THE SECURITY STANDARD™

Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by

CSO

The Encryption Conundrum

Daniel Srebnick

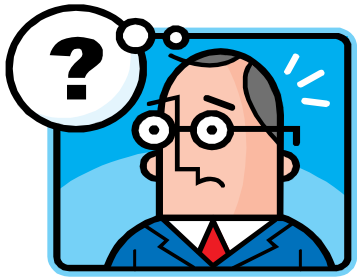
CISO

NYC Department of Information Technology and Telecommunications

From dictionary.com: co*nun*drum/Noun

1. A confusing and difficult problem or question.

2. A question asked for amusement, typically one with a pun in its answer; a riddle.



The Question:

Is encryption ALWAYS required and is it ALWAYS practical to encrypt all private data?

The Answer:
Let's Encrypt All Our Data!

We are security practitioners and professionals.

We are smart?

We know that the bad guys can't see our data if we encrypt it.

It's that simple…isn't it?

The basic questions…

- **W**ho are we protecting the data from?
- **W**hat data are we protecting?
- **W**hen does the data require protection?
- **W**here is the protection required?
- **W**hy does the data require protection?
- **H**ow are we going to do this?

Who?

- Network engineers and sysadmins should not be looking at private or confidential data.

- No unauthorized individual should be looking either.

What?

- What data has to be encrypted?
- City of New York data classified at a particular level must be encrypted in transit and at rest.

When?

- Encrypt data at rest
  - On disk
  - On backup media
- Encrypt data in transit over the wire
  - LAN
  - WAN
  - And SAN—that too is a network!

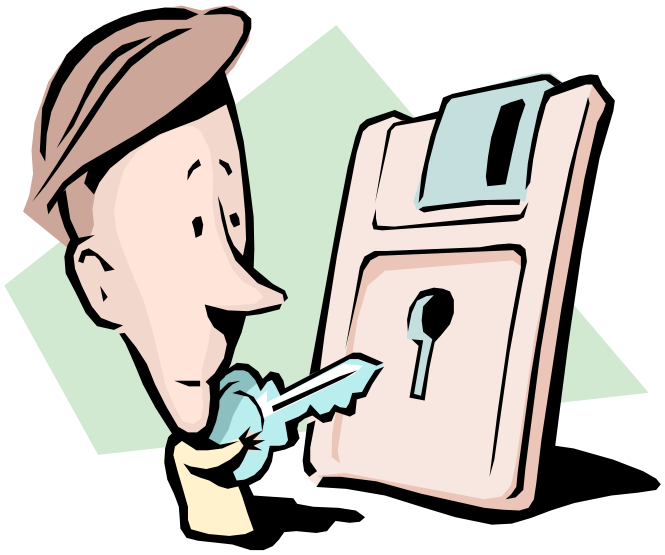
So the data has left the wire…

And now it is on some host

- First it is in memory, which is very hard to encrypt and process at the same time
- Although encryption is a great idea for non-volatile storage on mobile devices, there are key management issues
- And now you need to store the data on some permanent storage device such as disk

Where?

- Database columns (TDE)
- Fileshares and filesystems (efs, Bitlocker)
- Tapes (especially tapes that are exported outside of the datacenter!)



HHC - Data Theft Notification - Freequently Asked Questions - Windows Internet Explorer

http://www.nyc.gov/html/hhc/html/pr/notice-faq.shtml

nyc hhc data tapes lost

HHC - Data Theft Notification - Freequentl...

Page Tools

Search | Email Updates | Contact Us

Residents | Business | Visitors | Government | Office of the Mayor

NEW YORK CITY HEALTH AND HOSPITALS CORPORATION

nyc.gov/hhc

Michael A. Stocker, M.D. Chairman
Alan D. Aviles, President

ACUTE CARE HOSPITALS

Bellevue • Coney Island • Elmhurst • Harlem
Jacobi • Kings County • Lincoln • Metropolitan
North Central Bronx • Queens • Woodhull

Search GO Text Size: A A A

Find a Specialty | Locate Our Facilities | Physician Referrals | Newsroom | Translate

- Home
- About HHC
- Hospitals, Medical Centers and Home Care Services
- Affordable Healthcare
- Specialty Services A-Z
- Public Meetings
- Publications and Reports
- How You Can Help
- Contact HHC

Data Theft Notification

Printer Friendly
Email a Friend

FREQUENTLY ASKED QUESTIONS:

Q: *What is the North Bronx Healthcare Network?*

A: The North Bronx Healthcare Network is part of the New York City Health and Hospitals Corporation, commonly called "HHC." The Network consists of Jacobi Medical Center, North Central Bronx Hospital and two affiliated community healthcare centers: the Health Center at Tremont and the Health Center at Gun Hill. If you were a patient, or a Network workforce member, at any of these facilities between 1991 and early December 2010, you may be affected by this incident.

Q: *What was this incident?*

A: On December 23, 2010, computer backup tapes for two North Bronx computer systems were stolen from the truck of our vendor GRM Information Management Services while being taken to a secure storage location. The GRM truck was parked on the street in Manhattan at the time of the theft while the driver was making a pickup from another GRM customer. Our tapes contained patient protected health information.

Please be assured that only a person with specialized knowledge and access to the right software and computer hardware would be able to view the information on the stolen tapes. However, in the interest of the safety and protection of our patients' personal and health information, and to secure them from harm, we have arranged for each affected party, at his or her option, to receive identity protection services from Debix, the Identity Protection Network.

The North Bronx Healthcare Network regrets any inconvenience that this incident may cause you. Although we do not have any proof that your private information was accessed by any unauthorized persons, we are required by law to notify all individuals

Done | Internet | 100%

How?

Encryption: The path to secure commerce and data security

Secure Socket Layer (SSL)

- First 40 bit, later 56 bit, now 128 bit
- Protects data traveling “across the wire” from prying eyes
- Ensures secure online financial and e-commerce transactions by overcoming credential or credit card interception

Without SSL there would be no…

- eBay
- Amazon
- Online Banking
- Online Securities Trading

Can we encrypt it to keep it secure?

Let's start with a local disk…

- It makes complete sense to use some type of disk or file system encryption package.
- Someone can walk about with the disk and your data, so an encrypted file system is great protection if you hold the key.

iSCSI me please…

- iSCSI offers an over-the-wire solution for encryption
- iSCSI can be tunneled through IPSEC
- iSCSI also offers other security advantages such as CHAP (describe)

Encrypted File Systems

- Not seen much in production use
- The encryption occurs on the host rather than on the SAN
- Microsoft EFS
- Linux Ecryptfs

This seems difficult -- Is that why they're called "Hard Disks"?

- The not-for-profit Trusted Computing Group wants to make disk encryption easier.
- Self-encrypting drive solutions based on TCG specifications enable integrated encryption and access control within the protected hardware of the drive.
- Self- encrypting drives may provide the best solution for full disk encryption, protecting data when the machines or drives are lost or stolen.
- TCG's open standards provide multivendor interoperability.

Benefits of Self Encrypting Drives

- Better performance – hardware optimized
- Stronger security – always on
- Easier to use – completely transparent to users and softare
- Lower TCO – no key management infrastructure required.

How is your mobile device encryption?

- iPhone/iPad?
- Android?
- Blackberry?
- Laptop?
- Netbook?

- Any mobile device that stores the encryption key onboard is not going to be so secure
- Any mobile device requiring a user to input an encryption key is not going to be seen as user friendly


Russian Company Cracks IOS 4 Hardware Encryption CIO.com - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Russian Company Cracks IOS 4 H...
http://www.cio.com/article/682916/Russian_Company_Cracks_IOS_4_Hardware_Encryption
so magazine iphone 4 encryption
splunk> listen to your data
Learn More »
CIO
White Papers Webcasts Solution Centers IT Jobs Council Events Magazine Newsletters RSS Follow CIO:
NEWS ANALYSIS BLOGS SLIDESHOWS VIDEOS HOW TO
Google™ Custom Search
DRILLDOWNS Applications Careers Cloud Computing Data Center Mobile Operating Systems Outsourcing Security Virtualization Web 2.0 All topics
Russian Company Cracks IOS 4 Hardware Encryption
Having cracked Apple iPhone backups last year, Russian security company ElcomSoft appears to have found a reliable way to beat the layered encryption system used to secure data held on the smartphone itself.
By John E. Dunn
Wed, May 25, 2011
Like 5 +1 0
Leave a comment
2 Tweet
3 Share
0 Reddit
0 Digg
0
IDG News Service — Having cracked Apple iPhone backups last year, Russian security company ElcomSoft appears to have found a reliable way to beat the layered encryption system used to secure data held on the smartphone itself.
Since the advent of iOS 4 in June 2010, Apple (AAPL) has been able to secure data on compatible devices using a hardware encryption system called Data Protection, which stores a user's passcode key on an internal chip using 256-bit AES (AES) encryption. Adding to this, each file stored on an iOS device is secured with an individual key computed from the device's Unique ID (UID).
Apple products containing this security design include all devices from 2009 onwards, including the iPhone 3GS (which can be upgraded to iOS 4), iPhone 4, iPad, iPad 2 and recent iPod Touch models.
ElcomSoft has not explained how it hacked the hardware-stored key system in detail for commercial reasons, but the first point of attack appears to have been the user system passcode itself as all other keys are only vulnerable to attack once the device is in an unlocked state
You are here: Technology Topics » Security » News
Most Recent Encryption Stories
Cellcrypt Releases Encrypted Voice Call App for the IPhone
2011 Timeline of Major High Tech Awards: Cryptographers, Unix Pioneers Lead the Way
Memory Encryption Breakthrough Claimed By NC State Researchers
The Rising Use of SSL Raises New Risks
Improve
Simplify
Consolidate
Secure
Save
your Network Infrastructure
Virtualize
vmware PARTNER ENTERPRISE SOLUTION PROVIDER
Call Us Today!
1-877-726-8749
1-877-PANURGY
PANURGY Integrated Business Solutions
White Papers »

Android passwords are stored in plain text - Google says everyone is doing it | TechEye - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Android passwords are stored in pl...

http://www.techeye.net/mobile/android-passwords-are-stored-in-plain-text

"TechEye: We know how to liquidise soups" - Allan Rutherford

Search this site

TechEYE.net

RSS Twitter Facebook Email

HOME | BUSINESS | HARDWARE | SOFTWARE | CHIPS | MOBILE | INTERNET | SCIENCE | SECURITY | REVIEWS | EYETHINK

Monday 25 Jul 2011

Android passwords are stored in plain text

Google says everyone is doing it

25 Jul 2011 08:58 | by Edward Berridge | Filed in Mobile Google

0 Comments

+1 Tweet reddit this! Like Share

Security on the Android operating system has been dismissed as a joke after a hacker found that it was listing user passwords in plain text.

Hacker News has reported that Android user passwords are stored in plain text on the phone's harddrive, if you know where to look.

An Android user noticed that a password for email accounts is stored into the SQLite DB which in turn stores it on the phone's file system in plain text. He suggested that this was daft and Google should be encrypting or at least transforming the password.

Android Support's Andy Stadler wrote that the problem was caused by the fact that Android Email supports POP3, IMAP, SMTP, and Exchange ActiveSync. All of these require that the software present the password to the server on every connection.

Android has to retain the password for as long as users need to use the account. Newer protocols don't have this problem. They allow the client to use the password one time to generate a token, save the token, and discard the password, he said.

But he pointed out that obscuring your password or encrypting it with a key stored elsewhere will not make password or data more secure. It will just be somewhere else.

Stadler implied that other email clients had the same problem. Some pretended they were more secure because they were using obscuring or encryption. However it did not mean that the password was more secure.

If a user can boot up the device and it will begin receiving email on your configured accounts, then the passwords are not truly secure, he said. All the client has done is either obfuscate, or encrypte them with another key stored somewhere else.

Popular mobile stories


India's DoT sits on unallocated 2G spectrum


Ye Booke of WebOS


ZTE will succeed


Mediatek will not get Nokia 2G chip


Emerging markets will buy smartphones

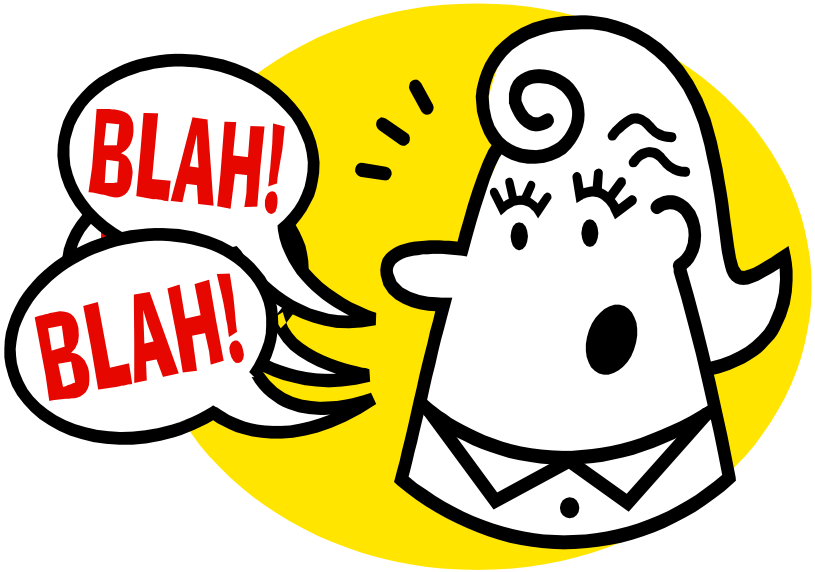
EyeThink - join the debate

- Is tablet computing a costly fad?

Solutions

- Encrypt where practical
  - SSL, sure
  - IPSEC where it works, sure
  - Databases, maybe but what about audit based solutions
- Find other solutions where not so practical
  - Database security gateways
  - Self encrypting drives
- Understand the limitations of user friendly mobile devices
  - Onboard keys make for easy targets
- Virtualize data on mobile devices to keep it secure in the datacenter

Discussion



Thank You!

Daniel Srebnick

CISO

NYC Department of Information Technology and Telecommunications

THE SECURITY STANDARD™

Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by

CSO