PRICEWATERHOUSECOOPERS

Issue 3

CCE Journal

Cryptographic Centre of Excellence

Information Assurance Advisory Council

Creating Trusted Partnerships for the Information Society

The IAAC is a private sector-led forum in which Industry and Government are working together to secure the nation's information infrastructure.

IAAC is a membership only organisation with strict membership criteria. Membership of IAAC provides:

- Information & research – often critical, always valuable
- Awareness raising and education
- Unique peer group networking
- Relevant seminars and symposia led by key experts
- Working Groups progressing crucial areas of Information Assurance policy
- Direct contact opportunities between Members and with the Board
- Input into national and international policy for protection of critical information infrastructures

If you wish to apply for membership, visit www.iaac.ac.uk or send for details from:

Information Assurance Advisory Council
King's College London,
Strand Bridge House, 138 - 142 Strand
London WC2R 2LS
United Kingdom
t: +44 (0)20 7848-1395

Sponsors include:

CESG

SYMANTEC.

CABINET OFFICE

BAE SYSTEMS

BT

THE POST OFFICE

PRICEWATERHOUSECOOPERS

hp

Anite Government Systems

ICSA

DEFENSE

November 2000

CCE Journal

Cryptographic Centre of Excellence

The PricewaterhouseCoopers Cryptographic Centre of Excellence (CCE) was formed by the company's Global Risk Management Solutions practice in order to unite members from around the globe with unique expertise in cryptography and cryptographic services. This was done to build a network of highly skilled professionals who could assist clients and one another throughout an engagement's lifecycle. By establishing relationships with academic institutions, leading security vendors, cryptographic research organisations and leading cryptographers, we are in a truly unique position to offer our global clients the best solutions for their cryptographic security needs.

Global Risk Management Solutions, part of PricewaterhouseCoopers, has over 5,000 professionals worldwide, many of them industry specialists, and offers a comprehensive identification of risks, whether they are strategic, financial or operational in nature. Our solutions-based risk identification and analysis offers guidance on industry best practices and common training programmes, using state-of-the-art methodologies and tools consistently.

By addressing the changing needs of today's business leaders, we are able to help organisations identify, assess and manage complex issues and risks across the whole enterprise – or within in any part of it – whether they are strategic, financial or operational in nature. We help clients to develop risk management solutions that minimise hazard, resolve uncertainty and maximise opportunity.

Contact Information

Dr. Alastair MacWillson

Partner in PricewaterhouseCoopers London and global leader for Technology Risk Services within the PricewaterhouseCoopers Global Risk Management Solutions practice

alastair.macwillson@uk.pwcglobal.com

Geoffrey C. Grabow CISSP

Americas Leader – PricewaterhouseCoopers Cryptographic Centre of Excellence

geoffrey.c.grabow@us.pwcglobal.com

John Velissarios M.Comp.Sci.

EMEA Leader – PricewaterhouseCoopers Cryptographic Centre of Excellence

john.velissarios@uk.pwcglobal.com

Stephen G. Wilson BSc. BE Elec (Hons)

Asia Pacific Leader – PricewaterhouseCoopers Cryptographic Centre of Excellence

stephen.g.wilson@au.pwcglobal.com

More information and previous editions of the Journal can be found at:

www.pwcglobal.com/cce

The views expressed in this publication are not necessarily the views of PricewaterhouseCoopers.

To SUBSCRIBE to CipherText, our weekly e-mail cryptographic newsletter, go to http://www.pwcglobal.com/cce or http://cce.external.listbot.com and follow the subscription instructions, or send an e-mail to: cce.external-subscribe@listbot.com

In this Issue

Editor's Soapbox 3
by Geoffrey C. Grabow CISSP

Charge of the CyberSabres 5
by N. MacDonnell Ulsch, PricewaterhouseCoopers

Attribute Certificates and their Limitations 8
by Stephen Wilson, Director, beTRUSTed, Asia Pacific

Building Partnerships for Secure E-business 10
by Dr Andrew Rathmell, Chairman, Information Assurance Advisory Council

Security in E-business: Obstacle or Key to Success 18
by Frank Heinzmann, PricewaterhouseCoopers

Roaring Twenties ... Roaring Internet 21
by Peter Taffae, President and CEO, e-perils.com™

Securing E-business with Practical PKI 24
by Dominic Storey, Director of Technology, RSA Security Inc

Upcoming Conferences 30

Editor's Soapbox

Root Certificates in Browsers – A Leap of Faith?

by Geoffrey C. Grabow CISSP

Whenever you download the latest version of a browser from Netscape, Microsoft or any other vendor, you are taking a leap of faith with all of your future security. This is because the browser contains within it a series of public keys from a variety of Certificate Authorities (CA). These keys allow the browser to exchange information with a web site and allow a secure session to be established.

When visiting a web site with the intention of entering some personal information such as your home address or credit card number, users are being trained to look for the lock on the browser. If the lock icon is showing (Microsoft) or shows a locked lock instead of an open one (Netscape) the user is to believe that their data entries are safe from prying eyes. However, that may not be the case.

The protocol involved in establishing a secure session between your browser and the web server to which you are connecting relies on the public keys loaded in your browser. If your browser has the GeoffCo CA Public Key loaded, and you visit a web site with a digital certificate signed by GeoffCo's CA, the secure session is established … but how did the GeoffCo Public Key get into your browser? Most people download their browser from the Internet, and trust that the contents of the .exe or .zip file are exactly as intended. If, however, someone has tampered with the browser in some way, or substituted the valid public keys with their own, we are now faced with a very powerful man-in-the-middle attack.

This attack will potentially let an attacker see everything you enter on a 'secure' site and simultaneously let you think that everything is working as it should.

This problem exists because it is a standard security practice to verify information of this sort 'out of band'. Meaning that you cannot simply trust the list of public keys in a download file, but rather, you must validate them via some means other than the one you acquired with the browser in the first place. Therefore, if you download your browser from the Internet, you cannot use information from the Internet to verify its contents. You must find a way to verify the keys by phone, fax, newspaper, etc.

Fortunately, there is a relatively simple method for accomplishing this task. When you examine the certificate details, one of the detail fields is called the 'Fingerprint'. This is the MD5 or SHA-1 hash of the certificate. So, in the case of GeoffCo's CA, when you get your browser you MUST get the hash from a source other than

the Internet and compare it to the value displayed in the certificate details.

Using this method also allows you to load certificates into your browser that were not preloaded for you. You can go to the GeoffCo web site and click a link that will cause the GeoffCo CA's certificate to be loaded. When that happens, the browser displays one (or both) of the hash values which you must then compare to a value you found in the newspaper, on a GeoffCo business card, etc. This method lets you load those certificates of the companies you personally choose to trust, not simply those chosen by the browser company.

Another consideration is that this problem doesn't affect only browsers. All applications that are Public Key Infrastructure (PKI) aware encounter this problem.

You must choose with whom you wish to do business, and which companies deserve your trust. Don't simply rely on that little lock icon to tell you if you're safe or not. Trust must be established by you and verified by you.

Comments on this topic are welcome and may be submitted to the CCE Journal via e-mail using the contact information at the beginning of this issue.

About the author

Geoffrey is the Americas leader of the PricewaterhouseCoopers Cryptographic Centre of Excellence, editor of the CCE Journal and CTO of beTRUSTed.

Charge of the CyberSabres

The Emerging Threat of the E-terrorist

by N. MacDonnell Ulsch, PricewaterhouseCoopers

"Mutual dependence and the interconnectedness made possible by the information and communications infrastructure lead to the possibility that our infrastructures may be vulnerable in a way they never have been before. Intentional exploitation of these new vulnerabilities could have severe consequences for our economy, security and way of life. A false or malicious computer message can traverse multiple national borders, leaping from jurisdiction to jurisdiction to avoid identification, complicate lawful pursuit, or escape retribution. If we fail to take strong action, then terrorists, criminals, and hostile regimes could invade and paralyze these vital systems, disrupting commerce, threatening health, weakening our capacity to function in a crisis."

President Bill Clinton

The financial services industry, part of US critical infrastructure, makes an attractive terrorist target.

The Internet has been called a breakthrough technology comparable to the automobile or the television, something that fundamentally changes business, government and individual life styles. That's all for the good. But the Internet also leaves the United States dangerously vulnerable to electronic terrorism. With half of the world's computer capacity and more than 60 percent of Internet assets, the US is the most advanced and most dependent user of information technology in the world. But as the 'Net' insinuates itself into all parts of American life, it gives adversaries a tunnel through which they can damage the soft underbelly of the country's emerging technologies.

That the Internet has become the Achilles heel of the US electronic infrastructure is both ironic and predictable. Ironic because American military scientists created the network to preserve a communication channel in the event of a nuclear holocaust. Predictable because the Internet is inherently insecure, a web of connections that link the lowliest laptop to just about any government agency or mom-and-pop business worthy of an e-mail address.

No segment of American life is more vulnerable to electronic terrorism than financial services companies. These institutions are at risk for the same reason banks have always been at risk: that's where the money is. They have also grown increasingly dependent on technology, using it to process funds, conduct transactions and communicate with customers and shareholders. But most financial service companies do not really understand the risks emanating from internal or external hackers or other saboteurs.

An attack can come from anywhere on the globe, and as more and more money flows through electronic channels of commerce, the risks intensify. All transactions occur over a network through databases. If terrorists decide they want to disrupt activities in the US, the banking system is a fine place to start. "Even if the terrorists don't shut down a bank, just by going in and manipulating data causes depositors to lose faith in the banking system," says Frank J. Cilluffo, Task Force Director of the Center for Strategic and International Studies (CSIS). "Confidence in the financial systems is a given in the eyes of the American public. That confidence could be shattered very easily, and I think that's a major concern."

Confidence is not all that can be shattered. Consider that for every $1 million stolen electronically from a financial or investment institution, the recovery cost is more than $100 million. That includes costs for forensic investigations, crisis management, litigation and lost customers.

As the millennium ends, some experts have already conjured apocalyptic high-tech scenarios, with the mushroom cloud replaced by a 'data error' message on an ATM machine. "A terrorist organization can devastate the United States by throwing a wrench into the financial system," says Tom Noonan, President and CEO of Internet Security Systems. "If a terrorist takes out a power grid in the Northeast and all of its banking and services along with it, investors may wonder: 'Is it going to happen again next month? Is it going to happen while my money is being transferred? Am I going to lose my savings?' That kind of erosion of confidence, I think, is much more devastating than just the incident."

The federal government has issued directives to promote cooperation between the private sector and the government, but frankly, these efforts have fallen short. Industry complains that the FBI, for example, "is reluctant to release information and seems mainly interested in having industry provide it intelligence," says Cilluffo. "The private sector will need to assume much of the responsibility for protecting itself. Government can help in specific, but limited ways."

There is no perfect defense against hackers, and whenever new intrusion techniques are discovered, new defensive measures will have to be invented. President Clinton's Commission on Critical Infrastructure Protection acknowledges the need for new ways to detect malicious infiltration into the electronic infrastructure from both internal and external sources. Without the proper technology tools to defeat intruders, the Commission concluded, 'it is conceivable that an orchestrated attack against US infrastructures could be underway for some time before it is recognized as such.' In fact, it is frightening to think that, as the Commission reported, 'It sometimes takes months, even years, to determine the significance of individual computer attacks.'

The financial and investment community must take immediate action to remain secure in the face of an increasingly diverse and sophisticated range of volatile threats – internal, external, global. While technology enables the expansion of our electronic business horizons, it also emboldens high-tech rogues. Information-security threats are complex, and so are solutions. But there are solutions, and every solution begins with awareness.

Global Technology Trends

Category	1981	1996	2002
Personal Computers	Thousands	400 Million	500 Million
Local Area Networks	Thousands	1.3 Million	2.5 Million
Wide Area Networks	Hundreds	Thousands	Tens of Thousands
Computer Viruses	Some	Thousands	Tens of Thousands
Internet Devices Accessing www	None	32 Million	300 Million
Population With Skills for Cyber Attacks	Thousands	17 Million	19 Million
Telecom Systems Control Software Specialist*	Few	1.1 Million	1.3 Million

Source: International Data Corporation

* Skills to take down or disrupt the public communications network

Department of Defense Assessment of Information Warfare Threat

Threats	Validated existence	Existence likely but not validated	Likely by 2005	Likely after 2005
Incompetent	Widespread			
Hacker	Widespread			
Disgruntled employee	Widespread			
Crook	Widespread			
Organized Crime	Likely		Widespread	
Political Dissident		Widespread		
Terrorist Group		Likely	Widespread	
Foreign Espionage	Likely		Widespread	
Tactical Countermeasures		Widespread		
Orchestrated Tactical IW			Likely	Widespread
Major Strategic Disruption				Likely

Source: The Center for Strategic & International Studies

About the author

N. MacDonnell Ulsch is in the Technology Risk Services practice of PricewaterhouseCoopers LLP in Boston. He served as Trusted Advisor to the Moynihan Commission on Secrecy. He can be reached at don.ulsch@us.pwcglobal.com or by telephone at +1 (617) 478 5171.

Attribute Certificates and their Limitations

by Stephen Wilson, Director, beTRUSTed, Asia Pacific

Attribute certificates are in vogue amongst some vendors and pundits, for conveying business credentials, independent from the holder's identity certificate. They are a new technology, supported by a handful of Certificate Authority (CA) vendors and only recently covered by the latest version of the X.509 digital certificate standard. They ought to be approached with caution on this basis alone. But more fundamentally, users should consider that 'identity' naturally comes in different guises, and should not be separated so strictly from 'attributes'. Traditional 'identity' certificates are in fact a powerful means for conveying business credentials in most e-business applications.

Identity need not be burdensome

It is often assumed that registering for identity certificates must be more complex and costly than it is for Attribute Certificates. This is because most certificate schemes today carry a burden of proof of personal identity, which can be traced back to the original notion of the digital certificate as an 'electronic passport'. This metaphor has moulded the way we conceive of identity in e-business and has led to a de facto burden of proof that is much higher than it is in the paper world.

Rather than adopt passport-level standards, there is no reason why a CA cannot design and enforce the minimum set of identification rules fit for the purpose of the certificates it issues. For example, ordinarily there would be no reason for buyers and sellers in a procurement system, to be enrolled on the basis of their passport or drivers license. Likewise, digital certificates in an e-procurement system should be issued specifically on the basis of the participant's roles and responsibilities.

Identity in context

There is no reason to restrict 'identity' certificates to asserting personal organic identity, as opposed to business identity in the context of specified types of transaction. For example, in everyday life we are accustomed to thinking of one's identity *'as a lawyer'*, separate from one's identity *'as an employee'* of ACME Inc, or one's identity *'as a citizen'*.

At the same time, it might be better to conceptualise 'identity' certificates as representing membership. An X.509 certificate represents the fact that its subject has met certain conditions laid down in the Certification Practice Statement and/or Certificate Policy. These conditions can relate

to the business rules of a community of interest and need not relate strongly to the subject's personal organic identity at all.

Where Attribute Certificates do fit

For closed communities and short term credentials, Attribute Certificates have definite advantages, especially for access control where a discrete signature is not required. The classic examples are temporary network access privileges and electronic letters of credit. Short lived Attribute Certificates do not need to be revoked, as they quickly lapse of their own accord, and so they eliminate the overhead of revocation management and checking.

Of course, if the natural lifetime of the credential is long, as it is with professional qualifications, trading partnerships, government-to-business relationships and so on, then the burden of managing revocation is unavoidable.

How do you trust an Attribute Authority?

Attribute Certificates also run into difficulties in open communities. If a relying party has no prior relationship with the Attribute Authority (AA), then they will need a third party to vouch for the AA. Technically, the relying party has to validate the AA's digital signature on the Attribute Certificate. The AA must have a CA, and the relying party needs the means to be able to accept that CA. In an open community, there is no necessary connection between the CA that issued your identity certificate and the CA which certified your AA, and this will lead to double certificate chains in order to validate the credential represented by an Attribute Certificate.

Implementation and support issues

At present, Attribute technology remains immature. Attribute Authority systems and Attribute Certificate toolkits are available in beta from a few specialist vendors but have yet to appear in mainstream Internet products. There are few if any client side applications in production.

A further practical problem is that broad rollout of Attribute Certificates is premised upon the availability of a general purpose (and high grade) Identity Certificate, yet no such option has emerged, let alone reached critical mass. All deployments of Attribute Certificates today must therefore take on the issuance of public key certificates as well, which begs the question: Why not simply use those public key certificates alone?

The Australian National Office for the Information Economy (NOIE) reached a similar conclusion in its recent paper *'Who Should Authorise and Use ABN-DSCs[1] in Businesses?'* (see www.ogo.gov.au/projects/publickey/ABN-DSCdiscussionpaper4.htm). NOIE wrote that 'Attribute certificates are not available or supportable for the foreseeable future, and the current priority for government is to develop support for identity certificates such as the ABN-DSC'.

Conclusion

Attribute Certificates bring fundamental costs and complexities, especially in open communities. While useful for representing short lived credentials, where the overhead of revocation can be avoided, Attribute Certificates are not particularly advantageous for managing longer term qualifications. In most cases, a conventional X.509 'identity' certificate can provide powerful and flexible proof of identity in the context of the application, especially if the issuer can customise the registration process and certificate profile to fit the application and reflect the intended purpose.

About the author

Stephen is the Asia Pacific leader of the PricewaterhouseCoopers Cryptographic Centre of Excellence and a Director of beTRUSTed Asia Pacific.

He can be contacted at stephen.g.wilson@au.pwcglobal.com

[1] ABN-DSC stands for 'Australian Business Number Digital Signature Certificate' and is an initiative of the Australian Government to introduce a general purpose business identity certificate.

Building Partnerships for Secure E-business[1]

by Dr Andrew Rathmell
Chairman, Information Assurance Advisory Council[2]

It is becoming ever more evident that e-business and the Information Society will not progress unless they are built on secure foundations. The dependability and robustness of large scale networked information systems is already a cause for concern but the rapid growth of e-business and e-government, which are critically dependent on these infrastructures, has placed trustworthiness firmly onto the corporate and political agenda.

However, devising policies to protect critical information infrastructures will require new modes of partnership across sectors and across borders. Ways need to be found of engaging all stakeholders and encouraging them to work together to secure information infrastructures through enlightened self interest.

This paper explores the requirements of partnership, in the hope that an understanding of the issues can help stakeholders in the Information Society to better protect themselves and their logical neighbours.

Rising Security Concerns

As businesses, governments and citizens around the globe rush to join the networking revolution, awareness is growing of the security implications of the new technological and market environment. Both dot.coms and blue chip bricks and mortar corporations are finding their reputations and share prices increasingly reliant on the dependability and security of their critical information infrastructures[3]. Widely publicised security fears are already acting as a brake on the growth of e-business and take up of e-government. As a survey of British consumers by the National Consumer Council concluded in August 2000, 'unless the total online shopping environment … is made more secure, some consumers will never have the confidence to explore the opportunities[4].'

These security concerns are also being taken seriously by governments. Around the world, states are determined not only to promote e-business and e-government but also to forestall more serious damage to their societies by structured cyber-attackers such as terrorists or nation states. International organisations such as the G-8, EU and UN are also starting to address the issues of cyber-crime, infrastructure dependability and Information Operations.

However, all efforts by governments and corporations to develop protective policies run into a number of common problems. A particularly pressing one is that of building effective inter-sectoral relationships. The need for public-private partnerships and

collaboration across industry sectors has been recognised by policy makers across the globe but no single solution has yet been found. As highlighted by the confrontation between business and government in the UK during the recent passage of the Regulation of Investigatory Powers (RIP) Bill, a failure to develop policies in partnership can be harmful for both businesses and governments.

This paper discusses approaches to managing the problem of inter-sectoral relationships in a global business context.

Protecting Critical Infrastructures

There are two discrete but overlapping security problems that government and commerce face. First, ensuring that day-to-day e-business and e-government function reliably. On a routine basis, the infrastructures need to withstand 'normal' levels of misuse and abuse – from accidental outages to natural disasters, through electronic vandalism and criminal activity. Measures that are required include R&D and education programmes, enforcement of standards, insurance-based mechanisms, legislation on cryptography and authentication, cyber-policing and appropriate legal penalties for computer misuse.

Second, ensuring that key parts of National Information Infrastructures (NII) are protected against deliberate attack at a higher level, from foreign states, major terrorist campaigns or politically motivated activists. It is in response to this problem area that the concept of Critical Infrastructure Protection (CIP) has emerged.

CIP is not a new concept. In the era of industrial warfare, economic infrastructures have increasingly been targeted. These infrastructures were those deemed critical for national defence and for survival of the state and of key economic and political activities. Since World War I, Britain has identified critical infrastructures and protected these 'Key Points' and 'Economic Key Points.' Protection ranged from anti-aircraft defences in WWII, physical defences against Soviet special forces in the Cold War and defences against terrorism since the 1960s[5]. Government also developed systems of early warning and alerting, as well as of emergency planning and crisis management. Many of these mechanisms worked in partnership with private sector entities who either operated the infrastructures or who were dependent upon them.

New Problems

Compared to traditional problems, securing the NII poses a formidable challenge. There are five problem areas that are common to corporate leaders and government leaders alike.

The first is vulnerability analysis. As post-industrial society has grown more complex, so have the interdependencies amongst and between infrastructures. However, it is precisely these complex interdependencies that make economic and social infrastructures so vulnerable to disruption through the cumulative impact of attacks that are transmitted throughout the whole system[6]. Thus it is no longer enough for any single organisation to protect itself; its critical processes may be dependent on a chain of interconnected processes over which it has no control.

The second problem is to define the Critical National Infrastructure (CNI). At a national level, the problem is defining what sectors and processes are critical. This of course begs the question of 'critical to whom?' Defence establishments are focusing on assuring a Minimum Essential Defence Information Infrastructure[7]. The problem they have found is that they are increasingly reliant, even for their core war-fighting functions, on networks and systems outside their control.

The third problem is to assess and monitor the threat. Without a reliable assessment of the level and vector of the threat and of the direction and rate of change, it is impossible to assess the level and type of protection needed.

The fourth problem is the balance between security and liberty. In responding to conventional war, crime and terrorism, governments have always had to balance the needs of national security and public safety against the desire for civil liberties and personal freedoms. The networked age is posing this dilemma in an even more acute form, as illustrated by the debate over cryptography and the RIP Act in the UK.

The fifth problem area concerns co-ordination, control and influence. This goes to the heart of the difficulties that established government and industrial structures have in dealing with cyber-threats. The vertically integrated organisations that have evolved in most countries at the end of the 20th Century find it hard to cope with the cross-cutting and rapidly changing nature of cyber-threats. The mismatch is evident in three areas: intra-governmental; public-private; international.

Within government, the drive to embrace digitisation and connectivity has proceeded haphazardly but often with a strong central push. Security concerns have tended to emerge

initially from defence establishments and have, in some countries, come to the attention of central authorities such as the US National Security Council (NSC) or the Swedish cabinet. Even in countries where the central authority has recognised the issue, however, it is proving difficult to ensure an effective intra-government response.

The problem of ensuring private-sector buy-in to the concept of infrastructure defence is proving harder to resolve. Fortunately, there is some experience to build upon. Many governments have integrated key utilities into their civil emergency planning mechanisms and in many nations there are privileged relations between central government and 'strategic' industries that allow exchange of data on physical security threats[8]. Ensuring private sector buy-in to the development of CIP policies is proving more difficult for three key reasons.

First, deregulation and globalisation have meant that governments have much less control over, or even knowledge of, the owners and operators of information networks than was once the case. Second, the fiercely competitive nature of the emerging electronic marketplace means that private sector entities are more reluctant to work with government agencies. Third, in a wired society, the digital front line runs through every home and every office. In other words, in order to monitor all potential or actual cyber-threats, investigators may need to gather unprecedented amounts of data.

The problem of ensuring private-sector buy-in to the concept of infrastructure defence is proving harder to resolve.

The effort to involve the private sector in national infrastructure defences raises the issue of the international aspects of the problem. As numerous cracking cases have demonstrated, the global network of networks means that cyber-attacks pay little heed to international boundaries. Furthermore, as critical utilities become increasingly dependent on transnational networks and partners, vulnerabilities as well as threats become truly transnational.

The international policy aspects of CIP are proving extremely problematic for two reasons. The first relates to timing and bureaucratic gradualism. Most governments take the attitude that they need to put their own house in order before they begin inevitably complex discussions with foreign governments. The second is the desire to balance the conflicting demands of national security and intelligence against threats to economic wellbeing. The US exemplifies this dilemma. On the one hand, the investments that it has made in Information Operations and electronic intelligence gathering give it a global lead in the ability to exploit other nations' vulnerabilities. At the same time, though, the US's reliance on the global knowledge economy for its prosperity and the fact that it is a target for terrorists, provide an incentive for it to improve the trustworthiness of global networks.

The Need for Trusted Partnerships

Within the set of new problems for policy makers outlined above, one of the most difficult is the creation of trusted partnerships between sectors that historically have been suspicious of one another. Business worldwide has become used to operating in a deregulated environment and governments need to find ways of protecting their critical infrastructures without resorting to the heavy hand of regulation. At the same time, the emergence of a global information infrastructure underpinning a globalised, post-industrial economy, will necessitate a rethinking of traditional inter-state rivalries.

The problem is that information infrastructure dependencies, vulnerabilities and threats do not fit neatly into established institutional structures but rather sprawl messily across many of the vertically integrated political, social and economic structures with which we are familiar. This problem is not unique to CIP. For instance, transnational environmental issues have forced the development of international and transnational management mechanisms. However, in the field of CIP the mismatch between fluid, rapidly changing, horizontal and transnational risks and relatively inflexible, static, vertically integrated and nationally distinct management mechanisms is particularly striking.

This mismatch has led policymakers to recognise the urgent need to address cross-sectoral issues. US national policy has moved most publicly to identify this problem. The Clinton Administration has identified two, high level, components. First, the need for partnership between the public and private sectors to identify and respond to risks. Second, the need for multilateral co-operation. Other states are beginning to recognise these requirements, whilst globalised business sectors such as finance are sometimes ahead of national governments in promoting collaboration[9].

Nonetheless, the requirement to develop mechanisms for promoting trusted relationships between sectors remains urgent. In order to tease out the policy requirements, it is helpful to consider systematically which sectors need to be linked and on which themes there needs to be co-operation. These sectoral linkages and themes are summarised in Figure 1.

Sectoral Linkages

It is important to be clear about exactly what sectors need to be involved in this multi-dimensional domain. Public-private and international represent only two of the elements in this matrix. This paper identifies six sets of linkages that are priorities.

Pan-governmental: The first problem that policymakers have found in all states is in gaining recognition that CIP is a pan-governmental issue. It is not just an issue for the defence and intelligence communities, nor just a criminal justice or emergency planning issue. In an era of e-government, critical infrastructures can only be protected if all parts and all levels of government build effective Information Assurance into their business processes.

Inter-corporate: In the wider Internet economy there is a tension between corporate self-interest and competitive advantage. On the one hand, the speed of change and the need to seize customer share before on-line brand loyalties are established means that there is a premium on not revealing weaknesses. On the other hand, the fragility of the information infrastructures and of public trust in the new commercial paradigm means that failures of any one component can pose major risks to all others.

Trans-sectoral: Within certain commercial sectors, there is an established pattern of cooperation on security matters. For instance, the banking sector has in place a fairly effective process of dialogue and information exchange, likewise for the oil industry. However, in the Internet economy we are seeing the emergence of tight couplings across sectors that were previously loosely coupled. An obvious example is the increasingly close couplings between the telecommunications, finance and power sectors – failures in any one of which could have cascading impacts on the others. This growth in interdependency requires enhanced dialogue between sectors.

Public-private: Government and the private sector have a history of working together on security issues in a number of countries. In Britain, central government and 'List X' companies established trusted relationships during the Cold War. The terrorist threat also provided a basis for wider collaboration. While these experiences are useful, the Information Age has made this sort of cooperation much harder due to the reasons outlined above – privatisation, outsourcing, globalisation, deregulation, transnational ownership. In addition, the more fluid geo-political environment means that corporations often no longer share government perceptions of certain states as being 'threats' but rather see them as 'opportunities' and partners. Further, the balance of information power has shifted; government can no longer claim a monopoly on threat information – this information often resides in the private sector.

Public buy-in: One area that is often neglected when examining inter-sectoral relations is the need for public buy-in. Increasingly, the general public are crucial stakeholders in the Internet economy, whether as consumers, as suppliers of educated labour or as politically concerned citizens. There need to be balances between policies desired by governments and corporations that will ensure security and the civil liberty downsides perceived by citizens.

International/transnational: National security concerns will always set limits to co-operation in CIP but, as with corporations, there is scope for defining areas of common interest that outweigh narrow national interest. Superficially, this problem has close parallels to efforts to bolster international collaboration on transnational organised crime. Although CIP policies must address transnational cyber-crime, developing international and transnational responses will be even harder than in the purely criminal domain since CIP responses involve a broader set of actors.

Partnership Themes

Whichever set of trans-sectoral relationships one is dealing with, there are a number of issues on which collaboration and co-operation will be required. Although these themes apply to all of the sectoral relationships mentioned above, here they will be outlined in relation to public-private relationships in the national context.

Co-operation vs competition: The starting point for any co-operative venture is to define areas of common interest but also to be clear about areas of fundamental difference. In the public-private sphere this can only be achieved by an open dialogue between government and representatives of the private sector.

Co-development of policy: A central area in which co-operation will be mutually beneficial is the co-development of policy. The central

role played by the private sector in implementing CIP and the knowledge that the private sector has of technology and market trends means that policies that are not co-developed will tend to be misconceived or unworkable. The EU and OECD have made great progress in recent years towards engaging industry in co-development of information security policies but this model has not yet been applied sufficiently in all domains.

Understanding of infrastructures: No single corporation or sectoral grouping has the perspective required to view the infrastructure as a whole but individual sectors and corporations will have detailed understandings of their dependency chains. Government can take a top down, holistic view that will allow large-scale interdependencies and vulnerabilities to be assessed. The combination of bottom-up and top-down perspectives on critical infrastructures can therefore be of mutual benefit.

Threat and incident data exchange: As with vulnerability and dependency analyses, governments no longer enjoy a privileged position. While governments have specialist intelligence collection mechanisms and the ability to analyse data at a high level, they are relatively blind to large components of the cyber-threat. This blindness comes in part from a lack of skilled personnel, technology and structures but, more importantly, from the fact that the bulk of incidents occur in the private sector and that the majority of targets are not under government purview. Many cyber-incidents will only come to government notice if the victims choose to report them.

Government's partial sightedness in this domain has serious policy implications. In strategic terms, it is impossible to evaluate and forecast threat trends without current data, thereby leading to policy that may be based either on complacency or on exaggerated fears. In tactical terms, it is left to an *ad hoc* grouping of private sector bodies to exchange early warning information – making it harder to identify coordinated patterns of malicious attacks. This reduces the ability of individual owners and operators of infrastructures to identify and respond to threats in a timely manner.

Approaches

There is a range of approaches that can be taken to bridge the public-private gap and to foster co-operation. At one extreme is a top-down regulatory approach. This would involve central government enforcing measures on the private sector such as mandatory reporting of incidents and conformance with security and management standards. At the other extreme is a market-led approach. In this, the private sector would be left to find its own level. Market forces would be allowed to generate solutions to the IA problem; these may include insurance-based mechanisms and the development of communities of interest among and across sectors.

In post-industrial democracies the tendency is to favour market-led approaches but these will have to be supplemented by a degree of central planning and regulation. The main activities of most states in this paradigm will involve exhortation, pump-priming of R&D, encouraging best practice and providing an appropriate societal framework – including legislation, policing and education.

In institutional terms, the traditions of different societies will lead to different mechanisms, some of which are highlighted in Figure 1. For instance, in the US the National Security

Themes

Sectoral Linkages	Co-operation vs Competition	Policy Co-development	Understanding Infrastructures	Threat & Incident Data Exchange
Pan-governmental			NISCC	NISCC NIPC/JTF CND
Inter-corporate	IAAC	IAAC, NSTAC	NSTAC	ISAC
Trans-sectoral	IAAC	IAAC	AKSIS	CERT/FIRST
Public-Private	NSTAC IAAC	NSTAC AKSIS IAAC NIAC	AKSIS NIAC	NIPC ISAC
Public Buy-in				
International		OECD		FIRST

Figure 1: CIP Partnership Matrix[13]

Telecommunications Advisory Committee (NSTAC) provides a tested institution for bringing together owners and operators of telecoms infrastructures and for providing an interface between the telecoms sector and other sectors as well as between telecoms and the Federal government.

For now, the prime examples of public-private sector co-operative institutions have emerged as a result of US government initiatives. The Presidential Commission on Critical Infrastructure Protection (PCCIP) provided an initial framework for policy co-development and the National Infrastructure Assurance Council (NIAC) may provide a more formal framework for co-development. Co-operation in the field of R&D is most advanced and, under the National Plan released earlier this year, there is an effort to integrate federally funded work with private sector R&D.

Whilst the National Infrastructure Protection Center (NIPC) is a government body, its Infragard programme has sought to involve the private sector in incident reporting and its Outreach programme to involve the private sector more broadly. Of more interest is the Information Sharing and Analysis Center (ISAC) concept. ISACs represent an innovative mechanism to build intra- and inter-sector relationships to exchange incident and threat data.

Other nations are also moving towards institutionalising co-operation. Sweden is putting in place a number of mechanisms for sharing of incident and threat data while Switzerland's *Stiftung Infosurance* and Germany's AKSIS have been established to encourage co-development of policy. In the UK, the Information Assurance Advisory Council is being used by industry and government as a private sector-led forum to facilitate policy co-development.

IAAC: Approaches and Experiences

IAAC was launched in March 2000, so this paper provides an opportune moment at which to review the lessons learned from half a year of activities. After only a few months in existence, the need for such a forum and the enthusiasm to participate are evident; it is equally evident, however, that a great deal more work will be needed to break down institutional barriers to ensure a coordinated approach to infrastructure protection issues.

IAAC is an independent, membership forum supported by industry and central government. The motivation for forming the Council was growing concern among key corporations, government departments and researchers over the trustworthiness and reliability of the UK's critical information infrastructures. The focus of IAAC is upon the development of national and international policies on information assurance and critical infrastructure protection.

An important principle behind IAAC is that it is led by the private sector with the support of central government, to ensure that industry concerns are taken into account. Another important feature is that it is a non-profit organisation hosted by London University, thereby enabling it to take an objective and non-partisan view of the issues.

IAAC's core consists of a board of sponsors and associate sponsors chosen to represent key policy-making and infrastructure stakeholders in the UK Information Society. The current sponsors are: British Telecom, Hewlett Packard, PricewaterhouseCoopers, BAE Systems, the Post Office, Symantec, Anite Government Systems Ltd, i-Defense UK Ltd, the Cabinet Office and the Communications-Electronics Security Group.

IAAC is a membership-only organisation, with membership criteria that ensure it brings together a focused group of infrastructure stakeholders, policy-makers and IA specialists. IAAC does not seek to include all components of the NII, rather it will involve a representative sample of the major organisations in order to ensure it can bring to the table best practice from all sectors and that it can engage key players in an ongoing dialogue[10].

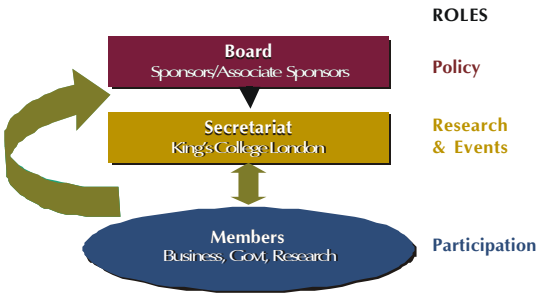


Figure 2: IAAC Structure

The interactive process in which IAAC's sponsors, members and the Secretariat initiate activities and devise policies is represented in Figure 2. It is important to note that IAAC's activities perform three vital functions for its members. First, they provide information and raise awareness of issues and developments. Second, they provide the opportunity to work with peer organisations in quite different sectors to develop common solutions to IA problems. Third, they enable IAAC's members to input into government policy and into policies being developed in commerce.

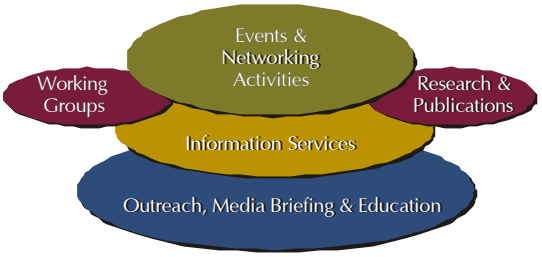


Figure 3: IAAC Activity Framework

IAAC performs these functions through the range of activities outlined in Figure 3. At the heart of its programme are regular seminars, workshops and symposia in which government officials and private sector representatives can work together to debate approaches to CIP policy. These events are supplemented by:

- Thematic Working Groups in which participants can progress the state of the art in crucial areas of CIP policy and IA. Currently, IAAC has working groups on: Threat Assessment and Early Warning; Risk Assessment and Dependency Analysis; Standards & Guidelines; R&D; Education & Outreach.
- Briefing papers that survey global state of the art as well as particular themes in IA and CIP policy[11].
- A web-based information service which provides IAAC members with a 'one stop shop' for information on CIP policy developments worldwide.
- An outreach and media briefing service in the form of a monthly newsletter and events round-up, supported by outreach activities such as articles in targeted publications, media interviews and conference presentations.

This programme of events and research has made IAAC an invaluable resource for infrastructure stakeholders and policy makers. IAAC has also had great success in bringing together leading government and industry players in a semi-private forum where they can work together to explore common problems and joint solutions.

However, the IAAC experience has also identified a number of persistent problems with the attempt to develop effective partnerships for CIP. Three are worth identifying here. First, although there is a growing recognition amongst businesses of the importance of assuring information assets, many sectors and organisations do not yet recognise that IA is a business critical activity. Moreover, even fewer organisations – whether in the private and public sectors – recognise the extent to which they are dependent on the complex web of infrastructures that make up the NII and even the Global Information Infrastructure. Second, although there is high level political support within many nations for e-business and e-government, there has not yet been a high level recognition of the need to support efforts to secure the NII, whether against criminals or against politically motivated threats. Third, even amongst those sectors with a good understanding of the problem and access to significant amounts of information, there remains a reluctance to co-operate and to share information outside sectoral boundaries.

Conclusion

Building the dependable infrastructures upon which the Information Society will rely poses a bewildering array of new problems to public policy makers and corporate leaders alike. Developing new forms of partnership and co-operation between sectors is one of the most pressing needs. Although IAAC and similar activities in other countries have begun this process, there are many obstacles to be overcome before effective new relationships can be established.

Thankfully, Europe is now following the US in beginning to give attention at the highest policy levels of the need to promote such co-operation. The European Council agreed at its summit in June 2000 that the eEurope Action Plan, which seeks to fast-track the Information Society in Europe, must urgently address the need to stimulate 'public/private co-operation on dependability of information infrastructures[12].' The EU and US have already initiated a dialogue that encompasses CIP policy development as well as R&D; the eEurope Action Plan provides the opportunity to advance this co-operation and to incorporate the private sector into the dialogue.

This call to action must be heeded by the private and public sectors alike if Europe, the US and their partners are to survive and prosper in the Information Age.

About the author

Dr Andrew Rathmell is Chairman of the Information Assurance Advisory Council (www.iaac.ac.uk). He is also Executive Director of the International Centre for Security Analysis at King's College London (www.icsa.ac.uk).

IAAC
King's College London
Strand Bridge House
138-142 Strand
London WC2R 2LS
United Kingdom

andrew.rathmell@kcl.ac.uk

Tel: +44 20 7848 1098
Fax: +44 20 7848 2972

Notes

[1] This paper draws upon material to be published by AFCEA in *Cyberwar 3*. Copyright remains with the author.

[2] www.iaac.ac.uk

[3] BBC, 'Barclays admits new security breach,' 2 August 2000, http://news.bbc.co.uk/hi/english/business/

[4] NCC, *E-Commerce and Consumer Protection*, http://www.ncc.org.uk/pubs/pdf/ecommerce

[5] Lawrence J. Vale, *The limits of civil defence in the USA, Switzerland, Britain and the Soviet Union : The evolution of policies since 1945* (Basingstoke : Macmillan, 1987).

[6] Steven M. Rinaldi, *Beyond the Industrial Web: Economic Synergies and Targeting Methodologies* (Maxwell AFB, AL: Air University Press, 1995).

[7] *A Minimum Essential Information Infrastructure for the DoD* (RAND, June 1998) at http://www.rand/org/organization/nsrd/MEII

[8] See FEMA's discussion of its activities at http://www.fema.gov/library/spln_1.htm.

[9] For instance, through the ISAC approach.

[10] An updated list of members can be seen at: http://www.iaac.ac.uk. At the time of writing, membership covers central government (e.g. Home Office, MoD, FCO), law enforcement and intelligence (e.g. NCIS, police forces, NISSC), finance and e-business (e.g. Prudential, Abbey National, KPMG, Ernst & Young), energy (e.g. BG Transco), research and education (e.g. IISS, JSCSC), ICT (e.g. Microsoft, Compaq, Cisco, BT) and parliamentarians.

[11] IAAC's briefing papers in 2000 cover issues such as comparative national CIP policies (Europe, North America, Asia), military dependencies, regulation of the Internet, global R&D.

[12] eEurope Action Plan 2002, Feira European Council declaration 20 June 2000. IAAC is actively engaged in this outreach initiative, having associate members from, *inter alia*, the USA, Sweden, Portugal and South Korea.

[13] The organisations featured in Figure 1 are merely a sample of the organisational structures in place in Europe and the USA. The table does not seek to provide a complete picture of each organisation's activities. NISCC – National Infrastructure Security Coordination Centre (UK); NIPC – National Infrastructure Protection Center (USA); JTF-CND – Joint Task Force Computer Network Defense (USA); IAAC – Information Assurance Advisory Council (UK); AKSIS – Arbeitskreis zum Schutz von Infrastrukturen (Germany); CERT – Computer Emergency Response Team; ISAC – Information Sharing and Analysis Center; NIAC – National Infrastructure Assurance Council (USA); NSTAC – National Security Telecommunications Advisory Committee (USA).

Security in E-business: Obstacle or Key to Success

by Frank Heinzmann, PricewaterhouseCoopers

The low costs and the worldwide availability of the internet – both for the private and for the business use – currently lead to a revolution: The revolution of 'Electronic Business'. E-business will change the way to make business radically; we are moving into the next era: from the information era into the communication era. Companies following this trend, hope for chances and opportunities in completely new markets, business initiatives and activities, which will be possible only through the use of electronic media. Existing business models shall be realised far cheaper and more effective because of the low working costs and the high speed of electronic transactions.

Despite some renowned success stories (eg Amazon, IBM) a lot of companies and private clients are still very reluctant and deal with e-business. On the one hand there is an uncertainty of the true potential of the electronic market and its maturity. Is it the right moment to make the required investments? Is the necessary technology available, stable and scalable? However, more often people mention the ostensibly missing security and lack of trust as main barriers. The main scepticism can be summarised as follows:

- Due to their connection to the internet, web-servers and internal systems, which support the e-business applications, are vulnerable for malfunctions, overload and targets of potential attacks (eg by hackers);
- Neither clients nor providers of e-business solutions have the required level of trust in the confidentiality and authenticity of transactions performed over the internet (eg credit card numbers);
- End-users' PCs and other devices are outside a company's influence and control and, hence, often offer insufficient security (eg poor or no virus protection); and
- The legal and regulatory framework concerning the security aspects of e-business still is not standardised and only partially developed (eg US export restrictions).

While some of these security doubts are justified, others are exaggerated. Today's cryptographic algorithms are able to dispel these security doubts. Cryptography covers three essential points:

- Confidentiality: The contents of electronic transactions can be protected against unauthorised disclosure;

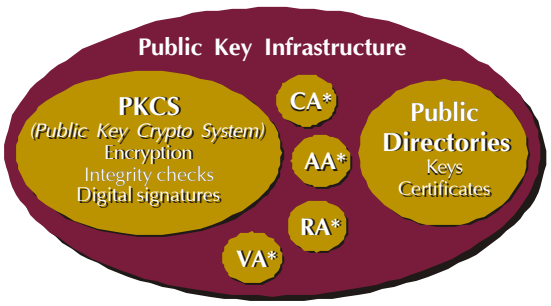
- Integrity: Every modification on an electronic transaction can be detected; and
- Non-repudiation: Sender and receiver of an electronic transaction can be clearly proven.

Confidentiality is ensured by encrypting the information with the recipient's public key (known to everyone), while integrity and non-repudiation are provided by signing the information with the sender's private (secret) key. Today, systems that are based on public key cryptography are offered by many vendors. The products are quite mature and various standards have been established. Hence, pure cryptosystems could – from a technical point of view – be implemented even in big companies within acceptable effort and time.

But: In order to integrate cryptographic methods in existing business processes, it needs several additional complex technologies, standards, processes and management practices which are summarised under the name 'Public Key Infrastructure' (PKI). A PKI is based on digital credentials – the certificates – which are checked and distributed by so called 'Certification Authorities' (CA). The certificates confirm a person's (or a company's) identity and the validity of the corresponding key pair, which is required to encrypt or sign information. A PKI allows:

- To define standards for digital certificates, so that they can be used over different scopes, companies and countries;
- To create, store and manage digital certificates and the corresponding cryptographic keys for it in a secure way;
- To renew expired or revoked certificates; and
- To revoke invalid or compromised certificates.

PKI is more than just Encryption



*C/A/R/VA: Certification/Administration/Registration/Validation Authority

PKIs play an essential role in the e-business field. They are the basis for the required trust in technology, security, confidentiality and authenticity of transactions and business partners. Furthermore, companies expect that a PKI can offer a standardised and flexible security architecture up to the end-user, which at the same time centralises and simplifies security processes (for the user as well as for administrators).

However, there are only a few examples of successful (that means profitable) implementations of PKIs. As mentioned before, this is less a problem of the technical feasibility but more because of the complexity of the organisational processes, which are required for the introduction and operation of a PKI. The companies are confronted with the following questions:

- Which applications should primarily be supported by the PKI? How can they be integrated?
- How and where will the keys and certificates be published? What information should these directories contain? How can existing directories be integrated?
- How can we securely integrate keys and certificates of remote employees, business partners or external consultants? Under what circumstances are we allowed to communicate with partners in foreign countries?
- Which additional requirements are introduced by the PKI in terms of end-user support and helpdesk (forgotten passwords, lost smart cards, invalid certificates, …)?
- Under what circumstances and by whom shall lost keys for encryption and digital signatures be recovered?
- What requirements related to user registration are introduced by the PKI (key creation, revocation of certificates, initialisation and issuance of smart cards, …)?
- How and where (internally or by external services) will the certificates be issued and checked? What do the certificate standards look like?
- How far does this concern the user? Do all the users have the competence and willingness to understand and apply the concepts of a PKI?

As many answers to the above mentioned questions require detailed (and hence expensive) investigations, most of the companies are still afraid to take the initiative and prefer observing the market (opinion 'leading edge = bleeding edge').

Companies that want or have to use the promising opportunities of e-business, should plan their strategies in the PKI field carefully. That means:

- Commitment and close integration of top management into the projects. This is true also for non-IT management;
- Generous budgeting of the necessary resources such as internal and external employees, project costs, soft- and hardware. Experience shows that supposed standard work (distribution of software, documentation, training etc.) swallow a lot of unanticipated resources, as they are often not included in the project plan;
- Checking of legal and regulatory requirements for the usage of crypto-systems in multi-national companies;
- Acquiring or building the necessary technical and management know-how;
- Definition, introduction and operation of the required organisational processes (user registration, helpdesk, CA, …);
- Decision if a PKI should be developed and operated in-house or if there should be an outsourcing service; and
- Piloting of PKI technologies, consultation and services.

A comprehensive introduction of a PKI still seems to be a challenge for companies, especially if we are talking about big, international firms. Nevertheless, PKIs – at least at today's state – are a must for a successful start into e-business. Security and trust are the essential factors: if they cannot be offered and made transparent to clients, e-business initiatives are subject to fail. But at the same time they are the key to e-business success, namely if they can be ensured by the introduction of appropriate technical and organisational measures.

Roaring Twenties ... Roaring Internet

by Peter Taffae, President and CEO, e-perils.com™

We have entered an era that future generations will study as we studied the Roaring Twenties. Today's Gates, Scullys, and Cases, parallel the JP Morgans, Rockefellers, and Carnegies of America's Roaring Twenties. Like the great times of the 20s, there are those that try to take advantage of an unregulated atmosphere. Today's 'robber barons' are known as hackers and crackers of the Internet.

History repeats itself and like the 1920s, there are people who for whatever reason try to take advantage. Sometimes with the Internet the robbers are kids just having fun (this 'fun' cost American businesses over $5 billion last year), or as is becoming more often the case, disgruntled employees (the single largest culprits of security breaches), or lastly third parties trying to make a political statement. A distinction needs to be made between a 'cracker' and 'hacker'. The media often confuses the two. The best way to differentiate between the cracker and hacker is his/her objective. The hacker is motivated to enter a site through unauthorized means for the intellectual challenge. The cracker is motivated by financial and/or political rewards. Unfortunately, even though the hacker does not do harm once he/she searches the site, a path has been established for those with less integrity.

The growth and magnitude of how the Internet is affecting the world's economies qualifies this new era as the Roaring Internet. The world has changed. The advances that technology and the Internet are bringing to our commercial and personal environments are influencing the economy and the lives of everyone.

The Internet economy is estimated to generate over $3 trillion this year. Growth is compounding at an astronomical rate. With only 250 million people having access to the Internet to date the indications are that this is only the beginning. In the US, approximately 50% of the companies that went public in 1999 (a record year for IPOs) were 'Internet companies'. Market capitalization of 'dot com' companies in many cases less than 3 years old exceeding $1 billion emphasizes the public's reaction and faith in the Internet's potential.

This new economy brings with it new perils that were never considered before. The insurance industry has responded in its traditionally reactive style, with few exceptions. One must recognize that as the Internet constantly changes so will the perils companies face. Be cautious when evaluating the products available as perils change often. The insurance products that address these perils need to

change in order to fully protect those living in the constant changing Internet.

The first generation of insurance products some of which are still used by a few insurance companies, used were miscellaneous E&O policies endorsed to cover e-perils? What most people did not fully understand was that these policies were endorsed in such a way that they became 'named peril' policies. With an ever-changing environment this severely limited coverage. Some insurance companies still use this approach. No matter how broad a 'named peril' policy is at the time of purchase it becomes obsolete in a short time. The alternative to 'named perils' is 'all-risk'.

The examples of new exposures for this new economy are long. Probably the first was the 'virus'. As in any crime the criminals become wiser as the protection gets better. We are now faced with 'Trojan Viruses', 'Worm Viruses', 'Logic Viruses' and others. Viruses were coupled with hackers, who then bred crackers.

The next best example of this ever-changing economy was the denial of service attacks that many of the most popular e-commerce companies experienced on February 9, 2000. Prior to this incident, the coverage for this type of peril was relatively unknown. What is the next new peril? Although no one knows, we can anticipate that cybercasting is gaining momentum. This is a logical next generation venue for Internet sites to incorporate into their marketing. Cybercasting brings with it media exposures that cyber underwriters are only beginning to address.

As the Internet moves from business to consumer (B2C) to business to business (B2B) the size of the losses can only increase.

The best way to understand the insurance exposures associated with the Internet is to divide cyber insurance into cyber property, which address the first party exposures and cyber liability, which addresses the third party exposures. The first party products will address the losses that directly warn the insured. Cyber liability protects the insured from third party litigation brought by any third party, including but not limited to government agencies, competitors, political or social organizations and clients. The industry has developed products that address these exposures with monoline policies as well as combined policies. There are pros and cons for each of these approaches. A careful review of these policies is mandatory to truly address the exposures that the insured face.

When evaluating the first party exposures some of the issues to consider include the triggers of coverage. Can an internal and external person cause the trigger? Internal security breaches are the most frequent and usually by disgruntled employees, but external is growing rapidly. Does loss include all types of viruses, including but not limited to malicious code being injected into the site? Is denial of service (which is not a virus) addressed? Like many e-commerce companies, the desire for market share is paramount so few are reporting net income. Because of this the traditional definition of 'net income' in the business interruption coverage is not acceptable. Keep in mind that a large number of e-commerce sites are service providers vs. product commercial establishments. Service companies do not have products (cost of goods) but are advertising revenue generators. These are important considerations when addressing cyber business interruption coverages.

The industry has developed products that address these exposures with monoline policies as well as combined policies.

Because we live in a litigious society, new allegations are surfacing almost as fast as the Internet is growing. Although case law is limited due to the infancy of the Internet, we have already seen litigation alleging things that did not exist in the brick and mortar world, or at least are taking new shapes and sizes. There are concerns that hyper-linking, which is the referral from one site to another, brings an implied recommendation. Plaintiffs could easily allege that if a site hyperlinks (recommends) the user to a service company's services, which results in an error and/or omission the origin can be traced to the original site and therefore bring unpredicted liabilities.

Another concern includes the jurisdictional issues that e-commerce companies face. Traditional companies choose the locations where they conduct business. And because of this can manage the legal issues arising out of the local jurisdiction. The Internet is global so the aggregate number of counties, states, provinces, and municipalities that exist in the world makes it almost impossible to manage each jurisdiction's local laws. An early piece of litigation was brought against Barnes & Noble for selling Mien Kampf to residents of Germany, where it is illegal to purchase this infamous book. Service companies regulated by

one state could be subject to 50 state regulators in the Internet world. If attorneys must be licensed in the state in which they practice is it not realistic that providing legal advice over the Internet (cross state lines) will subject them to scrutiny?

Insureds need to seek agents and brokers who have the experience and expertise in cyber insurance in order to avail them of the most comprehensive coverage available in the marketplace. Only those who are placing this fast changing coverage daily will be able to provide the best coverage to their clients. There are many 'technology', 'cyber', 'Internet' named policies available but few provide the coverage that ISPs and/or e-commerce companies require. This is an exciting and challenging time for insurance professionals and, as with any thing that is constantly changing, mistakes will be made. The true challenge is not to be the one making the mistakes but the one learning from them.

About the author

Peter R. Taffae is President and CEO of e-perils.com™. e-perils.com™ is an independent insurance wholesaler specializing in Cyber Insurance, D&O, E&O, Employment Practices Liability, Medical Malpractice, Crime, and Legal malpractice insurance for commercial and financial institutions.

Securing E-business with Practical PKI

by Dominic Storey, Director of Technology, RSA Security Inc

What happens when you add an 'e'? Business becomes e-business, commerce becomes e-commerce, banking becomes e-banking, birthday cards become e-greetings and so on. 'e' makes things current, but to get to 'e' means that you have interfaced your product or service to the Internet, dragging into the frame a whole series of issues: interoperability of multiple platforms and applications, scalability to millions of users, simplicity, client-less operation – and security.

Security used to be purely a corporate concern. How to keep the bad guys out, i.e. an insurance policy. E-security is different. It's as much about lowering the psychological barriers of service consumers against using your system: Is your service safe enough to use or should I use your competitors'? Will my credit card be hacked from your web site and posted on the Net?

On-line purchase with credit cards is easy: The principal risk of fraud in using a credit card on the Internet is exactly the same as in using a credit card over the phone (e.g. mail order, theatre tickets, etc). The fraud happens at the end point, usually by a dishonest vendor. We are comfortable with these risks because we are familiar with them (i.e. it doesn't happen often – regular use of our cards shows us that) and we know what to do when it does (ring the credit card company and they will sort it out). Which answers the second question: Whose risk is it? It's the credit card company's risk. When you buy an item with a credit card, it is actually the credit card company who is purchasing it – you are then buying it from the credit card company. Therefore, if you buy an item on the Internet with your credit card, the credit card company has purchased it, not yourself. Your risk is limited to a nominal amount (usually £30-50, depending on the credit card company). So go forth, log in and shop! That's what credit card companies want you to do!

However, shopping on-line is but one form of electronic commerce. Other forms of commerce do not involve credit cards and may involve the movement of such funds that no credit card company would underwrite. In general, e-security systems need to deal with interoperability, platform independence and scalability to millions of users. They need to meet traditional needs, such as boundary protection but they also have to meet the new needs, such as enablement for commerce. In many ways the problem of e-security is the hardest one of all. To understand how e-security can help, it's instructive to understand what processes need to be secured.

Four Tenets

E-commerce and indeed e-business as a whole involves the passage of information between parties. For this to make sense in a business context we need to be sure that:

1 We can guarantee the identity of the parties.

2 We can guarantee the information transmitted has not changed.

3 We can guarantee the confidentially of the information in transit.

4 We can protect against denial of transaction by one of the parties (non-repudiation).

These four tenets are routinely assumed in traditional business transactions, for example when people meet face-to-face, read and sign a contract which is then notarized by a solicitor. However, in electronic systems, such as e-mail, or web systems, these four tenets are not so simply achieved. Solving them requires the use of computer cryptography and unique, securely distributed keys (which can be used as proof of identity and for encryption), implemented in a vendor-independent fashion with a very, very simple user interface. Impossible? Meet PKI.

Solving The Problem – PKI

PKI is an acronym for Public Key Infrastructure. It describes a system for managing the essential elements of cryptography to enable the four tenets to be satisfied. To understand how this works, we need to look at how encryption solves these problems.

How do we guarantee the identity of parties? By providing them with a unique key that can be used with encryption to 'stamp' data or a transaction with a unique fingerprint. Since a user is the only person to possess a particular key, data stamped with that key is traceable to that user.

How do we guarantee that data has not been changed in the data transmitted between parties? By distilling a unique index (digest) of the data to be sent and sending it, stamped with the originators unique key, to the receiver. The receiver can prove that the digest came from the sender, and can also recalculate it from the received message. If the two digests are the same, the message has not changed. This is called a **digital signature**.

How do we guarantee the confidentiality of the data transmitted? By encrypting the data so that only the receiver can decrypt it.

How can we protect against denial of transaction? By using digital signatures. Since a digital signature is unique to a user, it can be used as proof that the user originated a transaction such as transferring funds voting, or signing a contract.

This is how cryptography can be used simply within business systems to satisfy the four tenets. However, simple cryptography this is not PKI. PKI fixes all the new problems that are thrown up *by* simple cryptography. For example, how do you connect a key with a user? Who's to say that this user and that key match? How does a recipient decode a sender's message, if the receiver does not possess the sender's key? And if the recipient **does** possess the sender's key, how do you guarantee that the receiver does not use it to impersonate the sender to someone else?

Public Key Cryptography

Three cryptographers, Rivest, Shamir and Alderman, the founders of RSA, solved the problem in the 70's by inventing a new form of cryptography, based on encryption key pairs, called **public key cryptography**. Each user has two keys, one which is in their sole possession (the private key) and the other freely given away (the public key). This form is the cornerstone of the PKI. The beauty of this system is that users don't have to be aware of encryption keys at all, but instead, exchange documents of trust called **certificates**. A certificate is a document generated by a third party called a **Certificate Authority or CA** (like the party in the contract-signing example above) and testifies that a public key belongs to the user named in the document. This certificate is in-turn digitally signed by the CA, proving its validity and origin and providing proof against tampering. The great thing about certificates is that they are user friendly and contain nearly all the information you need to trust them.

So what do you need to know in order to trust a certificate? You need access to the public key of the CA. This public key is needed to decode the digital signature the CA used to sign your certificate. This key is usually provided by the CA in a (you guessed it) certificate, known as a signing certificate, or signer.

Just as trust can be multi-level in real life, trust in PKI can also be multi-level. People trust your certificate because it is signed by an organization they trust (the CA). Furthermore, the CA may in turn be subordinate to a higher level of CA, forming a trust chain. Therefore, to trust a certificate, you need the signer of the

certificate and any higher signers, until you get to the root signer.

Why are most people ignorant of signers? Because most implementations of PKI use signers that are already contained in both Netscape and Microsoft browsers. It's only when companies create their own certificates that they find themselves having to distribute signers.

Public key cryptography and PKI are deep subjects and more than a match for the space allotted to this article. Probably the most important thing about PKI is that it's already pervasive. RSA have licensed it's algorithms to the leading computer suppliers, such as Microsoft, Netscape, Sun, Compaq and Novell. Indeed the RSA algorithms have become such de-facto standards that they are already used in all secure web transactions (that little key that appears in your browser when you initiate a secure connection to a web server indicates that the RSA algorithms have been engaged). The use of RSA algorithms is an excellent example of the application of **Metcalf's law**, which states that the usefulness of a system is proportional on the square of the number of people using it.

So where else is public key encryption used? Not only in browsers and web transactions but also in secure e-mail transactions. Microsoft, Lotus, Novell and Netscape all support a standard called Secure Multi-purpose Internet Mail Extensions (S/MIME), which allows you to digitally sign and encrypt mail communications. The benefits of using S/MIME e-mail is that you can start to use mail to convey legally binding and/or sensitive material, such as contracts. Another protocol that incorporates public key encryption is Secure Sockets Layer (SSL), which can be used across TCP/IP networks to secure any client-server application such as SAP R/3, PeopleSoft, Oracle or Lotus Notes, or a Virtual Private Network (VPN). Another application for public key cryptography is in the new Wireless Application Protocol WTLS, which will be used by mobile phones, and other mobile devices for Internet access, share dealing and Internet Relay Chat. Also, look out for PKI in electronic document systems such as *Adobe Acrobat, E-Lock Assured Office* and in forms software such as *Informs* or *Shana Informed* to name but a few.

One application of PKI is in notarized time. There are many times when agreements between parties need to come in force at a particular time, for instance in a stock transaction or property sale. Merely signing the agreed contract is not enough – somehow, a digital signature including time needs to be incorporated into the document. This is called time stamping. Authorized time is provided by a time server, connected to a reference clock such as an atomic clock service. Time is stamped using the time server's private key, creating in effect a 'certificate in time' used to notarize the document.

Physical Me, Digital Me

One problem that PKI does not really solve is the problem of *who* is actually behind a certificate. To illustrate this problem, think of a man who registers for home banking. He registers on-line with his bank and as part of the process, has digital credentials generated in his browser, he gets assigned a certificate by a certificate authority and hey, presto he is ready to go! However, the digital credentials and matching certificate are stored on the hard disk of his computer – which, while he is out, his son hacks into, makes some transactions and makes a huge increase in his pocket money allocation. How would the bank discriminate between the honest transaction of the father and the fraudulent transaction of the son? The answer would be that the bank doesn't know – it's up to the customer to protect his digital credentials.

So there are more to safe transactions than certificates, encryption and keys. One useful model for this is to think in terms of **two user entities** (Figure 1). The first user is the *physical me*. The second user is the *digital me*. The physical me is the biological entity that logs onto the computer and uses the machine. The digital me is the on-line entity that manipulates data and performs transactions. The process that binds the *physical me* to the *digital* me is called **authentication**. The components that bind the *digital me* to the data used and the transactions made are certificates and cryptography.

It is important to understand that the strongest systems are hybrids of strong authentication systems and PKI. Strong authentication systems usually replace passwords with a device such as a smart card or token. This strengthens the security of a basic PKI, which usually relies on a simple password. **Without strong authentication systems, the effectiveness of PKI boils down to the effectiveness of a password.**

How strong is PKI? Encryption strength

Codes, like rules are made to be broken. All encryption codes can (theoretically) be broken, if you have enough time. In the real world this

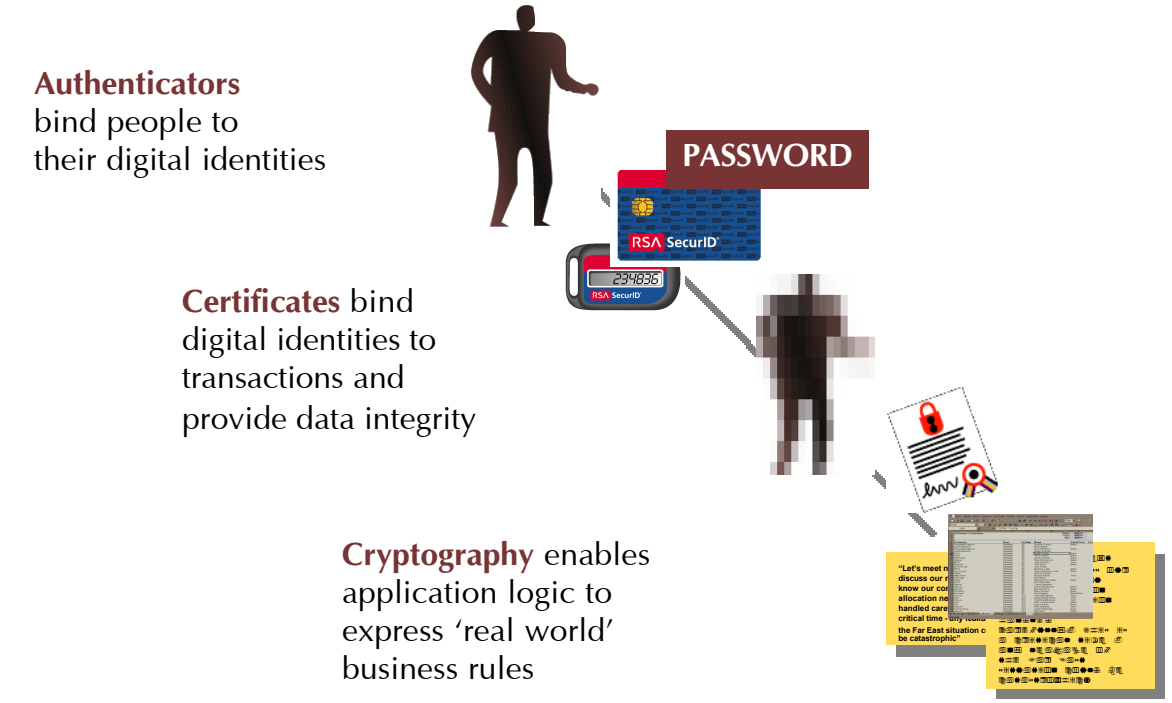


Figure 1. Physical me, Digital me

translates into one thing – computer power. The cryptography behind PKI is very strong – you need a lot of computer power to break modern codes.

How much power do you need? This really depends on the length of the encryption keys. Your public/private keys used in digital signing are going to be either 512 bits long or 1024 bits long. A different encryption system is used in SSL, which has characteristic key lengths of 56 bit or 128 bits long. To give you a sense of how hard it is to crack, a message encrypted with a 56 bit key took 10,000 Internet-connected computers a day to crack (RSA Challenge, 2000). However, Moore's law shows that every 18 months, computer speeds double, therefore we must similarly make encryption harder to crack. Fortunately, we can double the strength of encryption by using keys which are 1 bit longer, eg 57 bits would take 2 days, 58 bits 4 days, 59 bits 8 days, … and 128 bits would take 10,000 of today's interconnected computers two hundred thousand billion years to crack! However, as these machines themselves obey Moore's law, key length increases are really about maintaining 'e-détente', whereby traders have a means to always make impractical the cracking of messages used in their e-commerce.

Munitions of War

Why are signing keys 512 or 1024 bits long and SSL keys either 56 or 128 bits long? The answer lies in the fact that governments view cryptographic technologies as munitions of war – and they don't want too strong cryptography getting into the hands of potential enemy governments. What this has meant in the past is that the US required security software companies to provide two versions of their software – a domestic version for use within the US and an international version for use outside the US. The domestic version used stronger keys, (1024 and 128-bit) for encryption and the international version weaker keys (56 and 512-bit). However, in 1999, the US government relaxed control on encryption strengths allowing US subsidiaries and financial institutions to use128-bit encryption. In 2000, the US government passed legislation to allow the export of domestic strength cryptographic products to all friendly nations. Does this mean that arbitrary length crypto can be exported? No, key lengths longer than 1024/128 are still under control and products that allow substitution of cypher are still denied export permission.

Is this an issue? Not to general commerce, as 1024/128 has already been shown to be strong enough for some years to come. As for most governments and high security military establishments, many of them 'roll their own' and would not use a foreign product.

The law and PKI

Because PKI solves the four tenets so well, it is the core technology behind e-commerce law. Most European governments are looking at implementing digital signature law, whereby electronic contracts can be made binding in law. All systems meeting these proposals require the use of PKI. If you are interested in

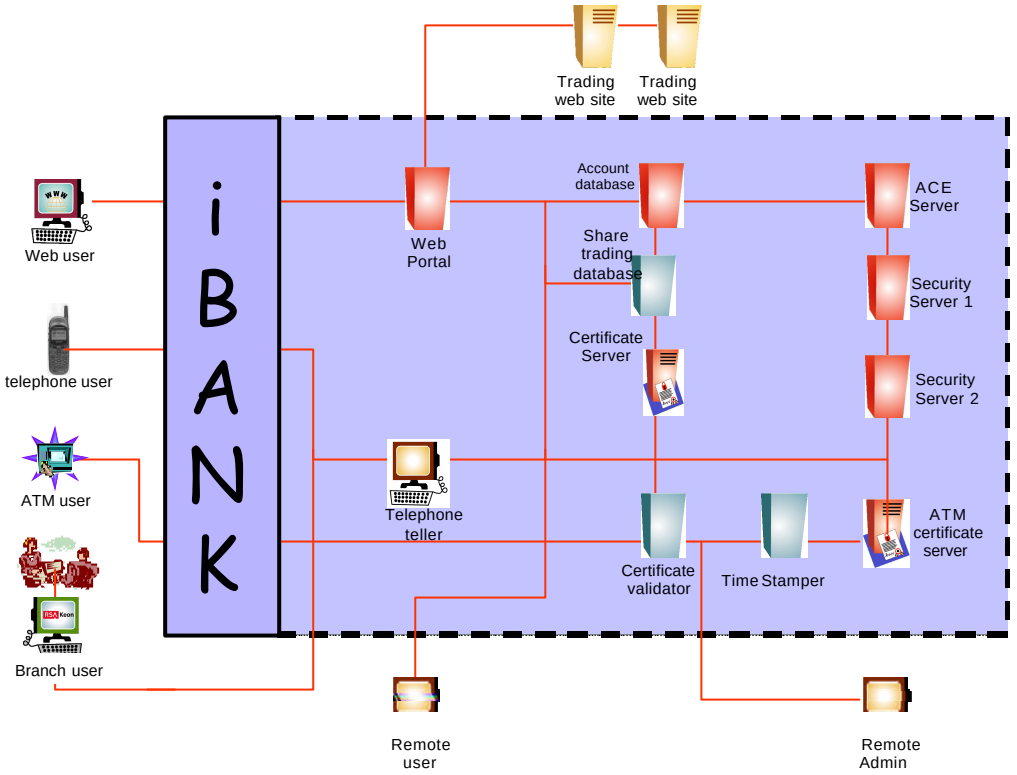


Figure 2. iBank

the EU directives, you may wish to check the EU web site of http://www.europa.eu.int. Effective digital signature laws will vastly accelerate the introduction of electronic commerce, for a range of transactions much greater than demonstrated by credit card purchases.

Beyond simple PKI

Many organizations have found that first-generation PKI systems have been difficult to implement in the real world. Why is this? Because first-generation PKI has not taken into account issues such as ease of use, ease of deployment, centralized management requirements and security service integration issues. For example, many first generation PKI systems rely on password-protected storage of private keys, certificates, etc. on the workstation hard disk. This opens up the system for attack and is difficult to enforce via central policy. Furthermore, it becomes difficult to distribute signing certificates to users, making systems harder to use. Lastly, two incompatible standards of credential storage have evolved – Microsoft CAPI and Netscape PKCS#11. The implication of this is that users are forced to match their mail application to their web browser – a choice many users do not want to make.

Advanced PKI systems add layered services on top of simple PKIs to provide real world services, such as policy control, choice of authenticator, unified credential store, file encryption, session encryption, root signer distribution and so on. Architecturally, they add a **PKI client** to your user's PC's and a **PKI security server** to your network. Typically, the PKI client is either downloaded from a web server or automatically distributed by some other means. The PKI security server may be replicated for fault tolerance and scalability. Advanced PKIs also provide the means to integrate legacy applications into the PKI world, via the use of PKI proxies.

Putting it together: iBANK banking example

To illustrate how PKI can be applied in a real-world example, we have developed a 'concept customer' called iBANK (Figure 2).

iBANK is a modern bank that provides a set of services – Internet banking, telebanking, branch banking and ATM banking and share trading. Customers can open an account via the web and providing they pass their credit checks, their accounts are automatically initialized. Through the bank web access portal, they are additionally offered spot discounts on other services offered by the bank trading partners.

Once registered, clients are sent a RSA SecurID token, for telephone banking authentication. RSA SecurID provides them with a means of strong two factor authentication. This means that they do not have to remember telephone PINs or worry whether anyone else has them.

Clients are provided with a debit card for use in ATMs and shops. In addition to the normal magnetic stripe for use in standard ATMs, these cards are 'smart', and contain an RSA cryptographic co-processor for use in high value transactions. Each user generates a private key which is stored on their card, to be used to create digital signatures. From any iBANK ATM, users can authorize transactions far in excess of other ATMs because legally defensible digital signatures are used throughout the banking process.

Clients are provided with a smart card reader and Advanced PKI software for their PC. When they perform web transactions their digital signatures are used to sign transactions, making them non-repudiable

All transactions are signed and time stamped. If an agent is performing the transaction on behalf of the user, (as in the case of ATM access or as in telephone banking where a teller executes on behalf of the client via phone) then the agent's certificate is used. In this way, data is protected, personal responsibilities encouraged and internal fraud is minimized.

In addition to servicing its customers, iBANK must provide secure services to its staff. The bank has therefore provided remote access via VPN with RSA SecurID authentication. Furthermore, some resources within the bank must use additional means of security. For example, proximity sensors on workstations used by branch office managers limit customers from accessing unattended screens and strategic accounts within the environment are protected by RSA SecurID tokens or smart cards. Access to critical systems within the bank are protected with additional two-factor authentication – for example the UNIX root accounts on the stock transaction and bank account database servers.

Internal users in the bank are also protected with Advanced PKI – ensuring a comprehensive internal security policy can be deployed. Security servers are of course replicated for redundancy and efficiency.

The benefit? iBANK can provide a more comprehensive and competitive banking service to its customers than it's competition. It can use the same PKI infrastructure internally as it can for its customers, reducing costs. All transactions can be viewed along with time-stamp and digital signature, allowing no place for dispute. Records can be opened up for auditors making it easier for iBANK to pass audits. In summary, iBANK can do a better job at establishing its security pedigree, critical for attracting customers in today's competitive world.

Summary

PKI is a core technology for the new millennium as it is fundamental for enabling secure electronic commerce. Today, electronic commerce is somewhat limited for most people to credit card transactions, in effect, old technologies adapted to a new world. Once underwritten by law, electronic commerce can be used for transactions ranging from micro payments to payments of hundreds of millions of Euro. Voting and other community services can be implemented reliably, such as tax returns and driving license applications. The limits of commerce will be bound by accessibility to the Internet, and with WAP around the corner, this seems like no limitation at all.

About the author

Dominic Storey is Director of Technology at RSA Security Inc. He lives in Massachusetts, USA.

You can contact him via e-mail: dstorey@rsasecurity.com

Upcoming Conferences

The following list of conferences has been brought to our attention. We would welcome any additions.

November 27-30, 2000
Boston, Massachusetts

Ultimate Incident Response: Hands On

http://www.foundstone.com/scripts/training.asp

November 28-30, 2000
Philadelphia, Pennsylvania

Network Security & Firewall Administration

http://am.globalknowledge.com/sec

November 30-December 1, 2000
Arlington, Virginia

E-Security Conference & Expo

http://www.imgevents.com/conferences

December 10-15, 2000
Washington DC

Capitol SANS

http://www.sans.org/capsans.htm

December 3-7, 2000
Kyoto, Japan

Asiacrypt 2000

http://www.iacr.org/conferences/ac2000/

January 8-12, 2001
Paris, France

International Workshop on Coding and Cryptography (WCC 2001)

http://www-rocq.inria.fr/codes/WCC2001/

January 22-25, 2001
San Diego, California

Entrust Secure Summit 2001

http://www.securesummit.com/

February 7-9, 2001
San Diego, California

ISOC 2001 Network and Distributed System Security (NDSS)

http://www.isoc.org/ndss2001/

February 13-15, 2001
Cheju Island, Korea

International Workshop on Practice and Theory in Public Key Cryptography (PKC2001)

http://caislab.icu.ac.kr/pkc01/

February 19-22, 2001
Grand Cayman, Cayman Islands

Financial Cryptography '01

http://fc01.ai/

March 29-30, 2001
Providence, Rhode Island

Cryptography and Lattices Conference (CaLC 2001)

http://www.math.brown.edu/~jhs/CALC/CALC.html

April 2-4, 2001
Yokohama, Japan

Fast Software Encryption Workshop (FSE2001)

http://www.venus.dti.ne.jp/~matsui/FSE2001/

April 8-12, 2001
San Francisco, California

RSA Conference 2001

http://www.rsasecurity.com/conference

Call for Articles

If you are interested in contributing to this publication, we invite you to submit articles containing your thoughts, ideas and concepts.

Contribution guidelines for papers being submitted to the Cryptographic Centre of Excellence Journal are:

- Topic must fall under the umbrella of cryptography, security and/or privacy;
- Articles should not be of a promotional or product marketing nature;
- All submissions will be reviewed for content and may be declined at the discretion of the editor (for example, if the tone and/or content is overtly promotional or product marketing-oriented);
- Maximum article length to be 5,000 words plus tables/graphics;
- Submissions must be original work and, where appropriate, give credit to the original author(s);
- The editor reserves the right to edit the text with the agreement of the author; and
- All submissions must be made in MS Word or .RTF format.

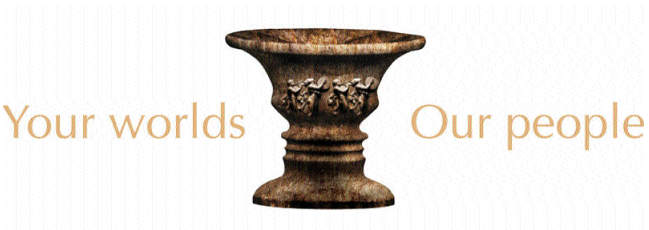
PricewaterhouseCoopers reserves the right to re-format for publication purposes and re-distribute as appropriate.

Authors maintain ownership of all submissions.

Completed submissions or abstracts should be submitted via e-mail to either:

geoffrey.c.grabow@us.pwcglobal.com

john.velissarios@uk.pwcglobal.com.



©2000 PricewaterhouseCoopers. PricewaterhouseCoopers refers to the individual member firms of the worldwide PricewaterhouseCoopers organisation. All rights reserved.