

I. Introduction

1. Casino and Network Background
2. Security Threats
3. Non-Cryptographic Defenses
4. Cryptographic Defense
5. Conclusion

II. Casino and Network Background

Introduction to a casino slot floor (Network graphic)

Slot Machine	- Primary customer interface
Hopper	- Coin Queue
Bill Acceptor	- Convert Paper Currency to Credits
Meters	- Counters use to track game play
Communications Port	- Used to transfer information to outside world
Accounting Data	
Bonus information	
Bonus commands	- Used to have slot machine pay above and beyond
Multiply Jackpot	
Pay Bonus	
Data Collection Node	- Used to conduct player tracking analysis, bonus eligibility, pay bonuses, etc.
Bank Controller	- Concentrate and route packets from serial net to Ethernet
Concentrator	- Concentrate and route packets

A MODEL FOR CASINO GAMING DEVICE NETWORK SECURITY

Mark Dailey

ECE 575 - Spring 98
Page 2 of 7

06/04/98

- Bonus Servers - Act on game play information and send display update and bonus pay commands
- Configuration Work Station - Used to configure the network
- Host Accounting System - Used to track meters and cash collected. Should balance.

Communications Flow

Meter information from all slot machines to host and bonus servers.

Desire "real time" response on bonuses. (500 ms)

5000 Machines on gaming floor

Game cycle time ~3 Seconds

Event reporting from all slot machines to host and bonus servers.

e.g. Door open, tilt, bonus pays, etc

Relatively small amount of data

Display and progressive updates

Need to keep signage updated.

Internal slot machine progressives need to know current pool

Program Downloads

Very infrequent in a well run casino

III. Security Threats

Attacker Assumptions

- | | |
|--------------------|--|
| Ethernet Access | - The attacker has unfettered access to the Ethernet |
| Protocol knowledge | - The attacker has full knowledge of all protocols used (including proprietary). |

Download Attack

In this attack the attacker substitutes a Trojan horse program for the valid program. In current system files reside on NT workstation. If we can access the NT station we can substitute files and we are done.

If Trojan horse program is discrete, attack can go undetected for many months.

Bonus Pay Attack

In this attack the attacker injects a fake bonus pay command into the network. Either the attacker or an accomplice collects the payment directly from the slot machine.

This attack is limited to the hopper pay limit for the slot machine. Typically \$300-\$500

Player Point Attack

In this attack the attacker injects a fake card out message with a large number of accumulated player points. These points have some monetary value based on a conversion formula.

IV. Non-Cryptographic Defenses

Physical Security

All Ethernet cables are supposed to be physically secured from General access. (Slot machine graphic)

Installed CCTV which can pan and zoom to every slot machine on the floor. Anyone playing on a slot machine floor will be randomly monitored some of the time, and suspicious activity gets much closer scrutiny.

Although we assumed the attacker knew the proprietary communication protocols, in fact these protocols are closely guarded. Most companies consider these to be trade secrets that give them a competitive advantage. The actual pool of potential attackers is relatively small. The point is that once the attack is discovered the investigation will quickly focus on this small pool.

Non-Cryptographic Network Security

All network nodes have their Ethernet Hardware Address recorded by the concentrator. Unknown EHA's are cause for investigation.

Events are reported to the host system. Among these events are bonus pay events. Any bonus pay event, which does not correlate to a bonus win event (as issued by a bonus server), is cause for investigation. Further, any large bonus pay event is thoroughly analyzed before a hand pay is actually issued.

Practical Limit Security

The best value to weight ratio for coins in circulation is the \$1 coin at 8.1g. If we want attack the system without involving any casino personnel (e.g. "Change Girls"), we will have to remove these coins from the premise. \$1000 worth of these coins would weigh almost 18lbs, and take up well over 67 cubic inches of space.

V. Cryptographic Defense

Secure Authentication Server

The proposal I am making for securing the network is based on the existence of a "Secure Authentication Server (SAS)". It should be capable of:

- 1) RSA Encryption / Decryption
- 2) International Data Encryption Standard (IDEA)
- 3) Generating 1024-bit Public-private key pairs
(RSA)
- 4) Generating 128-bit private keys (IDEA)
- 5) Secure Hash Algorithm (SHA)
- 6) Pass Phrase login protection for data entry

Note that the manufacturers public key needs to be entered into the SAS box. This is a potential weak point that must be addressed via physical security.

SAS Public Key Broadcast

On each new power up the SAS will compute a new Public / Private key pair. It will publish the public key by broadcasting it to the floor on regular intervals. It is the job of the concentrator to accept only One pre-programmed EHA for this broadcast on one Ethernet Line, and to send alarms to the host if any other party broadcasts this message.

Secure Key Exchange

The SAS will be responsible for the maintenance of all private keys used by the system. When any system component wakes up, it first generates a private key. That private key is then encrypted under the SAS's public key and shipped out to the SAS. The SAS will then hold at all times every components private key. Any time a component notices the SAS's public key change, it generates a new key and sends the new key to the SAS.

Secure Download

- 1) All software is signed by hashing it using SHA and then encrypting the hash using the manufactures' RSA private key. This is then put on a CDROM for distribution.
- 2) At the casino the CDROM is loaded into SAS and verified by
 - A) Decrypting the Hash using the manufacturers public key.
 - B) Computing the Hash on the software provided
 - C) Comparing the two
- 3) When a downloadable component requires new code it requests the code from the SAS. The SAS sends the code, and a Hash encrypted using the SAS's private key. When the downloaded component gets the code it compares the computed hash against the decrypted hash to validate the code.
- 4) Any time a downloaded component notices the SAS's public key change, it reboots into firmware and requests new code.

Secure Communications

If we notice that the SAS is also a Key Distribution Center (KDC) then we can implement the key distribution described by Stallings (Figure 3.10 pg 90). This sets up a session key for the two parties to use.

Authentication weakness

The Authentication server authenticates software from the manufacturer, but little else. With as many as 5000 machines on the floor this is always problematic. What it does do is insure all critical communications are processed by the SAS.

VI. Conclusion

A conservative estimate of the NRE costs associated with implementing the cryptographic protections outlined in this presentation is ~\$100,000 (6 man months of development plus licensing fees, etc).

Once in place this cryptographic protection makes it difficult to export the product beyond the borders of the US.

To effectively mount an attack on the existing system would almost certainly require a conspiracy. Conspiracies tend to fail due to the simple fact the people keep secrets poorly.

The potential rewards seem relatively small. Any large win will require the attention of the casino staff, and they will want to validate the pay through several independent means. Small pays are possible, but will certainly be discovered within 24 hours through basic accounting procedures, and perhaps sooner through event logs on the host.

I would not recommend cryptographic protection unless forced into it by a regulatory agency.