CS261: Computer Security
Prof. David Wagner
November 29, 2007
Scribe: Vahab Pournaghshband

E-Voting continued:

Problem: How can I trust electronic results from these machines?

Solution: Sample auditing: At the end of each voting session, the machine prints a record and the record is to be kept in a ballet for possible further manual check.

Precinct	Hilary	Giuliani
1	5	17
2	6	20
3	70	10

Take a sample from precincts (for instance, precinct 2 and 3) and verify the results by checking the electronic result and the manual count. If we check an enough number of them (let's say 1%) we are confident to a certain degree (for instance 95%) that the result is correct. However, keep this fact in mind that it is only an approximate verification.

A great advantage to sample auditing is that it is an end-to-end solution check; that is, it assumes the machines and computers totally misbehave, so it checks the result independently.

Therac-25 Incident:

Therac-25 was a radiation therapy machine produced by Atomic Energy of Canada Limited (AECL) and CGR MeV of France after the Therac-32 unit. It was involved with a number of accidents, in which patients were given massive overdoses of radiation, which were in some cases on the order of tens more. A few patients died of the overdoses.

The root cause of problem was that the new design did not have the hardware interlocks which were initially used in Therac-32 to prevent the electron-beam from operating in its high-energy mode without the target in place. A software bug allowed radiation overdose while the lack of hardware interlocks didn't prevent the machine to expose the patient with massive radiation.

Privacy:

1. Incentive to profile

A. price discrimination

Profiling customers is an incentive for the sellers to implement price discrimination. If I am a seller, I want to know as much information as possible about what you are interested in buying and how much you are willing to pay for it.

B. Advertising in market

Some companies like Google, Yahoo, and Facebook have revenues from advertising and their business models are based upon profiling. To make their advertising more effective, these companies have strong incentives to profile their users on what they are interested in and likely to buy. They might not go after names but certainly they are interested in your income, demographic information, age etc.

2. Consumers won't pay for privacy

Surveys from consumers about privacy have shown that they are very concerned about their privacy. However, when they were asked to tell how much they are willing to pay for their privacy, very few responded positively.

Because of this, for companies, privacy is more of a cost issue and not a profit issue. Companies can lose a lot if they fail to preserve privacy of their customers, but will not be rewarded otherwise. For instance, an oil company will lose remarkably if it is responsible of an oil spil. On the other hand, it is not effective for an oil company to advertise that it has not been responsible for any oil spil in ten years.

A few years ago, a start-up company called zero-knowledge released a privacy protection product called “freedom”. It claimed to protect privacy of Internet users by various ways such as anonymizing its customers' internet addresses. They sold approximately 10,000 units and as a result of such little success, they were forced to go out of business. On the other hand, some other companies like DigiCash and Paypal were successful in providing privacy protection solutions. Zero-knowledge is a good example of the fact that great technology doesn't necessarily lead to commercial success.

3. Driver's license:

The magstripe on the driver's license card contains information shown on the card and possibly more. The real incentive for the magstripe on the driver license has been to help law enforcement personnel with their duties.

Problem: Other companies (e.g. bars) also can read the information stored on the magstripe for various purposes

Solutions:
- *Online reader:* In this case, the only information stored on the magstripe could be an index that is sent to the master database to retrieve the requested information.

- *Offline reader:* In this case, the information could be encrypted by a private key only known to police officers (but this can lead to key management issues).

In US there is little law on privacy but there is always an exception: Video rental merchants are not permitted to reveal any information on what their customers have rented (Video Privacy Protection Act). The historical fact about this is the Judge Robert Bork's video rental history that was leaked to the public during his nomination which had serious consequences.

4. E-commerce:

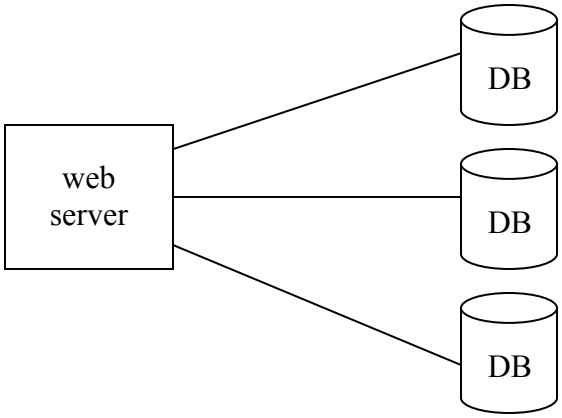
It is absolutely a killer for e-commerce businesses to lose sensitive information of their customers. A shinning example is TJ Maxx losing the database of its customers, including their name, credit card information, address, and phone numbers. The server was hacked because of an insecure wireless network used, and as a result there was a lawsuit against the company. TJ Maxx lost records of about 10 million customers and suffered a significant financial loss of more than $100 millions for this incident.

Problem: How to protect customers' sensitive information?
Solution? Simply not maintaining such information like credit card numbers by deleting them when the transaction is complete.

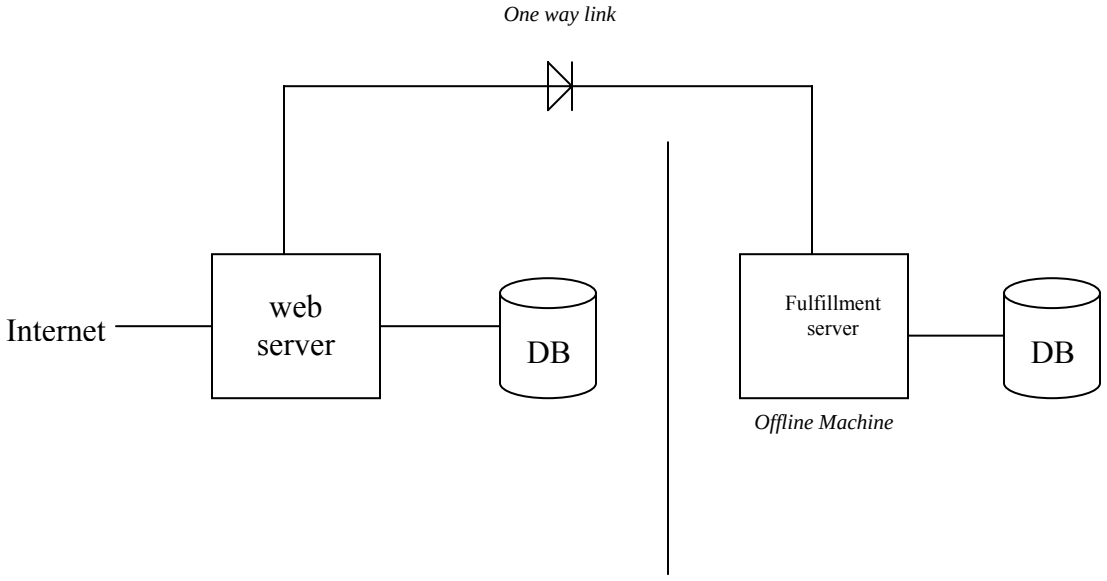
Challenge: The company may want to keep these information for various reasons. For instance, if the company wants to offer discounts based on a particular customer's interest and spending, it might need such information. They normally use the credit numbers as an index to their database.

Solution? One-way hashing of credit card numbers

Solution? Multiple database
Not very plausible. All databases are compromised by attacking only the web server

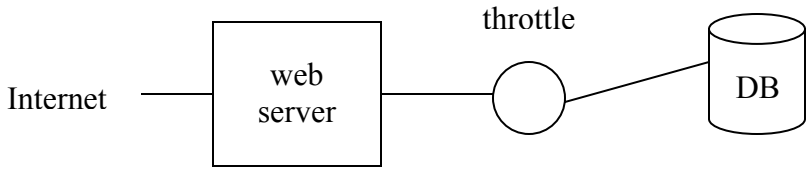


Solution: Separate out the database containing sensitive data from non-sensitive data, and allow only one way access to this database. The server is allowed to only send queries like charge the user ID by this amount with whatever credit card number you have on the database.



Problem: How to update information on the fulfillment server?
Solution: Having a trusted employee store the updates on a CD and then implement them to the database or using a trusted software program to do that.

Alternative solution: get use of a throttle between the database and the web server to limit the number of sensitive queries per time unit. For example, allow only 1000 sensitive queries per day, and depending on the database it might take over a month to pull off all the sensitive information, and hopefully it will be noticed by then.



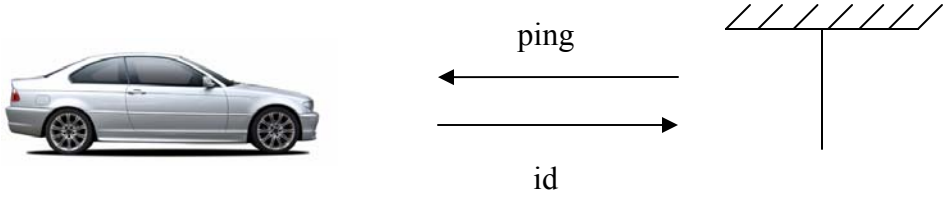
What do banks require from merchants?

Banks require the merchants to keep the information of transactions for several months for various reasons (e.g. disputed transactions). Thus, they are not allowed to just delete the transaction information once it is complete. To do this, banks require the merchants to protect credit card numbers using the PCI compliance.

One seemingly plausible solution is to keep only a transaction ID or code to eliminate the need for keeping the full transaction information including the credit card number.

5. FastTrack:

How the system works?
A radio antenna at the toll that pings (normally with a beeping sound as a communication indicator) and a transponder installed on the car that replies to it instantly with its ID.



The protocol is simplistic and no cryptography is involved. When the transmitter pings it, it can set the "beep?" to NO. This way the driver wouldn't notice that it is being pinged and replies accordingly. The risk is for a third party to get access to the database that kept the FastTrack information. Aside from the Big Brother issue of government keeping track of where people go, there was actually a divorce lawsuit that the lawyer used this information to prove that the husband had another affair.

There are, in fact, other occasions that FastTrack transponder is forced to reply unnoticeably by setting the beeping sound to NO. One is for the traffic control purposes and realizing how congested the traffic is; but it is not used to catch violation like speeding even though it is capable of catching it. So, because of this overly simplistic model that the FastTrack system has adopted, the system is vulnerable to attacks by third parties.

Question: So how can we assure that *only* the Caltrans can effectively communicate with the transponders?

Solution? A solution would be for Caltrans to have a public key *pk* and have the transponder to reply the encrypted ID: $(ID)_{pk}$ But this is also vulnerable to replay attack where the attacker can transmit $(ID)_{pk}$ and fake to be another person.

Solution: Encrypt a timestamp along with the ID: $(ID, timestamp)_{pk}$

6. E-passports:

US have recently adopted e-passports that contain an RFID tag that carry digital information such as a digital photo and possibly thumbprint in near future.

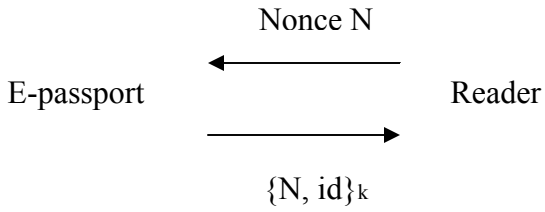
A major key management issue involved here is that passport control officer might need to know the private keys and whether US government wants to share its private keys to other countries' governments.

Problem: A third party pings the e-passport which can make us vulnerable to:

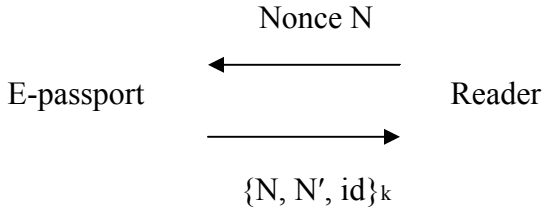
1. Stealing identity
2. Figuring out I am an American (by pinging it by a fake readers), which might be bad for various reasons!

Solution? Bar code might be a better solution since someone in 5 feet away can not read it or communicate with it.
Solution? Maybe implement something that it is active to respond ONLY when the passport is open.

Solution? The scheme below:



For this scheme to work, you don't want the response to be a deterministic function of the nonce, N, sent by the reader and the ID, so the E-passport must produce a new randomness N' and encrypt it along the N and the id.



7. Libraries:

Some libraries found RFID beneficial and have adopted this. Main advantage for libraries is self-check-out since they can cut the cost by reducing the staff. The RFID tag keeps information of the book and the circulation information

Problem: It puts the privacy of its patrons at risk since third parties might be able to read the RFID tags and infer, for instance, what books a particular patron has checked out.

Solution? Store a random 64-bit string as an index to the library database that matches with the desired information.

Problem: Tracking issues (the book I carry becomes a tracking device)

Characteristics of the solution: the scheme must let only the library to read the RFID tag and not any third party. In fact, it happens to be a cryptographic solution to the tracking problem which will be discussed in the next lecture.