The Challenges of HTTP Intrusion Detection

By Ivan Ristic

Who is Ivan Ristic?

1) ModSecurity (open source web application firewall), 2) Apache Security (book), 3) SSL Labs (research and assessment platform), 4) ModSecurity Handbook (book)

Currently working on a ***security-aware HTTP parser library****, intended for use in intrusion detection systems and web application firewalls.*

The library will be used in the intrusion detection system built by the ***Open Information Security Foundation*** *(OISF).*

Why should you care? *A robust HTTP parser library is difficult to build, because there are so many opportunities for* ***evasion attacks***.

Impedance Mismatch *Ambiguous protocols and faulty implementations.*

The old truth *They need to find only one weakness in what you do; you have to protect all of them.*

Attack strategies

1) Hide payload, 2) Fool them into seeing something different, 3) Obfuscate what they do see and 4) Attack their decision points.

Evasion categories *1) SSL, 2) Breaking of TCP streams into HTTP messages, 3) Message parsing, 4) Compression and chunked transport encoding, ...*

... *5) Query string and request body parsing, 6) File uploads, 7) Use of different character encodings, 8) application-level payload obfuscation.*

Understanding a single product (e.g., web a server) is difficult enough, but the interpretation of HTTP data streams is influenced by the ***combination of operating system, web server, application engine, and who knows what else…***

All of this is not rocket science, but it does require comprehensive and methodical ***research first, coding second***.

Thank you!

The slides will be available at
http://blog.ivanristic.com