

ESD264/1.264
Lecture 16 case studies
Fall, 2006

Based on your general experience and on reading chapters 1-4 in Anderson, discuss the two cases below. Short answers: two pages or less per case study. Be prepared to discuss them in class.

A. Public transport system with automated fare collection based on cash/tokens versus smart cards.

- 1. Prepare the same discussion of a public transit system as for the bank in Anderson chapter 1, section 1.1. Distinguish between a cash/token based system and a smartcard-based system; the core, risks, public face, and controls are quite different. Answer questions 1-6 separately for a cash-token system and a smartcard system.**

Core in cash and token systems: Core is the accounting function at bus depots and rail terminals that accepts cash and tokens from fareboxes and turnstiles, counts them, associates them with stations or buses (and staff who collected the cash and tokens).

Core in smart card systems: Core is the bookkeeping function in headquarters that tracks smartcards sold by machine, Web, and all other sales channels.

Internal risks in cash and token systems: Theft by employees, either those collecting the money, the supervisors in the field, or the employees and supervisors at the depots and terminals.

Internal risks in smartcard systems: Accounting irregularities in headquarters staff who account for sales and move funds between accounts; they have the authority to make adjustments, and that can be abused.

- 2. What is the public face of the transit system? If it is electronic or has to do with funds, what are the security risks from your passengers?**

Cash and token: Ticket sellers at each station; bus drivers. Passengers unlikely to be at financial risk in cash transactions; no credit cards, no identity issues.

Smartcard: Ticket machines at stations and sales outlets. Risk of credit card theft or fraud, ability to associate sales with purchaser, and possibility of abusing that information.

- 3. What systems are involved in getting public transport system funds collected from fares to its financial organization and then to banks? What are the risks?**

Cash and token: Mechanical systems to empty turnstiles and fareboxes into containers; transportation of containers to counting facility; systems to identify and resolve differences between machine counts and financial system; match against patterns of revenue to detect skimming. Risks are dishonest employees.

Smartcard: Electronic systems to transfer funds from credit card-based purchases of smart cards to transit agency accounts; same as other merchants. If smart card machines at stations accept cash, the same issues hold as for cash system, but for a much smaller fraction of total revenues.

Employee risk is much smaller. Higher risk is white collar crime, either at transit agency or outside, to manipulate electronic transactions.

4. What physical controls on smart cards or cash are needed?

Smartcards, tokens and cash must be physically secure, kept in safes or secure storage. Smartcards must be kept secure before being issued; cash must be kept secure after being collected; tokens must be kept secure before and after use.

5. What controls are needed with credit cards or debit cards used to purchase smart cards or other fare media?

Usual safeguards at any business: secure database, secure information processing facility; policies against staff seeing credit card numbers or copying them in any way; secure network.

6. What risks does a public transit system Web site pose that sells passes or other fare media?

Same as other businesses: bugs can be used to access back-end systems behind the Web site that, if broken into, can be manipulated to steal credit card numbers, personal information or possibly funds.

B. High tech manufacturing facility

Prepare the same discussion of a high tech manufacturing facility, with substantial process secrets, valuable inventory and high profitability as for the air force base in Anderson chapter 1, section 1.2:

1. What electronic espionage risks are there in a high tech manufacturing facility?

Risks:

Collection of data from discarded PCs, disk drives, memory sticks, CDs, backup tapes, etc.
Interception of emails or unprotected file transfers.
Compromise of employees to provide such materials.
Compromise of database, servers, systems to obtain confidential materials.
More exotic strategies, such as capturing keystrokes (passwords) through electromagnetic attacks

Countermeasures:

Encrypt data on CDs, tapes, etc. Shred disks at end of useful life.
Use virtual private network to authenticate users and encrypt emails.
Use secure file transfer protocols, preferably over virtual private network.
Make security a company priority, with strong support from management.
Keep servers, databases, etc. patched, firewalled, etc.
Manage passwords, users, permissions using good process.

2. What risks are there in Internet traffic to and from the manufacturing facility? What could an eavesdropper learn?

Communications in the clear (unencrypted) can be sniffed. These may include emails, file transfers, Web traffic, etc. Encrypted communications contents cannot be learned, but the origins and destination of messages can be found.

3. Does the plant need to keep information at different levels of security or secrecy? If so, how does it do so?

Probably, but it may be able to keep almost all information at roughly the same, baseline level of security, if it follows the suggestions in item 1 above.

Very highly secure information should be kept on physically separate servers on either no network or a physically separate network. Staff authentication must be managed and monitored; a stand alone server that logs all access should be implemented in a physically secure, publicly visible area (within the secure area). (This is recommended practice for HIPAA..)

4. How does the facility control ingress and egress? Do biometrics have a role?

All such facilities use badges, typically with photo IDs and levels of authority encoded, to allow access only to portions of the facility required. ID validity must expire frequently; there must be a revocation process. Cloning of IDs should be difficult; smart cards with encryption and challenge-response should be used. Biometrics may support the badge process (iris scans, fingerprints in particular) but the chances of false positives are high enough that these cannot be used as the primary methods currently.