Feed Journal

Issue #7 for AUEB CIS 4/27/2011 - 5/1/2011 feedjournal.com

Why We Need An Open Wireless Movement

(EFF.org Updates)

Submitted at 4/27/2011 5:20:42 PM

If you sometimes find yourself needing an open wireless network in order to check your email from a car, a street corner, or a park, you may have noticed that they're getting harder to find.

Stories like the one over the weekend about a bunch of police breaking down an innocent man's door because he happened to leave his network open, as well as general fears about slow networks and online privacy, are convincing many people to password-lock their WiFi routers.

The gradual disappearance of open wireless networks is a tragedy of the commons, with a confusing twist of privacy and security debate. This essay explains why the progressive locking of wireless networks is harmful — for convenience, for privacy and for efficient use of the electromagnetic spectrum.

We will need a political and technological "Open Wireless Movement" to reverse the degradation of this indispensable component of the Internet's infrastructure. Part of the task will simply be reminding people that opening their WiFi is the socially responsible thing to do, and explaining that individuals who choose to do so can enjoy the same legal protections against liability as any other Internet access provider. 1 Individuals, including Bruce Schneier and Cory Doctorow, have laid some of the groundwork. It's time to spead the message far and wide.

But an Open Wireless Movement will also need to do technical work: we need to build new technologies to ensure that people have an easy way to share a portion of their bandwidth without affecting the performance of their own network connections while at the same time ensuring that there is absolutely no privacy downside to running an open wireless network. The wireless world we ought to live in

Most of us have had the experience of tremendous inconvenience because of a lack of Internet access. Being lost in a strange place with no way to find a map; having an urgent email to send with no way to do so; trying to meet a friend with no way to contact them. Even if we have data plans for our mobile phones, we've probably had these experience in cities or countries where our phones don't have coverage or don't have coverage for less-than-extortionate prices. We may even experience this problem at home, when our Internet connection dies while we urgently need to use it.

Finding yourself in one of these binds is a bit like finding yourself parched and thirsty while everyone around you is sipping from nice tall glasses of iced water, or finding yourself cold and drenched in a rain storm because nobody will let you under their umbrella. At those moments when you are lost, or missing a deadline, or failing to meet your friend, it is almost always true that Internet data links are traveling through your body in the form of electromagnetic wireless signals — it's just that people have chosen to lock those networks so that you can't make use of them. A tragedy of the commons

When people turn on WEP or WPA encryption for their networks deliberately, there are two common reasons: a desire to prevent their neighbors from "free riding" on their connections; and a fear that unencrypted WiFi is a security or privacy risk. Both of those reasons have a degree of legitimacy, but neither of them changes the fact that we would be better off if there were more open networks. Also, both of these problems could be solved without password locking our networks. What we need, instead, is to develop and deploy better WiFi protocols.

Let's focus on the first issue for a moment: traffic prioritization.

Many people would like to have the fastest network connection possible, and for that reason are reluctant to let their neighbors share their link. After all, if your neighbor is streaming music or watching YouTube videos on your WiFi, that's going to slow your traffic down a bit! But those same people would probably be willing to give up some bandwidth at home from time to time, in exchange for having free open wireless everywhere else. In other words, we'd all be better off if we all left our WiFi open, but we each benefit slightly if we close our WiFi. Our failure to work together prevents us from enjoying better, more widespread Internet access.

The best solution to this problem is to have WiFi routers which make it very easy to share a certain amount of bandwidth via an open network, but simultaneously provide an encrypted WPA2 network that gets priority over the open network. Some modern routers already support multiple networks like this, but we need a very simple, single-click or default setting to get the prioritization right. Securing the Future for Open WiFi

If the problem of open WiFi was just about convincing people to share their connections, we'd be in a better situation. Enough people understand the importance of sharing that we'd have open networks more or less everywhere.

The problem that's really killing open WiFi is the idea that an unlocked network is a security and privacy risk.

This idea is only partially true. Computer security experts will argue at great length about whether WEP, WPA and WPA2 actually provide security, or just a false sense of security. Both sides are partially correct: none of these protocols will make anyone safe from hacking or malware (WEP is of course trivial to break, and WPA2 is often easy to break in practice), but it's also true that even a broken cryptosystem increases the effort that someone nearby has to go to in order to eavesdrop, and may therefore sometimes prevent eavesdropping.

It doesn't really matter that WiFi encryption is a poor defense against eavesdropping: most computer users only understand the simple message that having encryption is good, so they encrypt their network. The real problem isn't that people are encrypting their WiFi: it's that the encryption prevents them from sharing their WiFi with their friends, neighbours, and strangers wandering past their houses who happen to be lost and in need of a digital map. We need WiFi that is open and encrypted at the same time!

Insofar as there is some privacy (and psychological) benefit to using an encrypted WiFi network, there's actually no reason why users of open wifi shouldn't get those benefits too!

There is currently no WiFi protocol that allows anybody to join the network, while using link-layer encryption to prevent each network member from eavesdropping on the others. But such a protocol should exist. There are some technical details to work through, but they are manageable. 2

In fact, this proposed protocol offers some privacy/security benefits not available in shared-passphrase WPA2, which is the strongest easy-to-deploy WiFi encryption system. Under WPA2 all the users on the network can calculate each others' session keys and eavesdrop on each other. With our suggested design, that would cease to be possible. The Unintuitive Benefits of Open Wireless

Since 1994, the United States government has auctioned off huge portions of the electromagnetic spectrum to telecommunications companies. WiFi operates in tiny scraps of spectrum that were left over from the auctions. Similar processes have occurred in many other countries.

But WiFi networks (especially modern 802.11N networks) turn out to make inherently much more efficient use of spectrum than systems of widely spaced cell phone towers. This results from a property of wireless protocols called area spectral efficiency: basically, if your data only has to travel to a nearby router, the same frequency range can be used for someone else's data around the corner or across the street. In contrast, if your data needs to travel all the way to a cell tower, nobody else in between can use that same portion of spectrum.

If we want a future where anyone can watch high definition movies or make video calls from anywhere without wires, what we need is short-range networks with routers everywhere — like the one we'd have if everyone opened their WiFi. What Needs to be Done

EFF will be working with other organizations to launch an Open Wireless Movement in the near future. In the mean time, we're keen to hear from technologists with wireless expertise who would like to help us work on the protocol engineering tasks that are needed to make network sharing easier from a privacy and bandwidth-sharing perspective. You can write to us at openwireless@eff.org.

• 1. If you run an open wireless network, you may be able to receive significant legal protection from Section 230 of the CDA(against civil and state criminal liability for what others publish through the service) and Section 512 of the DMCA(against copyright claims based on what others use the service for). While these protections are not complete, EFF regularly engages in impact litigation to help ensure that these laws offer as strong protection to network operators as possible.

• 2. That kind of wireless network could use asymmetric cryptography to generate secret session keys for each user. The main challenge with this design is how to prevent man in the middle attacks. Wireless routers do not have canonical names, so they cannot be issued certificates in the same way that, say, TLS encrypted websites are. A feasible alternative is the trust-on-first-use design employed by SSH: the first time you connect to a wireless network, you might have to assume that the router's key is correct, but you will be notified if ever changes (which would mean that there is a new router, or the beginning or end of a man-in-the-middle attack). If you can actually see the router, you don't have to assume that the key is correct because you can check it against a number on the box itself. For other users, the security could be improved by using GPS, or some other means of remembering not only the keys of each router but also whether it was expected to be present in a given location

New FBI Documents Provide Details on Government's Surveillance Spyware

(EFF.org Updates)

Submitted at 4/29/2011 5:53:24 PM

EFF recently received documents from the FBI that reveal details about the depth of the agency's electronic surveillance capabilities and call into question the FBI's controversial effort to push Congress to expand the Communications Assistance to Law Enforcement Act (CALEA) for greater access to communications data. The documents we received were sent to us in response to a Freedom of Information Act (FOIA) request we filed back in 2007 after Wired reported on evidence that the FBI was able to use "secret spyware" to track the source of e-mailed bomb threats against a Washington state high school. The documents discuss a tool called a "web bug" or a "Computer and Internet Protocol Address Verifier" (CIPAV), 1 which seems to have been in use since at least 2001. 2

What is CIPAV and How Does It Work?

The documents discuss technology that, when installed on a target's computer, allows the FBI to collect the following information:

- IP Address
- Media Access Control (MAC) address
- "Browser environment variables"
- Open communication ports
- List of the programs running
- Operating system type, version, and serial number
- Browser type and version
- Language encoding
- The URL that the target computer was previously connected to
- Registered computer name
- Registered company name
- Currently logged in user name
- Other information that would assist with "identifying computer users, computer software installed, [and] computer hardware installed" 3

It's not clear from the documents how the FBI deploys the spyware, though Wired has reported that, in the Washington state case, the FBI may have sent a URL via MySpace's internal messaging, pointing to code that would install the spyware by exploiting a vulnerability in the user's browser. Although the documents discuss some problems with installing the tool in some cases, other documents note that the agency's Crypto Unit only needs 24-48 hours to prepare deployment. 4 And once the tool is deployed, "it stay[s] persistent on the compromised computer and . . . every time the computer connects to the Internet, [FBI] will capture the information associated with the PRTT [Pen Register/Trap & Trace Order]. 5

Where Has CIPAV Been Used and What Legal Process Does the FBI Rely On to Use It?

It is clear from the documents we received that the FBI—and likely other federal agencies—have used this tool a lot. According the documents, the FBI has used CIPAV in cases across the country—from Denver, El Paso, and Honolulu in 2005; to Philadelphia, California, and Houston in 2006; to Cincinnati and Miami in 2007. In fact, one stack of documents we received consists entirely of requests from FBI offices around the country to the agency's Cryptologic and Electronic Analysis Unit ("CEAU") for help installing the device. 6

The FBI has been using the tool in domestic criminal investigations as well as in FISA cases, 7 and the FISA Court appears to have questioned the propriety of the tool. 8 Other agencies, and even other countries have shown interest in the tool, indicating its effectiveness. Emails from 2006 discuss interest from the Air Force, 9 the Naval Criminal Investigative Service 10 and the Joint Task Force-Global Network Operations, 11 while another email from 2007 discusses interest from the German government. 12

The FBI's Crypto Unit appears to have viewed the CIPAV as a proprietary tool. In one email, an agent grumbled, "we are seeing indications that [CIPAV] is being used needlessly by some agencies, unnecessarily raising difficult legal questions (and a risk of suppression without any countervailing benefit)." 13 In another email, an agent stated, "[I] am weary [sic] to just hand over our tools to another Gov't agency without any oversight or protection for our tool/technique." 14 And a third email noted, "[w]e never discuss how we collect the [data CIPAV can collect] in the warrants/affidavits or with case agents. AUSAs, squad supervisors, outside agencies, etc." 15

It appears from the documents that the FBI wasn't sure what legal process to seek to authorize use of the spyware device. Some emails discuss trying to use a "trespasser exception" to get around a warrant, 16 while others discuss telling the AUSA (government attorney) to cite to the "All Writs Act, 28 U.S.C. § 1651(a)." 17 And one email suggests some agents thought the tool required no legal process at all. In that email, the FBI employee notes he considers the tool to be " consensual monitoring without need for process; in my mind, no different than sitting in a chat room and tracking participants' on/off times; or for that matter sitting on P2P networks and finding out who is offering KP." 18

Eventually, the FBI seems to have sought a legal opinion on the proper use of the tool, both from the Office of General Counsel and from the National Security Law Branch, 19 and ultimately, the agency seems to have settled on a "two-step request" process for CIPAV deployments -- a search warrant to authorize intrusion into the computer, and then a subsequent Pen/Trap order to authorize the surveillance done by the spyware. 20

What Does This Mean for the FBI's Push for New Back Doors into Our Internet Communications?

Over the past few months, we've heard a lot from the FBI about its need to expand the Communications Assistance to Law Enforcement Act (CALEA), a law that that requires all telecommunications and broadband providers to be technically capable of complying with an intercept order. Federal law enforcement officials have argued that under current regulations they can't get the information they need and want to expand CALEA to apply to communications systems like Gmail, Skype, and Facebook. However, these documents show the FBI already has numerous tools available to surveil suspects directly, rather than through each of their communications service providers. One heavily redacted email notes that the FBI has other tools that "provide the functionality of the CIPAV [text redacted] as well as provide other useful info that could help further the case." 21 Another email notes that CIPAVs are used in conjunction with email intercepts, perhaps using similar spyware-type tools. 22 If the FBI already has endpoint surveillance -based tools for internet wiretapping, it casts serious doubt on law enforcement's claims of " going dark."

A device that remains "persistent" on a "compromised computer" is certainly concerning. However, if the FBI obtains a probable cause-based court order before installing tools like CIPAV, complies with the minimization requirements in federal wiretapping law by limiting the time and scope of surveillance, and removes the device once surveillance concludes, the use of these types of targeted tools for Internet surveillance would be a much more narrowly tailored solution to the FBI's purported problems than the proposal to undermine every Internet user's privacy and security by expanding CALEA. We will continue to report on both the FBI's use of endpoint surveillance tools and on the agency's push to expand CALEA as more documents come in.

Click here to access full pdf versions of the documents we received or see below for the pages referenced in this post.

- 1. FBI_CIPAV_01 p.26
- 2. FBI_CIPAV_09 p.3
- 3. FBI_CIPAV_07 pp.10-11
- 4. FBI_CIPAV_07 p.50
- 5. FBI_CIPAV_08 p.67
- 6. FBI_CIPAV_10
- 7. FBI_CIPAV_07 p. 45, FBI_CIPAV_08 p.132, 143
- 8. FBI_CIPAV_14 p.52
- 9. FBI_CIPAV_08 p.20
- 10. FBI_CIPAV_09 p.21-22
- 11. Id.
- 12. FBI_CIPAV_08 p.9
- 13. FBI_CIPAV_05 p.1
- 14. FBI_CIPAV 09 p.21
- 15. FBI_CIPAV_07 pp.11
- 16. FBI_CIPAV_08 p.29
- 17. FBI_CIPAV_08 p.149
- 18. FBI_CIPAV_14 p.36."KP" is likely a reference to " kiddie porn."
- 19. FBI_CIPAV_14 p.42, 62
- 20. FBI_CIPAV_08 p.169
- 21. FBI_CIPAV_08 p.168
- 22. FBI_CIPAV_08 p.143

Playstation data for sale?

(Securelist / Blog)

Submitted at 4/29/2011 9:10:39 AM

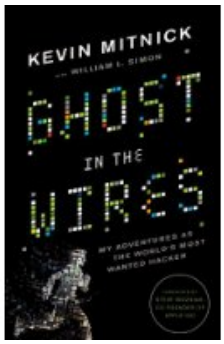
In the past few days we have read about how the Playstation Network has been hacked, and very sensitive information such as credit card information has been stolen. We are now seeing more activity in the underground community.

According to a forum post at PSX-scene rumors are spreading that the stolen information also includes the CCV2 numbers. A user on the underground forum Darkode says that the format of the stolen data would supposedly be: fname, lnam, address, zip, country, phone, email, password, dob, ccnum, CVV2, exp date But In a statement from Sony on their playstation-blog they write that the hacker does not have access to the CCV2 code, the statement follows:"Although we are still investigating the details of this incident, we believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/ Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and billing address (city, state, zip), and your PlayStation Network/Qriocity password security answers may have been obtained. If you have authorized a sub-account for your dependent, the same data with respect to your dependent may have been obtained. While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility. If you have provided your credit card data through PlayStation Network or Qriocity, out of an abundance of caution we are advising you that your credit card number (excluding security code) and expiration date may have been obtained." The question is who is correct? I would recommend everyone with a PSN account to request a new card from your bank, and if you use the same password for Facebook, MSN, email or forums that you used on the PSN I would recommend thatyou change it on those other sites.

Early Review of Ghost in the Wires

by Richard Bejtlich (TaoSecurity)

Submitted at 4/30/2011 9:09:00 PM



Kevin Mitnick was kind enough to send me a galley copy of his upcoming autobiography Ghost in the Wires. Amazon.com won't let me post a review yet, so I'll write what I would have supplied to the site.

In 2002 I reviewed Kevin Mitnick's first book, The Art of Deception. In 2005 I reviewed his second book, The Art of Intrusion. I gave both books four stars. Mitnick's newest book, however, with long-time co-author Bill Simon, is a cut above their previous collaborations and earns five stars.

As far as I can tell (and I am no Mitnick expert, despite reading almost all previous texts mentioning him), this is the real deal. Mitnick addresses just about everything you might want to know about. For me, the factor that made the book very unique was the authors' attention to detail. This sounds like it might have been a point of contention between the co-authors, but I found the methodical explanation of the social engineering and technical attacks to be relevant and interesting. Mitnick just doesn't say he social engineered a target; rather, he walks you through every step of the event! It's amazing, audacious, and in many cases beyond the pale.

One surprise for me was the amount of technical hacking Mitnick describes. He wasn't just crafty with a phone; he spent a lot of time at the keyboard executing technical exploitation of Unix variants. Interestingly, this may or may not include the so-called "Mitnick attack" whereby Tsutomu Shimomura's computer suffered the only documented TCP blind spoofing incident. In Ghost in the Wires, Mitnick says an Israeli hacker nicknamed JSZ wrote the code to implement the attack, and JSZ executed the Christmas Day 1994 exploitation of Shimomura's computer (p 326). Later on p 334, however, Mitnick notes the same attack worked against a different target (blackhole dot inmet dot com), so he may have executed that previously undocumented incident himself?

Ghost in the Wires also shares the human side of Mitnick's story. His description of solitary confinement and his anxiety of returning to those conditions seemed very real. They appear ever more relevant given recent treatment of Bradley Manning. One has to wonder about "cruel and unusual punishment" of those who are not convicted, such that they will sign plea deals just to avoid solitary confinement. Beyond prison issues, Mitnick's love for his family (especially his mother and grandmother) were clear throughout the book.

I very much enjoyed reading Ghost in the Wires, and I believe the majority of the computer security community would too.

Tweet

Video Game Phishing

by US-CERT (US-CERT Current Activity)

Submitted at 4/29/2011 9:15:46 AM

US-CERT is aware of reports that some users on the Xbox 360 video game system are receiving potential phishing attempts through an in-game messaging service. In-game message phishing is not a Microsoft issue and has nothing to do with Xbox LIVE. Games are products of third party developers that are playable on Xbox LIVE and other gaming systems.

Microsoft has posted a service alert on the Xbox LIVE status page regarding this issue.

US-CERT encourages users to take the following measures to protect themselves from these types of phishing attacks:

• Refer to the Recognizing and Avoiding Email Scams(pdf) document for more information on avoiding email scams.• Refer to the Avoiding Social Engineering and Phishing Attacks document for more information on social engineering attacks.

Royal Wedding or Royal hunt

(Securelist / Blog)

Submitted at 4/28/2011 10:44:26 PM

Instantly this news became very fruitful for all kinds of cybercriminals. Here is some of the proof we found: 1) SEO optimized Google image searches leading to a malicious site with the exploit for the " Help Center URL Validation Vulnerability". The exploit drops into the system a malicious executable file which is a password stealer malware.

At the moment we found it, Kaspersky Anti-Virus detected the sample as Heur.Trojan.Win32. Meanwhile the Jotti multiscanner results were 1/20 The exploit also works with Opera and Firefox browsers by dropping into the system a malicious PDF file:

2) SEO optimized for all non-Russian Google searchers leading to Rogue AVs, in particular to " XP Anti-Virus 2011" which actually is quite aggressive in blocking Internet access and extorting money for the activation

(Note: the third option anyway doesn't allow browsing) The infection scheme is quiet simple: a victim looks for pictures with the topic "Royal Wedding" and when the click comes with a Google reference a special malicious script redirects the victim to a malicious .cc domain with a classic Fake AV window. 3) Scams related to a fake Satellite TV where a victim should pay for the fake service. And of course, the credit card is being stolen once the payment is accepted. 4) Spam on Twitter just abusing TT and leading to misc. junk content sites We highly recommend using the latest patched Browser with a plugin like NoScript, don't click on any unknown link, and keep your AV updated and real-time protection working.

Ubuntu 11.04 Released

(Hack In The Box)

Submitted at 4/29/2011 12:45:31 AM

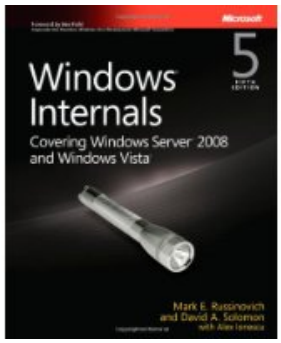
For those of you watching Ubuntu's website recently, you may have noticed a new version of the popular and easy to use variant of Linux has been surfaced - Natty Narwal. It can be downloaded from the previously linked site free of charge. Among the various new features, the Unity interface is set as the default UI, and includes the launcher (an OS X like dock), the dash (a popup menu with user defined shortcuts), and workspaces (a virtual desktop manager). According to the Ubuntu website, the OS can boot in as little as 7 seconds (following POST). Driving all of this eye candy is Gnome 2.32.1 (according to Ubuntu Vibes). If your current equipment is not capable of Unity, the classic desktop experience will kick in as to keep you moving along with minimal lag. Those of you wanting to experiment with Gnome 3, it cannot be installed via the Ubuntu repositories, and there have been reports of system instabilities post installation, though there is a workaround. If you're ready to install, there are 3 options for download, one for a CD/USB stick type installation, another to create a second boot partition alongside windows, and another for a standard standalone installation. The downloads are a one size fits all affair -- no longer is the Ubuntu Netbook edition or Desktop edition; there's just a single download for all platforms.

Three Foxconn employees charged over leaking of iPad 2 design

(Hack In The Box)

Submitted at 4/29/2011 12:48:22 AM

In the dark days before the iPad 2 announcement the rumour-mill was in full swing, with mockups doing the rounds of the usual tech blogs with even more frequency than usual. These mockups were unusually accurate this time around, thanks to various leaks of case specifications coming out of China and Taiwan. We even had photos of cases for an unreleased iPad 2, all but confirming the size and dimensions of Apple's next wonder-tablet. Apple wasn't happy, and now three Foxconn employees have been charged over the saga. Several online shopping retailers in China were able to sell iPad 2's protective case products before the iPad 2 was even launched, leading Foxconn to suspect that there might have been some employees leaking the design of iPad 2 which it reported to the local police. Foxconn is the main supplier of Apple hardware, especially iPhones and iPads - a leak of a new product more than likely originates from within the Foxconn walls. According to DigiTimes three Foxconn employees were arrested way back on Boxing Day, 2010 and they were officially charged with 'violating Foxconn's trade secrets' on March 23rd.



Review of Windows Internals, 5th Ed Posted

by Richard Bejtlich (TaoSecurity)

Submitted at 4/30/2011 9:07:00 PM

REVIEW page 4

REVIEW
continued from page 3

Amazon.com just posted my five star review of Windows Internals, 5th Ed by Mark Russinovich and David Solomon, with Alex Ionescu. Microsoft Press provided a free review copy. From the review:

Windows Internals, 5th Ed (WI5E) by Mark Russinovich and David Solomon, with Alex Ionescu, is a remarkable technical achievement. I read the book to better understand Windows to improve my security knowledge. I am not a Windows programmer, but I thought WI5E would provide context for some of the exploit and vulnerability information I occasionally encounter. I absorbed as much of WI5E as I could, but quickly found the scope and depth of the material to be incredible. While there is no substitute for reading source code, the explanations in WI5E come close! So many aspects of Windows are described, to such a deep level, that you might find yourself wanting to use Windows just to see WI5E's descriptions at work.

Tweet

CA discovers fake antivirus smartphone app

(Hack In The Box)

Submitted at 4/28/2011 7:00:00 PM

The shady but usually profitable world of fake antivirus software has arrived on mobiles with the discovery of a nameless Russian language app that claims its victimsâ€™ smartphones have become infected with malware. Discovered by CA, and apparently running on Windows Mobile, this example counts as a pretty crude one by established standards of trickery. The malware is naively similar to the sort of anti-malware programs found in the very different Windows desktop environment, and poorly attempts to impersonate security software from Kaspersky Lab. In fact, the program bears little resemblance to any of Kaspersky Labâ€™s mobile anti-malware software beyond the crude use of the companyâ€™s logo. As with any fake antivirus software, the program performs a fake malware scan before displaying two error codes that users are supposed to take as evidence of infection. How the criminals behind the attack get money from the scam is not clear but could involve phoning a number or contacting an email address to decode the phantom problems.

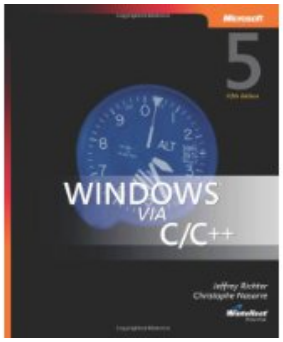
Review of Windows via C/C++, 5th Ed Posted

by Richard Bejtlich (TaoSecurity)

Submitted at 4/30/2011 9:01:00 PM

Amazon.com just posted my four star review of Windows via C/C++, 5th Ed by Jeffrey M. Richter and Christophe Nasarre. Microsoft Press provided a free review copy. From the review:

I will admit right away that I am probably not the target audience for this book, because I am not a professional Windows programmer. However, I am very interested in learning how Windows works, and Windows via C/C++, 5th Ed (WVCP5E) is one of the books that will help develop that expertise. Had I not also read Windows System Programming, 4th Ed (WSP4E) by Hart, I would have given WVCP5E 5 stars. Both are strong books, but WSP4E received 5 stars in a separate review. Still, I very strongly believe



that WVCP5E by Richter and Nasarre is a must-read for anyone who wants to know more about Windows applications.

Tweet

Royal spam

(Securelist / Blog)

Submitted at 4/29/2011 10:14:00 AM

The wedding of Kate Middleton and Prince William is by far the most popular topic of conversation today. It’s virtually impossible to look at a newspaper or a blog without seeing some mention of the royal newlyweds. And now we are getting in on the act.

And it’s not because we here at Kaspersky Lab take a major interest in the private lives of the British royals. But spammers obviously do - take a look at the offer we received today:

Yes, fake Swiss watches and iPads

are so passé - what you need is a replica of Kate Middleton’s engagement ring, originally given to Lady Diana by William’s father Prince Charles. The spammers claim you now have the chance to “own a piece of British royal history”. This royal family heirloom also comes complete with a “certificate of authenticity”.

Review of Windows System Programming, 4th Ed Posted

by Richard Bejtlich (TaoSecurity)

Submitted at 4/30/2011 9:04:00 PM

Amazon.com just posted my five star review of Windows System Programming, 4th Ed by Johnson M. Hart. Addison-Wesley provided a free review copy. From the review:

I read Windows System Programming, 4th Ed (WSP4E) by Johnson M. Hart after finishing Windows via C/C++, 5th Ed (WVCP5E) by Richter and Nasarre. While I liked WVCP5E, I found WSP4E to be the better book for the sort of understanding I was trying to achieve. I'm not a professional Windows programmer, but I wanted to learn more about how Windows works. Hart's book did the trick, especially for a person like me with more of a Unix background. If you want to better know how to program on Windows, and specifically

recognize differences among using the C libraries, the Windows API, and Windows "convenience functions," WSP4E is the book for you too.

Tweet

Malware Calendar Wallpaper for May 2011

(Securelist / Blog)

Submitted at 4/29/2011 3:53:00 AM

Here's the latest of our malware wallpaper calendars.

1280x800| 1680x1050| 1920x1200| 2560x1600

One of this month's highlighted malware incidents is the Morris worm. This worm was released on 2 November 1988 and by the following day was causing major problems for computers on the Internet. This would be nothing out of the ordinary in today's world. But it certainly was then. The worm quickly infected about 10 per cent of all computers connected to the Internet and, due to a programming error, made them unstable. Of course, in 1988 the Internet was made up of only 6,000 or so computers - it was an esoteric system used almost exclusively by government and academic institutions. So the Internet worm’s time had not yet come. But even so, the Morris worm was one of the first warnings of the importance of applying security patches in a timely fashion.

Nikon's image authentication algorithm cracked

(Hack In The Box)

Submitted at 4/28/2011 7:05:00 PM

Researchers have discovered a flaw in the system used by Nikon professional digital cameras to ensure images have not been tampered with. Normally, in high-end SLR digital cameras a unique and encrypted signing key is appended to an image when it is taken, which is verified in Nikon's case by its proprietary Image Authentication System. If an image is edited this key will be overwritten, an action that will be picked up by the software. Russian company Elcomsoft, however, said that it has found a way to extract the original verification key so that it can be attached to any image regardless of whether it has been edited or not. The security hole is said to affect all Nikon digital cameras supporting the verification system, specifically the D3X, D3, D700, D300S, D300, D2Xs, D2X, D2Hs, and D200 SLRs.