

Technologie a nástroje kybernetického boje

BSS152, 3.10. 2019

Jakub Drmola



Q WHAT WILL THE
WARRIOR-GUARDIAN
OF THE FUTURE
LOOK LIKE?

YO! DUDE.
BACK
HERE



CYBER
SECURITY

Reference	Definition	Citations	Discipline
Clarke, R. A., & Knake, R. K. (2011)	Cyber war is the act of nation state to penetrate another nation's computer or network in order to cause damage or disruption.	830	N/A
Arquilla, J., & Ronfeldt, D. (1993)	Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. (1993)	655	Strategic & Security Studies
Rid, Thomas. (2012)	A potentially lethal, instrumental, and political act of force conducted through malicious code	225	Strategic & Security Studies
US Department of Defence (2010-2012)	Computer Network Operations (CNO) as including computer Network Attack (CNA), computer network defence (CND) and computer network exploitation (CNE).	173+	Military Studies
Nicholson et al. (2012)	Attacks and defence issued by nation states take place over networks rather than by physical means	117	ICT
Schaap, A. J. (2009)	The use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state	95	Law
Nye Jr, J. S. (2011)	Hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence	65	Military

Fig. 9. Most influential definitions by citation count

Vymezení

- kybernetické útoky
- tj. mimo EWar, InfoWar
 - satelity, C3, drony, atp.

Archetypy útoků

- akvizice informací
 - a následná diseminace/exploitace
- šíření informací
 - propaganda
- disrupce
 - procesů a služeb
- destrukce
 - dat/zařízení

Co chráníme

- CIA
- Confidentiality
- Integrity
- Availability

Technické minimum

- aneb jak funguje internet
- a některé další důležité technologie

OSI Model Layers

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data-Link Layer

Physical Layer

TCP/IP Protocol Architecture Layers

Application Layer

Host-to-Host Transport Layer

Internet Layer

Network Interface Layer

TCP/IP Protocol Suite

Telnet

FTP

SMTP

DNS

RIP

SNMP

TCP

UDP

ARP

IP

IGMP ICMP

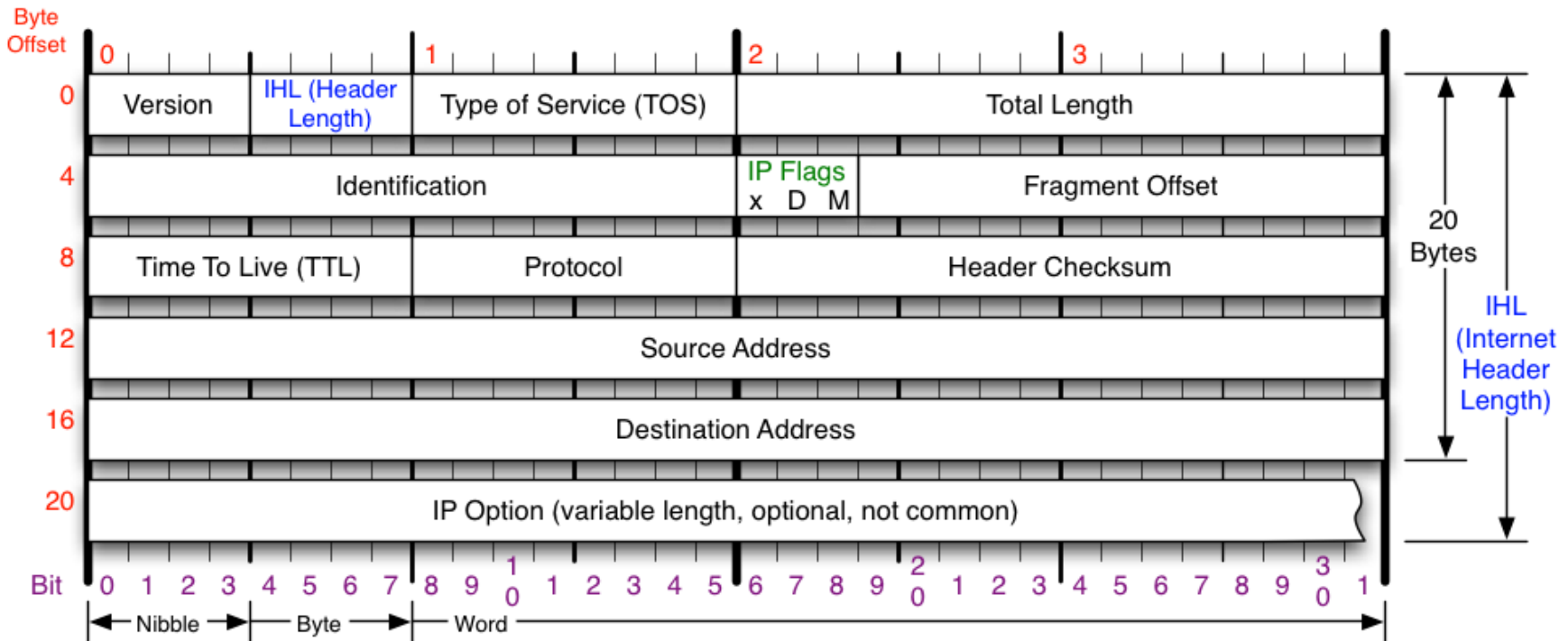
Ethernet

Token Ring

Frame Relay

ATM

IPv4 Header



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

1 User opens browser, enters URL...

2 Resolver.

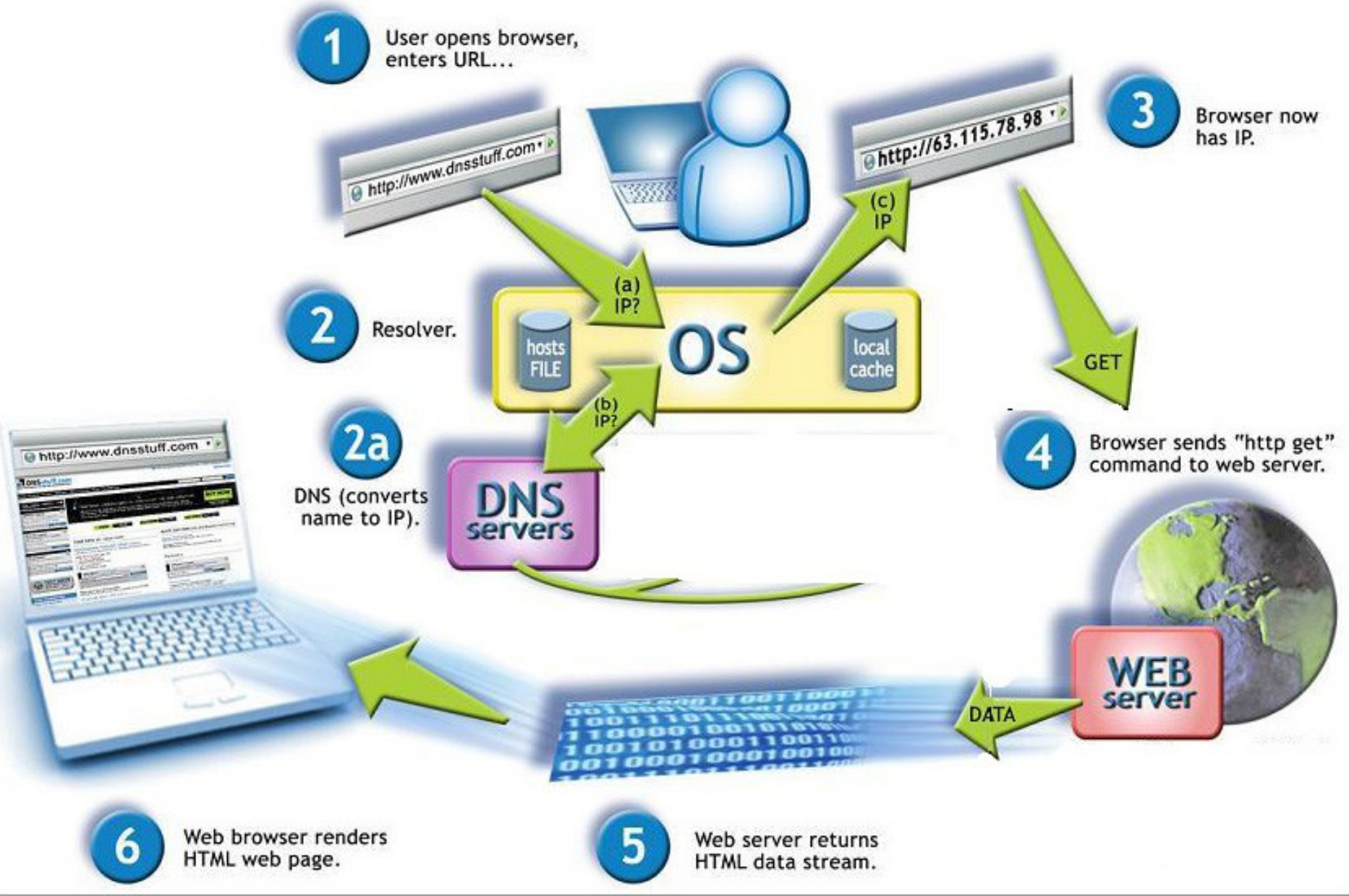
2a DNS (converts name to IP).

3 Browser now has IP.

4 Browser sends "http get" command to web server.

6 Web browser renders HTML web page.

5 Web server returns HTML data stream.



Východiska

- většina škod neúmyslná
 - bugy, nehody, přírodní katastrofy, ...
- případně útoky zevnitř
 - např. nespokojení zaměstnanci
- útoky v zásadě spočívají v nalezení a využití nějaké existující slabiny
 - lidské, strukturální, implementační, technické
 - neexistuje dokonalý systém

Častá tvrzení

- „biliony útoků“
- „jsme čím dál zranitelnější“
- airgap

Sít'ové útoky

- DDoS
 - botnet
 - LOIC
 - IRC
 - <https://threatmap.fortiguard.com/>
- spoofing
- Man in the Middle

Low Orbit Ion Cannon



newfag/LOIC

p.s cocks

Manual Mode (for pussies) **FUCKING HIVE MIND**

IRC server: Port: Channel: Connected!

1. Select your target

URL:

IP:

2. Ready?

Selected target

85.116.9.83

3. Attack options

Timeout: HTTP Subsite: Append random chars to the URL TCP / UDP message:

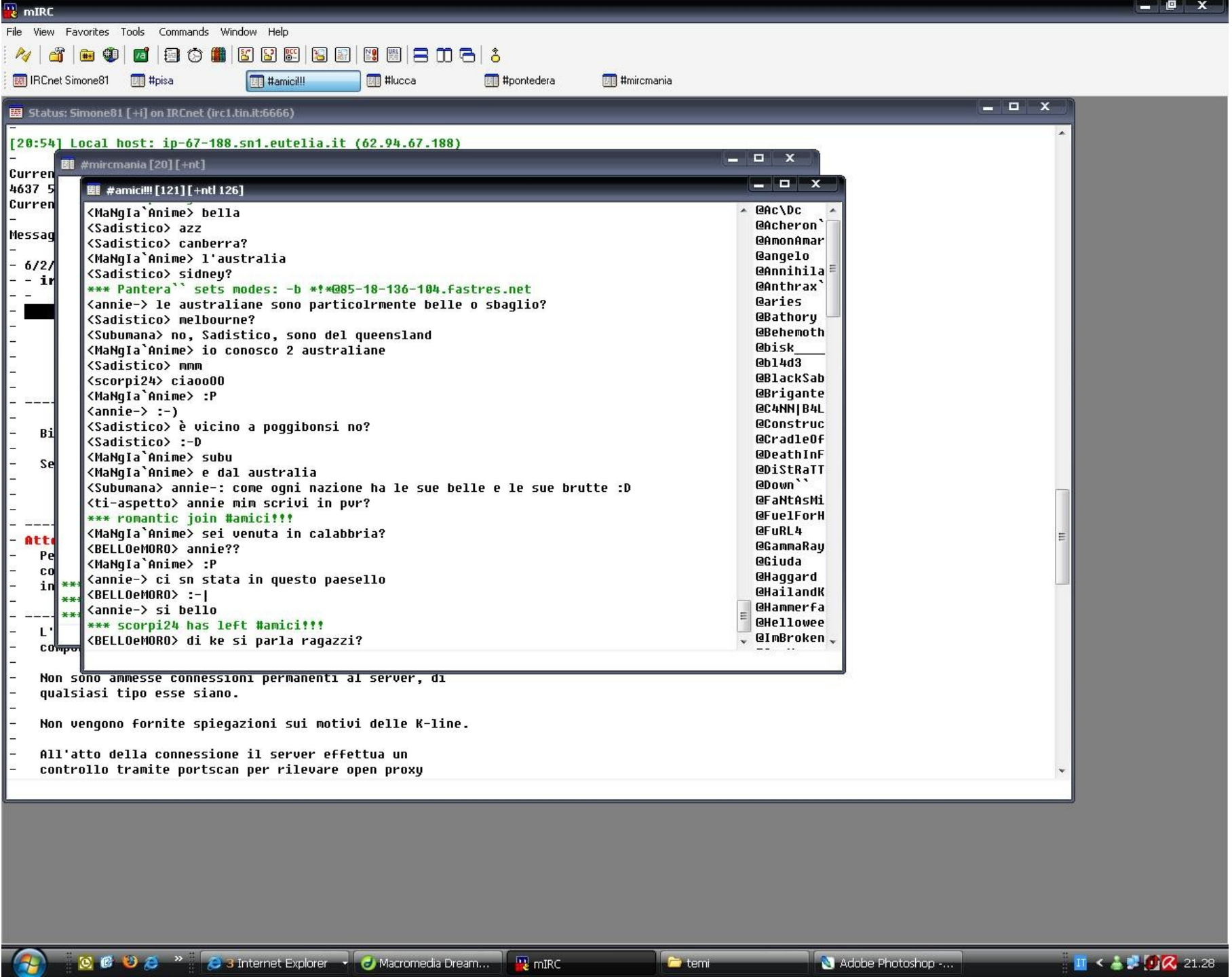
Wait for reply

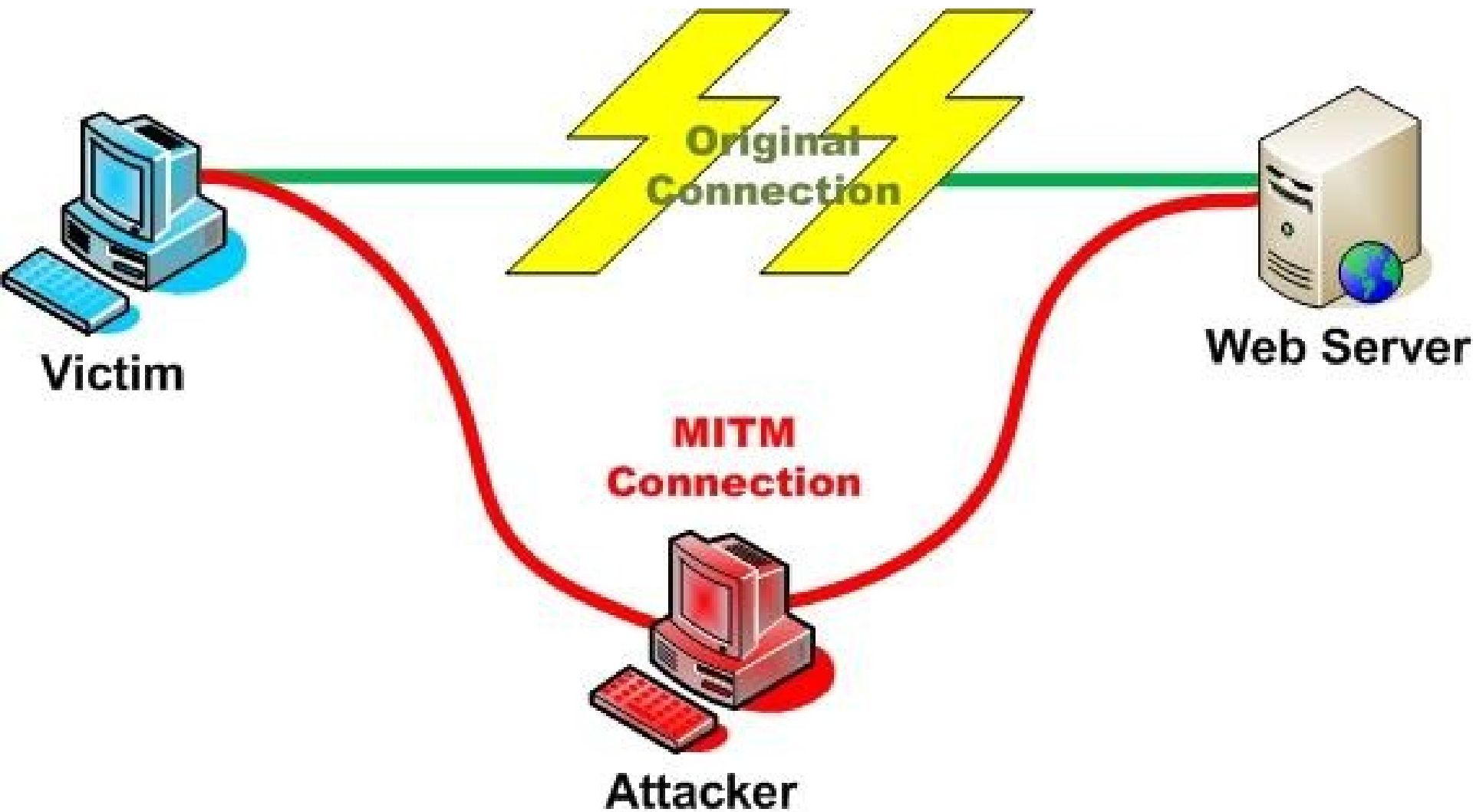
Port Method Threads

<= faster Speed slower =>

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
1	9	0	0	419	419	9

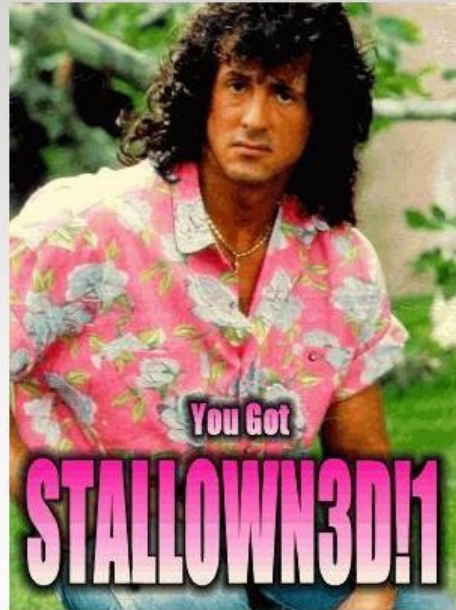




Koncové útoky

- defacement
- drive by, watering hole
- ransomware/spyware
- zero-day exploits

This page has been Hacked!



XSS Defacement

"> Search

Invalid list name.

Sociální inženýrství

- využívání lidské hlouposti a naivity
- phishing, spearphishing, whalephishing

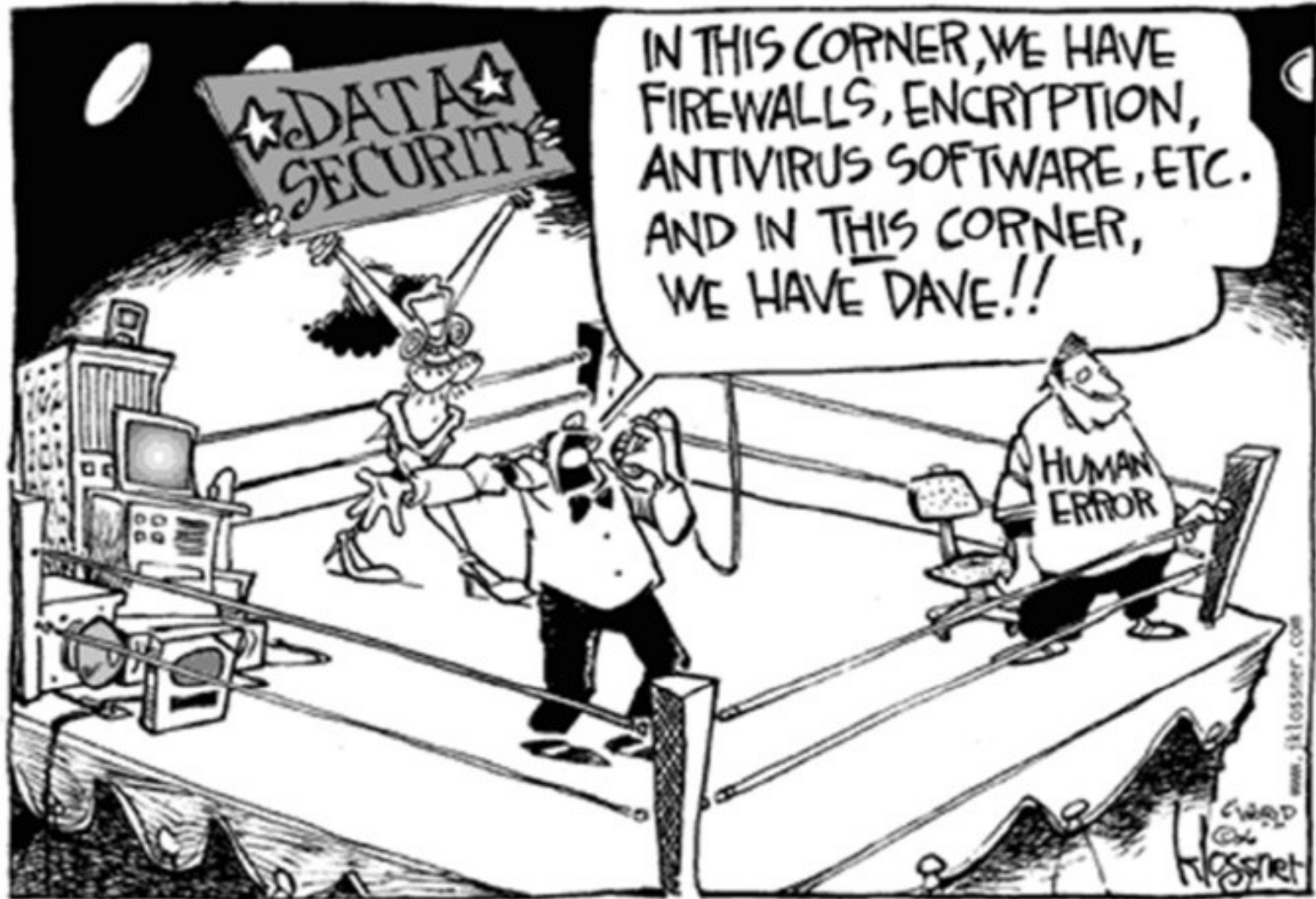
- slabost a opakování hesel
- přenosná média

SOCIAL ENGINEERING SPECIALIST

Because there is no patch
for human stupidity

- uživatelská podpora, servis, snaha pomoci
- na živo, po telefonu, mailem, IM

IN THIS CORNER, WE HAVE
FIREWALLS, ENCRYPTION,
ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER,
WE HAVE DAVE!!



Vypočetní síla

- kryptografie vs. mooreův zákon
- quantum computing

Kryptologie a bezpečnost

$$\textcircled{1} \quad y = f(x)$$

$$\Downarrow$$

$$y = c(x)$$

$$\textcircled{2} \quad \begin{aligned} y_0 &= \bar{x}_0 \bar{x}_1 \bar{x}_2 + x_1 x_2 \\ y_1 &= \bar{x}_0 \bar{x}_1 x_2 + x_0 \bar{x}_1 \bar{x}_2 + x_0 x_1 x_2 \\ y_2 &= x_0 \\ y_3 &= \bar{x}_0 \bar{x}_1 x_2 + \bar{x}_0 x_1 x_2 + x_0 x_1 \bar{x}_2 \end{aligned}$$

cleartext function
truth table

x_0	x_1	x_2	y_0	y_1	y_2	y_3
0	0	0	1	0	0	0
0	0	1	0	1	0	1
0	1	0	0	0	0	0
0	1	1	1	0	0	1
1	0	0	0	1	1	0
1	0	1	0	0	1	0
1	1	0	0	0	1	1
1	1	1	1	1	1	0

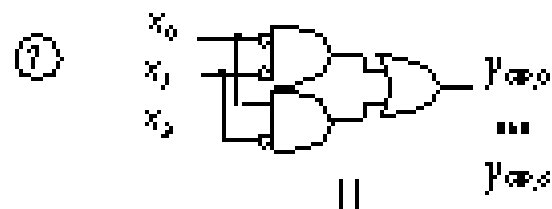
$\underbrace{\quad\quad\quad}_X \quad \underbrace{\quad\quad\quad}_Y$

GP

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} =$$

$\textcircled{4}$

$$Y_{GP} = Y \cdot GP$$



$$y_{GP} = c_{GP}(x)$$

$$\textcircled{5} \quad \begin{aligned} y_{GP,0} &= \bar{x}_0 \bar{x}_1 + x_0 \bar{x}_1 \\ y_{GP,1} &= \dots ; \quad \dots ; \quad y_{GP,6} = \dots \end{aligned}$$

partially encrypted function
truth table

x_0	x_1	x_2	$y_{GP,0}$	$y_{GP,1}$	$y_{GP,2}$	$y_{GP,3}$	$y_{GP,4}$	$y_{GP,5}$	$y_{GP,6}$
0	0	0	1	0	0	1	1	0	0
0	0	1	1	1	1	1	0	0	0
0	1	0	0	0	0	0	0	0	0
0	1	1	0	1	0	1	1	1	0
1	0	0	1	0	1	0	0	0	1
1	0	1	1	0	0	1	0	1	1
1	1	0	0	1	0	1	0	0	1
1	1	1	0	0	1	1	1	0	1

$\underbrace{\quad\quad\quad}_X \quad \underbrace{\quad\quad\quad}_Y$

$\textcircled{5}$

Figure 3: Encrypting a circuit : basic steps

For clarity sake, only GP matrix multiplication is represented. It produces a partially encrypted circuit c_{GP} . To obtain the encrypted circuit c' , it is necessary to use S and ztoo. The function to encrypt (1) is represented as a Boolean circuit c (2). The output matrix Y (3) is multiplied by GP (4). The result (5) is the partially encrypted output matrix Y_{GP} . It can be represented by the corresponding Boolean equations (5) or as a "partially encrypted circuit" c_{GP} (7).

Základní úvod

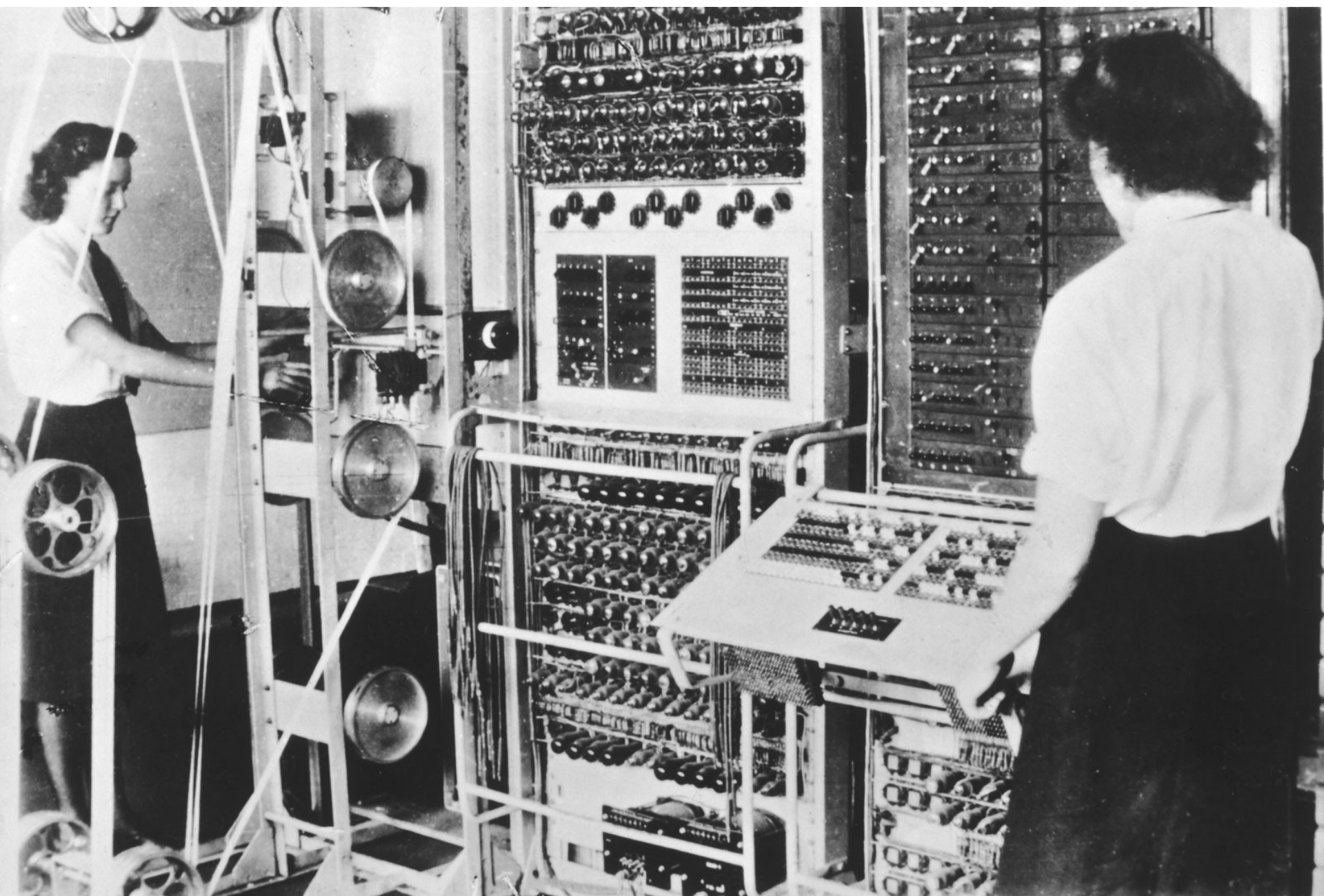
- bez matematiky
- a s obrázky
- kryptologie, kryptografie, kryptoanalýza

Historie

- od antiky
- pozvolný vývoj až do novověku
- revoluce ve 20. století (váčky)
- současnost

Prolamování kódů

- frekvenční analýza
- repetice
- chyby operátorů
- kódové knihy
- hrubá síla



Některé pojmy

- Steganografie
 - kdysi a dnes
 - text, obrázky, hudba, neviditelný inkoust...
- Hash
 - + salt
- „Security through obscurity“
 - dat, algoritmu, klíče
- Symetrie a asymetrie šifer
 - „handshake“

Examples of steganography

Example 1: Coded message

Apparently neutral's protest is thoroughly discounted and ignored.

Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.

Take second letter of each word to get message:

Pershing sails from NY June 1

Example 2: Coded images: Least Significant Bits (LSB) insertion

Original image



Altered image



□ Areas where binary code of pixel has been altered

Binary code from original image pixel **1**

10000000 10100100 10110101 10110101 11110011 10110111 11100111 10110011 00110000

Changes made on altered image pixel **1**

1000000**1** 10100100 1011010**0** 1011010**0** 1111001**0** 1011011**0** 1110011**0** 10110011 0011001**1**

Read last digit:

1000001 which is ASCII binary code for A

1 2 3 4

Fox

Hash
function

DFCD3454

The red fox
runs across
the ice

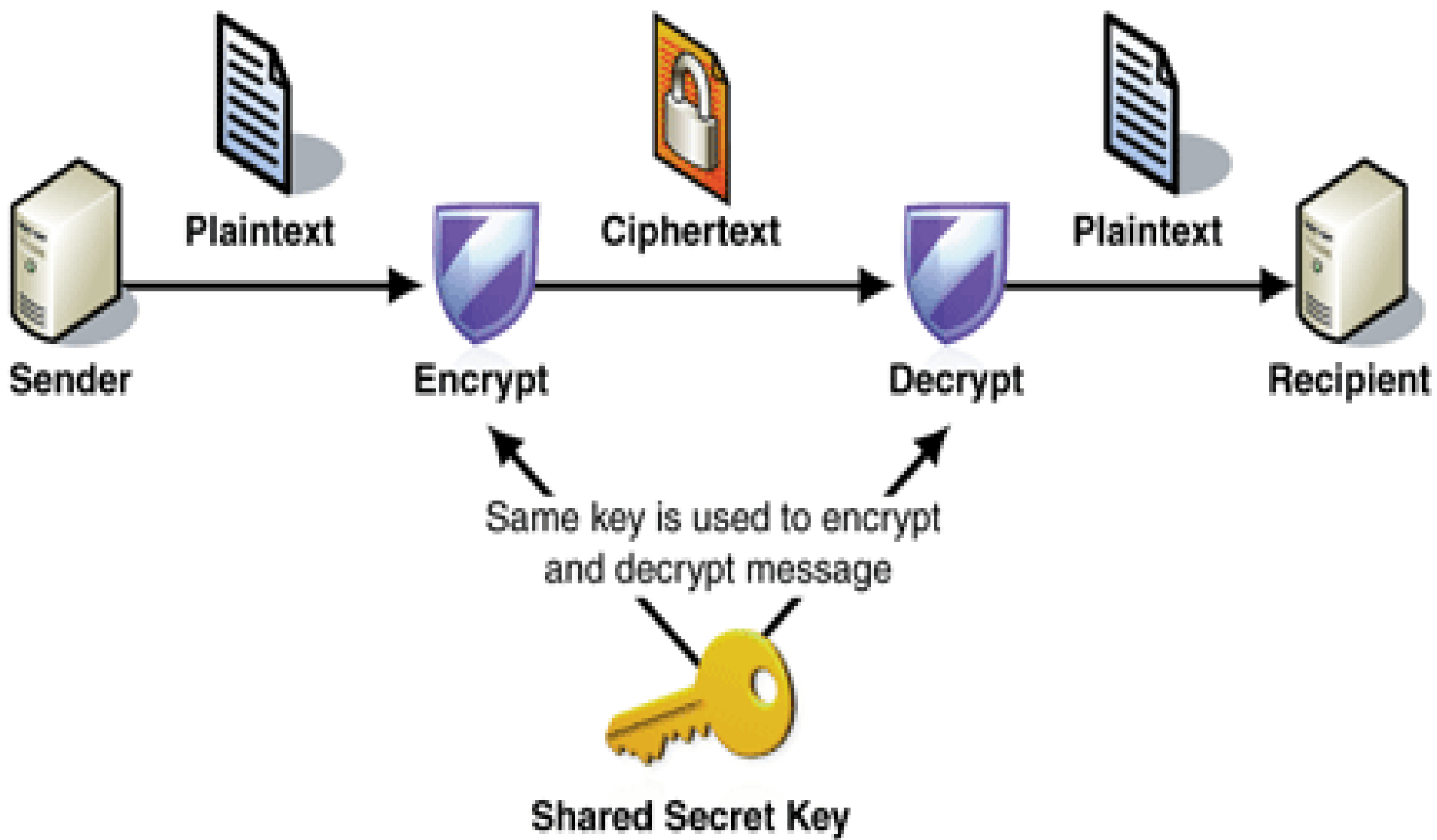
Hash
function

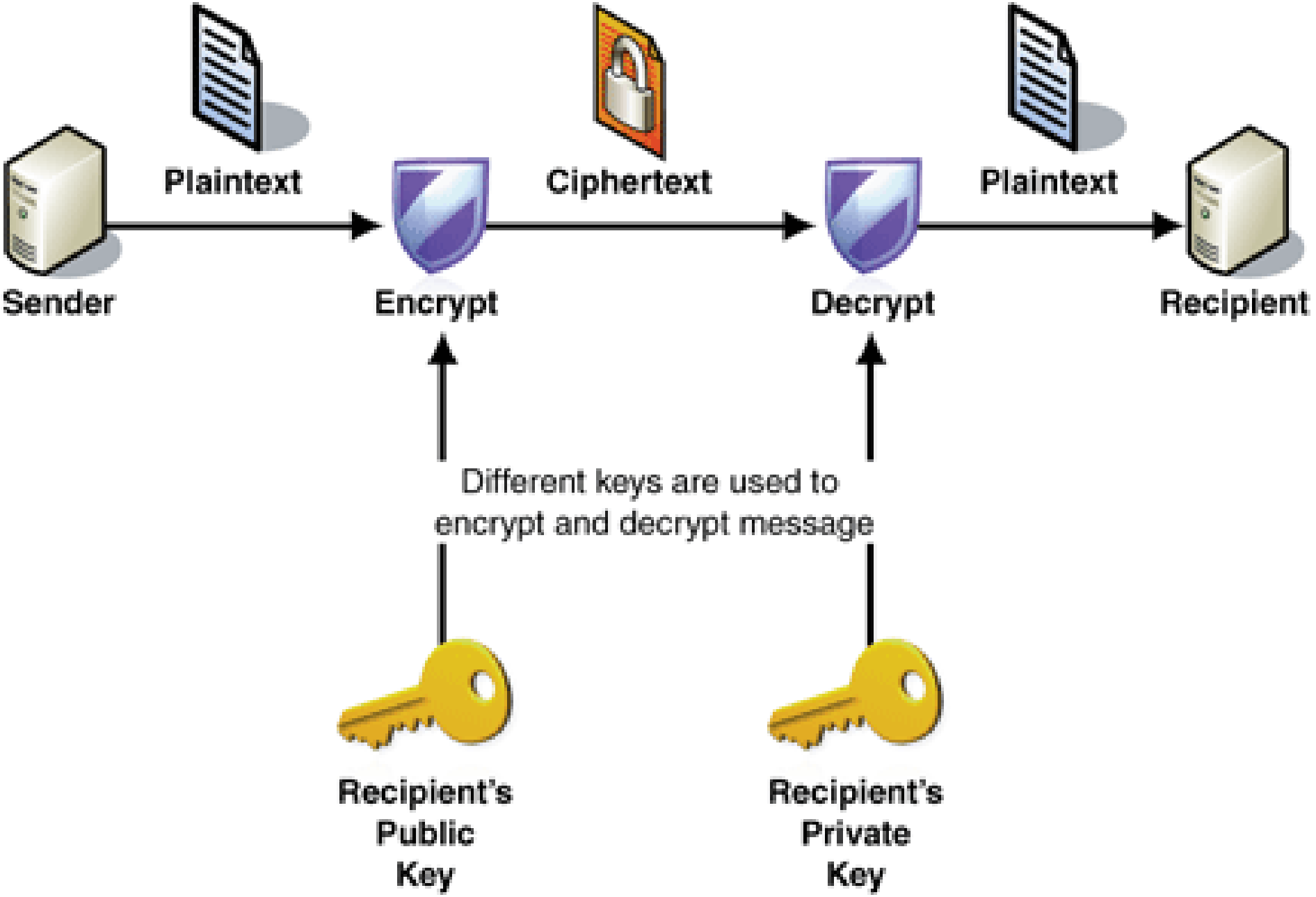
52ED879E

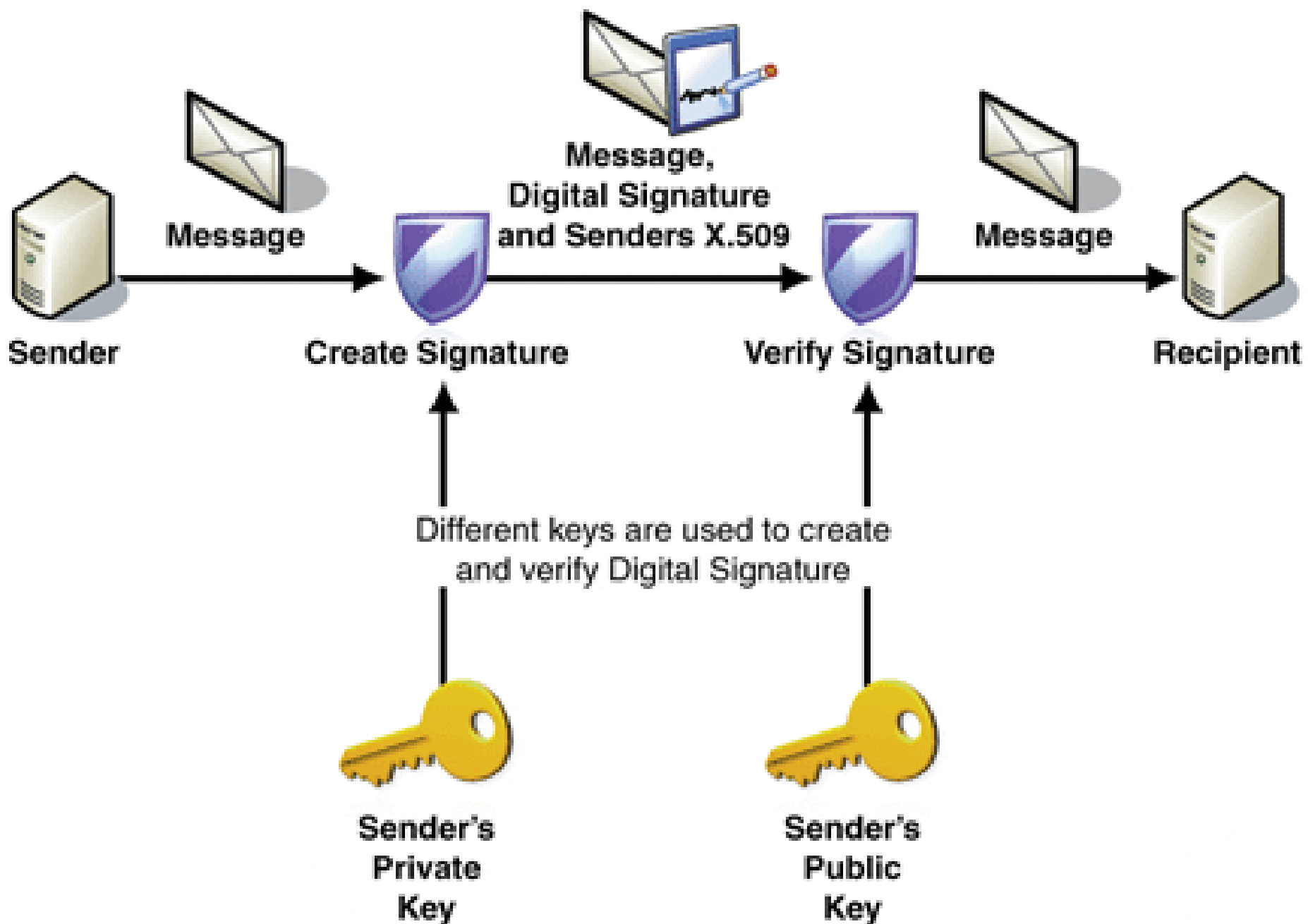
The red fox
walks across
the ice

Hash
function

46042841







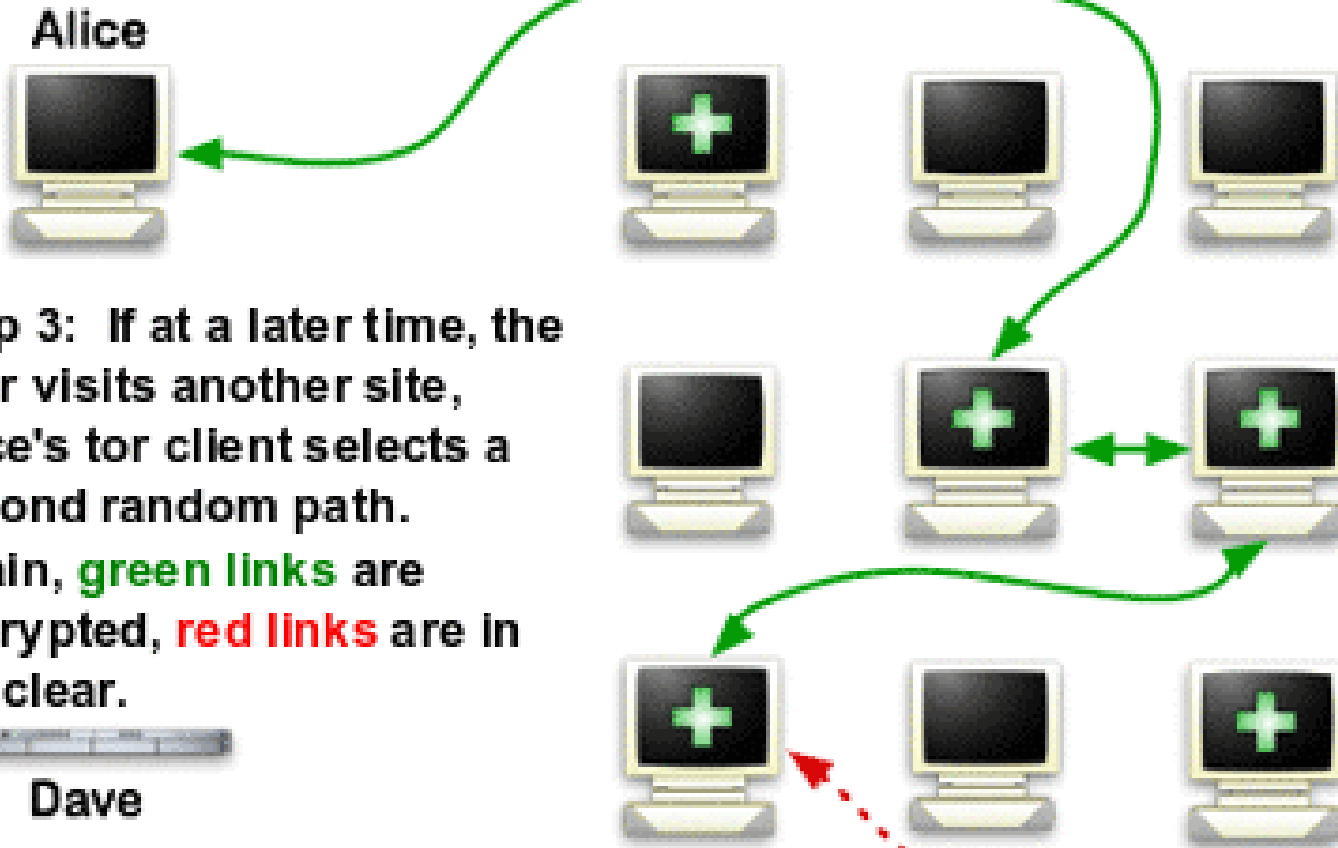
Současné využití

- všude a pořád
- digitální podpis
- bankovníctví
- komunikace

- TOR

How Tor Works: 3

-  Tor node
-  unencrypted link
-  encrypted link



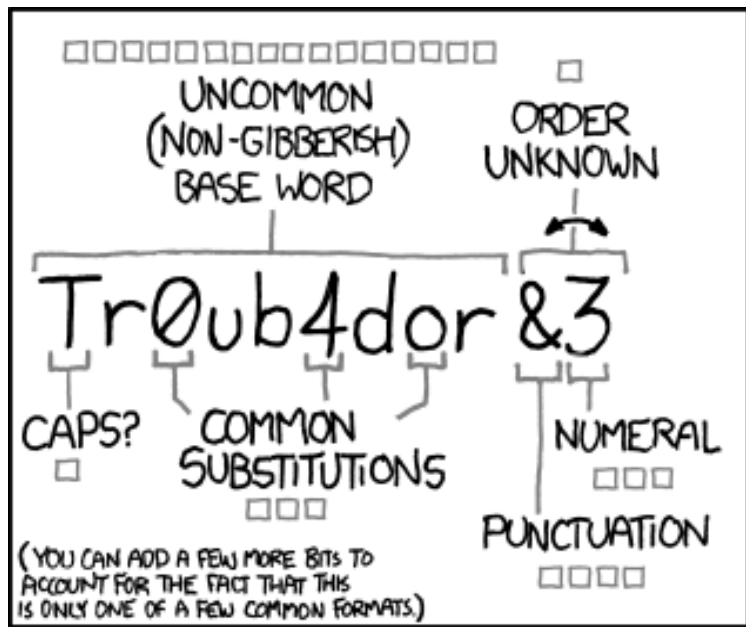
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.


Dave


Jane


Bob

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

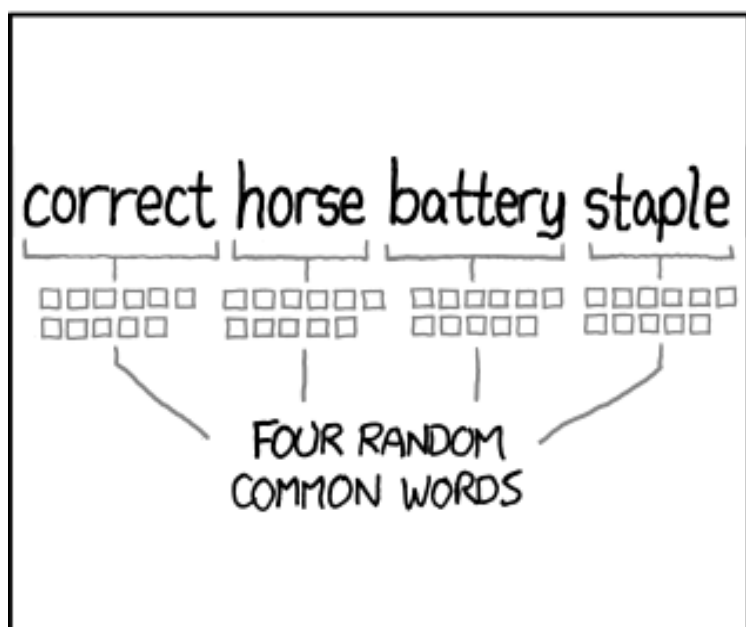
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

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.

Možná řešení

- password managers
- password policies
 - komplexita
 - neopakování

Výpočetní síla

- stále delší klíče
- Moore's Law
- kvantové procesory?

CIA(N)

- confidentiality
- integrity
- authentication
- non-repudiation

Řízení přístupu

- identifikace, autorizace, autentizace
- co jste, znáte, máte
- biometrika
 - výhody, nevýhody
 - FAR, FRR

Biometrics

Physiological

face



fingerprint



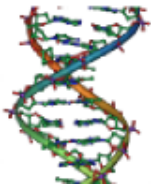
hand



iris



DNA



Behavioral

keystroke



signature



voice

