

Cool Vendors in Application Security and Authentication, 2008

Ray Wagner, Joseph Feiman, Neil MacDonald, Arabella Hallawell, Ant Allan, Gregg Kreizman

Chief information security officers (CISOs) and other security decision makers should be prepared to consider innovative new vendors in the application security and authentication markets. The vendors' offerings will not necessarily be appropriate for every enterprise's needs, but they point to important new directions in their market spaces.

Key Findings

- Application security testing is becoming a higher priority for technology vendors and their customers, as it becomes clear that eliminating vulnerabilities at the earliest possible state is the most cost-effective approach.
- In response to enterprise demands, authentication technologies are becoming more user-, role- and context-sensitive.

Recommendations

- Consider innovative new product and service providers — including Gartner's cool vendors — when looking for answers to application security and authentication problems.
- Do not base product or service implementation decisions entirely on technological innovation, but also on real-world workability and vendor capability.

TABLE OF CONTENTS

Analysis	3
1.0 What You Need to Know	3
2.0 Codenomicon	3
3.0 GrIDsure	4
4.0 ObjectSecurity	5
5.0 Privaris.....	7
6.0 Veracode	7

ANALYSIS

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

1.0 What You Need to Know

The cool vendors in application security and authentication that Gartner has chosen for 2008 represent the leading-edge technological innovation in these crucial areas. These five vendors may not offer solutions that are appropriate for every enterprise's needs, but CISOs and other security decision makers should keep their offerings, and the changes in the business and threat environments they represent, on their "radar screens" in the coming year. Gartner's security analysts have identified cool vendors in three other market segments, as well. For more information, see "Cool Vendors in Infrastructure Protection, 2008," "Cool Vendors in Identity and Access Management, 2008" and "Cool Vendors in Security Services, 2008."

2.0 Codenomicon

Oulu, Finland, and San Jose, California (www.codenomicon.com)

Analysis by Neil MacDonald

Why Cool: Codenomicon, founded in 2001 as an offshoot from the PROTOS project at the University of Oulu, provides dynamic application security testing (DAST) tools. Most DAST tools test only Web-enabled applications, using a limited set of Web-based protocols, typically HTTP. Enterprises risk developing a false sense of security if other, non-application-layer protocols that the application may use — for example, a Remote Procedure Call (RPC) connection to another server — are not tested.

Codenomicon addresses this problem by offering a software-based solution for the malformation ("fuzzing") of more than 120 different protocols, including Common Internet File System, Internet Small Computer System Interface, RPC, Session Initiation Protocol and Simple Network Management Protocol, as well as content formats such as JPG, WMF and MP3. Codenomicon also includes a full set of tests for wireless protocols using 802.11, Bluetooth and General Packet Radio Service connections. Custom protocol analysis for application or organization-specific protocols can be developed using Codenomicon's professional services division.

No DAST tool can be expected to exhaustively test every possible malformation. Codenomicon does, however, test each protocol systematically, in a repeatable fashion, so that when an issue is identified, it can be reproduced easily. Codenomicon's test suites use knowledge of protocol weaknesses and other common handling issues to test other related products and protocols for similar mistakes. Protocol fuzzing is also used to test for known vulnerabilities. Some competitive open-source solutions test in a random fashion, using random mutations, which makes repeatability and root-cause analysis difficult.

Challenges: The need for protocol fuzzing is well-understood in the telecommunications/networking market — Codenomicon's primary customer base — but is not so widely recognized for other embedded appliances, and particularly for typical enterprise applications. To address the enterprise market, Codenomicon must further develop its offerings to address common enterprise protocols, such as Simple Object Access Protocol; Universal Description, Discovery and Integration; Web Service Description Language; eXtensible Access

Control Markup Language; and other XML-based protocols used within enterprise applications, and must do so at a price point lower than its typical \$50,000 purchase price. Other possible ways for Codenomicon to lower barriers to adoption include offering its functionality in a formal hardware-based appliance (as its competitors BreakingPoint Systems and Mu Security do), as a service or by partnering with established enterprise DAST vendors.

Open-source protocol fuzzing tools will continue to challenge Codenomicon at the low end of the market, so Codenomicon must expand into the testing of radio frequency identification (RFID), WiMax and Universal Serial Bus (USB) protocols in future releases. For broader enterprise applicability, protocol malformation testing should expand beyond security to include response-time testing issues.

Who Should Care: The importance of protocol malformation testing extends beyond information security. Protocol and input file malformations can also cause operational and robustness problems, depending on how a given application or device is affected. Thus, protocol malformation testing should be of immediate security and operational concern to any enterprise or organization building or using embedded devices — for example, networking and telecommunications equipment, point-of-sale (POS) systems, Supervisory Control and Data Acquisition, automated teller machines (ATMs), medical equipment, manufacturing process controllers and critical infrastructure protection systems used for energy production. Enterprise financial services applications that handle critical information and use protocols other than HTTP/HTML should also be candidates for DAST testing for protocol and file format malformation.

Related Research

"Integrate Security Best Practices and Tools Into Software Development Life Cycle"

"Static Application Security Testing: Vendors and Products, Part 1"

"Static Application Security Testing: Vendors and Products, Part 2"

"Static Application Security Testing: Vendors and Products, Part 3"

"MarketScope for Web Application Security Vulnerability Scanners, 2006"

3.0 GrIDsure

Huntingdon, U.K. (www.gridsure.com)

Analysis by Ant Allan

Why Cool: GrIDsure's technology is one of many new authentication methods based entirely on "something known," an approach that avoids the use of tokens of any kind — a significant consideration in many online consumer security use cases, but still less vulnerable to attack than simple passwords. However, GrIDsure's offering stands out because of its conceptual simplicity and versatility. GrIDsure's "something known" is a distinctive ordered pattern or path on a small array of tagged squares — such as a move in chess — which GrIDsure calls a Personal Identification Pattern (PIP). The tagging of the squares changes with each use, so that simply by reading off the tags associated with his or her PIP, the user builds up a one-time password (OTP). The tags on the array are typically numbers, but they can be replaced by any keyboard characters or by graphical symbols if a custom hardware or virtual keypad is used. The tags are repeated across the array — each one appears two or three times — which means that knowing the OTP does not mean knowing the PIP. The method is, therefore, resistant to "shoulder surfing" and "sniffing" attacks, because reconstructing the PIP would require multiple observations.

Beyond this, the GrIDsure approach shares the common strengths and limitations of all OTP-based authentication methods.

The technology's use is not limited to interactive log-in for PCs, networks and Web sites; it can also be deployed in many other situations (for example, for building access, and in ATMs and POS terminals) as a replacement for any password or personal identification number for building access, ATMs and POS terminals. GrIDsure software can be implemented as a personalized OTP software token for mobile phones, which enables GrIDsure to provide transaction verification, with the array derived from input transaction details and the OTP providing an electronic signature confirming those details. GrIDsure's ease of use by people of varying ages and abilities has been established by a study at University College, London.

Challenges: GrIDsure is a small company that has worked hard to draw attention to its pattern-based OTP authentication method. The company has received endorsements from MasterCard, the U.K. Cabinet Office and Visa, but has relatively few technology partners and — because of the breadth of its vision — risks spreading itself too thin. GrIDsure must focus on key markets and build new relationships with partners that offer versatile authentication servers or in-the-cloud authentication services. (The only one of its current partners that does this is ActivIdentity.) To date, GrIDsure has focused on licensing its technology to equipment manufacturers, IT solution providers and system integrators, and a "productized" solution for — at minimum — Microsoft Windows PCs and network log-in is overdue.

Who Should Care: GrIDsure's technology should interest CISOs, as well as other corporate officers and senior executives responsible for logical and physical security, protection against financial fraud and related duties, particularly if they are looking to provide more-robust user authentication (and transaction verification) at a lower cost and with greater ease of use than traditional strong authentication options. Authentication infrastructure vendors seeking to broaden their portfolio of authentication methods should also evaluate GrIDsure's approach.

Recommended Research

"A Taxonomy of Authentication Methods"

"The Twilight of the Passwords: A Timetable for Migrating to Stronger Authentication"

4.0 ObjectSecurity

Cambridge, U.K. (www.objectsecurity.com)

Analysis by Neil MacDonald

Why Cool: ObjectSecurity, founded in 2000, is one of the few commercial vendors offering a model-driven security solution. Model-driven security tackles one of the more difficult problems in information security: capturing design-time intent and translating it into real-time security policy enforcement at runtime. Model-driven security tools can free developers from having to write security code and hard-code security policy into applications. This can speed development, ensure more-consistent application of security policy, enable easier changes to business applications and processes, and give business units and security organizations — rather than developers — the ability to define appropriate policy.

ObjectSecurity's technology was initially developed for use with the Common Object Request Broker Architecture (CORBA) and has been expanded to include service-oriented architectures (SOAs). ObjectSecurity's primary offering is OpenPMF, a model-driven security solution that enables centralized security policy management with automatic enforcement across distributed applications. Object-Security is not a Unified Modeling Language (UML) or business process modeling tool vendor, but rather uses its OpenPMF/SecureMDA bundle to generate security

policies from existing application models (for example, UML). What makes this cool is that SecureMDA consumes the UML models generated in model-driven application development and then uses these models to automatically generate most of the necessary security policies (for example, which applications should be permitted to interact with other applications) directly from them. This can dramatically reduce overall security policy specification and maintenance efforts. Additional policies can be developed using ObjectSecurity's Eclipse-integrated graphical user interface. OpenPMF is also available in a trusted SOA bundle that specifically targets SOA environments.

Object-Security's road map promises even cooler developments to come. The company is working on integration with Intalio, a popular open-source business process management suite (BPMS) vendor for BPMS-driven model integration. This would enable business process models to be used to define security policy, with OpenPMF generating the necessary security policies and enforcing them transparently on the SOA application server layer. OpenPMF supports enforcement on a variety of technology platforms, including SOA application servers (Glassfish, BEA WebLogic), CORBA (Secure MICO, JacORB), CCM CORBA Components (Qedo SecureMiddleware), messaging middleware (XMLBlaster) and Data Distribution Services (RTI DDS) middleware. It also integrates with an organization's established security infrastructure (for example, X.509 PKI, LDAP and firewalling).

Challenges: ObjectSecurity is a small company with limited marketing, few employees, limited channel capabilities and a somewhat confusing set of offerings. It has not sought venture capital funding and is constrained in its ability to sell and support its offerings outside the U.K. and its environments (although it plans to move into the U.S. market by 2Q09). ObjectSecurity also faces technical and competitive challenges. No standards exist for model-driven security, and ObjectSecurity uses its own policy definition language (PDL). The company is involved in defining standards with the OMG consortium. The OpenPMF offering overlaps with authorization management solutions from BEA Systems, BiTKOO and Cisco (Securent). Gartner expects the larger application development platform vendors to enter the model-driven security space — notably IBM and Microsoft, but also Oracle and SAP — as they develop BPMS capabilities that link with their identity and access management infrastructures.

Adoption of model-driven security will be slow overall, because this approach is, and should be, part of a broader enterprise move toward models and model-driven development. Furthermore, any successful model-driven security solution must incorporate legacy applications and application platforms into its architecture. The shift to model-driven security also requires that information security professionals' skills evolve, so that they can provide enterprise patterns for security policy, and leave the more mundane day-to-day security administration work to business people. In the longer term, enterprises will develop libraries of security patterns and models that embody security policy and can be consumed during model-driven development for consistency and reuse.

Who Should Care: ObjectSecurity's offerings should interest information security architects, enterprise architects and application architects with enterprises or organizations that are investigating visual application development tools for application composition or business process orchestration. Security architects should also investigate these technologies, because they need to begin planning for standardized enterprise security patterns for consistency, demonstrable compliance and reuse in development and for delivering security as a service for the enforcement of security policies at execution.

Recommended Reading

"Model-Driven Security: Enabling a Real-Time, Adaptive Security Infrastructure"

"Tear Down Application Authorization Silos With Authorization Management Solutions"

5.0 Privaris

Charlottesville, Virginia (www.privaris.com)

Analysis by Gregg Kreizman

Why Cool: Privaris manufactures the plusID, a combined logical and physical access token that is activated by fingerprint biometric authentication. The plusID supports multiple radio frequency standards for access to major physical access control systems, and either encrypted wireless Bluetooth or USB-connected access to workstations and networks. The device behaves like a standard smart card when authenticating to Windows, and is also RSA SecureID-ready, so OTP authentication can be added to the device for additional logical authentication.

What makes Privaris' plusID cool is not any one of the embedded technologies — multiple vendors can provide each of its capabilities — but rather the way it combines these capabilities into one device. The biometric enrollment and subsequent authentication capabilities are implemented on the device only, so there are none of the issues with a centrally held fingerprint template repository. The plusID can also replace physical access control system (PACS) access badges, adding biometric authentication to multiple PACS without the need to upgrade readers. This is a comparatively simple process, achieved by not allowing the radio frequency access code to be sent from the plusID without the user first being authenticated to the plusID.

Challenges: The plusID suffers from the same weakness as other physical authentication products, such as smart cards and OTP tokens: A small handheld device can easily be lost. If this happens, then the end user will require some type of "work-around" to gain access to protected assets. Like other small, venture-capital-funded vendors, Privaris is in its early days of building a customer base and does not yet have reference customers.

Who Should Care: Privaris' "sweet spot" in the market is enterprises with end users who require access to multiple PACS and stronger logical authentication than passwords alone. CISOs and physical security officers may find implementing this approach easier than one that requires integration between logical and physical access control back-end systems.

Recommended Reading

"A Taxonomy of Authentication Methods"

"A Taxonomy of Authentication Methods: Quick-Reference Outline"

6.0 Veracode

Burlington, Massachusetts (www.veracode.com)

Analysis by Joseph Feiman and Arabella Hallawell

Why Cool: Veracode, a static application security testing (SAST) vendor, differentiates itself from other market players in several ways: It searches for security vulnerabilities by analyzing binaries, not source code, which means it can cover an application's entire code base, including binary third-party libraries. Veracode addresses the needs of an important area, especially in software architectures where calls are made to programs — such as packaged applications, services subscribed to over the Internet and dynamic link libraries — whose source code is unavailable for security testing, but for which binaries are available. This approach also means analyzing the code in its compiled state, so that any externally included library- or platform-specific problems can be identified as well. (This approach is useful even when source code is available.) Once vulnerabilities in enterprises' own code have been detected, enterprises can fix them. Enterprises cannot fix detected vulnerabilities in packages, programs, components and Web services

acquired from third parties, but they can pressure their vendors, service providers and supply chain partners to remediate any problems that are found.

Another factor differentiating Veracode is that it does not sell its technology as a product, but rather provides software security testing services through an automated software-as-a-service (SaaS) business model. This approach should appeal to enterprises that lack the application security skills or resources to conduct application security testing on their own. Veracode's services include a security rating of software that Veracode tests for its clients — ranking vulnerabilities' severity and ease of exploitability — which provides its enterprise clients with a baseline "safety check" of the applications they build or buy.

To broaden application life cycle coverage, Veracode has integrated a DAST service (using technology from NTOjectives) into its code assurance platform in addition to its original SAST service.

Challenges: Veracode's appeal is limited to enterprises that want to use a managed service. It excludes enterprises that prefer to purchase a tool to conduct testing themselves. A critical element of Veracode strategic execution will be earning the trust of clients that will be uploading their code to the Veracode platform, especially by handling their sensitive vulnerability information appropriately. Veracode needs to prove that it can scale to host a multiplicity of clients, each of which has a multiplicity of applications. Veracode should streamline the process of fixing detected vulnerabilities by integrating its testing output into requirements management, quality control, and software change and configuration management tools. This would extend Veracode's appeal beyond information security organizations to development groups as well as quality assurance and testing groups within IT operations organizations.

Who Should Care: Veracode should be on the radar screens of CSOs, CIOs, directors of applications and other IT decision makers concerned with detecting and fixing security vulnerabilities before an application, package or service component is purchased and deployed. Vendors and service providers seeking to reassure customers through an independent analysis and verification of the security of their software offerings should also evaluate this technology.

Recommended Reading

"Market Definition and Vendor Selection Criteria for Source Code Security Testing Tools"

"Application Security Testing: Strengths, Weaknesses, Opportunities and Threats"

This research is part of a set of related research pieces. See "Cool Vendors 2008: Innovation From Around the World" for an overview.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509