Guest Editorial: Web Security

Using the web is a security risk. However, today's business world and our desire for useful and entertaining online services make it a necessity for almost everyone. The risks of using these services span from simple annoyances such as pop-ups, to financial loss, to deeply troubling invasions of our privacy. How the technical community deals with these risks has been the topic of active debate since the Internet's inception. Significant strides toward a secure and private web have been made. However, the investigation of web security is in its infancy and much work remains.

This special issue is devoted to an exploration of the breadth of issues in web security. We present six papers that contrast different avenues of inquiry in the area. The authors of these works consider, among other topics, the existence and exploitation of vulnerabilities, methods for vulnerability discovery and mitigation, and issues in web privacy. It is through these papers that we give a brief but informative view into the state of the art.

The systems which handle our critical data are fraught with peril. Vulnerabilities persist in contemporary web systems and services not only because of poor system design or implementation, but often because of bad management, ill-defined or poorly enforced security policy, or user error. While these problems arise in all environments, the Web presents unique challenges.

Security on the web is fundamentally different than traditional network security. Whereas a local network or host is often viewed as a fortress (complete with watch-towers and perimeters), the web is more like a bus station. Large communities of anonymous users frequent the public space representing the web service. Designers of web security infrastructure can make few assumptions about the behavior of the user community or environment. Hence, the web necessitates a reevaluation of established security engineering practices.

All of this begs the question: *What new problems does the web environment present?* Moreover, do traditional models and techniques of security work in this open environment? What new threats are present in the web? The papers contained in this issue originally appeared in top security, web, and networking conferences. They provide insight into the investigation and ultimately begin to answer some of these questions. They include:

- Originally appearing in the 12th USENIX Security Symposium, the paper "*Remote Timing Attacks are Practical*" by Brumley and Boneh demonstrates how seemingly inconsequential information leakage can expose critical information such as cryptographic keys. The authors show how a private key can be extracted from a web-server by correlating the query response time with the underlying cryptographic primitives. Such results were profoundly surprising to many, and have led to changes in the way public key algorithms are implemented.

- In their paper *A Multi-Modal Approach to the Detection of Web-based Attacks* that appeared in the 2003 ACM Computer and Communications Security Conference, Kruegel et al. consider methods of detecting anomalies in web interactions. They present a system that builds profiles of normal behavior based on client queries to web services. They use a range of learning and detection techniques to reduce the number of false positives that often undermine such systems.

- Huang et al. consider an alternate model of detection that analyzes the implementation a service before it is deployed. In that work, *A Testing Framework for Web Application Security Assessment* appearing in WWW 2003, the authors show how fault injection and execution monitoring can expose bugs before they reach a live service. Such tools are demonstrated on real web applications and new vulnerabilities identified.

- The paper *SSL-Spliting: Securely Serving Data from Untrusted Caches* by Lesniewski-Laas and Kaashoek which appeared in the 12th USENIX Security Symposium considers how to make secure web applica-

tions more scalable. Traditional web proxies cannot serve secure content because they have no visibility into the queries and responses. The novel barn-raising approach allows proxies to intercept and serve web queries carried over SSL from an integrity protected cache. Such services are useful in implementing authenticated content delivery in large-scale web applications.

- Denial of service (DoS) attacks typically prevent access to a web service by flooding the victim with bogus requests. In their paper appearing in 2003 ACM Computer and Communications Security Conference, *WebSOS: An Overlay-based System For Protecting Web Servers From Denial of Service Attacks*, Morein et al. describe an architecture that maintains web service availability in the presence of DOS attacks. When under attack, the system uses reverse Turing tests to validate user requests, and an overlay architecture direct the request toward servers not affected by the attack.

- We conclude with a discourse on privacy. Appearing in WWW 2003, the paper *An X-Path-based Preference Language for P3P* by Agrawal et al. considers an alternate language to APPEL, the current standard for privacy policy specification in P3P. The authors discuss the limitations of APPEL and show how the simple but elegant XPref language (based on the W3C XPath standard) can be used to address them.

These papers paint a small part of the larger picture of web security. It is the answers to the questions above that will dictate the future of the web. Hence, it is imperative that we continue to explore the requirements and design space of web security and embrace its lessons.

Patrick McDaniel, *co-guest editor*
Avi Rubin, *co-guest editor*
(January 2005)