

Featured this month:

Virtual worlds, real exploits

As the popularity of virtual reality worlds grows, their potential security vulnerabilities are coming under increasing scrutiny.

One such world is Linden Lab's Second Life, which offers significant scripting capabilities to its users, encouraging them to build their own in-world objects. Security researcher Charles

Miller from Independent Security Evaluators discusses the security risks inherent in virtual worlds and explores what such exploits might look like. He describes details of a proof of concept attack written for Second Life, and discusses potential malicious payloads that could be delivered in such an attack.

Go to page 4...

The challenge of federated identity management

Despite the slow uptake of federated identity management, it is still a means for companies to share numerous services, products and data.

However, like any form of comparable web application, many companies are still in the dark when it comes to managing and protecting federated identities. Don Smith, technical director at security services company DNS,

describes why companies take on federated identity management, and also explores the potential security challenges that they must overcome. To deploy the technology effectively, companies need an overall understanding of how the systems are used and how single sign-on technologies are evolving.

Go to page 7...

SEO poisoning epidemic explodes

CNet's network of business sites was hit by an outbreak of search engine optimisation (SEO) poisoning attacks in March.

The attack used the sites' habit of caching the results of searches conducted on their own internal search engines in order to improve their ranking in popular search engines. The attackers entered an IFRAME script along with popular key words to create a search result that, when displayed by search engines and clicked, directed visitors to a site hosting malware.

The sites themselves were not compromised, although failing to validate inputs and remove embedded HTML commands made it possible for the attackers to create

their bogus queries. When users' browsers visited the infected sites, they were infected with either Zlob malware or a piece of rogue malware (now listed as badware by Stopbadware.org).

Throughout the month, the attacks (originally identified by security researcher Dancho Danchev) intensified. His blog suggested that over a million bogus search queries had been created in this way. Other sites hit by the attack according to Danchev included those hosted by Wired.com, Unicef, USA Today, Walmart, Forbes and ABC News. To mitigate the attack, search engines began filtering the search results to prevent users seeing the iFrame links.

Contents

NEWS

| | |
|---------------------------------|---|
| SEO poisoning epidemic explodes | 1 |
| EU launches Primelife project | 2 |
| Attackers target epilepsy site | 2 |
| Adware tops charts in Q1 | 2 |

FEATURES

Virtual worlds, real exploits

| | |
|---|---|
| Charles Miller considers the security of virtual worlds, and discusses a proof of concept exploit which could have been used to steal money from other virtual residents. | 4 |
|---|---|

The challenge of federated identity management

| | |
|---|---|
| Implementing FIM strategies pose a number of security problems. dns look at core FIM development and best practice for FIM systems. | 7 |
|---|---|

The PTK: An alternative advanced interface for Sleuth Kit

| | |
|---|----|
| Dario Forte discusses the PTK, a project allowing forensic examiners to perform their operations faster and easier. | 10 |
|---|----|

Modern web attacks

| | |
|---|----|
| Over the past two years malware has made increased use of the web. Fraser Howard, principal virus researcher at Sophos, explores the methods of attack which have put businesses' IT infrastructures and corporate reputations gravely at risk. | 13 |
|---|----|

Managing multinational compliance efforts while addressing security needs

| | |
|---|----|
| This article discusses how security practitioners can deploy technology to address compliance issues. | 16 |
|---|----|

Scalable malware analysis

| | |
|--|----|
| There are many different ways to analyse your logs, traffic, and security events in an effort to find malicious software. Bruce Potter discusses some of them. | 18 |
|--|----|

REGULARS

| | |
|---------------|----|
| News in brief | 3 |
| Events | 20 |

Photocopying

The PTK: An alternative advanced interface for Sleuth Kit

Dario V Forte, CISM, CFE, founder and CEO Dflabs (www.dflabs.com)

We are living in a period where the number of systems that we must investigate is growing, but budgets are not expanding to match the complexity of the field. The examiners working in the public sector are assisting with budget reduction, while in the private sector, e-discovery is drawing resources away from the field of pure computer forensics. Finally, the number of small forensic laboratories is also growing.

More open source tools are needed. The IRItaly group at University of Milano at Crema, started to work at the PTK project.¹ PTK is an advanced graphical user interface (GUI) for the command line tools in the Sleuth Kit, which is an open source tool for analysing file systems.² This makes it usable and easy to investigate a system.

“Together, PTK and the Sleuth Kit will allow the examiners to investigate the file system and volumes of client-side computers and servers”

Although the PTK was conceived as a graphical interface for the Sleuth Kit's CLI, the development team quickly realised that the project had more potential and decided to integrate the two systems more tightly. Together, PTK and the Sleuth Kit will allow the examiners to investigate the file system and volumes of client-side computers and servers. They can be used to analyse Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).

A better interaction

The Sleuth Kit and PTK are both open source products running on UNIX platforms. As shown in figure

1, there is an interaction between the advanced interface and the Sleuth Kit's core. The Sleuth Kit (in green, labelled 'TSK') is responsible for acquiring, extracting and managing the first layer of data contained in the disk images. Thus, PTK adds three more level of data management, including an indexing engine and a database, which is one of the most important new features of the project.

PTK versus Autopsy

During the development of the PTK, it was necessary to conduct a gap analysis between the current analysis model based upon the Autopsy Forensic Browser and the PTK. The Autopsy Browser is an existing GUI designed to work in conjunction with the Sleuth Kit. In particular, the IRItaly Team examined the usability and the performance of the Autopsy Forensic browser, with particular reference to:

- Interface usability
- Time required to perform a single operation
- Scope of features

After a structured analysis phase, the development team found several limits and/or areas of potential improvement.



Dario Forte

The current interface was felt to be outdated and not particularly user-friendly. For example, the case management section is complex, and could be simplified. The file activity timeline lacked some functions, and was also difficult to consult compared with current examiner needs.

The team also found that there was not an effective bookmark facility.

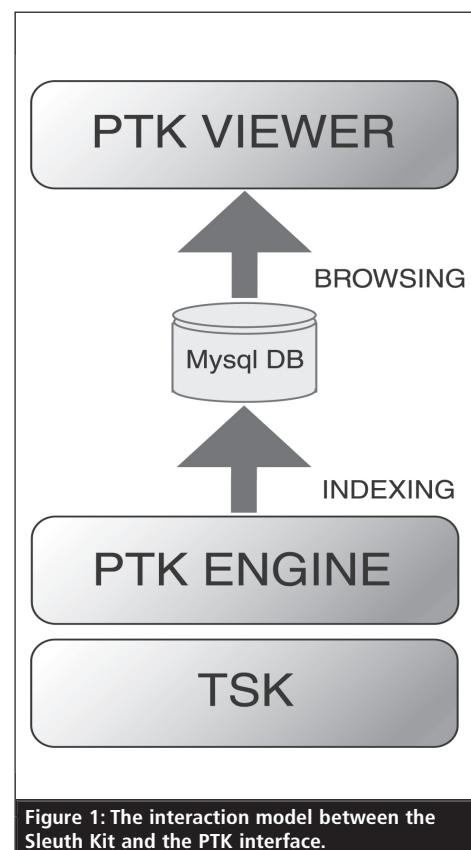


Figure 1: The interaction model between the Sleuth Kit and the PTK interface.

| Option | Sub-options |
|--|---|
| String extraction (Ascii-Unicode) | Allocated strings Unallocated strings Slack (NTFS and FAT) |
| Identification of the known good and the known bad (whitelist/blacklist) | |
| Options based on file content type | File signature analysis File extension mismatch File categorisation (graphics, documents, executables etc...) |
| Metadata and hash generation of the files present on the disc | Timeline generation File carving (Lazarus, Foremost, Scalpel) |

Table 1: Administrator options in PTK.

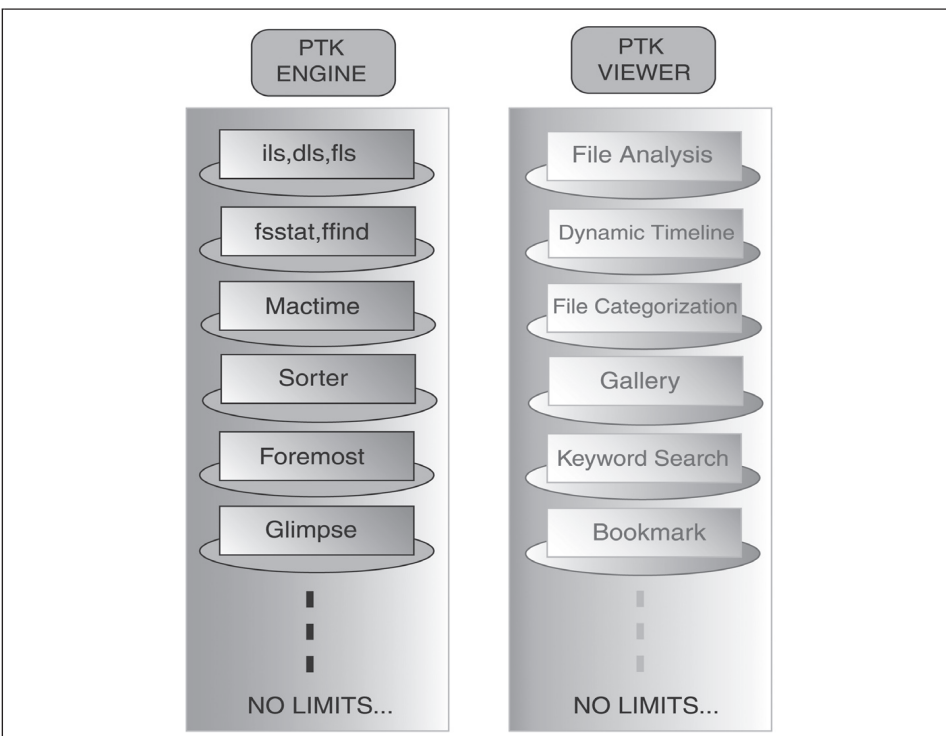


Figure 2: A list of preliminary indexing functions and related GUI features in PTK.

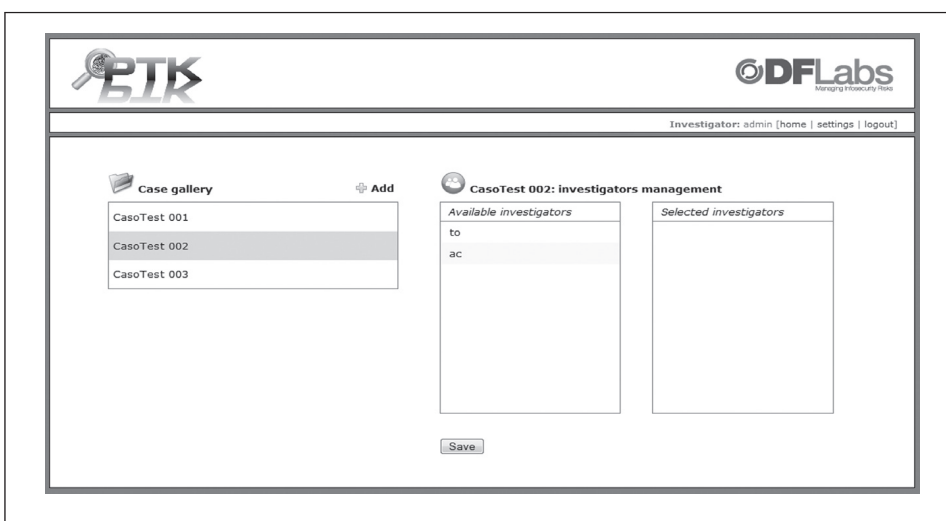


Figure 3: Administrative screen for various cases in the PTK tool.

Notes are the only way to include information and comments into a case, and the note management system was not felt to be effectively structured.

There is no dedicated function for report generation and/or exporting. Unless an external plug in is used, there is no gallery feature in the tool’s analysis zone, to visualise and manage the graphical evidences. A survey conducted by the team revealed that this could be a strong need/requirement of the forensic examiners, specially during a child pornography case.

Case export and sharing was also found to be inadequate for modern requirements. Investigators may need to work on the same case while using different machines And yet exporting a case to a second forensic workstation is a difficult task using Autopsy and does not guarantee effective case sharing. The main consequence is a lack of synchronisation between the several duplicated copies. Similarly, performing a backup of a case and/or copying or duplicating it to reduce the workload was an issue under the existing GUI.

The PTK team worked on some features in order to guarantee a preliminary indexing feature, and was able to scale the amount of data managed by the investigators, thus speeding the examination. PTK performs a preliminary indexing of images that investigator has to analyse.

The results of the preliminary operations are stored in the database for a better and faster analysis. The remaining operations (i.e: file and directory export) can be executed on user demand, directly on the disk image.

| Feature | Details |
|----------------------------------|--|
| Data storage | PTK uses a MySQL database User passwords are encrypted Data access is faster and easier The sensitive information is not in the file system anymore Concurrent examination (more investigators on the same database) |
| Log activity | All the operations can be logged, thanks to a logging sub-system: Timestamp IP client Username Action performed The administrator can also view the log via his interface |
| Asynchronous Java and MXL (Ajax) | More dynamic More usable The number of page loads are reduced Better application performances |

Table 2: PTK main features.

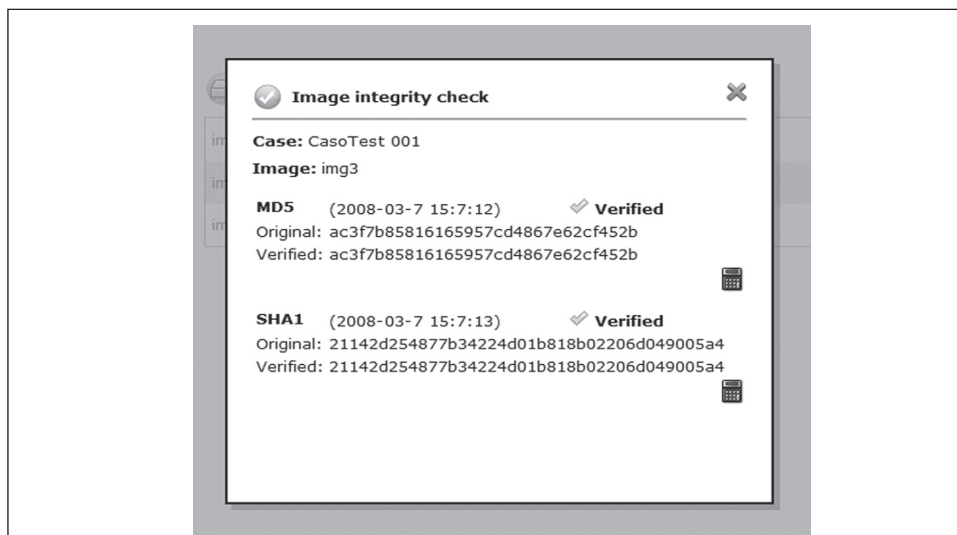


Figure 4: An image integrity check in PTK.

Concurrent work

The main aim of PTK is to provide a system that allow investigators to work on the same shared cases. This will reduce the workload and also expedite the results. To reach this goal, PTK uses a central database for the case management, so that more investigators can work on the same case simultaneously from different machines.

After the preliminary operations made by the indexing engine, the PTK DBMS takes charge of concurrency management. The number of simultaneous examiners able to work at the same time is dependent on several factors, such as

hardware, available bandwidth, and the number of disk images included in the case.

One of the main goals of the project, for which an extensive support from the community is required, is to evaluate performance and stability. However, the team at IRItaly DFlabs has expanded its operations beyond that, creating a security mechanism with reference to selected operations. The security mechanism can provide simultaneous access to the same case, or sequential access (enabling administrators to lock access).

The administrator may also add new cases and select the investigator who will be able to get access to them. This means

better security, role-based access control, and, most of all, tracking of every single operation.

Enhanced analysis

Another point of interest is the analysis phase. PTK introduces several new features that can help support analysis, including:

- File analysis
- Keyword search
- File type
- Image details
- Metadata
- Data unit
- Gallery
- Bookmark
- Tree view with directory and file listing
- Tabbed browsing to visualise file content

Most of these features naturally rely upon the underlying capabilities to be found in Sleuth Kit, but the development model used by the team is modular, meaning that new tools can be added.

For example, a new image hashing control has been included, so that PTK can guarantee the integrity of images that investigators are working on. When a new image is added to the case, the investigator can choose among two hash algorithms: MD5 and SHA1. PTK stores these values in the database for a later comparison. The investigator can open the 'Integrity check' panel at any time. Here, he can view the original image's hash value and the date-time of the last calculation. The investigator can then launch an integrity check. PTK will compute a new hash value and compare it with the one stored into the database. If anything is wrong, the user is immediately warned.

“For example, a new image hashing control has been included, so that PTK can guarantee the integrity of images that investigators are working on”

MD5 and SHA1 calculations are two separated processes: this allows the investigator to choose what algorithm

should be used to guarantee image integrity, according to available time and resources.

Conclusions

The PTK was launched at the DoD Cybercrime conference in St Louis, Jan 2008.³ Since that event, a series of webcasts have been held. The project Beta Test Program is still open to qualified users and will be a prelude to the official release, which will happen in September 2008. The project is very ambitious and has the goal of helping teams of investigators with reduced budget and a strong workload, for free. As we write, the beta tester list counts about 50 different

experts. Many of them are from international Government Agencies, Banks, Universities and so on. With PTK, one of the main limits of Sleuthkit's previous interfaces are resolved. The investigators will now be able to save time and money, at least for basic and intermediate investigations.

References

1. PTK Web page, DFK Labs. <<http://ptk.dflabs.com>>
2. The Sleuth Kit web site. <www.sleuthkit.org>
3. DOD Cybercrime Conference web page. Technology Forums. <www.technologyforums.com/8CC/index.asp>

About the author

Dario Forte, CFE, CISM, former police detective and founder of DFLabs, has worked in information security since 1992. He has been involved in numerous international conferences on information warfare, including the RSA Conference, Digital Forensic Research Workshops, the Computer Security Institute, the US Department of Defense Cybercrime Conference, and the US Department of Homeland Security (New York Electronic Crimes Task Force). He was also the keynote speaker at the Black Hat conference in Las Vegas. He provides security consulting, incident response and forensics services to the Italian Government, law enforcement agencies and private companies. www.dflabs.com

Modern web attacks

Fraser Howard, principal virus researcher, Sophos

There are many factors that can dictate the success of a piece of malware. These include how and to whom it is delivered, how it is executed, how rapidly it propagates and how successfully it evades detection. The first two of these describe the process of threat delivery and execution, which are perhaps the most influential factors in the success of a threat. Traditionally cybercriminals have used email as their preferred vector of attack, employing various social engineering tactics in order to entice the recipient into executing the malicious attachment. As companies have become more aggressive in blocking email content, criminals have shifted their attentions, and are now firmly focused on the web.

Not having to rely upon the user for code execution has always been an attractive goal for malware authors. Vulnerabilities in web browsers, and the various plug-ins they support, provide opportunities for the attacker. By constructing web attacks that exploit client-side vulnerabilities, they are able to achieve code execution with relative ease. This results in what have become known as 'drive-by download' attacks, where simply browsing a malicious page results in the user becoming infected.

"Not having to rely upon the user for code execution has always been an attractive goal for malware authors"

At the start of 2008, Sophos was discovering 6 000 new infected web pages a

day, or one every 14 seconds. Worryingly, over 80% of these pages were hosted on legitimate sites which had been illegally compromised by hackers.¹

The role of the web in current malware

Over the past two years, malware has made increased use of the web. The scope of the threat extends further than just malicious scripts embedded in web pages. Numerous downloader trojans use the web as a simple file repository, downloading other malicious files via HTTP. Malicious scripts hosted on sites often await visits by vulnerable client browsers before unleashing exploit code to infect the victim. With compromised sites providing a convenient mechanism to expose huge numbers of victims to malware, this

technique is being increasingly used for financial gain and to capture confidential information. Spammed emails and enticing websites lure the maximum number of victims towards the malicious code.

Web-based attacks may also deliver some form of traffic redirection payload, which can be used by malware authors to generate revenue through online advertising and affiliate marketing schemes.

The web provides the perfect framework for malware authors to blend the above techniques. Today's threats cunningly incorporate spam and web lures with exploit scripts to infect unsuspecting victims.

It is no surprise that today's web attacks are financially driven. The main threat comes from organised criminal gangs looking to infect users with malware to steal passwords, financial details and other sensitive information.



Fraser Howard