

Take Advantage of Software Improvements

New security technologies and software development methodologies have drastically improved the security posture of software and systems released over the last decade. Specifically, new software anti-exploitation features in conjunction with the adoption of systematic development processes have contributed to this improvement. Obtaining value from software improvements is only possible through product upgrades and timely deployment of patches.

Why Upgrade?

Software security countermeasures are reactive in nature and evolve with the attack landscape. As attackers discover new attack vectors, defenders devise new defensive capabilities. Typically, only major upgrades, to include service packs, incorporate new capabilities, as shown in Figures 1 and 2 below (Microsoft Windows^{®[1]} and Apple iOS^{®[2]}, respectively). Deploying software with the latest anti-exploitation

features significantly increases the difficulty for adversaries to exploit vulnerabilities. These features have the potential to make known and unknown bugs difficult or impossible to exploit. This forces an adversary to spend considerable resources to bypass defenses or find new vulnerabilities.

Examples of anti-exploitation features in operating system (OS) software include:

- ▶ **Address Space Layout Randomization (ASLR):**
Prevents loading of attack code into known memory addresses
- ▶ **Data Execution Prevention (DEP):**
Prevents data areas in memory from being used as attack code
- ▶ **Secure or Trusted Boot:**
Verifies that only the intended OS is loaded



Figure 1: Progression of security features in Windows operating systems.

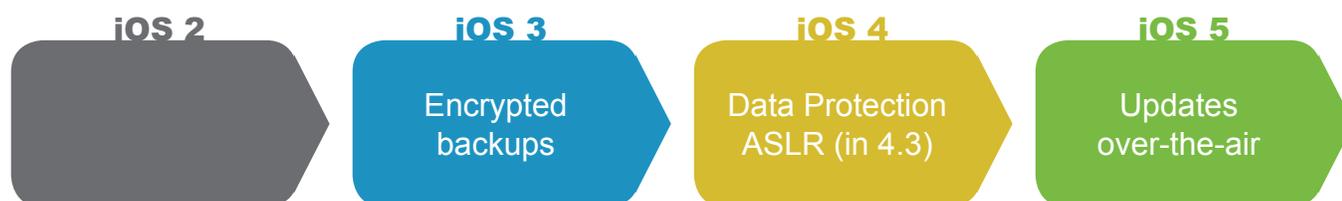


Figure 2: Progression of security features in Apple iOS operating systems.

FUTURE
DEVELOPMENTS



Confidence in Cyberspace

October 2013
MIT-011FS-2013





New features often require low-level architectural changes, so their adoption in older versions is unlikely or incomplete. For example, Bitlocker^{®[1]}, ASLR, DEP, and User Account Control (UAC) will never be fully backported to Windows XP^{®[1]}. By upgrading systems, enterprises make themselves dynamic, and therefore more difficult, targets. Although upgrading to newer operating systems and applications incurs costs, these costs pale in comparison to losses of strategic information from a compromise.

Why Patch?

The Common Vulnerabilities and Exposures (CVE) database at <http://cve.mitre.org> demonstrates the sheer volume of vulnerabilities that are reported daily and patched by vendors. Responsible enterprises — and malicious adversaries — act on this information. Malicious actors race to develop working exploits by analyzing and reverse engineering each software patch. Delaying or ignoring patches for vulnerabilities considerably increases the chance of systems being exploited, in particular Internet connected systems. Recent research¹ has found that for 88% of publicly disclosed vulnerabilities, a working exploit is available on the same day, which makes it imperative that patches be deployed immediately.

Some enterprises delay or ignore patches due to the misconception that patches often break or slow down applications. Administrators should be aware that vendors perform significant testing to these patches prior to the deployment of updates.^{2,3} in order to ensure this remains rare. For those enterprises with residual concerns about applying updates in their environment, the cost of pre-deployment testing is miniscule compared to the devastating cost incurred from a security breach. Furthermore, application deployment and updating is becoming increasingly streamlined, further decreasing

the cost of deploying updates. Many operating systems and applications, including Apple iOS, Microsoft Windows, Linux distributions, and Google Chrome^{™[3]}, provide automated update features to ease the update process and to facilitate timely deployment of updates. Instead of relying on administrators to manually deploy updates, automatic updates minimize the human factor and free up scarce enterprise IT resources.

Patch immediately. Upgrade periodically. If cyber security is truly a priority, there is no other choice.

Additional Information

- ▶ Software Development Lifecycle, Windows XP, Vista, Windows 7, Windows 8, and Bitlocker are all registered trademarks of Microsoft.
- ▶ iOS is a registered trademark of Apple.
- ▶ Chrome is a trademark of Google.

Contact Information

Industry Inquiries: 410-854-6091

USG/IC Client Advocates: 410-854-4790

DoD/Military/COCOM Client Advocates: 410-854-4200

General Inquiries: niasc@nsa.gov

Disclaimer of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

¹ Muhammad Shahzad, et al. A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles. Proceedings of the 2012 International Conference of Software Engineering, pages 771-781. June 2012.

² Monitoring and Managing Security Vulnerabilities. <http://www.microsoft.com/security/msrc/whatwedo/monitoring.aspx>

³ Browser Security: Lessons from Google Chrome. <http://queue.acm.org/detail.cmf?id=1556050>



Confidence in Cyberspace

October 2013
MIT-011FS-2013

