



Improving Security: What hackers don't want you to know

May 2007

Executive summary – Hacker techniques continue to evolve. Are the "good guys" keeping up? Many myths and misconceptions pervade the IT industry and create vulnerabilities in critical infrastructures. And there are new issues around Bluetooth hacking, Web 2.0 vulnerabilities, weaknesses in biometric technology and radio-frequency identification (RFID) exposures. Understanding the risks and taking a few simple steps can help you avoid getting hacked, even as the IT environment becomes more complex.

In this Executive Technology Report, Peter Andrews interviews Jeff Crume, who works as IBM executive IT security architect in Raleigh, NC. He is primarily involved with supporting the Tivoli security software. He is the author of "Inside Internet Security: What Hackers Don't Want You to Know."

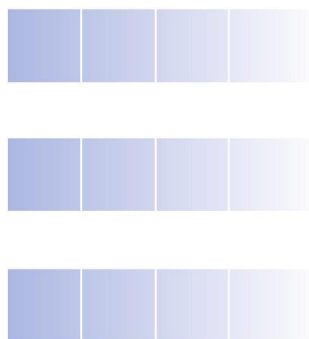
Peter Andrews: I know that your interests in security extend to the activities of hackers. Could you say a bit about what you have been doing to understand and counter them?

Jeff Crume: My "day job" deals with trying to help customers build architectures that are secure, which involves mostly identity and access management technologies. My "hobby" is keeping up with the latest hacking trends because: 1) it's interesting to me and 2) it helps me do better in my day job by being more aware of what I'm up against.

Peter Andrews: Tell me about some of the misconceptions people have about hacking.

Jeff Crume: There are many. So many that I wrote a book about them called *Inside Internet Security: What Hackers Don't Want You to Know*. In the book, each chapter is basically dedicated to a myth or misconception that seems to pervade the industry. It's easier for the "bad guys" to do their job if the "good guys" keep believing stuff that isn't true.

One common myth is that all the "bad guys" are "out there" – meaning they are on the other side of the firewall and, if we can just do a good enough job of keeping them out, that we will be safe. The truth is that a significant number of attacks are inside jobs – either by current or former employees who have either misused the privileges they have been given or whose access rights have not been removed in a timely fashion.





Maybe one of the biggest myths is that an operational computing system can be made invulnerable to attack. The truth is that any system can be broken into if an attacker is sufficiently motivated and given enough time. Our job then is not to have perfect security with no risks (because that can't happen), but rather to have adequate security for the task at hand and take prudent risks that we can tolerate.

All the time I see architectures that fail to provide means for protecting sensitive resources once an attacker penetrates the outer defenses. It means that if the hacker can get past the front door (metaphorically speaking), then there is little left to keep him from stealing the keys to the kingdom – and if that hacker happens to be an employee, then getting past the front door is trivial.

Peter Andrews: Could you tell me about the consequences of such a security breakdown?

Jeff Crume: Since I'm on the presales architecture side, I usually am spared the task of seeing the "train wreck" after it happens. However, all you have to do to get a taste is to follow the trade press and see how every week break-ins are being reported where the identities of tens of thousands of customers have been compromised. Most of these happen as a result of stolen laptops, but a significant number are the result of break-ins at a computing level.

Peter Andrews: How do you possibly restore order after this has happened?

Jeff Crume: Since my work focuses on prevention rather than remediation, I'm probably not the best person to say. But I do know that there are a growing number of regulations that specify, to some extent, what actions an organization must take. For instance, the 30-some-odd, state-by-state disclosure laws require that the organization notify all its employees/members/customers whose data might have been compromised.

The best way to prevent this in the first place is to ensure that you have adequate access controls in place, a good system for granting and removing privilege levels (provisioning/deprovisioning), good encryption of sensitive data and a means for monitoring it all so that you know when a breach has occurred.

Peter Andrews: Are the people you work with highly motivated to get this right? Or does it seem to some to be too much of a bother?

Jeff Crume: I see both types all the time. The ones who are the most motivated are the ones who have the threat of regulatory noncompliance hanging over their heads. The Sarbanes-Oxley Act (U.S. accounting regulations) has done more to provide this level of motivation than anything because it holds corporate officers personally responsible for failure to ensure that adequate internal controls are in place. When your CEO might go to jail, the organization tends to put that at the top of the priority list.





Peter Andrews: Any advice on handling those who are less engaged?

Jeff Crume: (The) best thing might be the judicious use of "war stories" – trade press articles about the consequences that other organizations have faced when they failed in this area – and there is more than ample supply of such evidence.

Peter Andrews: That brings up the people aspect of security. I know that "social engineering" is a big problem, as is training. Do you get involved in these aspects?

Jeff Crume: I don't, but I do cover it in the book. It's a huge problem because no matter how good you lock down the infrastructure, people are almost always the weakest link and will continue to be so until we develop a firewall for the human mind – and I'm not holding my breath on that one. :-) Inadequate training is a big contributor to the problem.

Security departments just end up saying "no" to everything rather than explaining why. Security awareness training needs to be more than a few posters or slogans. It needs to involve real education.

The other thing is that technicians need to be more sensitive to the needs of the user community. It doesn't matter how secure they think they have made a system if they have made the users' jobs so untenable that they feel compelled to violate the policy in order to get their work done.

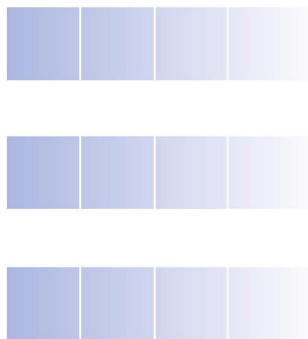
Single sign-on (SSO) is a great example. Telling users they have to keep up with a dozen different, hard-to-guess (therefore, hard-to-remember) passwords that must be changed every 60 days doesn't ensure that security will be better. The only thing it guarantees is that people will write passwords down – and they will invariably put these password lists in conspicuous places, thereby making security even worse than if a looser password policy were to be allowed.

I'm not advocating for "anything goes" when it comes to password selection, but it's important not to fall into the trap of a false sense of security that many security departments end up in. Single sign-on, however, makes life easier for users without compromising security (if it's done correctly). That means a win-win for everyone.

Peter Andrews: Is there a step by step that allows them to explore their users' needs and accommodate them? Or some rules of thumb?

Jeff Crume: I think the main things are to make security awareness training an ongoing activity that is more than just posters and slogans on pens, but involves some compelling, interesting education on what the risks really are. This CAN be done in an entertaining way, but rarely is.

The training should focus not only on the "thou shalt nots," but also on the "whys." You will never be able to come up with enough rules that will handle all situations, and even if you could, users couldn't possibly be expected to remember them all. So the focus should be on the underlying principles that make for secure behaviors.





Peter Andrews: Shifting topics a bit, could you talk about some of the new technologies, like biometrics, and how they might provide (or not provide) some answers?

Jeff Crume: Sure. Biometrics can be a blessing or a curse. The problem is that most people don't really understand them. That's why a big part of my presentation at the Technical Leadership Exchange is dedicated to trying to dispel some of these prevailing myths. Biometrics are not necessarily more secure than other means of authentication. They may be more secure – or they may be less secure – depending upon how they are implemented. All we know for sure is that they are more expensive in terms of initial, up-front costs.

Peter Andrews: Any practical hints? Questions to ask?

Jeff Crume: Too many to enumerate here, but one of the things off the top of my head that is worth considering is what is the organization's tolerance for false positives (incorrectly identifying someone as you that isn't you) and false negatives (incorrectly saying you aren't you)?” Unlike passwords, which either match or don't in a very deterministic way, biometrics are much fuzzier and probabilistic in nature.

You have to decide how much error you can tolerate in either direction, and the answer will vary from organization to organization and, sometimes, even from application to application.

Biometrics, when used alone for authentication, are really more of a convenience factor than a security factor. (You don't forget to bring your thumb with you). If you really care about security, you will use a biometric as part of a multi-factor authentication system that also requires that the user present something they know (e.g. password) and/or have (e.g. smart card) in addition to the thing that they are (e.g. biometric).

Fraud detection and data mining efforts have similar probabilistic characteristics in that you are looking for needles in fields of haystacks. Lots of false positives and false negatives are the result if you get it wrong. And it's really hard to get it right unless you have a very well-defined behavior you are looking for.

Peter Andrews: The message is "proceed with caution!" eh?

Jeff Crume: Definitely. Don't assume that more technology always equals more security. Sometimes it does and sometimes it doesn't.

Peter Andrews: Do some of the new technologies, like Web 2.0 applications, put us at more risk?

Jeff Crume: Definitely. Web 2.0 leverages a lot of client side, mobile code (a.k.a. active scripting) such as Java, Javascript, AJAX, etc. It's always a risk when users have code running on their systems that they didn't explicitly ask to have installed and have no way to verify its veracity.



It's a myth that just by visiting a web site that you can't get hacked. There are loads of attacks that rely on browser vulnerabilities (and there are many regardless of the browser you choose) to break out of the "sandbox" and have free reign on the user's system with the highest level of privilege.

I'm not saying don't do Web 2.0, but I am saying that you should do it with your eyes open and know what the risks are and try to mitigate the ones that you can.

Peter Andrews: OK, short of cutting my cables, what can I, as a user, do to minimize my risks? Do you have a few essential recommendations?

Jeff Crume: There are many. (By the way, I don't recommend cutting the cables, but it certainly would reduce the risks.)

1. Run a good antivirus scanner and make sure it gets updated with new signatures every day (if possible).
2. Run a good personal firewall on every workstation, laptop, etc., and be cautious about which applications you allow to access the Internet. (Don't just grant permission to every application that asks for it – if you don't think that application needs to "phone home," then deny it access.)
3. Don't open e-mail attachments unless you know what they are and what they are going to do. It doesn't matter if it appears to be coming from the person you trust most in this world because the source address could be spoofed, or that person's system could have been compromised.
4. Don't run ActiveX/Javascript/Java in your browser by default if you can avoid it. Firefox, for instance has a plug-in (NoScript) that lets you easily turn scripting on and off on a site-by-site basis. This way, you can turn it on for the sites that you trust and leave it off by default for the ones you don't.
5. Always, always, always keep a good back up. There's no such thing as perfect security, so you need a back up or you're doing a high-wire act without a net.
6. Secure your home LAN (local area network), especially if it has wireless capability. Turn on 128-bit encryption and change the default SSID to something else that a hacker wouldn't easily guess.
7. Stay current with patches, especially to key components like the operating system, browsers, e-mail clients, productivity applications like word processors, etc. This is very, very important and not that hard to do these days with the automated mechanisms available.

Again, there are many more, but if most folks would do that, it would go a long way.

Peter Andrews: Great suggestions! Looking forward again, what are the emerging vulnerabilities or hacker strategies?

Jeff Crume: I think biometrics and Web 2.0 are two of the more interesting ones we've already discussed. Others involve the pervasive nature of computing. What used to only be on mainframes in raised-floor rooms behind badge readers and



locked doors in the 70s-80s has made its way to PCs and laptops in the 90s – and now is moving to handheld devices like PDAs and phones, which are highly portable, easy to steal and easy to compromise.

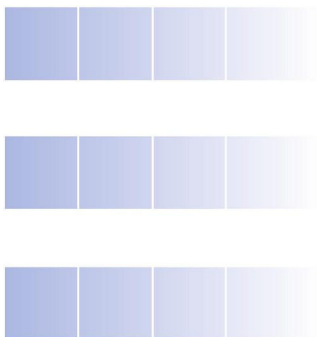
Another is the pervasive nature of wireless technology such as Bluetooth, WiFi and RFID. All potentially extend the range of an attacker and potentially expose sensitive information in ways that most people haven't even thought of.

Peter Andrews: Without giving too much away, what are the approaches and strategies for keeping up or getting ahead of the hackers?

Jeff Crume: Basically it is to understand what the fundamental themes are in making systems secure. That's what the focus on my book was about – rather than trying to chase every new attack, figure out what the repeatable patterns are and get to the root of defending against those. The variations keep changing, but the underlying themes haven't changed over time.

My Lotus QuickPlace (<http://extranet1.lotus.com/crume>) has links to info on the book, as well as links to some of the better IBM Redbooks and white papers on security management and IBM's products in that space.

Technology to watch
Internet Security
Web 2.0
Biometrics
Radio-frequency identification





Further Reading

Books

Inside Internet Security: What Hackers Don't Want You To Know by Jeffrey Crume. http://www.amazon.com/Inside-Internet-Security-What-Hackers/dp/0201675161/ref=pd_bbs_sr_1/103-1145266-2427008?ie=UTF8&s=books&qid=1178628582&sr=8-1

Articles

Inside Internet Security

https://extranet1.lotus.com/QuickPlace/crume/Main.nsf/h_Toc/443b02fc33b8ae8485256b0b004b2382/?OpenDocument

Enhancing security and privacy in biometrics-based authentication systems

<http://researchweb.watson.ibm.com/journal/sj/403/ratha.pdf>

Biometrics for secure border management

http://t1d.www-03.cacheibm.com/industries/government/doc/content/bin/Border_Management_Biometrics_July05_2.pdf

Wikipedia: Biometrics <http://en.wikipedia.org/wiki/Biometrics>

IBM Tivoli security management solutions

<http://www-304.ibm.com/jct03002c/software/tivoli/solutions/security/>

What Is Single Sign-On? <http://www.authenticationworld.com/Single-Sign-On-Authentication/>

IBM Tivoli Access Manager for Enterprise Single Sign-On V6.0

http://www-306.ibm.com/common/ssi/OIX.wss?DocURL=http://d03xhttpcl001g.boulder.ibm.com/common/ssi/rep_ca/2/897/ENUS206-332/index.html&InfoType=AN&InfoSubType=CA&InfoDesc=Announcement+Letters&panelurl=&paneltext=

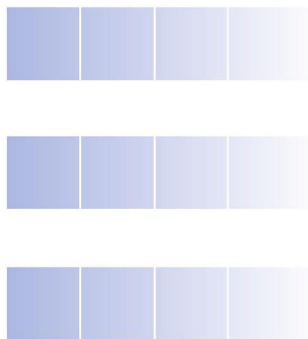
Social Engineering Fundamentals <http://www.securityfocus.com/infocus/1527>

"Methods of Attack" (excerpt from High-Assurance Design: Architecting Secure and Reliable Enterprise Applications)

<http://www-128.ibm.com/developerworks/rational/library/feb06/reader/excerpt.html>

Ethical Hacking <http://researchweb.watson.ibm.com/journal/sj/403/palmer.html>

Wikipedia: Web 2.0 http://en.wikipedia.org/wiki/Web_2.0





About this publication

Executive Technology Report is a monthly publication intended as a heads-up on emerging technologies and business ideas. All the technological initiatives covered in *Executive Technology Report* have been extensively analyzed using a proprietary IBM methodology. This involves not only rating the technologies based on their functions and maturity, but also doing quantitative analysis of the social, user and business factors that are just as important to its ultimate adoption. From these data, the timing and importance of emerging technologies are determined. Barriers to adoption and hidden value are often revealed, and what is learned is viewed within the context of five technical themes that are driving change:

Knowledge Management: Capturing a company's collective expertise wherever it resides – databases, on paper, in people's minds – and distributing it to where it can yield big payoffs

Pervasive Computing: Combining communications technologies and an array of computing devices (including PDAs, laptops, pagers and servers) to allow users continual access to the data, communications and information services

Realtime: "A sense of ultracompressed time and foreshortened horizons, [a result of technology] compressing to zero the time it takes to get and use information, to learn, to make decisions, to initiate action, to deploy resources, to innovate" (Regis McKenna, *Real Time*, Harvard Business School Publishing, 1997.)

Ease-of-Use: Using user-centric design to make the experience with IT intuitive, less painful and possibly fun

Deep Computing: Using unprecedented processing power, advanced software and sophisticated algorithms to solve problems and derive knowledge from vast amounts of data

This analysis is used to form the explanations, projections and discussions in each *Executive Technology Report* issue so that you not only find out *what* technologies are emerging, but *how* and *why* they'll make a difference to your business. If you would like to explore how IBM can help **you** take advantage of these new concepts and ideas, please contact us at insights@us.ibm.com. To browse through other resources for business executives, please visit

ibm.com/services

Executive Technology Report is written by Peter Andrews, Consulting Faculty, IBM Advanced Business Institute, and is published as a service of IBM Corporation. Visit

ibm.com/abi





Copyright ©1999-2007 IBM Corporation. All rights reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

G510-6620-00

