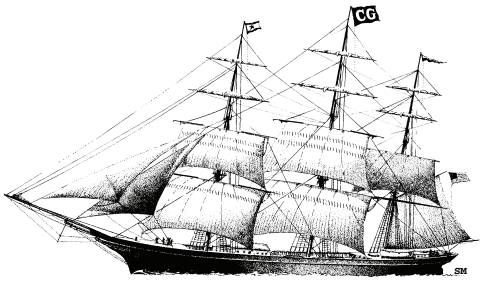
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2007081 August 16, 2007

Codenomicon *DEFENSICS* Finds Risks that Lurk in Your Protocols

Analyst: Anne MacFarland

Management Summary

Alas, the time is right. Hackers have cut their teeth and gained their reputations attacking pervasively-deployed applications and operating systems such as *Windows*, *Linux*, *MacOS*, etc. While bringing sites to a stop is a stylish way to make a statement, the real money is more likely to be made in attacking specific companies with the goal of creating operational mayhem. This can be done quite efficiently by attacking at the protocol level. Corrupted network protocols can cause anomalous packets or message sequences to confound your workflows. Corrupt data frames can be introduced at wireless hot spots. Malformed audio, video, and images can derail collaboration. Corrupt file protocol can cause data to be unreadable. Most security focuses on finding published vulnerabilities in enterprise systems or in analyzing application code. Attacks on protocols, often associated with zero-day attacks and anomalous data, can also disable a device, service, or application.

Because they are knowable in detail, standard protocols are an attractive target for hacks, but even proprietary protocols can be perverted. Improvements both in hacking approaches (pharming, spoofing, spyware, botware, malware, etc.) and in network monitoring (packet sniffing, etc.) that allow enterprises to run at peak efficiency also allow malicious forces to find ways to do harm.

Protocol exposure is part of the recognized risks that come with wireless connectivity in hotspots, but that risk is just the tip of an unpleasant iceberg. With more and more workers mobile, the risk of protocol-focused attacks across all sorts of networks – including enterprise networks – becomes significant. What are you going to do – pack everybody back in cubicles and curtail their connectivity to shouting across partitions? Of course not.

The most effective countermeasure is pre-emptive testing for protocol vulnerabilities before software is deployed. Network equipment providers, carriers, and software vendors, have recognized this and form the core customer base of a company named Codenomicon, based in Oulu, Finland. With the spread of mobile workers, integration with partners, and opportunistic collaboration, Codenomicon sees protocol subversion as increasingly large risk to business. For enterprises, Codenomicon sees their test suite as a basic best practice for enterprise-developed software. It should be as natural, inherent a pre-deployment process as looking in the mirror to insure you are zipped and buttoned, and that your clothes hang right before you go to work.

If you want to do risk management right, the prudent path should include assessment of protocol vulnerabilities as part of pre-release quality assurance. For more details, read on.

IN THIS ISSUE

Where's the Risk? Everywhere You Want to Be

Put aside, for a moment, the risks of attacks on your applications. Put aside the domain of Web applications that you already know carry other risks. Put aside the risks of unpatched servers and applications. Check out the protocols in the bundles in the box. Many will be familiar to you. Think, now, of your increasing domain of protocol vulnerability. With more workers mobile, the risk of protocol attacks becomes unavoidable. **As more and more enterprises use Web services and composite applications and mash-ups, there are more interstices that may become points of vulnerability at the protocol level.** Encryption does not stop malformed packets, created either inadvertently or maliciously, from degrading your systems. In addition, where apps are joined or reach out to others, in open systems or integrated open servers, traditional forms of segregation (like piping) may be an inadequate prophylactic. Detection is too late to prevent outages. **Testing during application development, and before deployment, is a more pre-emptive approach.**

Codenomicon *DEFENSICS*

A Nokia think tank started to worry about the network security and the vulnerability of standard protocols back in the mid '90's. In 2001, their findings led to an initiative at Oulu University in Finland, which produced a shareware testing tool called *Protos*. A few years later, the core researchers formed Codenomicon. The company has followed the shockwave of security vulnerabilities that have echoed outward as business expanded from telephone networks to the Internet, network services, VoIP and outsourcing, each of which extended the business space to be defended.

Codenomicon's *DEFENSICS*[1] security test platform is delivered in bundles of related protocol testing tools (see box, at right). Additional protocols can be added *a la carte* as needed. Codenomicon also can analyze and develop tests for custom protocols. Licensing can be by the dongle, site, area, or world-wide. It is based on concurrent seats, and starts at $50,000, DEFENSICS can be delivered as an annual subscription, a perpetual license, or as a periodic service. Most early customers have chosen the subscription model.

The primary use of DEFENSICS is as part of quality assurance process within development or deployment cycles. Codenomicon asserts random data and sequences in a systematic way against supported protocols to discover anomalous response, slower system reaction, or terminated operation – all material quality and security issues. There is no need to understand the system (other than the protocols being used) and no need to create test documentation. This saves time and resource costs. The company's value rests in how their system targets protocols, the broad protocol coverage, and the detailed test documentation, and how the use of DEFENSICS can streamline developer resolution, regression testing, and fix validation. This "blackbox" testing, whether of integrated systems or high-profile commercial devices, can reveal exposures and zero-day threats not discovered by code and vulnerability testing.

DEFENSICS addresses development and test compliance due process standards such as ISO 2001 and NIST CC-EAI. The system can also be employed by security analysts, who can use it to test staged application and service systems prior to deployment.

Codenomicon has been selling their test suite directly to enterprises in the US and Europe, and through partners in Japan. Expanding carrier and enterprise sales through strategic systems integrators is their next beachhead. To sell to enterprises, they are developing a channel strategy. They will have to bring prospects and repeatable services to enlist name brand providers as their channel.

DEFENSICS Bundles

Codenomicon has protocol-testing tools for over 135 protocols. The most popular bundles are the following.

Internet:

HTTP, SSL/TLS, SSH, IPv4, IPv6, ISAKMP/IKE, SMTP, FTP, DNS, NTP, LDAP, IPSec, IMAP, POP3.

Routing and Remote Access:

BGP, OSPF, IS-IS, IPv4, IPv6, GRE, PIM-DM/SM, RADIUS, Diameter, TACACS+, LDAP, SNMP, SSH, HTTP, SSL/TLS, IPSec, EAP, MPLS/LDP, RIP, DVMRP.

Telecommunications:

GTP, SIP, SigComp, RTP, MGCP, H.323, Audio, Video, H.328.

Multimedia:

Images, Audio, Video, Bluetooth, RTP, SIP, H.323, RTSP, RSVP, MGCP, Compression, H.248.

Storage:

CIFS, NFS, iSCSI, HTTPS, SSL/TLS, IPSec, VPN.

Source: Codenomicon

Conclusion

The security of e-business depends on all parties taking steps to avoid risks. Most organizations are using public networks to support more and more of their operations. If all software is tested for protocol risks, enterprise use of networks, including external networks, becomes more secure. Patching becomes less risky, and deployment becomes safer.

If you analyze opportunity from the hacker point of view, you realize that protocol hacks are an attractive way to attack key processes of specific companies. It is time to plan your defense. Codenomicon DEFENSICS lets you minimize business risk.

[1] DEFENSICS is the third generation of a product based on *Protus*. Protus itself is no longer supported.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Anne MacFarland **is Director of Data Strategies and Information Solutions for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group Captain's Log**, **The Clipper Group Voyager**, **Clipper Notes**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.