PenTest magazine

Vol.2 No.10 ISSN: 2084-1116
Issue 10/2012(18) October

80+ PAGES

Biometrics

INTERVIEW WITH MICHAEL LARGUE – CEO OF BIOTECNIX LIMITED

THE PROBLEM WITH BIOMETRICS FOR ESTABLISHING IDENTITY

BIOMETRICS AS A SECOND FACTOR OF AUTHENTICATION

BIOMETRICS: SOMETHING MORE THAN SECURITY

HOW BIOMETRICS ENHANCE OUR ENTERPRISE SECURITY

MALWARE: ‘PASS THE GAUSS’

NISPOM: SUBCONTRACTING AND INFORMATION SYSTEM SECURITY titania

nipper® STUDIO

KEY FEATURES

Configuration Auditing with no Network Traffic

Advanced, Detailed Reporting

CVSSv2 Rating Systems

Customizable Settings

Easy to Action Mitigation Reports

Multi-Platform Support

Secure Offline Activation

Over 100 Plugins

Technical Support and Updates

PLUS much more...

CYBER SECURITY AUDITING SOFTWARE

Nipper Studio is your cyber security expert in a box. Our industry leading security auditing tool allows you to produce detailed and thorough security audits of your network devices in seconds, at a fraction of the cost of manual testing.

Companies worldwide depend on their computer systems to successfully run their businesses. These systems will often contain classified information, therefore it is imperative that they are secure. However due to time and cost restrictions manual penetration tests may happen only once or twice a year. Nipper Studio not only dramatically reduces the time taken for penetration testing but also helps you to feel secure in the intervals between manual audits. With Nipper Studio you can audit the same set of devices as many times as you like during your subscription period, so you can feel secure and stay secure.

With years of experience in the network auditing industry we understand it is important that a security audit highlights all potential threats and doesn't just review firewall rules. As a result Nipper Studio's advanced and detailed reporting is used and trusted by global organisations in the financial, telecommunications, defence, government and security sectors and has users in 40 countries worldwide.

NEW FEATURES!

Raw Configuration Change Tracking: Nipper Studio reports now include the raw configuration changes from your network device. Nipper Studio highlights the different options within your configuration that have been added or removed since the previous audit.

PLUS!..

Audit Change Tracking: Now you can include a change comparison within your security audit. The report then highlights the vulnerabilities fixed, the issues still remaining and any new vulnerability that has occurred since your last audit. This allows you to have a clear view of how your system's security has progressed.

Save Time

Security audits are time consuming for both the systems owner and the auditors. A detailed examination of an average sized configuration can take half a day and 2 to 3 weeks to complete the report. Nipper Studio can perform the audit and produce the final report in just a few seconds.

Save Money

Audit companies typically charge per man day for auditing and reporting. For a 25 device network an audit and report could take up to 3 weeks. An experienced security auditor would typically cost £1,000 per day, so an audit of a small network could cost up to £20,000. A Nipper Studio license for 25 devices costs only £600!

Nipper Studio Supported Devices

Cisco · Check Point Software Technologies Ltd. · hp · Juniper Networks · IBM · Cyberguard · crossbeam · Blue Coat · 3com · extreme networks · Brocade · Netgear Connect with Innovation · Fortinet · f5 · Foundry Networks · Technology Associates, Inc. · Huawei · Dell · Nokia Connecting People · Nortel · McAfee Proven Security · secure computing · Microsoft · SonicWALL · WatchGuard · Barracuda Networks

PLUS more...

Multi-Platform Support for... Windows Linux Mac

Titania Limited • County House • St Mary's Street • Worcester WR1 1HB • UK

Telephone: +44 (0)845 652 0621 • Email: enquiries@titania.com • www.titania.com

Titania Limited is a company registered in England and Wales. Registered Number: 6870498. VAT Registration Number: 984 3990 61

PenTest magazine

Managing Editor: Krzysztof Sikora
krzysztof.sikora@software.com.pl

Associate Editor: Trajce Dimkov
dimkovtrajce@gmail.com

2nd Associate Editor: Aby Rao
abyrao@gmail.com

Betatesters: Harish Chaudhary, David Kosorok, Robert Kriz, Stefanus Natahusada, Emiliano Piscitelli, Aby Rao, Marcelo Zúñiga Torres, Gareth Waters, Steven Wierckx

Proofreaders: George Bormes, Dyana Pearson, Eric Shultz, Jeff Weaver, Ed Werzyn

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl
DTP: Ireneusz Pogroszewski

Production Director: Andrzej Kuca
andrzej.kuca@software.com.pl

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.pentestmag.com

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear PenTesters!

In this issue you will learn about Biometrics and whether it is a well-understood technology and a panacea to verifying and authenticating identity.

In the Biometrics section we start with a rough introduction. Bogdan Nacuta clears up some of the misconceptions behind fingerprint, iris, face, vascular pattern recognition and others. In the next article, José Alberto Canedo will show you how Microsoft and Google use Biometrics as a security element and what are the obstacles to its adoption. The article by Marcos Faundez-Zanuy proves that apart from security, biometrics has its applications in health and ambient intelligence. Shubhra Deo makes you aware that the word "Biometrics" is not all about biology and describes a new set of biometrics on which research is still going. What is more, Enric Sesa Nogueras will make you familiar with handwriting being a biometric modality and its analysis that attracts a growing attention from the scientific community in security-related fields. In his two articles, Colin Renouf makes us aware of some problems, which might occure while adopting different biometrics systems and how a criminal can access and steal the use of a trusted identity. Juliet Lodge explains why using the term 'biometric' in an inconsistent way may contribute to combating serious crime, enhance security and boost certainty in a person's claim to be genuinely who they claim to be. Have you ever missesd your flight due to a faulty face recognition system? The section ends with the article about the flaws of face recognition adopted in an airport.

In the Mobile Security section, the author explains terms like BYOD (Bring Your Own Device) and consumeration, which define how enterprises use mobile devices to increase productivity.

Review section is about networks and systems' safety. William Whitney presents to you a new book entitled Penetration Testing: Protecting Networks and Systems. Check why it is worth having.

Our guest in this issue is Michael Largue from Biotecnix Limited. Over the 22 years he has worked for some of the world's leading IT organisations and have today gained certifications in (MCSE) Systems Engineer, (MCSA) Systems Administrator (MCSD) Solutions Developer, (RHCE) Red Hat Certified Engineer, (CCNP) Cisco Certified Network Professional, Certified Ethical Hacker (CEH). Currently he is the CEO of Biotecnix Limited.

This month, we arranged for you a new section on Malware. Adam Kujawa will introduce you to a new form of "Super-Malware" known as 'Gauss', which is essentially banker malware with a state-sponsored twist.

We continue with Marc Gartenberg's section on NISPOM. We focus on chapters 7 through 9, which introduce us to the requirements for subcontracting, information security and special requirements.

In this issue, we prepared for you the next chapter from John B. Ottman's book "Save the Database, Save the World!" This time you can read about the Database SRC in the Cloud.

I hope that you will find this issue worthwhile. Should you have any questions or suggestions concerning topics you want to read about, feel free to contact us at en@pentestmag.com.

Thank you all for your great support and invaluable help.

Enjoy reading!
Krzysztof Sikora
& PenTest Team

Biometrics

The Struggles of a Misunderstood Technology

This article has a dual purpose: to provide insight into the world of biometrics, by explaining how some of the systems actually work behind the scenes; and by doing so, to clear up some of the miss-conceptions that many people have regarding this technology. You will find information on the most popular biometrics, including fingerprint, iris, face, vascular pattern recognition and others.

Biometrics: measurable physiological and behavioural traits that can be used for automated recognition. To be considered as such, the traits have to meet 7 characteristics: universality, distinctiveness, permanence, collectability, performance, acceptability, circumvention. One by one, universality: all of individuals should possess the trait; distinctiveness: the trait should be sufficiently different to distinguish between any two individuals; permanence: the trait should remain largely unchanged throughout the individuals life; collectability: it should be relatively easy for the trait to be presented and measured quantitatively; performance: high level of accuracy and speed of recognition of the system given the operational and environmental factors involved; acceptability: individuals should be willing to accept the use of that trait for the purpose of biometric recognition; circumvention: refers to the degree of difficulty required to defeat or bypass the system.

There are a number of biometrics that satisfy the above conditions, however some do perform better than others. Thus, the most commonly used biometrics today are: fingerprint, face, iris, signature, voice, hand geometry and vascular patterns. Other less popular modalities, that have found application in the real world include: DNA, gait analysis (simply put, the way an individual walks), ear geometry, typing dynamics, retinal scans, thermograms, brain waves, skin spectroscopy, cardiac and others.

It is important to make distinction between identification and authentication. To be used for identification needs, a 1:N biometric system – with N in the size of millions, has to fulfil some extra, rather common-sense, characteristics: extreme accuracy, small-sized templates and very low comparison times. Today, only two biometrics are capable of delivering such performance: fingerprint and iris. Face, voice, signature and hand geometry may also

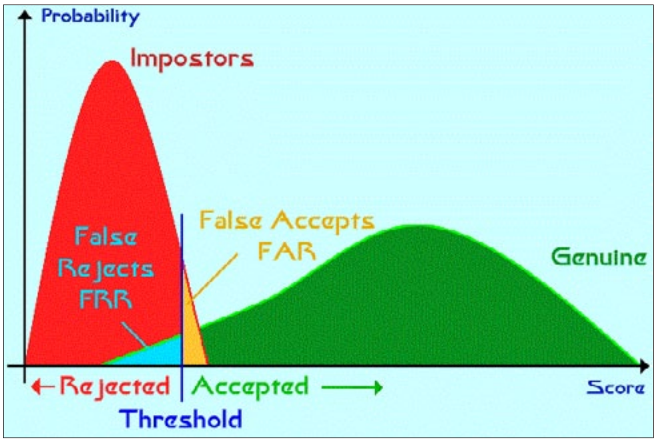


Figure 1. *Generic distribution of False Acceptance Rate and False Rejection Rate*

Biometrics Institute 8th Technology Showcase and Exhibition

BIOMETRICS INSTITUTE

TUESDAY 27 NOVEMBER 2012, HOTEL REALM, CANBERRA

Biometrics

as a Second Factor of Authentication

With the main platforms welcoming and integrating biometrics into their authentication systems, this article discuss when and how biometrics can be a security element and what are the major obstacles to its adoption. We show how Microsoft and Google are playing the biometric card.

Historically, human beings have being establishing each other's identities through biometrics. Using complex mental abilities that we don't fully comprehend to this day, we are able to recognize familiar faces, voices, hand writings and even gaits. Obviously, we do that by recognizing features unique to each individual or what makes a person *that* person (Figure 1).

As powerful as the human recognition can be, it presents severe limitations in the modern world where we have to deal with machines or people who don't know us at all such as the officials at the airport. Even when we are interacting with people who we know, we might need to verify their identities through a machine. For instance, like when we're in a chat room.

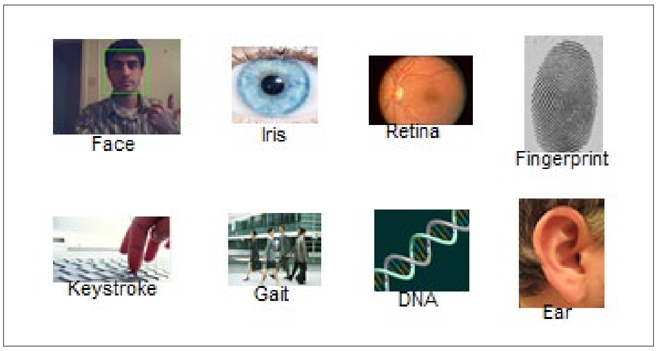
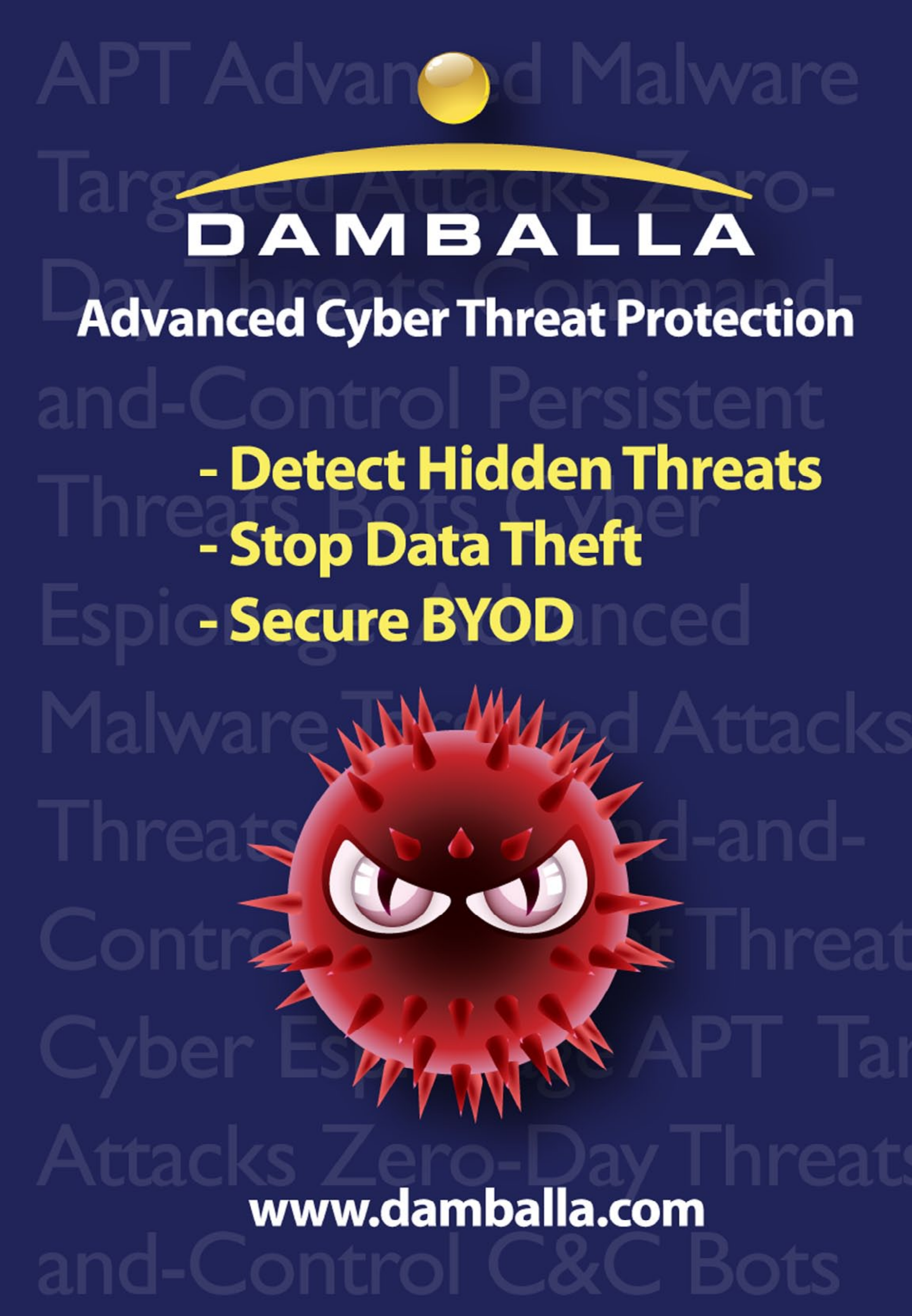


Figure 1. *Types of Biometrics*

In security, identity is the claim a user makes when attempting to access a system. Automated systems are not as smart as human beings and, naturally, the biological recognition is substituted for simpler forms of identity representations such as user names, ID cards, certificates (public keys) and ATM cards. Numbers and strings of characters are easy to process, store and compare making the creation of these "surrogate" identities more or less simple:

- Breeding documents like birth certificate or driver's licence are verified by human operators and a new surrogate identity is generated, like a passport or an e-mail.
- Inside the system, this surrogate identity in uniquely tied to the original identity, so that the original identity does not need to be verified again.

Figure 2. *Authentication Factors*


DAMBALLA
Advanced Cyber Threat Protection
- Detect Hidden Threats
- Stop Data Theft
- Secure BYOD
www.damballa.com
APT Advanced Malware
Targeted Attacks Zero-
Day Threats Command-
and-Control Persistent
Threats Bots Cyber
Espionage Advanced
Malware Targeted Attacks
Threats Command-and-
Control Persistent Threat
Cyber Espionage APT Tar
Attacks Zero-Day Threats
and-Control C&C Bots

Biometrics

Something More Than Security

In this article you will find that biometrics is something beyond security because it has applications and implications in health and ambient intelligence. You should know that sometimes these applications are not independent. Some relationship exists between them and once a biometric signal is provided, several kinds of information can be extracted.

The term "biometrics" originates from the Greek words Bio (life) and Metron (measure) and is defined as the science and technology of measuring and statistically analyzing biological data.

Although many people consider biometrics only relevant to security applications; in reality, the relevance of biometrics is very far reaching. This field has applications relevant to animals, plants and human beings. Some examples are:

- Statistical methods for the analysis of data from agricultural field experiments to compare the yields of different varieties of seeds
- Analysis of data from human clinical trials evaluating the relative effectiveness of disease therapies
- The analysis of biometric characteristics for animal/human verification or identification

The main components of a hypothetical biometric application system are shown in Figure 1. The first

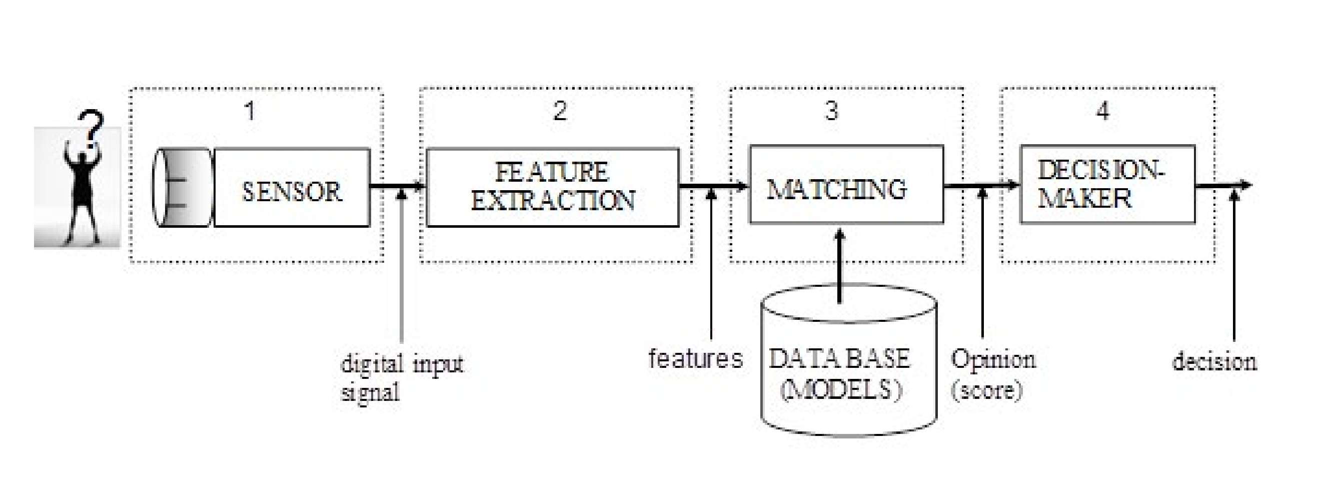


Figure 1. *Main blocks of a hypothetical biometric application system*

How Biometrics

Enhance Our Enterprise Security

The word "Biometric" make us feel that it is all about biology, right…? Wrong! It's more about pattern matching. When you read the title biometrics and the first thought which came to your mind was fingerprint and retina scans, then you must continue reading to expand your view on the wide range of biometrics that are in use today and another set of biometrics on which research is still going.

Biometrics has entered into our daily lives and we all must be aware of it. If not, there are lots of movies in which we can see the use of biometrics such as a retina scan or hand geometry as a high security measure to protect critical areas from unauthorized people. Biometrics is one of the oldest forms of identification. We all have been recognizing each other by faces, voice, signature etc. over the course of time. The difference is that now we have automated tools to do the same. Biometrics is considered to be one of the most developing and secure forms of technology when compared with traditional security. In this article, we will come to know that as rapidly as biometrics is expanding, the techniques to break the biometrics are also emerging with a similar speed. An attempt has been made to provide an overview and detailed knowledge of not only the concept of biometrics but also the various facets of biometrics which are affected. This article will try to answer various questions in your mind such as:

- Why biometrics when traditional password security which can be deployed anywhere?
- How biometrics works?
- What biometrics technology is best for me?
- What are the benefits of biometrics over our comfortable passwords and access cards?
- How biometrics differs from traditional security in terms of efficiency?
- Is biometrics hack proof?
- Does biometrics affects the privacy of an individual?

Introduction

Biometrics is a widely accepted methodology for identification and verification using unique physical or behavioral assets. There has been a lot of study and research on the biological assets that are unique to each person which can be used in biometrics. The commonly used traits are fingerprint scanning by examining ridges, bifurcation, or dots of finger; voice recognition by analyzing speech that is produced by vibrating the vocal cords; iris recognition analyzes the pits, striations, filaments, rings, dark spots, and freckles of eyes; and face recognition analyzes facial parameters. Biometric technology is one area that no segment of the IT industry can afford to ignore. Security is a top notch concern for the modern day business process. Ranging from banking to medical industries privacy of information has been a vital topic and has gained a lot of attention with standards like HIPAA and PCI DSS which focuses on the protection of the sensitive information at various degrees.

Biometrics had been considered a favorable option as it is readily available and cost effective.

RSA® CONFERENCE EUROPE 2012

9-11 OCTOBER | HILTON LONDON METROPOLE | U.K.

PRACTICAL SOLUTIONS TO HEADLINE THREATS.

Three days of information security insight.

Only RSA® Conference Europe 2012 delivers the steps and strategies needed to protect your organisation's assets. From managing smartphones and tablets, to the workplace risks from social media tools, get the techniques you want and the answers you need.

Hear from highly regarded keynotes including Wikipedia founder Jimmy Wales, internationally renowned security technologist Bruce Schneier, and investigative journalist, author and broadcaster Misha Glenny – one of the world's leading experts on cybercrime and global mafia networks.

- Leave with actionable solutions
- Build your skills
- Network with like-minded professionals
- Stay informed, stay ahead

Get the practical insight your organisation needs. Attend and play your part in Europe's most informative information security event.

Date: 9 - 11 October
Venue: Hilton London Metropole Hotel, U.K.

Hear how the world's security experts manage challenges like:

- **Mobile security**
- **Data breaches**
- **Hacktivism**
- **Cybercrime**
- **Malware threats**
- **Cloud computing**

THE GREAT CIPHER
MIGHTIER THAN THE SWORD

Find out more at
www.rsaconference.com/pen

Biometric Security

by Means of Online Handwritten Text

You will learn about online handwritten text, a biometric modality that benefits from modern acquisition devices capable of recording the invisible parts of the handwriting. You will also learn that these invisible parts (the in-air trajectories) have a considerable recognition potential, which makes them suitable to discriminate among writers.

In today's society, with security being a matter of growing concern, biometrics has conquered an important role in applications where the fast and reliable identification of individuals is deemed as an issue of paramount importance. Handwriting being a biometric modality (Fingerprint, hand-geometry, iris, retina or gait are other examples of biometric modalities), its analysis has attracted a growing attention from the scientific community, especially in security-related fields.

The term *handwriting* refers to the complex movements performed by the hand while writing a text and to the results of this process, that is, a piece of text written by hand. As a process, handwriting is a complex perceptual-motor task, a skill usually learnt at school. The hand is a very complex structure that contains 27 bones (including the wrist), more than 40 different muscles and that is innervated by 3 nerves each of which performs sensory and motor functions. Different types of factors exert influence on the production of handwriting: the muscular movements involved in the process are controlled by the central nervous

Figure 1. *Modern digitizing tablet and pen by WACOM® (image from [6])*

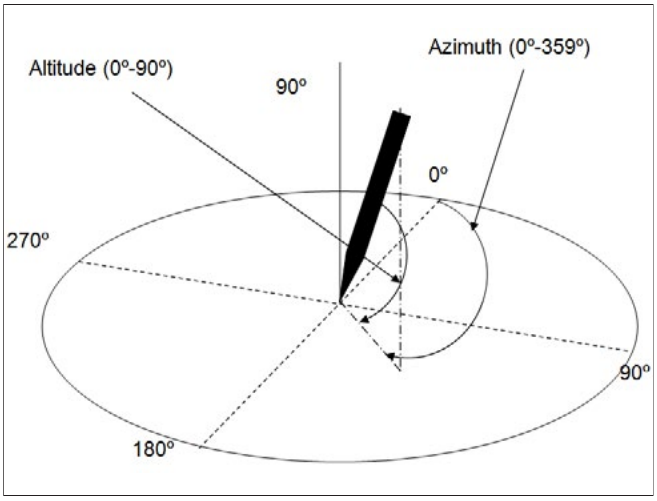


Figure 2. *Azimuth and altitude angles of the writing device with respect to the plane of the writing surface*

The Problem

with Biometrics for Establishing Identity

In this article we will look at how the non-IT parts of biometric identity cards are used to access a biometric identity, but why the lack of proper standards in this physical area inhibits the use of a true and complete biometric identification process. Security professionals working with biometric identities should understand the issues, which are outside the realms of IT, and should push for proper standards.

In the IT profession, we have a tendency to look upon technology as the solution to all of the world's ills and often ignore the big issues on the boundary between a technological solution and the physical interfaces to that technology. So it is with the world of biometrics.

In this industry, we are told to consider physical security as well as technical security, but often it is the starting point for a complete security solution and so it is for most cases involving biometric solutions. Biometrics have been hailed as the solution to guaranteeing the identity of an individual; and from a technology only perspective that may be the case, but it ignores a huge aspect of the identification process, i.e., how do we get to the biometric solutions in the first place. This obviously needs explanation, and once the explanation is understood – which is not complex – it should be easy to see why biometric passports, driving licenses, etc., have not had the impact expected. In this article we hope to not only highlight the issue with the use of biometric identities, but also the obvious solution; which isn't in the realm of IT.

The Process of Biometric Identification

To understand the issues and shortcomings of biometric identification, we first have to understand the process that describes how the identity cards, passports, etc., are used. For this we need to have a little history lesson. Biometric identity is fairly new to the identity scene and has been added to passports, driving licenses, work permits, student cards, and social services support identity cards. These more manual identity artifacts have had a long history before computers, and it may not be a surprise to learn that these have never been the subject of industry standardization. These are often introduced at town, county, state, etc., levels rather than at country or industry levels; as when they were introduced the "small world" that modern day jet travel has brought about meant that there was little benefit in setting up industry standards.

Biometrics has been subjected to ISO standards from the beginning because they were introduced into the modern world. However, the ID artifacts have not been subjected to the standards. This has not been a problem in a world where the Mark 1 Human Eyeball, coupled with the "Advanced Human Brain" have been at play, as the fuzzy logic applied by the brain, coupled with simple rules as to what an identity is, have abstracted out the common features that give us information about a person. We all have a repository of information and "learn by experience" rules that tell us what constitutes a name, an address, etc. Computers generally have to have these rules explicitly coded and that is not as easy

Problems Biometrics

Make Worse – Identity Validity Escalation in Enterprise CRM Systems

In this article we will cover at a high level how master data management (MDM) and customer relationship management (CRM) systems work, and how this can represent a risk to how much we trust the use of a validated biometric identity. We will also look at how a criminal can access and steal the use of this trusted identity. Security professionals need to understand these processes and ensure the objectives of confidentiality and integrity are adhered to.

Towards the end of the 1990s, businesses were trying to find new ways to make money and the focus in many saturated markets had moved from capturing new business with new customers to customer retention and selling more products to existing customers. Thus, the *Customer Relationship Management* (CRM) approach was born.

At the core of most CRM programs is the customer database and "master data management (MDM)" system, or "customer hub"; usually a core database which holds the "single customer view" of an individual customer that replicates to and from other representations in other systems. Most companies bought an off-the-shelf product for CRM, and some wrote their own components, but at the core there is a central representation of a customer or "party", along with related data such as addresses, telephone numbers and a product holdings table that lists what products the customer already has. CRM systems then integrate an analysis process that examines the data held about the customer and what market segment they occupy; and then analyzes what new products could be targeted to the customer, and what adjustments or incentives may be needed to get the customer to buy the product.

The key to understanding the CRM systems and the reason they represent a problem is to understand the core MDM customer database and the way it is used. Remember that CRM systems were introduced after enterprises had existing systems to sell in stores, sell over the internet (in many cases), handle calls in call centers and handle delivery – each of which may have had its own completely different representation of a customer. Thus, the "customer hub" was in many ways an integration technology, which took representations of a customer and changes to those representations in downstream systems, and manipulated the details into a single common format. These "clean" details were then replicated back to the downstream systems. This helped overcome the commonly heard, "I told my bank I had changed my address in the branch, so why does the head office still write to me at my old address?" issue – all of which assisted in customer retention.

To come up with a common representation, the customer hub has to establish that the different identities in the downstream systems all represent a single individual and in this the "scrub, match, merge" and "demerge" mechanisms were established, where information such as full name, address or previous address, date of birth, telephone number and postal code are all used to see what is common; which is then applied with weightings to create the single identity.

DIGITAL FORENSICS
/ MAGAZINE

Keep up to date on the latest developments in the world of digital forensics

Read Feature Articles on:

- Training and Certfication
- Management issues
- Tools and Techniques
- eDiscovery/eInvestigation
- Incident Response/First Response
- Hardware and Software
- Network Forensics
- Cyber Forensics
- and much more...

Apple Autopsy:

- A Digital Forensics look at all things Apple

From the Lab:

- In depth technical articles on products and techniques

Legal Section:

- In-depth articles on legal matters affecting Digital Forensics along with the latest legal news from around the world

VISIT DIGITALFORENSICSMAGAZINE.COM for the latest news and views from the digitalforensic community with special articles for registered users.

NEXT ISSUE OUT SOON
SUBSCRIBE NOW

Prospective authors should contact editorial@digitalforensicsmagazine.com for information on submissions.

Biometrics:

A Panacea to Verifying and Authenticating Identity?

Biometric applications that allow machines automatically to verify or authenticate a match between a code and an item give rise to over-optimistic expectations as to their reliability and what they can do, notably in the service of public policy objectives like territorial border controls requiring identity assurance.

Using biometrics for identity management attracts governments keen to cut costs, whether in relation to border management, ehealth or use for accessing egovernment services. The problem is that the term 'biometric' is not used in a consistent way. This leads to inflated claims about how biometrics can contribute to combating serious crime, enhance security and boost certainty in a person's claim to be genuinely who they claim to be.

The lack of consistency in the use of the term biometrics, moreover, leads to confusion over the reach of data protection legislation.

This article briefly shows why this arises and identifies areas where improvement is vital.

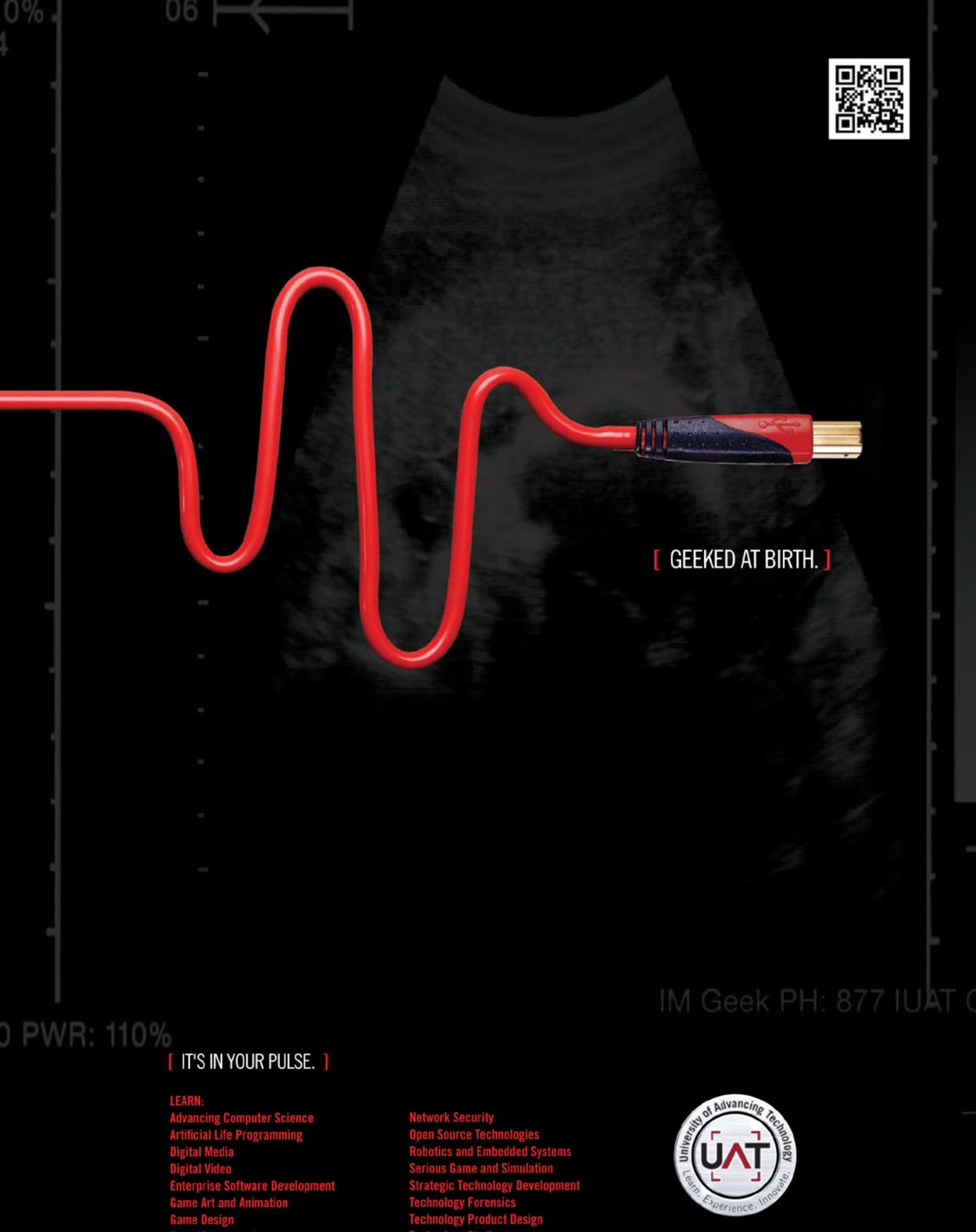
Defining biometrics

The European Union's definition of biometrics was originally narrow. It related to an algorithmic representation of a physical characteristic such as a fingerprint or an iris. By contrast, the United States' definition went further and included behaviour. This fundamental difference between the two muddies understanding of the extent to which data privacy and data protection laws reach.

Any definition of a biometric that includes the imprecise term 'behaviour' potentially brings everything that a person does into its scope. This means that if it is legitimate to collect information about biometrics, it is legitimate to collect information about 'behaviour'. This could include, for example, data gathering, mining, phishing, and tagging on social network sites, social plug-ins, and data given to or obtained from third party sites or disclosed to third parties (such as 'friends') or linked pseudononymously. This in turn creeps into all kinds of areas that a person might normally see as part of his/her private life, something that is protected under EU rules.

Behaviour can be deduced from association with other people as well as from things like a signature, gait, voice, travel patterns, leisure and sporting activities, social and educational background, employment and health records, online purchasing, advertracking, and internet browsing and so on. That brings it into the area of intelligence and all the guess-work as well as analysis of hard data that implies. It also implies a potential to expand exponentially access by the authorities to information that an individual may have provided for a very specific purpose only.

This in turn means that principles guiding legislation on data protection and privacy that seek to provide safeguards against function and mission creep, excessive intrusion and data sharing and mining, data linkage, reselling, splicing, tagging and out-sourcing are eroded.


0%
06
[GEEKED AT BIRTH.]
IM Geek PH: 877 IUAT
PWR: 110%

How Effective

is Face Recognition in an Airport?

Have you ever tried to go on a vacation and had to miss your summer holiday because when passing through airport security the system says it is not you? Well, this can happen. Nowadays, airports are adopting the face recognition system which takes a picture of you and compares it with the one stored on your passport. What happens if the picture taken is not under normal conditions?

This article will discuss using a series of tests to identify the accuracy of these systems. Conditions such as normal condition (e.g. normal photos of persons), ambient lighting (e.g. darken photos and brighten photos), framing the users face (e.g. zoom in to photos) and additive noise (e.g. altered photos with noise) are evaluated.

- A list of all 31 normal photos is created in a text file to use in order to compare which is matching with whom and in what percentage.
- The software analysed all 88 images together and matched the faces having the number 1 with the remaining photos.

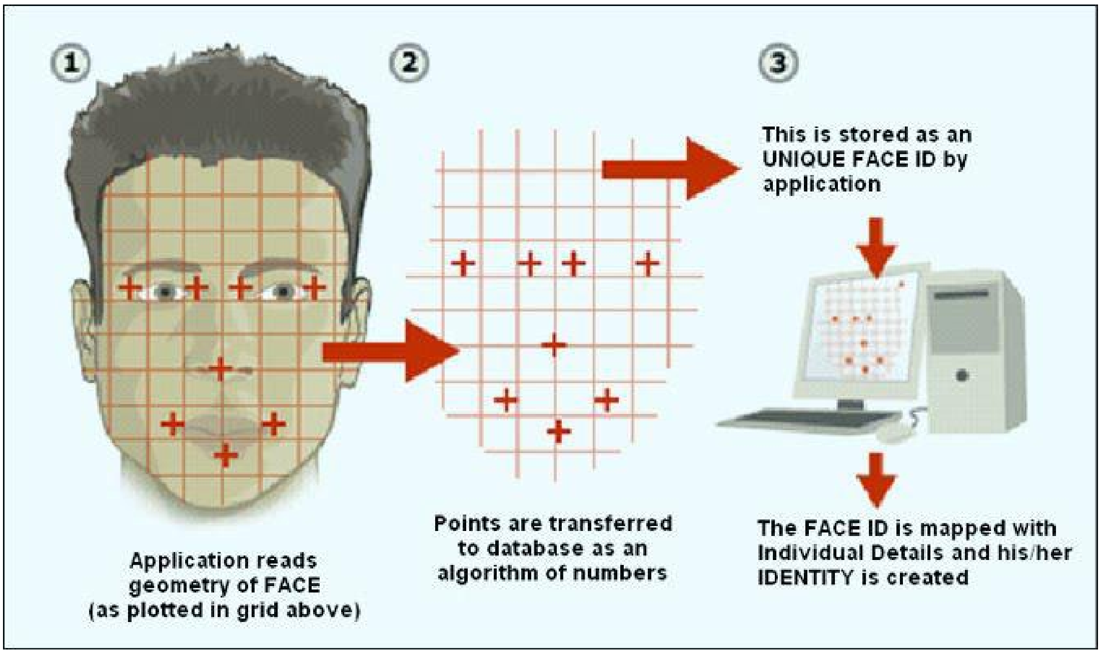

1
2
3
This is stored as an UNIQUE FACE ID by application
Application reads geometry of FACE (as plotted in grid above)
Points are transferred to database as an algorithm of numbers
The FACE ID is mapped with Individual Details and his/her IDENTITY is created

Figure 1. *Image recognition using FPGA devices (iproject ideas, 2010)*

Security Measures

to Consider When Preparing for a BYOD Environment

In the following sections a list of some of the well-known security risks associated with allowing users to bring their own devices to work will be presented. There will also be coverage of the suggested mitigations of the risks involved and a closing discussion. It is important to note that not all experts agree on what is the best BYOD solution and it is up to organisations to consider what will work for them given the research available and the context of their work environment.

Consumers and enterprises are adopting mobile device for professional use to increase productivity which has since become the topic of discussion amongst industry leaders. Terms like BYOD (*Bring Your Own Device*) and consumeration are used to define this trend in information technology. At some point, every organisation will have to consider whether to include the mobile device as part of its IT strategy. The information security challenges that are presented by the device will need to be addressed and the possible mitigations considered.

What are the risks?

As much as there is a great opportunity to leverage the mobile device for organisational productivity, it is important that the security risks involved with this effort are managed properly. Experts acknowledge the need for preparation through both the technology and policies within any given organisation, should it desire to leverage mobile device technology. Most organisations have strategies in place to manage the mobile devices they offer to employees. However, much is left to be desired when it comes to managing the devices owned by employees who would like to access organisational using their personal devices. The term "mobile devices" typically refers to PDAs, smartphones, tablets and laptops. These devices now have many of the same technological capabilities as a computer, such as the ability to connect to the Internet or to other devices on a network. For enterprises, allowing any device to connect to the internal network is not as simple as it may sound and comes with multiple threats. Chris Wyspol, Co-Founder & Chief Technology Officer of Veracode Inc. mentioned that the security issues faced by mobile devices are not the same as a static machines in an enterprise setting. These risks can be attributed to the lack of security mechanisms for smartphones and tablets such as anti-virus software. The following list was compiled from studies conducted by Ponemon Institute, Symantec Security Response, TATA, AT&T, Juniper Networks and other expert reports and presentations.

Device loss and theft are among the top threats that researchers acknowledge as an enterprise security risk. Employees use their mobile devices to store valuable personal and professional information such as client contacts and email. For some, it may include report drafts, marketing strategies and other sensitive business-related data. A study by Ponemon Institute following 116 organisations in March 2011, found that 62 percent of data bearing mobile devices lost by employees contained

A 24/7 Geek?

Interview with Michael Largue, CEO of Biotecnix Limited

At the age of 8 he was curious what made things tick and how little green boards (PCB's) as we know them could control moving parts. His dad's electric shaver was the first bit of hardware he pulled apart/broke/fixed and tried to hide all evidence. Then the fun began when he was introduced to a Tandy TRS-80/Commodore 64's/Spectrum/Atari's. Over the 22 years he has worked for some of the world's leading IT organisations and now he is the CEO of Biotecnix Limited.

Tell us about Biotecnix.

Biotecnix is a leader in the deployment of vein recognition biometric identification solutions. We deliver intelligent, secure and bespoke solutions to customers across a wide range of industries including construction, fleet, education, logistics, human resources, infrastructure and high value consumers leveraging vein recognition technologies.

Biotecnix ensure ultimate delivery of people identification enabling clients to manage operational challenges including driver identification, site security, access control, project reporting, identity verification, safeguarding workers, plant, property and mobile identify management.

Biotecnix has extensive knowledge of security, threats and biometrics and continues to innovate whilst maintaining focus on developing next generation solutions to today's identity and security problems.

Vein Secure™
BIOTECNIX
innovative security systems

Our goal is to continuously develop and implement high-performance, user-friendly vein recognition biometric products and solutions, meeting the rapidly growing need for positive identification and effectively countering the increasingly widespread phenomena of identity theft, forgery and asset theft.

How has your company grown in the past few years?

As the most promising biometric technology, vein recognition is quickly taking root around the world and has the ability to dominate applications where people focus is key.

Biotecnix has grown steadily over the past few years due to the growing acceptance and use of the technology. It is more accurate than many other biometric methods, it offers greater resistance to fraud, and it focuses on people, their privacy and has few negative cultural connotations.

What security areas does Biotecnix cater to?

Biotecnix operates in a number of vertical markets, including vehicle and plant security, commercial enterprises, education, access control, time and attendance and transportation security and takes great pride in delivering leading-edge technology and exceptional service.

‘Pass the Gauss’

If you have been keeping up with current malware news, you would have heard about a new form of “Super-Malware” known as ‘Gauss’. Gauss is essentially banker malware with a state-sponsored twist. Discovered in the Middle East, Gauss had been infecting the same general area as Flame.

While performing analysis on Flame, Kaspersky noticed suspicious Flame like operations originating from non-infected systems. When they investigated the activity, they discovered the Gauss malware. Unlike Flame, however, Gauss was built for a more general purpose that mirrors the intent of cyber-crime malware seen in the wild. However, underneath the sheep’s clothing of a common banking malware hides the functionality and intent of a cyber-espionage wolf.

According to the report by Kaspersky Labs, they discovered some “distinguishing features” in the Flame modules. These same features were found in a Stuxnet variant from 2009, leading researchers to believe that not only was there connection between the development teams for Flame and Stuxnet but that there might still be unknown modules yet to be found. While performing a search they discovered a previously unknown malware using the same identifying characteristics as Flame. This new malware shared similar design and coding practices as Flame and the researchers came to the conclusion that Flame and the new malware they dubbed as ‘Gauss’ were developed by the same team.

On the surface, Gauss was designed to install itself on a system, infect the browser and monitor the web activity of the user, waiting for them to navigate to one of numerous bank websites, wherein it steals their credentials and sends the data back to its *Command and Control* (C&C) servers. All of the banks targeted, service the same locations where the malware was discovered, namely Lebanon, Israel and Palestine. In addition, social networking

The Physical Aspects

of Cybersecurity and Their Importance – NISPOM

This an analysis will provide a detailed explanation of the requirements for the federal government contractor industrial base, as well as explore the ways in which the policies are utilized and also tested to ensure their timely effectiveness and currency. Any vulnerabilities identified are strictly for educational purposes and not to be taken as anything other than examples for learning and instructional purposes only.

For those who just joined, we are analyzing the different aspects behind the central policy document of the US Federal Government and its various Agencies titled NISPOM. The National *Industrial Security Program Operating Manual* (NISPOM) looking at the strengths and weaknesses of what the United States Department of Defense set out as standards and methods for their contractor base.

In this installment we'll take a look at Chapters 7 through 9, which detail the requirements for subcontracting, information security and special requirements.

The Physical Reality

To refresh, the Chapters we'll be discussing in this series of articles are from NISPOM as follows:

- General Provisions and Requirements
- Chapter 2 – Security Clearances
  - Section 1 – Facility Clearances
  - Section 2 – Personnel Security Clearances
  - Section 3 – *Foreign Ownership, Control, or Influence* (FOCI) (Highlight indicates the areas to be discussed in this installment of The Physical Aspects of Cybersecurity and Their Importance – NISPOM)
- Chapter 3 – Security Training and Briefings
- Chapter 4 – Classification and Marking
- Chapter 5 – Safeguarding Classified Information
- Chapter 6 – Visits and Meetings
- Chapter 7 – Subcontracting
- Chapter 8 – Information System Security
- Chapter 9 – Special Requirements
  - Section 1 – RD and FRD
  - Section 2 – DoD Critical Nuclear Weapon Design Information (CNWDI)
  - Section 3 – Intelligence Information
  - Section 4 – Communication Security (COMSEC)
- Chapter 10 – International Security Requirements
- Chapter 11 – Miscellaneous Information
  - Section 1 – TEMPEST
  - Section 2 – Defense Technical Information Center (DTIC)
  - Section 3 – Independent Research and Development (IR&D) Efforts
- Appendices (*en.wikipedia.org/wiki/NISPOM*, downloaded 17 June 2012)

Special Requirements

Within the government and its agencies, the most common aspect of imparting learning skills and developing human resource optimization is carried out through training. The reason is simple.

Save The Database, Save The World!

Chapter 8
DATABASE SRC IN THE CLOUD

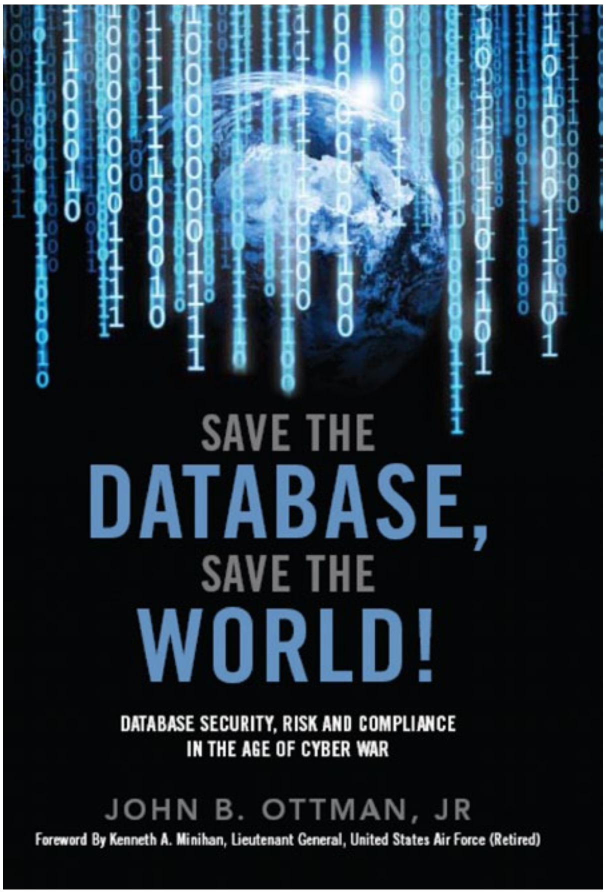
“Organizations that outsource their IT management and support also outsource a great deal of trust to these partners.”

In their research document “The Cloud Wars: $100+ billion at Stake,” Merrill Lynch predicts that by 2011 the cloud computing market will reach $160 billion in revenue.lxix Some say that the unprecedented hype surrounding this new paradigm stems from the disruptive departure cloud computing represents from traditional computing and operational processes. Cloud computing offers important on-demand benefits such as “pay-as-you-go” and self-service where capacity is elastic and applications are deployed without regard to underlying architecture.

The evolution of software to a service delivery model frees users from the limitations of traditional infrastructure such as scalability, performance bottlenecks, and capacity. But these are the business implications of the cloud paradigm. What are the underlying technology and operational implications? How do we enable database SRC in the cloud?

Whether cloud computing is delivered from a public, private, or hybrid cloud model, the underlying infrastructure is built upon the same technical building blocks as before. Behind the curtain of every cloud-computing model we still find software, servers, storage frames, and networks built and integrated by the same suppliers as before.

Databases still require backups, software patches must still be applied, and “super users” must still be entitled with universal access to manage operations. What has changed?


SAVE THE
DATABASE,
SAVE THE
WORLD!
DATABASE SECURITY, RISK AND COMPLIANCE
IN THE AGE OF CYBER WAR
JOHN B. OTTMAN, JR
Foreword By Kenneth A. Minihan, Lieutenant General, United States Air Force (Retired)

In the Upcoming Issue of

PenTest magazine

Exploitation Framework: BeEF

Available to download on November 5th

More topics in PenTest Magazine:

Information Security Governance, Hacking an Isolated Network, Phishing, Spoofing, BeEF, Business Application Change Control, Recoinnaissance & Network Mapping, DNS & ARP, Android as a Pentesting Platform, Intrusion Detection Systems, Sandbox

... and more

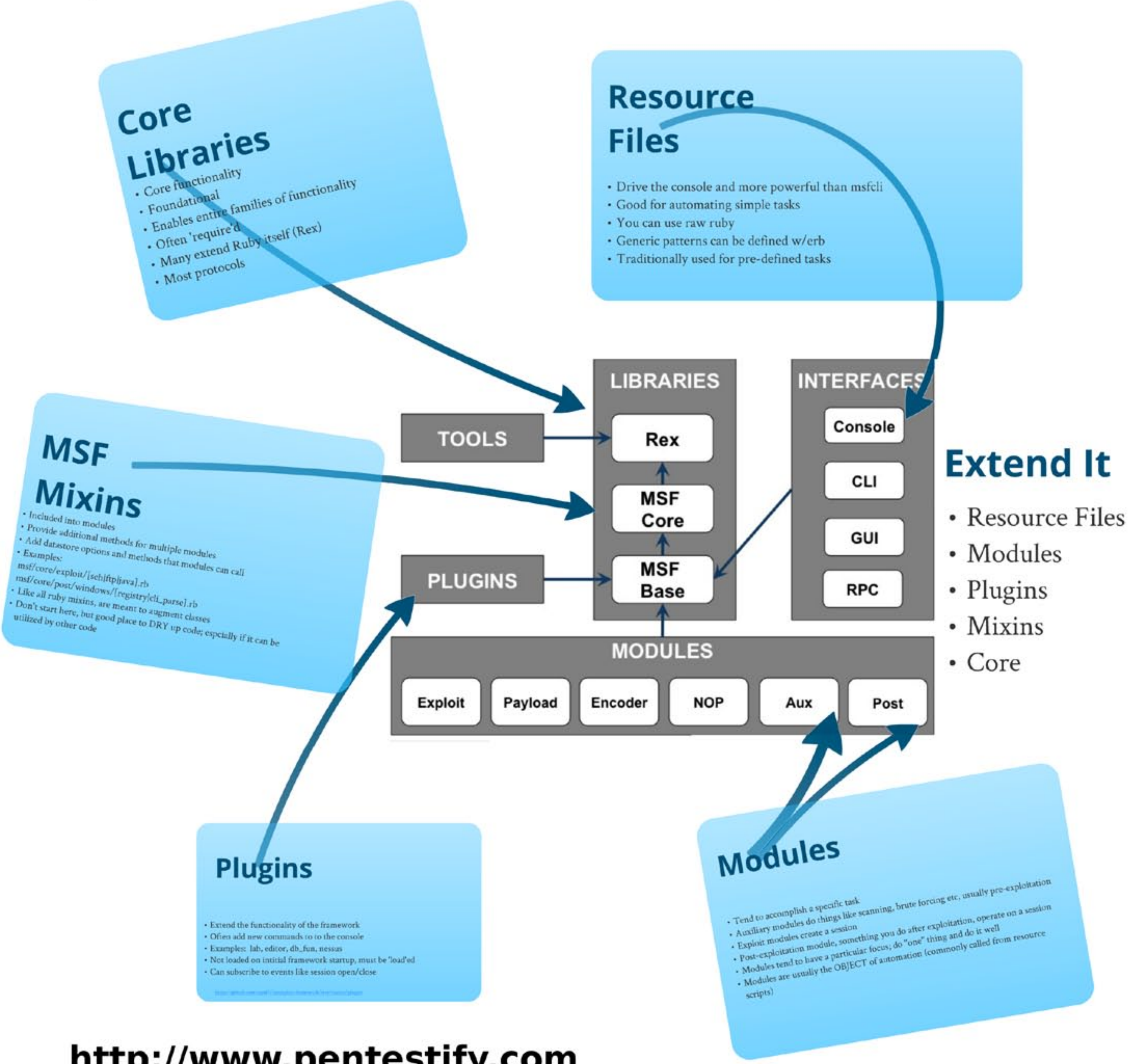
If you would like to contact PenTest team, just send an email to
krzysztof.sikora@software.com.pl or ewa.dudzic@software.com.pl .
We will reply a.s.a.p.

PenTest Magazine has a rights to change the content of the next Magazine Edition.

Pentestify, LLC
Tactical Offensive Security

- Metasploit training
- Custom Metasploit Modules
- Advanced Penetration Testing
- Offensive Security Consulting
- Security Tool Automation

```
class Defender < Attacker
   include Tactics::Attacker
   include Tools::Msf
end
you = Defender.new
msf = Msf.new
msf.desc = "Swiss Army Knife"
you.arsenal << msf
```



Core Libraries

- Core functionality
- Foundational
- Enables entire families of functionality
- Often 'require'd
- Many extend Ruby itself (Rex)
- Most protocols

Resource Files

- Drive the console and more powerful than msfcli
- Good for automating simple tasks
- You can use raw ruby
- Generic patterns can be defined w/erb
- Traditionally used for pre-defined tasks

MSF Mixins

- Included into modules
- Provide additional methods for multiple modules
- Add datastore options and methods that modules can call
- Examples:
  msf/core/exploit/[seh|ftp|java].rb
  msf/core/post/windows/[registry|cli_parse].rb
- Like all ruby mixins, are meant to augment classes
- Don't start here, but good place to DRY up code; especially if it can be utilized by other code

Extend It

- Resource Files
- Modules
- Plugins
- Mixins
- Core

Plugins

- Extend the functionality of the framework
- Often add new commands to to the console
- Examples: lab, editor, db_fun, nessus
- Not loaded on intitial framework startup, must be 'load'ed
- Can subscribe to events like session open/close

Modules

- Tend to accomplish a specific task
- Auxiliary modules do things like scanning, brute forcing etc, usually pre-exploitation
- Exploit modules create a session
- Post-exploitation module, something you do after exploitation, operate on a session
- Modules tend to have a particular focus; do "one" thing and do it well
- Modules are usually the OBJECT of automation (commonly called from resource scripts)

http://www.pentestify.com