



beSTORM Frequently Asked Questions

What is beSTORM?

beSTORM is a security assessment tool that performs an exhaustive analysis to uncover new and unknown vulnerabilities in network-enabled software applications during the development cycle. By automatically testing billions of attack combinations, beSTORM ensures the security of products before they are deployed saving companies millions in costs associated with fixing security holes after products are shipped. beSTORM is different than older generation tools that use attack signatures or attempts to locate known vulnerabilities in products.

Why is beSTORM an important tool for software vendors?

Security is now a primary concern among end-users and software vendors are struggling to make their software more secure before it ships. As corporate professionals are driven by compliancy regulations for financial records and overall data security, there is a growing requirement for many companies to ensure that third party software applications meet stringent security certifications. Software applications that are not fully tested prior to deployment make companies more vulnerable and leave customers feeling insecure.

With beSTORM, software developers can test their software for security holes during the development process, the way Quality Assurance (QA) is done today. Since this is done automatically, developers can test and re-test new versions as they are coming out, no matter how short their development cycle is.

How does vulnerability assessment help alleviate security problems in software?

Checking for vulnerabilities can help spot the security flaws before the software is shipped. This means that flaws that are discovered today by hackers will be identified and fixed by developers – before the product is released to the market. This will result in increasingly secure software and lower the number of security flaws that can be used by attackers.

Why are tools that monitor software vulnerabilities growing in importance? Aren't the majority of problems focused on operating systems?

The operating system (OS) is, in fact, software. There are many different software components in the OS that are susceptible to flaws and Microsoft's dominance in the IT world has made them a convenient target for security attacks. As security fixes have progressed, it has become increasingly difficult to find new flaws in the OS components and relatively easy to find software vulnerabilities in other applications. As hackers have done their own cost effective calculations, they have begun to target non-OS software components. Therefore, today we are seeing a large increase in vulnerabilities found in other software applications.



How does beSTORM work?

beSTORM is an automated tool, programmed to make an exhaustive search of all possible input combinations of a network protocol in order to test the protocol implementation for weaknesses. However, attempting to cover all theoretical input combinations to the program is not a trivial task and requires the ability to test for billions of combinations automatically. beSTORM is equipped with prioritization algorithms to enable complete coverage of all inputs that are likely to 'trigger' a security hole, and within a reasonable time frame.

To do this, beSTORM converts the protocol specification into an automated set of tests and exercises the network protocol with a specific emphasis on technically legal but functionally erroneous and stressful cases. As an example, beSTORM automatically tries every protocol combination possible until a buffer overflow is triggered. Another example - What if the application is expecting a file name and you send it characters that are not valid? What if you do illogical things with protocol sequence numbers? beSTORM is not limited to specific cases – it will eventually cover the entire protocol search space.

Who will use beSTORM?

beSTORM is designed to be used in a software engineering environment and should be exercised by developers, quality assurance teams and security professionals. beSTORM arms these individuals with a tool that helps them to test for security holes while they are still in the development phase. The new product enables development teams to schedule security testing into the product release process giving them time to fix their code before product is shipped.

Is beSTORM easy to use?

beSTORM is no more complicated than typical QA tools, and is in fact much easier to use than most. Due to the fact that the testing is automated, the average beSTORM user can start using beSTORM within minutes. The security testing expert will enjoy the many optional parameters that are available in order to tweak and fine-tune the testing to cover certain parts of the protocol or to increase the testing speed.

How does beSTORM test for security holes during the development cycle without the need for source code?

beSTORM tests the binary application, and is therefore completely indifferent to the programming language or system libraries used. This allows a separate testing team that may not have access to the source code, to use beSTORM for security testing of the application.

beSTORM will report the exact interaction that triggers the vulnerability, and this report can be sent to the programmers that can now debug the application in whatever development environment they wish to see what causes the fault.



How is beSTORM different than Automated Scanning?

Automated Scanning, like other Vulnerability Assessment (VA) tools, searches for known vulnerabilities in known products. While it will sometimes find unknown vulnerabilities, this is usually due to similarities to known vulnerability signatures.

beSTORM exhaustively tests the protocol implementation and will find all known, as well as unknown, vulnerabilities that relate to buffer overflow, format string and off-by-one vulnerabilities (currently over 95% of the known security flaws belong to one of those vulnerability types).

Also, Automated Scanning is used by the end-user for scanning their network machines. beSTORM is used by the software vendor itself, to scan the product during development.

What other alternatives are available to software vendors?

Security auditing today is usually done manually by expert security researchers. Despite the fact that security auditing has been done on Internet products for many years, few automated tools have been created for this purpose. Today, these products are usually in-house tools created by security researchers to assist them during their audits. Products like these usually require a high expertise level in usage, and convey very little machine "intelligence." Most of those tools have no automated functionality beyond assistance to the manual analysis nor do they do a full and comprehensive analysis of the protocol.

Other alternatives include source code audit software. These solutions search the source code for what appears to be bad code that could indicate a potential security hole. And, there are other security testing tools that rely on a relatively small number of case studies (thousands or tens of thousands) that are known to trigger buffer overflows in certain protocol implementations.

How is beSTORM different from other security products available today?

The main difference between source code testing tools and beSTORM is that beSTORM does not require the source code. beSTORM tests the protocol rather than the product and can therefore be used to test extremely complicated products with a large code base whereas source code testing tools usually do not scale for large code bases

Another key differentiator from source code analysis is the accuracy of the reporting: beSTORM checks the application externally by actually triggering the attacks and vulnerabilities are reported only if an actual attack has been successful. Source code analysis tools, on the other hand, suffer from a large number of false positives.

In comparing beSTORM to tools that run a certain number of case studies or scenarios - beSTORM performs millions and sometimes billions of attack combinations as compared to thousands or tens of thousands of case studies. Here is the difference between fighting yesterday's war (checking for known problems) and fighting tomorrow's war (checking for still-unknown vulnerabilities).



What do I need to use beSTORM? Do I access it via the Internet or do I license and install the software on my own servers?

beSTORM is a software you install on your servers. One component of beSTORM (the monitoring component) is installed on the server where your product is installed, and the other component – the one that initiates the testing – can be installed on that same server or on a separate machine on the network to increase throughput and allow more realistic testing scenarios.