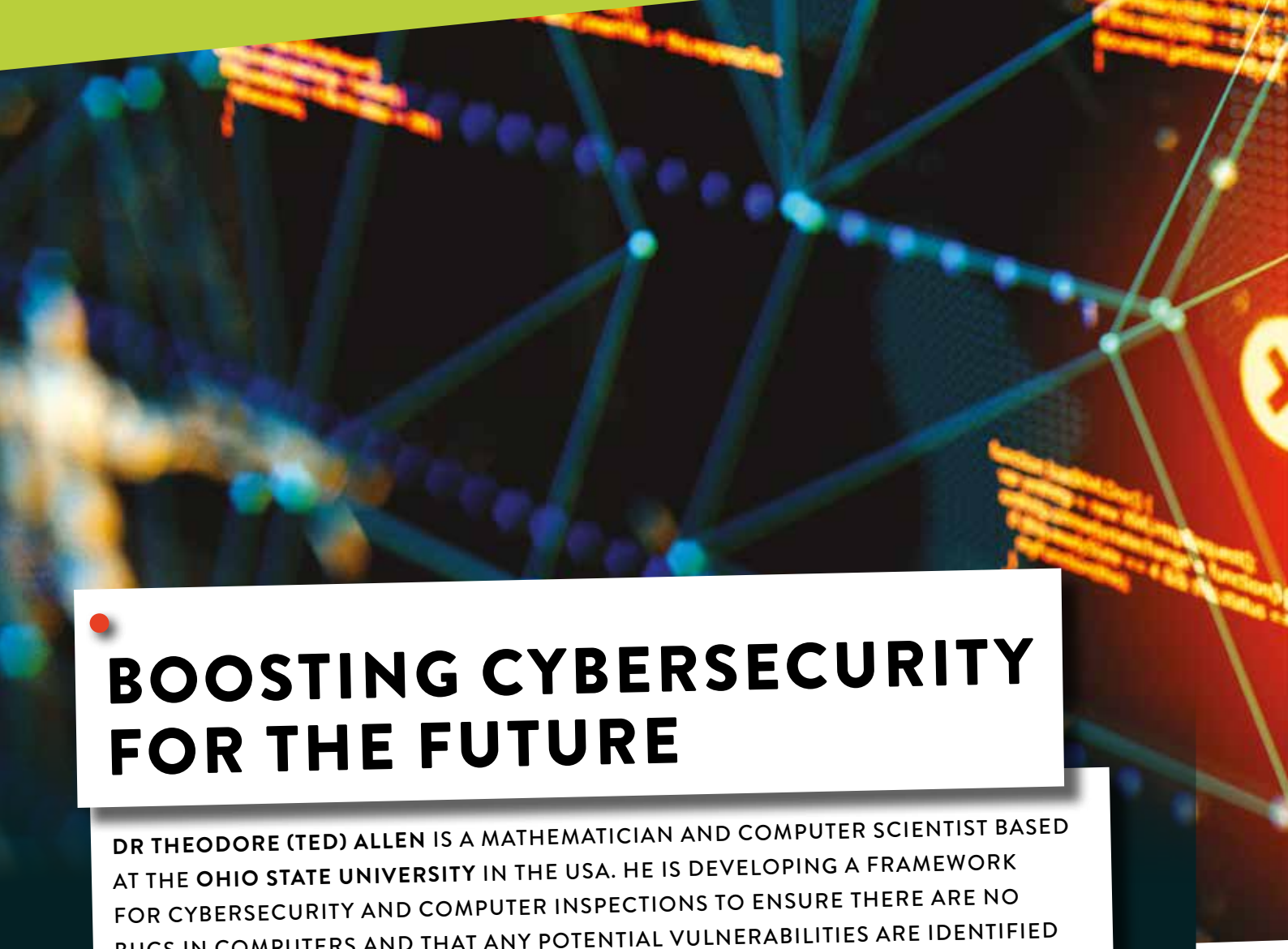
BOOSTING CYBERSECURITY FOR THE FUTURE

DR TED ALLEN



BOOSTING CYBERSECURITY FOR THE FUTURE

DR THEODORE (TED) ALLEN IS A MATHEMATICIAN AND COMPUTER SCIENTIST BASED AT THE **OHIO STATE UNIVERSITY** IN THE USA. HE IS DEVELOPING A FRAMEWORK FOR CYBERSECURITY AND COMPUTER INSPECTIONS TO ENSURE THERE ARE NO BUGS IN COMPUTERS AND THAT ANY POTENTIAL VULNERABILITIES ARE IDENTIFIED

TALK LIKE A COMPUTER SCIENTIST

BUG – an error on a computer

CURVE FITTING – using a mathematical function to construct a curve that fits a series of data points

CYBER-ATTACK – an attempt to damage a computer system or network

CYBERSECURITY – the protection of computer systems

HACK – to gain access to a computer system without permission (as part of a cyber-attack)

OPEN-SOURCE – information that is freely available for anyone to access and use

SEMI-AUTOMATIC PRIORITISATION SYSTEM – a computer system that can prioritise potential vulnerabilities with minimal human input

INTERNET OF THINGS – the billions of physical devices around the world that are connected to the internet

VULNERABILITY – a weakness on a computing system that has the potential to cause a problem. Some may only cause minor inconvenience, while a super-critical vulnerability may cause serious damage

With ongoing developments in computers, software and technology, as well as the rise of the Internet of Things, it is hardly surprising that cybersecurity is becoming increasingly important. Indeed, there are people around the world who work tirelessly to infiltrate computer systems in order to steal information.

Dr Theodore (Ted) Allen is a mathematician and computer scientist based in the Integrated Systems Engineering Department and the Industrial & Systems Engineering Program at The Ohio State University. Fortunately, researchers like Ted, are working to protect our computers from cyber-attacks by developing frameworks for cybersecurity and computer inspections. Such frameworks ensure there are no bugs in computers and that any potential vulnerabilities can be identified and addressed before the security of any given system is compromised.

QUALITY ASSURANCE AND INSPECTION

Computers and computing services must conform to what people expect and need. To ensure this is the case, computers constantly conduct auto-inspections, which are always running in the background of any computer system. These inspections will look for parts of software that are not conforming to the expected standards and alert the user to them.

However, assuring quality at the same time as conforming to expectations is extremely expensive. Inspecting every attribute on a computing system would be impossible. Instead, mathematical approaches have been developed so that only a few attributes need to be inspected and educated guesses can be made about the rest.

DR THEODORE ALLEN

Associate Professor of Integrated Systems Engineering and Computer Science and Engineering, The Ohio State University, USA

FIELDS OF RESEARCH

Integrated Systems Engineering, Artificial Intelligence

RESEARCH PROJECT

Developing a framework for cybersecurity and computer inspections to ensure there are no bugs in computers and that any potential vulnerabilities are identified

FUNDER

National Science Foundation (NSF)

SMART INSPECTION METHODS

Ted's work is primarily concerned with developing smart inspection methods that achieve desired outcomes without costing too much or being too time-consuming. These methods can then be adapted to cybersecurity. As it is too expensive to inspect whether 100% of items on a computer conform to expected standards, and it is too risky to inspect 0%, as vulnerabilities will not be detected, Ted uses a smart inspection strategy called 'single acceptance sampling'. He only inspects a small proportion of the total attributes on a computer, rather than testing them all. If only a small number (below a set threshold) of inspected attributes fail the tests, it is assumed that all attributes on the computer are acceptable. However, if too many of the tested items do not conform to standard, then the computer does not pass the inspection, and every attribute must be individually tested.

"To test the usefulness of our methods, we try to get organisations to use our approaches and then estimate practical benefits like cost savings and intrusions avoided," explains Ted. "We can also simulate the processes to see if they will work in realistic virtual worlds."

PROBABILISTIC MODELLING

The number of devices connected to the internet is expected to double within the next four years and will soon reach 10 billion. "Each of these 10 billion devices could have up to 1,000 vulnerabilities," explains Ted. The devices can be in various states of compromise and if each vulnerability requires a unique test, regularly inspecting all these devices for vulnerabilities, even approximately, is an immense challenge. Worse, a device may have a vulnerability that no one knows how to detect. "An innovative idea in simulation that we are experimenting with is using curve fitting, or 'modelling', to predict which vulnerabilities are on devices based on cleverly picked samples using a variety of inspection methods," says Ted. "We call this 'multiple-fidelity' acceptance sampling because each type of inspection has a different level of trustworthiness, or fidelity."

One great property of the cybersecurity domain is the immense amount of data available, such as session log data and user authentication data. "When you look at the data, it often feels immense and random. Yet, when you fit curves and use statistical techniques, you can begin to see what is going on," explains Ted, highlighting how mathematical skills are essential in the field of computing.

PROTECTING COMPUTERS WHILE SAVING MONEY

One of the key focuses of Ted's work is developing a semi-automatic prioritisation system to deal with cyber threats. Some of these involve sophisticated learning models, such as reinforcement learning, in which computer programs adaptively improve by inspecting and fixing bugs in certain situations. These modelling efforts can sometimes provide helpful insights, including how to save money and even lives. "Five years ago, our models indicated that it was possible to save a lot of money in cybersecurity. This has now happened in many places," says Ted. "People implemented restrictions on who can install software, which we predicted would help. These restrictions did indeed help save money."

Ted and the team have also developed software that 'scrapes' data from many open-source databases, including Twitter. Open-Source Intelligence (OSINT) involves collecting and analysing open-source data. This is a valuable method of generating information about computer vulnerabilities, allowing Ted to learn from data available on the internet. "Our automatic OSINT creates models to predict which vulnerabilities are super-critical and will be attacked by hackers. Combining this information with local inspection data, we can create alerts that certain devices desperately need to be turned on, scanned and patched, or hidden from the internet," explains Ted.

WHAT NEXT?

So far, Ted and his team have discovered the importance of super-critical vulnerabilities and have developed a special modelling system to detect them. "We are trying to combine this system with economic modelling methods to save money at our university," says Ted. "There are clearly some worries about taking risks and so getting management onboard is a challenge. Yet, we are getting better and better and our case for enacting these changes is getting stronger." Hopefully, the cybersecurity systems that Ted is designing will help to save money while also protecting computers from cyber threats.

ABOUT CYBERSECURITY

Cybersecurity has become something of a buzzword in recent times. The unfortunate truth is that many of us do not pay much attention to cybersecurity until it is too late and our devices or accounts have been hacked. While losing access to our social media accounts can be extremely upsetting, for some organisations, being hacked can lead to the loss of extremely valuable intellectual property or can result in private data being exposed.

HOW CAN WE PROTECT OUR COMPUTERS?

There are many important steps to consider, but the good news is that most of them are simple and straightforward. Ted recommends the following:

- Use strong passwords that are long and very hard to guess
- Use two-factor authentication (which is a password plus a call or message to your phone to confirm it is you logging on)
- Avoid downloading files or clicking on links from disreputable or unknown sources
- Where possible, avoid email attachments and use drop boxes like Google Drive
- Do not give personal information to those requesting it on the internet unless you initiate the process and, even then, be careful
- Consider using antivirus and endpoint security

WHAT DOES TED ENJOY MOST ABOUT HIS JOB?

Mathematics can help almost any type of person in almost any type of job and given that Ted is massively interested in maths, his job is perfect for him in many ways! "On one day, I might help a manufacturer make more products with lower cost, then help a pipeline inspection company avoid oil spills, then help election officials reduce voting queues, and then support improved battlespace communications using drone swarms," explains Ted. "Mathematics can be overwhelming, yes, but it is also beautiful. You can see patterns in our world and feel a type of deep connection with people and things."

WHAT SKILLS ARE NEEDED BY THOSE WORKING IN CYBERSECURITY?

Ted works in cybersecurity analytics, but this is just one of many areas of study in the field. "The truth is that some of the biggest contributors in cybersecurity study management, others study political science, and some are even psychologists," says Ted. "Of course, hardcore computer science, operations research and artificial intelligence are critical. Yet, policy and procedures and leadership are arguably even more critical." Ultimately, Ted says that those interested in pursuing a career in the field really just need a thirst for learning and compassion – inspiration and wisdom can come from anywhere!

EXPLORE A CAREER IN CYBERSECURITY

- Ted recommends building computing skills by taking courses through providers such as Coursera (**www.coursera.org**) or the Ohio Cyber Range (**www.ohiocyberrangeinstitute.org**).
- Explore organisations such as the International Information Systems Security Association (**www.issa.org**) or the Chartered Institute of Information Security (**www.ciisec.org**) to learn what those working in cybersecurity are doing.
- Prospects provides a job profile for a cybersecurity analyst: **www.prospects.ac.uk/job-profiles/cyber-security-analyst**
- According to **www.talent.com**, the starting salary for those working in cybersecurity is $87,500, which will increase with experience.

TED'S TOP TIPS

01 My accomplishments have been modest considering how lucky I have been with my parents, education and citizenship. Yet, what accomplishments that I have come mainly from trying hard. I highly recommend everyone puts effort in. You really do get out what you put in.

02 Curiosity has long been my strength and I am happiest and at my best when I am learning or explaining things that I understand well. If people are curious and interested in finding answers, a large part of the work is already done.

03 Learning mathematics takes time to understand for everyone, but related subjects will also help you learn. For example, if you study physics, you will learn differential equations and probability theory for free!

PATHWAY FROM SCHOOL TO CYBERSECURITY

- At school, study computing or information technology to learn computing and coding skills. It will also be very useful to study maths.
- Many universities offer degrees in computer science or informatics, where you will be able to take modules in cybersecurity. A degree in maths will also enable you to enter the field of cybersecurity.
- If you are interested in pursuing a career in cybersecurity, Ted highlights that you can get certification in cybersecurity, regardless of your degree subject. "Cybersecurity relates to digital pollution," says Ted. "Like regular pollution, we all have a stake and can all contribute."

HOW DID TED BECOME A COMPUTER SCIENTIST?

WHAT WERE YOUR INTERESTS WHEN YOU WERE YOUNGER? HAVE YOU ALWAYS BEEN INTERESTED IN COMPUTERS?

No! When I was in high school, computers were only just entering schools. I first thought they were for non-athletes or 'computer jocks'. I thought I was an athlete and I was too unwise to see how important computers would become. Oops!

WHO OR WHAT INSPIRED YOU TO BECOME A COMPUTER SCIENTIST?

I draw immense inspiration from the great Sir Ronald Fisher, who invented a lot of what we now call 'statistical science'. His contributions helped the world increase food production six-fold. By varying many aspects of production at one time, and with careful curve fitting, nature reveals itself efficiently. In my mind, Fisher was more important than any US president (except, possibly, Washington and Lincoln). We owe a lot of our prosperity to the techniques in mathematics that he invented.

WHERE ELSE HAVE YOU APPLIED MATHEMATICS TO SOLVE REAL-WORLD PROBLEMS?

Through my own experiences working with companies, I have seen many magical benefits from applying mathematics and computer science. For example, I am part of a team that is saving the delivery company DHL $160M by improving the routing of their delivery vehicles. We are saving thousands of kilotons of CO_2 every year by reducing driving. A lot of the time, applications of mathematics and computer science are about overcoming our own biases and seeing clearly with the help of computers and models. If we do not see a need to use computers, that is often our own blindness.

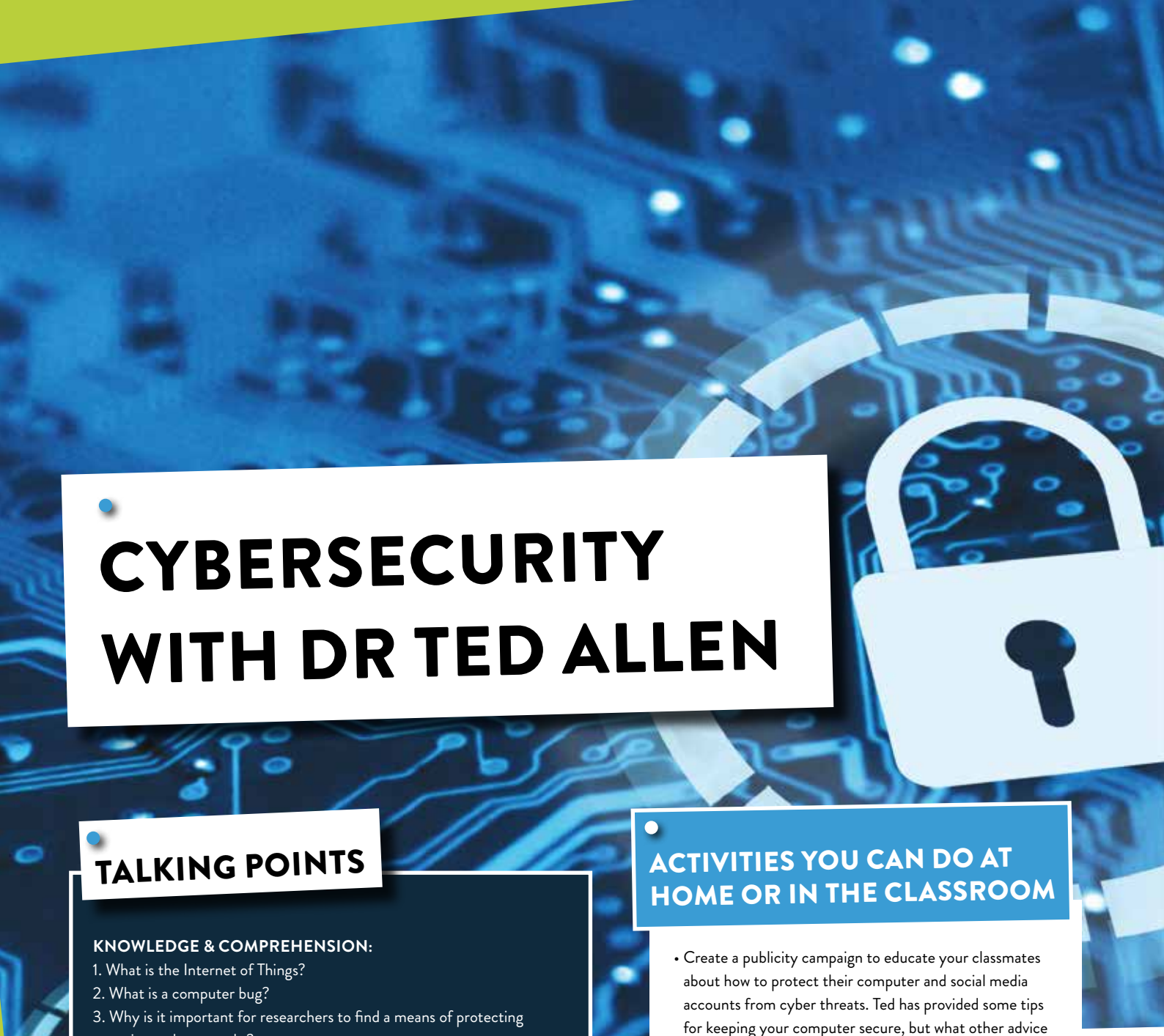
AS WELL AS CYBERSECURITY, WHAT ARE YOUR OTHER RESEARCH INTERESTS?

Like many operations researchers and computer scientists, I am interested in designing methods to help people design things. This level of indirection seems weird. Yet, it is true that the process of making decisions is surprisingly important. With this in mind, we are developing innovative approaches to predict the future (Optimal Classification Trees), to schedule jobs in manufacturing (genetic algorithms with active evaluation), to monitor robots and manufacturing cells (special control charts), design the routes for trucks (red-black ant colony searchers), and to allocate resources such as voting machines (generalised 'indifference zone' binary searches). Mathematicians seek out the most important problems and we try to help solve them.

WHAT DO YOU ENJOY DOING IN YOUR FREE TIME?

I love spending time with my family, including playing games. I like cycling and listening to podcasts and audiobooks. I am huge fan of Ezra Klein and Fareed Zacharia. Also, I play Magic the Gathering online and sometimes in person. It is expensive and addictive, but I like it!

Ted cycling with his family



CYBERSECURITY WITH DR TED ALLEN

TALKING POINTS

KNOWLEDGE & COMPREHENSION:

1. What is the Internet of Things?
2. What is a computer bug?
3. Why is it important for researchers to find a means of protecting against cyber-attacks?
4. What are some of the limitations with current cybersecurity methods?
5. Why is it unfeasible to test every part of a computer when looking for bugs?

APPLICATION:

6. How might some of Ted's systems help deal with cyber threats?
7. How does Ted apply skills and techniques from mathematics to deal with issues in computer science?
8. What problems would occur if an individual or organisation had their computer system hacked?

EVALUATION:

9. Ted talks a little about how some of the skills required for a career in cybersecurity exist well beyond the realm of mathematics – how do your skills, knowledge and interests fit within some of his suggestions? Why do you think it is important that the field of cybersecurity includes people with many different areas of interest and expertise?

ACTIVITIES YOU CAN DO AT HOME OR IN THE CLASSROOM

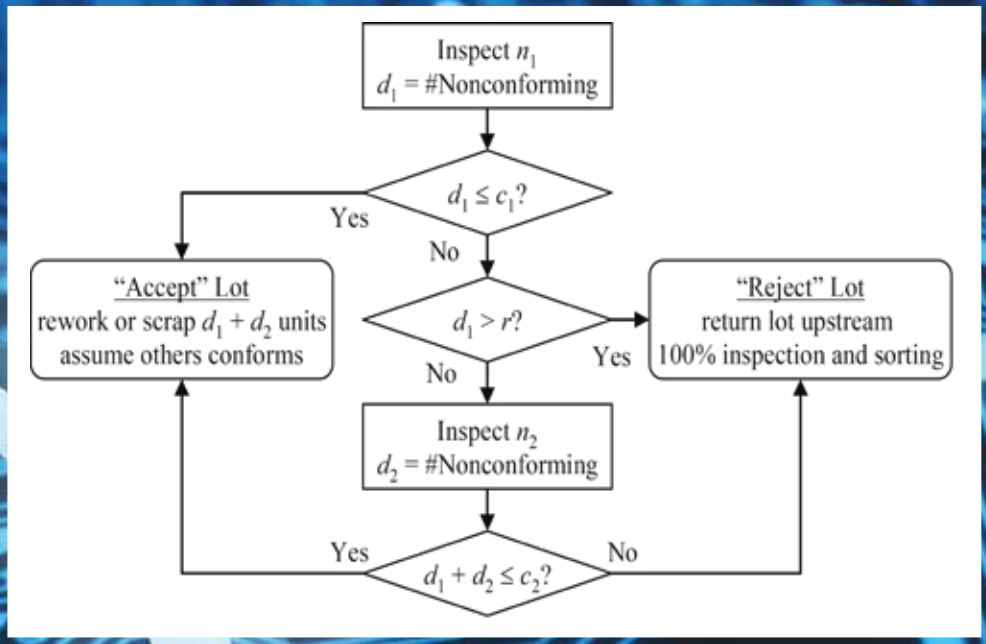
- Create a publicity campaign to educate your classmates about how to protect their computer and social media accounts from cyber threats. Ted has provided some tips for keeping your computer secure, but what other advice would you give people? How will you communicate this information to your audience?

- Cyber-attacks come in many shapes and forms. Research the different types of cyber threats that individuals or organisations may face, create a list of them, and provide a definition of each type of attack.

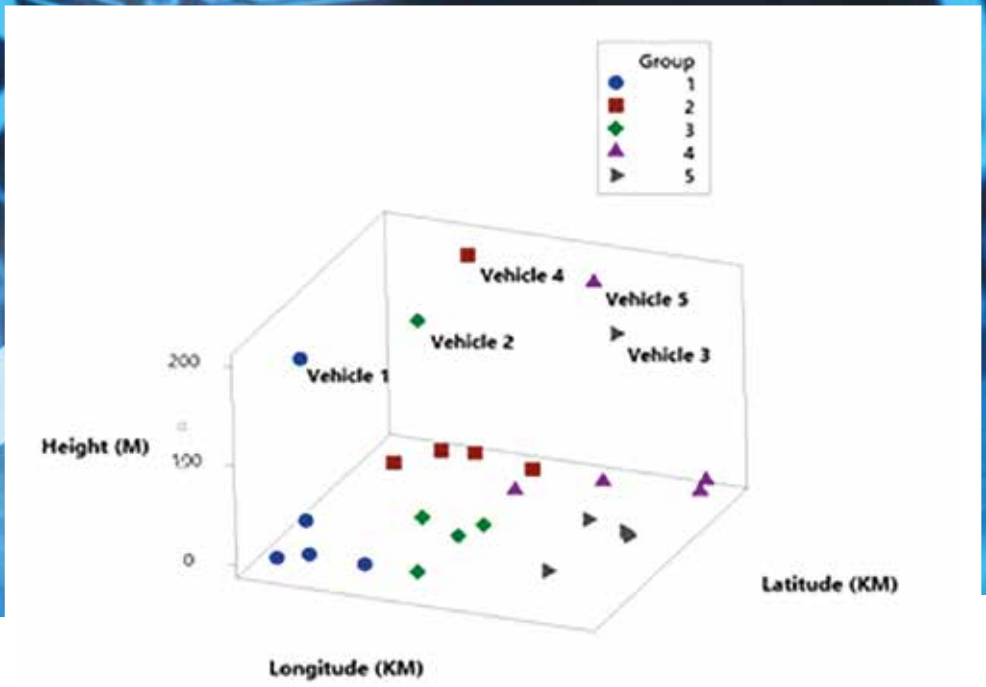
MORE RESOURCES

- Visit Ted's website to learn about the range of computing activities his research team conducts: **www.blying.com/index.html**

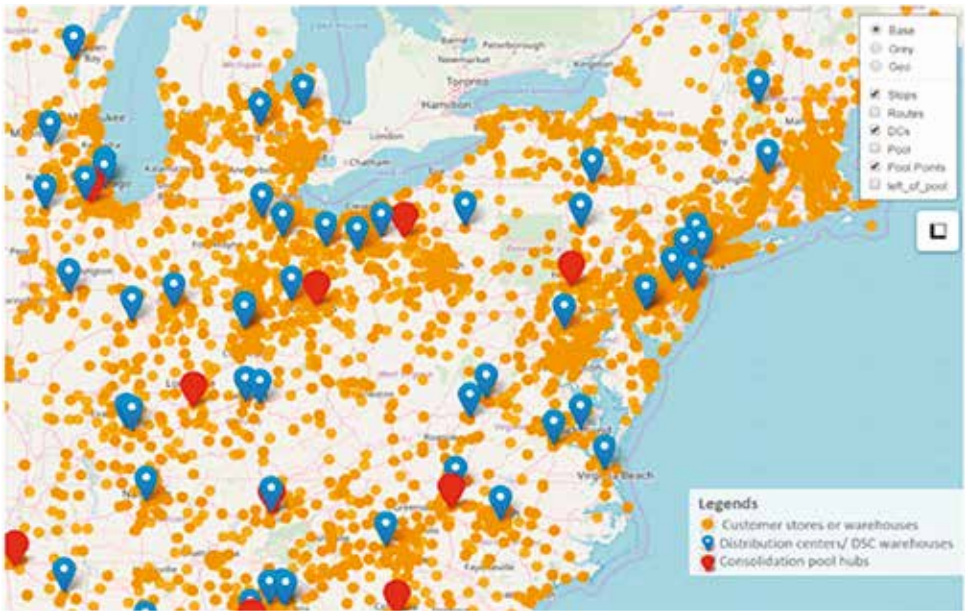
- Here are some games that you can play which will put your cyber defence knowledge to the test! **www.helpsystems.com/blog/break-time-6-cybersecurity-games-youll-love**



Ted's smart inspection method allows him to evaluate the quality of a large number of items on a computer without testing too many. By testing just a few items, he can assess whether the computer passes the inspection. If too many items fail, he must then inspect every item individually.



Ted has been modelling how drones flying in the air (labelled as vehicles in the graph) can provide mobile phone service to customers on the ground. Such a situation might be relevant after a natural disaster or in a battlefield.



This map shows customer stores (yellow) and distribution warehouses (blue) that need to send and receive packages. Ted has been conducting 'red-black ant colony searches' to determine which delivery truck should deliver which package via which route, while minimising the total costs.

futurum
Inspiring the next generation

WWW.FUTURUMCAREERS.COM

TEL: +44 117 909 9150

EMAIL: INFO@FUTURUMCAREERS.COM

The Ohio State University

Department of COMPUTER SCIENCE AND ENGINEERING

Institute for CYBERSECURITY & DIGITAL TRUST

Department of ELECTRICAL & COMPUTER ENGINEERING

FACTSPREAD

Security & Efficiency SEAL Analytics Laboratory

NSF