securityrisk
solutions

. Security . with . Clarity .

Electronic Banking

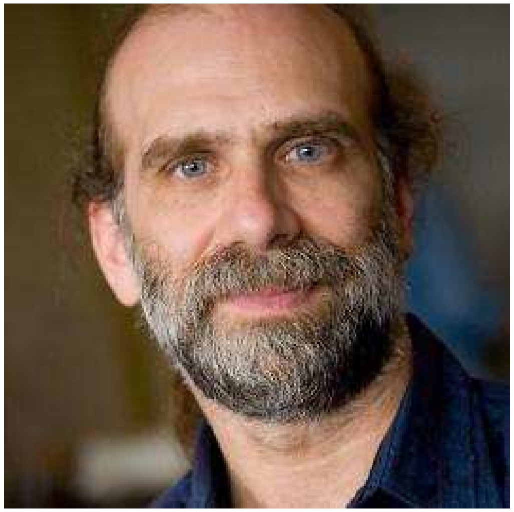
Compatibility Issues and Prospects in Kenya

Kostja Reim

Thought of the day

- “Computer insecurity is inevitable. Networks will be hacked. Fraud will be committed. Money will be lost. People will die”.

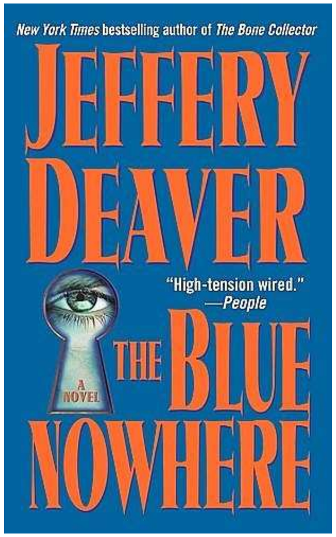
(Bruce Schneier, Master Cryptographer, 1989)



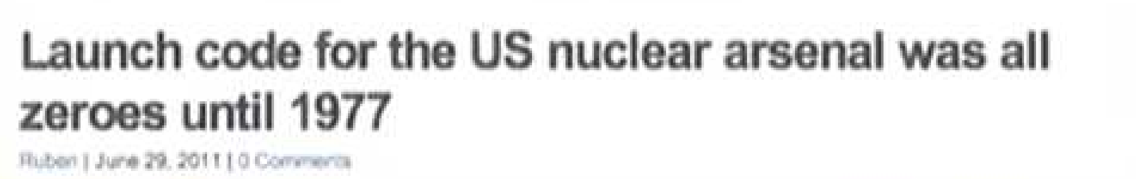
More recent …

- " Most of today's Internet is a combination shopping mall, USA Today, multiplex cinema and amusement park. Browsers and search engines are populated with cartoon characters and decorated with pretty pictures (plenty of those damn ads too). The point and click technology of the mouse can be mastered by a three year old. Simpleminded Help menus await at every new window. This is the Internet as packaged for the public through the glossy facade of the commercialized World Wide Web.
- But the REAL Internet - the Internet of the true hacker, lurking behind the Web - is a wild, raw place, where hackers use complicated commands, telnet utilities and communications software stripped bare as a dragster to sail throughout the world at, literally, the speed of light. ”

(Jeffery Deaver - The Blue Nowhere - pgs 97/98)


New York Times bestselling author of The Bone Collector
JEFFERY DEAVER
"High-tension wired." —People
A NOVEL
THE BLUE NOWHERE

Codes … Did you know?



Launch code for the US nuclear arsenal was all zeroes until 1977

Ruben | June 29, 2011 | 0 Comments

Management priorities

- "The best way to get management excited about a disaster plan is to burn down the building across the street." (**Dan Erwin, Security Officer, Dow Chemical Company – 2008)**

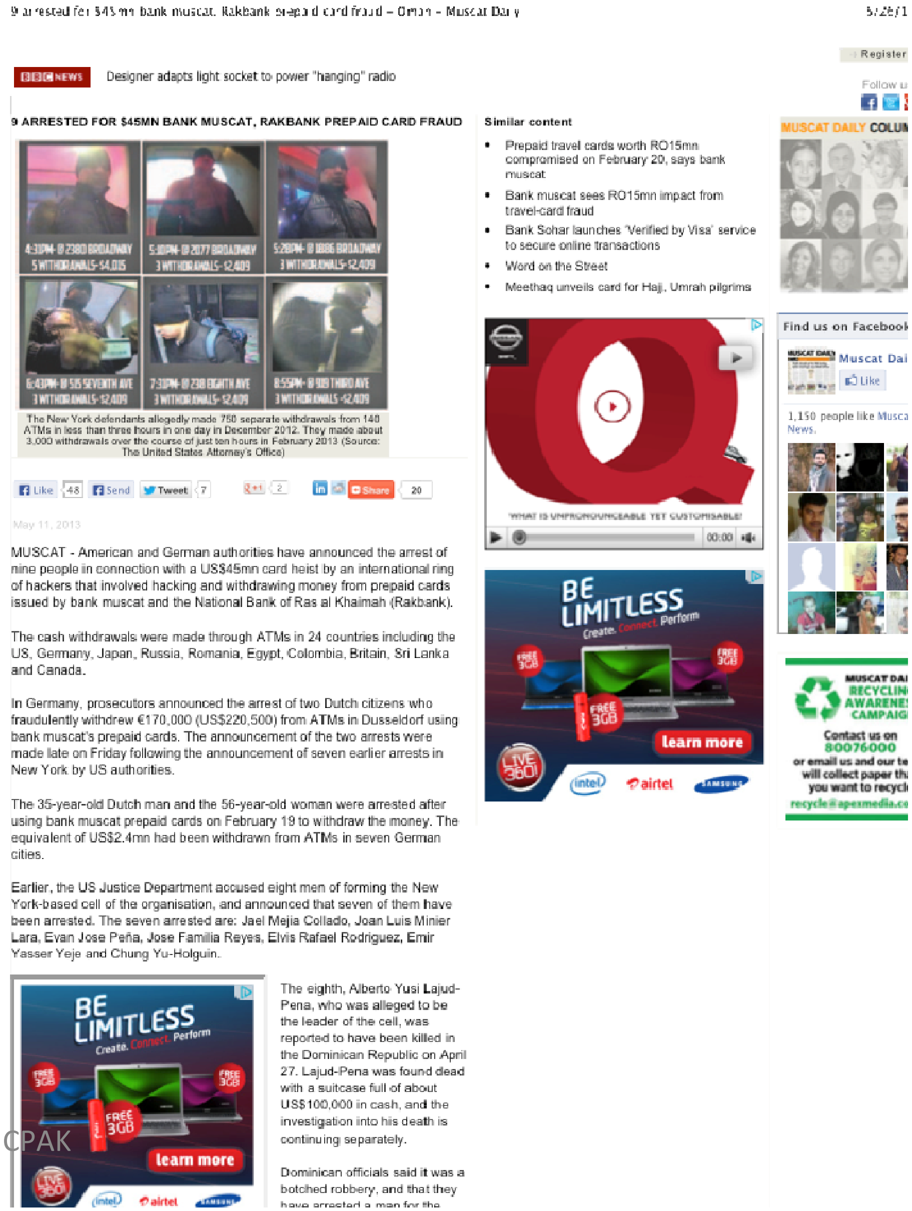
The Hype Around eCrime

How Barclays Bank's Shs80bn Fraud Was Planned

Today's Crooks Target Computer Systems To Swindle Billions Of Dime

BARCLAYS BANK'S Shs80bn FRAUD

"As banking goes digital, so does the traditional bank heist. Hacking bank's computers and transferring millions electronically can be as simple as know-



9 arrested for $45mn bank muscat, Rakbank prepaid card fraud – Oman – Muscat Daily 5/28/1

Designer adapts light socket to power "hanging" radio

9 ARRESTED FOR $45MN BANK MUSCAT, RAKBANK PREPAID CARD FRAUD

The New York defendants allegedly made 750 separate withdrawals from 140 ATMs in less than three hours in one day in December 2012. They made about 3,000 withdrawals over the course of just ten hours in February 2013 (Source: The United States Attorney's Office)

May 11, 2013

MUSCAT - American and German authorities have announced the arrest of nine people in connection with a US$45mn card heist by an international ring of hackers that involved hacking and withdrawing money from prepaid cards issued by bank muscat and the National Bank of Ras al Khaimah (Rakbank).

The cash withdrawals were made through ATMs in 24 countries including the US, Germany, Japan, Russia, Romania, Egypt, Colombia, Britain, Sri Lanka and Canada.

In Germany, prosecutors announced the arrest of two Dutch citizens who fraudulently withdrew €170,000 (US$220,500) from ATMs in Dusseldorf using bank muscat's prepaid cards. The announcement of the two arrests were made late on Friday following the announcement of seven earlier arrests in New York by US authorities.

The 35-year-old Dutch man and the 56-year-old woman were arrested after using bank muscat prepaid cards on February 19 to withdraw the money. The equivalent of US$2.4mn had been withdrawn from ATMs in seven German cities.

Earlier, the US Justice Department accused eight men of forming the New York-based cell of the organisation, and announced that seven of them have been arrested. The seven arrested are: Jael Mejia Collado, Joan Luis Minier Lara, Evan Jose Peña, Jose Familia Reyes, Elvis Rafael Rodriguez, Emir Yasser Yeje and Chung Yu-Holguin.

The eighth, Alberto Yusi Lajud-Pena, who was alleged to be the leader of the cell, was reported to have been killed in the Dominican Republic on April 27. Lajud-Pena was found dead with a suitcase full of about US$100,000 in cash, and the investigation into his death is continuing separately.

Dominican officials said it was a botched robbery, and that they have arrested a man for the

Similar content

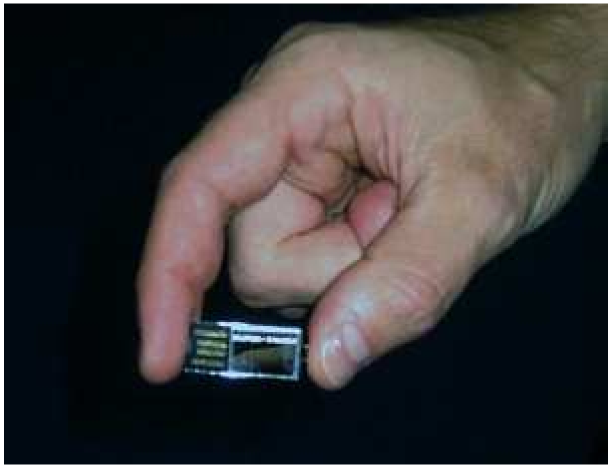
- Prepaid travel cards worth RO15mn compromised on February 20, says bank muscat
- Bank muscat sees RO15mn impact from travel-card fraud
- Bank Sohar launches 'Verified by Visa' service to secure online transactions
- Word on the Street
- Meethaq unveils card for Hajj, Umrah pilgrims

Find us on Facebook

Muscat Daily Like

1,150 people like Muscat Daily News.

$5-15 on eBay



Why eBanking?

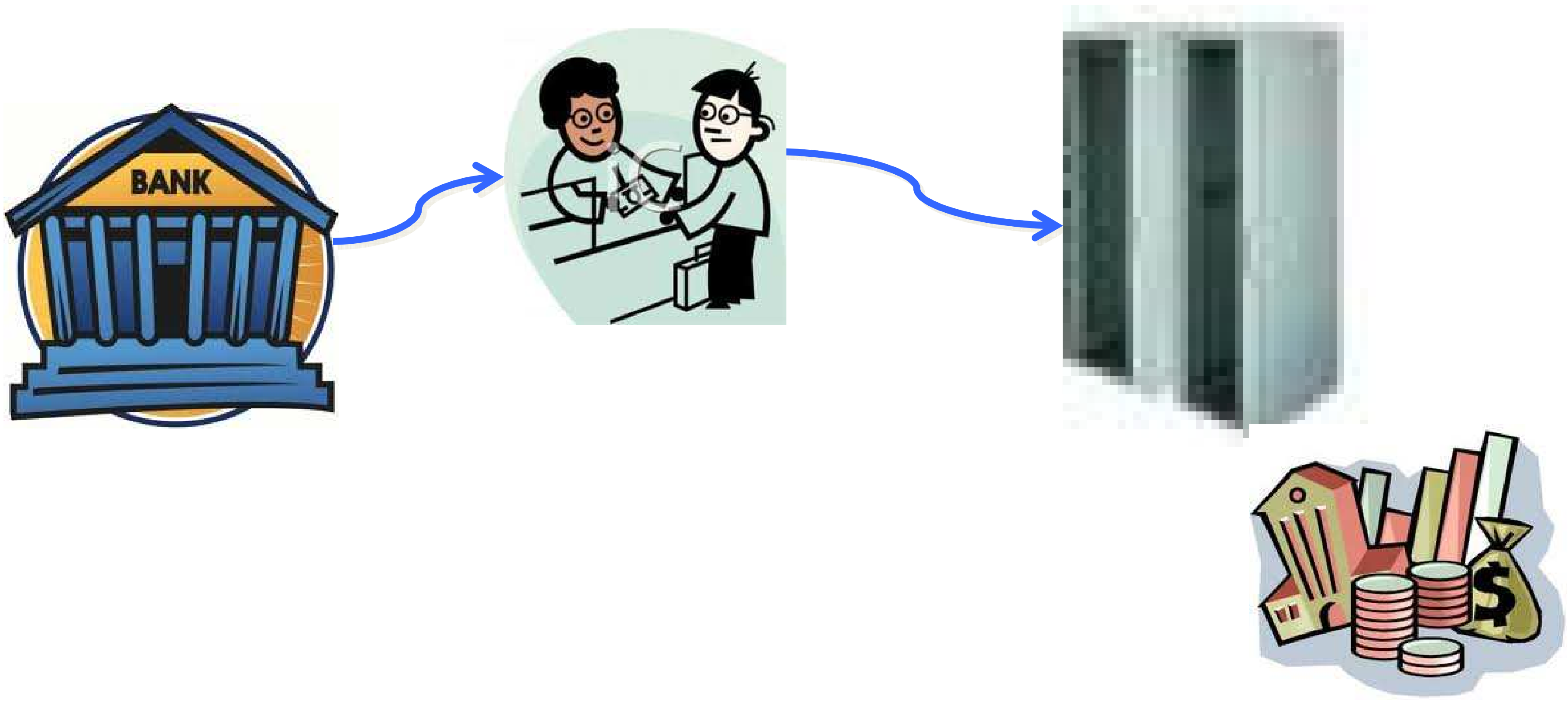
Constraints

- Availability and growth of telecommunication infrastructure
- ICT penetration in electronic banking sectors
- Culture of using electronic banking
- Legal and regulatory framework
- Security

Internet and Mobile Banking Demystified

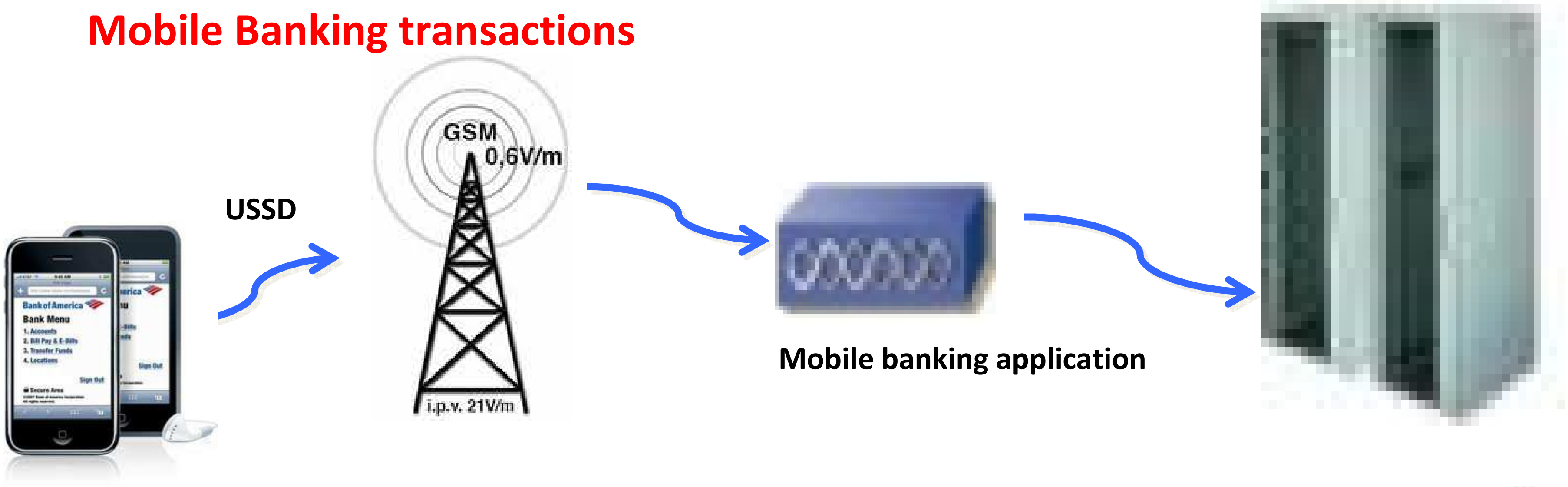
Over the counter transactions

Core banking application



Internet and Mobile Banking Demystified

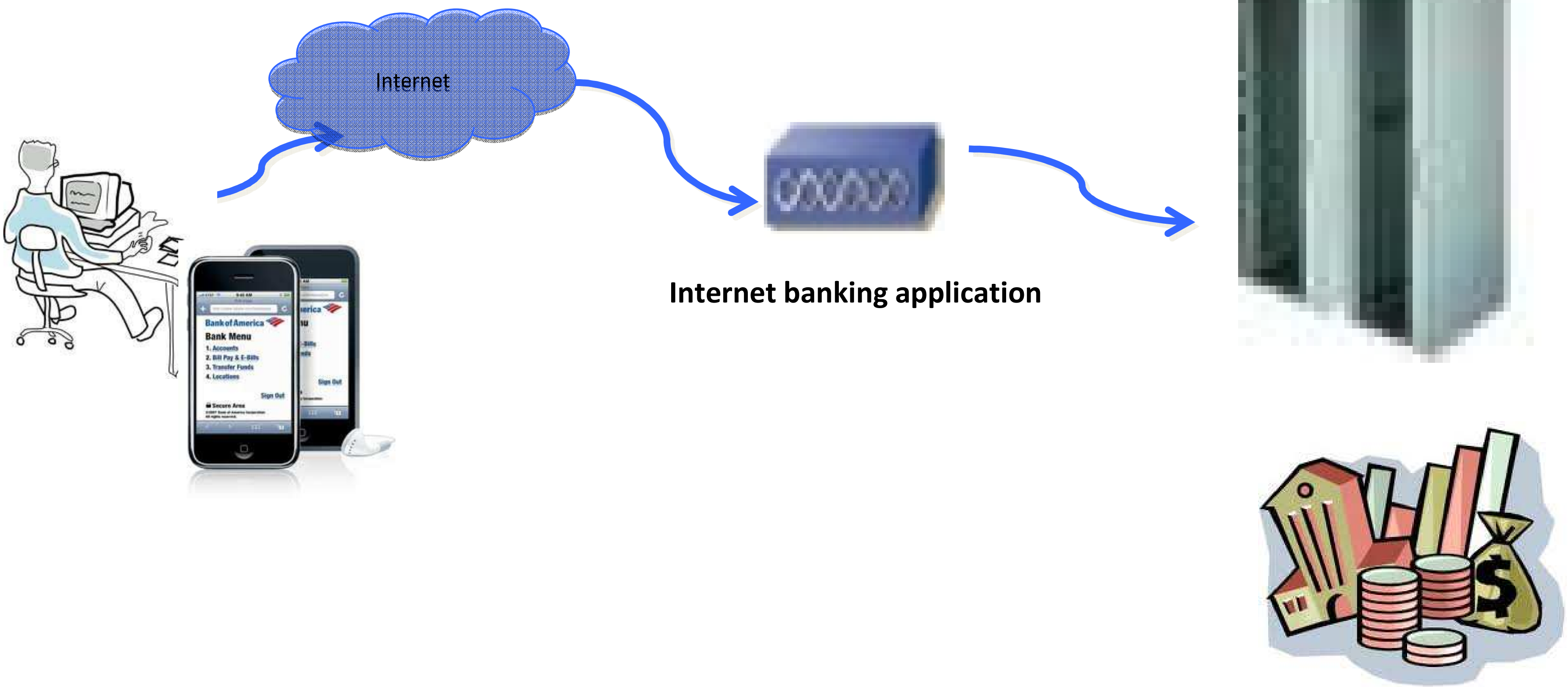
Mobile Banking transactions



Internet and Mobile Banking Demystified

Core banking application

Internet Banking transactions



Internet

Internet banking application

Internet and Mobile Banking Demystified

Internet/Mobile Banking categorization

Inquiry Based	Transaction based
• No transaction takes place • Checks on bank balances • Checks last transaction amounts etc.	• Full transactions rights • Can transfer money • Can give the bank instructions

Internet and Mobile Banking Demystified

Internet/Mobile Banking categorization

Retail	Corporate
• Normal customer account • Usually small amounts transacted • Transaction limits • Single user	• Corporate account • Multiple large amounts Transacted • No transaction limits • Multiple users • Maker / Checker

Internet and Mobile banking Demystified

Internet/Mobile Banking categorization

	Inquiry based	Transaction based
CIB	Medium	Very High
RIB	LOW	High

Common Security Objectives

C – Confidentiality

I – Integrity

A– Availability

Common Security Objectives

Availability

"Availability is the proportion of time a system is in a functioning condition. This is often described as a **mission capable rate"** **Wikipedia**

Based on business model:

- **Disaster recovery – Based on RTO**
- **Fault tolerance 99.999 – 100% uptime**

Common Security Objectives

Confidentiality

“the state of being secret; spoken, written, acted on, etc., in strict privacy or secrecy;”

- **Bank transactions details**
- **Salaries/payroll**
- **Bank balances**
- **Credit worthiness**

Common Security Objectives

Integrity

“the state of being whole, entire, or undiminished; a sound, unimpaired, or perfect condition”

From an information security perspective it is the assurance that:

(a)Information has not been altered either in transit or at rest without proper authorization.

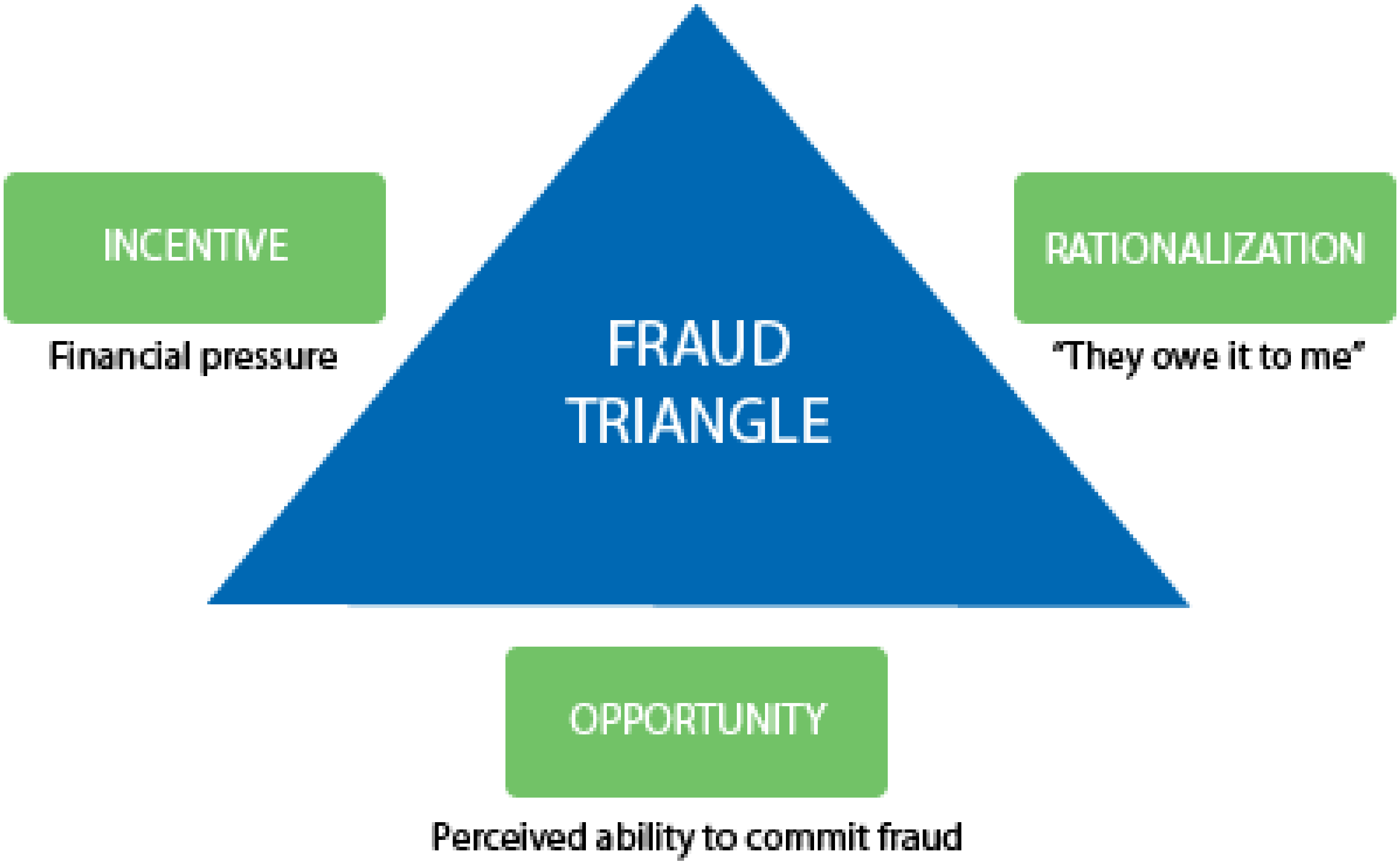
(b)The claim to be the authorized individual is factual.

✓Repudiation/None repudiation

Common Security Objectives

You can never tell whether the person on the other side is a dog

Fraud Triangle



FRAUD TRIANGLE

INCENTIVE

Financial pressure

RATIONALIZATION

"They owe it to me"

OPPORTUNITY

Perceived ability to commit fraud

Threats to Security Objectives

Banks Point of view

1. Usual insider fraud 2.0:

- **Dormant accounts suddenly being registered for Internet/Mobile banking**

2. User fraud

- **Repudiation of transactions**

3. Attacks on the internet banking/mobile banking application itself (Hacking)

- **Attack on the application to cause a denial of service/defacement (Hactivism)**
- **Attack the application to gain access to the core banking application-to transfer money**

Threats to Security Objectives

User Point of view

1. Theft of user credentials

- **Key loggers**
- **Man in the middle attacks**
- **Social engineering**
- **Shoulder surfing**
- **Phishing**
- **Application vulnerability (credential harvesting)**

Threats to Security Objectives

User Point of view

Denial of service

- **Account lock out**

Achieving Security Objectives

Control requirements

- Internal Audit
  - Independent
  - Audits IT
- Defined RM Framework
  - Annual assessment
  - Risk Treatment Plan
  - Investigation of all significant incidents
- ICT Strategy and Head of ICT
- CISO insourced or outsourced
- Regular VA and Pentesting
- Segregation of Duties documented
- BCM (processes, systems, succession) and IR
- Logging and Monitoring – 1 Year! Correlated
- Purchased Software only
- Sandboxing of new Products
- Security Policy of accepted standard (PCI DSS, ISO27002)
- Outsourcing Controls and Regulator approves of any contract

Achieving Security Objectives

Availability

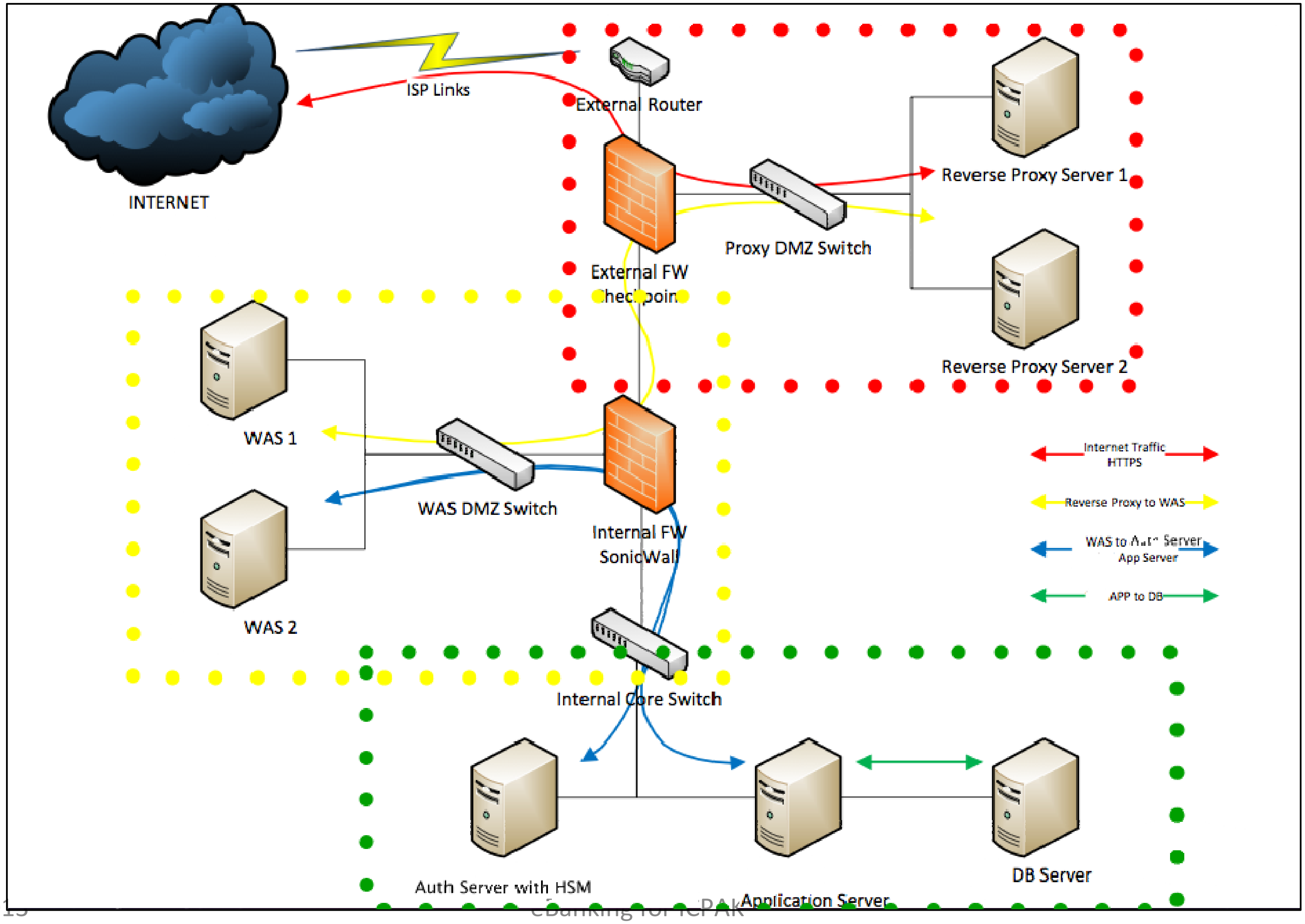
- Redundant systems
- Traffic Filtering
- Secure coding practices

Achieving Security Objectives

Confidentiality

- Secure protocols (encryption)
- Secure coding practices
- Secure network design

Defence in Depth



Achieving Security Objectives

Integrity

Use of secure protocols and file transfers

- encryption and hashing

Proper site authentication

- Digital certificates
- Unique Identification

Proper backend management (administrator management)

- Access controls over critical tables
- Multi factor authentication
- User maintenance audited

Secure process design

Customer and helpdesk education

Achieving Security Objectives

Integrity

Proper authentication mechanisms (Multifactor authentication)

Username and passwords are no longer adequate.

Consisting of:

□Something you know

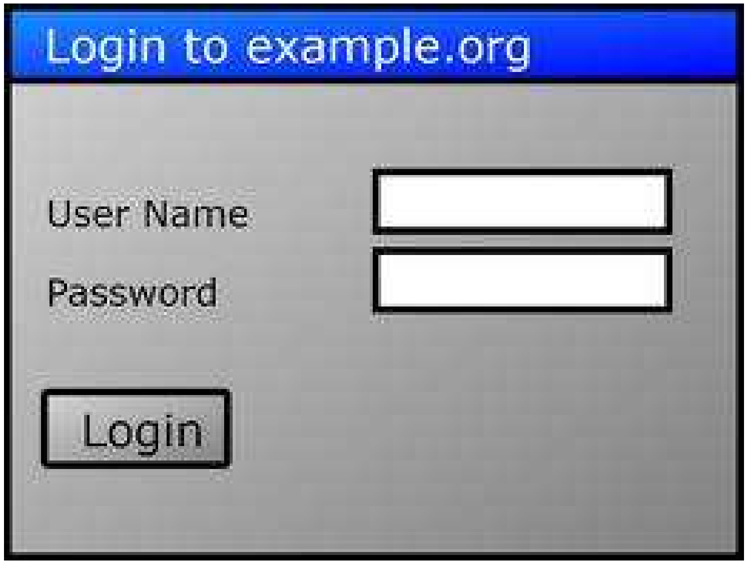
□Something you have

□Something about you

Achieving Security Objectives

Integrity

- Something you know

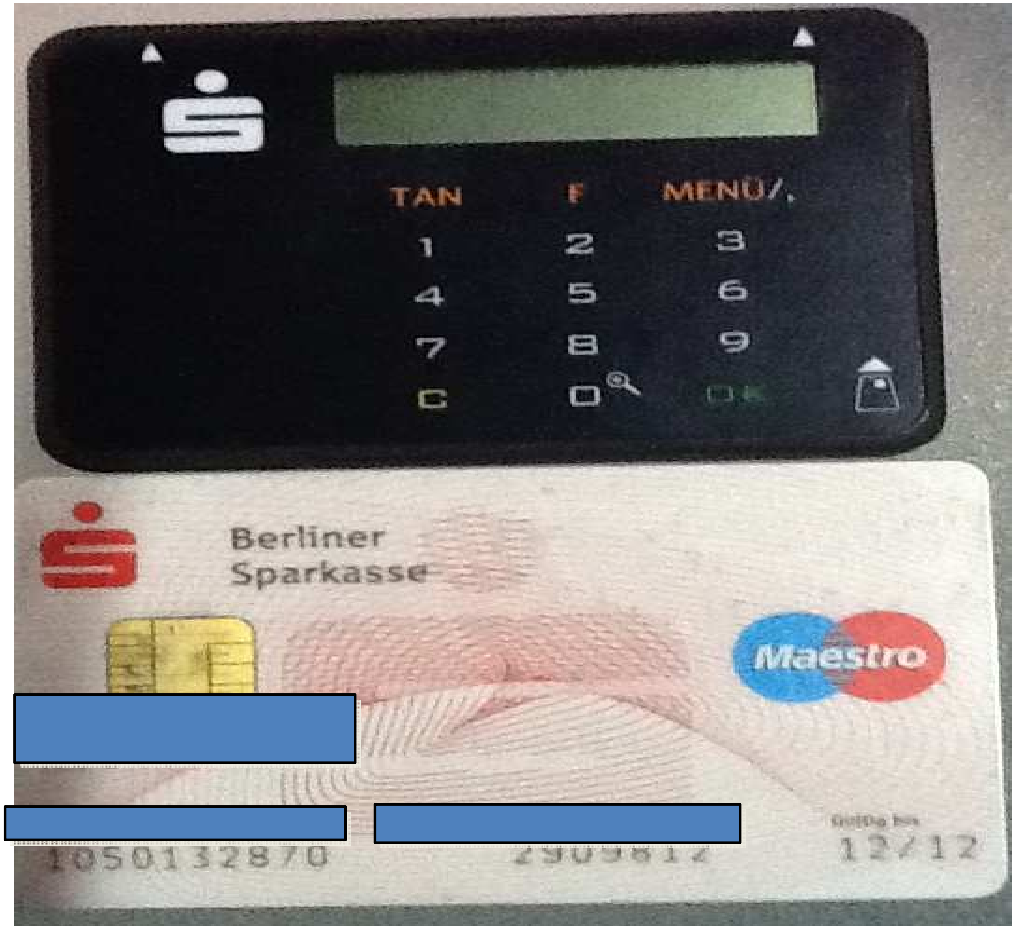


Achieving Security Objectives

Integrity

Something you have

- **Tokens**
- **Tan Lists**



[redacted]

[redacted]

[redacted]

Achieving Security Objectives

Integrity

- **Something about you**

Achieving Security Objectives

Integrity

Logging and monitoring

Thank you!

QUESTIONS