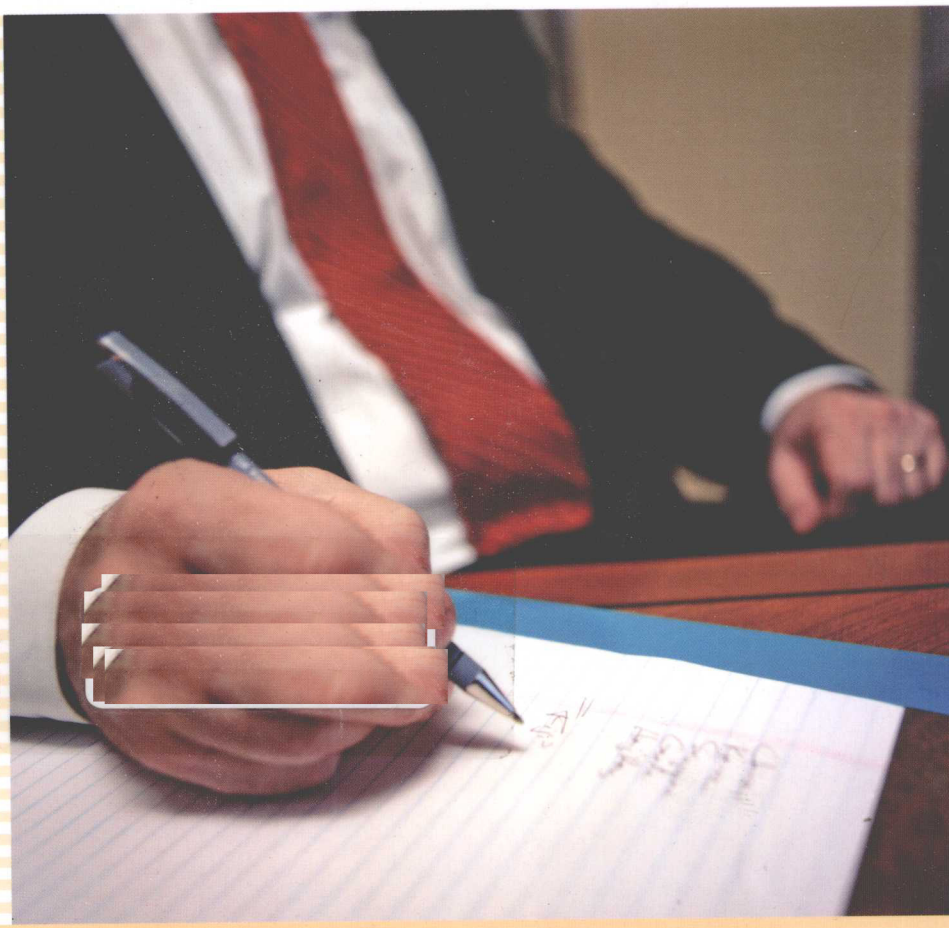
高等学校“十一五”规划教材

新编科技英语阅读教程

主编　范莹芳　副主编　杨　琪　杨振华



哈爾濱工業大學出版社

高等学校“十一五”规划教材·科技英语系列

新编科技英语阅读教程

主　编　范莹芳

副主编　杨　琪　杨振华

哈爾濱工業大學出版社

内 容 简 介

本书主要是为大学本科高年级学生及研究生编写的，是与《科技英语翻译教程》和《科技英语写作教程》相配套的教材。本书侧重于提高读者的英语语言能力，内容丰富，信息前沿，语言地道。本书所选文章分精读和泛读两类，难度适中，实用性较强。每个单元均设计了练习题，针对性较强。本书可作为理工科本科高年级学生及研究生教材，也可供英语爱好者作为英语科普读物使用。

图书在版编目(CIP)数据

新编科技英语阅读教程/范莹芳主编. —哈尔滨：哈尔滨工业大学出版社，2010.4

全国高等学校“十一五”规划教材·科技英语系列

ISBN 978-7-5603-3005-1

Ⅰ.①新… Ⅱ.①范… Ⅲ.①科学技术-英语-阅读教学-高等学校-教材 Ⅳ.①H319.4

中国版本图书馆 CIP 数据核字(2010)第 066453 号

责任编辑 郝庆多
封面设计 张孝东
出版发行 哈尔滨工业大学出版社
社　　址 哈尔滨市南岗区复华四道街 10 号　邮编 150006
传　　真 0451-86414749
网　　址 http://hitpress.hit.edu.cn
印　　刷 哈尔滨工业大学印刷厂
开　　本 787mm×960mm　1/16　印张 18　字数 417.6 千字
版　　次 2010 年 6 月第 1 版　2010 年 6 月第 1 次印刷
书　　号 ISBN 978-7-5603-3005-1
定　　价 30.00 元

前　言

科技英语作为一种实用英语文体形式，用于定义现象、阐释理论、描述过程等。为了准确客观地传递信息，科技文献往往要运用结构复杂、修饰繁多，甚至有些晦涩难懂的长句来表达事理现象的逻辑关系，这给读者的阅读和理解带来诸多困难。

根据多年对本科生和研究生的教学反馈情况，针对阅读障碍问题，我们结合多年的教学与研究实践，收集和整理了32篇不同类型的科普文章，从不同的侧面反映了当今科技发展的现状和趋势，同时展现了科技英语自身的语言特点。

本书所选内容丰富，难易兼顾，共分16个单元，内容均选自互联网上的科普文章，涉及能源、环境保护、互联网、生物、计算机、农业、基因工程、气候、地理等领域。每个单元包含两个内容相关联的篇章，每个篇章后设有一般词汇与科技术语解释以及与课文相关的练习等，并在全书的最后提供了练习的参考答案，以便读者使用。

本书具有以下特点：

题材新颖，时代性强：收录了热门科技领域的最新报道。

难度适中：每单元收录A、B两篇文章，分别适合精读和泛读，方便老师和学生根据实际教学情况灵活选用。

练习形式多样：包括阅读理解、简答、选词填空以及语义解释等，帮助学生了解科普文章的特点和相关知识。

读、译相结合：每个单元后都选取了同本单元主题一致或相近的篇章、长句练习以帮助学生提高翻译技能，并更好地熟悉和掌握科技文体的英汉转化过程。

本书编写中吸收了最新的科技研究成果，参考和引用了有关论著、文章及其他文字资料，文中未能一一注明，在此向有关作者表示感谢。由于编写时间较为仓促，如有遗漏或不当之处，敬请同行专家及广大读者随时提出宝贵意见。

编　者

2010年5月

目　录

Unit 1 Cybersecurity

Text A

BioVault Locks Up Biometrics

1. If a user, a web customer say, wishes to send a message or other data to another user, an online shop, over an unsecured network, the message must be encrypted to avoid interception of sensitive information such as passwords and credit card information.

2. Encryption relies on authentication being symmetric to work. In other words, the user's password or PIN must match the password or PIN stored by the online shop to lock and unlock the data. This is because encryption systems use the password or PIN to produce, or seed, a random number that is used as the cipher for encrypting the data. If the passwords do not match exactly then the seed will be incorrect, the random number different and the decryption will fail.

3. One way to avoid users having to remember endless, complicated passwords is to use biometrics, including fingerprints, iris pattern, face recognition. However, biometrics is not a symmetric process. The initial recording of biometric data samples only a limited amount of the information, the pigment patter in one's iris, for instance. The unlocking process then compares the iris pattern, or other biometric "token", being presented for access with the sample stored in the database. If the match is close enough, the user can gain entry.

4. The reason for this asymmetry is that any biometric system takes only a digital sample of data from the fingerprint or iris, for instance. Moreover, even the legitimate user will not be able to present exactly the same biometric data repeatedly. The close enough aspect of biometrics does not make biometrics insecure, provided that the closeness is very precise, but it does mean that biometric tokens cannot be used to create a secret key for an encryption algorithm.

5. Bobby Tait and Basie von Solms of the University of Johannesburg, Gauteng, South Africa, explain how biometrics can nevertheless be used to make a consistent secret key for encryption.

6. In conventional encryption, if Alice wishes to send a secret message to Bill, then she must encrypt the message, whether it is an email or credit card details transmitted from her computer to the online shop. In order for the encryption algorithm to provide cipher text that is random, a secret key must be

provided. Alice and Bill must share exact copies of their secret key for this to work.

7. Aside from the asymmetry in biometrics, this approach will not work because Alice and Bill cannot provide the same biometric token to encrypt and decrypt the message. Now, Tait and von Solms have used the so-called BioVault infrastructure to provide a safe and secure way for Alice and Bill to share biometric tokens and so use their fingerprints, iris pattern, or other biometric to encrypt and decrypt their data without their biometrics being intercepted.

8. The BioVault encryption system works as follows:

9. In phase 1, Alice identifies herself to the authentication server, and indicates that she wants to send an encrypted message to Bill and requests Bill's biometric key from the server.

10. In phase 2, the server retrieves a random biometric key from Bill's stored biometric keys.

11. In phase 3, Alice uses the biometric key to encrypt her message and sends it to Bill.

12. In phase 4, Bill receives the message sent by Alice, and decrypts the message by testing the biometric keys in his database against the received cipher text.

13. The fact that each biometric key (data) is unique means that the BioVault system can irrevocably identify and authenticate users through their biometric keys (data) and detect fraudulent use of biometric keys.

14. Tait adds that the same approach could also be used to digitally sign electronic documents, files, or software executables using biometrics. He will be presenting the team's results on this aspect of their work in the UK at the beginning of September. "If passwords or tokens are used for authentication, only the password or token is proven as authentic—not the user that supplied the token or password," he explains. "Biometrics authenticates the user directly—this was one of the drivers behind the BioVault development."

(http://www.sciencedaily.com /releases/2009/07/090731085817.htm.)

Glossary

biometrics [baiəu'metriks] a branch of biology that studies biological phenomena and observations by means of statistical analysis *n*. 生物测定学

encrypt [in'kript] convert ordinary language into code *v*. 加密

interception [intə(:)'sepʃən] the act of intercepting; preventing something from proceeding or arriving *n*. 截击,截取,截住,截断,拦截,窃听

authentication [ɔ:θenti'keiʃən] validating the authenticity of something or someone *n*. 证明,鉴定

symmetric [si'metrik] having similarity in size, shape, and relative position of corresponding parts *adj*. 对称的

cipher ['saifə] a message written in a secret code *n*. 暗号

iris ['aiəris] muscular diaphragm that controls the size of the pupil; it forms the colored portion of the eye *n*. 虹膜

token ['təukən] an individual instance of a type of symbol *n*. 表征,记号

asymmetry [æ'simətri] a lack of symmetry *n*. 不对称

insecure [insi'kjuə] lacking in security or safety *adj*. 不安全的

algorithm ['ælgəriðəm] a precise rule (or set of rules) specifying how to solve some problems *n*. 算法

decrypt [di:'kript] convert code into ordinary language *v*. 译,解释

infrastructure ['infrə'strʌktʃə] the basic structure or features of a system or organization *n*. 基础结构,基础设施

retrieve [ri'tri:v] get or find back; recover the use of *v*. 取回

irrevocably [i'revəkəbli] in a way incapable of being retracted or revoked *adv*. 不能取消地

fraudulent ['frɔ:djulənt] intended to deceive *adj*. 欺诈的,不正的,不诚实的

Exercises

A. Fill in each blank with one of the given words in its correct form.

retrieve	identify	legitimate	consistent	token
insecure	fraudulent	irrevocable	decrypt	infrastructure

1. In the wild, New Caledonian crows use a range of tool types for extracting invertebrate prey from holes and crevices, and in captivity, they have been shown to make, or select, tools to _____ food rewards.
2. The result is that the resource, whether it is a website, an email server, or a database, cannot respond to _____ traffic in a timely manner and so essentially becomes unavailable to users.
3. The study, authored by a professor at the Rotman School of Management at the University of Toronto and his collaborator at Northwestern University, calls such individuals " _____ contributors", people who contribute all the time, regardless of others' choices.
4. At any given time, as many as 18 percent of those surveyed felt _____ about their jobs. But only about 5 percent of respondents in the first survey and 3 percent of respondents in the second survey reported feeling anxious about their jobs both times they were interviewed.
5. The agencies are also advising operators of offending web sites that they must take prompt action to correct and/or remove promotions of these _____ products or face enforcement action.
6. A number of prominent politicians, including Sen. Edward Kennedy, who wrote a foreword for her earlier book on school _____, strongly support efforts to fund much-needed school repairs, remodeling and rebuilding.
7. For instance, during a concert, when the sound of the crowd mixes with several instruments, our brain

can still _____ the specific notes played by the trumpet, the violin or any other instrument in the orchestra.

8. In one study, a control group asked to do a favor without compensation was significantly more willing to help move a sofa than those offered a _____ payment.
9. Cancer is primarily caused by _____ alterations to genes, called mutations.
10. Modern cryptography relies on the use of digital "keys" to encrypt data before sending it over a network, and to _____ it at the other end.

B. Skim the text and then answer the following questions.

1. What is BioVault?
2. Why must message be encrypted if a person wants to send message to another over an unsecured network?
3. Why is biometric system asymmetric?
4. Is it possible for two persons to share biometric tokens to encrypt and decrypt their data without their biometrics being intercepted?
5. What can be used to ensure cybersecurity?

C. Read the text and choose the correct answer to each of the following questions.

1. Which feature of authentication does encryption rely on? _____.
   A. The user's PIN matching that stored to lock or unlock data
   B. The user's PIN changing dynamically
   C. The authentication being asymmetric to work
   D. The user's PIN matching the password of the computer
2. One way to avoid users having to remember endless, complicated passwords is to use the following except _____.
   A. fingerprints B. iris pattern C. hand recognition D. face recognition
3. In order for the encryption algorithm to provide cipher text that is random, _____ must be provided.
   A. a secret key B. biometric token C. a secret message D. a password
4. The fact that each biometric key (data) is unique means that the BioVault system can _____.
   A. revocably identify users B. irrevocably authenticate users
   C. detect fraudulent use of passwords D. detect biometric keys
5. Biometrics cannot help people to _____.
   A. use fingerprints to encrypt and decrypt data
   B. digitally sign electronic documents
   C. log in with incorrect password

D. authenticate users directly

D. Explain the underlined parts.

1. If a user, a web customer say, wishes to send a message or other data to another user, an online shop, over an unsecured network, the message must be encrypted to avoid interception of sensitive information such as passwords and credit card information.
2. Encryption relies on authentication being symmetric to work.
3. However, biometrics is not a symmetric process. The initial recording of biometric data samples only a limited amount of the information, the pigment patter in one's iris, for instance.
4. The close enough aspect of biometrics does not make biometrics insecure, provided that the closeness is very precise, but it does mean that biometric tokens cannot be used to create a secret key for an encryption algorithm.
5. Bobby Tait and Basie von Solms of the University of Johannesburg, Gauteng, South Africa, explain how biometrics can nevertheless be used to make a consistent secret key for encryption.
6. Aside from the asymmetry in biometrics, this approach will not work because Alice and Bill cannot provide the same biometric token to encrypt and decrypt the message.
7. The fact that each biometric key (data) is unique means that the BioVault system can irrevocably identify and authenticate users through their biometric keys (data) and detect fraudulent use of biometric keys.
8. Alice identifies herself to the authentication server, and indicates that she wants to send an encrypted message to Bill and requests Bill's biometric key from the server.
9. Bill receives the message sent by Alice, and decrypts the message by testing the biometric keys in his database against the received cipher text.
10. "Biometrics authenticates the user directly—this was one of the drivers behind the BioVault development."

E. Read the passages in this section and decide whether each of the following statements is true or false.

Passage One

Ethical hacking is a white hat technique, wherein the hacker breaches the security of a computer system or the network, to expose the security systems vulnerability. A career in ethical hacking, as a consultant, has bright prospects considering the dependence of the entire world on computer technology, and easy access to world wide web.

What is Ethical Hacking?

In ethical hacking, the hacker identifies the weakness in the system, but instead of taking advantage of the situation, alerts the owner, so that the later can fix the problem and make his system secured. The

ethical hacker can convey the message to the owner by various means ranging from a simple phone call to leaving an electronic card in the system, as an obvious signal that the system was breached. Ethical hackers use the same tools as hackers do, but they are not a threat to the system. Some people do ethical hacking as a hobby, while some pursue it as their career.

Basic Requirements to Become an Ethical Hacker

The ethical hacker has to posses excellent programming and networking skills, as well as good working knowledge of various operating systems. All these skills should be backed up with the knowledge of necessary hardware and software. More importantly a certified ethical hacking or cyber security course is the basic requirement to become an ethical hacker. Ethical hacking is not a process which can be executed with a snap of the finger, being patient is the important key, especially in ethical hacking for beginners. In some cases, you may have to monitor the system for days or weeks to get a single opportunity to hit the jackpot.

(http://www.buzzle.com/articles/ethical-hacking-for-beginners.html)

_____ 1. In ethical hacking, the hacker identifies the weakness in the system, and takes advantage of the situation.

_____ 2. Ethical hackers and hackers use different tools.

_____ 3. Ethical hacking is not an easy process, and being patient is the important key, especially in ethical hacking for beginners.

Passage Two

We live in an Internet age. Socializing is extremely easy today. Communicating to people around the world is a matter of a few clicks on the Internet. The Internet has facilitated an easy access to information across the globe, thus making life easy. However, if you look at this Internet age from a different point of view, you will realize that it has in fact bred many illegal and unethical practices. While some use the Internet for gaining information, others use it for destruction of sensitive data. While some use the web as a communication platform, others derive pleasure from intruding in the Internet privacy of individuals and seek enjoyment from breaching Internet security. Cyber-bullying is one such activity that this section of Internet users indulge in. Let us find more about this unethical Internet practice, cyber bullying.

Cyber Bullying—An Introduction

Cyber bullying is the act of threatening, harassing or humiliating a person through use of Internet or any other digital interactive media. Targeting a person by means of emails, text messages or online postings is also referred to as cyber bullying. Teens are often seen falling prey to online bullying practices. Some of them might indulge in practices like sending online messages to cell phones with intention to hurt or embarrass the receiver.

Cyber bullying is not just associated with children and youngsters. It is also observed in adults and

is referred to as cyberharassment. Cyber bullying practices range from simple activities like continuously bombarding someone with emails right up to sexual abuse by means of the Internet. Passing abusive remarks about someone, making him/her a subject of ridicule in online forums and spreading gossip or rumors about him/her are also classified under the category of cyber bullying practices.

Cyber bullying is of two types, namely direct or through a proxy. Direct attacks often involve the use of instant messengers and emails to humiliate individuals. Sending vulgar photographs through emails or uploading them on blogs and social networking sites is a form cyber bullying through direct attacks. Sending junk mails or spams and spreading malicious code by means of emails are some other examples of direct cyber bullying. When cyber bullying practices take place without the knowledge of the person being used as a bully, it is said to take place through a proxy. At times, warnings and "click here" messages can be deceptive. They may be programmed to send wrong information to the Internet service providers, thereby resulting in a legal action against the user clicking on these warnings or messages. In cyber bullying through a proxy, the cyber bullies victimize benign users by committing Internet crimes in their name.

(www.buzzle.com/articles/cyber-bullying.html)

_____ 4. Cyber-bullying is an activity in which people can derive pleasure from intruding in the Internet privacy of individuals and seek enjoyment from breaching Internet security.

_____ 5. Targeting a person by means of emails, text messages or online postings is not cyber-bullying.

_____ 6. Sending vulgar photographs through emails or uploading them on blogs and social networking sites is a direct form of cyber bullying.

Passage Three

Spyware is a hidden software program. It is often used to monitor the browsing and shopping habits of computer users. Spyware can also be a remote control program that steals confidential banking and personal information.

Spyware has quickly become the most prominent internet security problem. According to the National Cyber Security Alliance, spyware infects more than 90% of home PCs. Recent survey shows that spyware is also sneaking into the network of corporate computers.

Spyware is often coupled with free downloads, such as free music, game and software downloads. Spyware may slow down computer, hijack homepage and create uncontrolled pop-up advertisements. Some spyware programs can remain unnoticed, secretly gathering information from the computer. Once installed, spyware is difficult to remove without the help of dedicated antispyware software.

Due to the rise of spyware activity, antispyware software are in great demand these days. But are these spyware removal tools the same? Do they provide what the security consumers need?

There are many reports that some antispyware programs installed their own spyware and adware to the

computer. One consumer was quoted saying: "It's a rip-off. I downloaded the free trial of an antispyware program, only to find out that it added its own adware to my computer." Other consumers have complained that the antispyware program they use cannot detect all spyware programs. Some even slow down the computer and create pop-up advertisements.

There are a few good antispyware programs in the market today. On the other hand, dozens of spyware removal programs are blacklisted by consumers. Beware of spyware removal tools that are heavily promoted by e-mail campaigns. Never run any free downloads and free scans from unknown software publishers. Their programs may as well be spyware programs themselves. Read independent product reviews from renowned computer magazines or reputable sources. Spending some extra time in research can save you a lot of hassles in the long run.

(http://www.buzzle.com/editorials/6-1-2006-97948.asp)

_____ 7. According to the National Cyber Security Alliance, spyware infects 90% of home PCs.

_____ 8. Download free music or free game may create uncontrolled pop-up advertisements.

_____ 9. Antispyware does not introduce adware or slow down the computer.

_____ 10. Dozens of spyware removal programs are blacklisted by organizations.

F. Cloze. Fill in each blank with one suitable word.

Hackers have developed increasingly __1__ means of tampering with the Web, including __2__ or pirating critical software applications in both public and private sectors of business. Traditional security measures have protected software only by using __3__ activities such as encrypting files or hiding programs behind firewalls and security perimeters. The problem with passive approaches is that they provide just a single defense layer that experienced hackers can __4__ of quickly, leaving applications with no protection once that security level is __5__.

The Internet obviously has opened up new markets and business opportunities, but it has also provided for the rapid dissemination of malware, different types of viruses, and compromised applications that can bring business to a __6__. With companies increasing global distributions and online sales, and increasing numbers of businesses conducting operations online, the risk to transactions and software is growing __7__. __8__ the perimeter of a network, application, or system is no longer sufficient in today's distributed computing environment. To safeguard their __9__ property, companies need to adopt new approaches that __10__ security directly into software and data.

1. A. sophisticated	B. complex	C. compound	D. delicate
2. A. defecting	B. infecting	C. affecting	D. effecting
3. A. passive	B. active	C. positive	D. negative
4. A. remove	B. displace	C. dispose	D. destroy

5. A. broken	B. exceeded	C. retained	D. breached
6. A. halt	B. stop	C. termination	D. setback
7. A. slightly	B. gradually	C. exponentially	D. suddenly
8. A. Securing	B. Sustaining	C. Overcoming	D. Maintaining
9. A. intellect	B. intellectual	C. intelligent	D. intellective
10. A. involve	B. engage	C. integrate	D. unite

G. Translate the following passages into Chinese/English.

1. SearchWiki is a tough sell because most of us are already trained to surf the Web quickly, skipping ahead and back through links without taking the time to rank those results or comment on them. And it only works with Google searches. If you like the idea of more personalized Web searches but would like to use other search engines or don't want to do extra work, you might like Surf Canyon. Once downloaded, this tool displays bull's - eyes beside certain results to show that Surf Canyon has found additional related hits. Clicking on this bull's - eye reveals those suggested links, pulled from deeper down in the search results, and these links might have bull's - eyes of their own. This cascade of data goes on and on as an algorithm studies which of the returned results you do or don't choose.

2. Surf Canyon 最近针对那些希望长期享受个性化服务的用户推出了一款软件包，在 my.surfcanyon.com 上可以查到。借助它，用户可以挑选出一些喜欢的网站并从中接收新闻、购物、研究或体育和娱乐搜索结果。用户还可以在这个网页的可用网址名单上加入没有列入其中的自己喜欢的网址；同样也可以将不喜欢的网址加入黑名单，这样就不会有来自此类网站的搜索结果了。跟谷歌不同，Surf Canyon 不会保存你的历史记录或搜索偏好。如果你没有使用上述提及的那个链接建立起个人偏好记录，它就会完全依据你的即时操作——比如当你优先选择了某个而不是另一个链接时——作出反应。

Text B

New Chip Brings Military Security to Commercial Processors [Abridged]

1. Last week, a spot check of electric grid systems revealed that hackers had infiltrated the U.S. electric grid. The government inspections, motivated by a 2007 Idaho National Laboratory demonstration of the vulnerabilities of the U.S. grid, revealed more than the inspectors had bargained for: The invaders had left behind potentially disruptive malware. The increasing threat from better-financed hackers, the growing need to build security into a chip at the start of the chip-design process (rather than as an afterthought), and the blurring line between military and civilian targets have been at the center of many

U.S. Department of Defense concerns. The mounting hysteria has led the government to pour millions into the problem, and on 1 April, Congress introduced a bill that would let the president declare a "cybersecurity emergency", shutting down Web traffic to compromised infrastructure such as the power grid.

2. But the answer could be found in something decidedly less grandiose: Last month, Pleasanton, Calif. based CPU Tech introduced into the commercial market a secure processor that had previously been available only for military systems. The Acalis CPU872 is the first microprocessor born of new methods the Pentagon learned from its hunt for secret kill switches in the commercial chips the agency buys. But beyond just defense contractors, CPU Tech is targeting commercial users of PowerPC processors at big firms and agencies including those responsible for securing public infrastructure, such as electric power generators and subway systems.

3. CPU Tech vice president Pat Hays says the Acalis CPU872 has three features that other secure processors don't: First, instead of being integrated on the same board with the processor or functioning as a coprocessor like a graphics-processing unit, the Acalis puts the security muscle in the same chip with the processor. Second, each chip is manufactured at a trusted foundry certified by the U.S. Department of Defense. Finally, the security key —the "secret handshake" that secure chips create to make sure trusted sources can gain access and other sources can't—is generated on the chip in a way that thwarts two of the most common attacks on secure systems.

4. "We made sure a chip would be protected from people like us," says Hays, referring to CPU Tech's other business—reverse-engineering chips for military contractors. As a subcontractor on Trust in Integrated Circuits, a program of the Defense Advanced Research Projects Agency (DARPA), CPU Tech gleaned knowledge that it applied to the design of the CPU872 processor. "Our work, in fact, laid the groundwork for TIIC," says CPU Tech founder Ed King.

5. By necessity, the U.S. military uses many commercial off-the-shelf chips manufactured outside the United States because of a shifting integrated-circuits industry. Security experts have written extensively about the risk this creates for the country's national security, as malicious hardware and software modifications can theoretically be introduced during the manufacturing process. But the line between military and civilian targets has blurred significantly in the United States as well as in other Western countries. Hacking into civilian infrastructure could lay the groundwork for organized, government-coordinated warfare. This goes beyond conspiracy theory: A September 2008 Idaho National Laboratory report found a link between the Russian attack on Georgia and a preceding wave of malicious cyberactivity, primarily distributed denial-of-service (DDoS) attacks. Even off-line structures are vulnerable to online sabotage. The same study established the alarming feasibility of gaining access remotely to electricity generators that are commonly thought to be immune to online threats.

6. Hays says the chip's onshore pedigree reduces the risk of Trojan horses being built into the hard-

ware during the manufacturing process. The 90-nanometer processor is fabricated at IBM's Fishkill, N. Y., foundry—a trusted foundry—which goes through an exhaustive vetting process to be deemed secure enough to manufacture the U.S. military's specialty chips, with security features built directly into the hardware.

7. But despite the built-in security, Hays, who was in Bell Labs' digital signal processing division in the 1980s, says the Acalis chip won't divulge its secrets, even if it's reverse-engineered down to the mask layer. This is to prevent physical scrutiny if a chip falls into the wrong hands. Military experts have speculated that billions of dollars in U.S. military R&D were compromised. CPU Tech anticipates a similar fate for the secure processors it releases into the commercial world. Buying or even stealing a server is much easier than bringing down a spy plane. "We understand the chip itself will find its way to an untrusted source through distribution channels," says Hays, so the chip was designed to be useless if it were to be physically reverse-engineered. Nothing can be gleaned from the hardware, which can be securely configured to work only in concert with CPU Tech's proprietary security software. "We'll be a lot more restrictive about handing out the software that makes it work," says Hays.

8. But reverse-engineering a physical chip is not the only way to break in or create countermeasures. To eavesdrop on communications or impersonate a genuine user, a malefactor needs only decipher the secret encryption key.

9. "Getting the key is the key, so to speak, to being able to generate encrypted data," says David Blaauw, an electrical engineering professor at the University of Michigan, in Ann Arbor.

10. The key is generated using the National Institute of Standards and Technology's Advanced Encryption Standard (AES) algorithm, certified by the National Security Agency. AES algebra is very secure. "But when the key comes out of its cave to do its job once in a while," says Hays, "that's when the key is most vulnerable." Another way of getting the key is a so-called DRAM attack, in which a malefactor freezes the dynamic RAM to ferret out where the key has been temporarily stored. Cooling the DRAM after shutting off a computer can prolong a well-known property of DRAM called remanence—during which the key temporarily remains in memory—for several minutes, giving attackers an ample window to get into the DRAM and extract the key. "Basic disk encryption is very vulnerable," says Hays. "Wherever you put the key, on a chip or in DRAM, the smart bad actor will find a way to get it."

11. The hardware and software of the Acalis chip, Hays says, makes both of these methods impossible for two reasons: For one, the key can be changed at will. The system allows the owner to change the key every day or during every session to guard against side channel attacks. "If you change the key often enough, by the time you figure out the key, it's already irrelevant," says Hays. "There would be no chance to find it in time."

12. Further, instead of depending on secrecy, the system merely ensures that there is no key to be