Keystone Business Models for Network Security Processors

Arthur Low and Steven Muegge

> “*Your ability to negotiate, communicate, influence, and persuade others to do things is absolutely indispensable to everything you accomplish in life. The most effective men and women in every area are those who can quite competently organize the cooperation and assistance of other people toward the accomplishment of important goals and objectives.*”
>
> Brian Tracy
> Entrepreneur, business coach, author, and speaker

Network security processors are critical components of high-performance systems built for cybersecurity. Development of a network security processor requires multi-domain experience in semiconductors and complex software security applications, and multiple iterations of both software and hardware implementations. Limited by the business models in use today, such an arduous task can be undertaken only by large incumbent companies and government organizations. Neither the “fabless semiconductor” models nor the silicon intellectual-property licensing (“IP-licensing”) models allow small technology companies to successfully compete. This article describes an alternative approach that produces an ongoing stream of novel network security processors for niche markets through continuous innovation by both large and small companies. This approach, referred to here as the "business ecosystem model for network security processors", includes a flexible and reconfigurable technology platform, a “keystone” business model for the company that maintains the platform architecture, and an extended ecosystem of companies that both contribute and share in the value created by innovation. New opportunities for business model innovation by participating companies are made possible by the ecosystem model. This ecosystem model builds on: i) the lessons learned from the experience of the first author as a senior integrated circuit architect for providers of public-key cryptography solutions and as the owner of a semiconductor startup, and ii) the latest scholarly research on technology entrepreneurship, business models, platforms, and business ecosystems. This article will be of interest to all technology entrepreneurs, but it will be of particular interest to owners of small companies that provide security solutions and to specialized security professionals seeking to launch their own companies.

Introduction

New business models are needed for small suppliers of network security processors and specialized security products. The conventional business models in use today favour large, established incumbents who develop products for large and well-understood markets. Ideally, new business models would enable and reward continuous innovation by both large and small companies to produce a continuous stream of novel security products for niche markets. The beneficiaries would include the buyers of specialized cybersecurity products and their users, the technology entrepreneurs who develop and commercialize specialized security products, and the engineers and product designers with a broader range of employment and contracting opportunities.

Keystone Business Models for Network Security Processors

Arthur Low and Steven Muegge

Network security processors are specialized components of high-performance security systems used by organizations such as banks, government embassies, and multinational corporations. They provide *acceleration* of the cryptography functions that encrypt and decrypt outgoing and incoming information and protect against intrusion by adversaries. Security systems with hardware acceleration have greater performance than systems that implement the cryptography functions in software, but are more costly and require more time and specialized expertise to develop, implement, and deploy.

There are two broad categories of business models in use today for providers of network security processors and the security products that employ them. Both categories favour large multinational incumbents such as IBM (ibm.com), Hewlett-Packard (hp.com), Bull SAS (bull.com), SafeNet (safenet-inc.com), and Thales Group (thalesgroup.com) rather than small companies and new entrants. "Fabless semiconductor" models require commitment of large up-front capital, exposing investors to significant risk. Silicon "IP-licensing" models prevent the small company from interacting directly with customers and end-users, and because the customer relationship is owned by the systems integrator who packages the complete solution, small suppliers cannot easily appropriate a significant portion of the value that their innovations create for customers.

This article contributes an alternative approach that we refer to here as the "business ecosystem model for network security processors". It builds on lessons learned from the industry experience of the first author and implements concepts from the latest scholarly research on technology entrepreneurship (Bailetti, 2012: timreview.ca/article/520; Bailetti et al., 2012: 557), business models (Muegge, 2012: 545; Bailetti, 2009: 226), platforms and keystones (Bailetti, 2010; 355), and business ecosystems (Muegge, 2013: 655; Muegge, 2011: 495; Bailetti, 2010: 325; Carbone, 2009: 227; Hurley, 2009: 276; Bailetti, 2008: 138). This approach has several parts, including a *network security processor platform* that companies can use and reconfigure to build innovative security solutions for niche markets, a *keystone business model* for the company that leads platform maintenance and evolution, and a *business ecosystem* of companies that develop complementary products, services, and technologies, contribute assets to the platform, and build security products that utilize the platform. The ecosystem approach enables new business models for participating companies. Building solutions on top of the proposed platform does not require the sale of large volumes to generate profits. Moreover, it allows small companies to interact directly with end-customers and retain the rights over the intellectual property they create.

The body of this article is structured in four sections. The first section reviews the conventional business models used by providers of network security processors and discusses their weaknesses and limitations. The second section presents lessons learned from the industrial experience of the first author as a cryptography chip designer and entrepreneur. The third section builds on the lessons learned to develop the business ecosystem model for network security processors; it explains the business model of the ecosystem keystone, the technology that supports the ecosystem, and the new opportunities for business model innovation by companies participating in the ecosystem. The fourth section concludes with a renewed call for innovation in the cybersecurity domain – not only of novel technology but also of *novel business models* that fully exploit the opportunities enabled by technological innovation.

Conventional Business Models

A business model provides a concise explanation of how a business operates. Many business model frameworks have been proposed. This article employs the technology entrepreneurship framework previously published in the *TIM Review* (Muegge, 2012; timreview.ca/article/545) and employed with technology entrepreneurs in the Lead to Win ecosystem (Bailetti and Bot, 2013; timreview.ca/article/658). Although each company's business model may comprise a unique combination of customer pain points, stakeholder value propositions, a profit formula of revenues and costs, and the company's capabilities, it is often useful to identify and label groups of business models that share some similar features. The three groups of interest in this section are: i) integrated device manufacturers, ii) fabless semiconductor companies, and iii) silicon IP-licensing companies.

Prior to the 1980s, most companies that developed integrated circuit devices were *integrated device manufacturers*. Vertically integrated firms would own and control their own production facilities, including a foundry for fabricating semiconductor wafers, and perform basic research, product design, manufacturing, sales, and support – all in-house.

Keystone Business Models for Network Security Processors

Arthur Low and Steven Muegge

Fabless semiconductor business models became possible in 1987 when the Taiwan Semiconductor Manufacturing Company (tsmc.com) first offered the use of an integrated circuits fabrication facility to companies who could design their own integrated circuits. Instead of investing billions of dollars up-front to acquire and operate an integrated circuits fabrication facility, a fabless semiconductor company could acquire electronic design automation (EDA) software, employ engineers to design integrated circuits using the EDA software, and outsource the manufacturing to others. The non-recoverable engineering costs to produce a new integrated circuit must be recouped from product sales. To be profitable, a fabless semiconductor company requires high sales volumes – typically in the tens of thousands or hundreds of thousands of units.

Silicon *IP-licensing* business models require a company to license modular design units to become parts of integrated circuits designed by others. An IP-licensing company generates revenue from some combination of fixed fees per unit of intellectual property and royalties paid per device manufactured. ARM Holdings (arm.com) was the first company to successfully employ a business model with IP-licensing. ARM developed a “soft” reduced instruction set (RISC) microprocessor design that customers could license and embed within their integrated circuit designs to control applications-specific logic. The consumer electronics market grew rapidly when highly integrated microchips with embedded ARM processors enabled significant cost and size reductions. Smart, hand-held communications-enabled devices, such as cell phones, moved from science fiction to fact almost overnight. By 2012, ARM was employing more than 2000 people and ARM's partners had shipped more than 30 billion ARM-based integrated circuits (ARM Annual Report, 2012; tinyurl.com/kvgzuf6).

Despite these large-company successes, neither the fabless semiconductor models nor the IP-licensing models are appealing for small providers of security solutions – for reasons developed in the next section.

Background and Lessons Learned

The business model insights and platform architecture that enable the business ecosystem model for network security processors have evolved over the past 13 years. In 2000, Chrysalis-ITS extended its business of developing specialized hardware and software for the public-key infrastructure (PKI) market by opening a fabless semiconductor division to develop a high-performance line of network security processors as "systems on chips". Chrysalis-ITS's first system on a chip, the Luna 340, integrated five microprocessors with instruction sets extended to implement a number of important security operations, such as Internet Protocol Security (IPSec) and the RSA public-key cryptographic (PKC) algorithm. Both are used in banking networks and Internet security based on the secure socket layer (SSL) protocol. In 2001, Chrysalis-ITS introduced the Luna 510, a product that delivered 100 times greater performance than the Luna 340. One microprocessor provided SSL-protocol control and data-flow management between multiple instances of highly optimized encryption and hashing algorithm processors. In 2004, Chrysalis-ITS was acquired by Rainbow Technologies, which then merged with SafeNet (safenet-inc.com). In 2007, Elliptic Technologies (elliptictech.com) developed a public-key cryptographic algorithm compute engine. The engine was based on an arithmetic logic unit designed to flexibly compute over any integer size up to thousands of bits the modular arithmetic functions that are the basis for security applications based on public-key cryptography. In 2009, Crack Semiconductor (cracksemi.com), a company founded by the first author of this article, developed a scalable, modular architecture for optimally computing these modular arithmetic functions in a very low-cost field-programmable gate array (FPGA). The architecture was refined over several generations so that current implementations rival the performance of the Luna 510 when coupled to an embedded applications processor. The proposed platform of the business ecosystem model for network security processors is an implementation of the next generation in the evolution of this architecture.

The first author’s industry experience as a designer and entrepreneur suggests five lessons for small suppliers of security solutions, each of which is expanded upon in the subsections that follow:

1. Control the key technology components that differentiate your business from others.

2. Avoid fabless semiconductor models for small markets.

3. Go after niche markets that are unattractive to large incumbents.

4. Implement the best-available design methodologies, tools, algorithms, and architectures.

5. Look to emerging industry standards for global opportunities to innovate.

1. Control the key technology components that differentiate your business from others
Silicon IP-licensing models place the IP supplier in a subordinate role in the value chain; from a subordinate role, it is difficult to charge license fees that are high enough to recoup R&D costs. ARM has been very successful with IP-licensing for high-volume consumer devices, but comparable mass-market sales volumes are not feasible for security applications. Furthermore, the downstream systems integrator controls the relationship with customers and end-users. For these reasons, silicon IP-licensing models are not appealing for small providers of security solutions.

The Luna 510 provides a cautionary tale regarding IP licensing and loss of control of key technology components. The Luna 510 was a technological breakthrough in network security processor design, but failed to reach the market when the Luna 340 failed. Despite the viability of the Luna 510 design, investors shut down the entire semiconductor division when it became clear that the sunk costs of the Luna 340 project would produce no revenue. Furthermore, the entirely independent and original in-house development of the Luna 510 was tainted by a clause in the Luna 340 development contract with a third-party that assigned a small but meaningful right to “derivative works” to the third-party. Because the IP was “tainted” with unquantified legal issues, new investors were unwilling to recapitalize the semiconductor division as a separate company. Thus, due to factors outside the control of the development team – in particular, the failure of another product and the loss of control over intellectual property – the Luna 510 was never produced.

2. Avoid fabless semiconductor models for small markets
Fabless semiconductor models incur high R&D costs and non-recoverable engineering costs to produce a custom integrated circuit. To recoup these costs, revenues must be in the hundreds of millions of dollars, which requires in-depth market knowledge, large sales volumes of tens or hundreds of thousands of units or very high selling prices and profit margins, and venture-capital or other institutional backing. Opportunities with these characteristics are rare for small providers of security technologies.

PMC-Sierra (pmcs.com) is an example of a successful fabless semiconductor company. PMC-Sierra achieves sales in the hundreds of millions of dollars per year by providing high-performance optical-networking integrated circuits to large telecommunications equipment manufacturers such as Cisco Systems (cisco.com) and Huawei (huawei.com). Development of a new integrated circuit may cost PMC-Sierra $30 million to design, and it may incur $3 million in non-recoverable engineering charges. The integrated circuit design will be developed to a specification that meets the needs of several key clients, and features are included based on significant volume commitments. Like other companies employing fabless semiconductor models, PMC-Sierra assumes significant risk and revenue loss if the integrated circuit design is late or fails to function as specified.

3. Go after niche markets that are unattractive to large incumbents
Large incumbents employing either silicon IP-licensing models (such as ARM in the consumer products market) or fabless semiconductor models (such as PMC-Sierra in the telecommunications equipment market) *cannot* be profitable in small niche markets where their high cost structures and requirements for large sales volumes become a liability. Markets that are unattractive to large incumbents such as ARM and PMC-Sierra are an opportunity for small security providers – if those companies can be profitable at small-to-medium sales volumes.

Going after niche markets of *a thousand units* or *a hundred units* is not possible with the same technology and business models used today by incumbents; innovation is required in both the technology and business models used by small security providers.

4. Implement the best-available design methodologies, tools, algorithms, and architectures
Technology failure guarantees business model failure. Getting the technology right is necessary but not sufficient for success.

The Luna 340 network security processor is an example of what can go wrong when companies do not implement the most appropriate design methodologies, tools, and algorithms, and architectures. A team of engineers worked for several years to design and implement the Luna 340. Several early management decisions, intended to reduce costs and eliminate steps, became serious problems late in the development process. To save money on expensive EDA software licenses, a critical integrated circuit layout tool was not upgraded. Fatal circuit-timing errors were introduced, which the tool upgrade would have detected and fixed. A second design iteration – an expensive and time-consuming redesign of the integrated circuit – also failed to get the timing right. These problems were further compounded by other performance-degrading design flaws and by an inefficient architecture. In contrast, the technically successful Luna 510 employed more efficient architectures for a faster and more physically controllable hardware implementation, state-of-the-art synthesis algorithms for placement and routing, and a prototyping methodology including verification in full-speed FPGA-based prototypes, then in fabrication "shuttles" (where many companies would share a silicon wafer) before commitment to the full fabrication and manufacturing process. These design methodologies, tools, algorithms, and architectures could have been employed from the beginning of the Luna 340 project; cuttings costs in these areas was very costly later. Past research on product development has consistently found that greater early investment in architecture and flexibility results in better-performing projects (e.g., MacCormack et al., 2001; tinyurl.com/am6axfs) and the experience of the Luna 340 developers supports these findings. Greater upfront exploration of architecture and algorithms and upfront adoption of appropriate tools and prototyping methodologies could have avoided the costly delays that happened later.

For a conventional integrated circuit design, these upfront items appear as "sunk costs" to be minimized by management. However, when innovation occurs within and on top of a platform – the ecosystem approach recommended here – design methodologies, tools, algorithms, and architectures are investments in the future, to be recouped over many niche custom designs and derivative products.

5. Look to emerging industry standards for global opportunities to innovate

Small companies need to address opportunities that are global rather than local or regional (Tanev, 2012; timreview.ca/article/532), and emerging industry standards can provide insights into global opportunities. An example is the new ISA100.11a standard (isa.org/ISA100-11a) for wireless sensor networks. ISA100.11a differs from WirelessHART, a competing standard from the HART Communications Foundation (hartcomm.org), by including the *option* to use public-key cryptography technology for the provisioning of new devices joining the network. Because ISA100.11a is a new standard, and public-key cryptography is optional rather than required, few vendors are implementing this option in their first-generation ISA100.11a- and WirelessHART-compliant products. However, activity within the standards groups suggests that public-key cryptography will become increasingly important in the future: the International Society for Automation (isa.org), steward of the ISA standards, is also pursuing standardization of public-key cryptography technology in many areas, for example, to enable over-the-air (OTA) provisioning of devices. Participation in standards development can provide small security providers with valuable insights into possible futures, as well as opportunities to gain early access to information, build relationships with potential collaborators, shape requirements, and influence the technical direction of standards.

Participation in industry standards development has traditionally been a gamble for small companies using conventional business models. Costs include money and time, and the outcome is always uncertain: standards can fail for technical or political reasons, or adopters may converge on a different competing standard. However, the payoffs can be large. For example, Crack Semiconductor has developed security technologies ahead of an expected global market for wireless sensor networks for industry control (Low, 2013; timreview.ca/article/682). Furthermore, a business ecosystem approach to developing security products can substantially reduce the costs and risk of participating in standards development while retaining all the potential benefits. Participation in the development of the ISA100.11a standard is an important aspect of Crack Semiconductor's network security processor platform strategy. Other companies in the ecosystem benefit from the information and influence while sharing the costs and obligations.

In summary, for small companies of security solutions to compete successfully with established incumbents, a new approach is needed. That new approach should address global opportunities in niche markets, using the best-available design methodologies, tools, algorithm, and architectures, with business models unlike those commonly in use today by large incumbents. The next session describes one such approach.

An Alternative Approach: The Business Ecosystem Model

Business ecosystems provide a way for small companies to achieve more, learn faster, and reach farther than otherwise possible, while sharing risks and costs with others (Muegge, 2013; timreview.ca/article/655). Hurley (2009; timreview.ca/article/276) identifies several benefits enjoyed by participating entrepreneurs, including reduced barriers to market entry, increased access to customers, reduced operating costs, and the means to overcome regional limitations. Carbone (2009; timreview.ca/article/227) argues that business ecosystems can also enable business model innovation, especially by companies providing complementary assets.

Business ecosystem approaches have been previously developed for various domains, including job creation through technology entrepreneurship (e.g., the Lead to Win ecosystem: leadtowin.ca; Bailetti and Bot, 2013: timreview.ca/article/658), community development of open source software tools and frameworks (e.g., the Eclipse ecosystem: eclipse.org; Muegge, 2011; timreview.ca/article/495), and communication-enabled applications (e.g., the Coral CEA ecosystem; coralcea.ca; Pyke, 2010; timreview.ca/article/347). This article is the first known application of the business ecosystem approach to the domain of network security processors. However, the basic premise is similar to that of these other domains: ecosystem participants innovate together to solve bigger network-security problems that any one small or medium-sized company could address on its own.

As in other domains, the business ecosystem model for network security processors has several codependent parts. The most essential components in this domain are: i) a *keystone company* that owns, operates, and evolves the platform; ii) a *platform* of modular technology building blocks that others can utilize, build on, and contribute to; and iii) a *network of participating companies* that can innovate in new ways. Below, each component is briefly described in its own subsection.

Keystone business model

The keystone is the company that owns, operates, and evolves the platform (Bailetti, 2010; timreview.ca/article/355). The keystone plays a central role; for this ecosystem model to succeed, there must be a keystone business model that earns attractive profits for the keystone company.

Table 1 compares the proposed business model of the ecosystem keystone with the conventional fabless semiconductor business models and IP-licensing business models described in previous sections. The rows in Table 1 are a subset of the components of the technology entrepreneurship business model framework, selected to emphasize the salient differences. There are many similarities not shown in the table; for example, all three models are different ways of addressing the same basic "pain points" of cybersecurity.

Consistent with lesson 1, the keystone controls the key components of the technology platform – especially the cryptography algorithms, hardware acceleration, and platform architecture (described in the second subsection) – while enabling complementary innovation by other companies. Incentives are aligned, because success of the keystone business model *critically depends on* success by participating companies (described in the third subsection). Also consistent with lesson 1, participating companies keep control of their own differentiating innovations, with the option to selectively contribute specific innovations back to the platform for use by others.

Technology that supports the keystone business model

The platform that anchors a business ecosystem can take many different forms – including a product, process, location, service, or technology (Bailetti, 2010; timreview.ca/article/355). The platform for network security processors is the continued evolution of the architecture previously described in the section on background and lessons learned. It provides the essential technology components of a network security processor, tested and verified together as a system, in a modular form that can be configured in different ways, and extended with new application-specific functionality implemented in software. Cryptography functions are implemented in flexible programmable logic, avoiding the non-recoverable fixed costs of new custom silicon integrated circuits, while providing real-time performance far exceeding a software-only system on an embedded microprocessor. Thus, a new design built on the platform can be profitable at much lower sales volumes than previously possible.

The platform is made possible by an innovative network security processor architecture developed by Crack Semiconductor (cracksemi.com). The current implementation is built on the Xilinx (xilinx.com) Zynq Extensible Processing platform (EPP; tinyurl.com/kecww6k), a flexible "system on a chip" that combines a large array of programmable logic with general purpose microprocessors – more specifically, a hardened dual-core ARM-9 processor. The first microprocessor runs an SSL software library that interfaces to public-key cryptography algorithms implemented on the chip in programmable logic. The second microprocessor runs the software that provides custom requirements for specialized niche applications. The platform includes a default software stack for the second processor that includes a Linux-based operating system, a suite of open source

Table 1. Comparison of network security processor business models

	Fabless Semiconductor Business Models	**IP-licensing Business Models**	**Keystone Business Model for a Network Security Processor Business Ecosystem**
Customer	Systems integrators and providers of high-performance security products that require hardware acceleration by network security processors.	Systems integrators that provide integrated circuit products that require on-chip network security processors.	Various levels of systems integrators and demanding end-customers of high-performance security solutions. Systems integrators can participate in the ecosystem to become partners rather than customers or competitors.
Profit formula	Revenues are *product sales* of silicon integrated circuit devices. Costs include the EDA tools, R&D, and non-recoverable engineering (NRE) of outsourced integrated circuit manufacturing. For revenues to exceed costs, high sales volumes are needed (e.g., PMC-Sierra providing products to telecom equipment manufacturers).	Revenues are some combination of fixed *license fees* per unit of IP and *royalties* paid per device manufactured. Costs include the EDA tools and R&D to develop modular blocks of IP to license. For revenues to exceed costs, high sales volumes are needed (e.g., ARM providing IP for mass-market consumer electronics industry).	Revenues are *product sales* from a continuous stream of novel security products for niche markets. Products could include modular components of cybersecurity systems or complete security solutions. Costs include maintenance and extension of the platform, orchestration of innovation within the ecosystem, and investment in ecosystem health and growth. Revenues and costs are shared with participating companies.
Capabilities required	• Multi-domain experience in semiconductors and complex software security applications • Multiple iterations of hardware and software configurations	• Multi-domain experience in semiconductors and complex software security applications • Multiple iterations of hardware and software configurations	• *Platform* to be reconfigured and built on by others • *Network of participating companies* of at least three types: i) providers of security products, ii) providers of platform complements, and iii) users of security products
Applicability and context	• Favours large incumbents	• Favours large incumbents	• Attractive to small and large companies and new entrants • Enables *opportunities for business model innovation* by participating companies • Can be profitable with sales of thousands or hundreds of units

middleware, and assorted security applications. A niche application could require a custom stack that removes unneeded components, swaps out some components for specialized substitutes, and adds new proprietary custom code.

Opportunities for ecosystem companies
Participation in the network security processor ecosystem is appealing for at least three categories of company: i) providers of specialized niche technologies that complement the platform assets; ii) system integrators that build specialized security products on top of platform assets; and iii) demanding users of security products that participate in order to influence the evolution of the platform and of products that build on the platform. Examples of platform complements include hardware and software interfaces and drivers, specialized software at the middleware and application layers of the stack, and new cryptographic algorithms; providers may choose to selectively contribute some technologies and assets into the platform for use by others, for example to stimulate demand for the provider's proprietary products and services. Examples of demanding users of security products include banks and other financial institutions, governments (especially military applications and government foreign offices), institutions in the medical industry, the operators of critical infrastructure such as nuclear power facilities, and corporations. Such participants could be motivated to shape requirements, send strong signals of support, influence technical work with their investment, and gain early access to information. These motivations are similar to those for companies to participate in standards groups (lesson 5).

The network security processor ecosystem enables new opportunities for business model innovation by participating firms of all three categories identified previously (providers of complements, providers of security products, and demanding users). Returning to the components of the technology entrepreneurship business model framework (Muegge, 2012; timreview.ca/article/545), participants can: i) gain access to new capabilities; ii) reduce cost structures; iii) enable new revenue streams; iv) reach new stakeholders with new and stronger value propositions; and v) address new problem spaces that would otherwise be unavailable.

Security products developed with this approach could be profitable at sales volumes of thousands or hundreds of units – orders of magnitude below the minimum volumes required for security products using the conventional business models in use today. Providers can develop highly specialized niche products that would not otherwise be viable, for customers willing to pay high selling prices for dedicated solutions to their specialized security problems.

The network security processor ecosystem would be membership-based with restrictions and approvals required for entry. Closed membership is an important and necessary point of difference from, for example, the open ecosystems anchored around community-developed open source software where anyone can participate (e.g., Muegge, 2011; timreview.ca/article/495). The most important factor requiring this difference is government policy and regulation of cybersecurity technology: some nations regulate strong cryptography and the exchange of cryptography technology with other nations as a security concern. The United States, for example, has a body of rules including the International Traffic in Arms Regulations (ITAR; tinyurl.com/8l9zvhh), the United States Munitions List (USML; tinyurl.com/k8tvoj5), and the Arms Export Control Act (AECA; tinyurl.com/8yhb7wx), that have implications for international collaboration on cybersecurity. Some engagements may require approval from one or multiple jurisdictions. The keystone company plays a central role in developing and maintaining the membership criteria and rules of conduct, in accordance with the laws of its jurisdiction.

Conclusion

This article has argued that small innovative suppliers of network security processors and high-performance security applications that require network security processors for hardware acceleration should consider forming a business ecosystem. The configuration described here includes a platform of reconfigurable and extensible network security processor technology, a business model for the keystone company that maintains and evolves the platform architecture, and a network of participating companies that innovate within and on top of the platform. The ecosystem enables new opportunities for business model innovation by participating companies. Incentives are aligned: success of the keystone critically depends on the participation and business success of the companies that build on and contribute to the platform, including providers of niche security technologies, providers of security products that utilize the platform, and demanding end-users of security products. The outcome is a continuous stream of security innovation and of specialized security products – including products with projected sales volumes in the thousands or hundreds of units that are not economically viable with conventional business models. We call upon managers of companies large and small, and upon technology entrepreneurs seeking new opportunities, to join us in making this happen.

This ecosystem model requires some aspects of the overall solution to be shared with collaborators and partners. The platform provides a high entry barrier that protects the ecosystem from competitors, because there is no disclosure of the proprietary acceleration technology that integrates high-performance cryptographic compute offload processors with a low-level cryptographic library. Partners can therefore more rapidly develop advanced software solutions because they do not need to solve the optimization problems they would encounter if they had to develop their own network security processor. The platform's value increases significantly due to the strong network effects that are associated with multiple third-parties developing software that complements the platform.

We conclude with a renewed call for innovation in the cybersecurity domain. The technological challenges of cybersecurity have received much attention in this issue of the *TIM Review* as well as within this article. But equally daunting are the business model challenges. Just as business model innovation is required to fully exploit the network security processor platform described here, we expect that the commercial value of future innovation in cybersecurity technology may remain latent and unrealized until it is unlocked by corresponding innovation in business models and commercialization.

About the Authors

Arthur Low is the founder and Chief Executive Officer of Crack Semiconductor, a supplier of high-performance cryptographic silicon IP used in some of the most demanding security applications. Arthur has a number of patents in the field of hardware cryptography. He has worked for a number of IC startups as a Senior IC designer and Architect and gained much of his fundamental IC design experience with Bell-Northern Research in the early 1990s and with IBM Microelectronics in the late 1990s. Arthur has a BSc degree in Electrical Engineering from the University of Alberta in Edmonton, Canada, and is completing his MSc degree in Technology Innovation Management in the Department of Systems and Computer Engineering at Carleton University in Ottawa, Canada.

Steven Muegge is an Assistant Professor at the Sprott School of Business at Carleton University in Ottawa, Canada, where he teaches within the Technology Innovation Management (TIM) program. His research interests include open and distributed innovation, technology entrepreneurship, product development, and commercialization of technological innovation.

Citation: Low, A. and S. Muegge. 2013. Keystone Business Models for Network Security Processors. *Technology Innovation Management Review.* July 2013: 25–33.

Keywords: cybersecurity, business model innovation, technology entrepreneurship, commercialization, business ecosystems, platforms, semiconductors