

## **A UBIQUITY INTERVIEW WITH STEPHEN COBB:**

### **Literature Scholar, Author, and Security Expert**

**UBIQUITY:** Tell us something about your website, [www.cobb.com](http://www.cobb.com).

**COBB:** We think of it as an old school website. It has been around for over ten years now and does a variety of things, covers a variety of topics, such as my professional and personal stuff, and so on, as well as Chey's stuff.

**UBIQUITY:** Chey Cobb is your wife, but who are some of these other Cobbs, like Mike Cobb and Erin Romfo Cobb?

**COBB:** Erin Romfo is our daughter, with a different last name than ours. Mike Cobb is my brother and he is heavily involved in computer security as well. Chey and Mike and I are all CISSPs, although I'm not sure if we actually hold the record for the most CISSPs in one family. Mike has also got several other qualifications, like qq, because he's probably more active in terms of day-to-day computer security work than I am. He and another friend of ours, Michael Miora, another CISSP/qq have an incident management product they've developed and are actively marketing right now.

**UBIQUITY:** What has your career in Internet security been like in recent years?

**COBB:** In 2004 Symantec purchased the anti-spam technology I'd been working on with several other guys, so after that happened I went to work for STSN, which is now iBAHN, the company that does high-speed internet for hotels such as the Marriot. I was their Chief Security Executive, but at the end of 2004 I decided to take some time off and give myself a sabbatical, and I got involved in a number of non-computer endeavors, such as real estate, and I've also gotten involved in some film work, which is actually very digital these days, since film is going digital. But on the security side I'm really just trying to take a step back and look at computer security from some new angles.

**UBIQUITY:** New angles such as what?

**COBB:** What I mean is that a lot of computer security, when I first got involved in it in late 80s and early 90s was kind of groundbreaking stuff. There was an opportunity to think about things that people hadn't considered before, and a lot of companies needed help and education. But now security is a part of any self-respecting enterprise, certainly in medium- to large-size companies, so a certain amount of security work has become repetitive. A fairly clear set of standards and principles have emerged about what you should and shouldn't be doing in order to protect your information. So in a sense we're largely in the implementation phase of security now, where people are applying the things that those of us who were involved early on kind of came up with. I hope that doesn't sound too self-serving, but there's an entire layer of people who started to think about security issues earlier than others, particularly in the areas of local area networking

personal computers. There was a history of security thinking in the mainframe world which was essentially caught flat-footed when PC networks took off, because PC networks, and then the Internet, are a very different beast from mainframe computers. And so as technology made the shift to distributed computing, security concerns and challenges changed. Then the emergence of the Internet and e-commerce created an environment where there was much more need for discrete security, which is where you are sharing a lot but not all of your information, and where's there's a lot more computer interactivity with the general public.

**UBIQUITY:** Where does that leave things today?

**COBB:** Today a lot of people shop and bank online, manage their retirement plans, investments, business expenses and so on. That requires controlled access to small parts of much larger collections of data. Those changes in behavior introduced challenges which really hadn't been addressed before, and now we're seeing that omission rectified. There's been a lot of good technology developed, including standards and principles for approaching security problems. But you get a bit tired of going out and giving the same message, time after time. And actually the message tends to be: Well we're making progress, but not enough progress, and it's not coming fast enough, because the bad guys are still out there trying to get in. The same message, over and over again. Tends to get boring, I'm afraid. But it's still very important, as the recent mega-breaches, like the veterans' data exposure, clearly indicate.

**UBIQUITY:** How would you rate the successful application of security procedures by different industries?

**COBB:** The telecommunications companies were probably right at the forefront, closely followed by big banks--particularly banks that do financial trading. And the telecom companies and the banks were followed by pharmaceutical companies. The latter started to pay attention when we pointed out that the 'negative value' of some data, such as personal health data, was potentially greater than the positive value of internal data, like product formulas. There is really no cap on the cost of exposing someone's health data, in terms of lawsuits, customer confidence, stock price, and so on. Some manufacturing companies have also been pretty good, but manufacturing companies tend to vary widely. Some large manufacturing companies now have very sophisticated systems in place, particularly for things like collaborative work and so on. Certain sectors -- for example FedEx and the delivery sector -- have some pretty good security in place. Whereas retail has generally not done as well, and higher education continues to be beset with problems.

**UBIQUITY:** Where are the problems with retail and with higher ed?

**COBB:** Quite a number of the big security breaches have occurred through various aspects of retail, from web sites to in-store system. I think that's because what has emerged as one of the main targets of value now is personal information. Personal information has evolved over the last five years into a saleable commodity, so retail became a very attractive avenue to go after that. Retailers tended to be focused on their

inventory and on proper accounting as far as computer security went, but paid much less attention the consumer information they were holding or processing.

**UBIQUITY:** You've explained these problems in many of the two dozen or so books you've written. Which of those many books are you most proud of?

**COBB:** I'd have to say the very first book I did on security, which came out in 1992, although I started on it in 1988. That was the Stephen Cobb Complete Guide to PC and LAN Security. I think it's generally accepted as the first attempt to look at PC and LAN security in depth and apply some systematic thinking to it. In that book I presented a layered approach to protection of PCs and LANs, and what was interesting is that when the book came out it really didn't sell well, at least not relative to some of my other books. For example, I did a book on Quattro Pro that sold 80,000 copies in the first quarter. Then I wrote a book on PC and LAN security, thinking it would sell even better because it would appeal to everybody, not just people who used one specific piece of software.

**UBIQUITY:** But apparently it didn't sell well?

**COBB:** No, it sold just a few thousand copies. And it was not until two years after the book came out that I got any reaction at all, and that was a request to speak at the 1994 Virus Bulletin conference. That's when I found that a lot of the people there knew me or knew my name from the book. So the book had not sold to the general public but other people in security had picked up a copy. And 1994 is when I met people like Dr. Richard Ford, who pretty much created the ICSA virus labs. He is now professor of computer science of the Florida Institute of Technology. At the same conference I also met Winn Schwartau, who wrote "Information Warfare," and later that year met Bob Bales, who headed the National Computer Security Association (NCSA), which later went on to become True Secure, headed by Dr. Peter Tippet. Bob Bales went on to create Pest Patrol, which was acquired last year by Computer Associates. I was also very fortunate at that time to meet Dr. Michel Kabay, whom I also met through NCSA. Mich now runs the Master of Science and Information Assurance program at Norwich University in Vermont where my wife and I have taught. I also met Michael Miora at that time because he was managing the consulting leads that the NCSA was getting, along with Vince Schiavone. With Michael and Vince and David Brussin we formed a company that became InfoSec Labs, which was acquired by Rainbow Technologies in 1999. The same group went on to form ePrivacy Group, which developed the Turntide anti-spam technology that Symantec acquired in 2004. And so there's kind of a network of you what you might call the "old guard."

**UBIQUITY:** Are you still in touch with them?

**COBB:** Yes, most of us are still in touch. I talk to Richard quite frequently, and Winn Schwartau and I recently went to Russia together to speak at Interop Moscow. My wife Chey Cobb was actually the NCSA's first webmaster so she got to know a lot of the firewall and antivirus people because NCSA was testing firewalls and antivirus

technology back then and posting the results on the website. Then They went on to work for the NRO, doing secret security stuff we can't talk about.

**UBIQUITY:** When you think of the "good guy" security people, is it a happy community or are they a contentious bunch?

**COBB:** I think it's a pretty happy community with a fairly large cast of well-known characters. We each of us have our foibles and idiosyncrasies, yet there is a good sense of camaraderie amongst those of us who have been in the business for awhile. I think the good guys still tend to see themselves as pulling together against the bad guys, especially when new problems come up. The advice you'll get on how to approach a particular security problem will typically not vary a great deal amongst the experts in the field now because we've been thinking about this stuff for a long time and have generally come to very similar conclusions. One of the areas which can be problematic is emerging threats. A good five years ago we proposed an approach to authenticating e-mails so that basically you could shut spammers out, but there are still arguments going on in that community about how exactly e-mail authentication should be carried out.

**UBIQUITY:** Some have suggested that the problem would best be solved by charging for e-mail, right?

**COBB:** Well, we suggested charging for e-mail back in 2001 and we developed a scheme for doing that which we presented to Microsoft and the other big email players. The problem with it is simply a business problem, in the sense that nobody wants there to be somebody else charging for e-mail. Since the Internet isn't owned or managed by any particular entity, Internet changes have to happen by consensus. One of the pushes to introduce authentication floundered because of concern over Microsoft making patent claims in the area. At one point we made a gesture to donate patentable technology to solve that problem, but there was then the possibility that some companies might still want to go and patent the collection of money for e-mail. It is such a juicy pie that you'll have a lot of arguments about it. And recall that back, in the nineteenth century, Westinghouse gave Tesla, who most of the original patents on AC electricity generation, a royalty contract of two dollars and fifty cents for every horsepower of AC equipment sold. That proved unsustainable as a business model and Tesla, basically for the good of the planet, let Westinghouse cancel the contract.

**UBIQUITY:** Well, what are the bad guys up to now?

**COBB:** I think the most significant aspect of bad guys today is that they are much badder than bad guys 10 or 15 years ago, when the primary motive for messing with computers was first of all curiosity, then some malice, whereas now a lot of it is the underground market in personal information for identity theft. I think the big problem now is that whatever interests are backing this activity are increasingly moneyed interests.

**UBIQUITY:** What are your thoughts on identify theft?

**COBB:** Identify theft certainly existed before online banking. People would steal checks, fake identifies, open bank accounts, and so on. The computer has really just become a facilitator of that, and it's also created a black market in identity data. You have the people that are out there trying to steal your personal data to resell it. And then people who are attempting to acquire personal data to abuse it. In addition to that, there's a marketplace for compromised systems, which could be then used for different forms of attack and for routing spam. Because most of us are now online all the time on broadband connections, there's a constant probing of those connections to find systems, compromise them, install back-doors so that you can then turn them into zombies for transmitting either phishing attacks or spam attacks.

**UBIQUITY:** What's keeping the problem from getting worse than it is?

**COBB:** Diligence on the part of security professionals. You know, the hiring rate for security professionals has been going up and up. The number of people who are certified, such as with the CISSP, have been going up and up. And there now are programs like Mich Kabay's Master of Science in Information Assurance at Norwich University, which is turning out very well-qualified information security managers with advanced degrees in the subject. But I don't see the problem going away, and defensive measure have to become more sophisticated. On top of that, it's my opinion that until there is an improvement in the general ethical level within society, computer security problems are going to continue to exist and get worse not better. At its root computer security is a people problem, not a technical problem. I'm very worried that we're not doing enough at a younger age in our school systems to teach kids about the ethics of intellectual property. In the first six months of 2005 something like 60 million personal records were exposed. And 2006 looks to set a new record.

**UBIQUITY:** What conclusion should we draw?

**COBB:** Well, if everybody's data gets exposed, the question is: what does that do to the value of data. The result in a sense is the devaluing of data. And one area where this impacts security is shared secrets, a standard technique still used for control of access to discrete data, things like your password, your pin, your mother's maiden name, favorite color, and so on and so forth. All of us have a limited number of unique attributes and if that data keeps getting exposed, our ability to maintain the privacy of our information under current systems, well it pretty much disappears. Plus, as more and more of our information is exposed, we have less and less of it protected. It's out there. And people generally don't like their information being out there. But for 60 million people last year it was out there without their permission, and that's not a very nice feeling. There's plenty of evidence to suggest that these involuntary exposures of information impose a drag on the growth of e-commerce. There are plenty of statistics out there to show that there's a portion of the population that's still worried about the Internet and still doesn't shop online and still doesn't bank online and so on. In any case, I certainly feel that ethical standards are really the key to long-term improvement in computer security.

**UBIQUITY:** Give us some information, voluntarily, about the Cobbs.

**COBB:** Sure. The Cobb family that I come from was already well established in Kent in England in the thirteenth century. I've actually participated in some DNA studies which indicate that many if not most of the Cobbs in America came from that family. Going back the other way, it looks like the Cobbs came to Kent during the post-Roman Saxon invasions.

**UBIQUITY:** Are you related in any way to the baseball legend Ty Cobb ?

**COBB:** Actually, yes. If you go back seven generations on my tree and then over and then back up there's Ty Cobb . Yes. But my interest in other Cobbs is not to find out if I'm related to any rich ones or famous ones, it's more an interest in how societies and peoples develop. A lot of people tend to assume that if they talk to somebody with the same last name but don't know actually know of any immediate relatives they have in common then they must be from different families. Well, that may be the case with some names, but it's clearly emerging from these DNA studies that most of the Cobbs in America come from this one family and it could be true of many others. It seems plain to me that, if you take DNA backwards in time far enough then we are all of us related and we all come from pretty much the same original stock. To me, race is a completely artificial distinction between people, and from a DNA point of view that is being shown to be the case.

**UBIQUITY:** Our time is almost up. Let's close on a quick recitation of your intellectual history.

**COBB:** Back in the seventies I did a joint honors degree in English and comparative religion at Leeds University in England, and then started a master's degree in comparative religion at McMaster University in Canada. I also started a PhD in English at Sussex University in England. But then the first oil crisis of the 70's essentially cut off the funding for anything exotic like comparative religion (although if more governments had stuck with the subject back then we might not be in such deep inter-faith turmoil today). Anyway, I just kind of scrambled to find what work I could and got involved in banking, which is where I started to learn about computers. Then I was hired by the state of North Dakota as a chief oil and gas tax auditor and that's where I started to learn about fraud and the abuse of computers. It was an interesting part of my development because I actually learned about computers in the context of developing programs to detect tax fraud. Although I went through a phase where the books I was writing were really manuals to help people use computer applications, such as how to use a spreadsheet or how to use a word processor and so on, when I started to do network installations for IBM in 1985, I could immediately see that when you take two personal computers and connect them together you have a whole new range of issues and opportunities for abuse. I happened to do consulting at that point to some people who had computers stolen and lost data so by the late 80s I was very interested in security and started writing a book which came out in '92. From then it was really a question of learning on the job through consulting contracts.

**UBIQUITY:** Has your perspective on information security changed much over the years?

**COBB:** I still find information security very challenging and very interesting, but I'm now trying to look at it from several steps removed and within a broader context -- within the context of society, within the context of economics, and within the context of values. Because it seems clear that society's values have a big influence on the actions that people take and what actions are tolerated in society. So when you beat your head against the wall trying to solve a problem like spam at some point you have to step back and ask yourself, "Wait a minute, why are all these people still doing this? Exactly what is going on here?" Questions like that are what I'm thinking about and writing about at the moment.

[END]

Source: Ubiquity, Volume 7, Issue 26 (July 19, 2006 - July 26, 2006)  
<<http://www.acm.org/ubiquity/>>.