CYBER SECURITY

Protecting digital infrastructure through CIE

Last September, on the recommendation of the Emerging Disciplines Task Force, PEO council recognized communications infrastructure engineering (CIE) as the practice of professional engineering under the *Professional Engineers Act*. What's special about this emerging discipline? And why is it critical to Canadians' physical and economic well-being?

By George R. Comrie, P.Eng., CMC, FEC

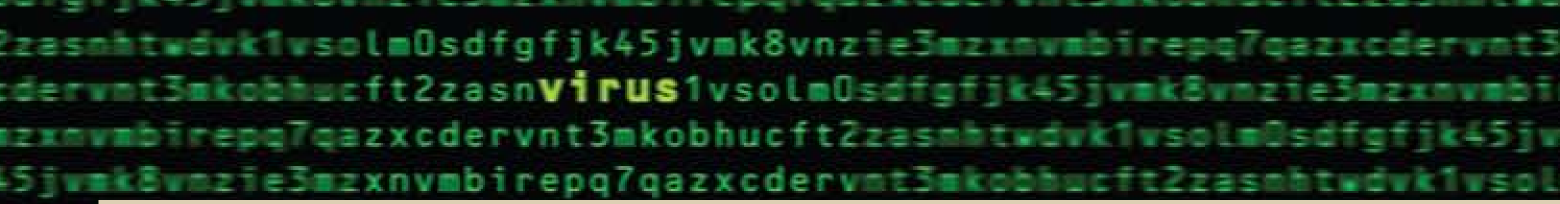
In less than 40 years since the invention of the Internet Protocol (IP), the developed world has become utterly dependent on the Internet for much of its daily activity. Stop and consider the things you take for granted that you could not do if our digital communications infrastructure were unavailable or compromised–things like paying bills online, exchanging documents with suppliers and customers, or filing your tax return.

Canadians depend heavily on our digital infrastructure:

- 74 per cent of Canadian households use paid Internet services;
- 59 per cent of personal tax filings are electronic;
- 67 per cent of Canadians bank online;
- 87 per cent of businesses use the Internet;
- total Canadian online sales: $63 billion;
- federal government offers 130 online services to consumers and businesses (e.g. tax, EI, student loans).

But the risks to society associated with communications infrastructure are even greater when you realize that all of our other critical infrastructures–like transportation, health care and public safety, for example–are themselves dependent on that same communications infrastructure.

So by disrupting or compromising critical data and network assets, it is possible to inflict widespread harm on individuals, organizations, even nations. And as we have seen, this can be done over the Internet from any-



where in the world without the perpetrators ever setting foot on our soil.

Hardly a day goes by without some incident of cyber abuse being reported in the press: the theft of customer data from Sony's online gaming service, forcing shutdown of the service; foreign spies penetrating Canadian government systems, forcing the government to disconnect from the Internet; industrial/commercial espionage conducted to give the perpetrators unfair competitive advantage; denial-of-service attacks against popular websites; and so on.

At a personal level, most of us have received email correspondence as part of a scam designed to defraud us or to trick us into disclosing account numbers and passwords (known in the cyber security industry as *phishing*). And many of us have experienced the infection of our personal computers with *spyware* designed to capture and report our online activities to others, or some form of *malware*, such as a worm or a virus designed to render the computer inoperable and/or its data unusable.

These abuses are all predicated on the unrestricted connectivity provided by the Internet.

ATTACKS INCREASING

Both the frequency and the sophistication of such attacks appear to be increasing, in spite of attempts by industry and government to bolster cyber security. Worse, we appear to have moved from the more benign kind of *hacking* that dominated the early days of cyber security and was motivated by the hacker's desire for prestige and influence, to a more malicious kind of attack motivated by financial gain or by the desire to disrupt and destabilize society and harm citizens (*cyber terrorism*).

Perhaps the most insidious example to date of the latter kind of malware is the so-called *Stuxnet* worm that was discovered earlier this year. Stuxnet is a library file containing complex code that infected Windows computers connected to the ubiquitous Siemens Step 7 programmable logic controllers (PLCs) that are used to control many different kinds of industrial processes and machinery. The file was distributed via the Internet, then introduced into secure facilities via infected USB keys.

Its malicious payload was code that ran secretly and transparently in specific PLCs, controlling specific machines–in this case, centrifuges used to enrich uranium at Iran's Natanz nuclear facility–temporarily changing the frequency at which the centrifuges operated and thereby damaging them.

Stuxnet was clearly created with the goal of disrupting Iran's nuclear program, since it had no affect on PLCs that were not controlling the specific centrifuges used in that program.

Much of the success of the Internet as we know it today may be attributed to the fact that its evolution has been largely unconstrained by regulation and economics. Innovators have responded to its promise of virtually free access to a world-wide market with a flood of applications, products and services. There have been relatively few restrictions on what one can offer or to whom.

The downside of this lack of regulation is that it has exposed us to harm in ways we did not imagine and are unprepared to deal with. Over its short lifespan, the Internet has profoundly changed the way we communicate, entertain ourselves, do business, even govern ourselves, and it has contributed greatly to our productivity and prosperity. But as cyber technology matures, we must expect some discipline to be imposed in the public interest. The challenge will be to balance public safety with the freedom necessary to continue to innovate.

Well, so much for our growing cyber security problem. How do we solve it? Or perhaps a better question: Who is going to solve it? Clearly, it will require highly trained and disciplined professionals to design and operate critical systems that can survive sophisticated attacks of this nature. The consensus of industry and government stakeholders we have talked to is that such individuals are in very short supply–which is where the communications infrastructure engineer, or CIE, comes in.

Communications infrastructure engineering is concerned with the systems-level architecture, design and management of reliable, secure networks for mission-critical and safety-critical applications, including those that support other critical infrastructures.

So what do we mean by communications infrastructure engineering? The first task in addressing a new engineering discipline is to define its scope, and its principal scopes of practice.

TRUSTED NETWORKS

The essential activity of CIE is the system-level design and management of secure or trusted communications networks. A trusted network has the characteristics of availability, confidentiality, integrity and privacy. Our task group decided to limit the scope of the discipline to data in transit (as opposed to in repository or in use), and to exclude from it the configuration and troubleshooting of network devices, such as routers and firewalls (the work of network technicians, and for which vendor certifications exist), as well as application-specific security considerations (which fall within the scope of software engineering).

The principal scopes of practice for CIE are:

- planning and design of trusted communication networks;
- operational oversight of trusted communication networks; and
- risk analysis of, and contingency planning for, network infrastructure.

Engineers have always been at the forefront of innovation and exploitation of technology, so it is no surprise that a number have turned their skills to the challenge of building and maintaining trusted network facilities. Thus far, most have acquired the special technical skills necessary to do this work on the job. Only recently have accredited engineering programs started to emerge that focus on this area of professional practice.

For its initial report, the CIE task group proposed a core body of knowledge that it believes is essential for a CIE practitioner. Beyond subjects that are common to other electrical engineering subdisciplines, like communications engineering, computer engineering and software engineering, it includes:

- information theory and coding;
- OSI model;
- IP and related technology: IPV6, DNS, DHCP, etc.;
- network security;
- networking standards (e.g., ISO 27000 series);
- critical infrastructure protection;
- network risk assessment; and
- compliance and governance.

Several of the industry and government stakeholders we consulted suggested these subjects should also be included in software engineering and computer engineering programs, given the importance of security to all aspects of systems work.

What work remains to be done to bring CIE to maturity as an engineering discipline? Besides enabling PEO to regulate CIE effectively in terms of licensing, discipline, enforcement and professional standards, the goal of the CIE task group is to contribute to solving the world's cyber-security crisis by defining and expanding the CIE labour market, improving CIE practice standards within industry and government, collaborating with other stakeholders, and shaping future legislation and regulations.

Of particular importance to addressing the skills shortage will be to establish data on existing CIE practitioners and their educational backgrounds. Sources of additional training and certification for those already working in the field will be required. More CIE programs and program options will be required to establish the discipline within the engineering profession. Further refinement of the CIE body of knowledge will occur as part of this process.

DEFINING KNOWLEDGE AND SKILL

It will also be important to define the knowledge and skill (academics and experience) requirements for CIE limited licences, to enable the profession to license competent individuals who lack the breadth of engineering background necessary to obtain a P.Eng. licence.

The need for a CIE practice standard should be considered. While progress is being made on technical standards and best practices in the field, it is equally important for licensed engineering practitioners to know what is expected of them in terms of consistent practice.

In terms of regulation, we will need to monitor and respond to government cyber-security initiatives, and to the development of technical and best practice standards, particularly in the US and Europe. In addition, we need to be prepared to propose regulatory policy initiatives to our own Canadian federal government.

It is worth noting the strong parallels between CIE and software engineering in terms of the evolution of these disciplines. In both cases:

- Unlike more traditional engineering fields, the engineering work product is largely intangible and invisible;
- The practice began as an art, with little regulation and few standards;
- Initial practitioners were largely self-taught;
- The introduction of accredited engineering programs was significant in establishing them as engineering disciplines; and
- Industry has been slow to accept standards and certifications.

The CIE task group hopes that, by starting early and being proactive in establishing CIE as an engineering discipline, we may streamline the maturation process for this important field.

The interim report of the CIE task force is available on PEO's website at www.peo.on.ca/publications/Reports/EDTF-CIE Interim Report2011.pdf. Comments are welcome. Σ

George Comrie, P.Eng., CMC, FEC, is a computer systems engineer and management consultant whose career has focused on mission-critical, safety-critical computer systems. A past president of PEO, he chairs the emerging disciplines task group on communications infrastructure engineering.