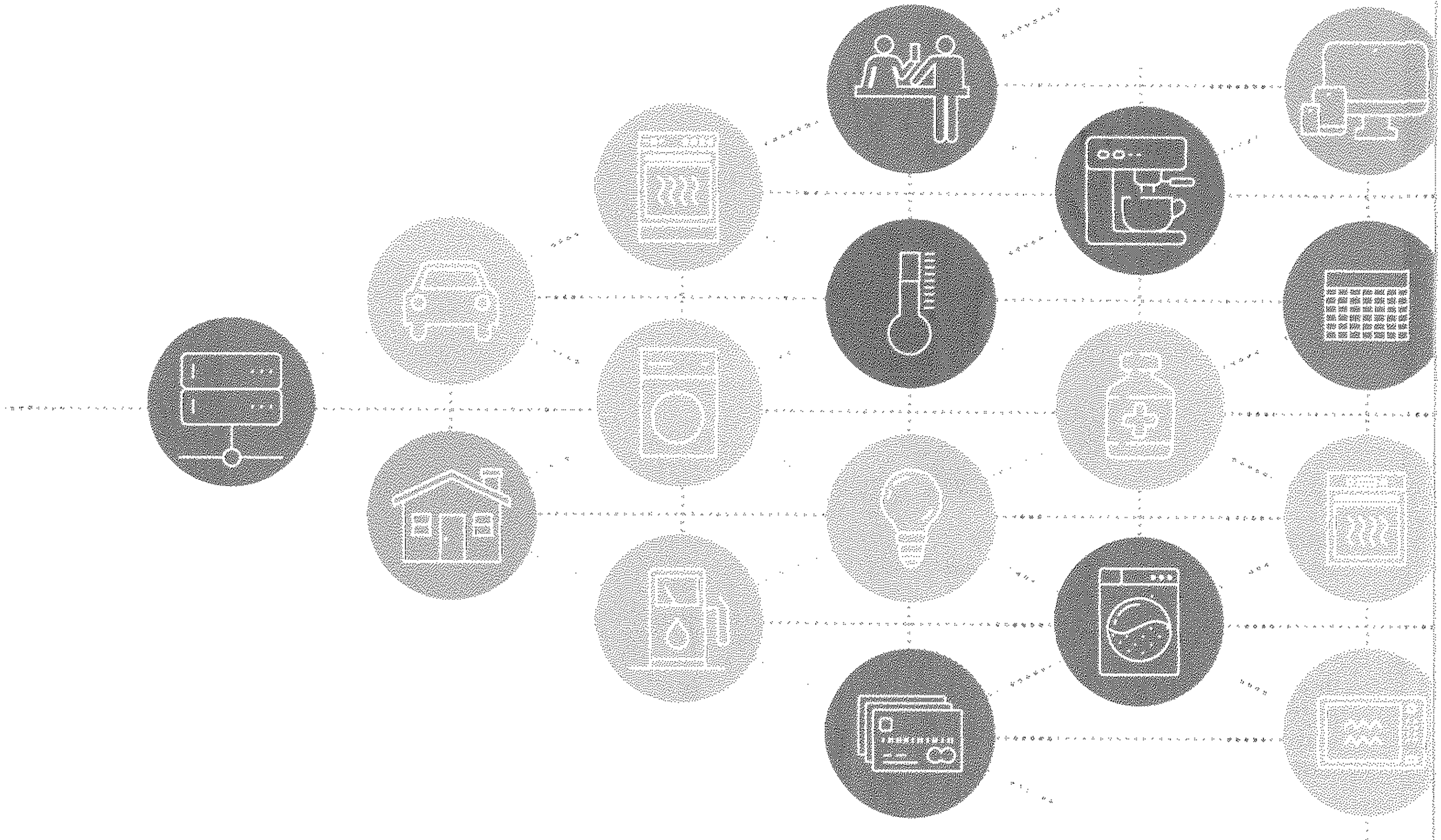
This Internet-age scenario comes from futurist and author Daniel Burrus, and there are scores of others: using an app to preheat the oven while you're still in rush-hour traffic, or stopping to grab a gallon of milk because your refrigerator texted your cell phone that you're out. Such conveniences are sure to lower your stress levels—those improved physiological readings will be sent automatically to your doctor via the heart-monitoring strip you wear on your chest.

There is a name for the next tidal wave of technology: Internet of Things, or IoT. Place the emphasis on "things"—Internet of *things*—because that's the key piece: everything from your car to your thermostat to your dog and, yes, even you, could one day be wirelessly connected to the Internet to transmit and receive information and, theoretically anyway, improve quality of life.

"This is not something that's brand new," said Stephen Fickas (left), a professor in computer and information science at the UO. "It's just that enough people are getting their head around it to call it something. 'The Internet of Things' refers to the proliferation of computers into every nook and cranny of daily life."

Some predict 2016 will see an explosion in IoT applications and related jobs such as data-communications analysts and network-system experts. Hype around IoT might even understate its potential, which could bring an economic impact of $11.1 trillion annually by 2025, the McKinsey Global Institute reported.

Fickas isn't waiting to see if the predictions come true. Known for an innovative approach to education, he has



launched a course that gives students—inside and outside computer science—basic skills in programming, networks, and data analysis. The CIS department has seen the future: they believe it's one in which UO graduates must be able to speak "IoT"—regardless of whether they plan to be a software specialist or a Shakespeare scholar.

POCKET-SIZED BUT POWERFUL

On a recent morning in the Colloquium Room, an expansive setting in Deschutes Hall with blue couches and wall-length windows, freshman Sierra Battan clapped her hands for all she was worth: "CLAP! CLAP-CLAP-CLAP! CLAP-CLAP!"

On the desk before her, a dime-shaped sound sensor connected to a palm-sized computer recorded each instance and reported it, via the Internet, to the laptop computer of classmate Carson Hauth, sitting next to Battan. On Hauth's screen, each "clap" showed up as a data point like this:

192.168.0.100 [18/Nov/2015 18:14:04] "POST / HTTP/1.1" 200-

Battan had learned to write code that instructed the tiny computer to assign a value to each clap based on its volume. Hauth, meanwhile, had written code directing the same computer to send a message—"Got Em"—and trigger a buzzer once Battan and classmate Jordan Blackburn had reported a specified amount of data.

The coding language is called Python. It's named for the British comedy group, Monty Python, and it's one of the hottest languages in the industry because it is both powerful and easy to learn. Fickas likes Python because it's "scalable"—blocks of coding can be easily grafted onto existing instructions to dramatically boost the computer's capability.

The computers themselves are also advanced: the class uses a half-dozen UK-made Raspberry Pis, which retail for about $35 each and can fit into your pocket, yet have enough oomph to provide an entire high school with a wireless Internet connection.

COME TOGETHER

This combination of cheap, powerful computers and an easy-to-grasp coding language enables Fickas to put undergraduates in computer science classes in an unfamiliar but invaluable setting: working together to solve problems.

"The way computer science is taught in schools, it's stand-alone," Fickas said. "You're on your laptop, I'm on my desktop, and we're building webpages and websites and so forth.

"The world is moving away from that," he continued. "The world is heading to 'distributed systems'—distributing the work among many computers. That's IoT. We need a sea change in the way we teach the introduction to computer science to capture this whole trend. This course is a pilot, in some ways."

As Fickas teaches it, the Internet of Things includes three elements: sensors in the field, capable of collecting raw data on everything from river temperatures to the location of a wayward herd of cows; a series of small computers that collect and transmit this data; and a powerful, central bank of computers—sometimes referred to as "cloud computing"—to analyze reams of information, produce answers, and even trigger actions.

Fickas' course, which he developed and taught for the first time a year ago, is a practical exploration of this increasingly computer-connected, computer-dependent world—both how it operates and what it means for society.

Working in groups, students program

Hauth (left) and Battan learned to write code that enabled a tiny computer to read and process loud noises and bright lights.

the small computers and link them together through a network of wireless and wired connections. They write code that enables the computer and its sensors to capture the activity around it—the sound of someone clapping or a bright light shone from a cell phone—and convert it into data that can be analyzed. Then, the students use the computers to analyze the data; with more coding, they instruct the computers to cull through thousands of data points to produce averages, means, and standard deviations.

By the end of the term, students are dreaming up theoretical applications for "smart cities"—think: how to program traffic signals to get commuters through rush-hour traffic—and fending off cyberattacks launched by Fickas himself.

NO COMPUTER SKILLS NEEDED

Fickas, who was honored last year as a UO Williams Fellow for his commitment to creating academically engaging classes, teaches the course in a "flipped" style, wherein students receive lectures at home via videos or electronic documents and class time is reserved for working on problems. The approach gets rave reviews: "I love this course to my core," one student wrote. "This is the way all college courses should be taught."

But the real innovation is that Fickas has modeled the class on the interconnected world that will await his charges once they graduate. With students such as Hauth acting as managers and others such as Battan and Blackburn assuming the roles of data reporters, the class approximates the IoT relationship between a central computer and the numerous smaller computers in the field that must work together to send, receive, and analyze data.

None of the three students began the course with a shred of programming experience—making them precisely those Fickas hoped to draw.

Hauth, an international studies major, isn't sure what his career will be. But regardless, he's assuming that computer skills will be "a large advantage to finding a job."

"There are so many things you can code your Raspberry Pi to do," Hauth said. "I'm just starting to get a sense of that. When I chose this class, I was just thinking, 'that sounds like something cool.' Now, I could definitely be into the actual coding of things. It's very fun to be able to solve problem coding or even make programs that do something."

Asked what kind of computer skills she had before the IoT course, Battan smiled and shook her head.

"I knew how to go to a website, (or do) word processing," she said. "Now I know how to write code, how to fix it, what integers and (programming) strings are. I know how to connect to a different computer and how to have computers communicate with each other. I know how to collect and analyze data."

Like her father, who works in information technology, Battan has always been good at math. But she never really

Fickas (below, with Hauth) launched cyberattacks that his students repelled by using secret words embedded in their computer messages.

NONE OF THE THREE STUDENTS BEGAN THE COURSE WITH A SHRED OF PROGRAMMING EXPERIENCE—PRECISELY THOSE FICKAS HOPED TO DRAW.

possible applications for IoT. In fact, he requires it: the final project of the term is to devise ways that an elaborate system of sensors and small computers could improve the quality of life in Eugene.

It was easy for Sophia Gossard, a freshman majoring in architecture, to dream up some ideas—as a daily biker, she's encountered numerous situations that could be improved with the emerging technology.

Bike theft, for example: Gossard proposed putting sensors in bike locks that could send a text to the owner if the lock is being jimmied or broken. Cars could be equipped with sensors that indicate when a biker in the blind spot is close to the car; in the event of a collision, the bikes themselves could carry impact sensors that send an emergency text to the police and paramedics, complete with the bike's location.

"Before this class, I had no idea what 'the Internet of Things' meant," Gossard said. "There are so many ways that you can use this technology to gather information and then distribute it."

WHEN TEACHERS ATTACK

On a Wednesday morning near the end of the 10-week term last fall, Fickas introduced Battan and the rest of the class to the flip side of the Internet of Things—namely, its vulnerability to attack.

Working from his laptop, Fickas was able to eavesdrop on data messages that the student teams were sending one another. Then, he injected faulty information and commands into the communication, corrupting how the students' computers performed their tasks.

"Aaaaaah," Battan muttered—"no, no, no . . ." Her network had been invaded, and now the sensors connected to her computer were producing line after line of fraudulent data.

"Your goal is to stop me from doing this," Fickas said, chuckling—"other than throwing my laptop out the window."

The students were instructed to come up with a secret word and include it in the coding used to make their computers perform tasks and talk to each other. Then, by directing their computers to recognize only messages and commands carrying that word, they were able to repel Fickas' attacks.

Battan was a quick study: within minutes, she had set up an effective defense and could watch with amusement as Fickas—posing as her partner, Carson Hauth—tried and failed to hijack her computer. "He's trying to hack me, but my computer is not running," she said, smiling. "It's waiting for the real Carson, not the fake Carson."

Fickas calls these man-in-the-middle attacks. It was clear from the laughs erupting every time a team repelled his advances that this lesson in online security was a big hit.

But where IoT is concerned, the real lesson is that there's no such thing as a perfect defense.

"It's a cat-and-mouse game," Fickas said. "You can stop a certain type of attack, but another one always springs up."