ATINER CONFERENCE PAPER SERIES No: COM2013-0428

Athens Institute for Education and Research
ATINER

ATINER's Conference Paper Series
COM2013-0428

The Use of Honeytokens in Database Security

Penny Ross
Senior Lecturer
University of Portsmouth
UK

Amanda Peart
Senior Lecturer
University of Portsmouth
UK

ATINER CONFERENCE PAPER SERIES No: COM2013-0428

Athens Institute for Education and Research
8 Valaoritou Street, Kolonaki, 10671 Athens, Greece
Tel: + 30 210 3634210 Fax: + 30 210 3634209
Email: info@atiner.gr URL: www.atiner.gr
URL Conference Papers Series: www.atiner.gr/papers.htm

ISSN **2241-2891**
18/07/2013

An Introduction to ATINER's Conference Paper Series

ATINER started to publish this conference papers series in 2012. It includes only the papers submitted for publication after they were presented at one of the conferences organized by our Institute every year. The papers published in the series have not been refereed and are published as they were submitted by the author. The series serves two purposes. First, we want to disseminate the information as fast as possible. Second, by doing so, the authors can receive comments useful to revise their papers before they are considered for publication in one of ATINER's books, following our standard procedures of a blind review.

Dr. Gregory T. Papanikos
President
Athens Institute for Education and Research

This paper should be cited as follows:

Ross P. and Peart, A. (2013) "**The Use of Honeytokens in Database Security**" Athens: ATINER'S Conference Paper Series, No: **COM2013-0428**.

The Use of Honeytokens in Database Security

Penny Ross
Senior Lecturer
University of Portsmouth
UK

Amanda Peart
Senior Lecturer
University of Portsmouth
UK

Abstract

Information security is a growing concern for organizations. Data and Information stored in companies' databases are often considered as one of their most valuable assets; and as a result, ensuring their security is of significant importance. Changes to the IT landscape including remote access for employees, virtualisation, cloud provisioning, mobile devices and the growing interest in Bring Your Own Device (BYOD) are bringing new challenges. Despite huge investments in database security the global statistics for data security indicate that breaches have been on the increase. Also of concern is the fact that when these leaks occur, it can take system administrators weeks and in many cases months before they are aware that a security breach has happened. In this time the damage inflicted by its perpetrators may have reached sizable proportions. Mechanisms such as authentication, privilege management, views, firewalls, intrusion detection tools auditing and logging have become standard database security tools. However, as Maheswari, Sankaranarayanan, (2007) state as the methods of attack increase in number and sophistication, interest in more aggressive forms of defence to supplement existing methods needs to be developed. This paper discusses the use of Honeytokens in database security specifically in addressing the insider threat. A Honeytoken is a digital or information system resource whose value lies in the unauthorized use of that resource. The key to a Honeytoken is that it is enticing, something a hacker views as valuable. It is then integrated into the system and no one should interact with it. Any interaction with a Honeytoken most likely represents unauthorized or malicious activity.

Keywords:
Corresponding Author:

Database Security

Database security is designed to prevent external and internal threats to the system. Three key components of security being confidentiality, availability and integrity. Mechanisms such as authentication, privilege management, views, firewalls, intrusion detection tools, auditing and logging have become standard database security strategies. These strategies are effective against external threats but have limitations on insider abuse. Maheswari, Sankaranarayanan, (2007) cite that as the methods of attack increase in number and sophistication, interest in more aggressive forms of defence to supplement existing methods needs to be developed.

Kolodgy (2009) categorises two sources of threat to data, namely external and internal threats. External threats are widely recognised and security solutions are developed with this type of threat in mind. External threats originate from sources outside the organization; Verizon (2009) provide a number of examples of these external threats that include hackers using tools like Port scanners, Vulnerability scanners, Rootkits, and Sniffers, organized crime groups, concerted attacks by "black hats" with the backing of organized crime or national governments, physical theft of hardware or software containing sensitive company information, careless disposal of used computer equipment or data storage media.

The greatest potential threat to databases comes from internal threats, insiders with legitimate access to the system. Although internal data breach threats are fewer in number, they have more damaging effects on the companies affected. The internal threat is harder to trace. These users have already bypassed the firewall, authorisation and have been given privileges to access areas of the database. Research conducted by Orthus discussed in Computerworld UK (2007) suggests that most insiders are trusted to a certain degree and some IT administrators in particular, have high levels of access and privilege. Until the insider threat is addressed no real security can be achieved. A database system consists of different users using applications that read or update the database. Each user is authorised to use a certain set of applications and access to a particular set of data. The privilege management method is a key existing security mechanism limiting users and applications to particular functions and data, based on task analysis. In general a graphical interface will be used for the database interaction to allow the user to accomplish their set tasks. The interface masks a set of SQL statements that perform the required transaction. These transactions are task depended, embedded in the application and remain transparent to the user. The allocated privileges are linked to these tasks inhibiting users from accessing other data.

However, many users have access to sensitive data through these applications and as many users are customer facing they require some level of access to the sensitive data. Although limiting the tables and attributes is relatively simple it does not prevent users accessing records that are of no concern to them.

To gain competitive advantage organisations are adopting the paradigm of access to data anytime, anywhere for employees and also customers. This

brings changes to the IT landscape including remote access for employees, virtualisation, cloud provisioning, mobile devices and the growing interest in Bring Your Own Device (BYOD). Each of these strategies increases security risk, particularly from insider attack. Within an organisation trust of the employees is a key security concern. Employers often require references and also use vetting procedures before allowing staff to access the company's resources. But with the rise in offshoring and outsourcing this is becoming problematical. Security is cited as one of the main concerns for CIOs when considering both offshoring and use of cloud services. Many of these service providers offer the assurances of firewalls, antivirus software, secure data centres - but what about their employees? Additionally, companies are having to allow greater access to their enterprise systems with users such as auditors, contractors, sub-contractors and supply chain partners many of whom exist outside of the organisation's direct control.

Identifying key sensitive data and protecting it is a common security strategy, however the task of having to sort through the large volume of files in larger organisations where data is so dispersed, disorganized, and voluminous to determine which data is to be considered as sensitive is too burdensome and resource-intensive a task for most IT departments in organisations to undertake [6][7][8]. A simple corporate database may have hundreds of thousands of records and this can be compounded by the hundreds of users who have legitimate access to this data and identifying a leak may be extremely difficult.

According to the United States Department of Justice (2012) with enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes: for example, false applications for loans and credit cards, fraudulent withdrawals from bank accounts or obtaining other goods or privileges which the criminal might be denied if he were to use his real name. If the criminal takes steps to ensure that bills for the falsely obtained credit cards, or bank statements showing the unauthorized withdrawals, are sent to an address other than the victim's, the victim may not become aware of what is happing until the criminal has already inflicted substantial damage on the victim's assets, credit, and reputation.

Despite huge investments in database security the global statistics for data security from the Privacy Rights Clearing House (2008) indicate that the frequency of data breaches around the globe is continuing to increase with a reported 218 million records containing sensitive information including credit card numbers, social security numbers, bank account numbers and driving licence numbers were stolen in the period January 2005 to July 2008.

Also of concern is the fact that when these leaks occur, it can take system administrators weeks and in many cases months before they are aware that a security breach has happened. A study conducted by Verizon Business (2009) revealed that 63% of enterprises don't learn about data breaches until months after their data has already been compromised and by this time the damages inflicted by its perpetrators would have reached sizable proportions. The study also revealed that 70% of all data breaches are discovered by third parties, such as customers or banks, meaning that most companies have no idea that their

data has been compromised. Any privacy failure, or even the mere perceived failure to protect customer data, can result in loss of consumer trust, affect customer retention, cause significant damage to brand and company reputation, or lead to civil penalties such as prosecution under the UK Data Protection Act and the European Data Protection Directive 95/46/EC.

Data Leakage Prevention

One key strategy to ensuring an organisation's data is being kept safe is the use of Data Leakage Prevention (DLP) solutions. Defined by Giannoulsi (2008) Data Leak Detection (DLD) is the process of identifying behaviour indicating a breach is in process and information is leaking or has leaked from a network DLPs are similar to firewalls but differ only in terms of the data traffic they monitor; where firewalls monitor inbound traffic to the networks to ensure that there are no malicious entries, DLP solutions monitor outbound traffic to see if any sensitive information is leaving the organization in an unauthorized manner. Although the operational logic behind these DLP solutions are good, the task of having to program the DLD software through all the organisational data and identify only sensitive data is a huge task that not many organisations can justify.

Honeytokens

Spitzner (2003) states that Honey Traps have been used for a time in network protection by making an area of the network seem attractive to hackers inferring that sensitive data and key operational systems exist in a particular area. In fact, this is a trap for the hacker.

A Honeytoken is based on the same idea. Spitzner's definition --is a digital entity or information system resource whose value lies in the unauthorized use of that resource. It can be a credit card number, Excel spreadsheet, PowerPoint presentation, a database entry, or even a bogus login. These Honeytokens do not correspond to real entities but appear realistic and any interaction with them represents unauthorised or malicious activity thereby indicating to system administrators that there has been a breach of sensitive database records either from external or internal sources [14]

The operational logic of the Honeytoken is to create realistic but fake records and include them with the real business application data. Since these Honeytokens are fake, there should be no authorized activity with them. Detection mechanisms such as Intrusion Detection System (IDS) signatures and DLD are then created to look for and detect these tokens being accessed or used. If the tokens are used, it most likely represents unauthorized or malicious activity and an alert message is sent to system administrators [15]. Intrusion Detection Logs and System Logs can be used in conjunction with the Honeytoken to provide valuable information as to who is perpetrating the crime.

Data collected from the logs can help the system administrator in identifying new methods and trends of attacks. Without this information when breaches have been identified often it can be difficult to determine how it occurred [16].

The idea of Honeytokens is not new and has been used significantly in other areas to identify data leaks. For example some map-making companies insert bogus cities or roads into their maps to determine if competitors are selling copied versions of their own maps.

The development of Honeytokens cannot be generic. Data structures as well as data types used for organisations vary and honey tokens need to be developed to mimic exactly the genuine data already used by an organisation. Attention must be paid to ensuring the data looks genuine is essential otherwise when accessed it will immediately alert the thief to its nature. Credit card numbers should contain the same bank codes, sort codes and card number length as the genuine card information. Honeytokens also need to be continually added to the system to ensure that they reflect current data and again appear genuine and so accessed in an attack.

The Honeytokens need to be sufficient in nature to probabilistically be accessed during attack along with genuine data. In a system containing hundreds of thousands of records this is not an insignificant amount. Organisations will also have to develop policies to ensure that honey tokens are not included in operations to calculate profit and loss or in tax returns.

Programming the intrusion detection system or data leak software to recognise signatures attached to the honey token data means that the parameters required to detect a leak can be reduced. Care should also be taken to ensure that you do not rely on the Honeytoken as the only flag that something is wrong.

Conclusion

The challenge now is not only to protect data from the threat of theft but also to detect and respond accordingly when it occurs. Organisations that discover leaks only after they have occurred face loss of customer trust and may result in customers leaving the company. Whilst there are various approaches for DLD and IDS, the use of Honeytokens is being adopted in many security infrastructures mainly because they are cost effective, simple to deploy, and highly effective especially in detecting internal data leak threats. Honeytokens are still a new field for data leak detection concepts, and while there is expected to be much more development in this area, institutions that hold sensitive data should seriously consider implementing these tokens to serve as an early intrusion detection mechanism.

For Honeytokens to be of use to organisations they need to generate enough data to be found by an intruder in a dataset of hundreds of thousands of records, there needs to be a probabilistic chance the data will be found. The data must also appear genuine, records need to genuinely reflect the real data they are stored with otherwise it would become obvious to the thief that the records are there as a trap. In ever more complex data environments Honeytokens deployed with IDS and DLD can help to protect an organisation's most valuable asset, the data.

Maheswari, V., & Sankaranarayanan, P. (2007). *Honeypots: Deployment and Data Forensic Analysis*. Retrieved March 13, 2010, from ieee Explore website: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04426464&tag=1

Kolodgy, C. e. (2008). *Oracle DatabaseSecurity: Preventing Enterprise data Leaks at the Source*. Retrieved March 5, 2010, from Oracle inc. Website: http://www.oracle.com/corporate/analyst/reports/infrastructure/sec/209752.pdf

Kolodgy, C. (2009). *Preventing data leaks*. Retrieved March 5, 2010, from Oracle inc website: http://www.oracle.com/corporate/analyst/reports/infrastructure/sec/209765.pdf

VERIZON security report (2009) http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Computerworld UK, Security News, (2007) retrieved April 12, 2013 from http://www.computerworlduk.com/technology/security-products/authentication/news/index.cfm?newsid=6510

http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1301484_mem1,00.html

http://infotech.indiatimes.com/photo.cms?msid=3946142

Giannoulis, P., (2008) retrieved April 12, 2013 from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1301484_mem1,00.html

The United States Department of Justice, Identity Theft and Identity Fraud Report, (2012) retrieved April 14, 2013 from http://www.justice.gov/criminal/fraud/websites/idtheft.html

'A Chronolgy of Data Breaches', Privacy Rights Clearing House, Feb 2008, http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total

Verizon data breach investigations report. (n.d.). Retrieved August 12, 2010, from Network World: http://www.networkworld.com/newsletters/sec/2008/063008sec2.html

Data Protection Act 1998, Information Commissioner's Office, http://ico.org.uk/for_organisations/data_protection

European Data Protection Directive 95/46/EC, Eur-Lex, Access to European Law, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT

Spitzner, L. (2003). *Honeytokens: The other Honeypots*. Retrieved March 3, 2010, from Symantec Connect Web site: http://www.symantec.com/connect/articles/honeytokens-other-honeypot

Olzak, T. (n.d.). *Preventing Data Breaches*. Retrieved March 2010, 2010, from http://it.toolbox.com/blogs/adventuresinsecurity/preventing-data-breaches-isnt-just-about-stopping-stuff-coming-in-25325

Choudhury, T., (2012) 'Honeypots; The Trap is Set', Infosecurity Europe, April 2012.