SECURITY SYSTEMS

RUPERT STANLEY

ROSS SYSTEMS INTERNATIONAL

04 April 2006

SECURITY TOPICS

- Introduction to Security
- Security Standards
- Smart Cards and HSMs
- Banking Security Systems
- Multithreading. Telos v Pathway
- Documentation
- Testing
- Emerging Issues

INTRODUCTION TO SECURITY

WHY BOTHER?

FORGET SECURITY AND NASTY THINGS HAPPEN
TERRORISM, THEFT AND ERROR

IN OTHER WORDS THERE ARE SOME PEOPLE WHO ARE

- **NASTY AND/OR**
- **DISHONEST AND/OR**
- **STUPID**

PEOPLE AND INSTITUTIONS NEED PROTECTING

TERRORISM

DISHONESTY

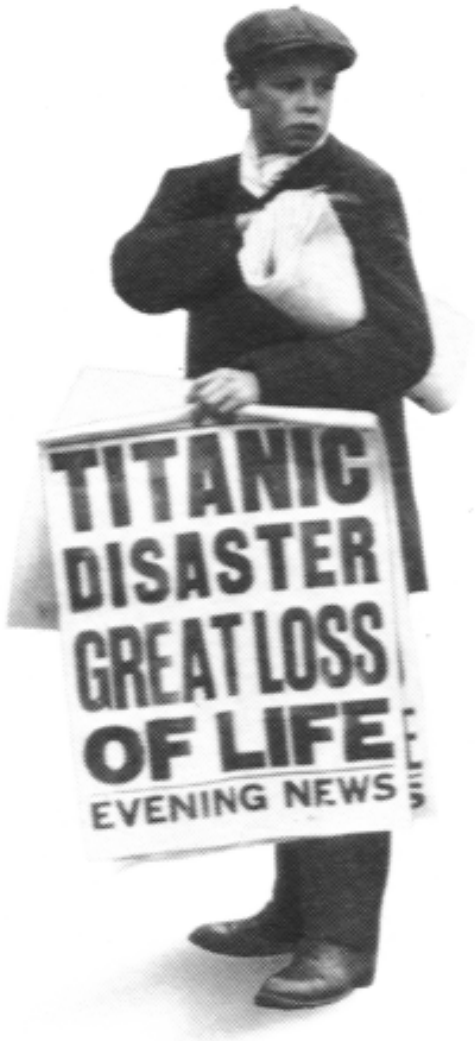
Tuesday, June 22, 1999 Published at 15:58 GMT 16:58 UK

Business: The Economy

How Leeson broke the bank

Nick Leeson guessed he faced jail when he was extradited to Singapore

STUPIDITY



INTRODUCTION TO SECURITY

RISK EVENTS

ARE THE KEY TO SECURITY
MANAGE YOUR RISK EVENTS AND YOU ARE SECURE

A RISK EVENT IS A POTENTIAL OR ACTUAL THREAT, A VULNERABILITY TO THAT THREAT AND CRUCIALLY A MOTIVE TO EXPLOIT THAT THREAT

THREATS MAY BE: EXTERNAL OR INTERNAL
ACCIDENTAL OR DELIBERATE
ELECTRONIC OR PHYSICAL

INTRODUCTION TO SECURITY

MANAGING RISK

THERE ARE A NUMBER OF APPROACHES

1. EMPLOYING ONLY PROPERLY VETTED STAFF
2. DEAL WITH VULNERABILITIES BY SAY
   OPERATING SYSTEM PATCHES OR
   FORTIFYING THE DATA CENTRE
3. REDUCE VALUE OF ASSET TO AN ATTACKER
   I.E. DATA ENCRYPTION, KEYS ETC.
4. TRANSFER RISK BY MEANS OF:
   INSURANCE OR
   OUTSOURCING TO A SPECIALIST

INTRODUCTION TO SECURITY

SURVIVAL STRATEGY

1. CORPORATE WILL, TO PROTECT THE ORGANISATION
2. RISK ASSESSMENT, MALICIOUS AND ACCIDENTAL
3. BUILD SECURITY POLICY, BALANCE COST/RISK
4. IMPLEMENT POLICY, PEOPLE/PROTOCOLS/DEVICES
5. MONITOR SECURITY, BOARD LEVEL, CONTINUOUS

INTRODUCTION TO SECURITY

CORPORATE WILL

BOARD LEVEL INVOLVEMENT IN SECURITY STRATEGY

IMPLIES WILL TO COMMIT TO SECURITY:

1. BOARD LEVEL EFFORT AT ALL STAGES

2. PEOPLE, ESPECIALLY A SECURITY OFFICER

3. RESOURCES, AUTHORITY, TIME MONEY

AND TO KEEP ON DOING IT WITH AN ISMS

INTRODUCTION TO SECURITY

ISMS

IS AN

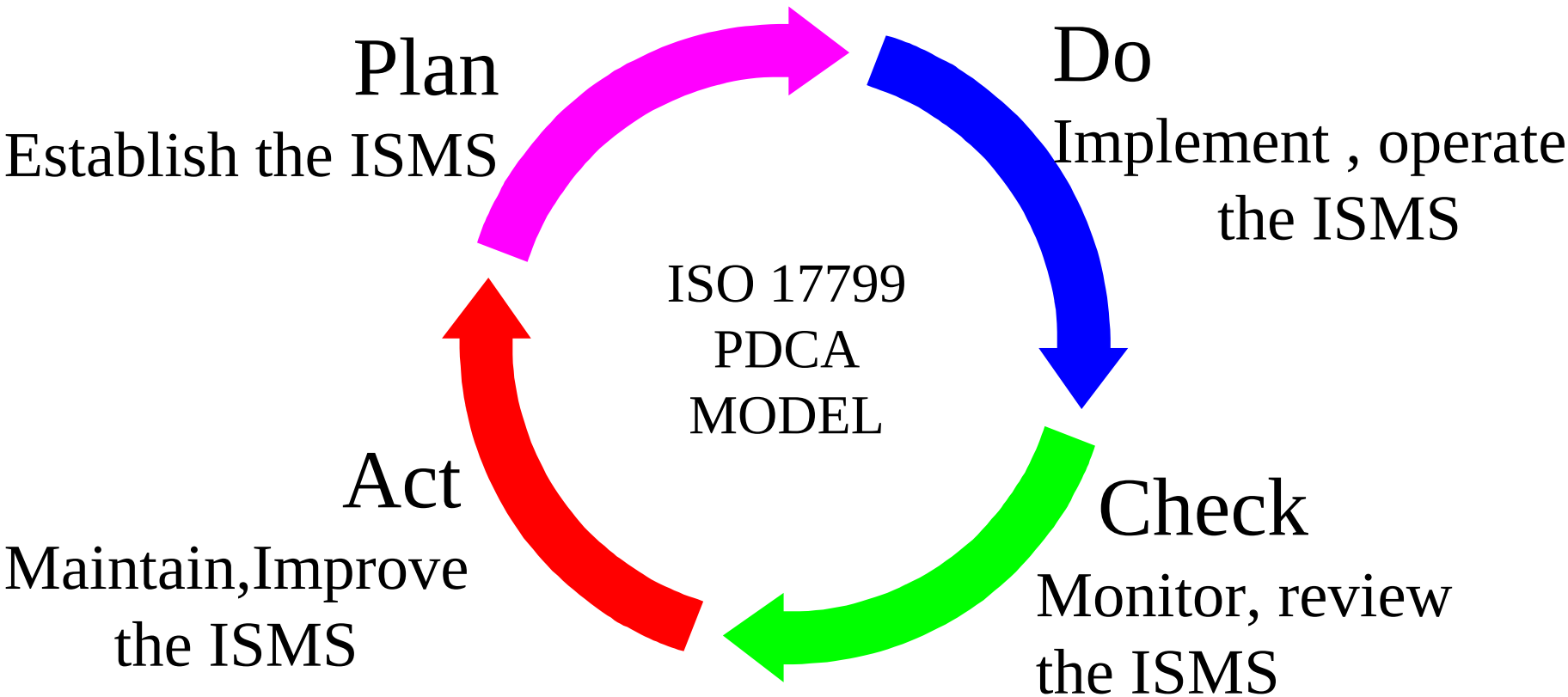
INFORMATION SECURITY MANAGEMENT SYSTEM

THE MEANS WHEREBY SENIOR MANAGEMENT MONITOR AND CONTROL THEIR SECURITY, MINIMISING THE RESIDUAL BUSINESS RISK AND ENSURING THAT SECURITY CONTINUES TO FULFIL CORPORATE CUSTOMER AND LEGAL REQUIREMENTS

THE EUROPEAN STANDARD FOR AN ISMS IS ISO/IEC 17799

INTRODUCTION TO SECURITY

PLAN – DO – CHECK - ACT



INTRODUCTION TO SECURITY

PLAN - ISMS

1. DEFINE THE SCOPE OF THE ISMS
2. DEFINE AN ISMS POLICY
3. DEFINE APPROACH TO RISK ASSESSMENT
4. IDENTIFY THE RISKS
5. ASSESS THE RISKS
6. IDENTIFY AND EVALUATE OPTIONS FOR THE TREATMENT OF RISK
7. SELECT CONTROL OBJECTIVES AND CONTROLS
8. PREPARE A STATEMENT OF APPLICABILITY (SOA)

INTRODUCTION TO SECURITY

DO - ISMS

1. FORMULATE RISK TREATMENT PLAN
2. IMPLEMENT RISK TREATMENT PLAN
3. IMPLEMENT CONTROLS
4. IMPLEMENT TRAINING AND AWARENESS PROGRAMS
5. MANAGE OPERATIONS
6. MANAGE RESOURCES
7. IMPLEMENT PROCEDURES TO DETECT/RESPOND TO SECURITY INCIDENTS

INTRODUCTION TO SECURITY

CHECK - ISMS

1. EXECUTE MONITORING PROCEDURES
2. UNDERTAKE REGULAR REVIEWS OF ISMS EFFECTIVENESS
3. REVIEW LEVEL OF RESIDUAL AND ACCEPTABLE RISK
4. CONDUCT INTERNAL ISMS AUDITS
5. REGULAR MANAGEMENT REVIEW OF ISMS
6. RECORD ACTIONS AND EVENTS THAT IMPACT ISMS

INTRODUCTION TO SECURITY

ACT - ISMS

1. IMPLEMENT IDENTIFIED IMPROVEMENTS
2. TAKE CORRECTIVE PREVENTATIVE ACTION
3. APPLY LESSONS LEARNT (INCLUDING OTHER ORGANISATIONS)
4. COMMUNICATE RESULTS TO INTERESTED PARTIES
5. ENSURE IMPROVEMENTS ACHIEVE OBJECTIVES

INTRODUCTION TO SECURITY

RISK ASSESSMENT

AIM: TO ASSESS THE RISKS TO THE ORGANISATION

FIND: THE VARIOUS RISKS FOR THE ORGANISATION

CALCULATE FOR EACH RISK:

SEVERITY LIKELIHOOD

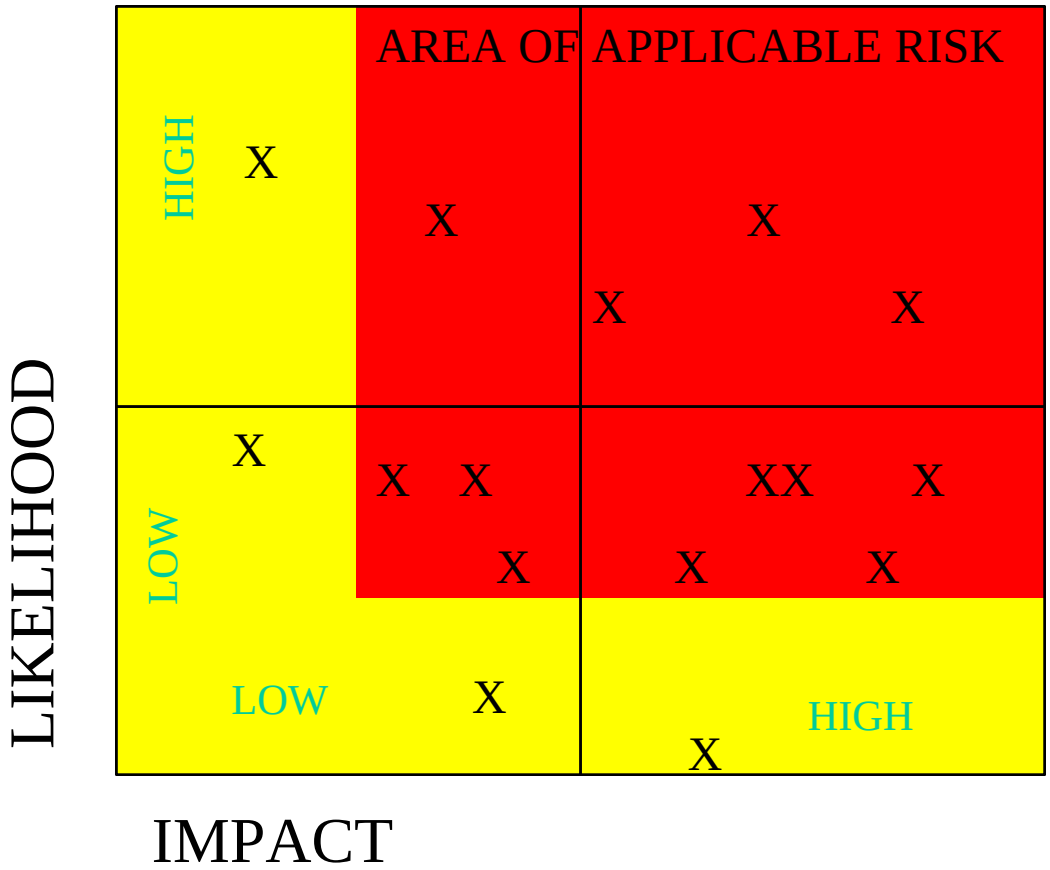
CHECK THAT ALL RISKS HAVE BEEN COVERED:

MALICIOUS ACCIDENTAL

NOTE: DRAMA IS NOT ALWAYS EQUATED WITH COST

INTRODUCTION TO SECURITY

RISK ANALYSIS DIAGRAM



INTRODUCTION TO SECURITY

DRAMA VERSUS COST

BANK ROBBER MAY GET $10,000 IF LUCKY!

CORPORATE FRAUD TYPICALLY RUNS INTO MILLIONS

WHERE WOULD YOU PUT YOUR CHIEF EFFORT?

BARINGS HAD VERY GOOD TELLER SECURITY

BUT

LEESON COST THE BANK $800 MILLION

INTRODUCTION TO SECURITY

SECURITY POLICY

AIM: TO MINIMISE RISKS TO A MANAGEABLE LEVEL

METHOD: INVESTIGATE PROCEDURES AND DEVICES WHICH CAN BE USED TO MINIMISE RISKS
DETERMINE RESPONSE TO EACH OF THE SECURITY RISKS. THE COST MUST BALANCE THE RISK, COST MAY BE REPUTATION
DON'T FORGET ACCIDENT CONTINGENCY AND BUSINESS CONTINUITY PLANNING

NOTE: COST AND EFFICIENCY SAVINGS MAY RESULT FROM THIS, AN INEFFICIENT PROCESS IS A RISK!

INTRODUCTION TO SECURITY

BUSINESS CONTINUITY RISKS

EMPLOYEES

- LOSS OF SERVICE FROM KEY EMPLOYEES
- KEY EMPLOYEES CAN'T GET TO WORK
- LOSS OF KEY SKILLS FROM YOUR BUSINESS

CUSTOMERS

- WHO ARE YOUR MOST IMPORTANT CUSTOMERS
- WHY DO THEY CHOOSE TO TRADE WITH YOU
- DISRUPTION OF SERVICE TO KEY CUSTOMERS

INFORMATION

- LOSS OF KEY INFORMATION
- IT OR TELECOMS INFRASTRUCTURE IS COMPROMISED

SUPPLIERS

- FAILURE OF DISRUPTION OF KEY SUPPLIER
- EFFECT ON CUSTOMERS OF KEY SUPPLIER LETTING YOU DOWN

INTRODUCTION TO SECURITY

IMPLEMENT POLICY

1. DRIVEN BY SECURITY OFFICER. MONITOR HIM!

2. INVOLVE ALL MEMBERS OF STAFF
   TRAINING AND AWARENESS

3. USE TOOLS TO MAKE PEOPLE FOLLOW POLICY

4. ENSURE THAT ALL ASPECTS OF THE POLICY ARE IMPLEMENTED. THE BEST CRYPTOGRAPHY IN THE WORLD IS USELESS IF YOU LET PEOPLE WANDER AROUND “SECURE AREAS” OR IF YOU LET ONE PERSON HOLD ALL THE KEYS!

INTRODUCTION TO SECURITY

MONITOR SECURITY

1. ANYONE IN THE COMPANY CAN BE A SECURITY RISK WHICH IS WHY THERE ARE SECURITY PROCEDURES.

2. A CARELESS PERSON IS NOT NECESSARILY A CRIMINAL SO MONITOR EVERYONE BOARD LEVEL INCLUDED

3. CHECKS AND BALANCES ARE GOOD BUSINESS PROCEDURES

4. BUSINESS DOES NOT STAY STILL SO KEEP THE SECURITY PLAN UPDATED IN THE LIGHT OF THE GROWING BUSINESS AND NEW RISKS AS THEY APPEAR.

5. MONTHLY/WEEKLY REPORTS FROM THE SECURITY OFFICER

INTRODUCTION TO SECURITY

COMPUTER SECURITY

1. COMPUTERS ARE AT THE HUB OF BUSINESSES

2. THEY HOLD VALUABLE PROPRIETRY AND CONFIDENTIAL INFORMATION.

3. THIS SECRECY IS ENFORCED BY LAW FOR:, I.E.
   - A) EMPLOYEE RECORDS,
   - B) CUSTOMER INFORMATION
   - C) BANKING DATA

4. SECURING THESE SYSTEMS IS CRUCIAL TO SECURING THE BUSINESS

INTRODUCTION TO SECURITY

SECURING COMPUTER SYSTEMS

THE CORPORATE DATA SYSTEMS NEED:

- PHYSICAL SECURITY I.E.
  - LOCKED DATA CENTRES, TERMINAL ACCESS
  - STAFF SEPARATION PROGRAMMING/OPERATION/USER
  - SECURE STORAGE OF SECURITY KEYS
- LOGICAL SECURITY I.E.
  - PASSWORDS
  - FIREWALLS
  - ANTIVIRUS AND SECURITY SOFTWARE
  - SECURITY MODULES

AGAINST

- EXTERNAL THREATS, INTERNET (HACKING/SERVICE DENIAL)
- INTERNAL THREATS, STAFF (FRAUD/COMMERCIAL THEFT)

INTRODUCTION TO SECURITY

PHYSICAL & LOGICAL SECURITY

REVIEWS OF THESE ARE TO BE FOUND IN THE LITERATURE, SOME OF WHICH ARE IN THE NOTES.

WILL CONCENTRATE ON LOGICALLY SECURING THE ENTERPRISE USING CRYPTOGRAPHIC TECHNIQUES INCLUDING PROCESSES, SMART CARDS AND HOST SECURITY MODULES

INTRODUCTION TO SECURITY

SECURING THE ENTERPRISE

THERE ARE TWO GROUPS OF PRINCIPLES

1. ACCESS RULES

   A SYSTEM MUST BE ACCESSED TO BE USEFUL BUT TO BE SECURE NEEDS TO BE PROTECTED BY CRYPTOGRAPHY

2. DEFENCE IN DEPTH

   DEFENCE SHOULD BE COMPARTMENTALISED BY

   A) TIME
   B) LOCATION
   C) USER

   THUS A SECURITY FAILURE WILL NOT PROPAGATE TO OTHER TIMES, LOCATIONS OR USERS

INTRODUCTION TO SECURITY

ACCESS SECURITY

SECURE ACCESS TO COMPUTER SYSTEMS NEED TO CONFORM TO THE FOLLOWING PRINCIPLES:

1. PRIVACY. No third party can gain access to data

2. AUTHENTICATION. Mutual User/System Verification

3 INTEGRITY. Detection of Alteration in Data Transferred.

4. NON-REPUDIATION. User can't deny transaction.

INTRODUCTION TO SECURITY

PRIVACY

EXCLUSION OF THIRD PARTIES TO TRANSACTION DATA

THIS IS PERFORMED BY ENCRYPTING THE DATA
GOOD PRIVACY IS WHERE YOU KNOW THE ALGORITHM BUT STILL CAN'T DECYPHER THE DATA

TWO FORMS OF ENCRYPTION AVAILABLE

1. SYMETRIC. BOTH PARTIES HAVE THE SAME KEY

2. AYSYMETRIC. PUBLIC KEY/PRIVATE KEY

INTRODUCTION TO SECURITY

AUTHENTICATION

THE VERIFICATION OF THE IDENTITY OF ONE OR BOTH COMMUNICATING PARTIES

CAN BE PERFORMED BY

1. THE SUPPLY OF AN IDENTITY AND

2. A) THE ENCRYPTION OF TOKEN(S) PASSED FROM ONE PARTY TO THE OTHER, OR
   B) THE TRANSMISSION OF A PREARRANGED PASSWORD.

INTRODUCTION TO SECURITY

INTEGRITY

THIS ENSURES THAT ANY MODIFICATION OF THE DATA IS DETECTED, INCLUDING REPEATED MESSAGES

THIS CAN BE PERFORMED BY:

1. CRC OR MDC CODES
   ENSURES THAT ANY ALTERATION IS DETECTED.

2. SESSION NUMBERS
   ENSURES THAT EACH SESSION IS UNIQUE

BOTH OF THESE MUST BE ENCRYPTED

INTRODUCTION TO SECURITY

NON-REPUDIATION

THE ELECTRONIC SIGNING OF MESSAGES TO ENSURE THAT THE USER CANNOT DENY THE TRANSACTION

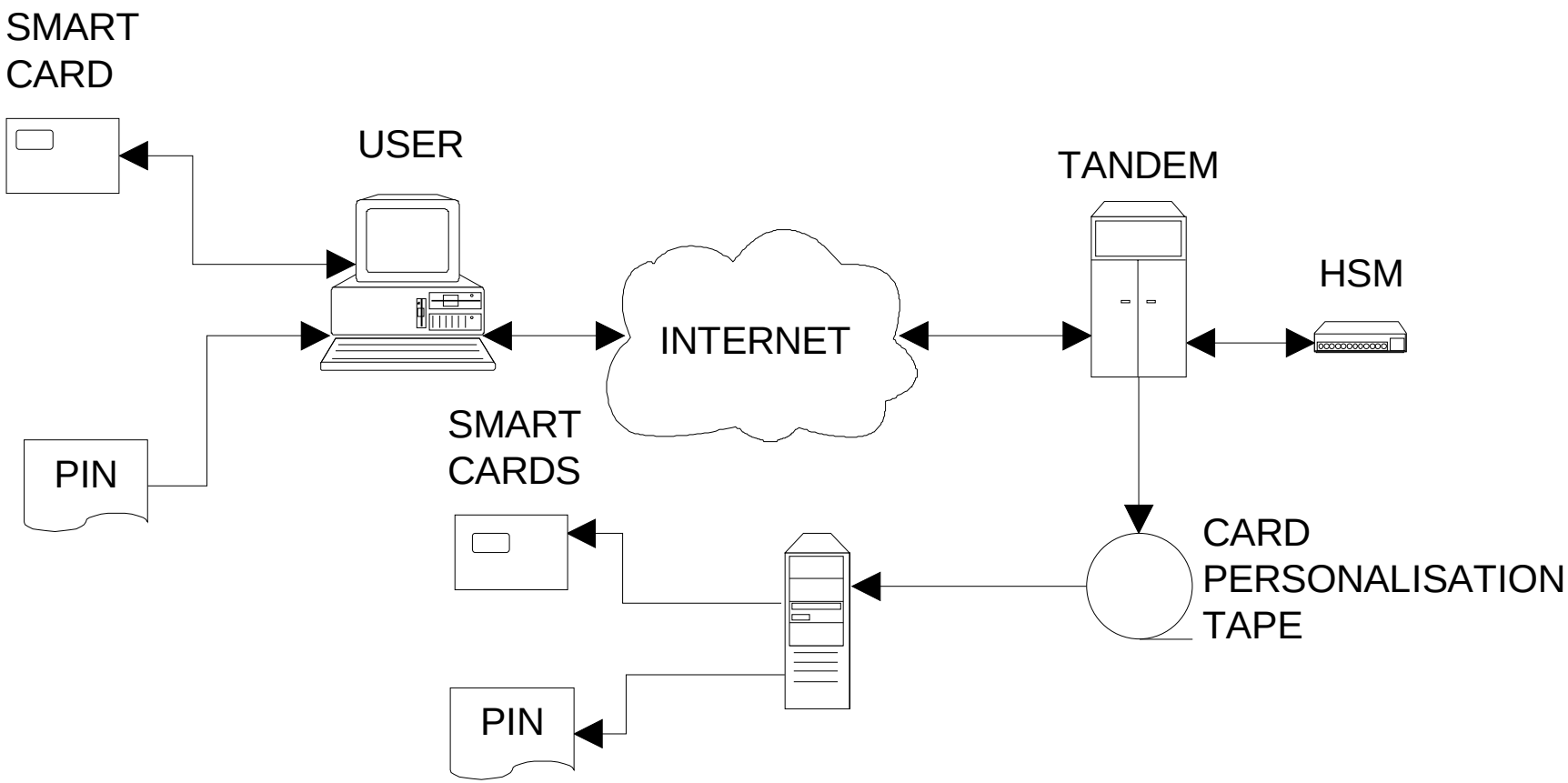
THIS IS PERFORMED BY:

1. THE GENERATION OF A MDC OR SECURE HASH CODE OVER THE COMMERCIALLY SENSITIVE DATA

2. THE ENCRYPTION OF THE CODE WITH A SECRET KEY, WHICH IS UNKNOWN TO ANYONE BUT UNIQUELY IDENTIFIES THE USER.

INTRODUCTION TO SECURITY

COMPONENTS



INTRODUCTION TO SECURITY

DEFENCE IN DEPTH

THIS IS NORMALLY ACHIEVED BY HAVING A HIERARCHY OF KEYS, FOR INSTANCE

1. LOCAL MASTER KEYS

2. ZONE MASTER KEYS

3. USER MASTER KEYS

4. TEMPORY SESSION AND AUTHENTICATION KEYS

INTRODUCTION TO SECURITY

LOCAL MASTER KEYS

THESE ARE ALSO KNOWN AS LMKS

THEY ARE HELD IN THE HOST SECURITY MODULE (HSM) A SECURITY BOX ATTACHED TO THE TANDEM

THEY ARE SELDOM CHANGED

THEY ARE USED TO DERIVE ALL THE OTHER KEYS

INTRODUCTION TO SECURITY

ZONE MASTER KEYS

THESE ARE ALSO KNOWN AS ZMKS & TRANSPORT KEYS

THEY ARE HELD IN ENCRYPTED FORM FOR USE IN THE HSM AND ON A PERSONALISATION SMART CARD

THEY ARE SELDOM CHANGED

THEY ARE USED TO TRANSPORT USER KEYS FROM THE HOST TO THE PERSONALISER WHERE THE USERS SMART CARDS ARE PRODUCED

INTRODUCTION TO SECURITY

USER MASTER KEYS

THEY ARE HELD ON A USER'S SMART CARD AND IN ENCRYPTED FORM FOR USE IN THE HSM

THEY ARE DIFFERENT FOR EVERY USER CARD

THEY ARE USED TO:

ENCRYPT TEMPORY SESSION KEYS

DIVERSIFY TEMPORY AUTHENTICATION KEYS

INTRODUCTION TO SECURITY

TEMPORARY KEYS

THEY ARE RANDOMLY GENERATED FOR EACH SESSION, ENCRYPTION AND AUTHENTICATION

THEY ARE DIFFERENT FOR EVERY TIME AND NEED TO BE ENCRYPTED/DIVERSIFIED BEFORE USE

THE SESSION TEMPORARY KEYS NEED TO BE SYNCHRONISED FOR AUTHENTICATION

THEY ARE USED TO:
ENCRYPT TOKENS AND DATA
GENERATE ELECTRONIC SIGNATURES

SUMMARY

INTRODUCTION

AN INFORMATION SECURITY MANAGEMENT SYSTEM

ISMS

IS BASED ON A PLAN-DO-CHECK-ACT CYCLE

THIS FIGHT TO KEEP INFORMATION SYSTEMS IS NEVER AT A REST

THERE WILL ALWAYS BE PEOPLE WHO FOR SOME REASON OR OTHER WANT TO BREECH YOUR SECURITY SYSTEM

THE TOOLS THEY ARE USING ARE GETTING MORE SOPHISTICATED AND CAPABLE OF COMPROMISING YOUR MISSION CRITICAL SYSTEMS

WHERE DO WE GO FROM HERE?

SUMMARY

MEANS OF DEFENCE

THE FOLLOWING MEANS OF DEFENCE ARE AVAILABLE:

1. PHYSICAL SECURITY BY LOCATION/PERSON/TIME
2. SMART CARD/HSM BASED CRYPTOGRAPHY INCLUDING
   A) AUTHENTICATION TOOLS
   B) APPLICATION SIGNING
   C) DATA CRYPTOGRAPHY
3. FIREWALLS TO GUARD NETWORKS, APPLICATIONS & DESKTOPS
4. VIRTUAL PRIVATE NETWORKS
5. NETWORK AND HOST BASED INTRUSION DETECTION SYSTEMS
6. INTRUSION PREVENTION TOOLS FOR SERVERS AND DESKTOPS
7. ANTIVIRUS SOFTWARE FOR DESKTOPS AND GATEWAYS
8. HONEYPOTS TO LURE POTENTIAL ATTACKERS

THINGS ARE GETTING COMPLEX THIS CAN BE A THREAT TOO!

SUMMARY

FUTURE THREATS

THERE ARE THREE MAIN THRUSTS AT THE PRESENT MOMENT:

1. EVER MORE SOPHISTICATED SPYWARE, TROJANS AND WORMS

2. OVERWHELMING DENIAL OF SERVICE ATTACKS

3. HIGH SPEED CODE CRACKING BASED ON
   A) FASTER & MORE SOPHISTICATED CODE CRACKING MACHINES
   B) DEVELOPMENTS IN MATHEMATICS

SUMMARY

FUTURE SOLUTIONS

GET FASTER, DEEPER AND SMARTER, I.E.

1. THROW OUT THE DENIAL OF SERVICE ATTACKS WHEN THEY HIT YOU FIRST FIREWALL NOT WHEN THEY HAVE BOGGED DOWN YOUR SYSTEM. I.E. SSL, ANTI SPOOFING SOFTWARE AND DYNAMIC IP IDENTIFICATION AND BLOCKING.

2. WORK OUT THE VULNERABILITIES OF YOUR SYSTEM BEFORE YOUR ENEMIES DO AND ATTACK THE ATTACKER.

3. DEVELOP MORE ADVANCED CRYPTOGRAPHIC AND IDENTIFICATION TECHNIQUES BEFORE THE CRACKERS BREAK YOUR CURRENT TECHNIQUES. I.E BIOMETRICS AND AES.

SUMMARY

CONCLUSION

YOU CAN'T STOP ALL ATTACKS BUT IF YOU ARE WISE AND LUCKY

THEY WILL NOT HURT YOU, THIS TIME

MAKE SURE THERE'S NOT A NEXT

USE YOUR ISMS TO PROVIDE DEFENCE IN DEPTH

BE PROACTIVE, OFFENSIVE AS WELL AS DEFENSIVE AND NEVER COMPLACENT

GOOD LUCK!