Compendium

TDT4237 - Software Security

By Marte Løge

Contents

1 What is Security Engeneering? 2

1.1 Definitions . . . 4
1.1.1 System . . . 4
1.1.2 Subject, Person and Principal . . . 4
1.1.3 Identity . . . 4
1.1.4 Trust and Trustworthy . . . 5
1.1.5 Confidenciality, Privacy and Secrecy . . . 5
1.1.6 Authenticity and Integrity . . . 5

2 Usability and Psychology 7

2.1 Attacks Based on Psychology . . . 8
2.1.1 Pretexting . . . 8
2.1.2 Phising . . . 9
2.2 Insights from Psychology Research . . . 10
2.3 Passwords . . . 15
2.3.1 Difficulties with Remembering the Password . . . 16
2.3.2 User Abilities, Training and Design Errors . . . 16
2.3.3 Social-Engineering Attacks . . . 17
2.4 System Issues . . . 19
2.5 CAPTCHA's . . . 20

3 Protocols 21

3.1 Password Eavesdropping Risks . . . 22
3.2 Simple Authentication . . . 22
3.2.1 Challenge and response . . . 23
3.2.2 Reflection Attacks . . . 23
3.3 Manipulating the Message . . . 23
3.4 Changing the Environment . . . 23
3.5 Chosen Protocol Attacks . . . 23
3.6 Managing Encryption Keys . . . 23
3.6.1 Basic Key Management . . . 23
3.6.2 The Needham-Schroeder Protocol . . . 23
3.6.3 Kerberos . . . 23

3.6.4 Practical Key Management 23
3.7 Getting Formal 23
3.7.1 A Typical Smartcard Banking Protocol 23
3.7.2 The BAN Logic 23

4 Access Control **24**

5 Cryptography **25**

8 Multilevel Security **26**

9 Multilateral Security **27**

Chapter 1

What is Security Engeneering?

A Framework Good security engeneering requires four things to come together:

1. **Policy:** what you're supposed to achieve.
2. **Mechanism:** the chipers, access controls, hardware tamper-resistance and other mechinery that you assemblein order to implement the policy.
3. **Assurance:** the amount of reliance you can place on each particular mechanism.
4. **Incentive:** the motive that people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat your policy.

Why ae poor policy choices made? Quite simply, the incentives on the decision makers favor visible controls over effective ones. The result is what Bruce Schneier calls "security theatre" - measures designed to produce a feeling of security rather than the reality.

The role as a security engineer:

- We need to be able to put risks and threats in content.
- We need to be able to make realistic assessments of what might go wrong.
- We need to give our clients good advice.

Case studies: I will not describe these in detail. It is described in the book (pages 6-11).

- A bank
- A military base
- A hospital
- The Home

1.1 Definitions

1.1.1 System

1. a product or component, such as a cryptographic protocol, a smartcard or the hardware of a PC.
2. a collection of the above plus an operating system, communications and other things that go to make up an organization's infrastructure.
3. the above plus one or more applications (media player, browser, word processor, accounts / payroll package, and so on).
4. any or all of the above plus IT staff.
5. any or all of the above plus internal users and management;
6. any or all of the above plus customers and other external users

1.1.2 Subject, Person and Principal

- **Subject:** By a subject I will mean a physical person (human, ET, ...), in any role including that of an operator, principal or victim.
- **Person:** By a person, I will mean either a physical person or a legal person such as a company or government.
- **Principal:** A principal is an entity that participates in a security system. This entity can be a subject, a person, a role, or a piece of equipment such as a PC, smartcard, or card reader terminal. A principal can also be a communications channel (which might be a port number, or a crypto key, depending on the circumstance). A principal can also be a compound of other principals

1.1.3 Identity

1.1.4 Trust and Trustworthy

The definitions of trust and trustworthy are often confused. The following example illustrates the difference: if an NSA employee is observed in a toilet stall at Baltimore Washington International airport selling key material to a Chinese diplomat, then (assuming his operation was not authorized) we can describe him as 'trusted but not trustworthy'. Hereafter, we'll use the NSA definition that a trusted system or component is one whose failure can break the security policy, while a trustworthy system or component is one that won't fail.

1.1.5 Confidenciality, Privacy and Secrecy

- **Secrecy** is a technical term which refers to the effect of the mechanisms used to limit the number of principals who can access information, such as cryptography or computer access controls.
- **Confidentiality** involves an obligation to protect some other person's or organization's secrets if you know them.
- **Privacy** is the ability and/or right to protect your personal information and extends to the ability and/or right to prevent invasions of personal space.

1.1.6 Authenticity and Integrity

Summary

- Framework
- Security theatre
- The role as a security engineer
- Case studies (bank, military base, hospital, the Home)
- Definition: System
- Definitions: subject, person and principal
- Identity
- Trust and Trustworthy
- Confidenciality, Privacy and Secrecy
- Authenticity and Integrity

Chapter 2

Usability and Psychology

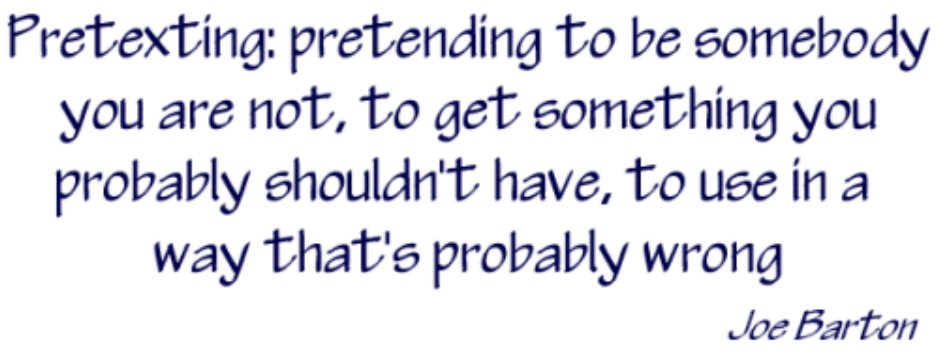
Social engineering

2.1 Attacks Based on Psychology

2.1.1 Pretexting

Pretexting is a form of social engineering in which an individual lies to obtain privileged data. A pretext is a false motive. Pretexting often involves a scam where the liar pretends to need information in order to confirm the identity of the person he is talking to. After establishing trust with the targeted individual, the pretexter might ask a series of questions designed to gather key individual identifiers.

The pretexter's goal is to obtain personal information about you, such as your SSN, your bank or credit card account numbers, mother's maiden name, information contained in your credit report, or the existence and size of your savings and investment portfolios. After getting your answers, the pretexter may call your financial institution pretending to be you or someone with authorized access to your account. The pretexter may, for example, claim that he's forgotten his checkbook and needs information about his account.



2.1.2 Phising

Phishing is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business — a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate — with company logos and content and has a form requesting everything from a home address to an ATM card's PIN.

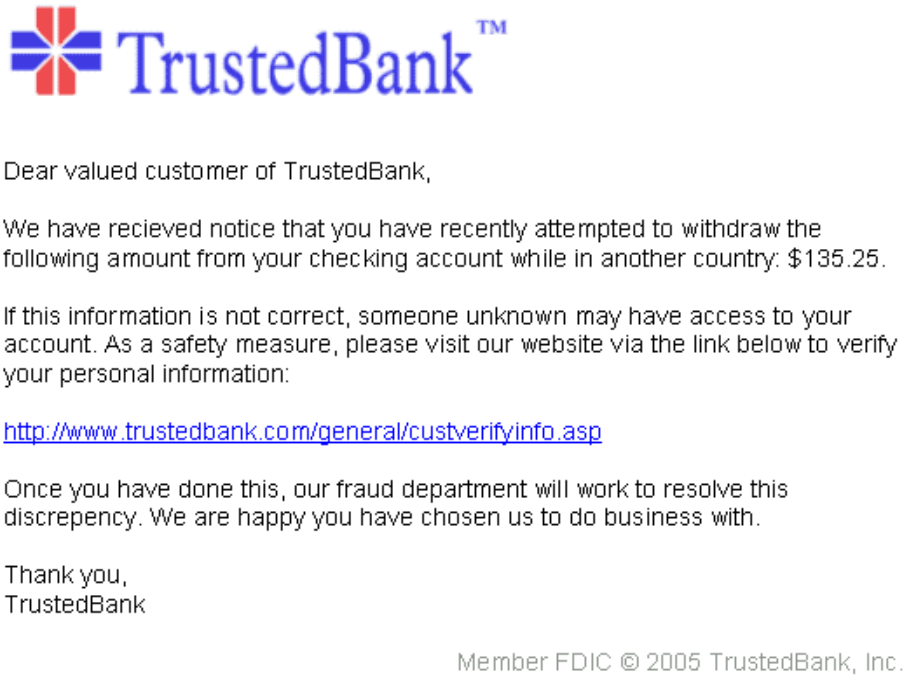


Figure 2.1: Phising attempt

2.2 Insights from Psychology Research

What the Brain does Worse Than the Computer

- Actions performed often become a matter of skill, but this comes with a downside: inattention can cause a practised action to be performed instead of an intended one. We are all familiar with such capture errors; an example is when you intend to go to the supermarket on the way home from work but take the road home by mistake — as that's what you do most days. In computer systems, people are trained to click 'OK' to pop-up boxes as that's often the only way to get the work done; some attacks have used the fact that enough people will do this even when they know they shouldn't.
- Actions that people take by following rules are open to errors when they follow the wrong rule. Various circumstances — such as information overload — can cause people to follow the strongest rule they know, or the most general rule, rather than the best one. Examples of phishermen getting people to follow the wrong rule include using https (because 'it's secure') and starting URLs with the impersonated bank's name, as www.citibank.secureauthentication.com — looking for the name being for many people a stronger rule than parsing its position.
- The third category of mistakes are those made by people for cognitive reasons — they simply don't understand the problem. For example, Microsoft's latest (IE7) anti-phishing toolbar is easily defeated by a picture-in-picture attack.

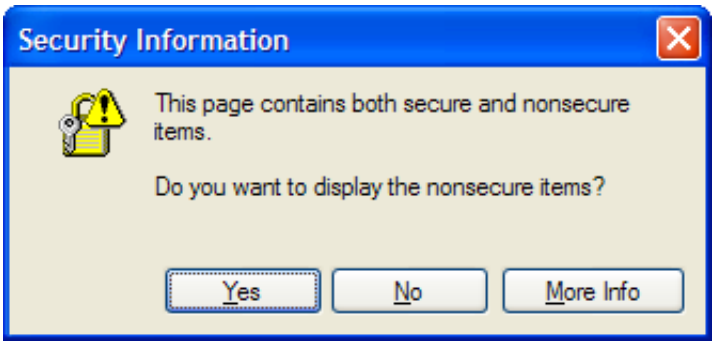


Figure 2.2: Actions performed often become a matter of skill

Preceptual Bias and Behavioural Economics

- How do people make decisions faced with uncertainty?
- By framing an action as a gain rather than as a loss makes people more likely to take it.
- We're also bad at calculating probabilities, and use all sorts of heuristics to help us make decisions: we base inferences on familiar or easily-imagined analogies, and by comparison with recent experiences.
- We also worry too much about unlikely events. We're morelikely to be sceptical about things we've heard than about things we've seen.
- Many frauds work by appealing to our atavistic instincts to trust people more in certain situations or over certain types of decision.
- Many people perceive terrorism to be a much worse threat than food poisoning or road traffic accidents: this is irrational. We overestimate the small risk of dying in a terrorist attack not just because it's small but because of the visual effect of the 9/11 on TV.
- Global warming doesn't violate anyone's moral sensibilities and it's a long-term threat rather than a clear and present danger. Humans are sensitive to rapid changes in the environment rather than slow ones.
- We are less afraid when we're in control, such as when driving a car, as opposed to being a passenger in a car or airplane and we are more afraid of uncertainty, that is, when the magnitude of the risk is unknown.
- We have a tendency to plump for the alternative that's 'good enough' rather than face the cognitive strain of trying to work out the odds perfectly. Another aspect of this is that many people just plump for the standard configuration of a system, as they assume it will be good enough. This is one reason why secure defaults matter.
- The appearance of protection can matter just as much as the reality. For example, many people don't use electronic banking because of a fear of fraud, so banks pay a fortune for the time of branch and call-center staff. It's not enough for the security engineer to stop bad things happening; you also have to reassure people.

Differences Between People - Gender

Most information systems are designed by men, and yet over half their users may be women. Recently people have realised that software can create barriers to females, and this has led to research work on 'gender HCI' — on how software should be designed so that women as well as men can use it effectively. For example, it's known that women navigate differently from men in the real world, using peripheral vision more, and it duly turns out that larger displays reduce gender bias. Other work has focused on female programmers, especially end-user programmers working with tools like spreadsheets. It turns out that women tinker less than males, but more effectively.

Women appear to be more thoughtful, but lower self-esteem and higher risk-aversion leads them to use fewer features. Given that many of the world's spreadsheet users are women, this work has significant implications for product design.

Simon Baron-Cohen, classifies human brains into type S (systematizers) and type E (empathizers). Type S people are better at geometry and some kinds of symbolic reasoning, while type E's are better at language and multiprocessing. Most men are type S, while most women are type E, a relationship that Baron-Cohen believes is due to fetal testosterone levels.

Figure 2.3: Are security mechanisms gender-neutral?

Social Psychology

This discipline attempts to explain how the thoughts, feelings, and behaviour of individuals are influenced by the actual, imagined, or implied presence of others. It has many aspects, from the identity that people derive from belonging to groups, through the self-esteem we get by comparing ourselves with others.

The growth of social-networking systems will lead to peer pressure being used as a tool for deception, just as it is currently used as a tool for marketing fashions.

Experiments has showed that people will obey an authority rather than their conscience. Most people will do downright immoral things if they are told to. A Experiment showed that normal people can behave wickedly even in the absence of orders. In 1971, experimenter Philip Zimbardo set up a 'prison' at Stanford where 24 students were assigned at random to the roles of 12 warders and 12 inmates. The aim of the experiment was to discover whether prison abuses occurred because warders (and possibly prisoners) were self-selecting. However, the students playing the role of warders rapidly became sadistic authoritarians. Abuse of authority, whether real or ostensible, is a major issue for people designing operational security measures. Abuse of authority are the key in in security experiments.

What the Brain Does Better Than the Computer

- We are extremely good at recognising other humans visually, an ability shared by many primates.
- We are good at image recognition generally; a task such as 'pick out all scenes in this movie where a girl rides a horse next to water' is trivial for a human child yet a hard research problem in image processing.
- We're also better thanmachines at understanding speech, particularly in noisy environments, and at identifying speakers.
- These abilities mean that it's possible to devise tests that are easy for humans to pass but hard for machines — the so-called 'CAPTCHA' test.

2.3 Passwords

It's hard to think of a worse authentication mechanism than passwords, given what we know about human memory: people can't remember infrequently-used, frequently-changed, or many similar items; we can't forget on demand; recall is harder than recognition; and non-meaningful words are more difficult.

There are system and policy issues too: as people become principals in more and more electronic systems, the same passwords get used over and over again. Not only may attacks be carried out by outsiders guessing passwords, but by insiders in other systems. People are now asked to choose passwords for a large number of websites that they visit rarely.

Passwords are not, of course, the only way of authenticating users to systems. There are basically three options. The person may retain physical control of the device — as with a remote car door key. The second is that she presents something she knows, such as a password. The third is to use something like a fingerprint or iris pattern

Passwords matter, and managing them is a serious real world problem that mixes issues of psychology with technical issues. There are basically three broad concerns, in ascending order of importance and difficulty:

1. Will the user enter the password correctly with a high enough probability?
2. Will the user remember the password, or will they have to either write it down or choose one that's easy for the attacker to guess?
3. Will the user break the system security by disclosing the password to a third party, whether accidentally, on purpose, or as a result of deception?

2.3.1 Difficulties with Remembering the Password

Our first human-factors issue is that if a password is too long or complex, users might have difficulty entering it correctly.

when customers are expected to memorize passwords, they either choose values which are easy for attackers to guess, or write them down, or both. In fact, the password problem has been neatly summed up as: "Choose a password you can't remember, and don't write it down."

People choose naive passwords. People will use names, single letters, or even just hit carriage return giving an empty string as their password. So some systems started to require minimum password lengths, or even check user entered passwords against a dictionary of bad choices. However, password quality enforcement is harder than you might think.

2.3.2 User Abilities, Training and Design Errors

So what can you realistically expect from users when it comes to choosing and remembering passwords?

After a experiment (page 35-36) on password an humans, the conclusion was:

- For users who follow instructions, passwords based on mnemonic phrases offer the best of both worlds. They are as easy to remember as naively selected passwords, and as hard to guess as random passwords.
- The problem then becomes one of user compliance. A significant number of users (perhaps a third of them) just don't do what they're told.

An important example of how not to do it is to ask for 'your mother's maiden name'. A surprising number of banks, government departments and other organisations authenticate their customers in this way. But there are two rather obvious problems. First, your mother's maiden name is easy for a thief to find out, whether by asking around or using online genealogical databases. Second, asking for a maiden name makes assumptions which don't hold for all cultures, so you can end up accused of discrimination: Icelanders have no surnames, and women from many other countries don't change their names on marriage. Third, there is often no provision for changing 'your mother's maiden name', so if it ever becomes known to a thief your customer would have to close bank accounts (and presumably reopen them elsewhere).

A general error is failing to reset the default password in systems. Often is the default password the same in many different systems!

Banks have put som effort into trying to train their customers to look for certain features in websites: check the english, look for the lock symbol, it is ok to click on images, but not on URL's, hover your mouse over links before clicking on it, etc. This sort of arms race is more likely to benefit the attackers because the customers get very predictable in how they act.

2.3.3 Social-Engineering Attacks

'This is the security department of your bank. We see that your card has been used fraudulently to buy gold coins. I wonder if you can tell me the PIN, so I can get into the computer and cancel it?'. This even works by email!

A huge problem is that many banks and other businesses train their customers to act in unsafe ways. It's not prudent to click on links in emails, so if you want to contact your bank you should type in the URL or use a bookmark — yet bank marketing departments continue to send out emails containing clickable links. Many email clients — including Apple's, Microsoft's, and Google's — make plaintext URLs clickable, and indeed their users may never see a URL that isn't. This makes it harder for banks to do the right thing.

If even the fraud department doesn't understand that banks ought to be able to identify themselves, and that customers should not be trained to give out security information on the phone, what hope is there? When even a bank's security department can't tell spam from phish, how are their customers supposed to?

Trusted Path: A thread in the background of phishing is trusted path, which refers to some means of being sure that you're logging into a genuine machine through a channel that isn't open to eavesdropping. Here the deception is more technical than psychological; rather than inveigling a bank customer into revealing her PIN to you by claiming to be a policeman, you steal her PIN directly by putting a false ATM in a shopping mall. A public terminal would be left running an attack program that looks just like the usual logon screen — asking for a user name and password. When an unsuspecting user does this, it will save the password somewhere in the system, reply 'sorry, wrong password' and then vanish, invoking the genuine password program. The user will assume that he made a typing error first time and think no more of it.

Have you wondered why Windows have the anoying ctrl-alt-del part befor login? It is there to make sure you will be entering genuine password prompt.

Other similar attacks is mofifoed keyboard, keyloggers, and skimmed bank terminals. I sometimes wonder, what if there is a keylogger in a windows system? If you press ctrl-alt-del, you will simply tell the attacker where your password is. The logged txt file will then have something like "ctrl alt del username password".

Two-factor authentication is now widley used. The basic idea is that it consists of something you have and something you know. It will be described in later chapters.

2.4 System Issues

There are also technical issues to do with password entry and storage that will be briefly covered here. Here are some examples of attacks we are trying to defend against:

- Targeted attack on one account (when sending email it is known as spear phishing)
- Attempt to penetrate any account on a system
- Service denial attack

Can you deny service? Banks often have a rule that a terminal and user account are frozen after three bad password attempts; after that, an administrator has to reactivate them. It sure works in a website, but what in the military? Could a system like this benefit the enemy/attacker? Many commercial websites nowadays don't limit guessing becuase of the possibility of such an attack (service denial attack).

Interface design: I usually cover my dialling hand with my body or my other hand when entering a card number or PIN in a public place — but you shouldn't design systems on the assumption that all your customers will do this. Many people are uncomfortable shielding a PIN from others as it's a visible signal of distrust. Because of this, a targeted attack against a person could be easy!

Eavesdropping: The latest modus operandi is for bad people to offer free WiFi access in public places, and harvest the passwords that users enter into websites. This is a kind of attempt to just get all sensitive information about anyone, and not just a specific person.

Timing attack: Many kids find out that a bicycle combination lock can usually be broken in a few minutes by solving each ring in order of looseness. The same idea worked against a number of computer systems. The PDP-10 TENEX operating system checked passwords one character at a time, and stopped as soon as one of them was wrong. This opened up a timing attack: the attacker would repeatedly place a guessed password in memory at a suitable location, have it verified as part of a file access request, and wait to see how long it took to be rejected

Car keys (fail): Have you ever heard a story about someone that could open many cars at a parking lot with their own key? Yes, this is a kind of system fails where the number of bits used for opening a car was to small in order of how many cars that needed an uniqe key.

One-way encryption and plaintext storage: Password storage has also been a problem for some systems. Keeping a plaintext file of passwords can

be dangerous. The best way of storing a password is password + salt + hashing (can also add pepper to it).

Prevent more than x attempts or log all attempts?

There are various problems with this doctrine, of which the worst may be that the attacker's goal is often not to guess some particular user's password but to get access to any account. If a large defense network has a million possible passwords and a million users, and the alarm goes off after three bad password attempts on any account, then the attack is to try one password for every single account. Thus the quantity of real interest is the probability that the password space can be exhausted in the lifetime of the system at the maximum feasible password guess rate.

To prevent more than one password guess every few seconds per user account, or (if you can) by source IP address. You might also keep a count of all the failed logon attempts and analyse them: is there a constant series of guesses that could indicate an attempted intrusion? (And what would you do if you noticed one?).

2.5 CAPTCHA's

Recently people have tried to design protection mechanisms that use the brain's strengths rather than its weaknesses. One early attempt was Passfaces: this is an authentication system that presents users with nine faces, only one of which is of a person they know; they have to pick the right face several times in a row to log on [356]. The rationale is that people are very good at recognising other people's faces, but very bad at describing them: so you could build a system where it was all but impossible for people to give away their passwords, whether by accident or on purpose. Other proposals of this general type have people selecting a series of points on an image — again, easy to remember but hard to disclose. Both types of system make shoulder surfing harder, as well as deliberate disclosure offline.

The most successful innovation in this field, however, is the CAPTCHA — which stands for 'Completely Automated Public Turing Test to Tell Computers and Humans Apart.'

The idea is that a program generates some random text, and produces a distorted version of it that the user must decipher. Humans are good at reading distorted text, while programs are less good.

It is inspired by the test famously posed by Alan Turing as to whether a computer was intelligent, where you put a computer in one room and a human in another, and invite a human to try to tell them apart.

Chapter 3

Protocols

3.1 Password Eavesdropping Risks

A good case study comes from simple embedded systems, such as the remote control used to open your garage or to unlock the doors of cars manufactured up to the mid-1990's. These primitive remote controls just broadcast their serial number, which also acts as the password. An attack that became common was to use a 'grabber', a device that would record a code broadcast locally and replay it later.

sixteen-bit passwords are too short. It occasionally happened that people found they could unlock the wrong car by mistake. By the mid-1990's, devices appeared which could try all possible codes one after the other. A code will be found on average after about 215 tries, which at ten per second takes under an hour. A thief operating in a parking lot with a hundred vehicles within range would be rewarded in less than a minute with a car helpfully flashing its lights.

3.2 Simple Authentication

Nonce: The term nonce can mean anything that guarantees the freshness of a message. A nonce can, according to the context, be a random number, a serial number, a random challenge received from a third party, or even a timestamp.

Security and business: Security mechanisms are used more and more to support business models, by accessory control, rights management, product tying and bundling. It is wrong to assume blindly that security protocols exist to keep 'bad' guys 'out'. They are increasingly used to constrain the lawful owner of the equipment in which they are built; their purpose may be of questionable legality or contrary to public policy. For example: Many printer companies embed authentication mechanisms in printers to ensure that genuine toner cartridges are used. If a competitor's product is loaded instead, the printer may quietly downgrade from 1200 dpi to 300 dpi, or simply refuse to work at all. Mobile phone vendors make a lot of money from replacement batteries, and now use authentication protocols to spot competitors' products so they can be blocked or even drained more quickly.

3.2.1 Challenge and response

3.2.2 Reflection Attacks

3.3 Manipulating the Message

3.4 Changing the Environment

3.5 Chosen Protocol Attacks

3.6 Managing Encryption Keys

3.6.1 Basic Key Management

3.6.2 The Needham-Schroeder Protocol

3.6.3 Kerberos

3.6.4 Practical Key Management

3.7 Getting Formal

3.7.1 A Typical Smartcard Banking Protocol

3.7.2 The BAN Logic

Chapter 4

Access Control

Chapter 5

Cryptography

Chapter 8

Multilevel Security

Chapter 9

Multilateral Security