

# Fishing for Passwords

*How dangerous passwords really are...*

## **Everybody has Access to your DATA!!!**

White-collar crime is the fastest growing type of crime in North America, and co-workers and disgruntled employees have many motivations to cause damages or increase their wealth. Especially in the current economy it is every company's responsibility to keep honest employees honest by preventing opportunities and temptation!

The first thing intruders do before taking any illegal action is to get access to another colleague's user profile for extended access so that the other person will be blamed. Below we will point out how easy this unfortunately is...

One of our customers lost over \$60 Million in a 4 year period. A director used one of his employee's user profiles and passwords to commit the fraud in the SAP financial system. When the fraud was discovered, this employee spent half a year in jail for a crime that she did not commit. Eventually, her boss was arrested for stealing her password and committing the fraud.

## **BUT - Our executives still believe that passwords are secure!**

How can IT experts today communicate to their business management that they have control weakness today without putting themselves in a "bad" position?

We would not want to put anybody in the position to declare that they have significant control weaknesses, but as our documentation and our power point presentation demonstrates, passwords are outdated and they are the weakest link within your controls. In a world of anti-malware scanners it is common knowledge that security threats evolve on a daily basis and that is why customers must update their anti-malware software frequently to be prepared for the latest attacks.

Passwords have been around since the first computers in 1963, and while they might have been fairly secure back then, technology is evolving and is making them more vulnerable on a daily basis:

- Password crackers get faster and more sophisticated, as well as the computers that run them\*
- Hacking tools are now legally sold in stores as Password Recovery tools\*\*
- Physical and logical key loggers have been invented and can be implemented without detection
- Hidden cameras and even cell phones tape passwords – surveillance cameras are everywhere
- Algorithms can decrypt passwords just based on sound
- Users have too many logons and passwords and are forced to write them down
- Systems require frequent password renewal (forcing users to write them down)
- Users are forced to create more complex and longer passwords (no choice but to write them down)

\* Computer clustering allows to crack passwords in 20 minutes instead of 5 days (details below)

\*\*Password recovery tools are tested, reviewed and free downloads are available:

<http://pcsupport.about.com/od/toolsofthetrade/tp/passrecovery.htm>



## Would your security guard STOP this guy walking through the main entrance?



### Hopefully the Security Guard will stop him or her!

Even this guy identifies himself as “Tom N.” on his space suit...

Without using biometrics we can only identify “Space Suits” with names on them (User Profile Names) walking around in the most critical part of our organization – the IT System.

We have NO WAY of identifying who is using the suit (User profile). Any intruder can steal a suit and walk around in critical areas (as seen in James Bond movies) biometrics will uniquely identify the user behind the “Space Suit”. You check ID in your building – do it in your IT System as well!

We would like to invite you to click through our PPT and ESPECIALLY Page 14 in “slide show mode” to find out why password protected access control poses an extreme security risk for any organization and find out how your access control will be 20 times stronger using bioLock technology (Page 9):  
[http://www.realtimorthamerica.com/download/biolock\\_presentation.ppt](http://www.realtimorthamerica.com/download/biolock_presentation.ppt)

## 7 % of a company’s revenue was lost to fraud in 2008

The so called “occupational fraud” (also known as internal theft) and abuse imposes enormous costs on organizations. The median loss caused by occupational fraud in this 2008 ACFE study was \$175,000. Nearly one-quarter of the cases caused at least \$1 million in losses and nine cases caused losses of \$1 billion or more. Participants in the study estimate U.S. organizations lose 7% of their annual revenues to fraud. Applied to the estimated 2008 United States Gross Domestic Product, this 7% figure would translate to approximately \$994 billion in fraud losses. Fraud schemes usually continue for years before they are detected. Fraud was mostly committed by upper management or accounting and most of the criminals were first time offenders.

Read the full study at: <http://www.acfe.com/RTTN/2008-rtn.asp>  
(Source: 2008 Study - Association of Certified Fraud Examiners – www.acfe.com)

## Billion Dollar Lawsuits, Bad Image and Firings as results of Data Breaches

In May 2006, personal records from roughly 26.5 million veterans were stolen from the Department of Veterans Affairs. In the aftermath and following investigations, there have been resignations, firings and a rethinking of how government agencies and private companies should be protecting personal information. Read the full story at: <http://www2.csoonline.com/exclusives/column.html?CID=21678>

On June 6th the Veterans Groups sued the VA seeking up to \$26.5Billion in Damages:  
[http://www2.csoonline.com/blog\\_view.html?CID=21794](http://www2.csoonline.com/blog_view.html?CID=21794)

Another article hit the email “news blast” recently with the subject line “\$400 million corporate espionage incident at DuPont”. A study about accounting challenges linked to passwords:  
[http://www.securityworldmag.com/head/weekly\\_view.asp?idx=1227](http://www.securityworldmag.com/head/weekly_view.asp?idx=1227)

Insider at Cal Water Steals \$9M and Runs - He gained access to computers from two executives:  
[http://www.csoonline.com/article/493377/Insider at Cal Water Steals 9M and Runs?page=1](http://www.csoonline.com/article/493377/Insider_at_Cal_Water_Steals_9M_and_Runs?page=1)

Former Intel Employee Indicted for stealing more than \$1BILLION of Trade Secrets (Nov. 2008):  
<http://www.cybercrime.gov/paniIndict.pdf>

Russian's steal from Citigroup - Hackers steal 10's of millions of dollars after hacking into the system:  
<http://compliance.typepad.com/compliance/2009/12/hackers-in-breach-of-citi-report.html>

### **SAP Info reported on Feb 25<sup>th</sup> 2008: Poor IT Procedures Enabled Societe Generale Fraud**

Inadequate IT security allowed a trader at French bank Societe Generale to make a series of unauthorized transactions that ultimately cost the bank 4.9 billion euros (US\$7.2 billion), an internal investigation has found. To prevent a recurrence, the bank should immediately introduce stronger security systems, including **biometric authentication** of trading staff, a special committee has recommended in its preliminary report to the bank's board of directors.

<http://www.realtimenorthamerica.com/download/PoorITProceduresFrenchBankFraud.pdf>

### **Baden (Pittsburgh) police officer gave a co-worker a password to a police data base. He identified his ex-wife's boy friend and KILLED him – but he got the wrong guy!**

A local cop gave his password to the state database to another officer who used it to look up info about his friend's ex-wife's boyfriend. The ex-husband then shot and killed the guy - but he got the wrong guy. If they had biometric protection for the state database very likely this could have been prevented. See the newspaper article for detailed info:

[http://www.timesonline.com/opinion/opinion\\_details/article/1373/2009/december/15/baden-cop-accused-of-giving-information-to-alleged-killer.html](http://www.timesonline.com/opinion/opinion_details/article/1373/2009/december/15/baden-cop-accused-of-giving-information-to-alleged-killer.html)

### **Passwords are Outdated, Insecure and Expensive and offer no accountability!!!**

As mentioned earlier, the first functional computers have been around since 1963. Since then, everything has changed on a computer except the way we log onto computers – the password. In the security world there are 3 ways to gain any kind of physical or electronic access: 1. What you know – the password; 2. What you have – a smart card, key or token and 3. Who you are – biometrics. Biometrics has been proven not only to be the most secure solution but also the most convenient method for users and the least expensive way to go for the IT department, when considering the cost of password administration. No more password resets, which account to a majority of every companies IT helpdesk cost. Smart Cards, tokens and keys can still be lost, stolen or passed on to a different person. They still don't offer the capability to uniquely identify the actual user. The commonly used passwords are very dangerous and offer no protection at all. Especially in a world, where most companies spend millions on compliance issues and they still rely on the (wrong) assumption, that only Joe Smith can log on to the IT system as Joe Smith.

## How easy can the intruder get access to “another” user profile to cause damage?

- Go to the computer while owner leaves or gets a coffee
- Ask or challenge colleagues (40% admit sharing password)
- Check the ‘history’ of the first ‘login field’ for password entry
- Call hotline with a different name or user login to get a reset
- Try the Default USER: SAP\* - Default Password: 06071992
- Create a fake password login screen that emails password to intruder
- Look for the password near the computer and in drawers (right upper drawer is your best chance)
- Look over shoulders of employees when they enter it (the FBI calls it shoulder surfing)
- Video tape it – watch for people with a cell phone around you
- Get Emergency password (in some companies at the security guard)
- Keyboard Click-and-Clack Reveals Passwords (Intruders record the sound)
- Key Catcher, Password Cracker – Now: Recovery Tools sold in stores
- Check ‘.INI’ files in Windows which might contain non encrypted passwords
- Or simply associate with the owner (hometown, car, children, wife, animal etc.)
- Password Monitoring / Sniffers (transfer from GUI is not encrypted)

**82% of all Passwords  
are written down!**

**SAP Info Magazine**

### Top 10 most popular Passwords:

Need a password for a website?

Try [www.bugmenot.com](http://www.bugmenot.com)

#### The top 10 Passwords:

1. password
2. 123456
3. qwerty
4. abc123
5. letmein
6. monkey
7. myspace1
8. password1
9. blink182
10. your first name

Source PC Magazine

*Did you ever wonder how many employees watch you on the security screen,  
while you type in the PIN number for your charge card at the supermarket?  
Look for the security camera – conveniently located over your head!*

## Shoulder Surfing – worse than you think

With many cell phones being equipped with digital cameras, how can you make sure that nobody is filming you while you put in your password? What do all these objects have in common?



Pen



Malboro Box



Motivational Picture



Wall Clock



Glasses or Tie on any person...



**They all have a camera built in to capture your password and more!**

<http://www.spysource.net/covertwirelesscameras.htm> or <http://www.hiddenpinholecameras.com/>

## Can't capture the image – just record the sound

The researchers, from the University of California at Berkeley, found that a 10-minute recording of a person typing at the keyboard reveals enough information for a computer analysis to recover nearly 90 percent of the words entered. <http://www.securityfocus.com/news/11318>

## Social Engineering

Many passwords are being shared during a chat in the cafeteria or in the smoking section. Some employees even brag about how secure their new password is (definitely if you challenge them). A survey during the InfoSecurity Tradeshaw in London revealed that over 70% of all people approached gave up their password for a candy bar: <http://news.bbc.co.uk/2/hi/technology/3639679.stm>

## Password Crackers - 80% of All Passwords cracked in 30 Seconds!

A recent article describes how Phil Fowler, VP of IT of Telesis Community Credit Union switches to biometrics, after his team could crack 80% of peoples passwords in 30 Seconds. Free password crackers can run over 4 million passwords a minute. Since the name "Password Cracker" has a negative image the tools have officially been renamed to "Password Recovery Tool" and can now be sold legitimately to recover your own and anybody's password at any point of time. Here is a list of top 10 password crackers: <http://sectools.org/crackers.html>

## Hacking Passwords in older versions of SAP was fairly simple:

There are at least two methods to this attack:

Dictionary hack (using common words)

Brute force hack (using all possibilities)

ABAP code for both of these can be found in the Internet. The dictionary and brute force attacks are not detected by the system and therefore will not set-off a warning or lock the user. There is a standard SAP module which helps to compare the passwords for the hack. There are also SAP plug-ins available for popular hacking software.

Hacking passwords in older versions of SAP is easily accomplished due to the following reasons:

- Hash values were stored in tables which are viewable by many users
- The hash algorithms were weak
- Passwords were not case sensitive
- The system was limited to 8 characters
- There were many back doors into an SAP system

After SAP NetWeaver 6.40, the password hash algorithm was changed from MD5 to SHA-1 to make hacking harder – but technology is catching up quickly.

**KeyCatchers can be built into keyboards, mice or other USB devices and are completely undetectable with the human eye or software!**

### KeyCatcher or Password Stealer

A KeyCatcher is a \$70 hardware that plugs in between the keyboard and the computer. It records any keystroke and password being typed in. The same technology is available as FREE software. Try Remote Password Stealer 2.7 !



KeyCatcher

### Trojans will send passwords to anybody over the Internet

You are certainly aware of Trojans that enter your network via email or IM's and that have the capability to send logon and password information back to the original creator. Even if your network is well protected with the latest software the intruders get very creative. One recent story describes intruders that distributed 20 thumb drives in the parking lot of a Credit Union. Sure enough, 15 of the thumb drives were found by employees and plugged into the corporate network minutes later. The included Trojan reported logon and password information back to the intruder:

[http://www.darkreading.com/document.asp?doc\\_id=95556&WT.svl=column1\\_1](http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1)

### An “Electronic Locksmith” will help the bad guys for a fee

Once you lock your key in the house you call a locksmith. There are many electronic “locksmiths” on the Internet. If you forget your logon and/or password they will be glad to help out, even if you are not the true owner of the logon. Just charge \$20 to your credit card and they will send you any password you want. In other words: a non-technical intruder can easily “recruit” a hacker to do the dirty work for them.

## Homeland Security Newswire published an article about WPA Cracker:

*Want to check whether the password to your wireless network (or your neighbor's) passes muster? For \$34, you can do just that by using a password-cracking service that is primarily aimed at "penetration testers" — people who are paid by a company to test its network's security.*

*Robert Lemos writes that the service, known as WPA Cracker ( <http://www.wpacracker.com> ), is one of the first hacking services to rely on cloud computing. WPA Cracker went live last Monday — it uses pay-as-you go cloud computing resources to search for an encrypted WiFi Protected Access (WPA) password from 135 million different possibilities, says creator and hacker Moxie Marlinspike. Normally the task would take a single computer about five days, but WPA Cracker uses a cluster of 400 virtual computers and high-performance computing techniques. It takes only twenty minutes, he says.*

<http://homelandsecuritynewswire.com/cybercriminals-begin-exploit-cloud-hacking?page=0,0>

## SAP Passwords are not encrypted

Did you know that between the SAP GUI and the server the password is not encrypted? Try any free Password Sniffer from the Internet and you will see all passwords being typed in from any user. A better program will display the SAP User Logon and password together!

### **The Fact is:**

**If a person wants anybody's password and access to anybody's user profile, they will get it without problems, and statistics confirm that they will use those user profiles with extended authorizations to cause damages!**

## According to SAP Info – Women are More Likely to Reveal Passwords (at least in the UK)

Women are four times as likely to give their computer passwords to a stranger than men, with the lure of a chocolate bar. Of the 576 people recently interviewed in London, 45 percent of women provided their passwords. Of men, ten percent did so.

<http://www.sap.info/public/INT/int/clicks/DBNF/22284480704cac4e95>

## What about smart cards or tokens:

Smart Cards and Tokens are definitely one step up from Passwords but they can still be lost, stolen, copied, borrowed or passed on to another person. There is still no proof that the actual user was the authorized user any lawyer would use the SODDI defense (Some Other Dude did It) in case of an attempted conviction.

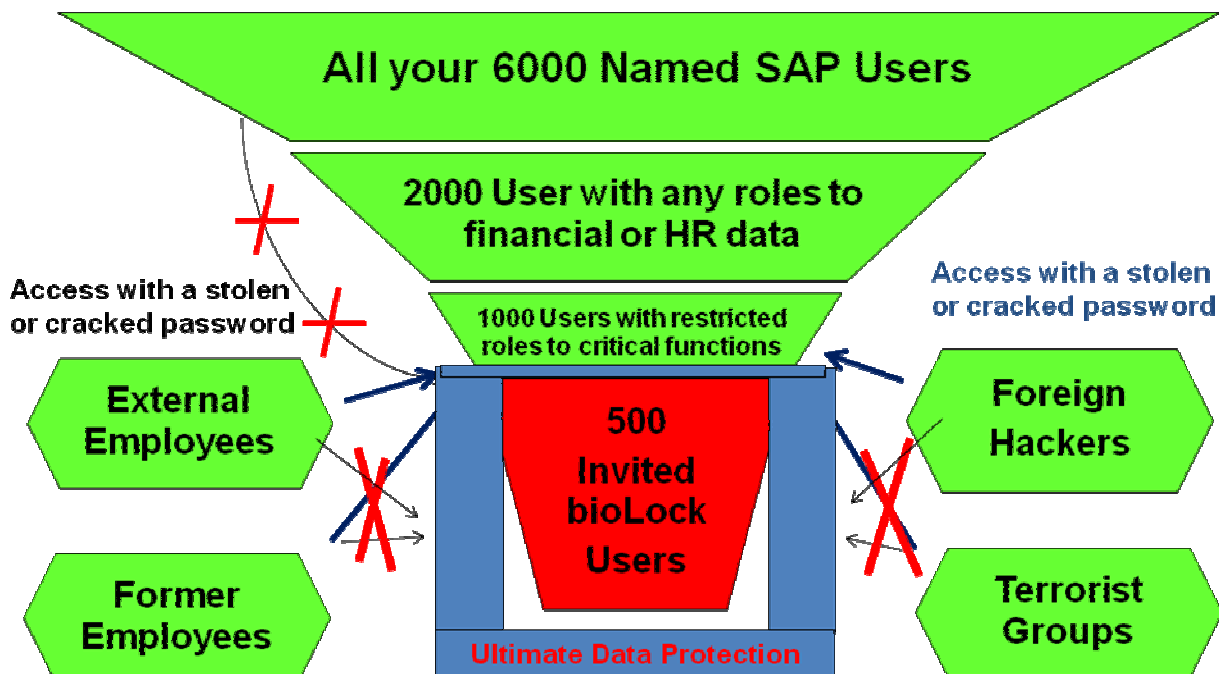
## Biometrics - More than just a "fancy" replacement for passwords...

With innovative technology, biometrics cannot only protect the logon to a computer or an application, but also prevents costly incidents within the SAP system. bioLock is the first technology that can basically protect any mouse click in the SAP system and offer you fraud mitigation within your system. Independent from the actual user that logged on to the SAP system (with or without biometrics), the security team can put an additional biometric "door lock" on any critical function within the SAP system: Common areas are Finance, HR, research or PM notifications. Once a transaction or function - like displaying a balance sheet, creating a purchase order or issuing a wire transfer - is requested bioLock will pop up a window requesting a biometric verification. A finger has to be placed on the sensor in order to proceed. View a brief demo movie at [www.biolock.us](http://www.biolock.us) .

## In Conclusion

As outlined in this document, intruders have many ways to obtain any password. The example below shows a company with 6,000 named SAP users. While only 1,000 employees have access to the companies most vital information, all of the 6,000 named users – or external employees, former employees, foreign hackers or terrorist groups – could simply access the critical information by obtaining a password for one of the top 1,000 SAP user profiles (Power users with critical authorizations).

bioLock allows a company to place a biometric door lock on ANY critical function in the SAP system. Once invited with their biometric credentials, only the top 500 power users indicated below in red (or how many biometric users the company chooses to invite) will be able to execute critical functions. The software will automatically reject any other user (all green groups) as well as administrators or external consultants!



**Get more detailed information about fraud mitigation at**

**[www.fraudmitigation.com](http://www.fraudmitigation.com)**

**For more information about realtime North America Inc. or to schedule an online bioLock demo go to [www.bioLock.us](http://www.bioLock.us) or contact us at info**

**@realtimenorthamerica.com; 1-877-bioLock**

Disclosure: This document is for educational purposes only. The content in this document is openly available on the Internet. This summary is prepared to help companies to prevent fraud and is not intended for individuals to commit fraud. We explicitly discourage any individual from attempting to commit fraud as the bad guys will usually get caught. realtime North America Inc. assumes no liability for the use or misuse of this educational information! We do not guarantee that the links are working and we also do not warrant that the web sites are safe to visit!

Copyright realtime North America Inc. 2009