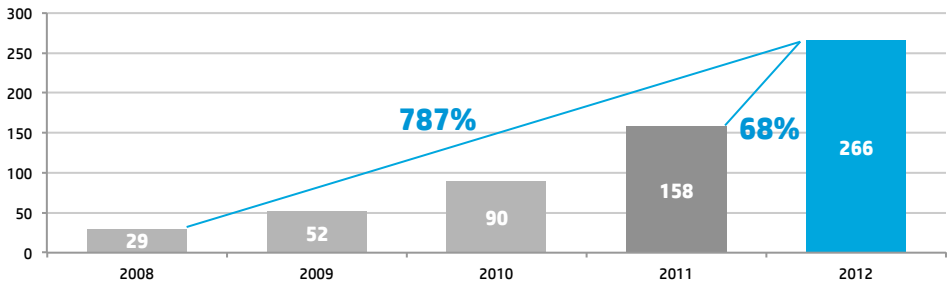
HP 2012 Cyber Risk Report Infographic

In the HP 2012 Cyber Risk Report, HP Enterprise Security provides a broad view of the vulnerability landscape, ranging from industry-wide data down to a focused look at different technologies, including web and mobile. The goal of this report is to provide the kind of actionable security that intelligence organizations need to understand the vulnerability landscape as well as best deploy their resources to minimize security risk. Here are some of the key report findings. For the full 2012 Cyber Risk Report, visit http://www.hpenterprisesecurity.com/register/hp-2012-cyber-risk-report-infographic.

Mobile

Mobile vulnerabilities rose 68 percent from 158 in 2011 to 266 in 2012

Over the last five years, mobile vulnerability disclosure rose 787 percent



Mobile vulnerabilities – by the numbers (round one)

77% were vulnerable to Information Leakage

- A lot of this information was simple, such as names, addresses, and phone numbers
- However, this data also included the current location of the user, and the specific device identifier (aka the UDID)
- Also discovered login information, user credentials, session IDs, tokens, and sensitive company data all being sent over unencrypted network protocols like HTTP

37.5% of the of the applications were susceptible to some form of authorization vulnerability

- This included clear text passwords, hardcoded passwords, and passwords included as part of the response
- Much higher percentage than in 'normal' applications

13.5% were vulnerable to Cross-Site Scripting

- Other mobile testing revealed a more consistent 33 percent were susceptible to Cross-Site Scripting
- While a lower percentage than expected, the affected applications were financial and database management applications

Mobile vulnerabilities – by the numbers (round two)

48% of the applications were susceptible to unauthorized access vulnerabilities

- These validate the authentication vulnerabilities (37.5%) that we encountered in our earlier sample set
- The numbers show that mobile developers need to concentrate on preventing unauthorized access to mobile applications as much as making them easy for legitimate users to access

33% were susceptible to Cross-Site Scripting

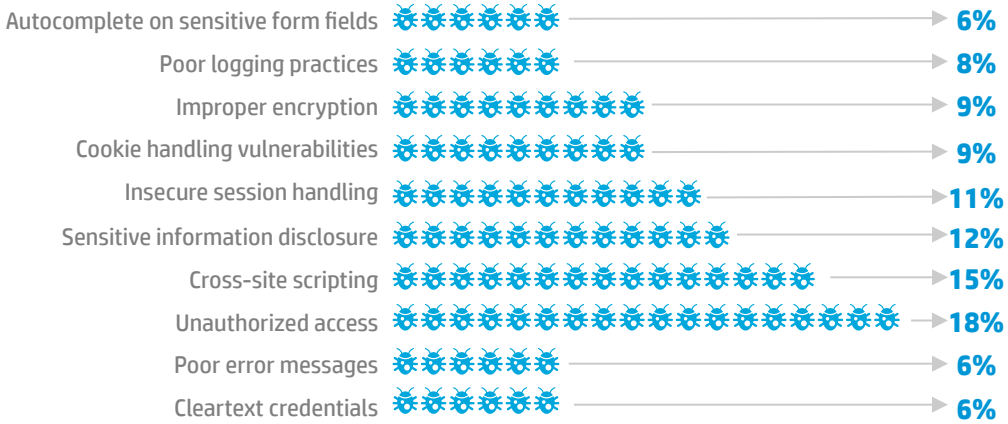
- Consistent with our testing of normal applications
- The same vulnerabilities that affect normal applications also affect their mobile counterparts

26% of the applications employed improper encryption

- The same encryption standards applied against PCs are not yet being applied to mobile devices
- In the age of BYOD, that's dangerous

Mobile applications – vulnerability prevalence

What vulnerabilities were found the most often by number?



Key findings

- The rise in usage of mobile devices has also come with a commensurate rise in application risk, especially as businesses try to capitalize on the advantages mobility provides
- When coding mobile applications, developers are not considering the security implications of how they store, transmit and access data
- The same security vulnerabilities that affect regular applications also affect mobile ones