Project 5

Lottery Security Design Review

Reviewers: Bernard Dickens III, Yan Liu, Jaime Arana-Rochel
Reviewing: Hao Tong, Haopeng Liu, Yuxi Chen

Overview of Merits

Criteria 1 (Ticket Forgery/Theft)

Having each terminal embed a digital signature on the QR code on each ticket using the terminal's private RSA key is a good way to ensure authenticity of purchase. This is further supplemented by the fact that the terminal's keys are frequently updated, which can mitigate an attacker who happens to obtain a terminal's private key to forge digital signatures. This design choice does present some issues which are explained later in the review.

Ticket theft is defended against by having winners present identification documents such as a driver's license and proof of residence at the time of claiming a prize. This is a simple and practical way to prevent thieves from cashing in a stolen ticket. The addition of a website where buyers can validate their tickets is also useful in a practical, real world setting.

Criteria 2 (Dishonest Storekeepers)

The design protects against dishonest storekeepers by fundamentally eliminating the need for store owners to even report ticket sales. The terminals are synchronized with the lottery office servers to provide real time data on ticket sales. Dishonest storekeepers would then have a hard time in actually lying about tickets sales and covering their tracks.

This design also addresses the situation where the store owner or attacker steals the terminal itself. In such a situation, this design protects against fraudulent printing of tickets by having the servers blacklist that specific terminal due to being disconnected from the wi-fi connection for a certain time during the theft. Furthermore, the design makes the case that store owners are incentivized to report stolen terminals because the state will collect the money from purported ticket sales from the store either way.

Criteria 3 (Cost)

Based on their choices, this design really does use the bare minimum of equipment to operate the lottery. The only other additions besides the terminals themselves are the wireless link and the USB sticks which store the logs. This effectively brings the cost down to $610,000 per week, which is not much more than the cost to maintain the terminals themselves.

Potential Adversaries

- Dishonest or malicious courier service
- Network attacker
    - (D)DoS
    - DNS poisoning and/or redirection
    - Man-in-the-Middle attacks DH key exchange
    - Keypair leaks anywhere in the protocol
- Dishonest clerk
    - May attempt to undercut the government's profits by any means necessary

- Lockpick/Thief
    - Can steal and/or alter logs stored on externally-accessible USB
    - Can steal an entire terminal
- Dishonest customer
    - May attempt to forge, copy, or otherwise manipulate tickets
- Corrupt government officials/database administrator **(outside of threat model)**
    - May manipulate values directly in the government database

Potential Security Flaws

Bogus Winning Ticket Defense

From the specification alone, it is not apparent that replays of winning ticket claims will not be received as valid from the server. Dishonest customers may abuse this Upon discussion with the team, however, it was verified that the database that stores the ticket data also carries a flag to ward against replay forgeries from winning ticket holders (i.e. photocopying the winning ticket).

Underreporting Tickets/Dishonest Clerk Defense/Dishonest Courier

Due to the potential for terminal log disagreement (described below), dishonest store clerks, working in tandem with thieves and/or lockpicks or even dishonest couriers, can modify the log data stored on the USB freely. It is not apparent from the given specification that the terminal encrypts the USB logs. If the terminal logs have been modified in the attacker's favor, there is no stated recourse for the integrity of the system or for the state that hosts the lottery.

Active and Passive Attackers on the Network

Active network attacks such as DNS cache poisoning and DoS/MitM are not properly accounted for by this specification. The team's proposed solution to DNS cache poisoning is to skip using DNS altogether (directly to IP), which would theoretically open them up to even worse DoS vulnerabilities and remove the opportunity to leverage DNS-based load balancing.

(Distributed) Denial of Service and Man-in-the-Middle

The specification does not mention any sort of mitigating factors or protections against service denial attacks from active network attackers. Further, using the DH key exchange, while establishing a secure channel, does not ensure terminal non-repudiation. There is no guarantee that the client the central server is talking to is actually the client (terminal) it thinks it is talking to, however confidential the conversation may be. From what we can gather from the specification as given, the protections against MitM may not prove as effective as necessary to prevent catastrophic loss on part of the state. Upon discussion with the team, however, it was said that specific attacks such as DoS are outside of the threat model they used to asses this problem.

Terminal Log Disagreement

The terminal keeps a USB stick with that week's logs on them. The central server also keeps a log of tickets sold and other similar data. What is the protocol for handling a case where

these two logs are not in agreement over the information about a ticket sale? No such protocol was mentioned in this specification.

RSA Key-Pairs

The rotating RSA key-pair algorithm as described by the specification is, due to the potential MitM vulnerability, completely broken. If the public key of the terminal is sent to the server, protected by a DH exchange without any protection against MitM, the adversary can record or even alter this key in transit and potentially undermine the secrecy of messages already sent and messages that will be sent in the future, including future requests to rotate the key-pair.

Practical Considerations

Suppose someone manages to buy the winning ticket for the week legitimately. However, right before the end of that week on Saturday, a thief steals the terminal that printed the winning ticket. Under the current design, the terminal is blacklisted on the lottery servers and all tickets sold from that terminal are deemed invalid; the winner can't claim his prize! This seems like an unjust measure on the part of the lottery. Winners would be justified in their anger at the state lottery for this theft protocol.

Furthermore, in the United States, lottery tickets are considered to be "bearer instruments". This means that, technically, anyone who is in the possession of the ticket has legal rights as its owner, regardless of who purchased it. This however only applies if the purchaser of the ticket has not personally signed their signature in pen on the ticket. So in the scenario that someone has stolen a winning ticket (or found a lost one), and the ticket has not been signed in pen, that person can still cash in the prize. Given that the security is designed to only allow purchasers of the ticket to redeem a prize, this poses an issue.

Strict Improvements

In the event that a terminal is stolen, instead of invalidating all ticket sales for that terminal, the state could instead invalidate ticket sales starting from the point in time when the terminal was stolen. This ensures that winners can still claim their prize and improves overall practicality.

If the state strictly wants only purchasers to redeem a winning ticket, simply have a reminder on the terminal screen or ticket itself that tells players to sign the ticket.

It is unclear why there absolutely needs to be a USB stick in the terminal that logs data, when that data is automatically sent to the lottery servers anyway. Given the proposed design, one could possibly eliminate the local USB sticks altogether, reducing the cost of the design by $10,000 each week.

It is unclear that why the strategy letting merchant to report the status of the terminal of its own store is enough for preventing dishonest store owners. Justifications to defending

multiple store owners gathering together and perform attack on current design is also necessary.

Reviewer Comments

In general, the design is simple and be able to prevent three important situation happening. And the balance between the security of the Lottery system and its building cost has been dealt very well, the cost to build the Lottery system is almost the lowest as possible.

In this design, the proposal of refreshing (public, private) key is especially aggressive, it might increase the difficulty for potential attacker who is going to steal the information from the communication between terminals and others, and use the information stolen to forge tickets/records. But by doing this also raise the security issue that the potential attacker could have bigger chance to perform a man-in-the-middle attack against the key refreshments.

Moreover, we could still see the design might suffer from potential attacks, which has been listed in previous section.

Advices:

1. It might be better to do a trade-off among different security issues. For example, the proposal of (public, private) key refreshments looks like increasing communication security level, but exposes to another type of attack.
2. General justification to both criteria are good, it would be better to list more potential security issues and the defense of those attacks. It would help the proposal to look more compact and reasonable.

To sum up, this Lottery security design is good in many sense, but also has lots of space to improve.