Security by design

Jan Joris Vereijken

Chief Technology Officer @ Crunchr

Amsterdam, September 23th, 2024

University of Amsterdam

crunchr

About me

ING 2001 - 2017

crunchr 2018 - now

Prelude

What is security by design?

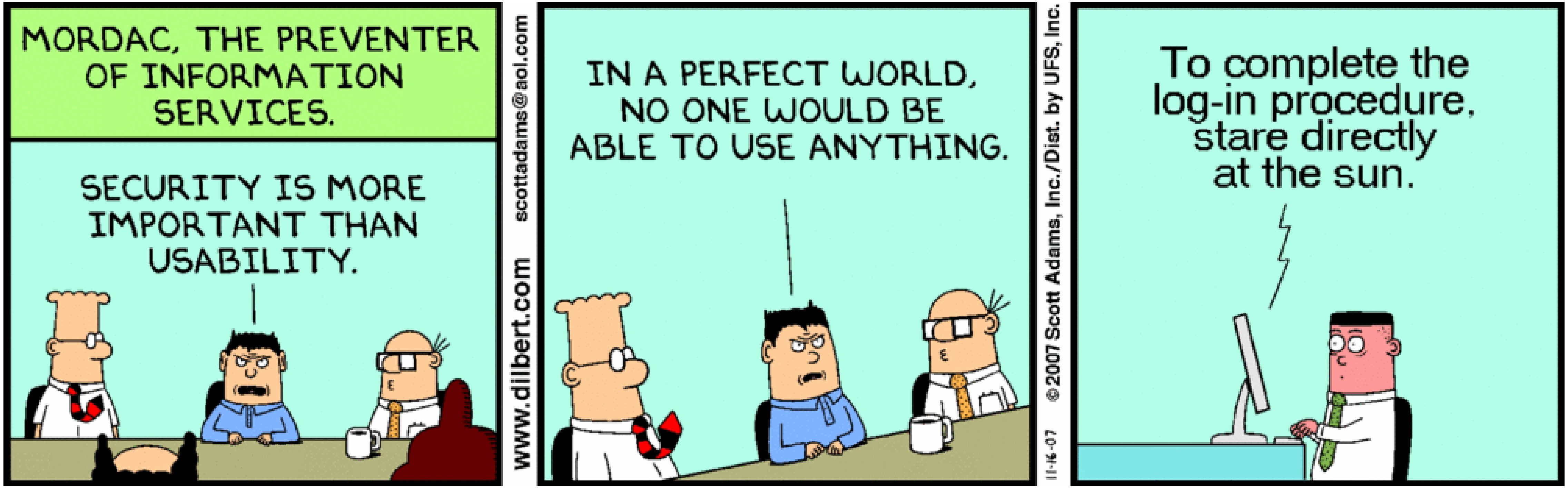
crunchr

Bridge design...

Principles

Principle #1: Help the user

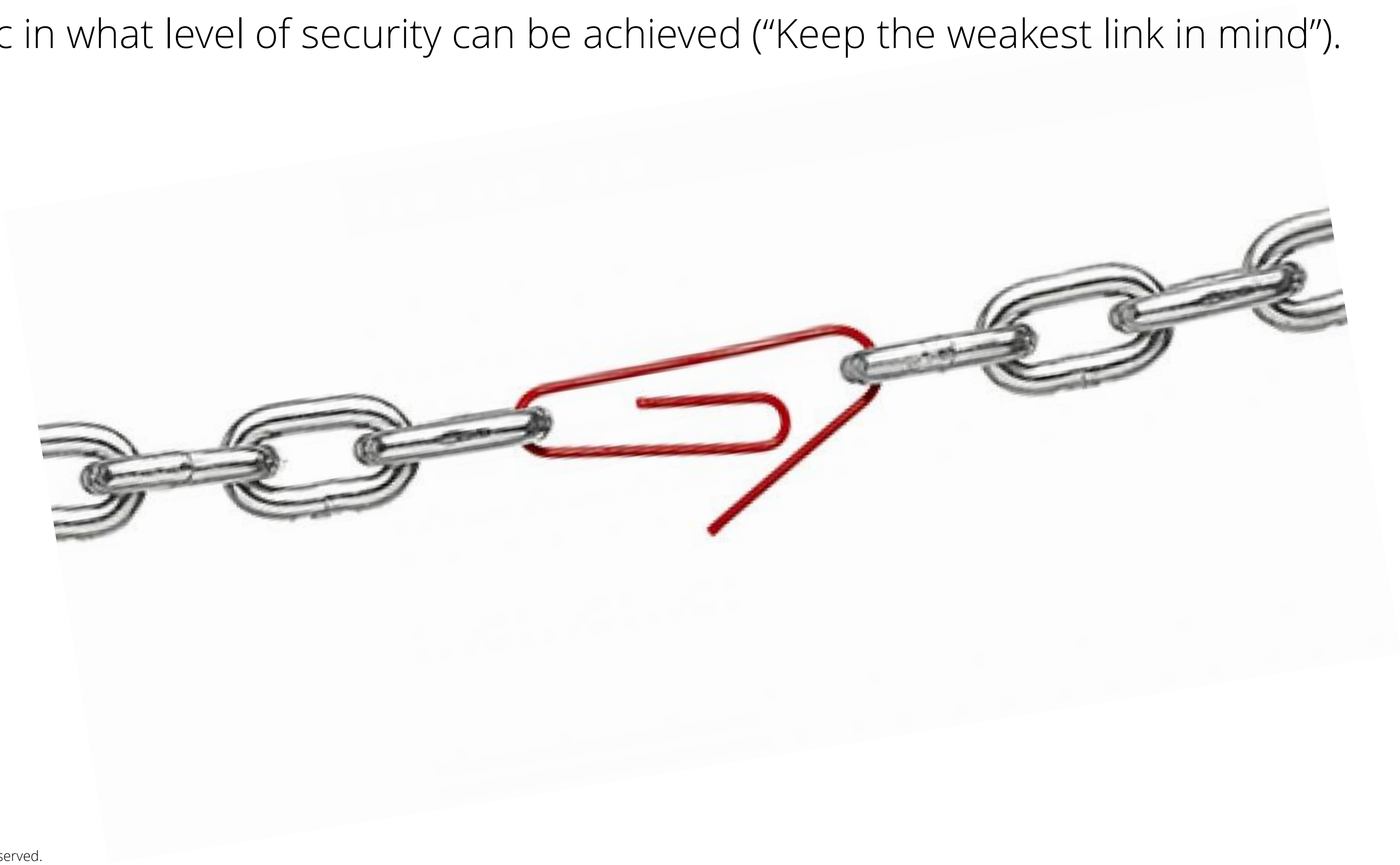
Help the user, don’t hinder him (“Don’t be the Business Prevention Departement”).


MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
11-16-07
To complete the log-in procedure, stare directly at the sun.

crunchr

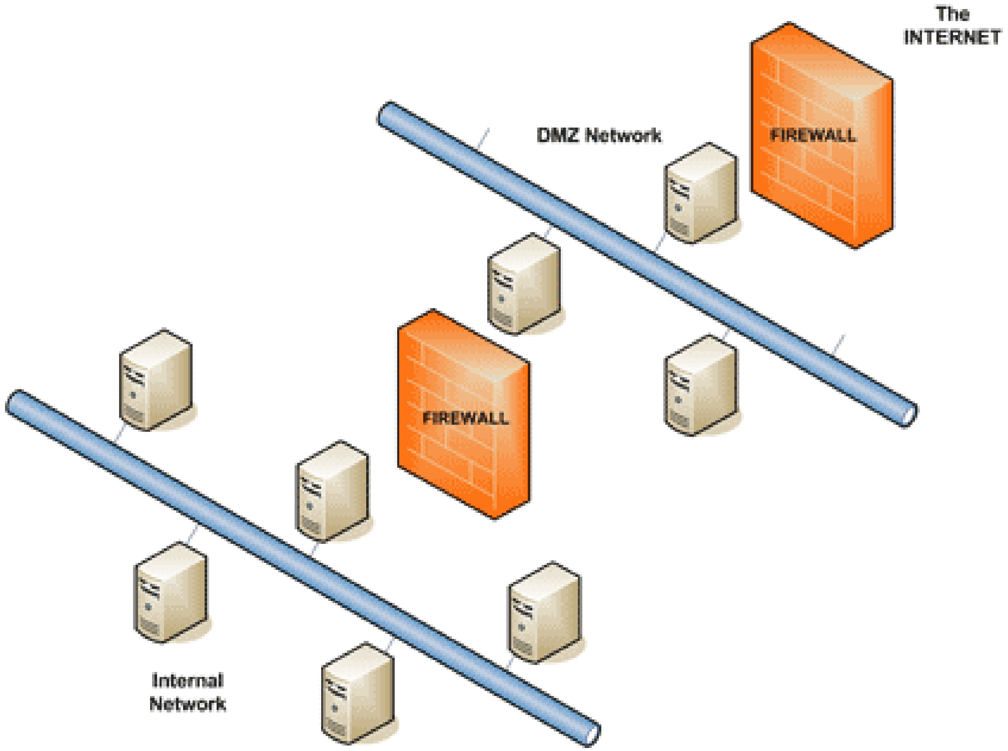
Principle #2: Be realistic

Be realistic in what level of security can be achieved (“Keep the weakest link in mind”).



Principle #3: Be conservative

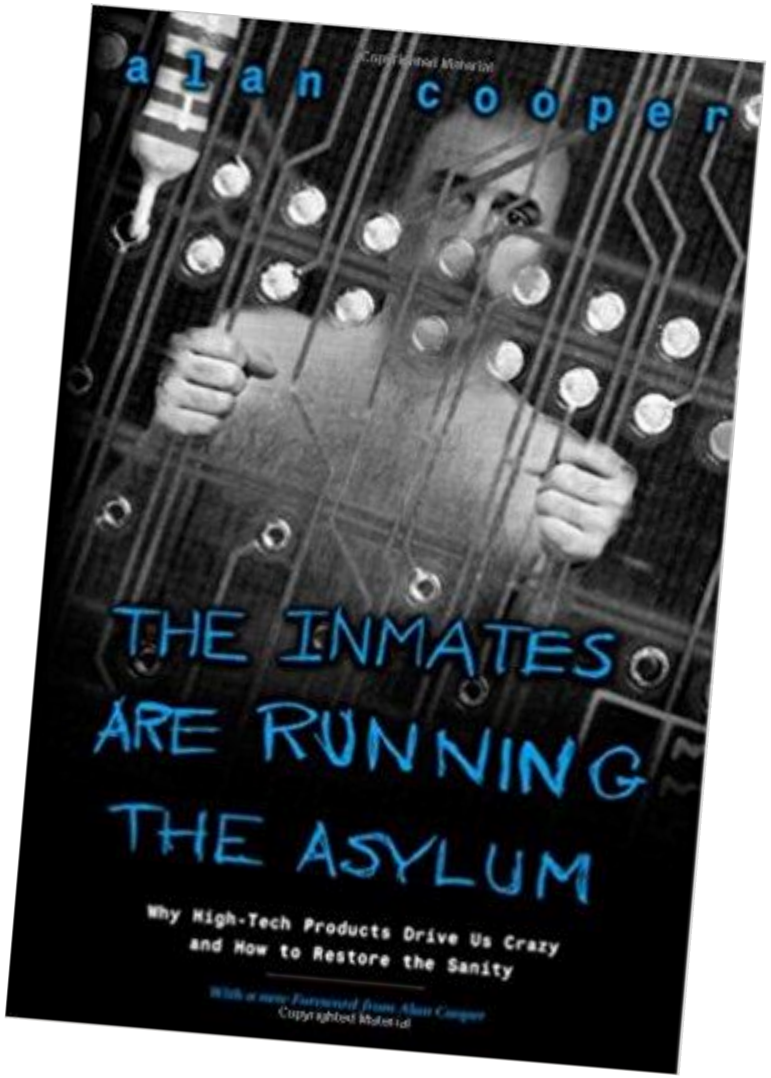
Be conservative ("Defense in depth, prepare for failure").



Principle #4: Embrace the ignorance

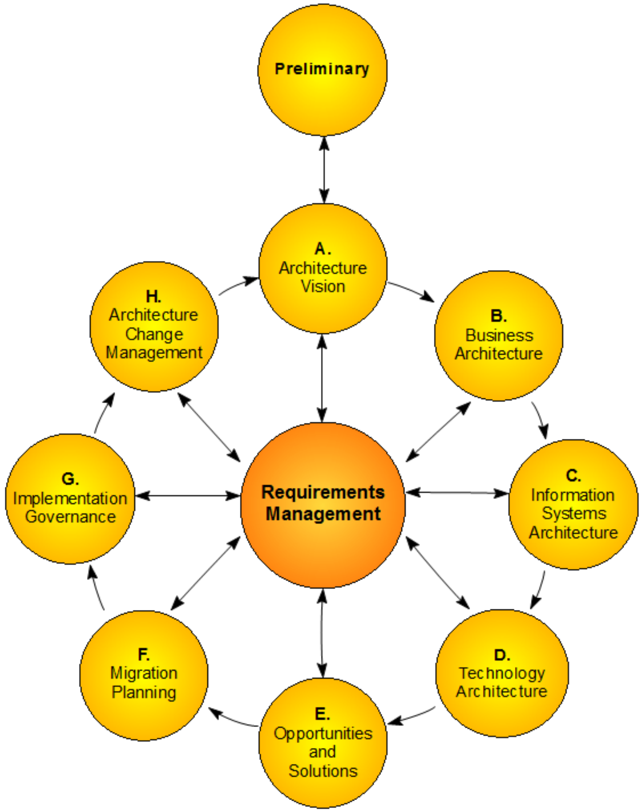
Embrace the ignorance of the user.

It’s you who’s the idiot! (and me too)


alan cooper
THE INMATES ARE RUNNING THE ASYLUM
Why High-Tech Products Drive Us Crazy and How to Restore the Sanity
With a new Foreword from Alan Cooper
Copyrighted Material

Principle #5: Apply security throughout

Apply security throughout the whole design cycle ("pervasive security").


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architecture
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

Principles:

1) **Help the user**, don’t hinder him (“Don’t be the Business Prevention Departement”)

2) **Be realistic** in what level of security can be achieved (“Keep the weakest link in mind”)

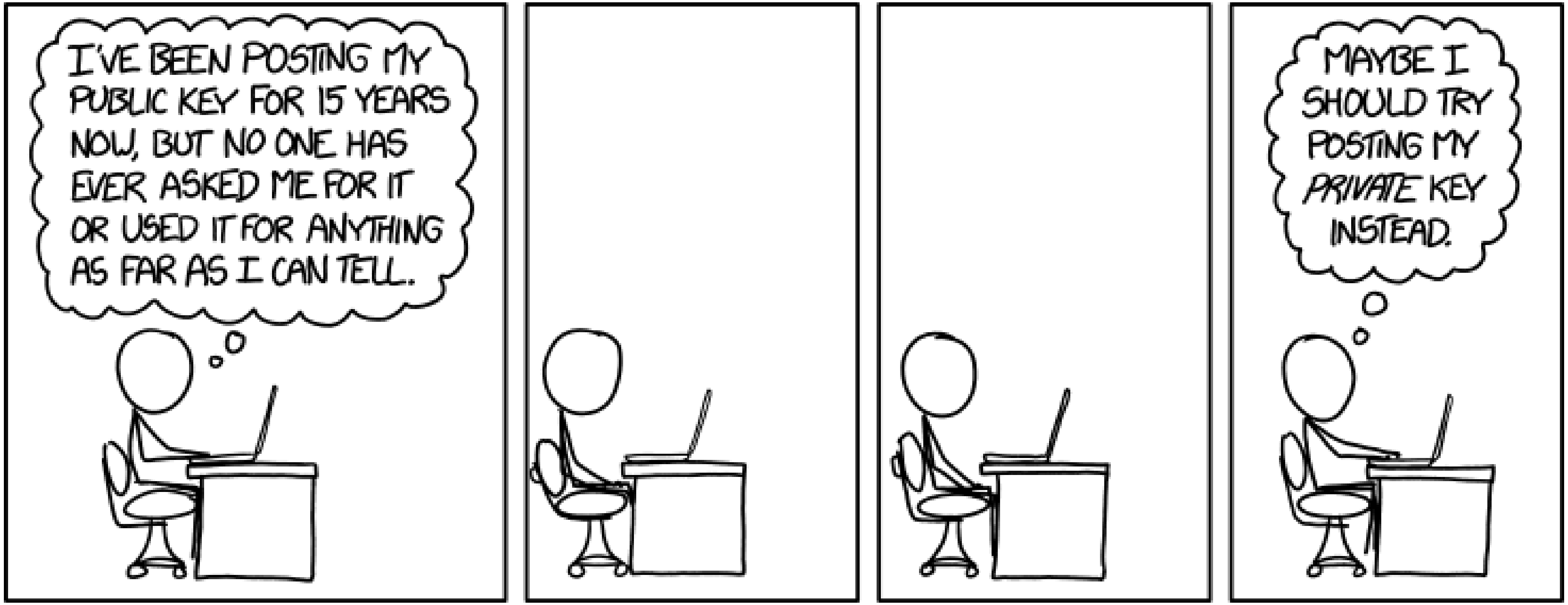
3) **Be conservative** (“Defense in depth”)

4) **Embrace the ignorance** of the user (“It’s you who’s the idiot!”)

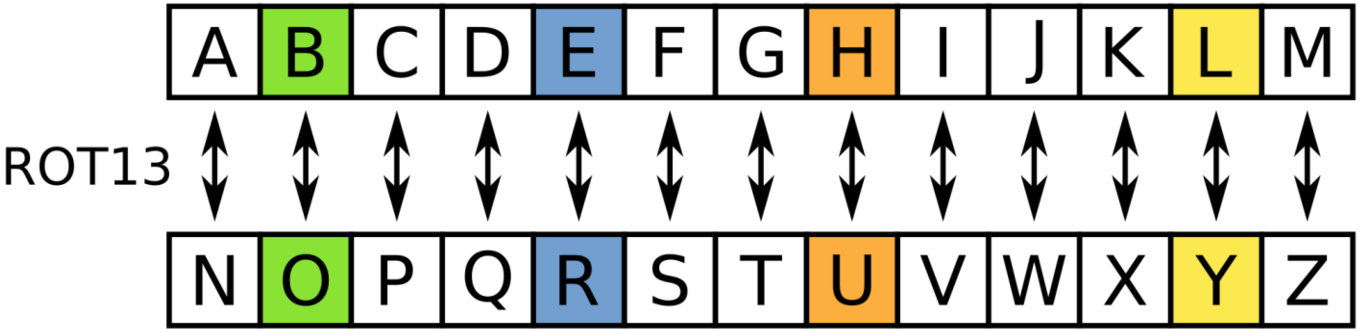
5) **Apply security throughout** the whole design cycle (“Pervasive security”)

Crypto

Crypto...


I'VE BEEN POSTING MY PUBLIC KEY FOR 15 YEARS NOW, BUT NO ONE HAS EVER ASKED ME FOR IT OR USED IT FOR ANYTHING AS FAR AS I CAN TELL.
MAYBE I SHOULD TRY POSTING MY *PRIVATE* KEY INSTEAD.

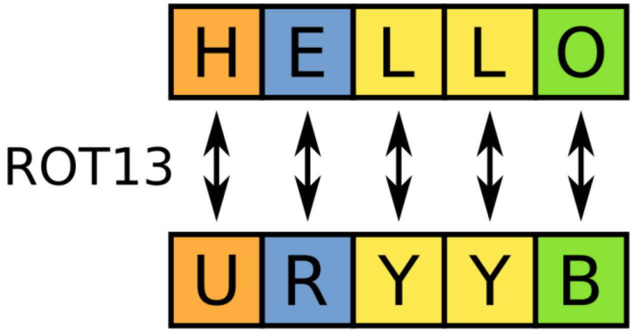
Why do crypto?



A B C D E F G H I J K L M

ROT13

N O P Q R S T U V W X Y Z



H E L L O

ROT13

U R Y Y B

Problems with crypto

- Symmetric crypto: key management
- Asymmetric crypto: also key management!
- Bugs in implementations of crypto libraries
- PKI: trusting certificate authorities
- Ignorant end-users

Problems with crypto

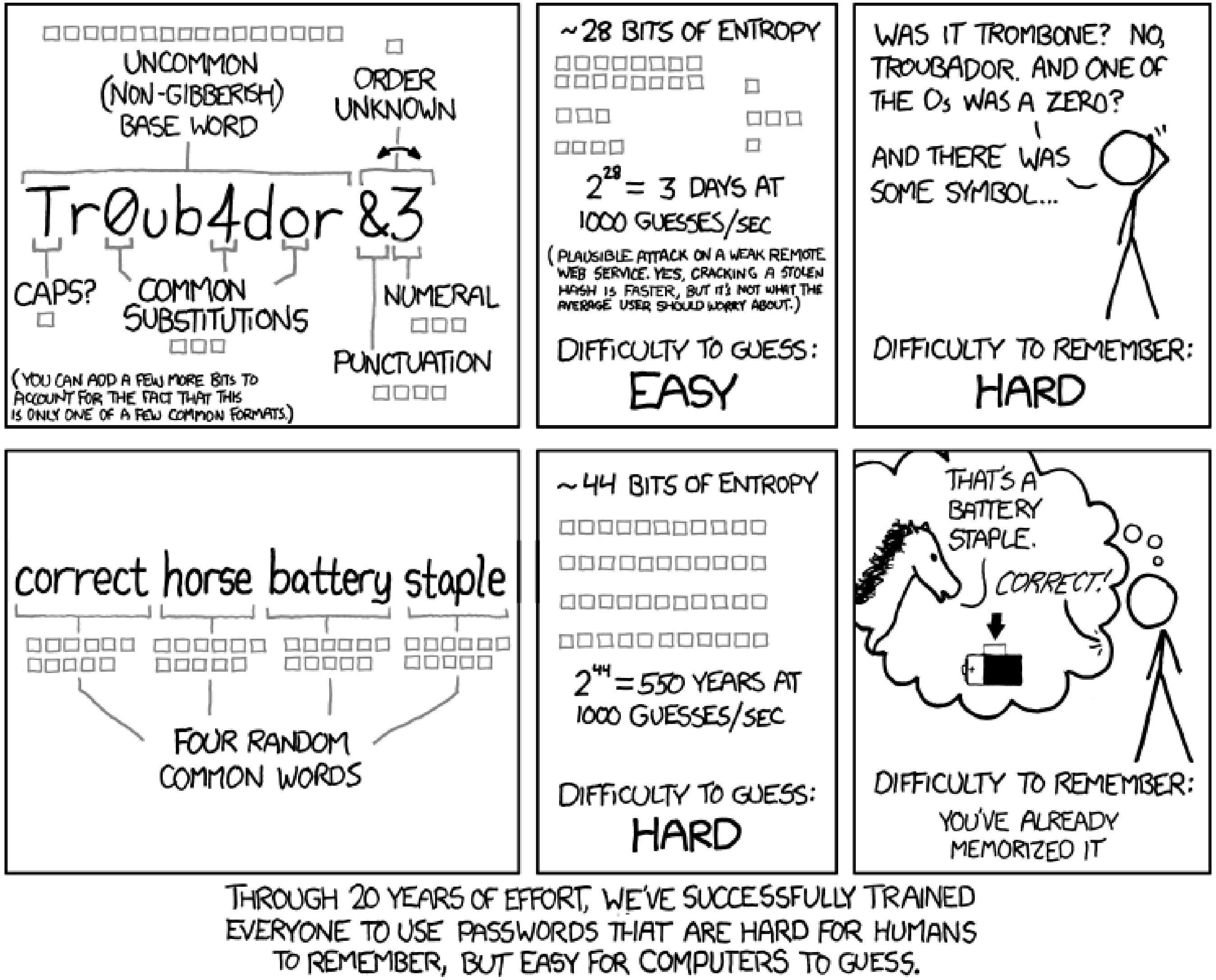
- Symmetric crypto: key management
- Asymmetric crypto: also key management!
- Bugs in implementations of crypto libraries
- PKI: trusting certificate authorities
- Ignorant end-users

Which principle applies most?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

Authentication & authorization

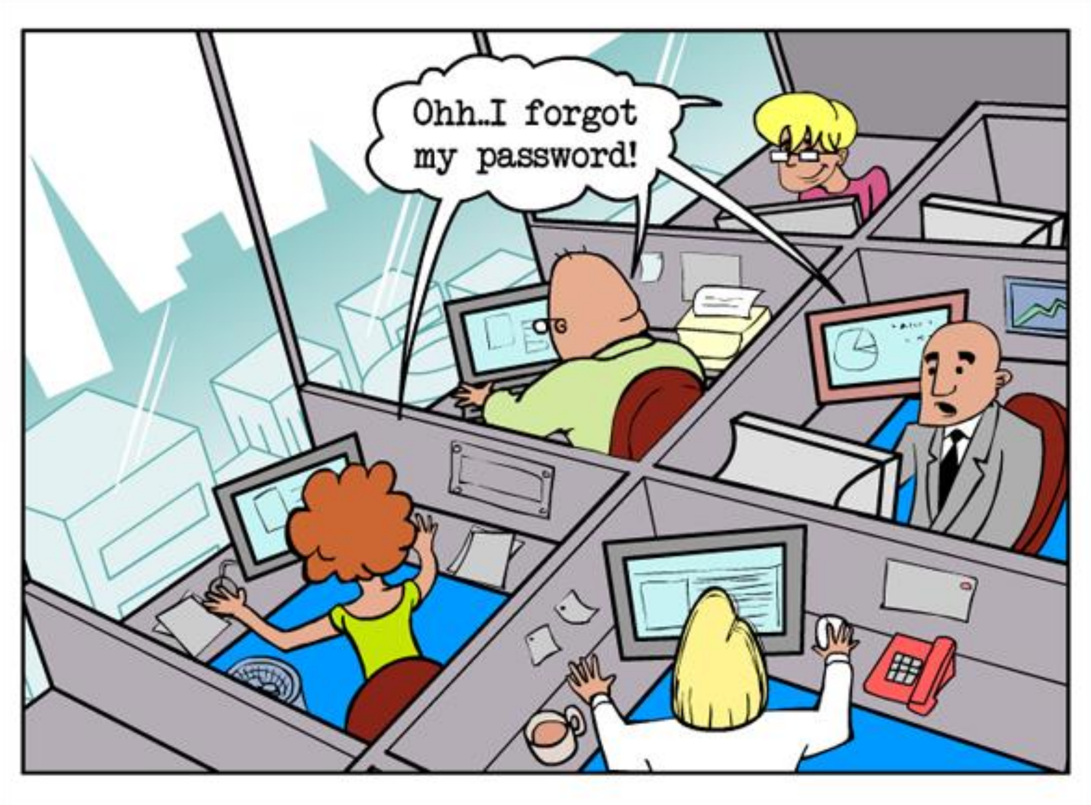
Authentication…


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Why do authentication and authorization?

Problems with authentication

- Credential reset
- Passwords: complexity
- Passwords: reuse
- Passwords: phishing
- Tokens: cost!
- Tokens: enrollment
- Voice: enrollment
- Voice: revocation



Real life attacks & cases

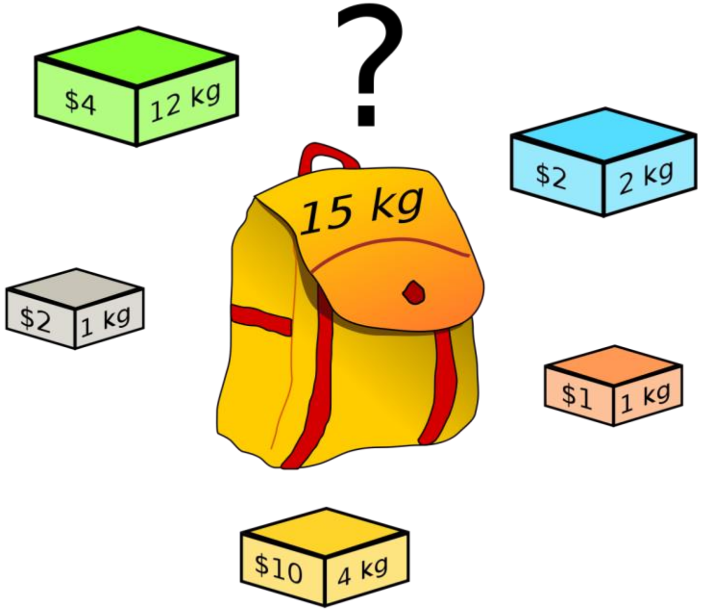
Real life attacks and cases

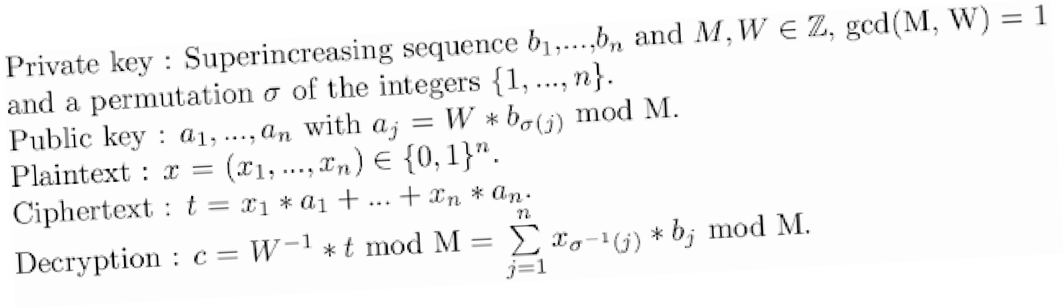
- Broken crypto implementations
- Malware
- Man-in-the-middle attacks
- Physical attacks
- Data driven attacks
- Social Engineering

DANG...I KNEW WE SHOULD'VE STORMED THE CASTLE BEFORE IT GOT TRENDY...
7-17

Broken crypto implementations

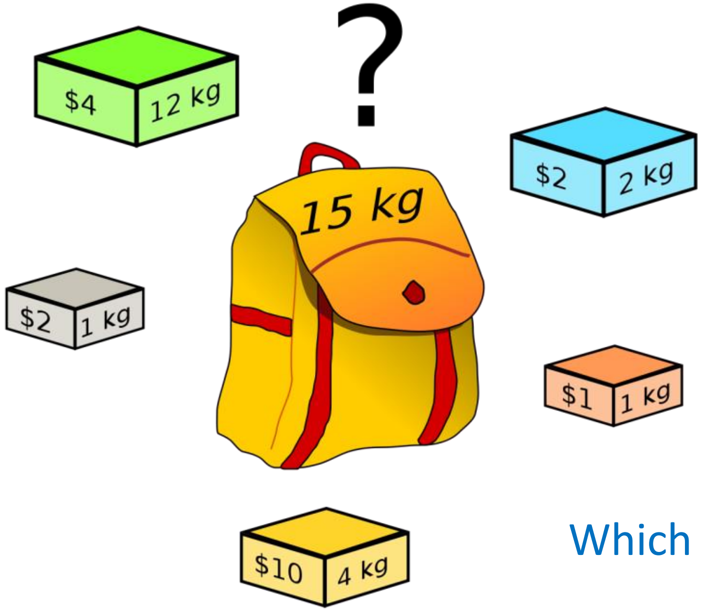
Broken crypto implementations: Case #1 – The Knapsack cryptosystem

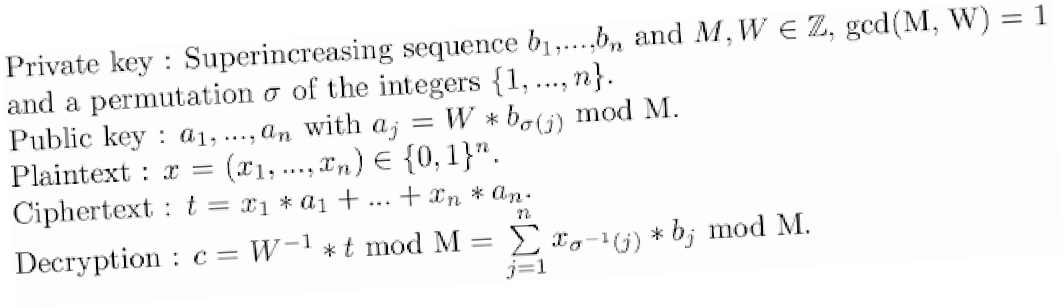




Private key : Superincreasing sequence $b_1,...,b_n$ and $M, W \in \mathbb{Z}$, gcd(M, W) = 1
and a permutation σ of the integers $\{1, ..., n\}$.
Public key : $a_1, ..., a_n$ with $a_j = W * b_{\sigma(j)}$ mod M.
Plaintext : $x = (x_1, ..., x_n) \in \{0, 1\}^n$.
Ciphertext : $t = x_1 * a_1 + ... + x_n * a_n$.
Decryption : $c = W^{-1} * t \text{ mod M} = \sum_{j=1}^{n} x_{\sigma^{-1}(j)} * b_j$ mod M.

Broken crypto implementations: Case #1 – The Knapsack cryptosystem





Private key : Superincreasing sequence $b_1,...,b_n$ and $M, W \in \mathbb{Z}$, gcd(M, W) = 1 and a permutation σ of the integers $\{1, ..., n\}$.

Public key : $a_1, ..., a_n$ with $a_j = W * b_{\sigma(j)}$ mod M.

Plaintext : $x = (x_1, ..., x_n) \in \{0, 1\}^n$.

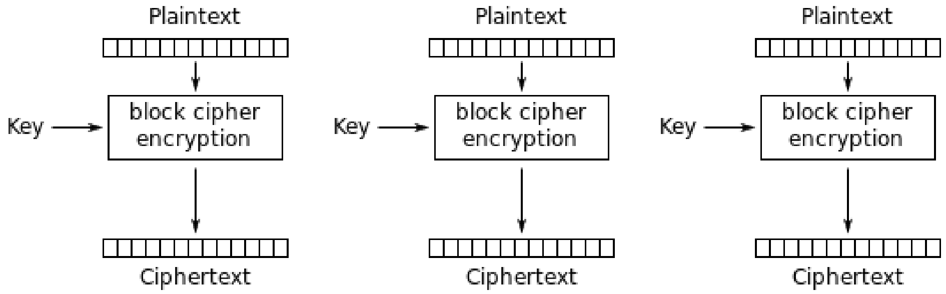
Ciphertext : $t = x_1 * a_1 + ... + x_n * a_n$.

Decryption : $c = W^{-1} * t \text{ mod M} = \sum_{j=1}^{n} x_{\sigma^{-1}(j)} * b_j \text{ mod M}$.

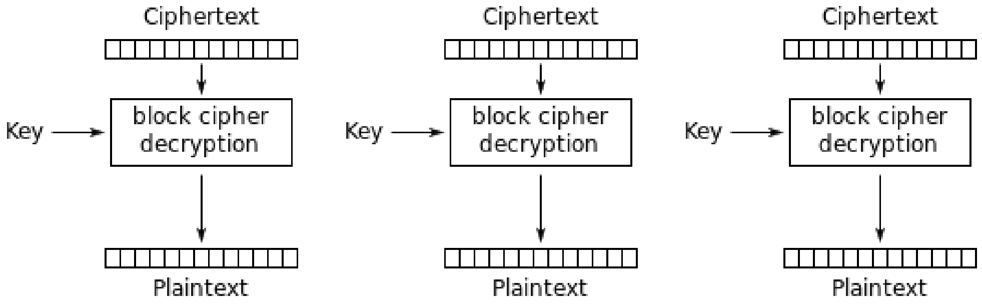
Which principle applies most?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

Broken crypto implementations: Case #2 – The encrypted Penguin 1/3

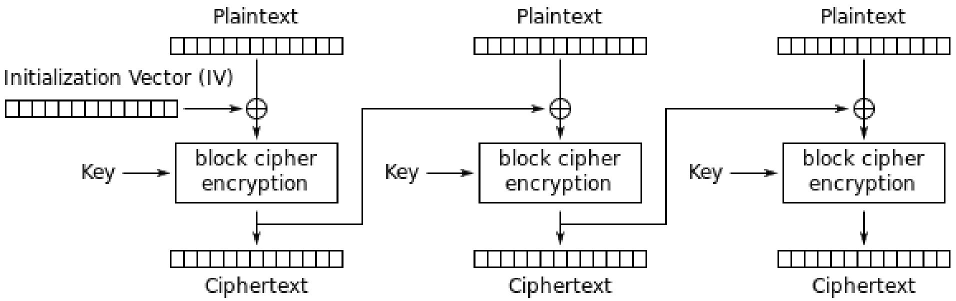


Electronic Codebook (ECB) mode encryption

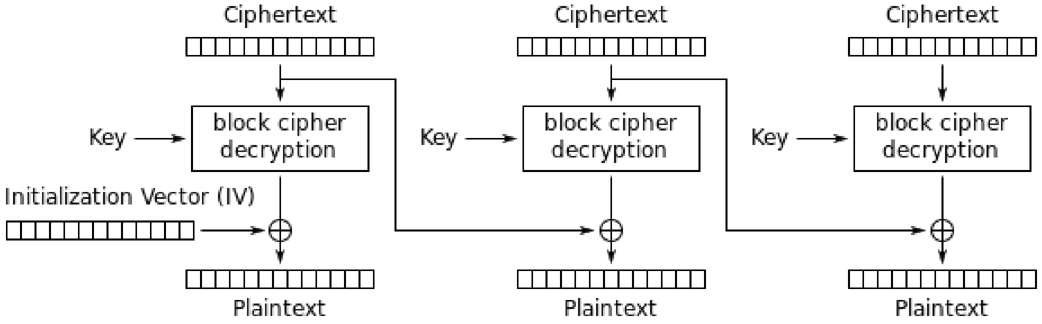


Electronic Codebook (ECB) mode decryption

Broken crypto implementations: Case #2 – The encrypted Penguin 2/3

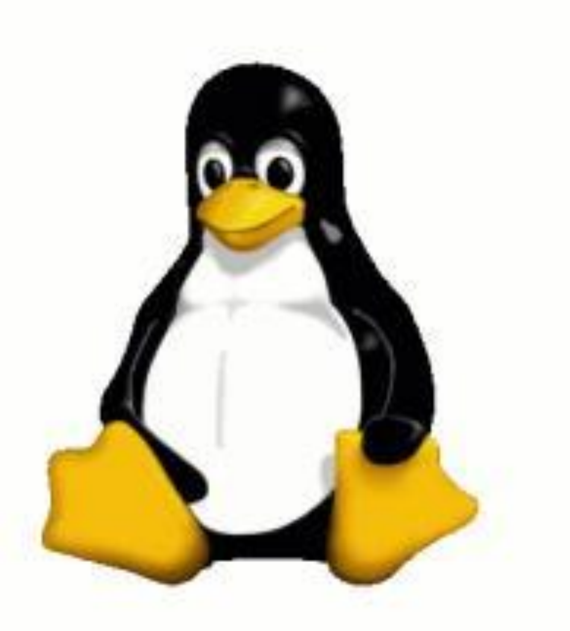


Cipher Block Chaining (CBC) mode encryption

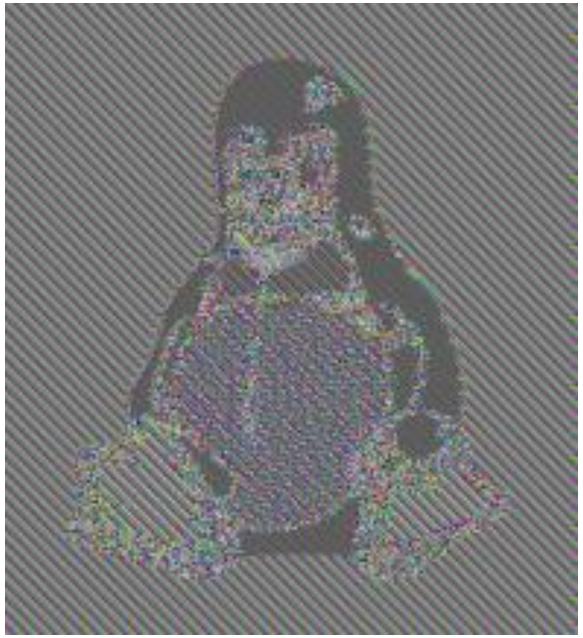


Cipher Block Chaining (CBC) mode decryption

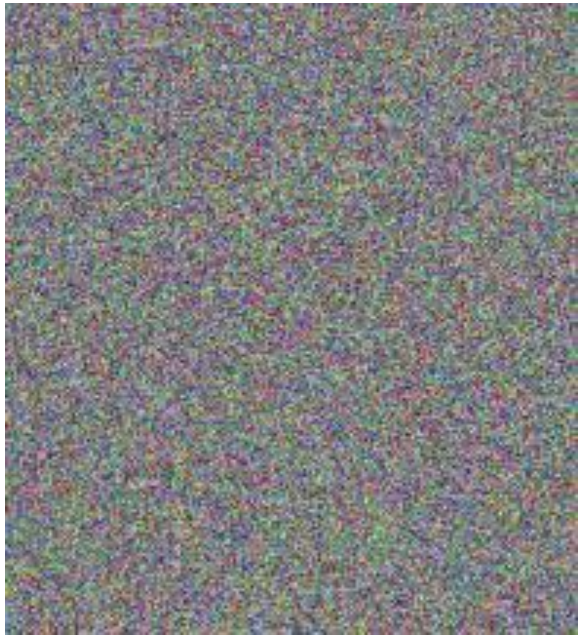
Broken crypto implementations: Case #2 – The encrypted Penguin 3/3



Plaintext

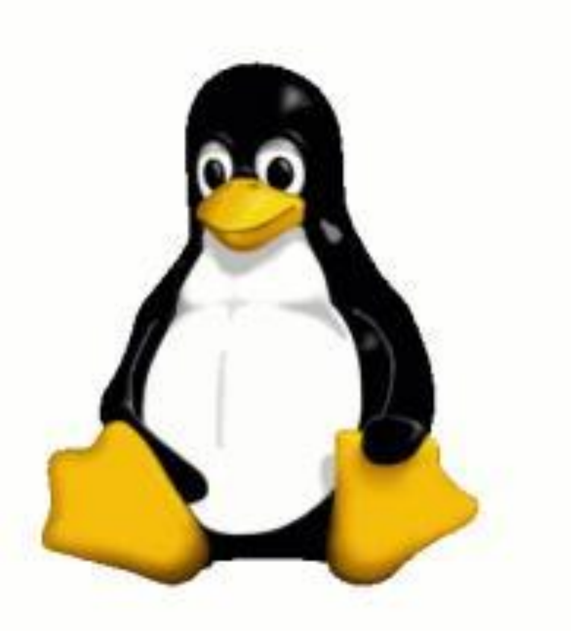


Ciphertext (ECB)

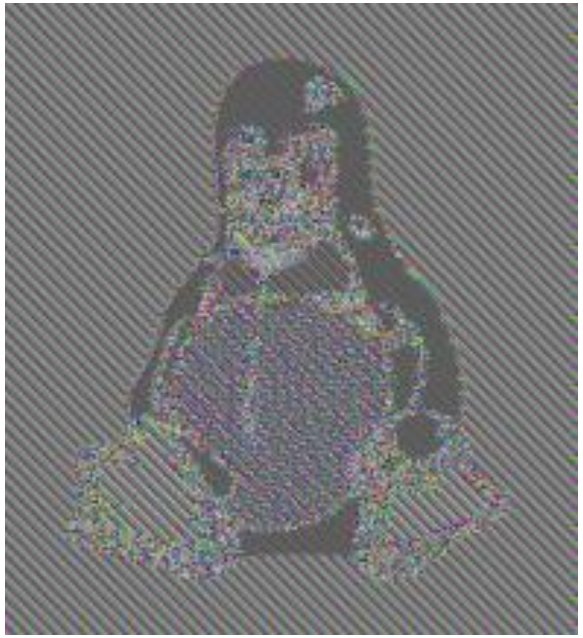


Ciphertext (CBC)

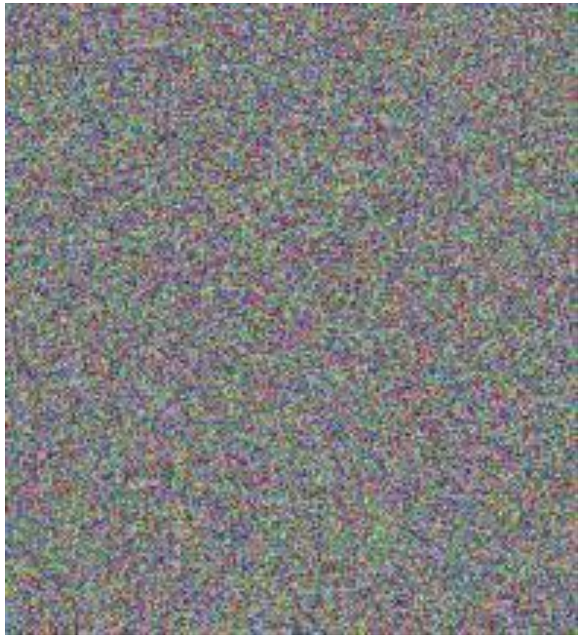
Broken crypto implementations: Case #2 – The encrypted Penguin 3/3



Plaintext



Ciphertext (ECB)



Ciphertext (CBC)

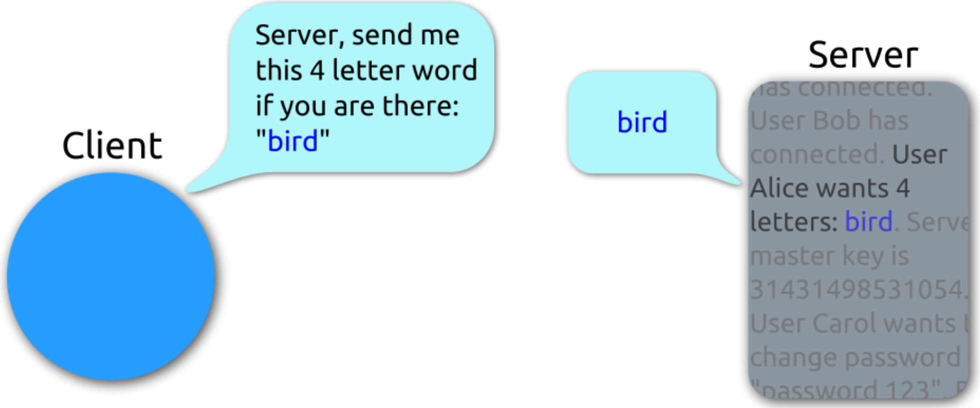
What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

Broken crypto implementations: Case #3 – Heartbleed

OpenSSL
Cryptography and SSL/TLS Toolkit

Heartbeat – Normal usage



Client

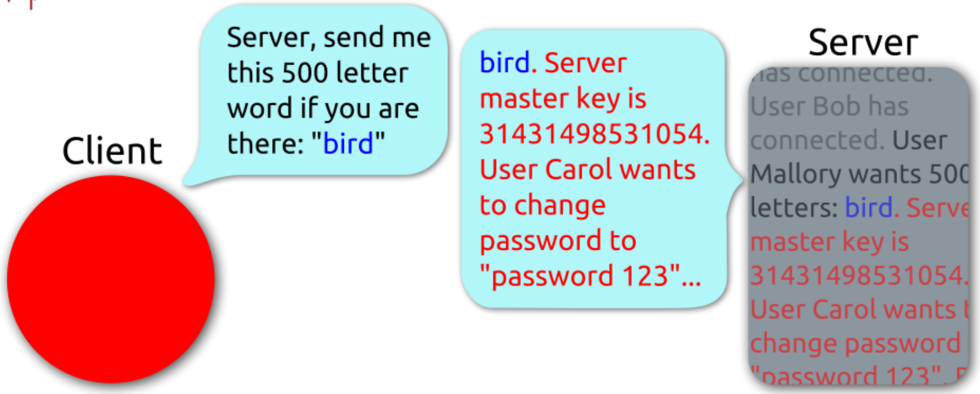
Server, send me this 4 letter word if you are there: "bird"

bird

Server

as connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

Heartbeat – Malicious usage



Client

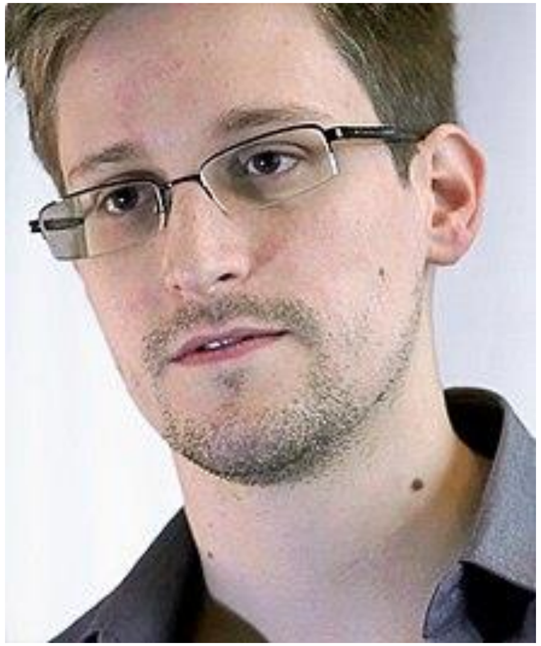
Server, send me this 500 letter word if you are there: "bird"

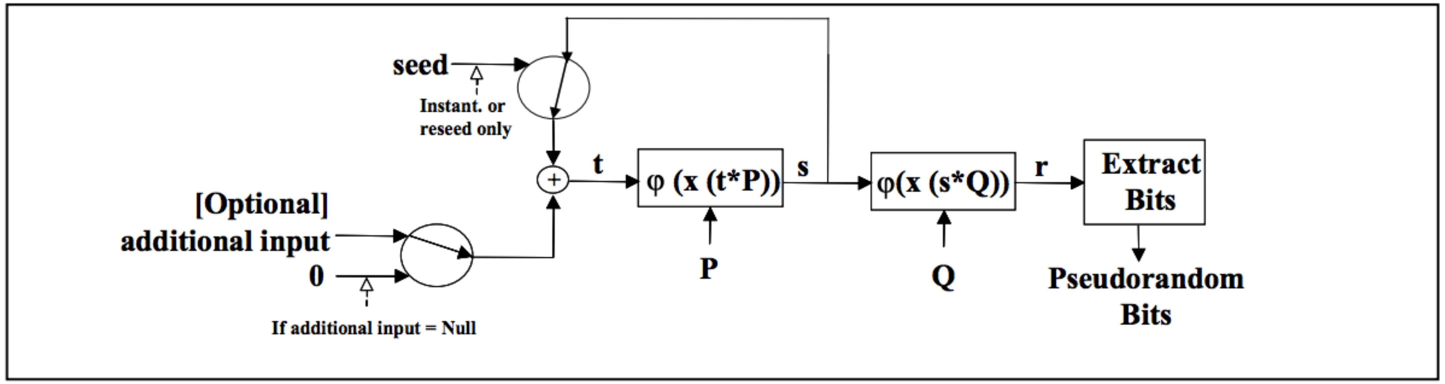
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...

Server

as connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

Broken crypto implementations: Case #4 – RSA BSAFE





seed

Instant. or reseed only

[Optional] additional input

0

If additional input = Null

t

φ (x (t*P))

P

s

φ(x (s*Q))

Q

r

Extract Bits

Pseudorandom Bits

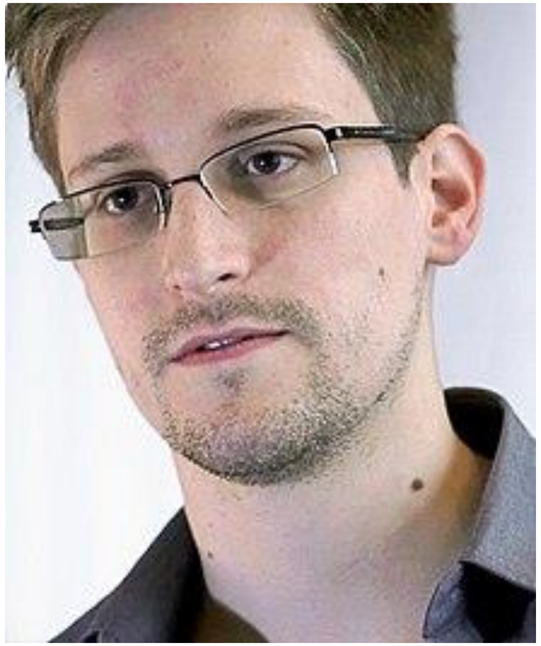
RSA BSAFE®

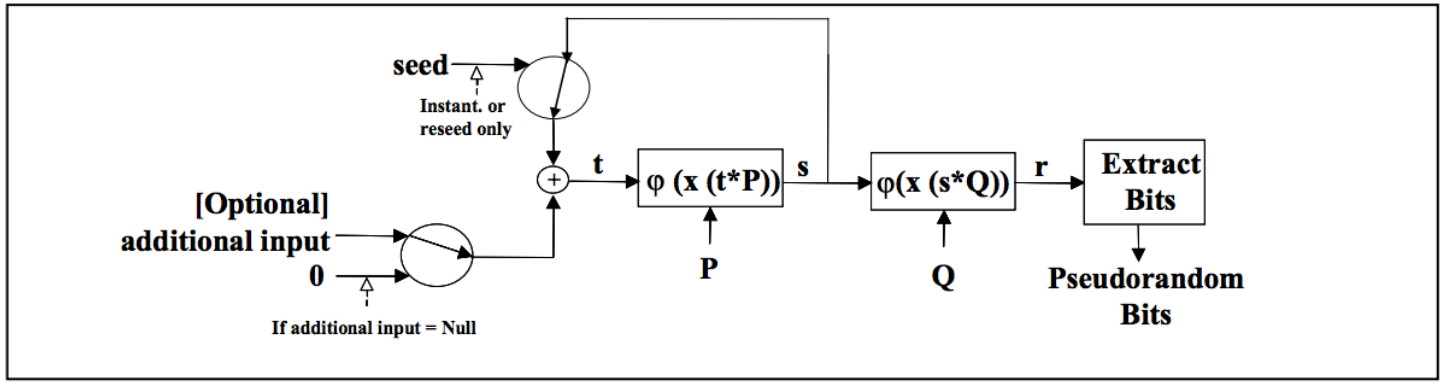
NIST

National Institute of Standards and Technology

U.S. Department of Commerce

Broken crypto implementations: Case #4 – RSA BSAFE





RSA BSAFE®

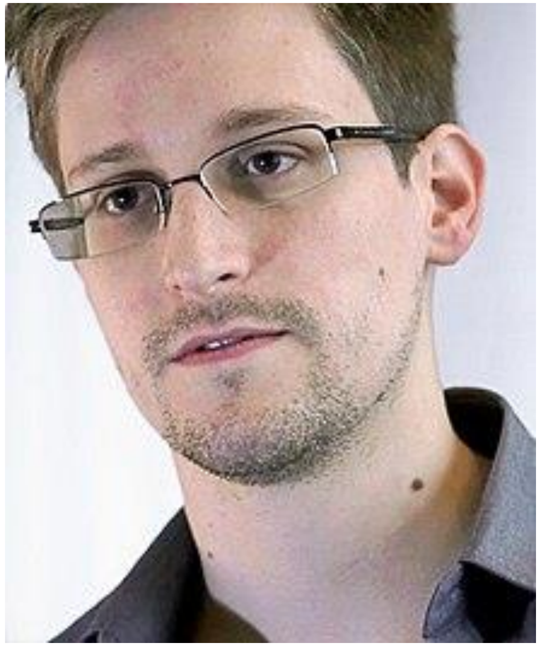
National Institute of Standards and Technology
U.S. Department of Commerce

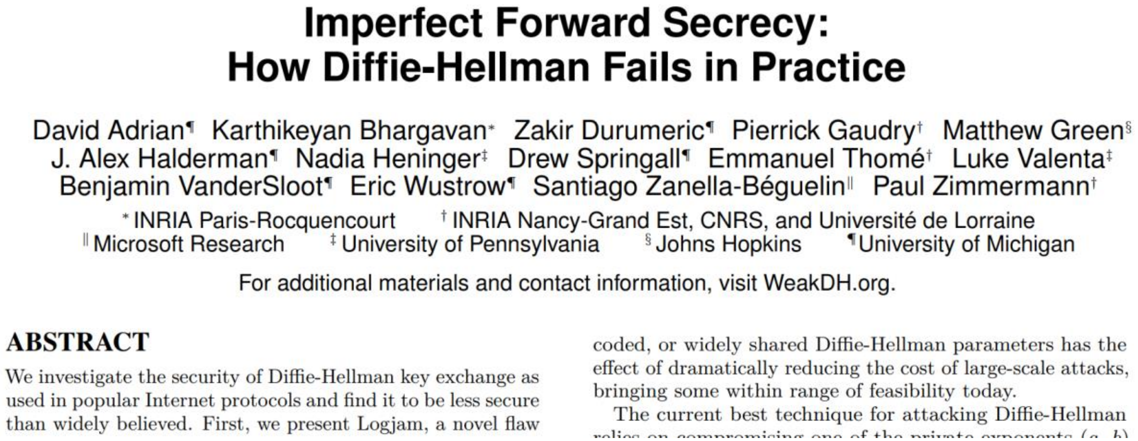
What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

crunchr

Broken crypto implementations: Case #5 – Weak Diffie-Hellman





Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice

David Adrian[¶] Karthikeyan Bhargavan[*] Zakir Durumeric[¶] Pierrick Gaudry[†] Matthew Green[§]
J. Alex Halderman[¶] Nadia Heninger[‡] Drew Springall[¶] Emmanuel Thomé[†] Luke Valenta[‡]
Benjamin VanderSloot[¶] Eric Wustrow[¶] Santiago Zanella-Béguelin[||] Paul Zimmermann[†]

[*] INRIA Paris-Rocquencourt [†] INRIA Nancy-Grand Est, CNRS, and Université de Lorraine
[||] Microsoft Research [‡] University of Pennsylvania [§] Johns Hopkins [¶]University of Michigan

For additional materials and contact information, visit WeakDH.org.

ABSTRACT

We investigate the security of Diffie-Hellman key exchange as used in popular Internet protocols and find it to be less secure than widely believed. First, we present Logjam, a novel flaw

coded, or widely shared Diffie-Hellman parameters has the effect of dramatically reducing the cost of large-scale attacks, bringing some within range of feasibility today.

The current best technique for attacking Diffie-Hellman relies on compromising one of the private exponents (a, b)

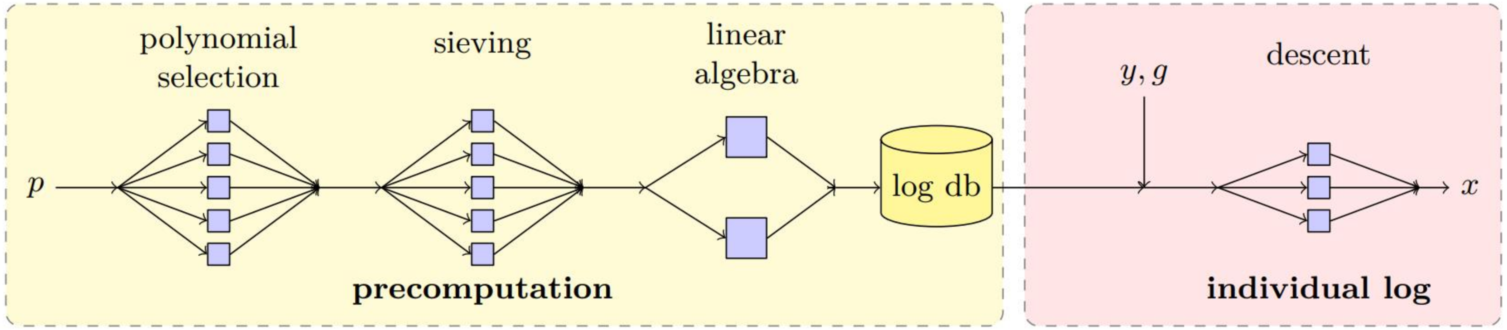
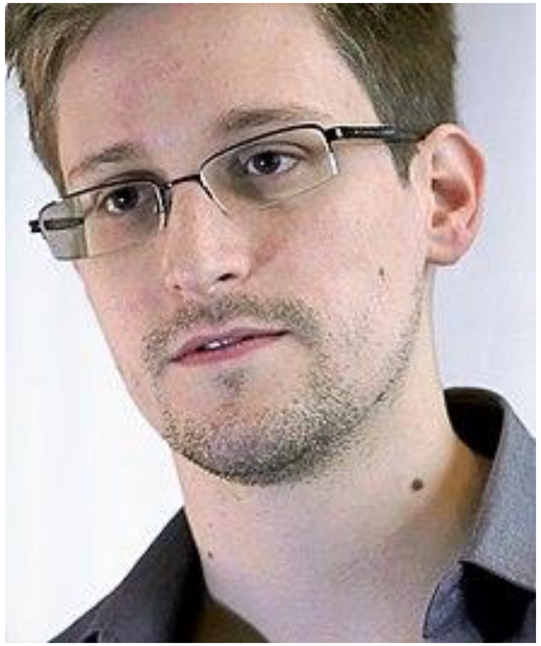
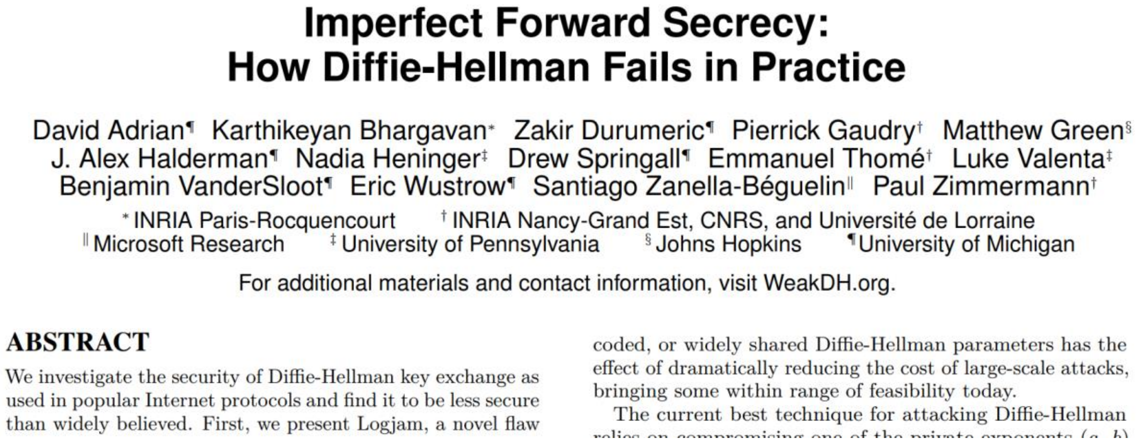


Figure 1: **The number field sieve algorithm for discrete log** consists of a precomputation stage that depends only on the prime p and a descent stage that computes individual logs. With sufficient precomputation, an attacker can quickly break any Diffie-Hellman instances that use a particular p.

Broken crypto implementations: Case #5 – Weak Diffie-Hellman





Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice

David Adrian[¶] Karthikeyan Bhargavan[*] Zakir Durumeric[¶] Pierrick Gaudry[†] Matthew Green[§]
J. Alex Halderman[¶] Nadia Heninger[‡] Drew Springall[¶] Emmanuel Thomé[†] Luke Valenta[‡]
Benjamin VanderSloot[¶] Eric Wustrow[¶] Santiago Zanella-Béguelin[‖] Paul Zimmermann[†]

[*] INRIA Paris-Rocquencourt [†] INRIA Nancy-Grand Est, CNRS, and Université de Lorraine
[‖] Microsoft Research [‡] University of Pennsylvania [§] Johns Hopkins [¶] University of Michigan

For additional materials and contact information, visit WeakDH.org.

ABSTRACT

We investigate the security of Diffie-Hellman key exchange as used in popular Internet protocols and find it to be less secure than widely believed. First, we present Logjam, a novel flaw coded, or widely shared Diffie-Hellman parameters has the effect of dramatically reducing the cost of large-scale attacks, bringing some within range of feasibility today.

The current best technique for attacking Diffie-Hellman relies on compromising one of the private exponents (a, b)

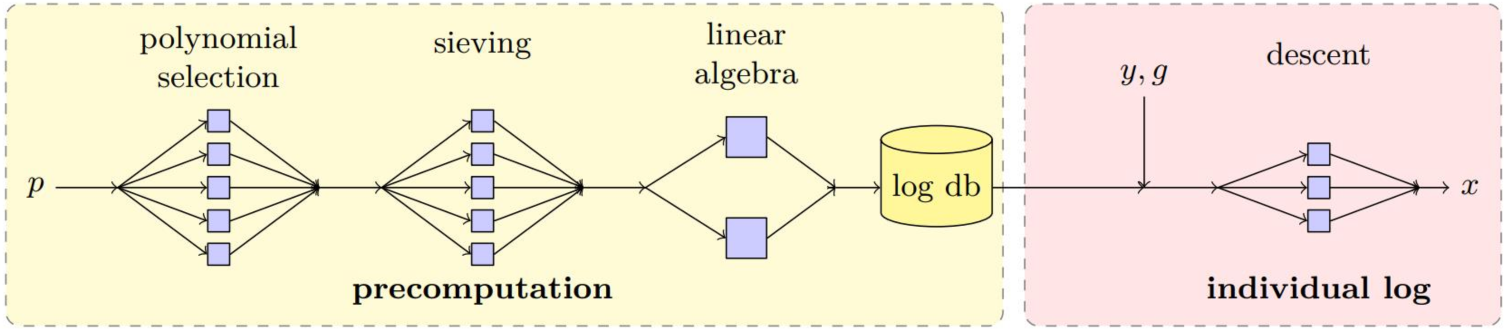
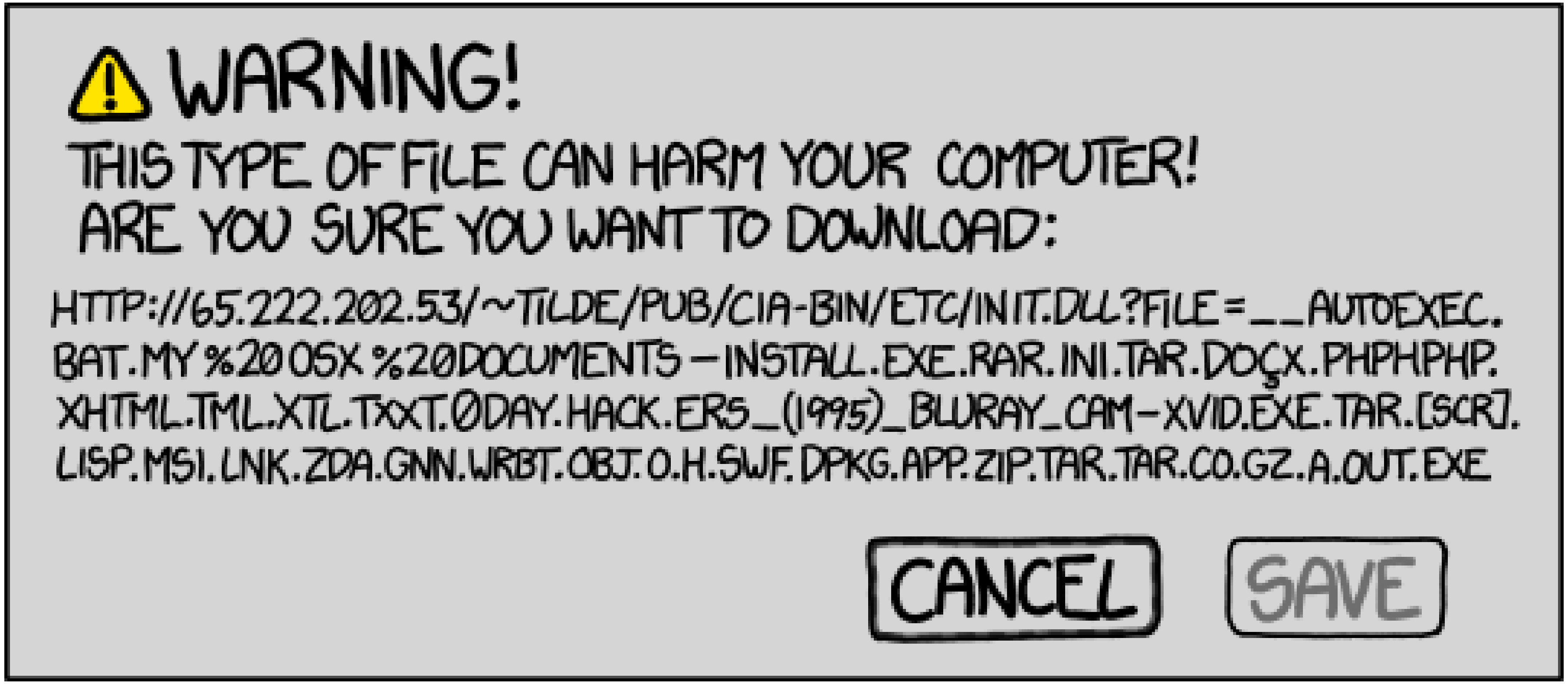


Figure 1: **The number field sieve algorithm for discrete log** consists of a precomputation stage that depends only on the prime p and a descent stage that computes individual logs. With sufficient precomputation, an attacker can quickly break any Diffie-Hellman instances that use a particular p.

What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

Malware

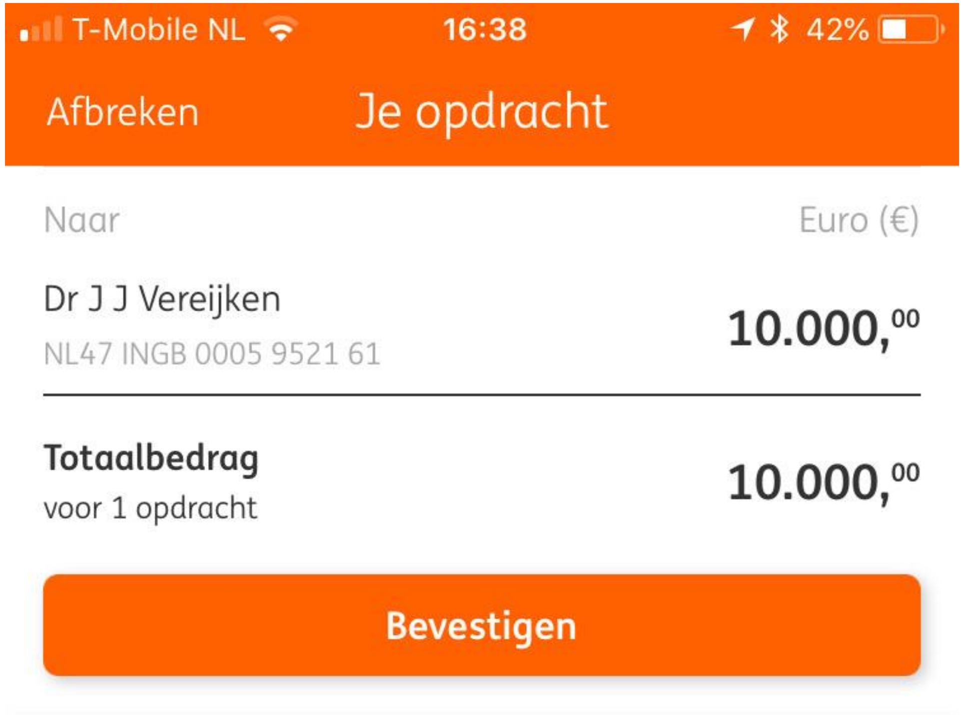


WARNING!

THIS TYPE OF FILE CAN HARM YOUR COMPUTER!
ARE YOU SURE YOU WANT TO DOWNLOAD:

HTTP://65.222.202.53/~TILDE/PUB/CIA-BIN/ETC/INIT.DLL?FILE=__AUTOEXEC.
BAT.MY%20OSX%20DOCUMENTS—INSTALL.EXE.RAR.INI.TAR.DOÇX.PHPHPHP.
XHTML.TML.XTL.TXXT.ØDAY.HACK.ERS_(1995)_BLURAY_CAM—XVID.EXE.TAR.[SCR].
LISP.MSI.LNK.ZDA.GNN.WRBT.OBJ.O.H.SWF.DPKG.APP.ZIP.TAR.TAR.CO.GZ.A.OUT.EXE

Malware: Case #1 – ING Mobiel Goedkeuren versus Rabo Scanner

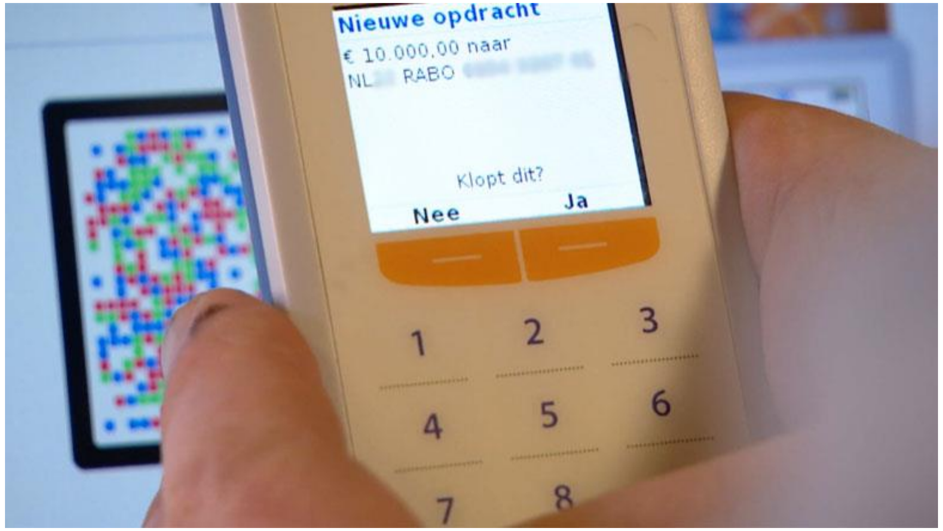


T-Mobile NL 16:38 42%

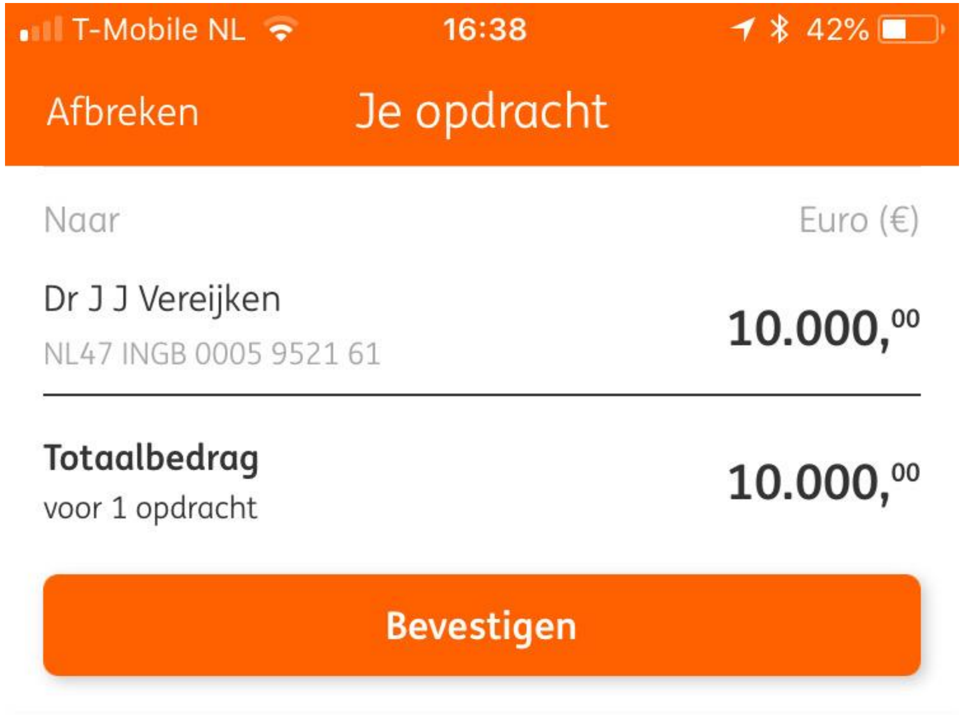
Afbreken Je opdracht

Naar	Euro (€)
Dr J J Vereijken NL47 INGB 0005 9521 61	10.000,^{00}
Totaalbedrag voor 1 opdracht	10.000,^{00}

Bevestigen



Malware: Case #1 – ING Mobiel Goedkeuren versus Rabo Scanner

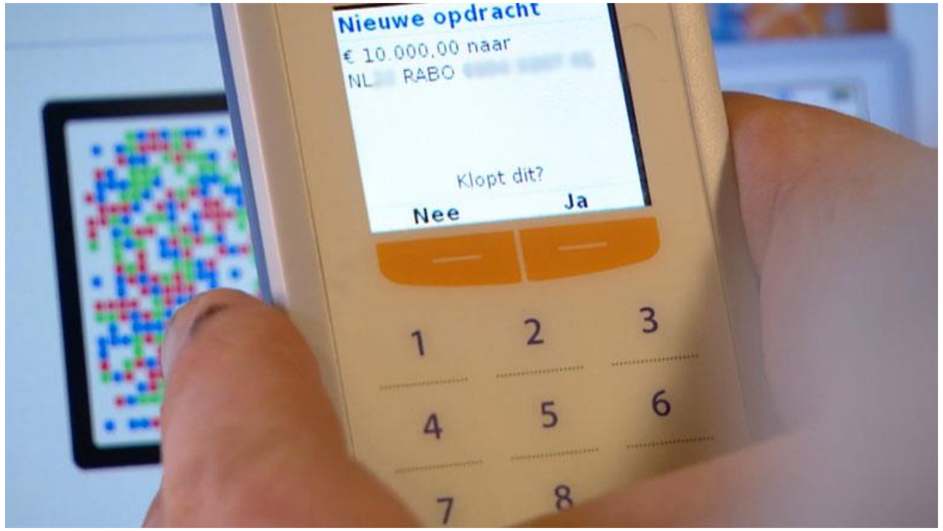


T-Mobile NL 16:38 42%

Afbreken Je opdracht

Naar	Euro (€)
Dr J J Vereijken NL47 INGB 0005 9521 61	10.000,00
Totaalbedrag voor 1 opdracht	10.000,00

Bevestigen

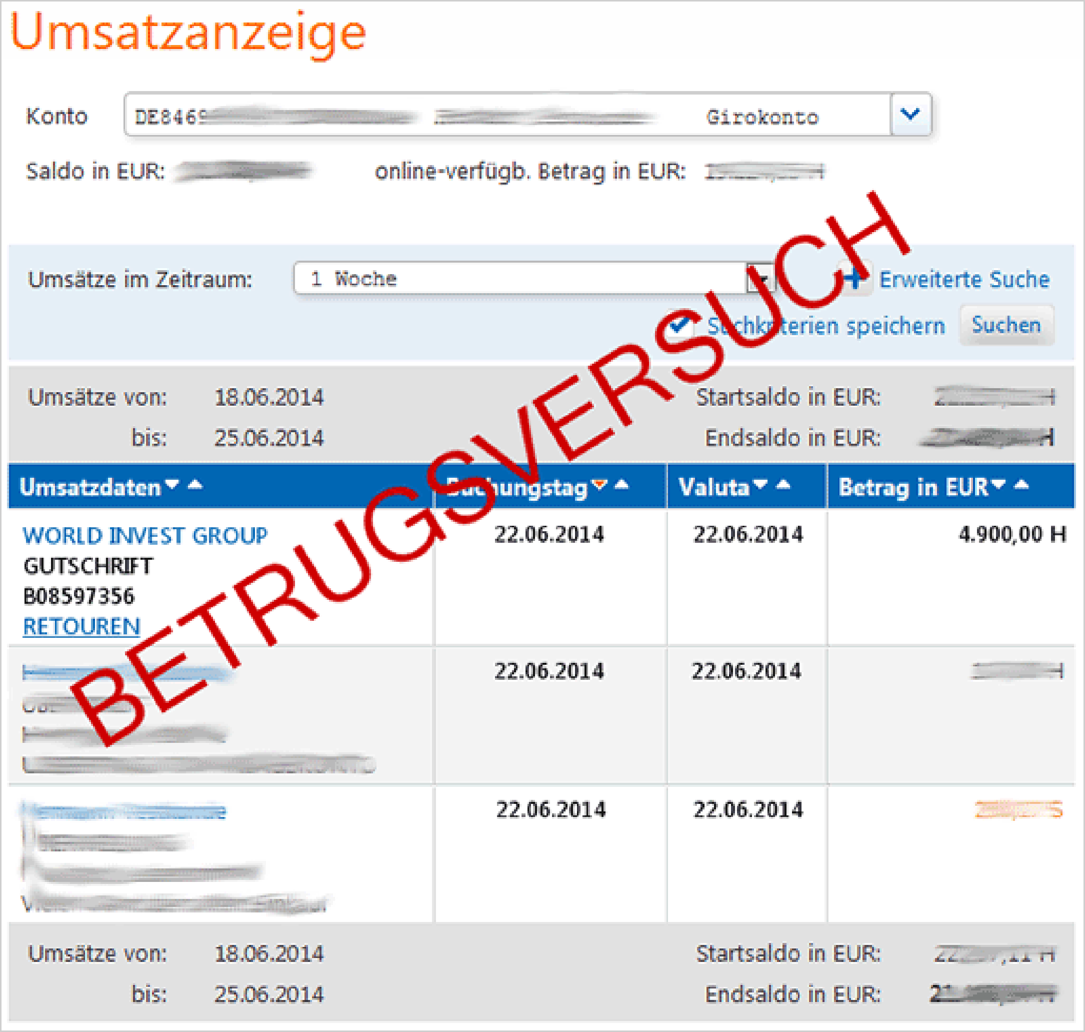


What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

crunchr

Malware: Case #2 – Fake credit transaction



Umsatzanzeige

Konto: DE846[redacted] Girokonto

Saldo in EUR: [redacted] online-verfügb. Betrag in EUR: [redacted]

Umsätze im Zeitraum: 1 Woche

+ Erweiterte Suche

✓ Suchkriterien speichern

Suchen

Umsätze von: 18.06.2014 bis: 25.06.2014

Startsaldo in EUR: [redacted]

Endsaldo in EUR: [redacted]

Umsatzdaten	Buchungstag	Valuta	Betrag in EUR
WORLD INVEST GROUP GUTSCHRIFT B08597356 RETOUREN	22.06.2014	22.06.2014	4.900,00 H
[redacted]	22.06.2014	22.06.2014	[redacted]
[redacted]	22.06.2014	22.06.2014	[redacted]

Umsätze von: 18.06.2014 bis: 25.06.2014

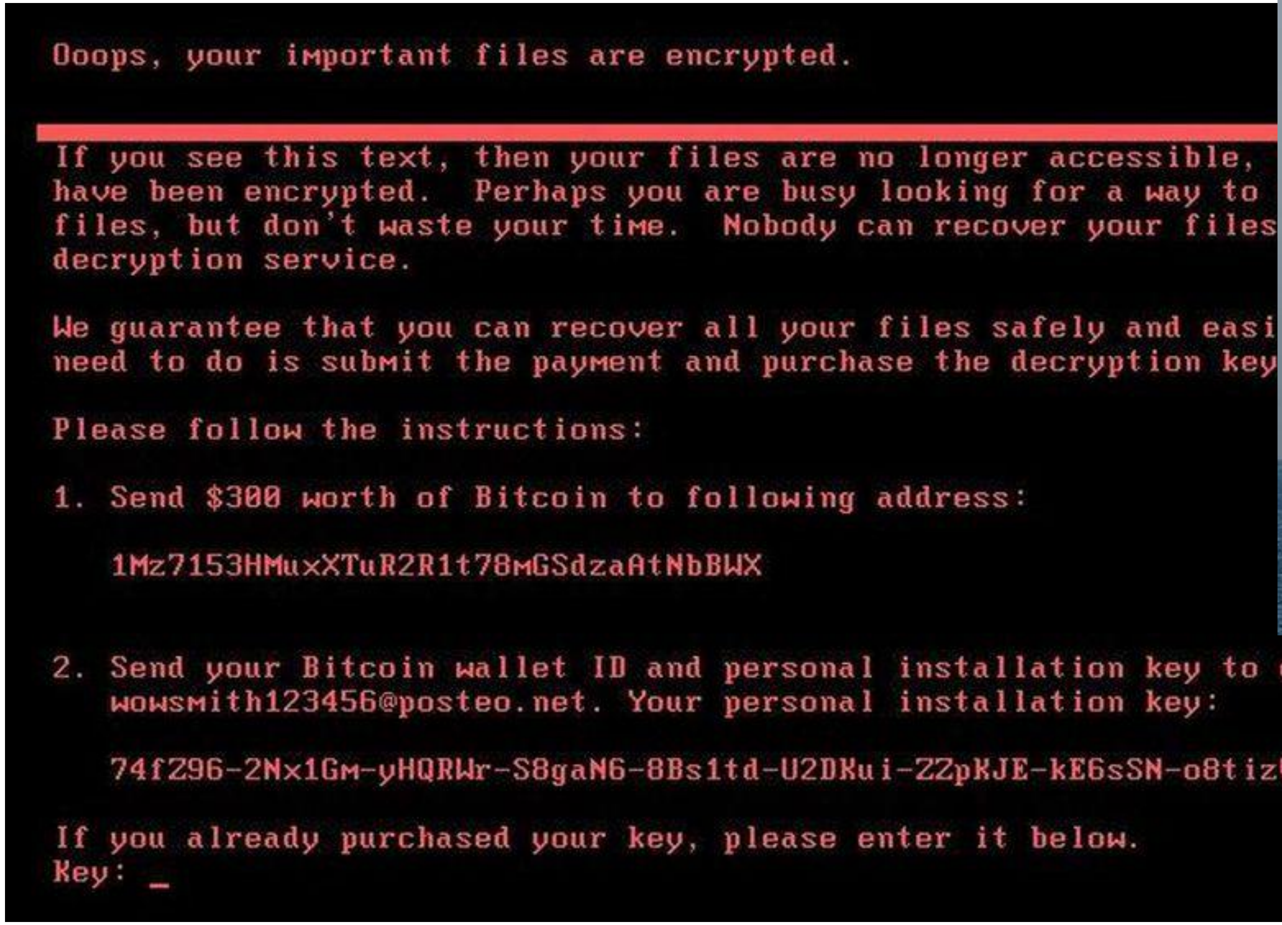
Startsaldo in EUR: [redacted]

Endsaldo in EUR: [redacted]

BETRUGSVERSUCH

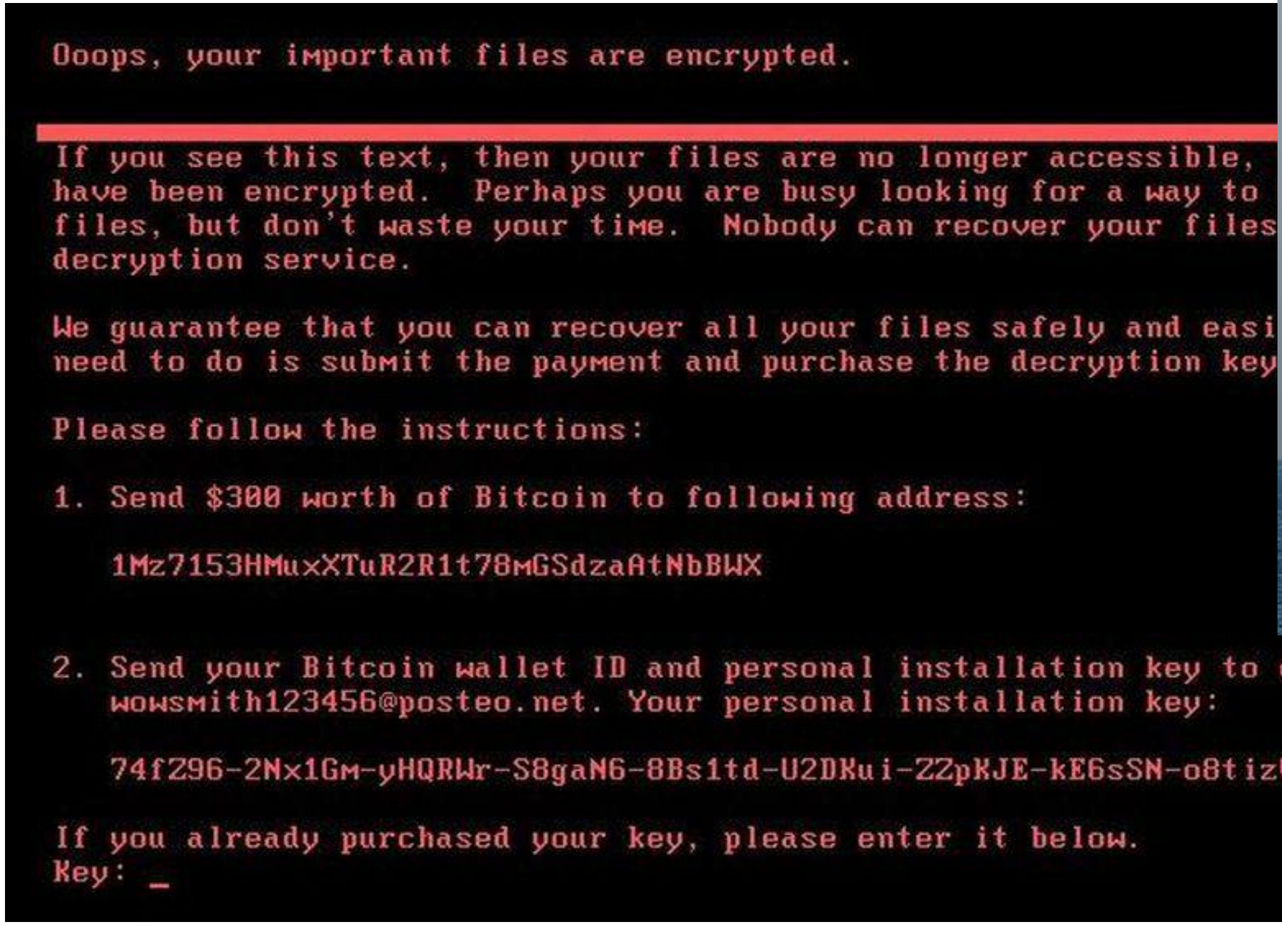
crunchr

Malware: Case #3 – NotPetya



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible,
have been encrypted.  Perhaps you are busy looking for a way to
files, but don't waste your time.  Nobody can recover your files
decryption service.

We guarantee that you can recover all your files safely and easi
need to do is submit the payment and purchase the decryption key

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

Malware: Case #3 – NotPetya



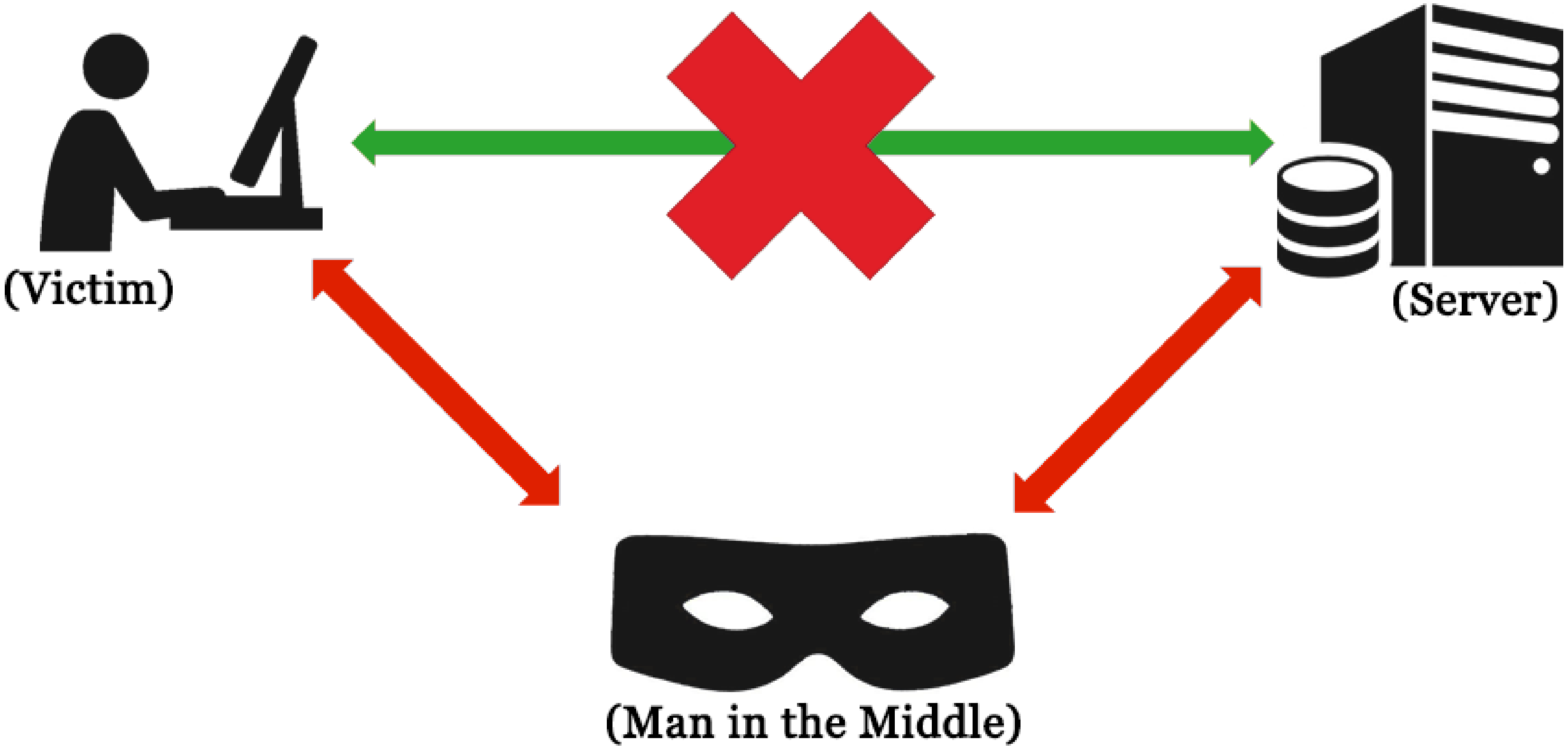
```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible,
have been encrypted.  Perhaps you are busy looking for a way to
files, but don't waste your time.  Nobody can recover your files
decryption service.

We guarantee that you can recover all your files safely and easi
need to do is submit the payment and purchase the decryption key

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

What principle applies?

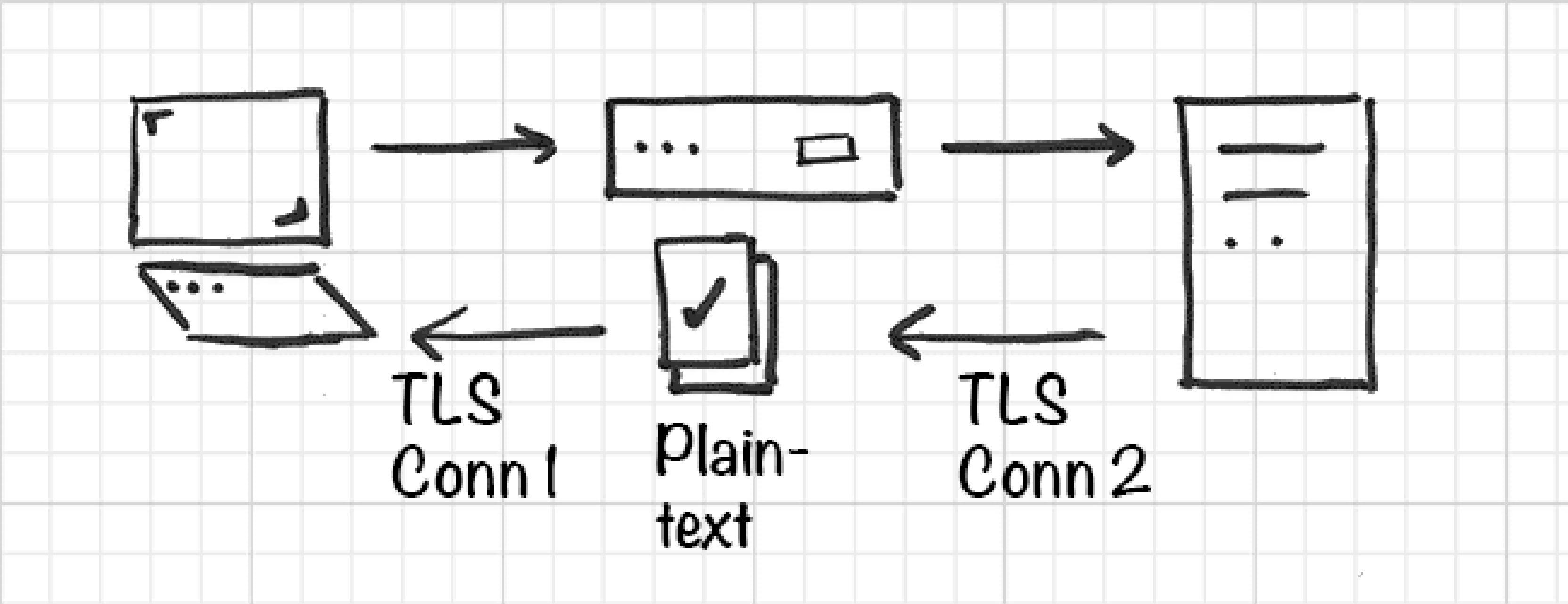
A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

crunchr

Man-in-the-middle attacks

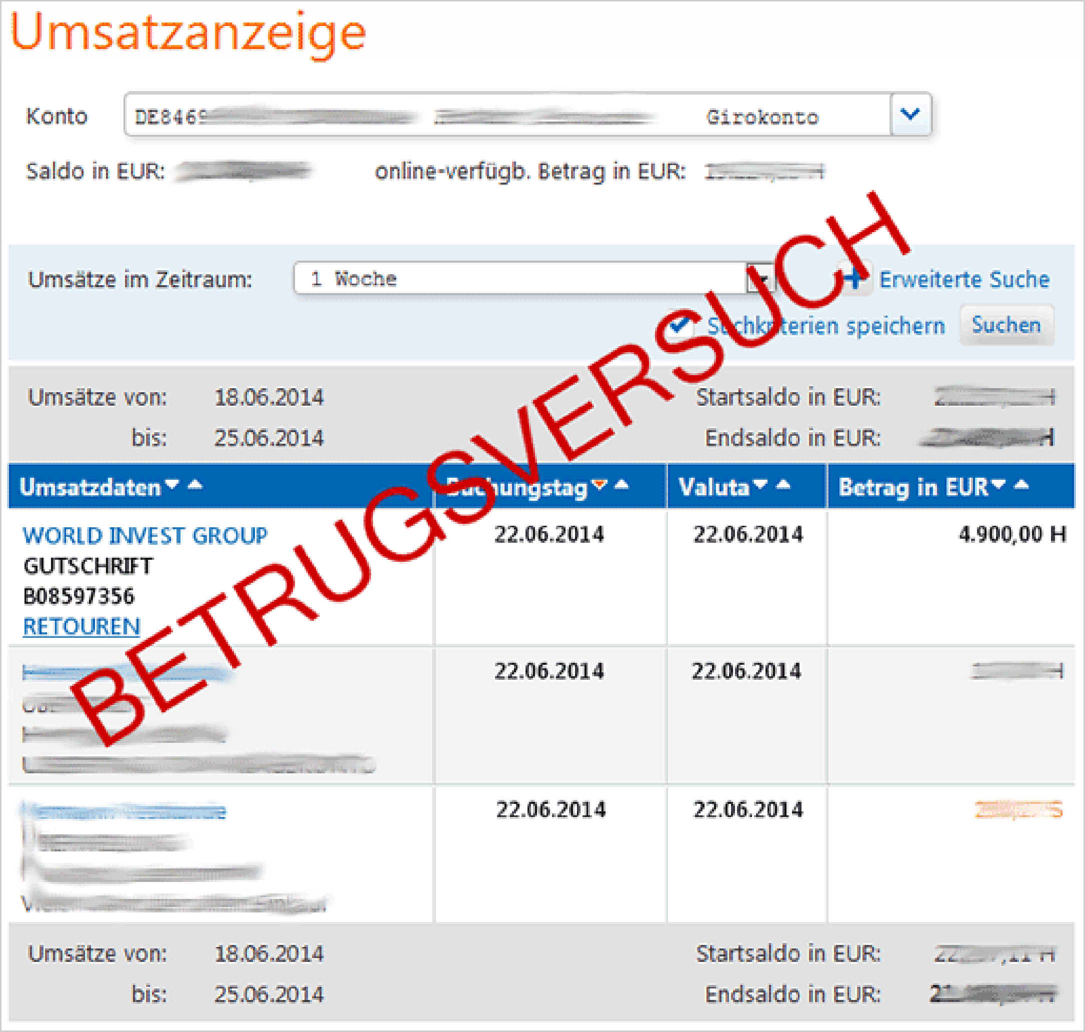


Man-in-the-middle attacks: Case #1 – Active TLS interception proxy



crunchr

Man-in-the-middle attacks: Case #2 – Fake credit transaction



Umsatzanzeige

Konto: DE846[redacted] Girokonto

Saldo in EUR: [redacted] online-verfügb. Betrag in EUR: [redacted]

Umsätze im Zeitraum: 1 Woche

Erweiterte Suche

☑ Suchkriterien speichern Suchen

Umsätze von: 18.06.2014 Startsaldo in EUR: [redacted]
bis: 25.06.2014 Endsaldo in EUR: [redacted]

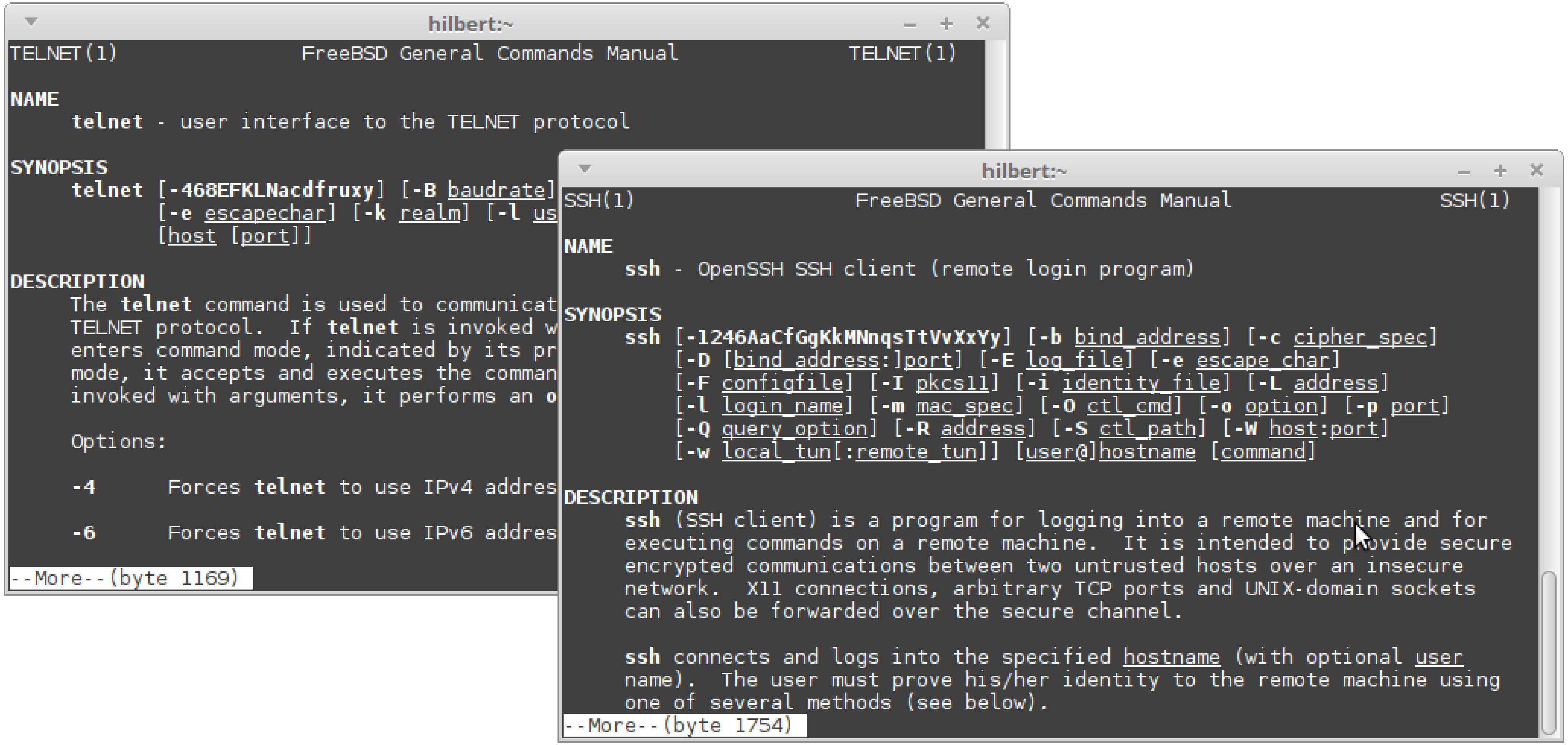
Umsatzdaten	Buchungstag	Valuta	Betrag in EUR
WORLD INVEST GROUP GUTSCHRIFT B08597356 RETOUREN	22.06.2014	22.06.2014	4.900,00 H
[redacted]	22.06.2014	22.06.2014	[redacted]
[redacted]	22.06.2014	22.06.2014	[redacted]

Umsätze von: 18.06.2014 Startsaldo in EUR: [redacted]
bis: 25.06.2014 Endsaldo in EUR: [redacted]

BETRUGSVERSUCH

crunchr

Man-in-the-middle attacks: Case #3 – Telnet versus SSH 1/2



```
TELNET(1)               FreeBSD General Commands Manual              TELNET(1)

NAME
     telnet - user interface to the TELNET protocol

SYNOPSIS
     telnet [-468EFKLNacdfruxy] [-B baudrate]
            [-e escapechar] [-k realm] [-l us
            [host [port]]

DESCRIPTION
     The telnet command is used to communicat
     TELNET protocol.  If telnet is invoked w
     enters command mode, indicated by its pr
     mode, it accepts and executes the comman
     invoked with arguments, it performs an o

     Options:

     -4      Forces telnet to use IPv4 addres

     -6      Forces telnet to use IPv6 addres
--More--(byte 1169)
```

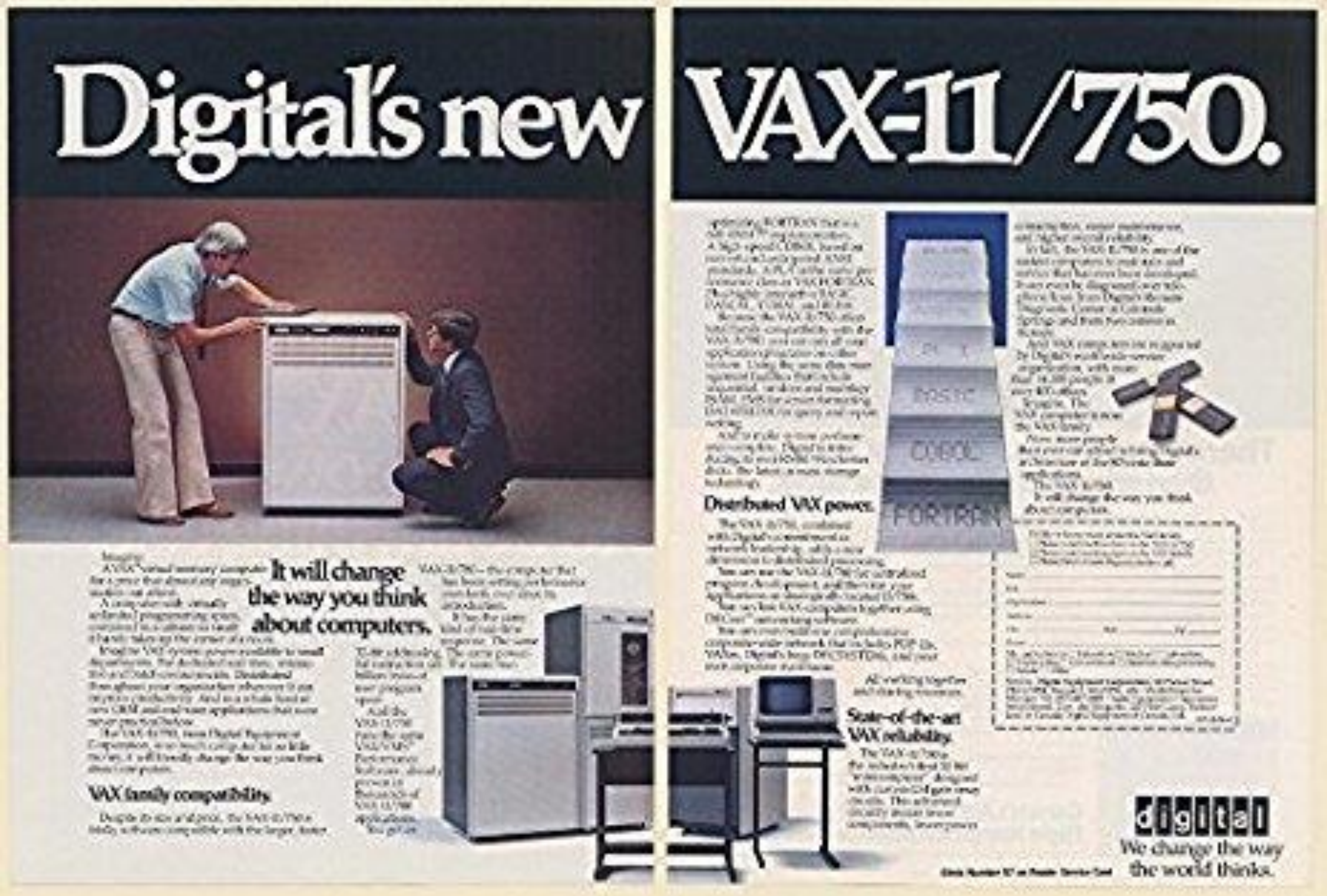
```
SSH(1)                  FreeBSD General Commands Manual                 SSH(1)

NAME
     ssh - OpenSSH SSH client (remote login program)

SYNOPSIS
     ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
         [-D [bind_address:]port] [-E log_file] [-e escape_char]
         [-F configfile] [-I pkcs11] [-i identity_file] [-L address]
         [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
         [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
         [-w local_tun[:remote_tun]] [user@]hostname [command]

DESCRIPTION
     ssh (SSH client) is a program for logging into a remote machine and for
     executing commands on a remote machine.  It is intended to provide secure
     encrypted communications between two untrusted hosts over an insecure
     network.  X11 connections, arbitrary TCP ports and UNIX-domain sockets
     can also be forwarded over the secure channel.

     ssh connects and logs into the specified hostname (with optional user
     name).  The user must prove his/her identity to the remote machine using
     one of several methods (see below).
--More--(byte 1754)
```

crunchr

Man-in-the-middle attacks: Case #3 – Telnet versus SSH 2/2

Digital's new VAX-11/750.
It will change the way you think about computers.
VAX family compatibility.
Distributed VAX power.
State-of-the-art VAX reliability.
BASIC
COBOL
FORTRAN
digital
We change the way the world thinks.

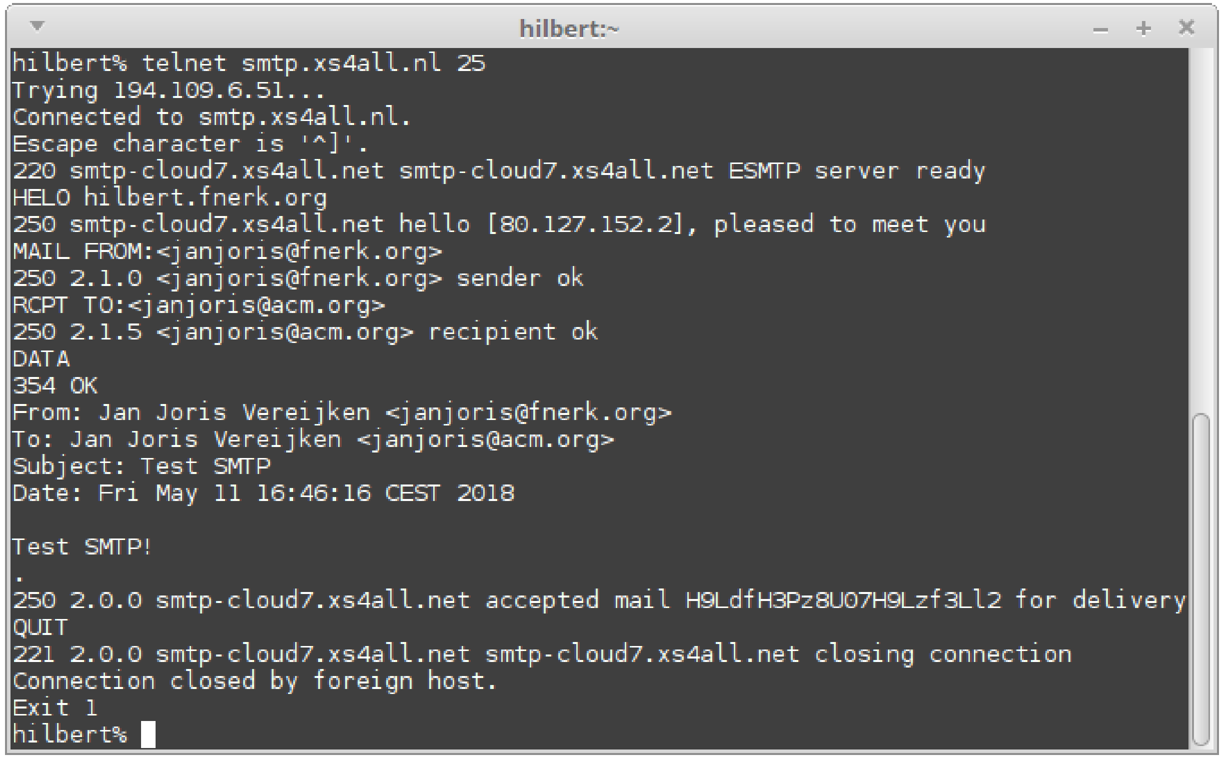
Man-in-the-middle attacks: Case #3 – Telnet versus SSH 2/2


Digital's new VAX-11/750.
It will change the way you think about computers.
BASIC
COBOL
FORTRAN
Distributed VAX power.
VAX family compatibility.
State-of-the-art VAX reliability.
digital
We change the way the world thinks.

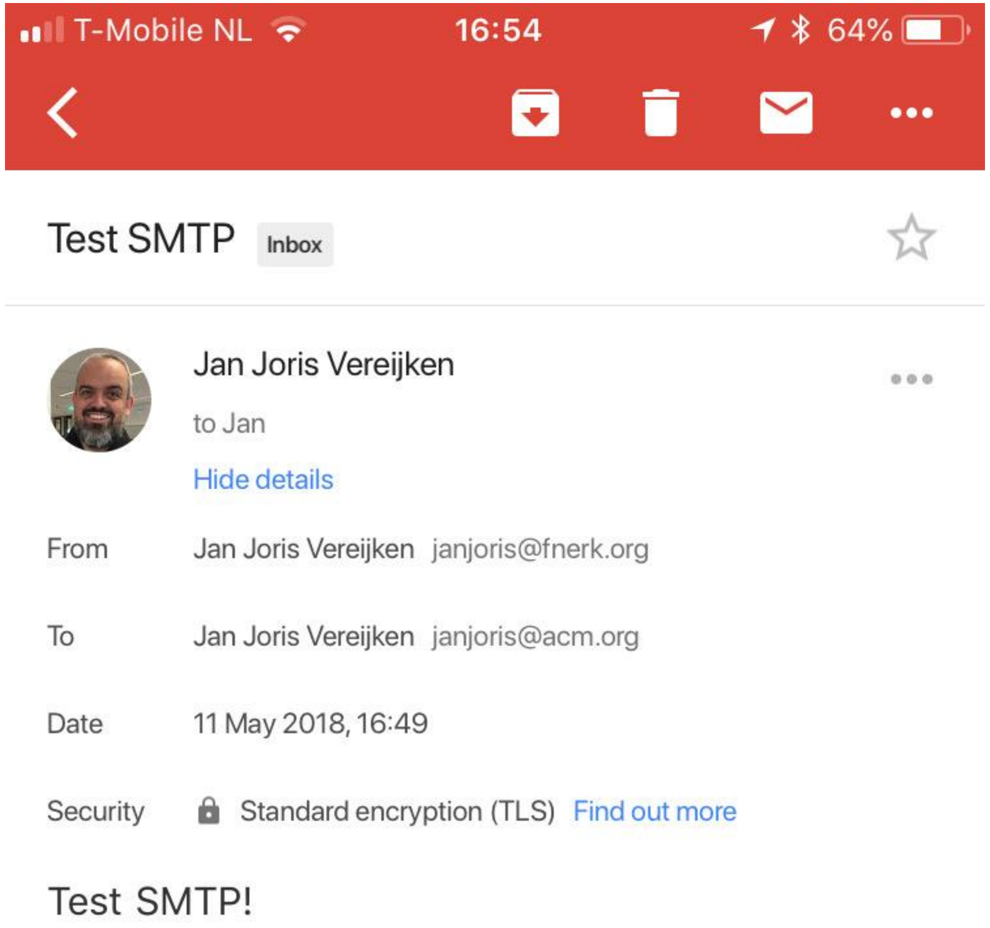
What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

Man-in-the-middle attacks: Case #4 – SMTP with STARTTLS



```
hilbert% telnet smtp.xs4all.nl 25
Trying 194.109.6.51...
Connected to smtp.xs4all.nl.
Escape character is '^]'.
220 smtp-cloud7.xs4all.net smtp-cloud7.xs4all.net ESMTP server ready
HELO hilbert.fnerk.org
250 smtp-cloud7.xs4all.net hello [80.127.152.2], pleased to meet you
MAIL FROM:<janjoris@fnerk.org>
250 2.1.0 <janjoris@fnerk.org> sender ok
RCPT TO:<janjoris@acm.org>
250 2.1.5 <janjoris@acm.org> recipient ok
DATA
354 OK
From: Jan Joris Vereijken <janjoris@fnerk.org>
To: Jan Joris Vereijken <janjoris@acm.org>
Subject: Test SMTP
Date: Fri May 11 16:46:16 CEST 2018

Test SMTP!
.
250 2.0.0 smtp-cloud7.xs4all.net accepted mail H9LdfH3Pz8U07H9Lzf3Ll2 for delivery
QUIT
221 2.0.0 smtp-cloud7.xs4all.net smtp-cloud7.xs4all.net closing connection
Connection closed by foreign host.
Exit 1
hilbert%
```



Test SMTP

Jan Joris Vereijken

to Jan

Hide details

From Jan Joris Vereijken janjoris@fnerk.org

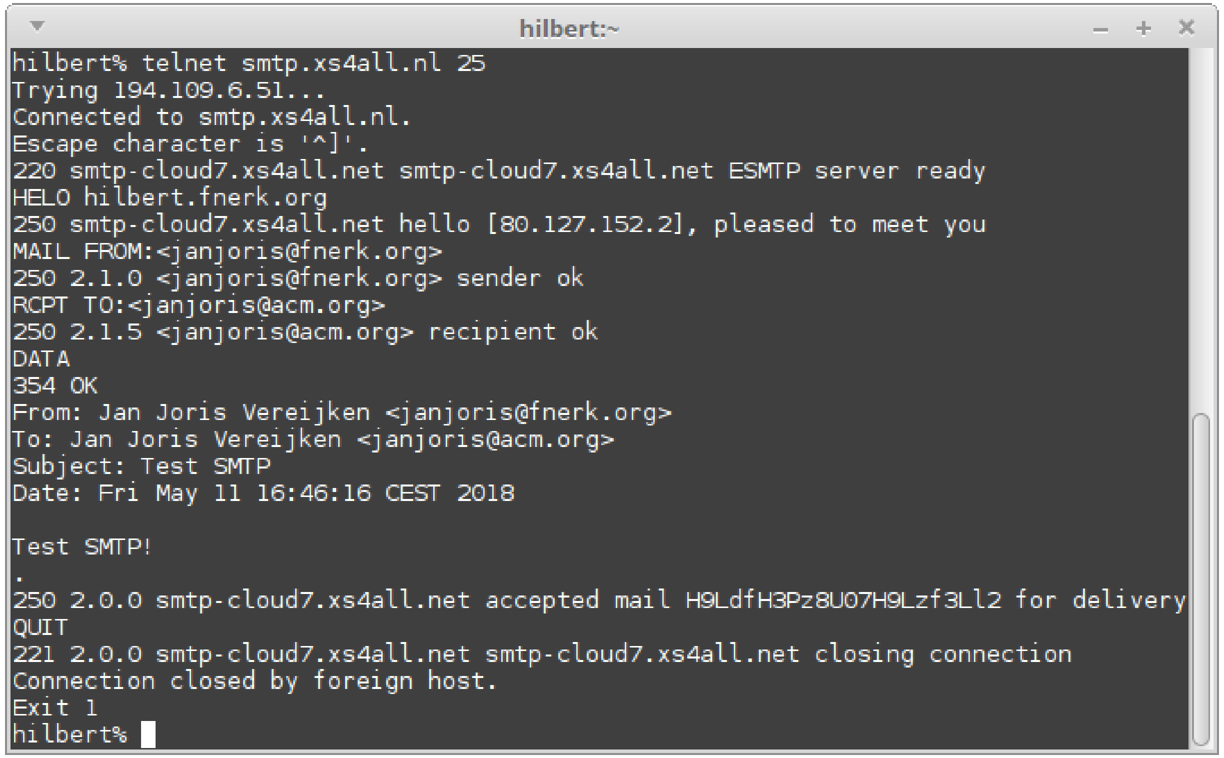
To Jan Joris Vereijken janjoris@acm.org

Date 11 May 2018, 16:49

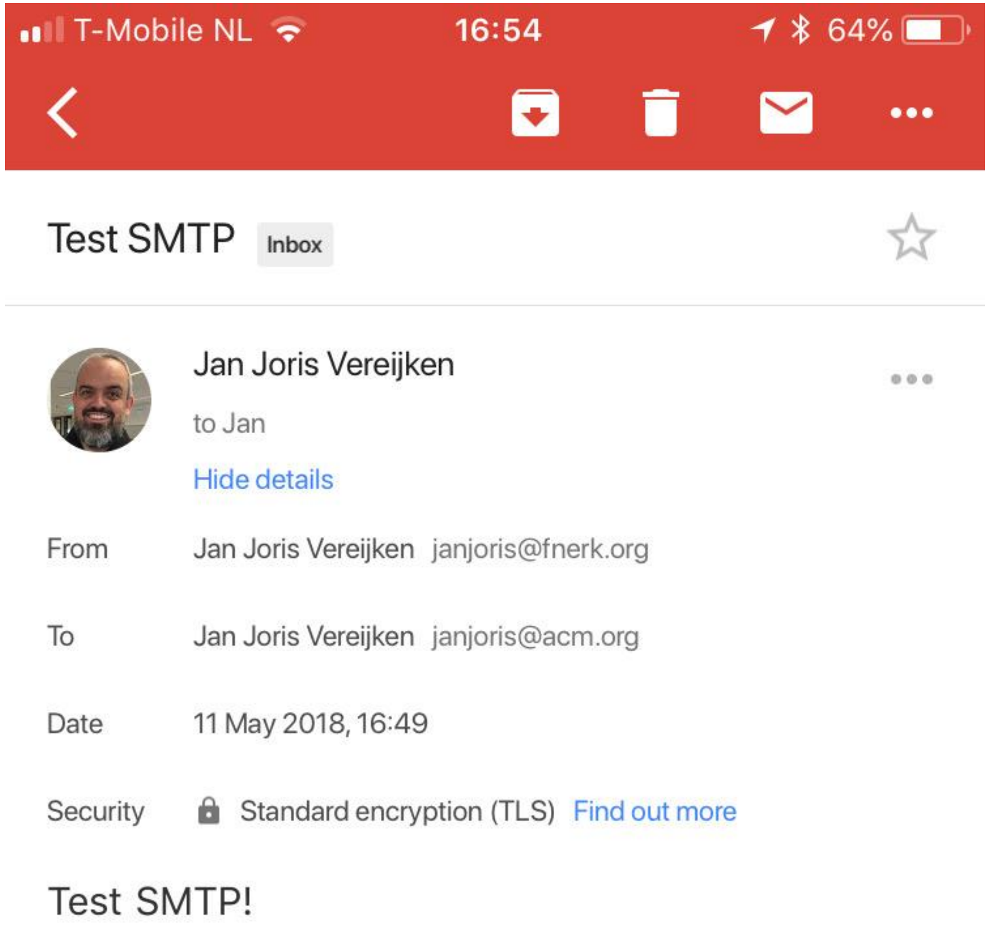
Security Standard encryption (TLS) Find out more

Test SMTP!

Man-in-the-middle attacks: Case #4 – SMTP with STARTTLS



```
hilbert% telnet smtp.xs4all.nl 25
Trying 194.109.6.51...
Connected to smtp.xs4all.nl.
Escape character is '^]'.
220 smtp-cloud7.xs4all.net smtp-cloud7.xs4all.net ESMTP server ready
HELO hilbert.fnerk.org
250 smtp-cloud7.xs4all.net hello [80.127.152.2], pleased to meet you
MAIL FROM:<janjoris@fnerk.org>
250 2.1.0 <janjoris@fnerk.org> sender ok
RCPT TO:<janjoris@acm.org>
250 2.1.5 <janjoris@acm.org> recipient ok
DATA
354 OK
From: Jan Joris Vereijken <janjoris@fnerk.org>
To: Jan Joris Vereijken <janjoris@acm.org>
Subject: Test SMTP
Date: Fri May 11 16:46:16 CEST 2018

Test SMTP!
.
250 2.0.0 smtp-cloud7.xs4all.net accepted mail H9LdfH3Pz8U07H9Lzf3Ll2 for delivery
QUIT
221 2.0.0 smtp-cloud7.xs4all.net smtp-cloud7.xs4all.net closing connection
Connection closed by foreign host.
Exit 1
hilbert%
```



Test SMTP Inbox

Jan Joris Vereijken

to Jan

Hide details

From Jan Joris Vereijken janjoris@fnerk.org

To Jan Joris Vereijken janjoris@acm.org

Date 11 May 2018, 16:49

Security Standard encryption (TLS) Find out more

Test SMTP!

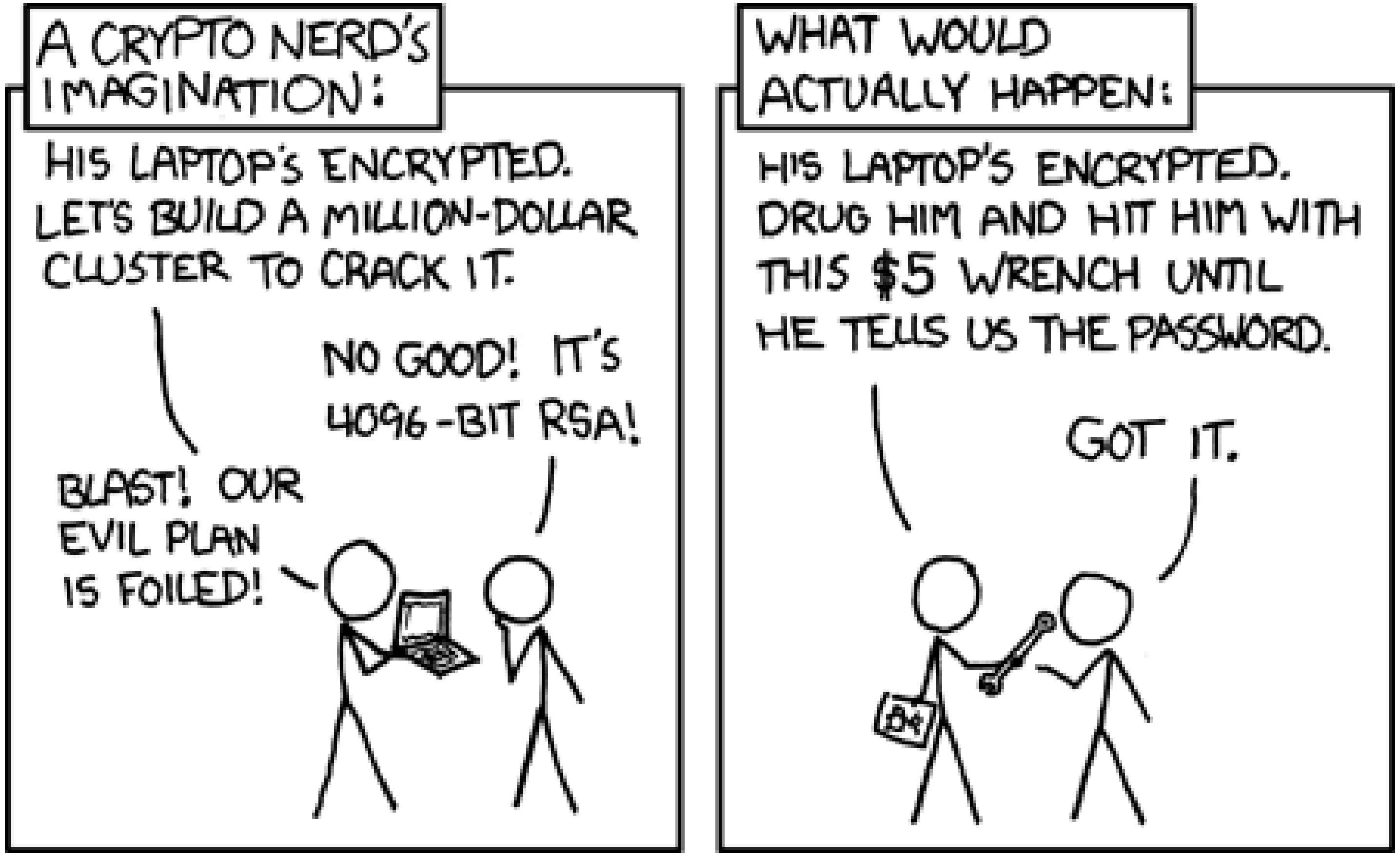
What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

crunchr

Physical attacks

Physical attacks: Case #1 – Litteral brute force


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Physical attacks: Case #2 – Full disk encryption 1/2

Physical attacks: Case #2 – Full disk encryption 2/2

Physical attacks: Case #2 – Full disk encryption 2/2

What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

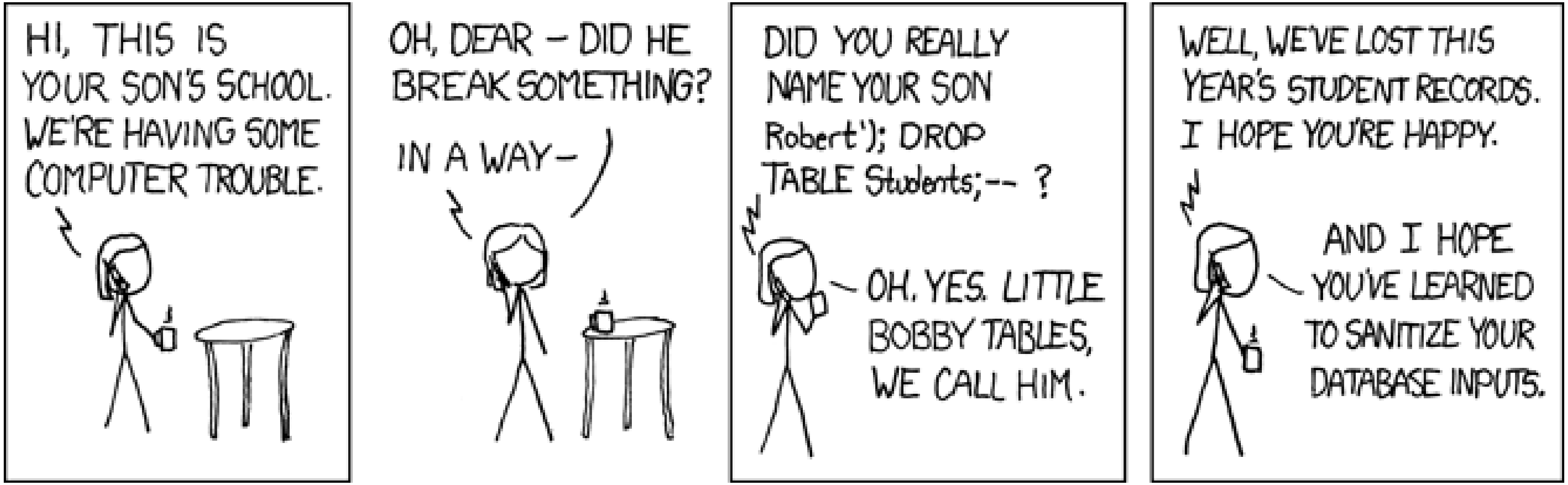
Physical attacks: Case #3 – Bike lock versus door lock

Physical attacks: Case #3 – Bike lock versus door lock

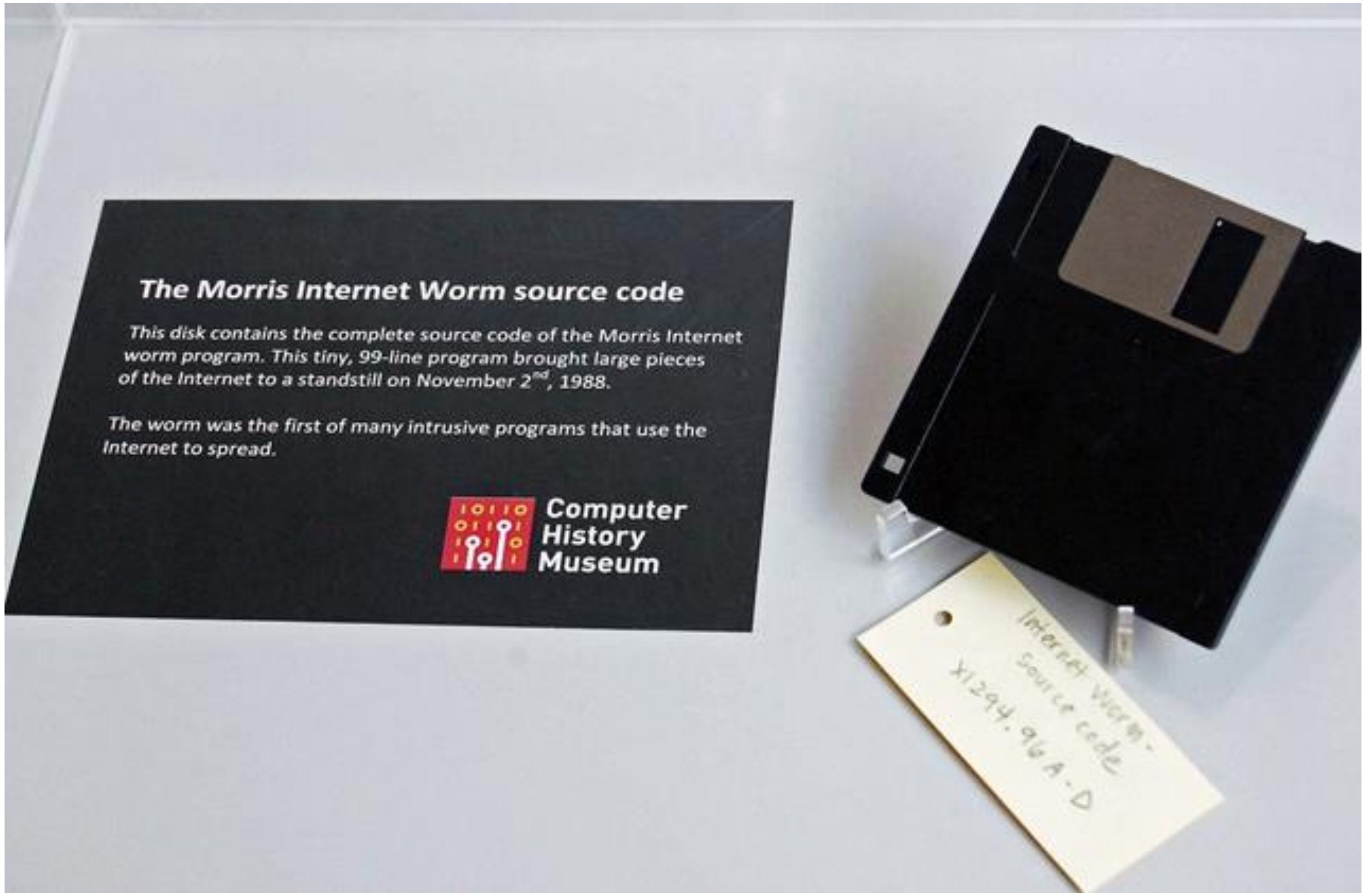
What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

Data driven attacks


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Data driven attacks: Case #1 – The Morris worm



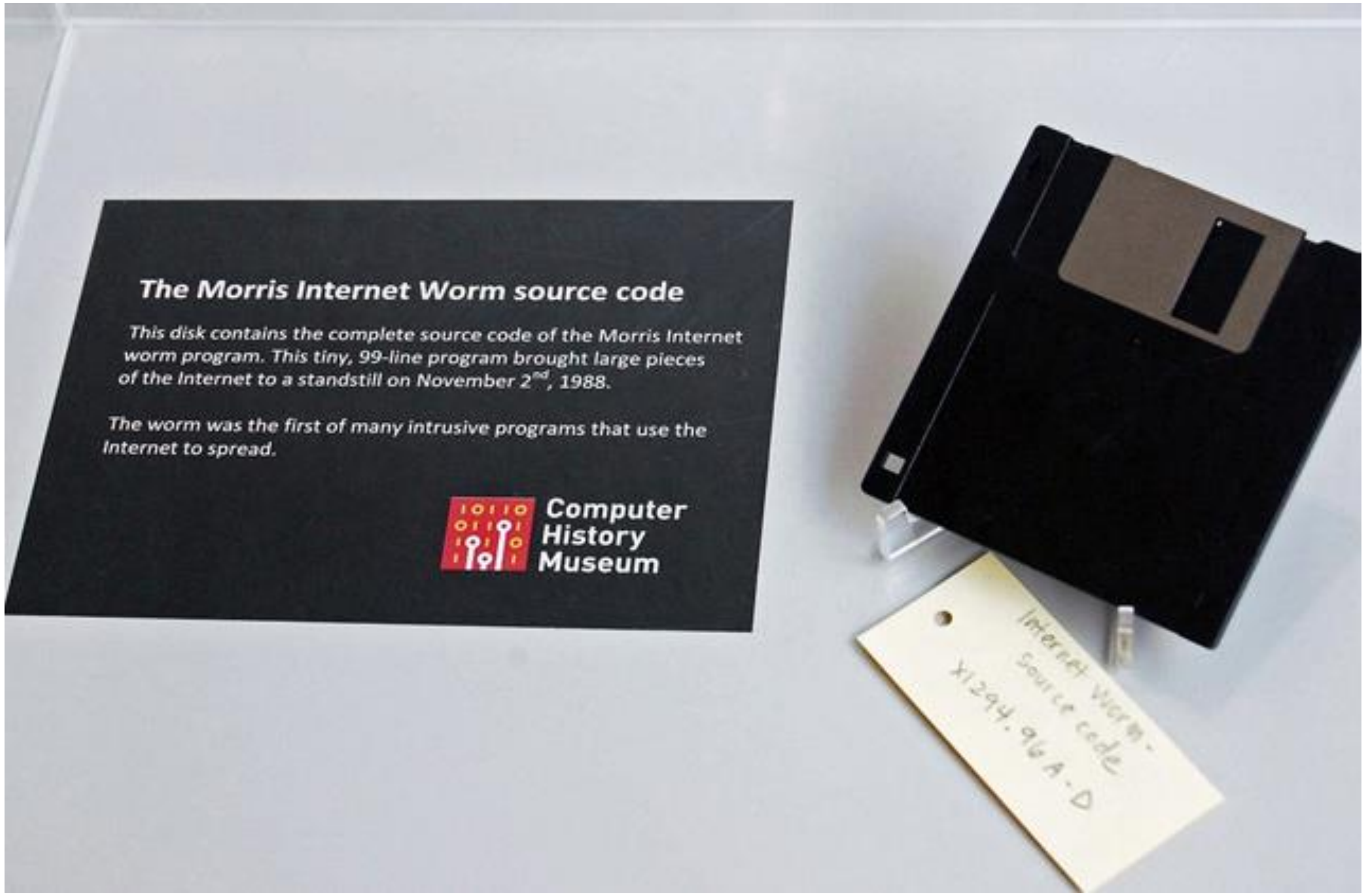
The Morris Internet Worm source code

This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

The worm was the first of many intrusive programs that use the Internet to spread.

crunchr

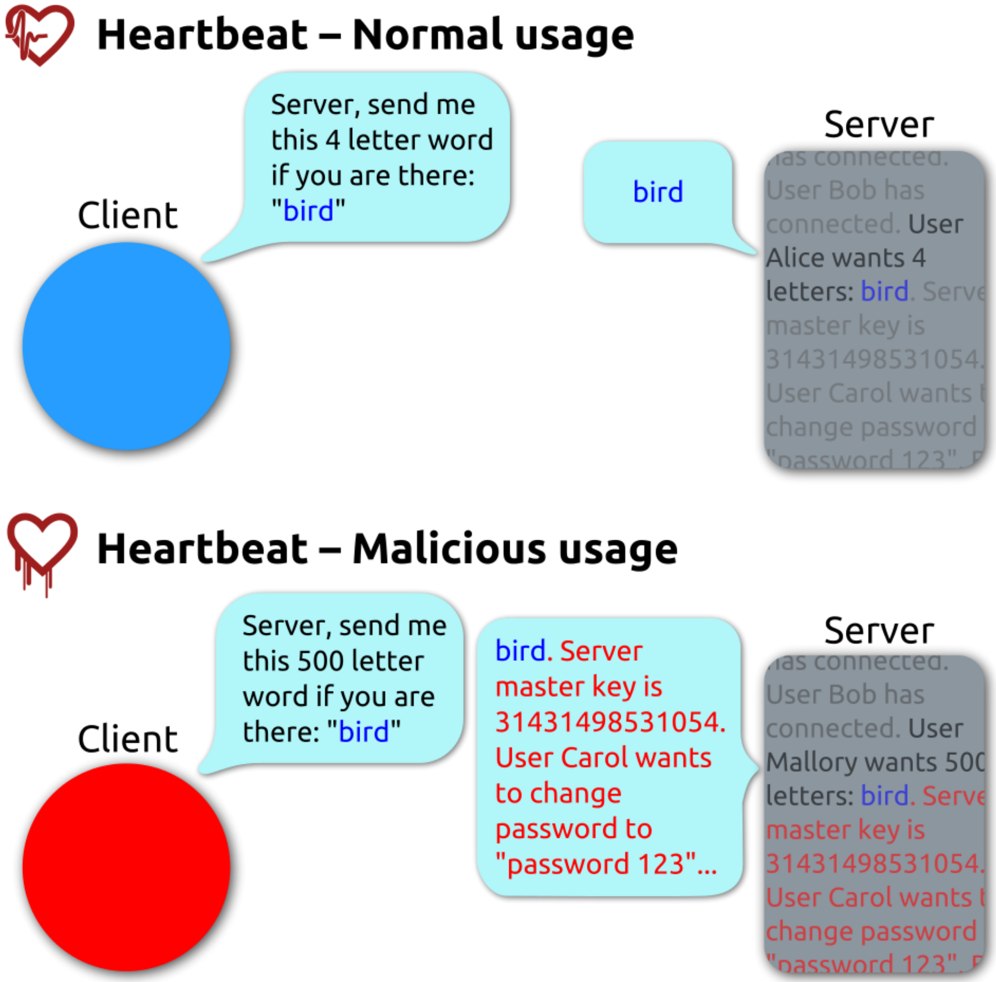
Data driven attacks: Case #1 – The Morris worm


The Morris Internet Worm source code
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.
The worm was the first of many intrusive programs that use the Internet to spread.
Computer History Museum
Internet Worm-Source code
X1294.96A-D

What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

Data driven attacks: Case #2 – Heartbleed



Heartbeat – Normal usage

Client

Server, send me this 4 letter word if you are there: "bird"

bird

Server

as connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

Heartbeat – Malicious usage

Client

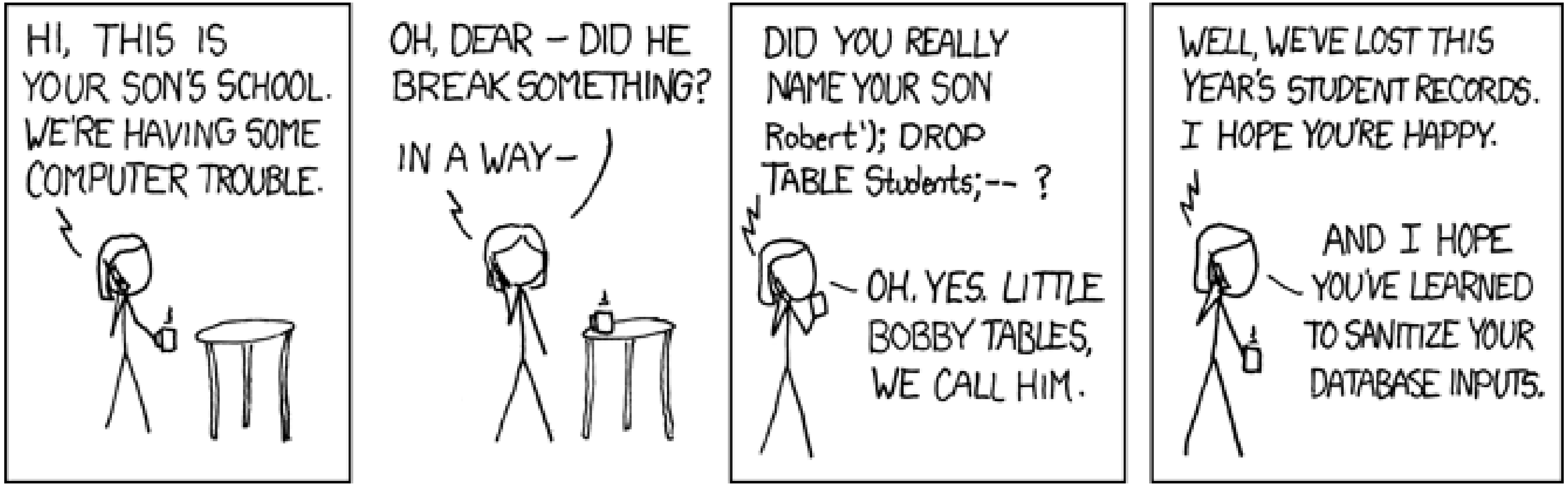
Server, send me this 500 letter word if you are there: "bird"

bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...

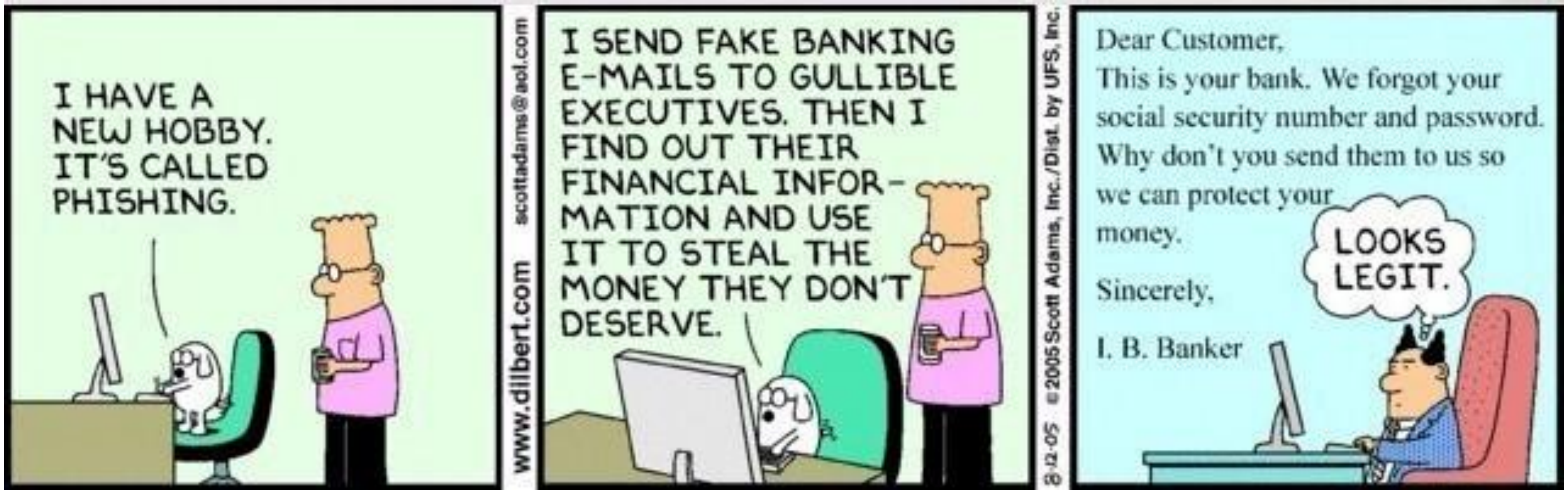
Server

as connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

Data driven attacks: Case #3 – SQL Injection and Cross-Site Scripting


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

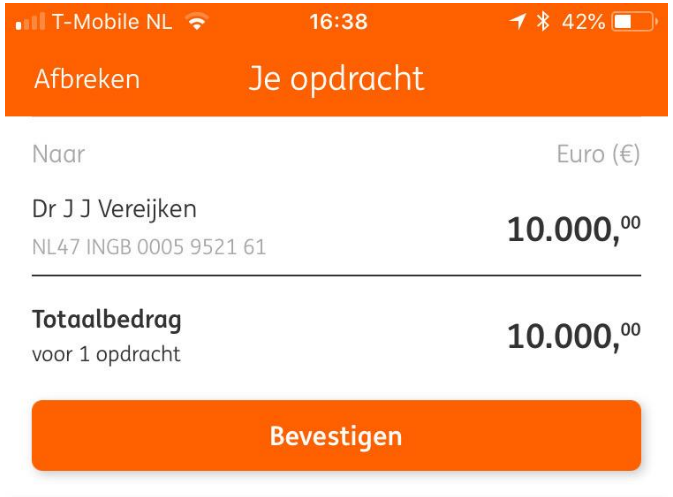
Social Engineering


I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.

www.dilbert.com scottadams@aol.com

8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.

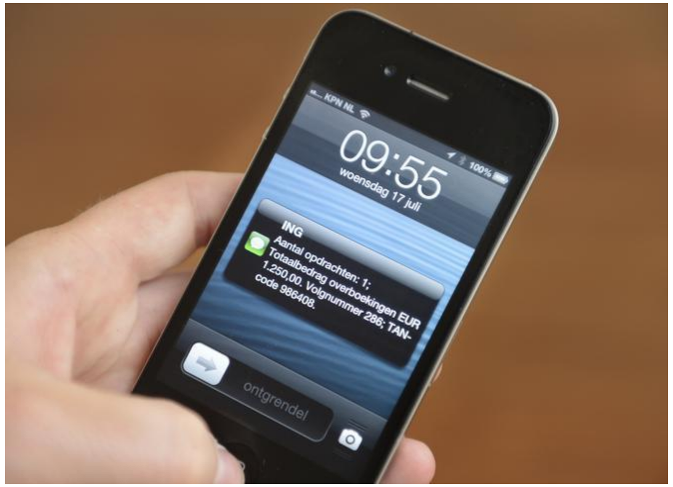
Social Engineering: Case #1 – ING versus Rabobank



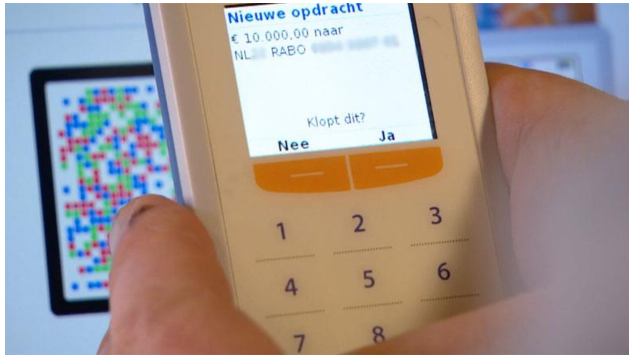
Afbreken Je opdracht

Naar	Euro (€)
Dr J J Vereijken NL47 INGB 0005 9521 61	10.000,00
Totaalbedrag voor 1 opdracht	10.000,00

Bevestigen



ING
Aantal opdrachten: 1;
Totaalbedrag overboekingen EUR
1.250,00. Volgnummer 286; TAN-
code 986408.

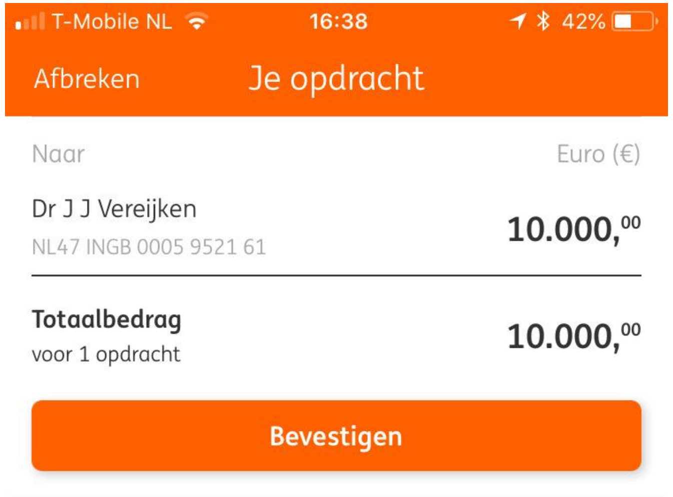


Nieuwe opdracht
€ 10.000,00 naar
NL[redacted] RABO [redacted]

Klopt dit?

Nee Ja

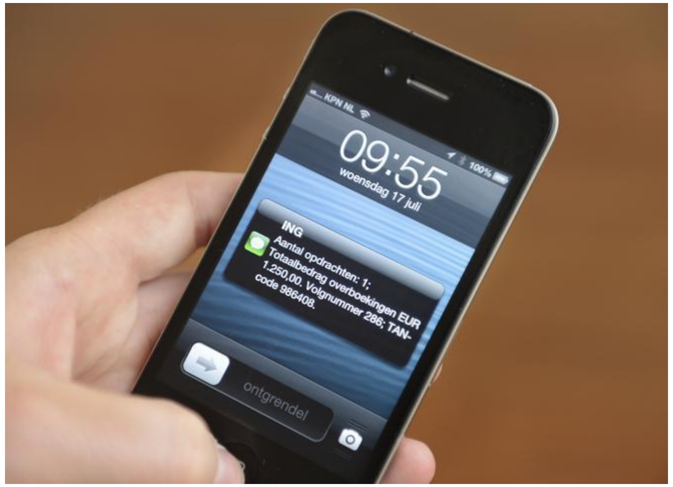
Social Engineering: Case #1 – ING versus Rabobank


T-Mobile NL 16:38 42%

Afbreken Je opdracht

Naar	Euro (€)
Dr J J Vereijken NL47 INGB 0005 9521 61	10.000,00
Totaalbedrag voor 1 opdracht	10.000,00

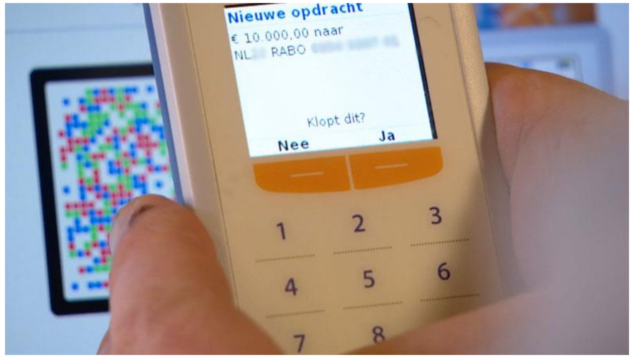
Bevestigen


KPN NL 09:55 100%
woensdag 17 juli

ING
Aantal opdrachten: 1; Totaalbedrag overboekingen EUR 1.250,00. Volgnummer 286; TAN-code 986408.

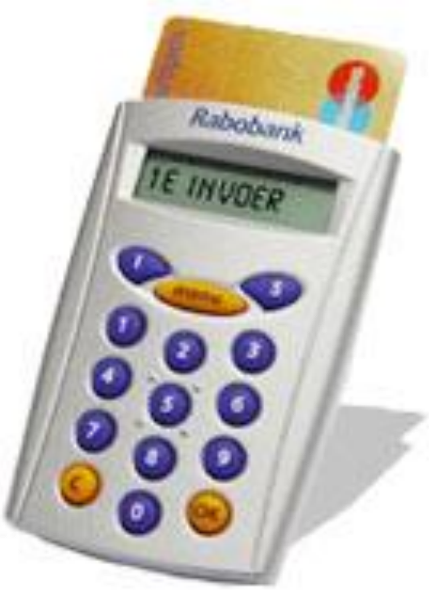
What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

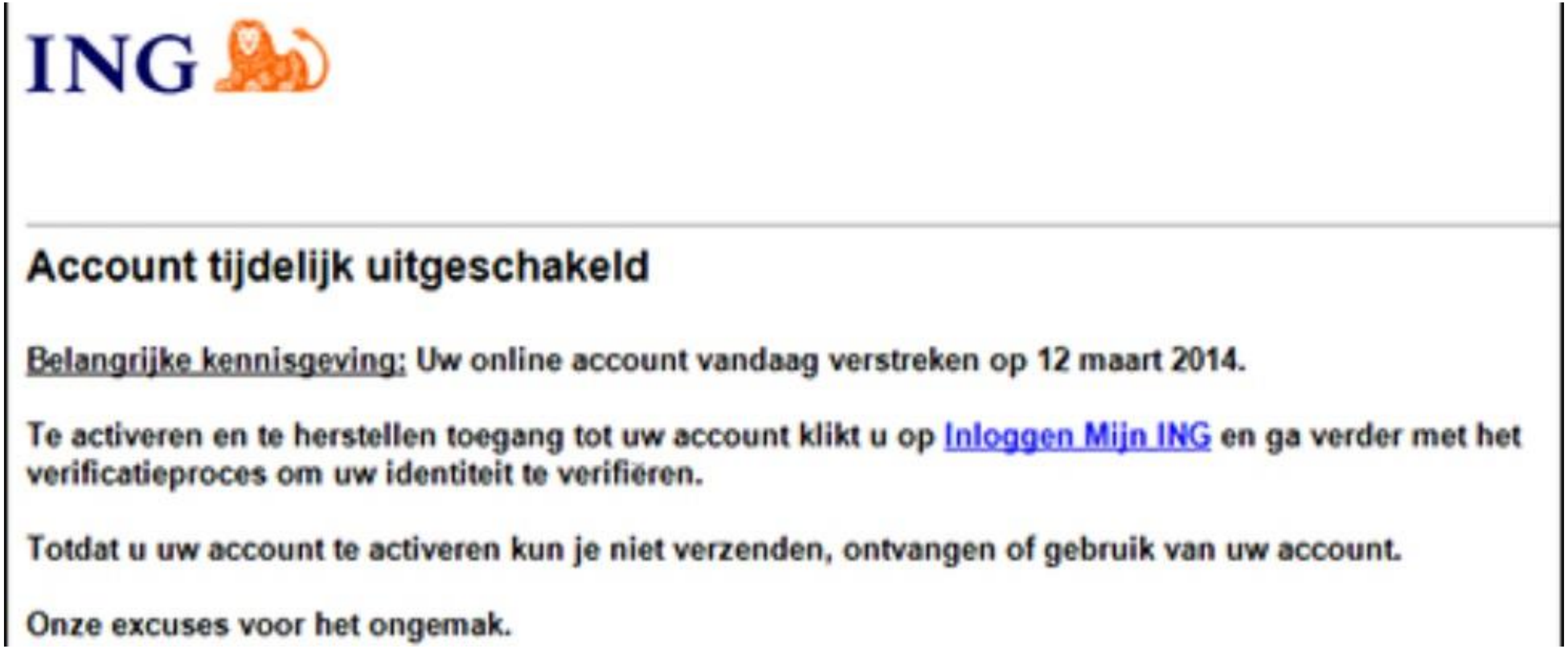

Nieuwe opdracht
€ 10.000,00 naar
NL[redacted] RABO [redacted]

Klopt dit?

Nee Ja



Social Engineering: Case #2 – Phishing mails with language mistakes!



Account tijdelijk uitgeschakeld

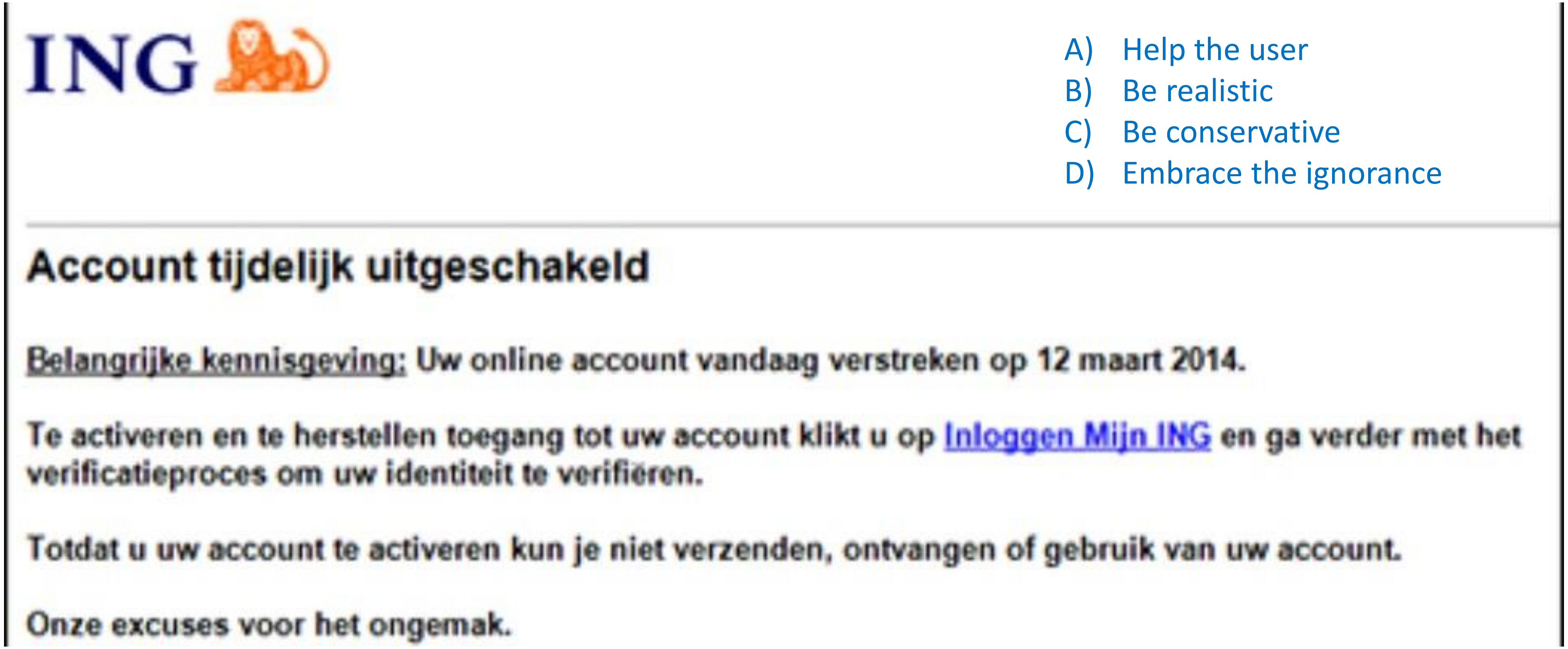
Belangrijke kennisgeving: Uw online account vandaag verstreken op 12 maart 2014.

Te activeren en te herstellen toegang tot uw account klikt u op Inloggen Mijn ING en ga verder met het verificatieproces om uw identiteit te verifiëren.

Totdat u uw account te activeren kun je niet verzenden, ontvangen of gebruik van uw account.

Onze excuses voor het ongemak.

Social Engineering: Case #2 – Phishing mails with language mistakes!



ING

Account tijdelijk uitgeschakeld

Belangrijke kennisgeving: Uw online account vandaag verstreken op 12 maart 2014.

Te activeren en te herstellen toegang tot uw account klikt u op Inloggen Mijn ING en ga verder met het verificatieproces om uw identiteit te verifiëren.

Totdat u uw account te activeren kun je niet verzenden, ontvangen of gebruik van uw account.

Onze excuses voor het ongemak.

What principle applies?

A) Help the user
B) Be realistic
C) Be conservative
D) Embrace the ignorance

Questions?

Questions?

crunchr