[Home] [Current Edition] [Compendium] [Forum] [Web Archive]
[Email Archive] [Guestbook] [Subscribe] [Advertising Rates]

# Security Revisionism

**Journal of Internet Banking and Commerce, April 2006, vol. 11, no.1**
**(http://www.arraydev.com/commerce/jibc/)**

**By Ian Grigg, Financial Cryptographer**

Web: Financial Cryptography
Email: *iang at systemics dot com*

Ian Grigg has been a Financial Cryptographer since 1995, building strong payment and real time trading systems for exotic instruments, in Europe, the Caribbean and North America. He is the author of the influential 7 layer model that integrates technology to business in digital commerce. He is currently working on new definitions in security and governance, as well as systems to integrate payments with instant messaging. He has a BSc(Hons) Computer Science from the University of New South Wales and an MBA from London Business School.

## Abstract

**Security isn't working, and some of us are turning to economics to address why this is so. Agency theory casts light on cases such as Choicepoint and *Lopez* . An economics approach also sheds light on what security really is, and social scientists may be able to help us build it. Institutional economics suggests that the very lack of information may lead to results that only appear to speak of security.**

## Security isn't working

It is slowly dawning on the world that Internet security isn't working. The brightening daylight is coming from a number of sources; you can see it in phishing journalism and the bemusement of victims like banks and individuals - wasn't online banking supposed to be safe?

*Before Windows 95, a few anti-social misfits wrote computer viruses. Now the top-selling software is for security -- anti-virus, anti-spyware, anti-phishing, anti-spam. Thank you Windows 95* [ 1 ].

You can see it in discussions by security specialists who note that security expenditure is going up and security itself is going down [ 2 ]. It's in the courts, as strangely scary legal cases reach into our very beliefs about who is reponsible for what. And you can see it in the ongoing soap opera known as national cybersecurity , where hardly a day passes when there aren't a half dozen articles all bemoaning in one superficial form or another that government efforts at what they call cybersecurity simply don't work [ 3 ].

Some people know what's going on. Some say they've known all along. Others say everything is fine, or will be if we just finish up on deploying PKI or this other hobby horse, or all try a little harder, or stop causing trouble by promoting bad agendas.

One group that is coming to accept the proposition that security isn't working is the security research community. The cryptographers, the protocol designers, and the academics are starting to question where it went wrong, if not the builders and sellers of systems. Mostly the ones that have links into academia are starting to ask hard questions, rather than the big corporate machines, as those latter still have a way to go before the bias of marketing is factored out.

So if security isn't working, what then? This is an attempt to list what I see as open security questions. It's my list - you can either write your own or criticise mine, whichever works best. We really are searching for ideas here, so apologies in advance, but I'm letting my muses flow today.

## The Agency Problem

That which economists and accountants call *the agency problem* is now being applied to security [ 4 ]. In this regime, the alignment of incentives is suggested as the primary reason why people (and, especially, employees) act. With security, we are concerned with fraud, and with weak protections, so we can ask ourselves what can we do to align the incentives better to get better protection?

In one case we have software vendors delivering insecure product and then not taking responsibility for the damage done when this software is hacked. Microsoft leads this race again, but are not alone: browser manufacturers do not cover you for phishing, firewall manufacturers do not make it easy for you to configure them, and intrusion detection system ("IDS") manufacturers do not make you read the megabytes of logs spewing forth every day.

In a related case, consider Choicepoint and all of the data breaches that have occurred in retail America. 2005 may well be remembered as *The Year I Lost My Identity* . By some accounts, " 50 million sets of identity " have been compromised, and it would be fair to ask whether everyone in America is now known intimately to a crooked database somewhere [ 5 ]. (Non-americans need to note that America is the land of easy credit, and everyone has credit data!).

Back to agency theory, and we find that like the software vendors, the (legal?) holders of those sets of data are not liable. They are not even *responsible* for the most part in the sense that only recently has it transpired that they have a duty of care for this data that is traded back and forth like popcorn at a movie. So, data miners in America have traditionally taken very little care to protect potential injured parties - a fact that was brought foremost by the rather quixotic response of Choicepoint to the maelstorm that they unwittingly released.

Fundamentally, users and companies understand that their own actions might benefit their security, and understand the concept of " aligned incentives ." The question then arises as to how to share and align those incentives so that better security is achieved [ 6 ] ?

## A Duty of Care?

We see then large corporations that could be more responsible. All things being equal, the english common law tradition has it that the larger party should take more care. Perhaps following this guideline, we now have calls for the banks to be totally liable for the harm of phishing, and similar cries [ 7 ].

Yet, not all things are equal [ 8 ]. One look at the case of *Lopez v. Bank of America* will clear that up [ 9 ]. In this case, we have the testimony of the US Secret Service that Lopez' computer was infected by a virus and that probably snaffled his password. Who then is the liable party? Do we hang the blame on Bank of America and why? Is the blame attached to Microsoft's operating system and applications for being so easy to infect? Maybe Lopez himself should have installed the right security software?

Consider the defendent, Bank of America. What did they do wrong? They installed SSL just like they were told to by the security industry. They probably purchased the best Verisign certificate, which even goes so far as to promise security up to some many $'000 of insurance. They secured their servers, just like they were told by rafts of consultants, probably employing all the latest tools to do so.

In short, they did pretty much everything they were told to do by the security industry, and by any large vendor of security product. What's perhaps even more perverse is that they will probably lose this case, because they missed the one crucial thing: they should have known that the user's computer is insecure, and it is too insecure to support Internet banking.

### The very meaning of the word

But you are hardly likely to see a rush to turn off Internet banking in America. Which brings up a very dramatic gulf in our understanding: what do we mean by security? How can we measure whether something is secure enough?

One line of very fruitful investigation is to ask, just what is this thing called *security* ? We see this uncertainty in every product pitch that screams "buy this and you'll be secure" at us. Inner voices scream "that's not security" to us, and shortly thereafter, "that won't work!"

But no inner voices inform us of what would work. To be fair, if that is *not* security, whatever it is, then what is? Can we define security? Can something be secure yet not secure? If something *is secure* , does that mean we *have security* ?

Is it to do with people feeling safe? Or to do with people saving money or coming out on top in net-present-value ("NPV") calculations? Or, is there some higher goal? Is it to do with our documents never being seized, or never being listened to? Is this a supply side question, in that we security engineers know what to supply, or a demand side question, in that users know what they want?

### Pareto-Secure

How do we measure security? How do we objectively look at a product or a situation and come up with a number of points out of 10, a pass level, or even a Yes or No? Is it in signals? Is it even fair to hope that there exist objective standards of security, or is it a subjective or relative good?

One view has it that certain cryptographic algorithms are in fact so secure we don't need to worry about them. These I call *pareto-secure* following the concepts of economics [ 10 ]. This suggests a way to create an objective standard of security for these components. Simply put, we craft a set of such pareto-secure components, make sure they meet the standard being set, and then our job might be done.

But, in a sense, the value of this concept is that it highlights how short of comprehensive we are: only relatively few components meet such a high standard and these are mostly limited to the narrow field of cryptography. Even more limiting, integrating two such components together does not necessarily create a further component of strong security.

If anything it isolates and lays bare how hard it is to achieve anything like complete security. Worse, the small subset of cryptographic components that allows us to make strong statements about just those components has contributed to a general composition fallacy in products: if your product uses RSA-4096, AES-256 and SHA-512 then it has to be secure, right?

Wrong. The selection of these components says very little about security other than that the author knew enough to read the right FAQs. In a sense this is even a negative signal as the author wants you to believe that pareto-secure components are what it is about, and not to question how these components are integrated.

### No-risk security versus Risk-based Security

Which leads us to the one thing that we do know: Security is not absolute, it's not "no-risk" and the 1990s generation of Internet cryptographic engineers were wrong on this.

Adi Shamir suggests that to double security we have to double costs [ 11 ]. The specific failings of the '90s generation were an over-attention on a perfect security model, which resulted in usability issues on the one hand, and crowding out other ideas primarily with public key infrastructures ("PKIs") on the other. We will pay the price for this in phishing for the next couple of years, until PKI is overcome.

## Usability

How do we build a secure product? We already know how to build a secure product on paper, but not one that actually seems to serve and prosper - that then doesn't count. How can we build a product that both is secure according to our theory and actually *gets users to use it* ?

The Usability of Security is one way forward here - one thesis of which is that we security engineers should stop trying to build it all in up front, but should follow on behind and help already successful applications then move on and secure themselves [ 12 ].

The reason for this approach is more systemic and integrative - while we may know a lot about security, we as security people know next to nothing about usability and the nature of applications in general. So by musts we find ourselves waiting until the application is built and has proven its usability model as well as its economic model, before we can understand enough to build a useful security model.

In short - this thesis proposes that *you should build it insecurely* , which is the complete reverse of what security experts promote! Now we say, if you are making money, we'll help you keep it. But otherwise, it's not worth securing something that doesn't make you money.

## Capabilities

Researchers are working through the ramifications of Usability and discovering it's hard work. One group that has recently achieved successes here is the Capabilities School. In this engineering approach to the creation of Rights in an insecure world, capabilities are used as the hooks to just about everything. Capabilities might be described as references to objects (similar to Java) that follow the the founding principle of POLA - the principle of least authority.

In order to demonstrate this, researchers at HP Labs have recently announced a safe environment for Microsoft tools [ 13 ]. By taking on a totally unsafe application such as a browser in Microsoft environment and wrapping a POLA layer around it, they've shown just how far we can go with sound engineering and rights designs.

The big challenge for the school is to take the advanced concepts of capabilities and graft enough of them into the production world to deliver security benefit. Picking on Microsoft is a good idea, as Microsoft promotes the reverse in the way its operating system and applications work - principle of maximal authority.

## The Wider Institution

Which all could just be mumbo-jumbo as far the security manager is concerned. He or she is more interested in where to buy it and that leads us to one of the big difficulties with not understanding security - what can't be understood cannot be bought, but it can be sold.

### The One Big Idea

One particular problem is that even though we know that security is driven by many and complicated threats, it is highly susceptible to *the one big idea* .

An example of this is seen in recent times in the geopolitical world of America's security. The administration's obsession with terrorism drove a rebuild of the country's federal security apparatus at much cost, but when Hurricane Katrina came along and devastated New Orleans, the federal machinery failed to respond in any timely fashion. What appears to have happened is that the parts of the apparatus tuned to natural disasters were downgraded and stripped of resources, and the whole meaning of a risk was reworked and retuned around the current big idea of terrorism. Because a hurricane wasn't terrorism, it was no longer considered an important risk at the federal level.

This is an important observation, and we'll come back to it.

### Herding.

A security good is one where the real test of the product is under aggressive attack by some third party that won't sit still for you. This means it is impossible to objectively test before hand - unlike road accidents, attackers don't operate to statistics, and don't perform according to routine like other machinery.

Security goods are then distinct from safety goods, which leads us to the following observation:
Because there is no way to create an objective set of measuring or testing standards, any good can

easily meet the benchmark!

Out of this dilemma arises a difficulty in figuring out what our poor security manager is to do, and again economics provides the answer: *herding* . This concept arises generally in over-regulated sectors such as banking where all participants are forced to be equivalent, because any that step out of line do so at risk of attack by other participants and the system of regulation itself.

In order to address security needs, herders creates a common set of goods which are agreed across a community. We can call this set of goods *best practices* and its arisal is relatively well understood in security communities.

### Michael Spence's market for education

Following on from the work of (Nobel Laureate) Michael Spence and his seminal paper on *the market for education* , I postulate that best practices arise that are disconnected to security. Spence shows that it is possible for metrics to become widely employed and sustainable that do not perform benefit; I go further and suggest that it is possible, even likely that metrics will arise that reduce security.

How is this possible? Consider the failure of the One Big Idea above. In security, the attacker doesn't sit still enough to validate any particular idea that one might have and only at quite significant up-front costs can any particular idea be tested. Even then an attacker can move more quickly than any one idea can close any one hole.

In this veritable nightmare of incentives and foggy rationales, we can suggest that no product is fully rewarded for good actions. We can imagine then that as there is no positive feedback, the incentives on suppliers to sell a good product are particularly weak. In sales, only the sale counts, so without the positive feedback of successful security, sales quickly shifts across to large expensive ideas and these require large expensive sales campaigns.

In other words, any One Big Idea is stable, and enters into the set of best practices. Every year we see the latest and greatest in security and forget what it was we were talking about last year. I call this *the market for silver bullets* , to use a term that is widely familiar in the computing field, and it is written up more fully in a draft paper [ 14 ].

## Conclusion

So where are we? In a sense we are in a greenfield setting. We have discovered that much of our security thinking is wrong (and that in and of itself raises interesting questions). What we now need to do is go back to first principles and rebuild our security apparatus.

If you think this is going too far, consider this: when we first started in computing security, we spent a lot of time trying to get people not to write passwords down. Now, we are trying to reverse that and get people to write them down on a piece of paper - even a postit note on their monitors is better for us than a weak, remembered and shared password!

Why is this? In part because the threats are moving faster than we are. And in part because we didn't know enough to begin with. Interesting times ahead!

# References

[1] Quote taken from *Bangkok Post* , formerly at http://www.bangkokpost.com/news/24aug2005_news33.php
[2] Marcus Ranum, "Going meta on Firewalls," http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-06/0032.html
[3] for example, Richard Bray, "Making haste slowly," http://www.itworldcanada.com/a/E-Government/d1a3c1e2-68d8-42f8-a824-4b0551dd31f6.html
[4] Ross Anderson, "Why Information Security is Hard -- An Economic Perspective," http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf
[5]Danielle Belopotosky, " Data security officials ponder response to 'year of breaches,'" http://www.govexec.com/story_page.cfm?articleid=32735&sid=1

[6] Fujitsu, "Web shoppers demand security dividend from banks," http://www.fujitsu.com/uk/news/pr/fs_20051031.html.

[7] Bruce Schneier, "A Real Remedy for Phishers," http://www.wired.com/news/politics/0,1283,69076,00.html, Wired.

[8] Ian Grigg, "Blaming the Banks won't work," https://www.financialcryptography.com/mt/archives/000560.html, FC.

[9] John Leyden, "Florida man sues bank over $90K wire fraud," http://www.theregister.co.uk/2005/02/08/e-banking_trojan_lawsuit/ . Also see case for defence and plaintif .

[10] Ian Grigg, "Pareto-secure," http://iang.org/papers/pareto-secure.html, Draft paper

[11] Adi Shamir, "3 Laws":https://www.financialcryptography.com/mt/archives/000147.html, Turing Award Lecture.

[12] Gutmann & Grigg, "Security Usability," http://iang.org/ssl/j4cry.pdf, "Security & Privacy,":http://iang.org/ssl/j4cry.pdf, July/August 2005, IEEE.

[13] Jamie Beckett, "Virus-safe computing," http://www.hpl.hp.com/news/2005/apr-jun/virussafe.html, HP Labs.

[14] Ian Grigg, "The Market for Silver Bullets," http://iang.org/papers/market_for_silver_bullets.html Draft paper.