Mitigating Server Breaches with Secure Computation

Yehuda Lindell
Bar-Ilan University and Dyadic Security
The Problem

+ Network and server breaches have become ubiquitous
+ Financially-motivated and state-sponsored cyber attacks pose an ongoing threat to commercial, government and defense organizations
+ The cost of server breaches is in the billions every year
  + *The average total cost of a single data breach in Q4 2011 was $6,027,405 and in Q1 2012 was $8,378,970 (a 39% increase)
+ **The number of breaches rose 48% from 2011 to 2012

*Navigant Consulting, June 2012 report (considered major publicly disclosed data breaches only)  
**Javelin Strategy and Research Report, 2013
The Cost of Server Breach

Healthcare Industry Loses $7 Billion Due to HIPAA Data Breaches

Posted on January 7, 2013 by Thu Pham

A recent study released in December 2012 by the Ponemon Institute, the Third Annual Benchmark Study on Patient Privacy & Data Security, reveals an inside look at the growing data breaches in the healthcare industry. Recurring data breaches are increasing among respondents, with 45 percent reporting more than five incidents in the last two years (an increase from 29 percent in 2010). Ninety-four percent of all respondents had at least one data breach in the past two years. The figure of a $7 billion loss to the healthcare industry overall was calculated by the Ponemon Institute by multiplying $1,195,135 x 5,754 (average economic impact for a healthcare organization over a one-year period x the total number of registered US hospitals per the AHA).
Adobe Hacked, Data for Millions of Customers Stolen

Adobe said Thursday that it recently suffered a massive security breach which compromised the IDs, passwords, and credit card information of nearly three million customers.

"Our investigation currently indicates that the attackers accessed Adobe customer IDs and encrypted passwords on our systems. We also believe the attackers removed from our systems certain information relating to 2.9 million Adobe customers, including customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders,"

Brad Arkin, Adobe's chief security officer, wrote in a security alert.

Arkin said the unknown attackers made off with encrypted credit and debit card numbers, "[a]t this time, we do not believe the attackers removed decrypted credit or debit card numbers from our systems."

The software firm also said "source code for numerous Adobe products" was stolen in a separate intrusion that could be related to the theft of customer information.

Adobe said it had alerted federal law enforcement authorities of the attacks as well as informing its banking and payment processing partners. The company said it would reset "relevant customer passwords" as a precaution, with affected customers due to receive email notifications instructing them to change their Adobe passwords. Arkin also recommended that any affected customers who use the same password for other sites as they do for Adobe change their login details for those other sites as well.

The company said customers whose credit or debit card information was compromised would be offered a year's membership in a credit monitoring service courtesy of Adobe.
Forty Million Target Customers Affected By Data Breach

Do you shop at Target TGT -0.24%? If so, you may want to pay extra attention to your credit and debit card bills during the next few months. According to Krebs on Security, Target is investigating a data breach that has potentially affected millions of customer credit and debit cards. These sources say the breach appears to have begun around Black Friday 2013 and involves the theft of data stored on the magnetic strip of cards used at stores. The breach apparently extends to nearly all Target locations across the U.S.

UPDATE 9AM ET, Dec. 19: Target confirmed today that the data breach has affected 40 million customers. According to its statement, “Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and
Modern computer systems ensure that there are no single points of failure

- RAID storage, server replication, database clustering, network redundancy

Cryptographic keys are a security single point of failure in most organizations

- In the case of server breach, keys are stolen
- Protecting the perimeter is not enough
- Intrusion detection is too late
Removing SPOFs in Security

- The conventional wisdom: you need to hold the secret key in order to compute a cryptographic function.

- The cryptographic reality: it is possible to compute without any single server knowing the secret key.
  - The cryptographic key (encryption/decryption, signing, authentication credential) is shared between two or more servers.
  - Both servers need to be breached, or nothing is learned.

- Consider an ideal model with a function that computes encryption/decryption/signing/authentication on two random shares of the secret key/credential.
Encryption is Vulnerable when the Key can be Stolen

If the database server is compromised, the attacker can steal the encrypted database with the key, and then decrypt...
Using Secure Computation

Decryption takes place without ever bringing the key together! The key is never in any single place to be stolen.
Long-Term Protection

- What happens when the second server is hacked?
  - We use a key refreshing technique at frequent intervals
  - The attacker must reside on both servers in a single time interval in order to learn any secret

- This uses a secure coin tossing protocol
  - The secret key is $k$
    - Party 1 has a random string $k_1$
    - Party 2 has a random string $k_2$
    - $k_1 \oplus k_2 = k$
  - The parties run a coin tossing protocol to obtain a random $r$
    - Party 1 sets $k_1' = k_1 \oplus r$
    - Party 2 sets $k_2' = k_2 \oplus r$
Server Configuration

- Different admins for each server
  - Lower insider threat and targeted credential theft

- Different operating systems
  - Reduce risk from malware and zero-days

- Different locations
  - Make physical theft harder
Applications

+ Database encryption
+ Authentication
  + Kerberos credentials (used in every Windows system)
  + One-time password keys
  + Regular passwords (web authentication)
+ System-to-system authentication
A Virtual HSM

- **HSM: Hardware Secure Module**
  - Strong protection of cryptographic keys
  - Keys are never exposed

- **HSMs are used where mandated but rarely otherwise**
  - They are very expensive to purchase and hard to deploy
  - The cost of integration is high, as is yearly maintenance

- With secure computation, can achieve the effect of an HSM in software
Comparison to HSMs

+ HSMs provide strong security for keys

+ But:
  + HSMs are not perfect (padding oracle attacks, timing attacks, API attacks, and more)
  + HSMs are not flexible: hard to fix, slow to update, hard to tailor for specific needs
  + HSMs are very expensive to buy and maintain
    + Multiple HSMs are needed for reliability
    + Repairs require a physical visit
  + HSMs are hard to scale in the enterprise and even harder to use in the cloud
Speed – Security for Malicious

- In an offline/online mode, we can do AES in under 20ms
  - By recent improvements, we believe that we can get to approximately 5ms

- We can achieve comparable times for HMAC-SHA1, and so on

- By the generality of secure computation, we can support any cryptographic function
  - Asymmetric key, including DSA/ECDSA
  - Symmetric key
  - Authentication protocols
Password Theft

Adobe Hacked, Data for Millions of Customers Stolen
By Damon Poeter | October 3, 2013 06:29pm EST | Comments

Yahoo's password leak: What you need to know (FAQ)

Yahoo is the latest online service to confirm the disclosure of passwords belonging to throngs of its users. Here's what we know — and, more important, what you need to do to protect yourself.

LinkedIn Password Hack: Check To See If Yours Was One Of The 6.5 Million Leaked
The Huffington Post | By Sara Gates | 7/2/2012 11:25 am Updated: 06/07/2012 12:20 pm

8.24 million Gamigo passwords leaked after hack
Summary: Gamigo was hacked back in February but only in July are we seeing the results. More than 8.24 million e-mail addresses and passwords have been leaked after what looks like the biggest security breach of the year (so far).
By Emil Protalinski for Zero Day | July 23, 2012 -- 15:27 GMT (08:27 PDT)

Twitter breach leaks emails, passwords of 250,000 users
Links to media site attacks suspected
By Neil McAllister, 2nd February 2013

Hackers Leak Thousands of Passwords From Large Private BitTorrent Tracker
enigmex | September 19, 2012
In an unprecedented data breach, tens of thousands of usernames and passwords from large private BitTorrent tracker RevTT have been leaked onto the Internet. The attackers, who call themselves Afghanistan Hackers, leaked the user/pass combinations via The Pirate Bay. The initial response
Massive Password-Theft Damage

“More than 90 percent of user-generated passwords, even those considered strong by IT departments, will be vulnerable to hacking. Inadequate password protection may result in billions of dollars of losses, declining confidence in Internet transactions and significant damage to the reputations of the companies compromised by attacks.”

Deloitte Technology, Media and Telecommunications Predictions 2013

+ Web servers are particularly vulnerable
  + They are exposed to the outside world
  + They have access to internal confidential data
Existing Architecture

User

Web server

Database

• Compute $h' = \text{HASH}(\text{pwd}, \text{salt})$
• If $h' == h$, accept login

If the web server is compromised, the attacker can retrieve the entire password file and break it offline.
New Architecture

Even if the web server is compromised, the attacker can do nothing but an online password guessing attack!

If $c$ is an encryption of $\text{HASH}(\text{pwd}, \text{salt})$, then output 1

$\text{usr}, \text{pwd}$

User

$\text{usr}$

Web server

$\text{usr}, \text{salt}, c$

Database
Value of Solution

- Complete password protection in presence of web server compromise
  - The key is never reconstructed and in one place (not even in RAM)

- Easy deployment
  - Almost no change to existing architecture
  - Additional server can be on any machine, in the enterprise and in the cloud
  - Can run side-by-side plain password solution initially for testing purposes

- We have an implementation running on Amazon
  - Security for malicious adversaries
  - Takes approximately 20 milliseconds (not optimized)
Web Server Protection 2: User Data

- Web servers access sensitive user data
  - Social security numbers (source of significant financial loss)
  - Credit card numbers
  - Client lists
- User data is encrypted (using a strong cryptographic key) and stored in the database
  - The decryption key is split amongst two or more servers
  - Secure computation is used to decrypt
- The decryption can be coupled to the authentication
  - A secure computation protocol takes place between the servers that decrypts only when the password is correct
A New Angle – One Part of the Decryption Key Outside of the US

Feds tell Web firms to turn over user account passwords

Secret demands mark escalation in Internet surveillance by the federal government through gaining access to user passwords, which are typically stored in encrypted form.

The U.S. government has demanded that major Internet companies divulge users' stored passwords, according to two industry sources familiar with these orders, which represent an escalation in surveillance techniques that has not previously been disclosed.

If the government is able to determine a person's password, which is typically stored in encrypted form, the credential could be used to log in to an account to peruse confidential correspondence or even impersonate the user. Obtaining it also would aid in deciphering encrypted devices in situations where passwords are reused.

"I've certainly seen them ask for passwords," said one Internet industry source who spoke on condition of anonymity. "We push back."

A second person who has worked at a large Silicon Valley company confirmed that it received legal requests from the federal government for stored passwords. Companies "really heavily scrutinize" these requests, the person said. "There's a lot of 'over my dead body.'"

Some of the government orders demand not only a user's password but also the encryption algorithm and the so-called salt, according to a person familiar with the requests. A salt is a random string of letters or numbers used to make it more difficult to reverse the encryption process and determine the original password. Other orders demand the secret question codes often associated with user accounts.
Server breaches cause massive damage every year, and the number of breaches is growing rapidly.

Secure computation can be used to mitigate the threat of server breach.

We are currently carrying out customer validation on directions and would be very happy to speak to anyone who is interested.

Please approach me or Nigel Smart.