IEEE IT Professional, Jan/Feb 2015.

IT Security

Morris Chang, *Iowa State University*
Rick Kuhn, *US National Institute of Standards and Technology*
Tim Weil, *US Department of the Interior*

Change is a factor in every area of life, but it often seems even more so in Information Technology (IT). This is particularly true in IT security. Organizations deal with daily patch management, continuous monitoring for vulnerabilities and attacks, and an endless stream of new releases of application software that must be installed. There are new challenges in established IT fields, such as the move from huge relational databases to even larger, but often less structured big data repositories. In addition, there are frequently completely new problems that emerge, such as "bring your own device" security challenges, because every employee's cell phone now has the capabilities and risks that used to be concentrated in mainframes or desktop computers. How can IT professionals adapt to these ever-changing security challenges quickly and without draining their organizations' resources?

Adapting Securely to Change

As with many problems, one of the best approaches can be to break the security problem down into component parts and separate concerns, then consider how the different components interact. Security is more than firewalls and cryptographic protocols, and a focus on these technical aspects can often lead to neglecting other issues, resulting in a breach.

We can view security from at least the following four aspects, and analyze problems accordingly:

Technical – This is the most commonly discussed concern, and indeed it can have an extraordinary impact. A recent example is the "Heartbleed" bug, an apparently simple coding error in the OpenSSL library that allowed a storage boundary to overflow, revealing sometimes sensitive information or, in some cases, complete compromise of systems. Heartbleed also illustrated the difficulty of analyzing security impacts. From one angle, Heartbleed appears to be a moderately severe buffer overrun vulnerability that can lead to compromise of random bits of memory. But with repeated runs, it was possible to obtain critical data such as authentication information, allowing attackers to log into systems. The key point here is that security can be very difficult to analyze outside of its particular application context.

Behavioral – One of the most poorly understood aspects of security is the problem of making mechanisms easy to use while retaining adequate strength for a particular application. Security principles going back nearly 40 years included the need for ease of use for security mechanisms, but the problem can be surprisingly difficult to solve, because of the needs of different application domains. A mechanism that is easy to use for employees with only minimal training may be unacceptable in a customer-facing application because customers will of course have no training in its use.

Legal – Regulations and laws have always been a part of life in industry and government, and legal complexities have multiplied along with technology. While technical aspects of security may be relatively similar across application domains, laws and regulations vary enormously, not only across industries but among jurisdictions as well. Further complicating the issue is the fact that corporations often have business in hundreds of countries. Successful methods for automating the regulatory and legal aspects of IT increase in importance as more and more of daily life happens online.

Basic principles – A common theme apparent in the three aspects of security above is the fact that often, everything depends on context and application domain. But what are the basics that IT professionals can apply in analyzing security problems? Not only computer security principles, which are well known, but broader questions of protection and conflict may be considered, with lessons that may be learned from other fields entirely outside of information technology.

In this Issue

"Insights from Nature for Cyber Security" provides thought-provoking analogies between the natural world and cybersecurity issues such as botnets, intrusion detection, distributed denial of service, and others. Considering the basic principles involved may spur creative thinking about how to improve cyber defenses.

"The Risks of Legalizing Hack Back" deals with a controversial topic: the legalities and practicalities of a "self-defense" approach to cyber security. When an organization is the target of a cyber attack, is it possible to accurately identify the attack source? If so, is it reasonable for the organization to take an offense approach to stopping the attack? These questions are being faced now by industry and governments around the world, and IT professionals should be aware of the issues involved.

"Securing the Users of Health Information" provides an overview of security issues in health care IT. The authors suggest that healthcare has lagged behind other industries in use of IT, but is changing rapidly now. The field is complex in particular because of the tradeoff between security and capacity to provide prompt and informed care, but solutions apply to many other industries as well.

Finally, "Protecting Web Components: Hiding Sensitive Information in the Shadows" deals with the ubiquitous problem of protecting web-based information and commerce using new features of the document object model (DOM). The authors also include statistics on the disturbingly high prevalence of security weaknesses in real-world web sites, which suggest that many organizations may be more vulnerable than they realize.

Articles in this issue highlight emerging trends and suggest ways to approach the four aspects of cyber security outlined above: basic principles, legal, behavioral, and technical issues. The breadth and depth of discussion in these articles should help readers recognize both problems and potential solutions.

Acknowledgment

Certain products may be identified in this document, but such identification doesn't imply recommendation by the US National Institute of Standards and Technology or other agencies of the US Government, nor does it imply that the products identified are necessarily the best available for the purpose.

Morris Chang

Rick Kuhn *is a computer scientist at the US National Institute of Standards and Technology. Contact him at kuhn@nist.gov.*

Tim Weil