F5 Security Vignette Series

Peter Silva, 2011-15-12

Over the last couple weeks, we've been rolling out a series of short Security Vignette videos about various IT security challenges. We've posted them to the F5News blog account but also wanted to share in case you missed them. If we were going to sum up the role of security in corporate IT today we'd have to say it's to "be prepared." This series looks at many of those security concerns which can be addressed proactively, before they are exploited or become a fire drill.

- **F5 Security Vignette: Proactive Security** - The F5 Security Vignette series looks at various security concerns, vulnerabilities and attacks which can cause headaches for Corporate IT and the business integrity overall. This video covers SSL Certificates.

- **F5 Security Vignette: DNSSEC Wrapping** - The dirty little secret of the Internet is how insecure DNS really is. The good news is, there's a solution -- DNSSEC. It secures the DNS query and response process.

- **F5 Security Vignette: Hacktivism Attack** – DDoS and other targeted attacks.

- **F5 Security Vignette: SSL Renegotiation** - The premise of the SSL Renegotiation DOS attack is simple: "An SSL/TLS handshake requires at least 10 times more processing power on the server than on the client". If a client machine and server machine were equal in RSA processing power, the client could overwhelm the server by sending ten times as many SSL handshake requests as the server could service. The counter measure against the attacks was to write an iRule to limit renegotiation requests to 5 per minute per session.

- **F5 Security Vignette: Credit Card iRule** - The consequences of exposing hundreds of thousands of customer credit card numbers is unthinkable. Fines, lawsuits, damaged brand -- the effects can be catastrophic. Even if it was accidental, the effect would be the same.

- **F5 Security Vignette: Apache HTTP RANGE Vulnerability** - When we hear about an Apache vulnerability, it gets our attention. In this case the issue was the way Apache handles HTTP RANGE headers, which are used to request individual sub-ranges of a given response, instead of the entire response. The problem is that responding to an HTTP RANGE request is computationally expensive. A simple iRule fixes this.

- F5 Security Vignette: iHealth - Security is a never ending battle. The bad guys advance, we counter, they cross over ... you're just never done. To give our side an edge we do a lot of research.

- **Security is our Job**

- **F5 YouTube Feed**

ps

Technorati Tags: F5, cyber security, predictions, 2012, Pete Silva, security, mobile, vulnerabilities, crime, social media, hacks, internet, identity theft, F5 News, security, web application security, apache, HTTP, threat mitigation, video