CYBER WARS
Brightest brains battle the hackers

MEMORIES
Are made of... more than you think

RAISING IQ LEVELS
How your family could help make you smarter

BOOKS SPECIAL
A look at works by Mensan authors

MENSA AT CAMBRIDGE: LAST CHANCE TO TAKE YOUR SEAT
Once the stuff of Hollywood movie plots, cyber security features in films as far back as the 1960s. In the film The Italian Job, a gang of well-organised criminals created a traffic jam in the city of Turin by first loading a malicious program onto a traffic control computer. During the 1980s we saw Matthew Broderick nearly starting World War Three in War Games, and in the early 1990s we first enjoyed watching Robert Redford saving the world in the classic Sneakers, before seeing Johnny Lee Miller and Angelina Jolie glamourising cyber crime in the movie Hackers.

Indeed, Cyber security has been on our RADA for some time now. However, some people are only just starting to appreciate that it’s a real problem which has the potential to significantly impact the economy. Not only can sensitive data be exfiltrated from poorly secured computers, but badly protected industrial sites with computers connected to real machines could result in significant kinetic impact.

Many small businesses are targeted as they begin to operate in the cyber space, and even critical national infrastructure can be threatened by skilled agressors. In the UK, The Centre for the Protection of National Infrastructure (CPNI) describes critical infrastructure as those elements whose loss or compromise could result in a major detrimental impact on the availability, integrity or delivery of essential services, or a significant impact on national security, national defence, or the functioning of the state.

Clearly it is important that we invest in protecting vulnerable assets, including businesses supporting the digital economy. However, one problem which might hamper future efforts in the UK is the looming cyber security skills gap. In fact, some estimates suggest the global appetite for experts in this field is predicted to exceed supply by one third by the end of this decade. A good career move perhaps?

Getting young people interested in cyber security is a step in the right direction, but how can we make cyber security fun? One way to help train the next generation of cyber security professionals is to introduce them to the tools of the trade through a competitive and challenging game environment. Such war games are today gaining increasing popularity amongst amateur enthusiasts and seasoned security professionals alike.

Often, such games will take the form of a “capture the flag” (CTF) competition. During such a competition, teams of hackers will battle through a series of challenging computer puzzles to retrieve a flag (a bit like a password). This flag could be a string of data retrieved by reverse-engineering a computer program, or it might be hidden in a text file on a remote file server which must first be broken into. The possibilities for challenge setters are endless, but puzzles usually fall into one of several categories: Binary reverse engineering and exploitation, web application security, cryptanalysis, and forensics.

Additionally, games are usually presented in one of two styles: “Jeopardy-style”, in which competitors unlock a series of unrelated discrete challenges, and “attack-defence”, in which teams must attack their enemies’ servers and services, while at the same time patching their own services to render them impervious to retaliation.

At The University of Cambridge we’ve been working hard to expose students to practical cyber security problems and have organised a number of CTF competitions. Earlier this year ten Cambridge students who’d performed well in preliminary CTF qualifying rounds were selected to travel to Boston to compete with their American counterparts in a large competition at MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL).
The competition had a brutal schedule and involved 24 hours of intensive hacking activity. Described by the challenge setters ForAllSecure as a "full spectrum" event, this included an attack-defence CTF, as well as several other challenges, including both a physical lock-picking session as well as a "rapid fire" competition in which hackers competed against the clock to exploit vulnerable computer programs in the fastest time possible. The event was staged within the iconic Ray and Maria Stata Center, a distinctive building designed by Pritzker Prize-winning architect Frank Gehry. Dubbed "Cambridge2Cambridge" and originally conceived in the context of a bilateral meeting between David Cameron and Barack Obama in Washington back in January 2015, this event was part of a series of initiatives between the two countries to improve their mutual cyber security stance. It certainly inspired several talented student hackers, and helped to shine a big spotlight on cyber security.

Importantly, it's not just technical skills which are forged in the heat of battle. Essential soft skills, perhaps sometimes lacking in computer science students, are developed too. This benefit was observed by Cambridge students.

One of them, Daniel Wong, said: "The synergy and teamwork during the live CTF was what I enjoyed most. Although our team members were not the best individually, together we were able to gel well together and that feeling of being 'in the zone' and working seamlessly together in attacking other teams, scripting our exploits and rushing to patch our services was fantastic."

Meanwhile another, Gabor Szarka, added: "Maybe somewhat surprisingly of a computer hacking competition, the live CTF was also an exercise in interpersonal skills, since collaborating with people you have just met under significant time pressure in a generally stressful environment does not come naturally."

None of the students, on either side of the Atlantic, had long to prepare for this experience. A substantial amount of the training was extracurricular. We developed a Linux binary reverse engineering and exploitation workshop in-house, part of a course based around free open source tools and a modern 64-bit Linux distribution. Two Jeopardy-style CTF training competitions were also run in-house, which included a number of specially engineered problems designed to expose students to the tools they would require for tackling a typical CTF event."
Gabor Szarka, who participated in these workshops, believes this type of training is important for developing the next generation of cyber security professionals. "This form of education is very difficult to implement in a conventional classroom setting so providing opportunities such as C2C for interested students is crucial to any initiative aiming to train a next generation of cyber security professionals."

Hot off the heels of the Cambridge2Cambridge venture, we were keen to explore the benefits of academic CTF competitions a little bit further. Almost as soon as we returned from Boston, we invited the 13 current Academic Centres of Excellence in Cyber Security Research to take part in a competition hosted by The University of Cambridge.

Ten universities responded, and committed to send a team of four of their best hackers to do battle. For this competition, dubbed Inter-ACE Cyberchallenge, we partnered with stalwart Facebook who set most of the independent challenges. We also asked each university to submit a special guest challenge. This time the game was played out on a "Risk-style" scoreboard, which presented a map of the world (see illustration). Teams could invade countries by solving the many fiendish computer problems. The University of Cambridge had submitted a problem which involved protecting the country of Panama, an Enigma code which needed to be broken by brute force! Only one challenger, Imperial College, managed to break the Enigma code in time.

Ultimately, the day went to The University of Cambridge, which collected the trophy for this inaugural annual event. Later the same evening, 70 competitors and guests enjoyed a lavish dinner together, another opportunity to mingle with other students interested in cyber security. A good time was had by all, another successful event!

A number of academic teams are already well established on the CTF circuit. There are many competitions to take part in around the year, many accessible online and requiring no travel. The "world cup" of hacking is almost certainly the Def Con® finals. This is a well-established attack-defense competition which takes place during a hacking convention held in Las Vegas every year.

The qualifying rounds are jeopardy-style CTF events, so the winners are clearly skilled in both forms of competition. If you want to get involved in CTF, or even organise an academic team, then you'll find the website CTFtime provides a useful list of upcoming events. You can find it at https://ctftime.org/

There are no age limits, and of course you'll find both men and women competing at the highest levels.

Cyber security is for everybody!

In addition to searching out CTF competitions, you might also be interested in The Cyber Security Challenge which offers a unique programme of activities and aims to introduce sufficient numbers of appropriately skilled individuals to learning and career opportunities in the profession. Find out more information about this at https://cybersecuritychallenge.org.uk

In time we hope to see more cyber security talent emerging from British universities and taking on the challenge of protecting our businesses and digital economy from even the most sophisticated cyber threats. A healthy community of motivated ethical hackers, helping to secure Britain and her interests long into the future.

About the author
Mensa member Graham Rymer is a Research Associate at the University of Cambridge's Computer Laboratory