The Threat

Cloud storage vendor failed/compromised

May, June 2011 – Microsoft Office 365 and BPOS outages plague customers

September 2011 – Google’s cloud goes down – affects 14% of users

April 2011 – Amazon EC2 cloud goes down for 3 days – lose customer data

* Cloud interruptions have been a very public grievance in the recent years. When a cloud goes down, customer data can forever be lost. This is one reason that companies are rightfully weary of relying on the cloud.

Attackers laterally move into the cloud from a compromised server

* Pivoting attacks are the favorite of hackers. Sony, a leader in technology. HB Gary, a leader in cyber security. Both of these companies were ruthlessly and publicly hacked by attackers in the past few years. The commonality of both hacks was the use of pivoting. Pivoting is when attackers break into a sister site, or a subsidiary company that is less protected, and use the information that they gather to leverage a break in the higher profile target.

MITM attack

* Man in the middle attacks are a commonplace technique of carders and data thieves alike. By intercepting traffic in the middle of a transmission, they are able to recreate the original data being sent.

Encryption Key disclosure

* It may surprise you how many companies have outward facing lists of passwords, and easily breakable encryption keys. Encryption key disclosure results in the ability of attackers to recreate stolen data that has been encrypted.

Unauthorized Access due to lack of Role Based Access Controls

* Attacks from within are another common attack in todays society. Malicous system administrators are given access to data beyond their need, and as a result, sensitive customer information can be disclosed to competitors and attackers.

Goals

Allow companies to compensate for data loss in the cloud

* Ozel leverages established mathematics to pad their shredded data – allowing cloud providers to lose parts of the whole data while still being able to recover all the original data

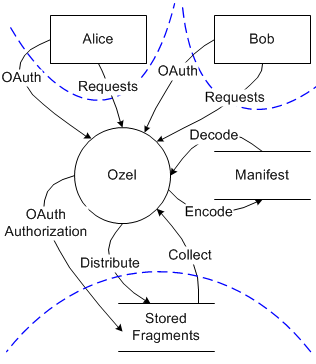
Protect companies from data disclosure in the cloud

* Shared hosting and cloud storage is risky because if an attacker breaks into one system, it becomes feasible for them to laterally navigate through the cloud and compromise more systems. Ozel protects against this by encrypting data with the strongest government grade encryption. Even in the event of an information leak your data is safe with Ozel.

Give companies a way to restrict access to authorized users without requiring trust of intermediaries

* The use of role based access controls will give companies the ability to let system administrators manage sensitive data, while having no personal access to said data.

STRIDE threat model



Potential

Our target audience is independent professionals and small firms that are required by law to store personal identifiable data. Laws like HIPA require organizations handling health records to comply to strict data privacy standards to ensure that customer data stay safe. Ozel will assist in HIPA compliance and data security for the 3 million lawyers, doctors and accountants in the US alone.

Professionals like this are typically not in the deep know of computer security, so they contract out their computer work to small businesses that deal with web hosting and integrated systems. This is our initial target audience. By appealing to the people who influence our costumers, we will allow for a faster spread of information regarding out product.

Users

Financial Projection