Issue 5/2012 (12) ISSN 1733-7186

ADDBE SECURITY

EXPLOITING ADOBE FLASH PLAYER ADOBE'S ASSET AND PSIRT POLICIES IOS VS. FLASH

Adobe



USER TRAINING AND WRITTEN SECURITY POLICIES

ATOLA DISK DIAGNOSTICS: OPPORTUNITIES AND SOLUTIONS

Atola Insight

That's all you need for data recovery.

Atola Technology offers *Atola Insight* – the only data recovery device that covers the entire data recovery process: *in-depth* **HDD diagnostics**, **firmware recovery**, **HDD duplication**, and **file recovery**. It is like a whole data recovery Lab in one Tool.

This product is the best choice for seasoned professionals as well as start-up data recovery companies.



- Automatic in-depth diagnostic of all hard drive components
- Automatic firmware recovery and ATA password removal
- · Very fast imaging of damaged drives
- Imaging by heads

- Case management
- Real time current monitor
- Firmware area backup system
- Serial port and power control
- Write protection switch



Visit <u>atola.com</u> for details



Air Freshener?

Printer PSU

ATURES:

✿ Covert tunneling SSH access over 3G/GSM cell networks NAC/802.1x bypass and more!

Industry's

commercia

testing

Discover the glory of Universal Plug & Pwn

@ pwnieexpress.com

t) @pwnieexpress

PWNIE EXPRESS

😑 🕒 info@pwnieexpress.com 🔁 🕨 802.227.2PWN

THE



Managing: Michał Wiśniewski m.wisniewski@software.com.pl

Senior Consultant/Publisher: Paweł Marciniak

Editor in Chief: Grzegorz Tabaka grzegorz.tabaka@hakin9.org

Art Director: Marcin Ziółkowski

DTP: Marcin Ziółkowski www.gdstudio.pl

Production Director: Andrzej Kuca andrzej.kuca@hakin9.org

Marketing Director: Grzegorz Tabaka grzegorz.tabaka@hakin9.org

Proofreadres: Dan Dieterle, Michael Munt, Michał Wiśniewski

Top Betatesters:

Ruggero Rissone, David von Vistauxx, Dan Dieterle, Johnette Moody, Nick Baronian, Dan Walsh, Sanjay Bhalerao, Jonathan Ringler, Arnoud Tijssen, Patrik Gange

Publisher: Hakin9 Media Sp. z o.o. SK 02-682 Warszawa, ul. Bokserska 1 *www.hakin9.org/en*

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage. All trade marks presented in the magazine were used only for informative purposes. All rights to trade marks presented in the magazine are reserved by the companies which own them.

To create graphs and diagrams we used program by Mathematical formulas created by Design Science MathType[™] DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

DEAR READERS,

UPON HEARING ON NOTORIETY OF FLASH EXPLOITS AND ADDBE SECURITY ISSUES, WE DECIDED TO DEDICATE MAY EDITION OF HAKIN9 EXTRA TO ADOBE SECURITY. OUR EXPERTS AND LONG-TIME COLLABORATORS HAVE EXPLO-RED THE VAST MAJORITY OF THE MOST DESIRABLE TO-PICS CONCERNING ADOBE SECURITY. WE WOULD NOT BE FAIR IF WE HAD NOT GIVEN ADOBE REPRESENTATIVES A CHANCE TO EXPLAIN THEIR SECURITY POLICY, AND SO WE DID. THE MEDLEY OF INFORMATION PRESENTED IN THE ADOBE'S ARTICLE IS PUBLICLY AVAILABLE, BUT HAS BEEN COMPILED ACCORDING TO HAKIN9 EXTRA'S EXPECTA-TIONS. IN THIS ISSUE KEITH DEBUS WILL EXPLAIN THE GLITCHES BETWEEN ADOBE AND APPLE, AND EXPAND ON THE TOPIC WHY APPLE DOES NOT WANT FLASH ON ITS IDS. AN ARTICLE BY SWETHA DABBARA EXPLORES THE TOPIC OF FLASH EXPLOITS. KEN KRAUSS WILL FOCUS ON THE IMPORTANCE OF WRITTEN SECURITY POLICIES IN THE ERA OF BYOD AND SOCIAL MEDIA. AND THE TIME FOR SOMETHING COMPLETELY DIFFERENT - DMITRY POSTRI-GAN IS GOING TO PRESENT YOU ON HOW TO PERFORM DISK DIAGNOSTICS WITH THE USE OF ATOLA TECHNO-LOGY. NEXT, AS PROMISED BEFORE, ADOBE SECURITY DIVISIONS WILL PRESENT THEIR SECURITY POLICIES AND THE TECHNICALITIES BEHIND THEIR PSIRT AND ASSET TEAMS.

WE GENUINELY HOPE THAT YOU WILL HAVE A PIECE OF GOOD READING ON ADOBE SECURITY AND WE HAVE NOT FAILED YOUR EXPECTATIONS. I WOULD ALSO LIKE TO THANK WIEBKE LIPS FROM ADOBE FOR PRESENTING US INFORMATION WE DESIRED.

STAY TUNED, AND GET READY FOR HAKIN9 BIBLE CO-MING OUT NEXT WEEK AND THE NEWLY-LAUNCHED CRYP-TOMAG COMING OUT IN JUNE.

> MICHAŁ WIŚNIEWSKI AND HAKIN9 TEAM M.WISNIEWSKI@SDFTWARE.COM.PL

SeagateDataRecovery.com

Bad things can happen to a laptop. They don't have to happen to the data.

Seagate Recovery Services work on any disk drive to support forensic investigations

Seagate takes the dread out of data mishaps in forensic investigation scenarios. From file deletions to physical tampering causing hard disk damage - from any brand - we make it easy to get the files back for law enforcement agencies to crack criminal cases. For more information, please visit www.seagatedatarecovery.com.



© 2012 Seagate Technology LLC. All rights reserved. Seagate, Seagate Technology and the Wave logo are registered trademarks of Seagate Technology LLC in the United States and/or other countries. Seagate reserves the right to change, without notice, product offerings or specifications.

Hakin9 EXTRA



8. Why Apple Doesn't want Flash on its iOS

by Keith DeBus

Ever since the advent of the iPhone in June of 2007, Apple's decision to forego Adobe's ubiquitous Flash software has raised eyebrows and more than a few hackles. Then, when Apple introduced the now revolutionary iPad in April of 2010, the controversy escalated to a white hot froth in short order. Apple and its CEO and founder, Steve Jobs, has claimed that Flash was a security vulnerability and threatened the convenience and usability of their mobile devices and therefore would be banned from iOS and their mobile devices. In this article, we will look at the long history of the relationship between Apple and Abobe than culminated in this ban, examine closely the claims and counter claims and then attempt to sort out the validity of Apple's claims against Adobe and its Flash software.

14. Exploiting Adobe Flash Player

by Swetha Dabbara

The vulnerability exists in Flash Player versions 11.2.202.233 and earlier for Windows, Macintosh and Linux systems, as well as versions 11.1.115.7 and earlier for Android 4.x and versions 11.1.111.8 and earlier for Android versions 3.x and 2.x. The company said the plan to include a Google Play link for Android users at some point today so that they can get the update for their devices. The patch is of highest urgency as there are attacks in the wild against the vulnerability. «Users that have opted-in to participate in the newly introduced silent update feature (currently only available on Windows), will have the update applied automatically on all browsers present on their system,» he continued. «Users of other operating systems and users that have opted-out of 'silent update' need to manually install on all browsers.»

20. User Training and Written Security Policies More Important Than Ever in a World of Social Media & BYOD

by Ken Krauss

Rather than having a standardized list of allowed applications on employee devices known to company security managers, with BYOD the list of allowed applications on computing devices is often non-standardized. Further complicating the issue, company IT staff might not even know which device(s) employees use, and might not now be allowed to connect remotely to employee devices for patch management, virus scans, and other security concerns. It is also much more likely that the BYOD employee will be sharing their devices with others that are even less skillfully trained on computer security than your employees are, such as their children or other family members.

26. Hard Disk Diagnostics: Opportunities and Solutions

by Dmitry Postrigan

It is not a secret that every data recovery specialist must perform a full diagnosis of a hard disk drive to find the problem or the disk state in general as the very first step in all data recovery cases. Only accuracy and competent approach can guarantee the extraction the maximum amount of a data to avoid further damage to the hard drive. Have you ever considered what it takes to find the exact state of the customer's drive? Usually, it is a quite complex task that involves a number of tests, guesses, and risks; and it has been like that for many years. I believe it's time to offer something better. Atola Insight provides the unique, ful-ly-automated in-depth diagnosis of any PATA or SATA hard drive. Just one click, and in a few minutes, you'll have the full diagnosis report outlining the exact issue.

30. Security Teams at Adobe

by Adobe

Adobe has a team in place (the Adobe Secure Software Engineering Team – ASSET), which is dedicated to ensuring our products are designed, engineered and validated using security best practices. Brad Arkin, senior director of security for Adobe's products and services, leads that team. A second team within ASSET (the Product Security Incident Response Team – PSIRT) is responsible for responding to and communicating about security issues. ASSET and PSIRT (as they exist today) were put in place during the integration of Macromedia and Adobe in late 2005 by combining the corresponding security teams from each company, and these teams continue to evolve to best address the threat landscape facing Adobe's products. All engineering teams at Adobe work very closely and proactively with the Adobe Secure Software Engineering Team (ASSET) during each phase of the Adobe Secure Product Lifecycle (SPLC). In addition, product teams have dedicated security development and testing groups in place. As a result of changes in the threat landscape, we have about seven times as many engineers dedicated to security today compared to 2009.





WHY APPLE DOESN'T WANT FLASH ON ITS IOS

KEITH DEBUS

This article will examine the making of the dispute between Apple and Adobe over Apple's decision to keep Flash from their mobile devices. We examine Apple's claims and evaluate their validity and ultimately, determine whether they made the right call on Flash.







ver since the advent of the iPhone in June of 2007, Apple's decision to forego Adobe's ubiquitous Flash software has raised eyebrows and more than a few hackles. Then, when Apple introduced the now revolutionary iPad in April of 2010, the controversy escalated to a white hot froth in short order. Apple and its CEO and founder, Steve Jobs, has claimed that Flash was a security vulnerability and threatened the convenience and usability of their mobile devices and therefore would be banned from iOS and their mobile devices. In this article, we will look at the long history of the relationship between Apple and Abobe than culminated in this ban, examine closely the claims and counter claims and then attempt to sort out the validity of Apple's claims against Adobe and its Flash software.

Background

Flash is an Adobe software product used as multimedia platform that became ubiquitous throughout the Internet for running video, animation, games and other interactive applications. It has been frequently used for advertisements, games and video



on the web. Flash's utility comes from ability to manage and manipulate vector and raster graphics. Flash generated apps can be run on a Flash player that is available across multiple platforms, including Windows, Mac, Linux, some phones and tablets (this strength was a big part of its early success, but eventually leads to its downfall, from Apple's perspective). The Flash player is a freely downloadable plug-in to most of the available web browsers including Internet Explorer, Firefox, Opera, Chrome and others.

Example of Flash Animation

Best Flash Animation 2006

Development of Flash

Flash was first developed by a small company then known as FutureWave Software. Originally known as SmartSketch, it was developed as a drawing program for pen-based computers running PenPointOS. PenpointOS was among the first OS's in the early 1990's that was meant as proprietary OS of for the then promising market of pen-based computers (remember Apple's Newton?). At the time, pen based computing was considered to be the next great wave in computing. With 20/20 hindsight, we can see that this concept of a pen based computer was a good one, but a bit premature. When PenPointOS failed, FutureWave decided to port their SmartSketch for the Mac and Windows-based systems. At that point, it was strictly a drawing program. Then, as the promising growth of the Internet became apparent, FutureWave added cell animation editing to their product. FutureWave, by now struggling under the weight of the collapsing pen computer market, offered to sell SmartSketch to Adobe (an obvious choice and seemingly good fit considering Adobe's strength computer graphics software) in 1995, but Adobe showed no interest. In 1996, Macromedia, seeing the growth of the Internet, began to develop and acquire applications to develop multimedia applications for the web, acquired FutureSplash. With its acquisition of FutureSplash, it contracted the product name to Flash (FuturespLASH). In 2005, Macromedia was acquired by Adobe and Flash became part of the Adobe stable of application for development of rich graphics, animation and web applications.

Apple and Adobe collaboration and partnership

Apple and Adobe have a long history of cooperation. In the early days of the Apple products, Apple and Adobe seemed inseparable. Adobe, founded in 1982 by John Warnock and Charles Geschke (both of the famous em-





bryo of computer technology, Xerox's Palo Alto Research Center. As legend goes, Jobs was first exposed to the concept of the mouse and the graphical user interface (GUI) at PARC soon after starting Apple which eventually resulted in his development of the first Mac

with mouse and GUI in 1983), began by offering the first Postscript page description language that Apple then adopted in its first LaserWriter printers that helped to spur the desktop publishing revolution (remember the DTP revolution?). Soon thereafter, Apple purchased a 19% stake in Adobe. By the mid 1980's, Adobe launched their flagship Illustrator program for drawing and then 1989 its now ubiquitous Photoshop for photo manipulation. Initially, developed only for the Macintosh, these state of the art graphics programs spurred Macintosh sales and gave them a foothold in the graphics design industry that they have never relinguished.

Interestingly, Jobs and Adobe continued their collaboration even after Jobs was ousted from his company in 1986. Jobs started his ill-fated NeXT Computer in 1987 and one of the few companies that wrote software for that short-lived platform was Adobe (a few of you may remember that Jobs NeXT computer ran a version of UNIX developed by Carnegie-Mellon named MACH that Apple acquired when they bought the assets of NeXT out of bankruptcy and became the foundation of Apple's wildly successful OSx). This turned out to be a huge strategic blunder for Adobe.

By the late 1980's and 1990's, it seemed that every Apple product was loaded with Adobe software. Much of the Apple products reputation among graphic designers and others in the desktop publishing and creative fields was result of the fact that the Apple products had Adobe software to develop on while competing platforms did not.

The over twenty year relationship and cooperation between Apple and Adobe has now been thoroughly tested by Apple's refusal to allow Flash on its mobile devices. Beginning in 2007 with the introduction of the iPhone, Apple and Adobe have been at loggerheads over Flash. Each company has made claims and counter claims about the other.

After years of silence on Job's part on why Apple refused to allow Flash on its iPhones and iPads(as you know, Apple apps are only available at the Apple store after Apple vets, tests and approves them), Apple's legendary founder and CEO released an open letter outlining his and Apple's objections to Adobe's Flash. Job's open letter laid out six (6) key reasons for banning Flash from Apple's stable of mobile products from the iPhone to the IPod to the iPad.

Let's look at each of the six reasons that Mr. Jobs objected to Flash in April 2010. I will attempt to summarize and paraphrase his objections in the interest of brevity.

Openness

Steve Jobs makes the claim that Flash is a proprietary software product and therefore isn't "open". He points out that Adobe Flash products are made only by Abobe and Adobe has sole authority "as to their future enhancement and pricing". Jobs goes on that although Apple has proprietary software products, Apple believes that all standards pertaining to the web "should be open". He points out that Apple, Google and others have adopted the open standards of HTML5, CSS and Javascript to provide the same functionality as Flash without requiring a proprietary third party plug-in.

Full web

Adobe had shot back at Apple that Apple users were being denied the *full web* by not be allowed to use Flash and the applications developed for it. Adobe claimed that because 75% of the video on the web is designed to use Flash, Apple was doing a disservice to their customers by denying them this content. Jobs responds by saying that these same videos and animations are available to Apple users and others without the Flash plug-in through other, more modern technologies such H.264.

In response to Adobe's claim that Apple users can't use Flash games, Jobs concedes that this is true, but that there are over 50000 games on the Apple App store that do not use Flash and many are free.

Reliability, security and performance

Jobs points out that Symantec, the Internet security firm, pointed out that Flash has one of the worst security records in 2009 (Jobs is writing this in 2010). He claims that Flash is the primary reason Macs crash and that Adobe has not fixed the problem. He says that Apple wants their mobile products to be among the most reliable and secure and doesn't believe that is possible with Flash installed.

Jobs goes on to point out that Flash does not perform well on mobile devices. Mobile devices,--with limited CPU power and battery life—could not sustain the power drain that Flash imposes on these smaller, more limited devices such as the iPhone and the iPad.

Battery life

To re-emphasize his point on Flash performance on mobile devices, Jobs points out that mobile devices must decode compressed video in hardware, not software, to limit power consumption and extend battery life. Jobs says that Apple and others prefer chips built with H.264 encoding for efficient video decoding without straining the CPU or battery life. He claims that when videos are being decoded with software, battery life is limited to 5 hours on the iPhone, while battery life with hardware decoding (H.264) is extended to 10 hours.

Touch

Jobs cites the fact that the new mobile devices largely use touch using the human hand as a pointing device, while Flash was designed in an era where mice where the dominant form of pointing device on PC's. He points out that many Flash based websites rely on "rollovers' where menus or other features are enabled when the mouse rolls over a specific spot and that this concept of a rollover doesn't exist in the



iPad/iPhone world. He goes on to say that these Flash based websites would need to re-written for mobile devices to make use of the new touch based interface. In short, Jobs points out that Flash was written for a PC/mouse paradigm and that new mobile device/touch paradigm demands a new technology such as HTLM5.

Cross platform

In the 1990s, one of the key elements of Flash's success is that it enabled developers to write applications, games, etc. that could run on any platform. Jobs sees this feature as a negative in the 21st century. Jobs and Apple wanted apps that were specifically developed and optimized for the iOS, not for all and any mobile device. He points out that letting a third party layer of software come between the platform and the developer results in substandard applications and "hinders the enhancement and progress of the platform". He reasons that if developers are dependent on a third party development library and tools, they can only take advantage of platform enhancements when the third party chooses to make those new features available. He did not want Apple to be at the mercy of such a third party. Jobs saw the multi-platform capability of Flash as a negative, reasoning that a third party development platform would not make features available unless they were available on all platforms, in other words, developers would be limited as Jobs said, "to the least common denominator set of features". In short, Jobs didn't want his devices to become the commodity platforms that PC's had become (and hence, lower profit margins), but rather a unique, high guality platform that users would choose and crave, even at a higher price.

Apple's Terms of Service

Even despite Job's stated objections in this letter to Flash and its shortcomings, it appears that Flash could never have become compliant to Apple's terms of service, in its earlier form. Apple's iPhone terms of service reads;

An Application may not itself install or launch other executable code by any means, including without limitation through the use of a plug-in architecture, calling other frameworks, other APIs or otherwise. No interpreted code may be downloaded and used in an Application except for code that is interpreted and run by Apple's Published APIs and built-in interpreter(s).

As Flash is a plug-in architecture and ran *other executable code*, Apple could not allow Flash on its phones without making an exception to their terms of service,

something that they are loath to do.

Evaluating the Job's Claims

Now, let's take a moment to examine Job's and Apple's objections to Flash on it merits and with, hopefully, some objectivity.

First, the charge that Flash is not open. This is probably Job's and Apple's weakest argument. Apple makes plenty of products that are not open and uses other products that are not "open". This, I believe is a smoke screen by Jobs and should be classified more into the heap of rationale for Apple desire to maintain full control of the app's on their devices. Not that this is a bad thing, but to use the excuse that Flash is not "open" is simply a smoke screen for the actual reasons.

Second, Jobs' claim that iPhone users can view nearly the full web is mostly true. Multiple web sites now offer their video in HTML5 including Youtube, MSNBC, to name just few. Considering Apple's intransigence on this issue of allowing Flash on their mobile devices, we are likely to see more and more sites adopt other technologies for enabling video, animation and games. It should be pointed out though, that few of these sites were viewable without Flash <u>before</u> Apple made an issue of Flash. In many ways, Apple is driving websites and developers to use other technologies, so that their content may be viewed by IPhone and iPad users.

Third, Jobs' argument that Flash is not secure is probably his most compelling argument he makes. Flash's record for security vulnerabilities is dismal. Flash has been racked with security issues from nearly day one to the present. The exploit database, an online database of security vulnerabilities, lists 105 Flash related vulnerabilities dating back to July 22, 2004 and running right up April 20, 2012. The CVE database of vulnerabilities lists 191 vulnerabilities. Obviously, the lack of security in Flash is a very real concern especially since many of these vulnerabilities enable the attacker to open a command shell on the victim's machine and take full control

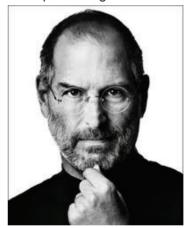
In recent months, new vulnerabilities have been found in Adobe's Flash. It's clear that Adobe has its hands full on security issues with Flash that don't seem to be going away.

As for Jobs' claims that Flash is the major reason for Macs crashing, he has another strong argument here. Flash's Shockwave has a horrendous reputation for crashing browsers and systems. Nearly all of us have experienced it. As one IT support person for a major mining company relayed me, *nearly half of our support tickets are related to Flash.*

Fourth, Jobs' claim that Flash is battery "hog" also has merit. Whenever graphics are rendered by software in a general purpose CPU, the drain on power is significant and the rendering much slower. Hardware decoding is almost always faster and more efficient. This is why nearly all gaming and graphic systems now have their own GPU (graphics processing unit) and graphics subsystems. Furthermore, there is strong empirical evidence that when Shockwave Flash crashes, it consumes huge amounts of CPU cycles and memory. Not something that would enhance our mobile device experience and battery life.

Fifth, Jobs' issue with touch seems to be a minor, but valid objection. Flash was developed for a PC-centric world where the mouse was the pointer of choice. First introduced in the microcomputer market by Apple, the mouse had superseded all other pointing devices from its introduction until the present. Jobs and Apple, the relentless innovator in human-machine interaction, took the pointing device to the next logical level when they incorporated touch into their iPhone and iPad. Flash was developed for a market where the mouse was the pointing device of choice, but had not adapted to the new touch-based market of mobile devices. I think this was minor factor in Apple's decision, but valid nonetheless.

Sixth, Jobs was obsessed with making the iPhone and iPad the best mobile device experience available and he was probably successful. In part, his success comes from his attention to detail and this sixth objection to Flash fits that bill. Jobs --having lived through the history of the PC and making much of it-- had seen how platforms had become "commoditized" and didn't want that to happen to his beloved iPhone and iPad. He wanted those platforms to be the best he could create without hindrance from the software community. He didn't want to follow, he wanted to lead. By leaving his platform at the mercy of a third party developer, he might not only lose control, but he relinguished the ability to lead. This would likely eventually lead to the "commoditization" of the iPhone as simply a piece of low margin hardware (are you reading this Android phone manufacturers?). Although this objection was less about Flash as software and more about Apple's control and leadership with iOS and mobile device platforms, it was definitely a wise business decision. It is necessary evil, if Apple wants is continue its mobile device leadership and outsized profit margins.



One has to say now-nearly five years after the first iPhone appeared and three years after the first iPad-- that Apple's decision to ban Abobe's flash software from its mobile devices was the right one. This once ubiquitous browser plug-in that enabled all of us to view online video, games and animations was just too riddled with security

flaws, too unstable and too much of a power hog for this new era of mobile devices. Despite the controversy that Jobs and Apple raised by this hard decision to ban a long time ally and business partner from their new line of devices, Apple has benefitted by having more secure, more reliable and more long lasting mobile platforms (Adobe's decision in November 2011 to abandon support for mobile Flash seems to further support and confirm Apple's decision). In addition, Apple seized for themselves control of the software that would run on their devices enabling them to optimize their platform and distinguish it from its many potential clones. Not only has Apple benefitted this decision, but so has the entire community of mobile device users. Just another lasting legacy of the incomparable Steve Jobs.

KEITH DEBUS

is the President of IT Securitas, an IT security consulting and training firm in Salt Lake City, UT. He has over 20 years of experience in the IT industry and is a former university professor of computer science.

Do You Want to Become a Cyber Security Expert? **OR ADVANCE YOUR IT SECURITY CAREER?**

- Cyber Security has one of the largest market shares in IT 0
- 0 Government & Compliance Regulations are more and more enforced
- 0 Gartner Group predicts unprecedented growth and need in Cyber Security
- Skilled Cyber Security Experts are in ever more demand 0

THE CYBER 51 EXPERT COACHING FORUM

- 0 Individual 1-on-1 Mentoring on Ethical Hacking, Penetration Testing and IT Security
- 0 Networking with other community members and moderators
- 0 Access to a wealth of tools and information not found on public domain
- Permanent Job & Contract offers, Webinars and much more! 0

YOUR BENEFITS

- Become an Ethical Hacker / Penetration Tester with 1-on-1 mentoring 0
- Learn at your own pace at a fraction of the cost of regular courses

CYBER 51 COACHING FORUM

CYBER SECURITY FORUM



CONTENT:

- 1. General Topics
- 2. Service Assessment
- 3. Ethical Hacking
- 4. Cyber Threats
- 5. Mitigating Cyber Threats
- 6. Penetration Testing

CYBER 51 INSTRUCTORS



OUR CERTIFICATION LEVELS:

- Certified Ethical Hacker (C|EH)
- Forensic Investigator (C|HFI)
- Certified Security Analyst (ECSA)
- Licensed Penetration Tester (C|LPT)
- Network Security Admin (ENSA)
- ISC Consortium (CISSP)

FEATURES



ADDITIONAL FEATURES:

- 1-on-1 Coaching
- Trainers with Years of Experience
- Wealth of Tools
- Webinars
- Networking with other members
- Contract & Perm. Job Opportunities

WHY CYBER 51?

- 0 Learn whenever you want to
- 0 Dedicated 1-on-1 Coaching
- 6 Information you will not find on public boards
- 6 All Mentors work as Senior Security Consultants
- 0 **Frequent updates**
- 0 Great Value for money



CYBER 51 LIMITED, 176 THE FAIRWAY, SOUTH RUISLIP, HA4 OSH, MIDDLESEX, UNITED KINGDOM EMAIL: INFO@CYBER51.CO.UK WEB: WWW.CYBER51.CO.UK



Web Audit Authority

The Internet service conducting fully-automatized web audits:

- Web Standards Audit
- Web Access Audit

FORMARY OR

• Web Usability Audit





hihi.

oac





WEBSITE

Co-funding support provided by European Union from European Regional Development Fund

EXPLOITING ADOBE FLASH PLAYER

SWETHA DABBARA

Security is a key concern for all the users who use adobe application and also for those who own websites or those who develop content. By default flash player has security rules and grouping is done based on the assets and known as security sandbox. It depends on the domain in which the origin is from for the SWF files, media and other assets when loaded.

ction Script plays a key role when it comes to Adobe flash player because it is the programming language for the above and for run time environments. The functionality of the language establishes the necessity to provide more secured environment relating to adobe application. Threat or attacks are more prone in this area when files (SWF) are accessed from a specific internet domain. This is when grouping or sandbox security rules play a major role in terms of security aspect.

The latest version of flash player (Version 10.1) addressed issues relating to performance, security and the level of consistency.

We won't get to see much of flash when it is concerned with enjoying the web videos which all of us prefer to watch in our PDA such as ipad or iphone or Apple products in simple. None of the touch screen mobiles have flash player support since Apple refuses to do so primarily keeping in view of the security aspect by blocking the IP addresses of those who are watching the videos online.

Flash player remains the defacto in spite of the web video story in contrast with the competitor HTML5 tag based technology because it has had its own holdings to stop by. Another concept of local connection communication using cross scripting makes it more vulnerable to attacks.

Accessing of methods, objects and other properties of one SWF file to another is possible through this cross scripting to make use of Action Script. There is no secure communication since cross scripting between any SWF files is permitted from the same domain always.

What will you learn?

- Flash Player application concept and possible attacks
- Action Script Programming language and Possible attacks

What should you know?

 Beginners knowledge about Flash Player and Action Script Current Security attacks and about Vulnerabilities in applications(Web)

Flash Player

For Rich Internet applications and for audio and video streaming, the browser needs some plug-in and is provided by Adobe Flash Authoring tool Adobe Flex. Many third party tools along with Macro media made this application followed by Adobe systems distribution and development. With the help of adobe flex, SWF files can be run by flash player for the purpose mentioned above. It need not be for only computers. It could be even for mobiles or any other supported devices.

Action Scripting

Scripting language is embedded for streaming purpose and for flash player to run graphics. A cross-platform framework for run-time environment very much suitable for mobile and desktop applications as mentioned earlier.

Attacks on Flash Player

Cross Site Scripting Vulnerability

HTML ecosystem in a way makes it difficult to exploit this vulnerability. It is the other way with Adobe Flash application which is easy to exploit this vulnerability. Cross-site scripting attack is the primary concern exploit for Adobe flash player by executing an arbitrary code.

"It's recommended that users of Adobe Flash Player 11.2.202.233 and earlier versions for Windows, Mac and Linux update to Adobe Flash Player 11.2.202.235".

The US-Cert reports the current activity with vulnerabilities many among Adobe products out of which our focus will be on Flash player of course. Patches are released for Adobe Flash Professional CS 5.5 (11.5.1.349) and earlier versions for Windows and Macintosh to remain safe from executing of arbitrary code or to avoid the attackers taking control of an affected system.

APSB12-12: This is the upgrade or patch provided for the vulnerability for Windows and Macintosh for by Adobe

for Adobe Flash Professional CS5.5 (11.5.1.349). With this upgrade utilized by every user, the attacker has less probability or no chance to attack using a vulnerability and take control of the affected system.

Attack with Emails(Spamming)

Another vulnerability that can be exploited using emails has created havoc while using Flash player.

The attackers plan in such a way that the user gets tricked and just with a click on the email message sent to the person, the malicious file is in the target system or mail box. This is specific for those Internet explorer users on WINDOWS. For the exploit launched to work without fail, the attachment which contains the malicious file must be opened and second of all will work for those systems with Adobe Flash player installed. With further details to dig through, According to reports submitted by Symantec, the process of exploitation using this code for the email strategy is explained this way: "The Adobe flash file located on the remote server will have the malicious document as reference".

Flash Files

They are in the SWF format and also known to be Shock-Wave Flash/FLash Applications/flash movies. They come with .swf extension and used in the form of web page plugin. Usually incorporated in a self-executing projector movie, these files can be player in a stand-alone flash player. The extension is .exe for Microsoft Windows. Video files will have .flv extension for the files and these are played through a fly-aware player such as VLC/Quick Time and with the external codecs added can be played with Windows Media Player too.

Stack Overflow Attack for Flash Player

Action Script Virtual Machine is the root cause while dealing with the Flash files which are malicious. This is where the vulnerability exists and the attacker can easily exploit this without the users knowledge. Flash files are crafted and when a user enters the web page containing these flash files without suspicion, the exploitation occurs and whole system gets controlled by the attacker. The patch/ Update solved the issue later.

Buffer Overflow attack with Flash Player

VUPEN Vulnerability Research Team discovered a critical vulnerabilityin Adobe Flash Player. The vulnerability is caused by a buffer overflow error when processing a malformed ActionScript FileReference method, which could be exploited by remote attackers to compromise a vulnerable system by tricking a user into visiting a specially crafted web page.

Phishing attack on Flash Player

Several spear phishing campaigns have been detected. The mails sent contain a Word document attachment. It contains a reference to a Flash file that is downloaded from a remote server once the document is opened. This Flash file exploits the CVE-2012-0779 vulnerability triggering a shell code that looks for the payload within the original word document. The payload is decoded using a one byte XOR scheme, dropped on the system and then executed. Adobe released an emergency update today to fix a critical vulnerability in Adobe Flash Player for Windows, which has come under attack. The vulnerability could allow hackers to crash or take control of an affected machine.

"There are reports that the object confusion vulnerability (CVE-2012-0779) addressed in this update is being exploited in the wild in active targeted attacks designed to trick the user into clicking on a malicious file delivered in an email message, and the exploit targets Flash Player on Internet Explorer for Windows only."

The vulnerability exists in Flash Player versions 11.2.202.233 and earlier for Windows, Macintosh and Linux systems, as well as versions 11.1.115.7 and earlier for Android 4.x and versions 11.1.111.8 and earlier for Android versions 3.x and 2.x. The company said the plan to include a Google Play link for Android users at some point today so that they can get the update for their devices. The patch is of highest urgency as there are attacks in the wild against the vulnerability.

"Users that have opted-in to participate in the newly introduced silent update feature (currently only available on Windows), will have the update applied automatically on all browsers present on their system," he continued. "Users of other operating systems and users that have opted-out of 'silent update' need to manually install on all browsers."

Alex Horan, senior product manager at penetration testing firm CORE Security, said Flash Player makes for a fantastic target for opportunistic attackers.

"For a lot of modern and exciting Websites you need Flash to view their content, see their videos, etc., so the first time a user visited a site like that they would have installed Flash," he said. "The likelihood that they ever considered upgrading it is close to zero—as such attackers know there are a lot of browsers running old and vulnerable versions of Flash and that their browser will automatically load their Flash attacks with no prompt to the user."

Flash Player Security Process Flow

In the Flash Player security model, there is a distinction between loading content and extracting or accessing data. *Content* is defined as media, including visual media Flash Player can display, audio, video, or a SWF file that includes displayed media. *Data* is defined as something that is accessible only to Action Script code. Content and data are loaded in different ways.

- Loading content You can load content using classes such as the Loader, Sound, and NetStream classes.
- Extracting data You can extract data from loaded media content by using Bitmap objects, theBitmapDa-ta.draw() method, the Sound.id3 property, or the SoundMixer.computeSpectrum() method.
- Accessing data You can access data directly by loading it from an external file (such as an XML file) using classes such as the URLStream, URLLoader, Socket, and XMLSocket classes.

The Flash Player security model defines different rules for loading content and accessing data. In general, there are fewer restrictions on loading content than on accessing data.

In general, content (SWF files, bitmaps, mp3 files, and videos) can be loaded from anywhere, but if the content is

from a domain other than that of the loading SWF file, it will be partitioned in a separate security sandbox.

There are a few barriers to loading content:

- By default, local SWF files (those loaded from a nonnetwork address, such as a user's hard drive) are classified in the local-with-filesystem sandbox. These files cannot load content from the network.
- Real-Time Messaging Protocol (RTMP) servers can limit access to content.

If the loaded media is an image, audio, or video, its data, such as pixel data and sound data, can be accessed by a SWF file outside its security sandbox only if the domain of that SWF file has been included in a URL policy file at the origin domain of the media.

Other forms of loaded data include text or XML files, which are loaded with a URL Loader object. Again in this case, to access any data from another security sandbox, permission must be granted by means of a URL policy file at the origin domain.

Why Action Script/ Benefits of Using Action Script

It is designed to facilitate the creation of highly complex applications with large data sets and object-oriented, reusable code bases. While Action Script 3.0 is not required for content that runs in Adobe Flash Player, it opens the door to performance improvements that are only available with the AVM2, the new virtual machine. Action Script 3.0 code can execute up to ten times faster than legacy Action Script code.

The older version of Action Script Virtual Machine, AVM1, executes Action Script 1.0 and Action Script 2.0 code. AVM1 is supported by Flash Player 9 and 10 for backward compatibility with existing and legacy content. Action Script 3.0 is architecturally and conceptually different from previous versions of Action Script. The enhancements in Action Script 3.0 include new features of the core language and an improved Flash Player API that provides increased control of low-level objects.

When working with an ActionScript 3 FLA file, managing assets and creating symbols is pretty much the same process that you're used to in ActionScript 2, but the rules for coding change a bit. Code can be added to keyframes along your timelines or linked to the main timeline or your symbols using external ActionScript files. When you publish your movie, the ActionScript code is compiled into the resulting SWF file. The ActionScript 3 compiler processes the ActionScript code by checking to make sure that the structure of the code and code assignment all match the strict rules of the ActionScript 3 language.

Error

Errors are notifications built into the ActionScript language and compiler process. Errors come in three flavors: compiler errors, runtime errors (ActionScript exceptions or error events), and warnings:

Compiler errors

These are generated when the file is published and the ActionScript is compiled into a SWF file. Compiler errors enforce rules that allow the ActionScript code to run in an optimal and expected way. When compiler errors ap-

pear, the SWF file will fail to export until the errors are removed.

Runtime errors

These are generated by ActionScript objects when issues arise after compile time, during playback. Runtime errors come in the form of error events or ActionScript exceptions containing error description objects. Flash Player tries to ignore runtime errors, letting them fail silently in the background, but if a fatal error occurs, it will flood the Output panel with messages and stop the playback of the movie.

Warnings appear at compile time, but generally don't stop the export or playback of the movie.

The Flash Player team is constantly improving the features, performance, and security of the Flash Player. From time to time Flash Player bugs and known issues do arise. Flash Player implements a security model which protects each SWF file and your computer from malicious attacks. When all your files are running within the same domain, you usually won't hit any security errors. However, it's common that you might want to aggregate content and data from different servers running on different domains. In that case, you will most likely hit security errors at one point or another.

Flash Player Security – Security Sandboxes

Client computers can obtain individual SWF files from a number of sources, such as from external web sites or from a local file system. Flash Player individually assigns SWF files and other resources, such as shared objects, bitmaps, sounds, videos, and data files, to security sandboxes based on their origin when they are loaded into Flash Player. The following sections describe the rules, enforced by Flash Player, that govern what a SWF file within a given sandbox can access.

Remote sandboxes

Flash Player classifies assets (including SWF files) from the Internet in separate sandboxes that correspond to their website origin domains. By default, these files are authorized to access any resources from their own server. Remote SWF files can be allowed to access additional data from other domains by explicit website and author permissions, such as URL policy files and the Security.allowDomain() method. Remote SWF files cannot load any local files or resources.

Local sandboxes

Local file describes any file that is referenced by using the file:protocol or a Universal Naming Convention (UNC) path. Local SWF files are placed into one of four local sandboxes:

- The local-with-filesystem sandbox—For security purposes, Flash Player places all local SWF files and assets in the local-with-file-system sandbox, by default. From this sandbox, SWF files can read local files (by using the URLLoader class, for example), but they cannot communicate with the network in any way. This assures the user that local data cannot be leaked out to the network or otherwise inappropriately shared.
- The local-with-networking sandbox—When compiling a SWF file, you can specify that it has network ac-

cess when run as a local file.These files are placed in the local-with-networking sandbox. SWF files that are assigned to the local-with-networking sandbox forfeit their local file access. In return, the SWF files are allowed to access data from the network. However, a local-with-networking SWF file is still not allowed to read any network-derived data unless permissions are present for that action, through a URL policy file or a call to theSecurity.allowDomain()method. In order to grant such permission, a URL policy file must grant permission to *all* domains by using<allow-accessfrom domain="*"/>or by usingSecurity.allow-Domain(``*").

- The local-trusted sandbox—Local SWF files that are registered as trusted (by users or by installer programs) are placed in the local-trusted sandbox. System administrators and users also have the ability to reassign (move) a local SWF file to or from the local-trusted sandbox based on security considerations. SWF files that are assigned to the local-trusted sandbox can interact with any other SWF files and can load data from anywhere (remote or local).
- The AIR application sandbox—This sandbox contains content that was installed with the running AIR application. By default, files in the AIR application sandbox can cross-script any file from any domain. However, files outside the AIR application sandbox are not permitted to cross-script the AIR file. By default, files in the AIR application sandbox can load content and data from any domain.

Communication between the local-with-networking and local-with-filesystem sandboxes, as well as communication between the local-with-file system and remote sandboxes, is strictly forbidden. Permission to allow such communication cannot be granted by an application running in Flash Player or by a user or administrator.

Scripting in either direction between local HTML files and local SWF files—for example, using the External Interface class—requires that both the HTML file and SWF file involved be in the local-trusted sandbox. This is because the local security models for browsers differ from the Flash Player local security model.

SWF files in the local-with-networking sandbox cannot load SWF files in the local-with-filesystem sandbox. SWF files in the local-with-filesystem sandbox cannot load SWF files in the local-with-networking sandbox.

Setting the sandbox type of local SWF files

You can configure a SWF file for the local-with-filesystem sandbox or the local-with-networking sandbox by setting the document's publish settings in the authoring tool.

An end user or the administrator of a computer can specify that a local SWF file is trusted, allowing it to load data from all domains, both local and network. This is specified in the Global Flash Player Trust and User Flash Player Trust directories.

The Security.sandboxType property

An author of a SWF file can use the read-only static Security.sandboxType property to determine the type of sandbox to which Flash Player has assigned the SWF file. The Security class includes constants that represent possible values of the Security.sandboxType property, as follows:

- Security.REMOTE—The SWF file is from an Internet URL, and operates under domain-based sandbox rules.
- Security.LOCAL __WITH __FILE—The SWF file is a local file, but it has not been trusted by the user and was not published with a networking designation. The SWF file can read from local data sources but cannot communicate with the Internet.
- Security.LOCAL __WITH __NETWORK—The SWF file is a local file and has not been trusted by the user, but it was published with a networking designation. The SWF file can communicate with the Internet but cannot read from local data sources.
- Security.LOCAL __TRUSTED—The SWF file is a local file and has been trusted by the user, using either the Settings Manager or a Flash Player trust configuration file. The SWF file can both read from local data sources and communicate with the Internet.
- Security.APPLICATION—The SWF file is running in an AIR application, and it was installed with the package (AIR file) for that application. By default, files in the AIR application sandbox can cross-script any file from any domain. However, files outside the AIR application sandbox are not permitted to cross-script the AIR file. By default, files in the AIR application sandbox can load content and data from any domain.

Security rules/Permissions

The way security model is designed meets the requirement of stakeholders. If I have to define who these stakeholders – owners of these resources. The model comprises of resources that are objects. They could be the URLs of some website or the local data and the SWF files. They have a hierarchy for security model to be designed and implemented.

On a business level, Phishing and spoofing emails is a big threat when considering Adobe. A Flash vulnerability that's being exploited by hackers to gain control of victims' machines is the target of a security update released yesterday by Adobe.

"There are reports that the vulnerability is being exploited in the wild in active targeted attacks designed to trick the user into clicking on a malicious file delivered in an e-mail message," Adobe said in a security bulletin.

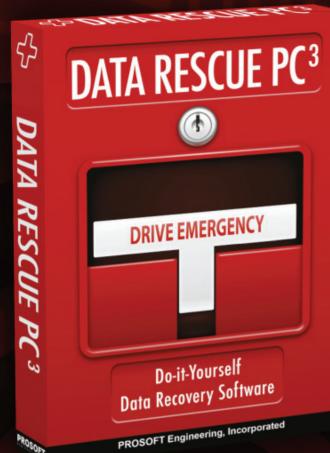
"The exploit targets Flash Player on Internet Explorer for Windows only," Adobe said, but the company urged Mac, Linux, and *Android* users to update their versions of Flash as well. The company provided a linkto help people determine which version of Flash they're running, and it listed which versions are vulnerable.



SWETHA DABBARA

I am a graduate in Computer Science and Engineering with a work experience of about 3 years in IT Sector. Holding a Diploma in Information Security and Ethical Hacking, I am working as a freelance writer for Triond and Wikinut Websites since the year 2010.

Need to recover deleted files? Hard drive crashed? Virus taken over?



System Requirements

Data Rescue PC3 requires no Operating System or installation.

Data Rescue PC3 is provided on a self-booting CD containing a special Operating System & user-friendly GUI-based Data Rescue PC3 software.

Award-winning technology, works when other software fails

- Recovers all types of files from your hard drive.
- Works if the drive fails to mount or only partially operates.
- Recovers deleted, lost and damaged files.
- Recovers digital pictures from your camera media even after it has been erased or reformatted.
- Recover your whole drive or just the files you need.
- Recovers pictures, movies and music from PC drives and any type of digital camera media.

Two ways to use this software!

Application within Windows™

Windows[™] 2000, Windows[™] XP, Windows[™] Vista or Windows[™] 7. Firewire, USB 2.0 or a second hard drive (external or internal) to recover to.

Using included emergency boot CD

PC with CD-ROM Drive, 64MB of RAM, Intel or AMD Processor 300MHz or greater. Firewire, USB 2.0 or a second internal drive to recover to.

Compatible with







www.prosofteng.com

CODENAME: SAMURAI SKILLS COURSE

Penetration Test Training Samurai Skills

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets (Websites , Networks , Servers) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos (Course Updated Regularly)
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace (any time, any where)
- * Our Course is Totally Different from Other Courses (new Techniques)

USER TRAINING AND WRITTEN SECURITY POLICIES MORE IMPORTANT THAN EVER IN A WORLD OF SOCIAL MEDIA & BYOD

KEN KRAUSS

Employees today are desiring access to company resources from all their computing devices rather than being limited to accessing company resources from only those devices owned and managed by the company. Social media and social media applications are also entrenching themselves in the everyday lives of consumers, and to reach many demographics today marketing plans are increasingly focused around social media.

o many companies who have seen their revenues and profits drop during the global economic downturn, having employees use their own computing devices ("Bring Your Own Device" or "BYOD") might now be seen as essential strategy when a few years ago it was unimaginable. If you as a security professional are wondering what steps you need to take in order to protect your organization during this wave of social media use and BYOD, you are not alone.

First, let's examine the individual currents of this wave. The BYOD employee is the administrator of their own machine, installing programs as they like and often in charge of patch management of the operating system, anti-virus program, and other third-party programs such as Adobe Reader, Adobe Flash, Microsoft Office, and the Java Run-time Environment. These programs have been targets for intruders for years, but these third-party programs are widely installed on various computing platforms and are becoming primary targets of hackers in today's security climate.

Rather than having a standardized list of allowed applications on employee devices known to company security managers, with BYOD the list of allowed applications on computing devices is often non-standardized. Further complicating the issue, company IT staff might not even know which device(s) employees use, and might not now be allowed to connect remotely to employee devices for patch management, virus scans, and other security concerns. It is also much more likely that the BYOD employee will be sharing their devices with others that are even less skillfully trained on computer security than your employees are, such as their children or other family members.

Social media relies extensively on blind links, user comments, third-party websites, and browser add-ons which have the potential for a slew of security issues. Further, social media encourages users to share what was formerly very private information about themselves. Thus it has never been so easy to find out heaps of information about company employees that might be used in security challenge questions because many are willingly posting this information on social media.

Just when the average user is becoming familiar with the dangers of viruses, worms, and spyware lurking in spam emails promising enhanced anatomy and revealing photos of celebrities, a new breed of criminal has been created who doesn't mind spending several hours, days, or weeks surfing the pages of your company executives' LinkedIn and Facebook pages during reconnaissance, or even hijack accounts for focused attacks akin to social engineering. This more determined criminal knows that users and company security personnel are more educated these days and much more likely to be updating operating systems with security patches as well as having up-to-date anti-virus and anti-malware protection. Because of that, this determined criminal knows attacks against the operating system directly are not going to be as successful as attacking Flash, Reader, Word, Excel, or Java vulnerabilities because these programs are often not patched as regularly as the operating system and anti-virus are. This more determined criminal also knows that some degree of human error is inevitable no matter how well trained the user, yet the users with the highest levels of access to company resources (such as owners and senior managers) might be among the most inexperienced users of computing devices in your company and thus the most likely to choose simple passwords, reuse passwords them across numerous accounts on numerous websites, and generally make more errors while responding to security threats.

Simultaneously, criminals and other nefarious persons operating online have powerful tools available at their disposal to use in penetrating your company network and extracting valuable information. What are the attack vectors they will take? First of all, either the attackers will be focused on your organization specifically, or they will have stumbled across your organization in a wide scan for the "low hanging fruit" of easy targets. If they are focused on your company specifically, they will likely have a wealth of information available online about your company's technical infrastructure and personnel to start with including "secret" information used in security challenge questions and weak passwords such as company executives' mother's maiden name, first job, kids' names, pets' names, birthdays, and hobbies.

Recent high-profile attacks against security companies such as RSA, defense contractors such as Lockhead Martin, and websites such as Google during the "Aurora" attacks have all spawned initially from unpatched vulnerabilities in Adobe Reader and Flash. Also recently, online and offline research coupled with brute force password and security challenge question guessing by an individual with limited technical skill led to the compromise of cell phone accounts of celebrities such as Scarlett Johansson, Vanessa Hudgens, and Jessica Alba. If someone with limited technical skill could compromise the cell phones of numerous Hollywood starlets, what could an attacker with lots of technical skill do to the senior executives of your company? And not just them, but those close to them, too?

Accounts on social media websites (as well as instant messaging and email accounts) can also be compromised and used to attack unsuspecting users who believe they are communicating with friends, family, and other known acquaintances rather than criminals who have hijacked an account. By taking over accounts of those individuals known to the target, the attackers can achieve a much higher level of implicit trust by the target and thus can achieve much more disastrous results. If your "boss" emails you and asks for the login to your company DNS registration, would you send it back without seeking any offline confirmation? What if your "mother" asks you to read a PDF file? Attacks using hijacked accounts have been some of the most successful I have seen recently, and I expect that to continue and be adapted for many different purposes such as social engineering attacks including

tricking an unsuspecting user into opening some type of compromised file.

What Can Be Done?

"Defense in depth" means layers of security defenses protecting valuable assets and is a well-respected methodology for protecting your network. Attackers are going to try and parlay any breach of defenses into a wider breach of defenses until they have complete control of your network and its valuable information. Assuming certain corporate defenses can't be totally breached simply by knowing one of your company executive's mother's maiden names or first jobs (these are common security challenge questions for your company's corporate website registration or hosting), attackers will have to probe to find the easiest route to penetrating your network and often the easiest route into a corporate network in today's security climate will be through popular third-party applications such as Adobe Reader and Flash. Due to the amount of personal information available online about company employees, it is easier than ever to craft emails written to specific individuals (aka "spearfishing") that can trick them into visiting compromised websites or opening infected third party application files that can breach lines of security defenses. If you're the "low hanging fruit" in the crosshairs of an attacker, it might be because they already tricked a user to open an infected Flash or Reader file that successfully penetrated at least one line of defense, or because the attackers have already brute forced at least one of your user accounts.

Training for End Users

Without a doubt, one of the biggest factors in network defense is the security knowledge of network users. Attackers will find your least-skilled user(s) with access to critical information (often company owners and senior managers) and exploit them. With more administrative tasks being shifted to the end users and more information available online that can be used as ammunition against your network defenses, user training is more important than ever. End users likely are being tasked with doing more with less resources, so their time is also more valuable than ever, and a security training program that fits their demanding schedules while being well-received by the employees and business management is ever more of a challenge.

Instead of trying to set up large, lengthy security training seminars, focus on extending the employee communications already used within your company to provide short, easy to understand security tips. Five to fifteen minutes should be enough time to convey several important security tips without overwhelming nontechnical users, and in this current economic climate, it will be seen as a cost advantage to add an extra few minutes to existing employee meetings for security training rather than schedule new meetings specifically for security training. Regular training across diverse media is also important for end user retention, so try to include security tips frequently in company emails; record audio and video training about security topics and post in a company wiki; manage an internal blog of important security tips and information; have employees role play scenarios with IT staff so that they are familiar with the situations where they make crucial decisions regarding security; and/or require employees answer short questionnaires on security awareness.

Focus on the education of your users, rather than blaming them for past or potential security lapses, and your security training will be much better received. Security awareness training will also be much more effective if you only have a few points to emphasize at a time rather than trying to educate the user on 20 or more security topics in a 15 minute time span. Give the user more frequent, easier-to-digest bits of information without being monotonous, and you will experience much less user pushback the next time a security awareness meeting comes around. Also, try to highlight any attacks that were successfully thwarted during your next security awareness meeting so that your end users receive positive feedback for a job well done. Praise publicly while keeping any criticism limited to private meetings.

Effective User Training

- ** Do not overwhelm your end users
- ** Short, easy-to-understand bits of information
- ** Focus on just a few things at a time
- ** Add security tips to existing staff communication (such as newsletters &emails)
- ** Post in common areas such as the break room
- ** Praise in public while saving any criticism for private, one-on-one meetings

Figure 1. Effective User Training

Training for Network Administrators and IT Staff

The continued need for training of IT staff, even in a difficult economy, is critically important to corporate safety. I encourage both vendor-neutral and vendor-specific training and certification for your IT staff. At a minimum, your staff should be familiar with the SANS Institute list of the Top 20 Critical Security Controls (Version 3.1, http://www.SANS.org/critical-security-controls/).

- Inventory of Authorized and Unauthorized Devices
- · Inventory of Authorized and Unauthorized Software
- Secure Configurations of Hardware and Software on Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defenses
- Application Security Software
- Wireless Device Control
- Data Recovery Capability
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defense
- Maintenance, Monitoring, and Analysis of Security
 Audit Logs
- Controlled Access Based on the Need to Know

Account Monitoring and Control

- Data Loss Prevention
- Incident Response Capability
- Secure Network Engineering
- Penetration Tests and Red Team Exercises

Take note that inventories of hardware and software are at the top of the SANS list of critical security controls. while properly configuring equipment is only ranked #3. In an organization of any size at all, managing an inventory list of hardware and software can be a challenge, especially if your staff are using their own computing devices. If your organization goes BYOD, managing the list of acceptable devices and software may be seen as too much administrative overhead for your company. If your company makes this policy decision, it is imperative to counter this with additional security controls elsewhere. It is especially important to have secure configurations of your laptops, phones, and workstations as well as the best available anti-virus and anti-malware protection if your organization is not keeping a comprehensive list of approved devices and software. Using remote management apps that are cross-platform such as TeamViewer (TeamViewer.com), your IT staff can help your end users keep their devices secure, even if your end user is responsible for most or all of the patch management and anti-virus scans on their own devices.

Honestly, most organizations struggle to keep up-todate lists of approved devices and software even when their employees are only using company-owned phones and computers, so this a broad area that most companies can improve on considerably. The amount of devices needing to be inventoried may double or triple when your users start using their own devices for work, but the additional security provided by the effort is worthwhile. If you suspect a security compromise, having an accurate list of allowed devices and software can dramatically increase your effective response time.

SANS Critical Controls

- #1: Inventory of Authorized Devices
- #2: Inventory of Authorized Software
- #3: Secure Configurations of All Workstations, Laptops & Servers
- #4: Continuous Vulnerability Assesment & Remediation (including Patch Mangement)
- #5: Malware Defenses (Anti-Virus & Anti-Spyware)

Source: http://www.SANS.org/critical-security-control

Figure 2. SANS Critical Controls

Written Security Policies

Security awareness training relies heavily on written security policies to underpin the foundations of security knowledge you are seeking to establish in your end users. They add another layer to your security defenses by giving your users something concrete to refer to if they are ever in doubt of your company's security policies. Additionally, written security policy serves to coordinate management agreement on aspects of how to secure the organization.

At a minimum. I recommend having all users read and agree to in writing an Acceptable Use Policy, a Password Policy, and a Non-Disclosure Agreement at their time of hiring. These policies should be reviewed frequently with end users, and your company may wish to have your users renew these contracts annually. Not all your company's security policies need to be written in contract form, with consequences stated for noncompliance, but they should all be written in easy-tounderstand language, dated, and released with version numbers. The more professionally written your company security policies are, and the more committed to the security policies your senior managers are, the more likely your employees are to follow them. Consider having posters created of your information security policies to post in common areas such as the employee break room much like OSHA workplace safety posters are in the United States.

An Acceptable Usage Policy traditionally lists items such as applications to be used or not used by the end user, how the user is to connect to company resources locally and remotely, and acceptable use of things like social media and instant messaging. In this era of BYOD, the Acceptable Usage Policy should be expanded to prescribe patch management policies for all installed programs, not just the operating system and security software, as well as anti-virus / anti-malware scanning and removal policies for those users that administer their own computers. Password Policies for those users that administer their own devices will be harder to enforce than on company-owned and managed devices, but still should be used.

* Secures management agreement on security

- & gives users something concrete to refer to
- ** Use easy-to-understand language
- ** Date & apply version numbers
- ** Employees most likely to follow policy if presented professionally & senior management is fully committed
- ** Plan how to handle non-compliance

Summary

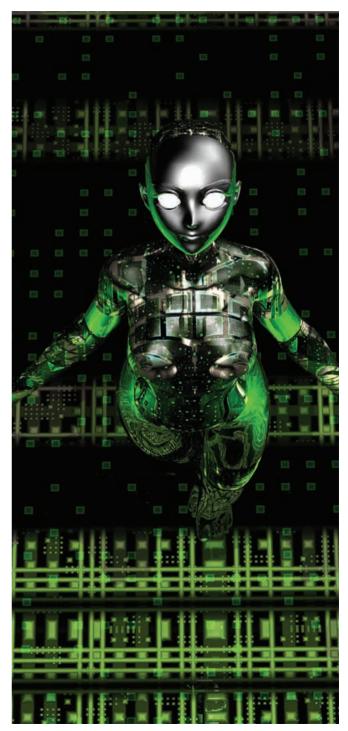
As the tech landscape continues to change, the way your company handles technology will have to change with it. Security administrators don't usually like change, because with change comes unknown security risks that could be exploited and reflect poorly on us, however two things security administrators have resisted strongly for years are now here to stay for many: social media use in the workplace and employees using their own computing devices (BYOD) for mission critical tasks on a day-to-day basis. Additionally, third-party programs are increasingly becoming the attack vector criminals are using in very targeted attacks to breach security defenses. However, time-tested techniques such as training for end users and administrators; aggressive patch management; comprehensive device / software inventories; and written security policies can keep the criminals attacking your enterprise at bay.



KEN KRAUSS

is a computer security consultant, network administrator, and web developer living in Kansas City, Missouri, USA. He holds many certifications including ISC² Certified Information Systems Security Professional (CISSP); CIW Security Analyst; and CompTIA Security+, Network+, and A+. He has helped everyone from home users to large companies with their technology challenaes through his businesses Computer Help Per-

sonalized (CHPKC.net), Kansas City Web Development (KCWebDev.com), and Vertical Data Recovery (VerticalDR.com).



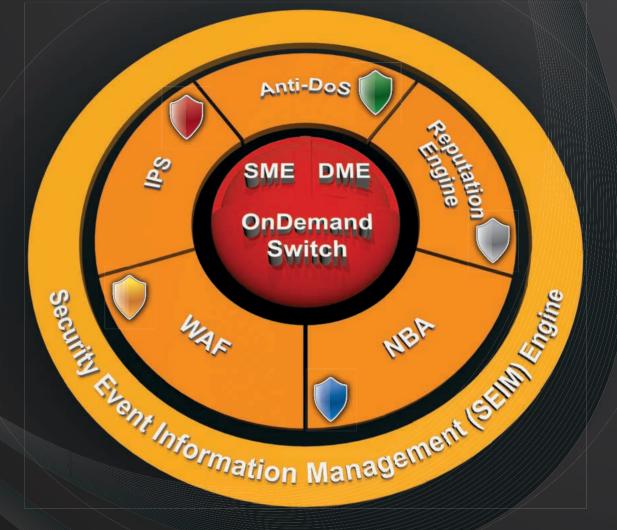
Reimagined for Small Business COMODO ENDPOINT SECURITY MANAGER

Centrally manages the deployment of award-winning Comodo Internet Security software to protect the desktops and servers your business relies on against internal and external threats.

COMODO®

www.comodo.com

radware



Protecting Networks from a New Age of Hacktivism

Radware Attack Mitigation System:

- Real-time, Multi-vector Attack Detection
- Hardware Accelerated DDoS Mitigation
- Integrated Event Correlation & Reporting
- 24x7 Emergency Response Team Support

Hakin9 EXTRA

HARD DISK DIAGNOSTICS: OPPORTUNITIES AND SOLUTIONS

DMITRY POSTRIGAN

It is not a secret that every data recovery specialist must perform a full diagnosis of a hard disk drive to find the problem or the disk state in general as the very first step in all data recovery cases. Only accuracy and competent approach can guarantee the extraction the maximum amount of a data to avoid further damage to the hard drive. Have you ever considered what it takes to find the exact state of the customer's drive? Usually, it is a quite complex task that involves a number of tests, guesses, and risks; and it has been like that for many years.

believe it's time to offer something better. Atola Insight provides the unique, fully-automated in-depth diagnosis of any PATA or SATA hard drive. Just one click, and in a few minutes, you'll have the full diagnosis report outlining the exact issue.

First steps in diagnostics. History remembers a lot of examples of fundamental diagnostics methods: earlier hard disk drives were big and heavy, and the process of testing was very complicated. One of the most unusual and, at the same time, effective ways of performing the initial testing of an HDD was through the noise it makes on start-up. This method, however, required significant skills in electronics design plus years of experience dealing with damaged hard drives.

The hard disk technology has progressed tremendously over the past years; the hard drives are so much more complex now than they were just several years ago. As technology evolves hard disk diagnostics become more and more challenging and sophisticated.

How it works. First of all, I would like to emphasize that the Atola Insight diagnostics function is performed in a fully automatic mode. The tool automatically detects the model and serial numbers, capacity, security status, and other characteristics of a hard disk drive. However, the tool does not stop there. It also analyzes the hard drive's SMART and firmware; performs media access tests for each head to detect degraded or damaged heads. Finally, if the drive is fully working, it runs a partition and file system checkup.





The most interesting part is done in parallel with all these tests: Atola Insight records and analyzes the current that is drawn by the hard drive. This is similar to analyzing the noise that the hard drive makes on start-up; however, the current analyzer approach is much more consistent and accurate. The use of the current analyzer allows diagnosing even non-identified or non-recognized drives with fried electronics, motor or head damage.

The automatic diagnostics process identifies damage in the following areas:

- Circuit Board (PCB)
- Motor
- Heads
- Media Surface
- Firmware Area
- · Partitions and File System

Circuit Board (PCB) and motor. The Circuit Board and the motor are the first parts to be examined. The tool applies power to the drive and analyzes the form of the current at is drawn by the drive. It also analyzes the state of the hard drive's registers and responses to the basic ATA commands.

Heads. The tool tests each head separately and measures its media access timing and speed in megabytes per second. This allows the detection of degraded and damaged heads.

Media Surface. Atola Insight verifies the outer, middle, and inner tracks for defects. This allows estimating the number of defects on the media.

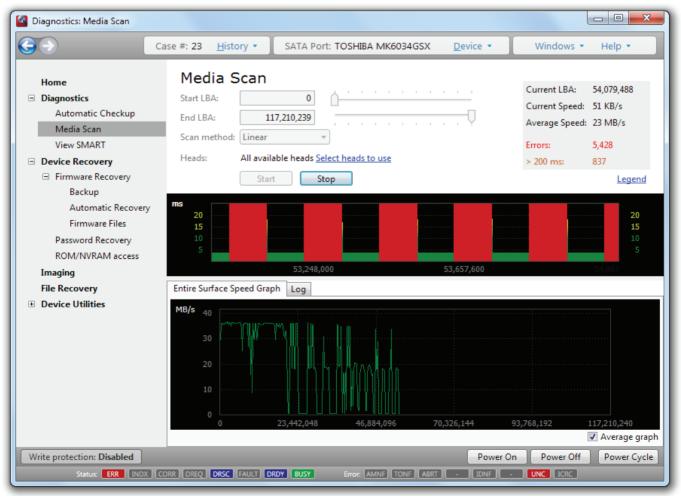
Firmware. The tool thoroughly verifies the state of all hard drive registers; examines ID sector, SMART tables, as well as, HPA, DCO and Security statuses and looks for signs of firmware damage. If there is any inconsistency, the tool will report it right away.

File system. At this point, the tool will determine whether it is safe to run the file system checks. If the drive is healthy, Atola Insight will verify all partitions and file systems for any damage.

Diagnostic report. In just a few minutes, Atola Insight presents you with a complete diagnostic report with high-lighted issues and recommendations. You can download samples of diagnostics reports from our website.

Media scan. It's an additional option for in-depth diagnostics. Three modes of scanning are provided here: linear, backward and fast. In the fast mode, the tool reads only several thousand sectors per million, which speeds up the process tenfold or even more. All of these methods are extremely effective for different situations.

Two graphs are displayed during the scanning: one shows the read speed of a range of sectors in milliseconds; the other shows the speed in megabytes per second. The tool also shows which part of the graph corresponds to each physical head. Media Scan is the perfect way to determine surface and head damage.



Media scan of damaged drive

Hakin9 EXTRA

→	IDE Master: Maxtor 6B200P0 Device • History	▪ <u>W</u> indows ▼ <u>H</u> elp ▼
Home Diagnostics Automatic Checkup Media Scan	Checking Heads Media access timing	Check list Circuit Board Heads Media Surface Firmware
View SMART Device Recovery	Stop	File System
Imaging File Recovery		
	Device is ready Registers: 0101 0501 0001 0000 0000 E0E0 5050 Alt: 5050 Peak power consumption during spin-up: 5V line = 961.91 mA; 12V line = Status register seems to be valid. Interface check passed. Device has been identified: Maxtor 6B200P0 SN: B41VD1CH Circuit board looks fine	= 3121.95 mA
	Heads Checking power consumption curves for signs of head damage Identifying the device Detecting device family All device identification checks have passed. Performing media access timing verification	

Disk Automatic Checkup

Hard drives with multiple issues. From time to time, data recovery specialists have to deal with hard disk drives that have more than one problem. In some cases, Atola Insight identifies multiple errors at once. In other cases, only the first and most critical failure is determined during the first diagnostics run; further failures will be determined after the most critical one is resolved. For example, if a hard drive has both PCB and firmware failure, only the PCB damage will be identified at first because the PCB is required to be fully operational in order to successfully diagnose firmware. Once the PCB is repaired, the HDD will need to be diagnosed a second time in order to identify the damage to the firmware area.

Case management. Looking into past experience working as a data recovery engineer and maintaining the proper history for each data recovery job were always big nuisances I had to make notes on everything I did with the drive, either on a piece of paper or in a separate software. In the end, I wasted a lot of time and could easily make a mistake putting a record into the wrong place. Atola Insight does all that for me automatically it tracks everything I do with the drive absolutely seamlessly; all actions and reports are stored in the database. I can also enter a custom note should I need to perform an action that does not involve Atola Insight. Everything is kept in one database, and all records can be pulled with just a couple of clicks of the mouse.

Conclusion. Whether you are a seasoned professional or just starting a data recovery business, you can't go without performing full diagnostics on all hard drives coming in for recovery. Atola Insight's diagnostics function is absolutely unique and unmatched in diagnosing hard disk drives. Its automatic in-depth diagnostics save a significant amount of time and help prevent further damage to drives due to a lack of diagnosis or even misdiagnosis (Figure 5).

Those who try Atola Insight at least once would never want to use anything else. Atola Insight is the only tool on the market that includes amazingly simple user interface combined with the latest data recovery technology.



DMITRY POSTRIGAN

Has been researching hard disk drives since 2000. He is the creator of MHDD, a widely known low-level hard disk diagnostics tool and is also founder of Atola Technology.



Szukaj nas takze na







www.ashampoo.com

SECURITY TEAMS AT ADOBE

Adobe has a team in place (the Adobe Secure Software Engineering Team – ASSET), which is dedicated to ensuring our products are designed, engineered and validated using security best practices. Brad Arkin, senior director of security for Adobe's products and services, leads that team. A second team within ASSET (the Product Security Incident Response Team – PSIRT) is responsible for responding to and communicating about security issues. ASSET and PSIRT (as they exist today) were put in place during the integration of Macromedia and Adobe in late 2005 by combining the corresponding security teams from each company, and these teams continue to evolve to best address the threat landscape facing Adobe's products.

A II engineering teams at Adobe work very closely and proactively with the Adobe Secure Software Engineering Team (ASSET) during each phase of the Adobe Secure Product Lifecycle (SPLC). In addition, product teams have dedicated security development and testing groups in place. As a result of changes in the threat landscape, we have about seven times as many engineers dedicated to security today compared to 2009.

The Adobe Secure Product Lifecycle (SPLC)

ASSET owns the Adobe Secure Product Lifecycle (SPLC), which is the equivalent to Microsoft's Security Development Lifecycle (SDL). All code and features in Adobe products are subject to the SPLC. The SPLC integrates standard secure software activities such as threat modeling, automated and manual security code reviews, and fuzzing into the standard Adobe Product Lifecycle we follow for all projects. The graphic/screen shot below shows the different phases of the SPLC as well as key aspects of each phase.

The ASSET Certification Program

A program that was introduced by ASSET in February 2009 and which has become a critical part of the SPLC is the "ASSET Certification Program." This is an internal program for Adobe engineering and product teams designed to raise security awareness and implement best practices prior to and during the planning and design phases of a product to ensure potential areas for vulner-

abilities are identified and addressed early. A majority of Adobe's product/engineering team members have gone through the program.

Product Security Incident Response

Adobe also has significant investment in our reactive capabilities in the event of a security incident. The Product Security Incident Response Team (PSIRT) coordi-



Figure 1.

nates with the security community (including vendors and researchers) as well as the internal engineering teams and communications teams to get relevant information such as threat mitigations out to users as soon as possible.

Product Security Initiatives

Over the last three years in particular, we have increased the investment in our security efforts with focused initiatives, increased response times, and improved communication to customers and stakeholders. This included improving the security of legacy sections of the code base by targeting high risk areas of the application for fuzzing, static code analysis, manual code review, threat modeling, and strengthening input validation. And we significantly improved incident response processes for regularly scheduled updates as well as for urgent situations, such as a zero-day.

We also made a number of significant security enhancements specifically to Adobe Reader and Acrobat:

- With the Adobe Reader / Acrobat update in October 2009, we included security enhancements around Adobe Reader and Acrobat's handling of JavaScript – at the time one of the main attack vectors for PDF/ Adobe Reader. These include the ability to disable JavaScript using an improved "gold bar" user interface (improvement from previous pop-up box), significant improvements to strengthen input validation on all JavaScript calls, as well as the introduction of a JavaScript blacklisting mechanism.
- With the April 13, 2010 Adobe Reader / Acrobat update, Adobe activated a *new Adobe Reader Updater / Adobe Acrobat Updater.* The new updater is designed to keep end-users up-to-date in a much more streamlined and automated way. It was introduced because the majority of attacks we are seeing are exploiting software installations that are not up-todate with the latest security updates. With the activation of the new updater, Windows users have the option to download and install updates for Adobe Reader and Acrobat automatically, without user interaction. The following three update options are available to users:
 - Automatic: Updates are downloaded and installed automatically, without user interaction. Adobe recommends this option for most end-users. (Available for Windows users only.)
 - Semi-Automatic: Updates are downloaded automatically, but the user has to choose whether or not to install the update.
 - Manual: The user has to manually check for updates and kick off the installation. This option may appropriate in particular for administrators in businesses following patch cycles specific to their organization.
- On November 18, 2010, Adobe *announced* the availability of Adobe Reader X with Protected Mode (aka sandboxing) under Windows. Adobe Reader Protected Mode represented an exciting new advancement in mitigating the impact of attempted attacks. Even if exploitable security vulnerabilities are found by an attacker, Adobe Reader Protected Mode will help prevent the attacker from writing files or install-

ing malware on potential victims' computers. In a future release of Adobe Reader, Adobe plans to extend the sandbox to include read-only activities to protect against attackers seeking to read sensitive information on the user's computer.

- With the Adobe Reader / Acrobat update on June 14, 2011, Adobe *introduced* Adobe Acrobat X (10.1) Protected View (aka sandboxing). This security enhancement for Adobe Acrobat extends the concept of Adobe Reader Protected to the Acrobat browser plugin; it also introduces Adobe Acrobat Protect View for document viewing with Acrobat in standalone mode. Adobe Acrobat Protected View offers similar mitigations and user workflows to Microsoft Office 2010 Protected View. Acrobat Protected View provides an additional layer of protection for Acrobat X users and will ultimately result in a safer experience, fewer urgent patches, and lower total cost of ownership in enterprise environments.
- On January 10, 2012, Adobe <u>added</u> a new JavaScript whitelisting capability in Adobe Reader and Acrobat X (10.1.2) and 9.5, allowing JavaScript execution in PDF files based on document trust. If a document is trusted, JavaScript execution will be allowed; but if it is untrusted, Adobe Reader and Acrobat will prevent all JavaScript execution.
- With the Adobe Reader / Acrobat on April 10, 2012, Adobe announced the following changes:
 - Rendering Flash (SWF) Content in Adobe Reader and Acrobat 9.5.1: We added an Application Programming Interface (API) to both Adobe Reader/Acrobat 9.5.1 and Flash Player to allow Adobe Reader/Acrobat 9.5.1 to communicate directly with a Netscape Plugin Application Programming Interface (NPAPI) version of Flash Player installed on the user's system. Starting with the release of Adobe Reader 9.5.1 and Acrobat 9.5.1, Adobe Reader and Acrobat 9.x on Windows and Macintosh will use the Adobe Flash Player plugin version installed on the user's system (rather than the Authplay component that ships with Adobe Reader and Acrobat) to render any Flash (SWF) content contained in PDF files. From a security perspective, this means that Adobe Reader/Acrobat 9.x users will no longer have to update Adobe Reader/Acrobat each time we make available an update for Flash Player. This will be particularly beneficial to customers in managed environments because fewer updates help reduce the overhead for IT administration. We are currently working on integrating the same API into Adobe Reader and Acrobat X, and will follow up with another blog post once this functionality is available in version X.

- Rendering 3D Content in PDF Files.

With the Adobe Reader and Acrobat 9.5.1 updates, 3D content is turned off by default, since the majority of consumers do not typically open PDF files that include 3D content. 3D content in untrusted documents can pose a security risk, so we disabled the option by default to cut down on potential risk for users of Adobe Reader and Acrobat 9.x. - Further Alignment of the Adobe Reader/Acrobat Update Cycle with Microsoft's Model After three years of shipping a security update once a quarter and announcing the date of the next update the same day we ship the current update, we are making a change. We are shifting to a model that more closely aligns with the "Microsoft Patch Tuesday" cadence. Since we introduced the guarterly update cycle in 2009, we have come a long way in putting mitigations into place that make Adobe Reader and Acrobat a less attractive attack target. Sandboxing Adobe Reader and Acrobat X, in particular, has led to greater than expected results. Attackers have indicated through their target selection thus far that the extra effort required to attack version X is no longer worth it. Additionally, we have seen a lower volume of vulnerability reports against Adobe Reader and Adobe Acrobat. Given the shift in the threat landscape and the lower volume of vulnerability reports, we feel that a strict guarterly release cycle is no longer warranted.

On the Flash Player side, note the following significant security (and privacy) enhancements made over the last two years:

- On December 1, 2010, Adobe and Google announced the development of a sandbox for Flash Player within the Google Chrome browser. This first iteration of Chrome's Flash Player sandbox for all Windows platforms introduced a modified version of Chrome's existing sandbox technology that protects certain sensitive resources from being accessed by malicious code, while allowing applications to use less sensitive ones. This implementation represented a significant step in further reducing the potential attack surface of the browser and protecting users against common malware.
- With the launch of Flash Player 10.3 on May 12, 2011, Adobe introduced a number of important security and privacy features: Flash Player 10.3 included a new auto-update notification mechanism for the Macintosh platform. With this new feature, Macintosh users started receiving Flash Player update notifications when new updates became available. (Note that this functionality was already previously in place for Windows users.) On the privacy side, Adobe worked closely with representatives from several key companies/open-source browsers-including Google and Mozilla-to define a new browser API (NPAPI ClearSiteData) for clearing local data. Any browser that implements the new API is able to clear local storage for any plugin that also implements the API. Flash Player was the first plugin to support the new API, providing users with a simpler way to clear local storage from the browser settings interface, similar to how they clear their browser cookies. In addition to coordinating with the open-source browsers, Adobe also teamed up with Microsoft to provide equivalent functionality within Internet Explorer. With the launch of Flash Player 10.3, users were able to take advantage of this

functionality in Internet Explorer 8 and 9. And last but not least, Flash Player 10.3 introduced a redesigned Flash Player Settings Manager to make it easier for users to manage their Flash Player settings, which allowed Windows, Mac and Linux users to access the Flash Player Settings Manager directly from the Control Panel or System Preferences on their computers.

- On September 21, 2011, Adobe introduced several security enhancements for Flash Player, including the addition of support for SSL socket connections, which will make it easier for developers to protect the data they stream over the Flash Player raw socket connections, and a secure random number generator.
- On February 6, 2012, Adobe launched a public beta of Flash Player with sandboxing (aka "Protected Mode") for the Firefox browser. Adobe Flash Player Protected Mode for Firefox 4.0 or later is expected to be available very soon and will be supported on both Windows Vista and Windows 7.
- With the release of Flash Player 11.2 on March 28, 2012, Adobe introduced a new background update mechanism for Windows users, designed to keep end-users up-to-date in a much more streamlined and automated way. Windows users have the option to download and install updates for Adobe Flash Player automatically, without user interaction. After a successful installation of Adobe Flash Player 11.2, users were presented with a dialog box to choose an update method. The following three update options are available to users:
 - Install updates automatically when available (recommended)
 - Notify me when updates are available
 - Never check for updates (not recommended)

Additionally, the user can change the update preferences at any time via the Flash Player Settings Manager, which for Windows users can be accessed via the Control Panel. The new Adobe Flash Player background updater updates all instances of a release version of Adobe Flash Player for all Web browsers on a computer. Previously, users had to perform separate updates for each Web browser running on their system. A Mac version of the Flash Player background updater is currently in beta and will be available very soon.

Community Engagement

In addition to working very closely with the security research community, ASSET/PSIRT have great working relationships with counterparts in other organizations such as Microsoft, Symantec and McAfee—which we leverage for the exchange of technical and process information as well as telemetry regarding attack data and techniques.

As part of our collaboration with Microsoft, we announced on July 28 that Microsoft will extend its Microsoft Active Protections Program (MAPP) to include vulnerability information sharing from Adobe starting this fall. See http://blogs.adobe.com/asset/2010/07/

working-together.html for additional information on this announcement.

In another example, Adobe has been working closely with Microsoft to help improve the software update experience for our mutual customers. We recently introduced support for Microsoft System Center Updates Publisher (SCUP) in Adobe Reader X and Adobe Flash Player, making it easier for Microsoft System Center Configuration Manager (SCCM) and Microsoft System Center Essentials (SCE) customers to import Adobe updates through the Microsoft System Center Updates Publisher (SCUP) and manage their distribution to client computers.

In September 2009, Adobe joined SAFECode (Software Assurance Forum for Excellence in Code), a nonprofit organization focused on the advancement of effective software assurance methods. As a SAFECode member, Adobe is actively involved in partnering with other SAFECode members to share lessons that we've learned with the software industry. Brad Arkin is a member of the SAFECode board.

Adobe is also one of the original participants of the "Building Security In Maturity Model" (BSIMM) study and a member of the BSIMM Advisory Board. BSIMM was first launched in March 2009, and is the industry's first and only structured set of best practices for software security based on real-world data. The BSIMM project is led by Fortify Software and Cigital, and is designed to help software vendors determine where they stand with their software security initiative and how to evolve their efforts over time. The original nine companies contributing to the BSIMM were Adobe, The Depository Trust & Clearing Corporation (DTCC), EMC, Google, Microsoft, QUALCOMM, Wells Fargo and two un-named financial institutions.

And last but not least, the Adobe Product Security Incident Response Team (PSIRT) is a member of the Forum of Incident Response and Security Teams (FIRST). FIRST brings together a wide variety of security and incident response teams, including product security teams from the government, commercial, and academic sectors.

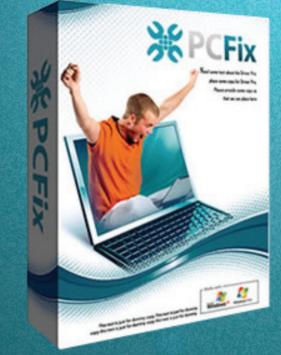
BRAD ARKIN

is also a member of the BSIMM (Building Security In Maturity Model) advisory board, the SAP Security Advisory Board, and the customer advisory boards for security consultancy iSec Partners and security tools vendor Veracode.

Adobe Security Resources

- Adobe Security Portal: http://adobe.com/security
- Adobe Secure Software Engineering Team (ASSET) Blog: http://blogs.adobe.com/asset
- Adobe Product Security Incident Response Team (PSIRT) Blog: http://blogs.adobe.com/psirt
- Adobe Security on Twitter: @AdobeSecurity
- Brad Arkin on Twitter: @BradArkin
- Wiebke Lips on Twitter: @WiebkeLips





Fix Windows Registry & Repair PC Errors!



Before you continue:

Free scan your Computer now! Improve PC Stability and performances Clean you registry from Windows errors

Instant Scan

Image: Starse starse

StaffCop Standard allows you to monitor all activities on company computers and prevent the unauthorized distribution of sensitive corporate information.

StaffCop will help you:

To locate possible data loss channels and prevent loss To gain insight into how your employees spend their work time To increase company and departmentals efficiency

You need StaffCop to:

Gather work time efficiency statistics Easily control your employees in real-time mode Improve discipline and motivation of your employees

Who needs StaffCop:

CEO/CTO Corporate Security Manager HR Manager System Administrator

More Information, Demo Versions, Videos and Technical Guides -

www.STAFFCOP.com

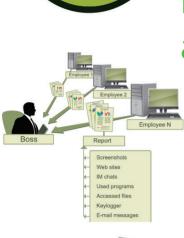
Phone: +1-707 -7098405 Skype: staffcop.com Email: sales@staffcop.com, paul@atompark.com





Main Features of StaffCop:

Screenshot recording Application monitoring E-mail monitoring Web site monitoring Chats/IM activity recording **USB** device monitoring **Clipboard monitoring** Social Networks Monitoring Search Term Tracking File and Folder tracking Keystroke recording System Event Monitoring Whitelists and Blacklists PC activities reporting Stealth installation/monitoring Strong security Alert notifications Remote Install / Uninstall



> Learn to follow the trail of digital evidence in UAT's cyber security lab funded by the Department of Defense.

> Support corporate, law enforcement and legal communities in the investigation and analysis of digital data.

> Evaluate, select, deploy and assess computer forensics measures to respond to and alleviate a security incident to prevent loss or corruption of sensitive information.

TechnologyFORENSICS

Join the new breed of detectives.

Program accreditations, affiliations and certifications



1010101001010101010101

010



010111101010 Dimion001010

1010101

-10

01010101010





CLUSTERGEEK WITH CAUTION

LEARN, EXPERIENCE AND INNOVATE WITH THE FOLLOWING DEGREES: Advancing Computer Science, Artificial Life Programming, Digital Media, Digital Video, Enterprise Software Development, Game Art and Animation, Game Design, Game Programming, Human-Computer Interaction, Network Engineering, Network Security, Open Source Technologies, Robotics and Embedded Systems, Serious Game and Simulation, Strategic Technology Development, Technology Forensics, Technology Product Design, Technology Studies, Virtual Modeling and Design, Web and Social Media Technologies



TAKE YOUR SLEUTHING TO THE NEXT LEVEL WITH A Degree in technology forensics www.uat.edu/techforensics

Please see www.uat.edu/fastfacts for the latest information on program performance, placement and costs.