EDAF35: OPERATING SYSTEMS

MODULE 9.B
SECURITY

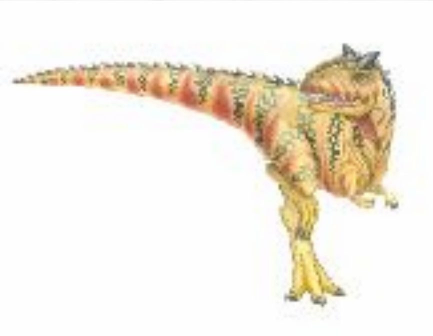
CONTENTS

SECURITY

- Basic Terminology
- Threats and Attacks
- Encryption, Authentication, Hashing
- Cryptography in Computing
- Countermeasures to Attacks

MATERIAL FOR SEVERAL WHOLE COURSES!

CHAPTER 15
SECURITY



BASIC TERMINOLOGY

SECURITY

- system is **secure** — if resources are used and accessed as intended at all time ("protection": internal problem, "security": includes environment/external actors)
- **intruders/crackers**
- **threat** — potential security violation
- **attack** — attempt to breach security (accidental or malicious)
- types of violations

BREACH OF CONFIDENTIALITY
BREACH OF INTEGRITY
BREACH OF AVAILABILITY
THEFT OF SERVICE
DENIAL OF SERVICE

Methods

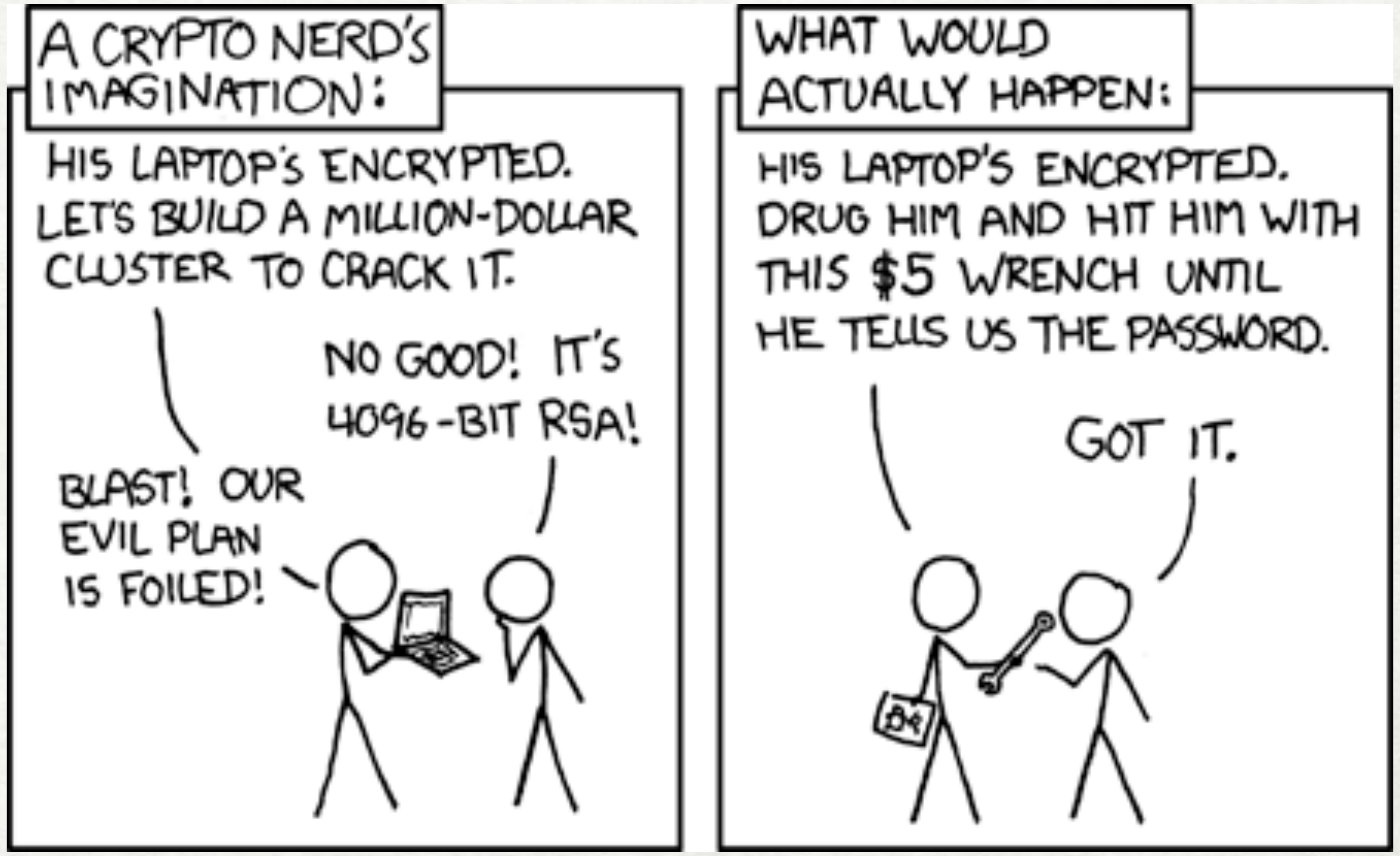
MASQUERADING
REPLAY ATTACK
MAN-IN-THE-MIDDLE
SESSION HIGHJACKING

SECURITY IS ABOUT THE WHOLE SYSTEM

- Address all levels:
  - Physical
  - Human
  - OS/Applications (includes protection, logging, debugging)
  - Networking/Connectivity

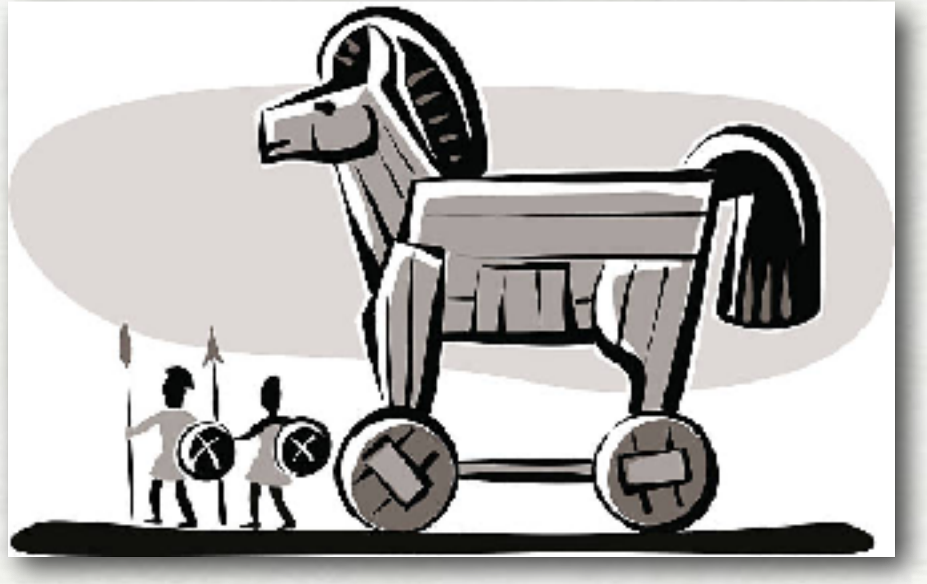
STRENGTH IS DECIDED BY THE WEAKEST LINK

https://xkcd.com/538/


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.

PROGRAM THREATS

MANY TYPES OF MALWARE



Trojan Horse

Logic Bomb

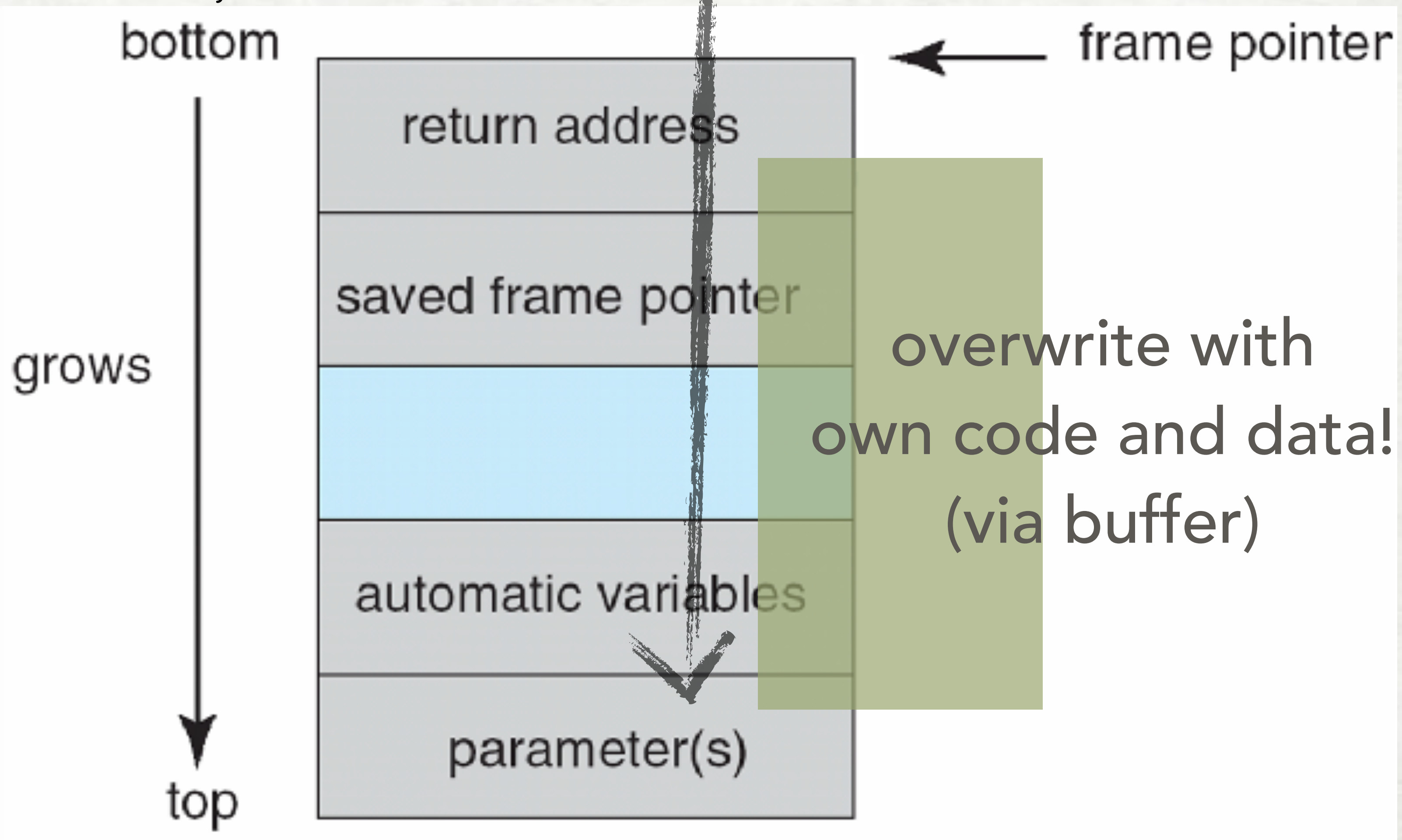
Trapdoor/Backdoor

Viruses

SEE ALSO
RETURN-ORIENTED
PROGRAMMING

Stack/Buffer overflow

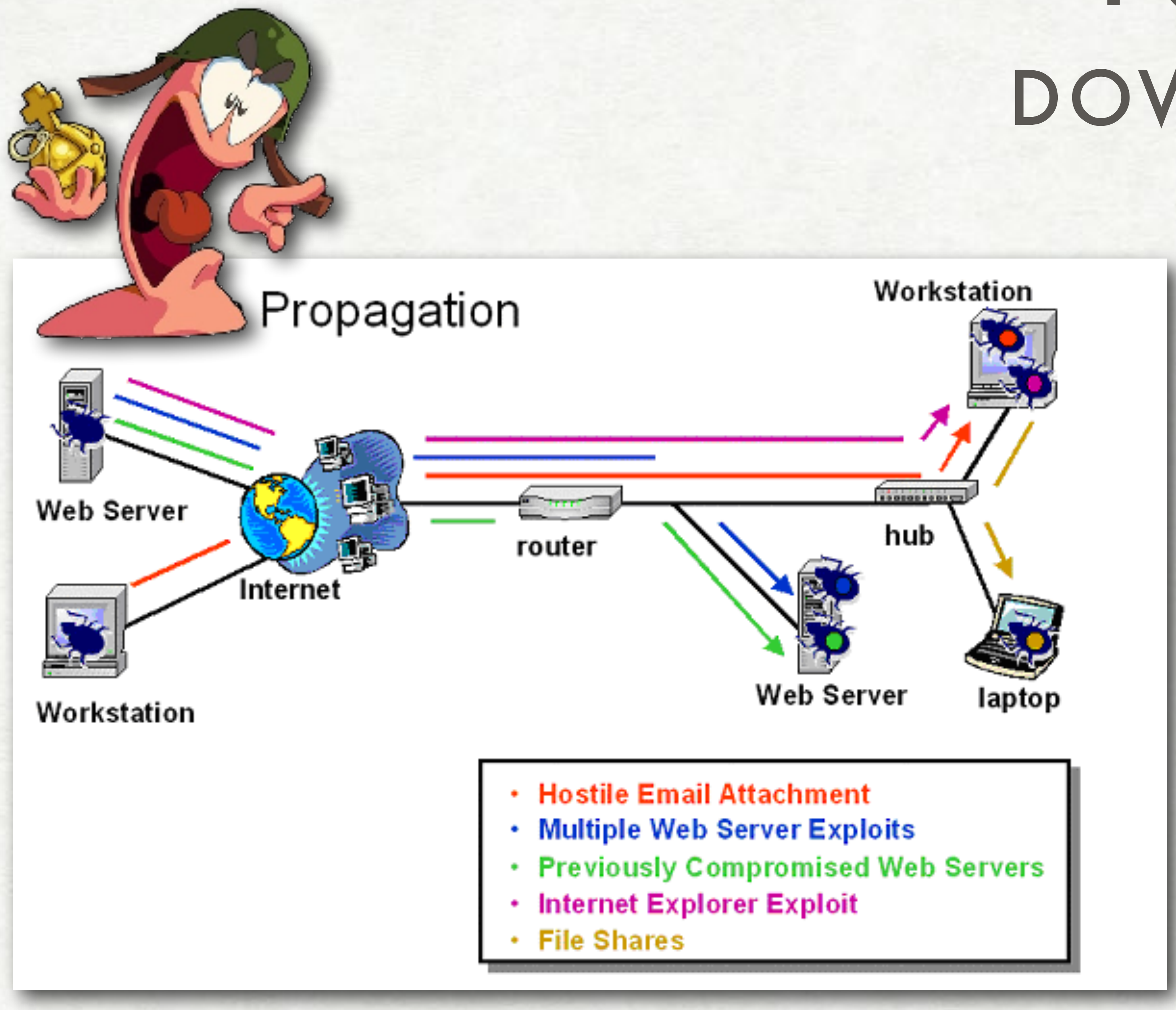
```
#include <stdio.h>
int main(int argc, char *argv[])
{
  char buffer[256];
  if (argc < 2)
     return -1;
  else {
     strcpy(buffer, argv[1]);
     return 0;
  }
}
```



overwrite with
own code and data!
(via buffer)

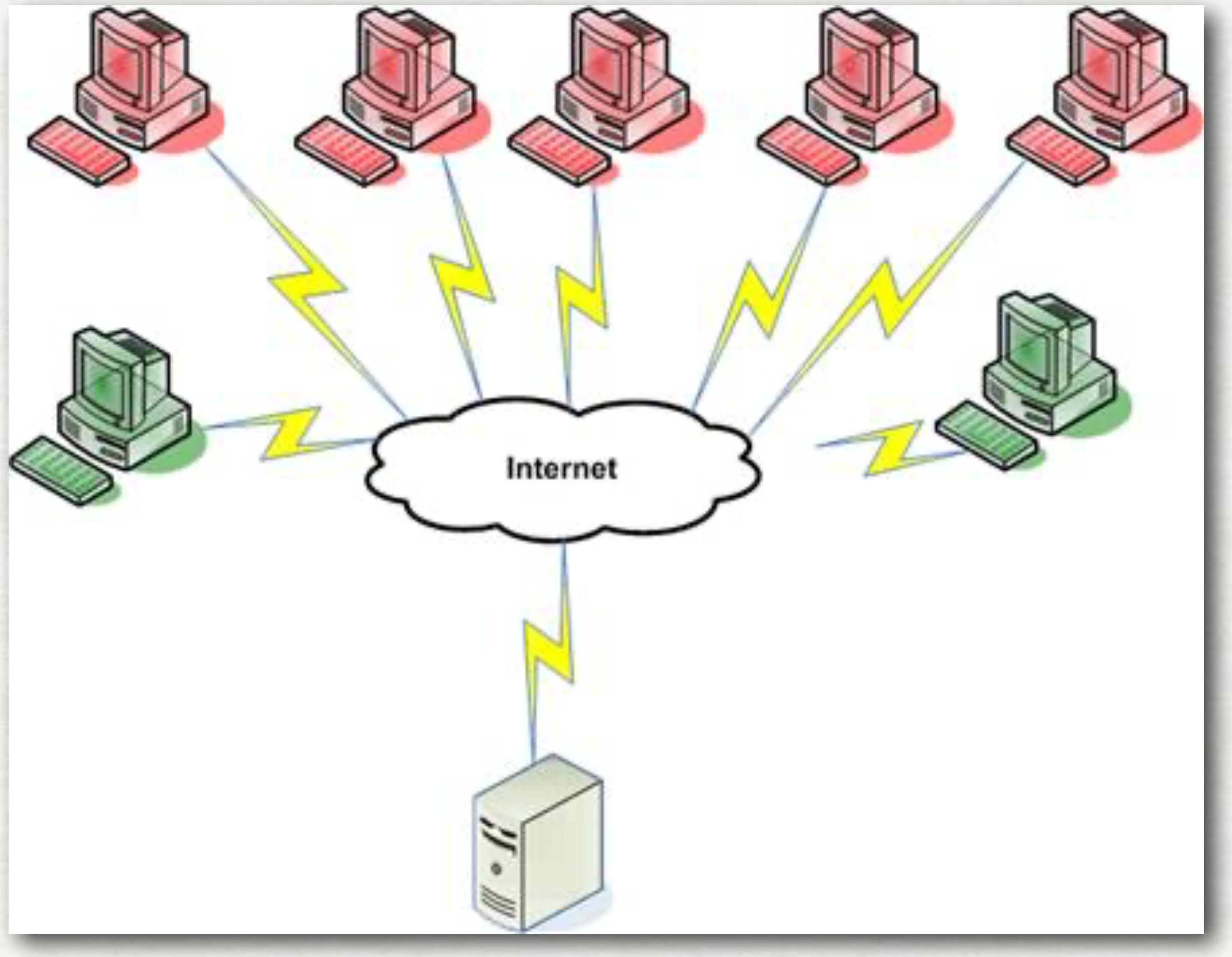
NETWORK THREATS

DOWNSIDE OF CONNECTIVITY


Propagation
Workstation
Web Server
Internet
router
hub
Workstation
Web Server
laptop
• Hostile Email Attachment
• Multiple Web Server Exploits
• Previously Compromised Web Servers
• Internet Explorer Exploit
• File Shares

Worms
(propagate across network
via multiple exploits)

Port scanning
(obtain information about
the system; open services)

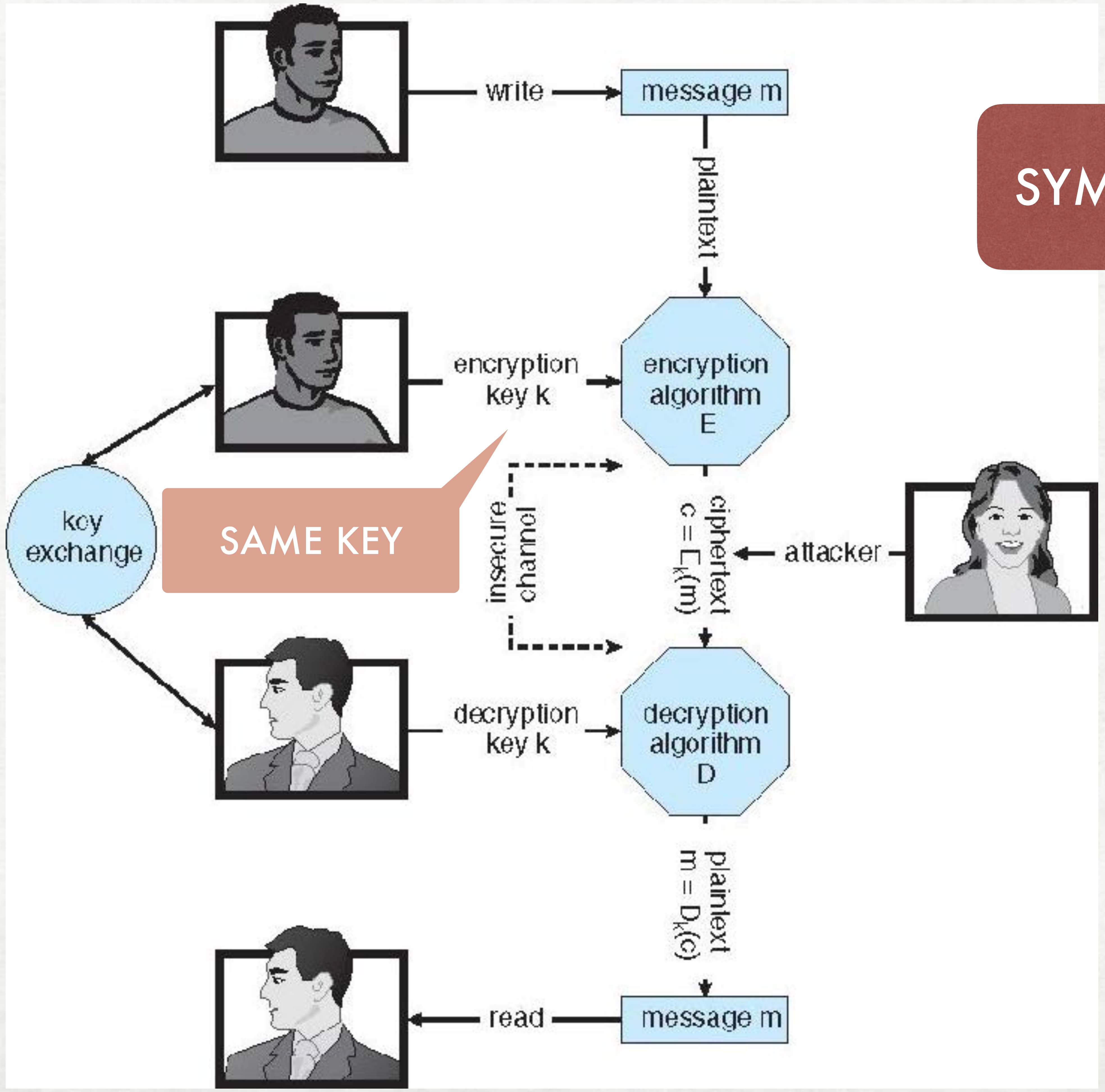


(Distributed) Denial of Service (DoS)

CRYPTOGRAPHY AS A TOOL

SECURITY

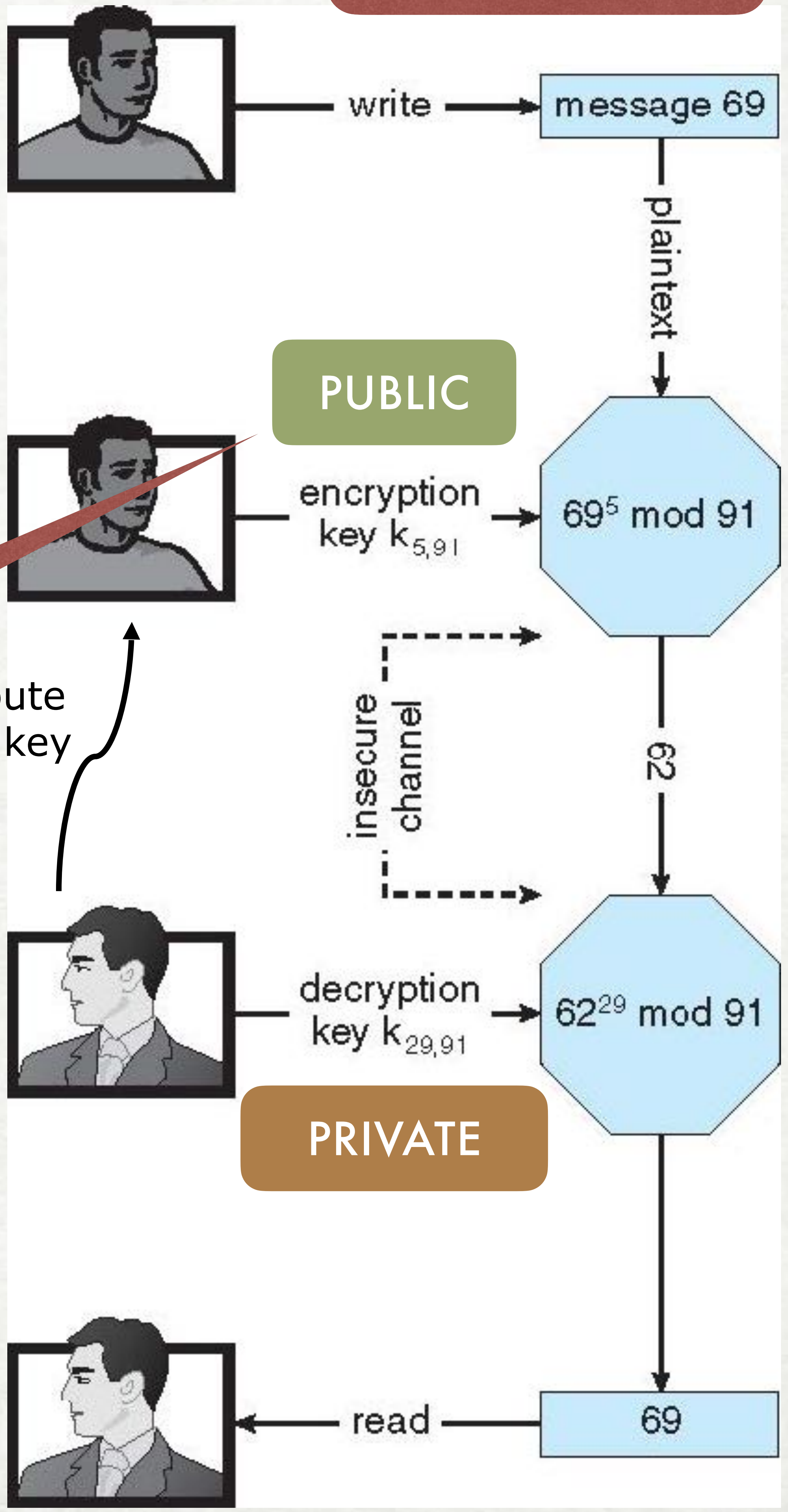
- use secrets (keys) to scramble messages



SAME KEY

SYMMETRIC

ASYMMETRIC



PUBLIC

PRIVATE

Distribute public key K5,91

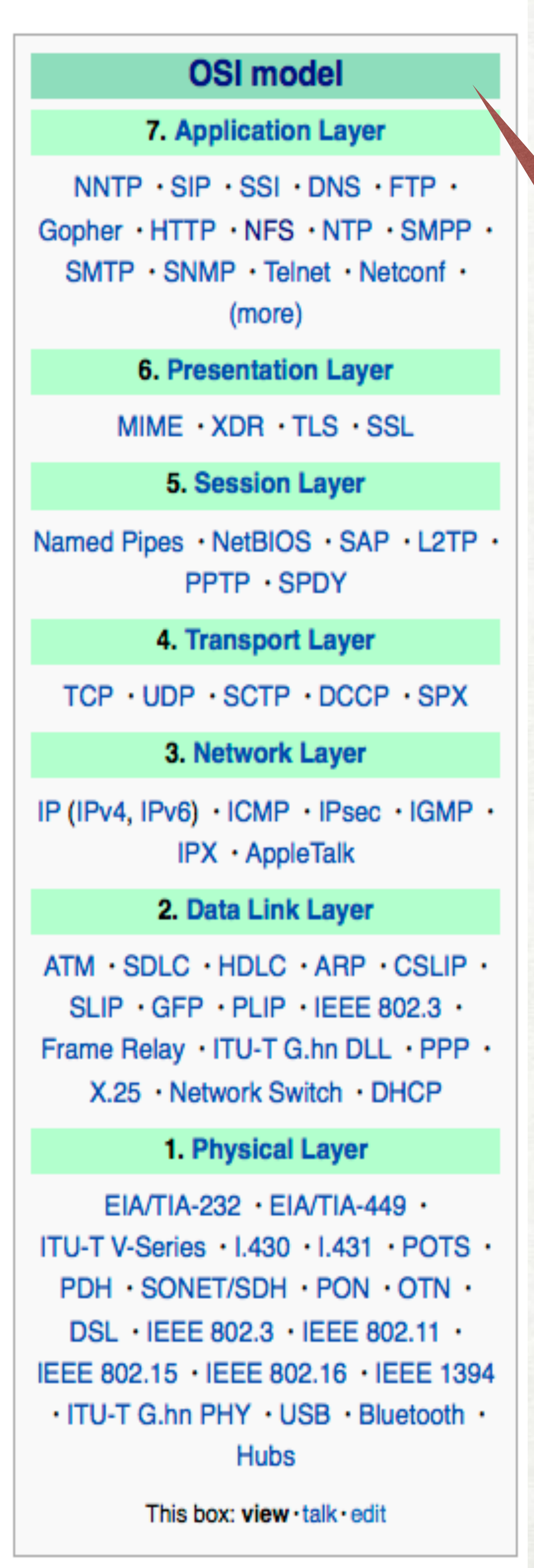
AUTHENTICATION:

E.G. TURN THESE AROUND! (SOURCE IS PROVEN)

HASHING:

PRODUCE A (SHORT) MESSAGE DIGEST (UNIQUE) – SHA-1, MD5 –

COMPUTER SYSTEMS AND SECURITY



OSI model

7. Application Layer

NNTP · SIP · SSI · DNS · FTP · Gopher · HTTP · NFS · NTP · SMPP · SMTP · SNMP · Telnet · Netconf · (more)

6. Presentation Layer

MIME · XDR · TLS · SSL

5. Session Layer

Named Pipes · NetBIOS · SAP · L2TP · PPTP · SPDY

4. Transport Layer

TCP · UDP · SCTP · DCCP · SPX

3. Network Layer

IP (IPv4, IPv6) · ICMP · IPsec · IGMP · IPX · AppleTalk

2. Data Link Layer

ATM · SDLC · HDLC · ARP · CSLIP · SLIP · GFP · PLIP · IEEE 802.3 · Frame Relay · ITU-T G.hn DLL · PPP · X.25 · Network Switch · DHCP

1. Physical Layer

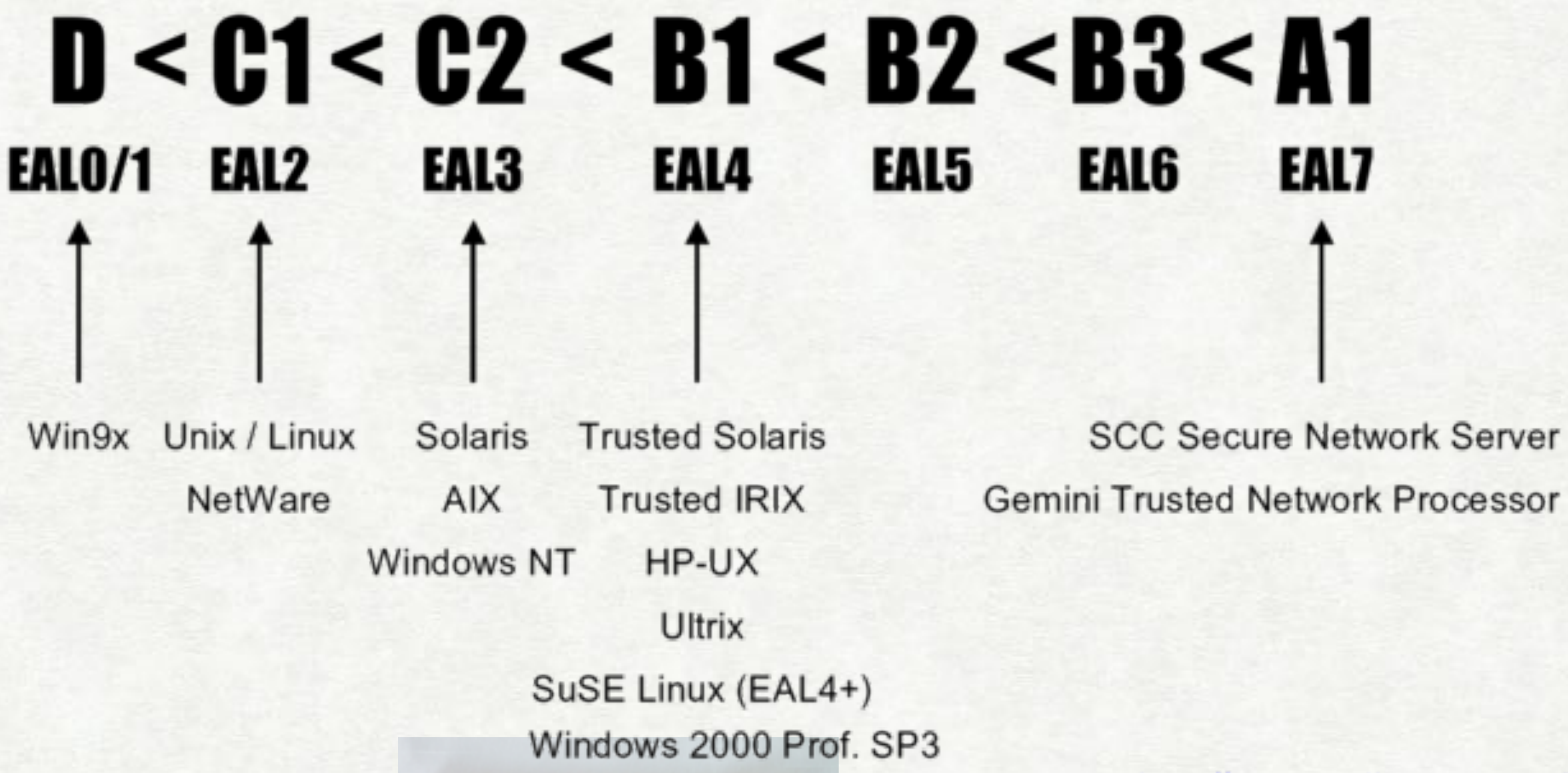
EIA/TIA-232 · EIA/TIA-449 · ITU-T V-Series · I.430 · I.431 · POTS · PDH · SONET/SDH · PON · OTN · DSL · IEEE 802.3 · IEEE 802.11 · IEEE 802.15 · IEEE 802.16 · IEEE 1394 · ITU-T G.hn PHY · USB · Bluetooth · Hubs

This box: view · talk · edit

SECURITY (CRYPTOGRAPHY) NEEDED AT ALL LEVELS
FOR NETWORKED SYSTEMS

+ USER AUTHENTICATION, INTRUSION DETECTION, AUDITING, ACCOUNTING, LOGGING, FIREWALLING, ...

Trusted Computer System Evaluation Criteria



D < C1 < C2 < B1 < B2 < B3 < A1

EAL0/1 · EAL2 · EAL3 · EAL4 · EAL5 · EAL6 · EAL7

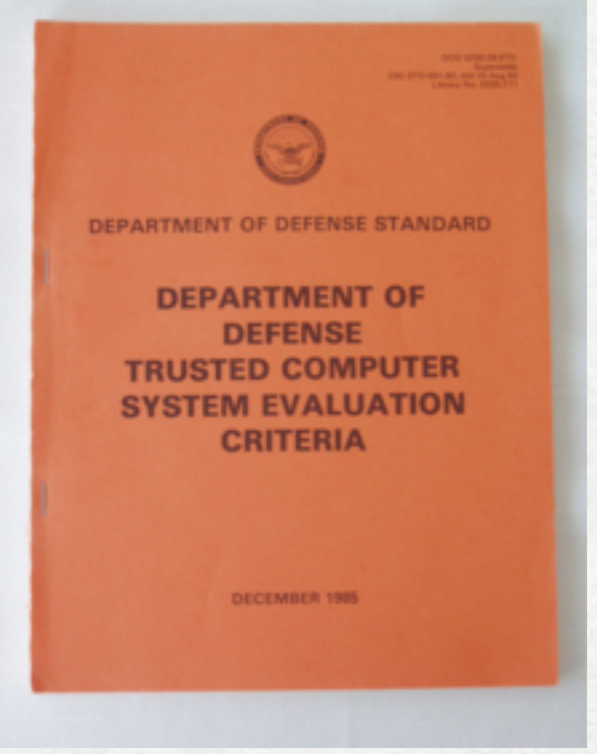
EAL0/1: Win9x

EAL2: Unix / Linux, NetWare

EAL3: Solaris, AIX, Windows NT

EAL4: Trusted Solaris, Trusted IRIX, HP-UX, Ultrix, SuSE Linux (EAL4+), Windows 2000 Prof. SP3

EAL7: SCC Secure Network Server, Gemini Trusted Network Processor


DEPARTMENT OF DEFENSE STANDARD
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
DECEMBER 1985

http://www.radium.ncsc.mil/tpep/
http://niap.nist.gov/cc-scheme/vpl/vpl_type.html

RELATED READING TOPICS

IF YOU WANT TO KNOW MORE

- **(Secure) Multi-Party Computation**
  - N parties compute a function together without sharing inputs
  - *e.g. cross-referencing flight passenger manifests with suspect lists*
- **Homomorphic Encryption**
  - F(enc(A), enc(B)) = enc(F(A, B))
  - *e.g. querying encrypted databases*
- **Safe, Narrow AI**
  - Federated ML, anonymous, local training on private data
  - *e.g. OpenMined.org*

END OF MODULE 9.B