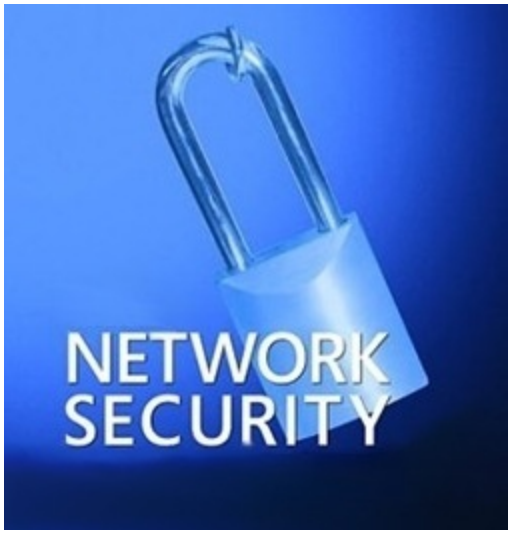


Layered Network Security

Achmad Mardiansyah

achmad@glcgroup.co.id

http://www.glclearningcenter.com

Agenda

- Introduction
- Layered Network
- Security
- Network Security
- Some security Techniques
- Layered security
- Demo
- Question and answer

About me…

- Name: Achmad Mardiansyah
- Born: Malang, base: bandung
- Linux user since ’99
- Certified trainer (MTCRE/WE/INE/TCE)
- MT Certified Consultant
- Work: Telco engineer, Sysadmin, PHP programmer, and Lecturer
- Founder of GLC (Garda Lintas Cakrawala)

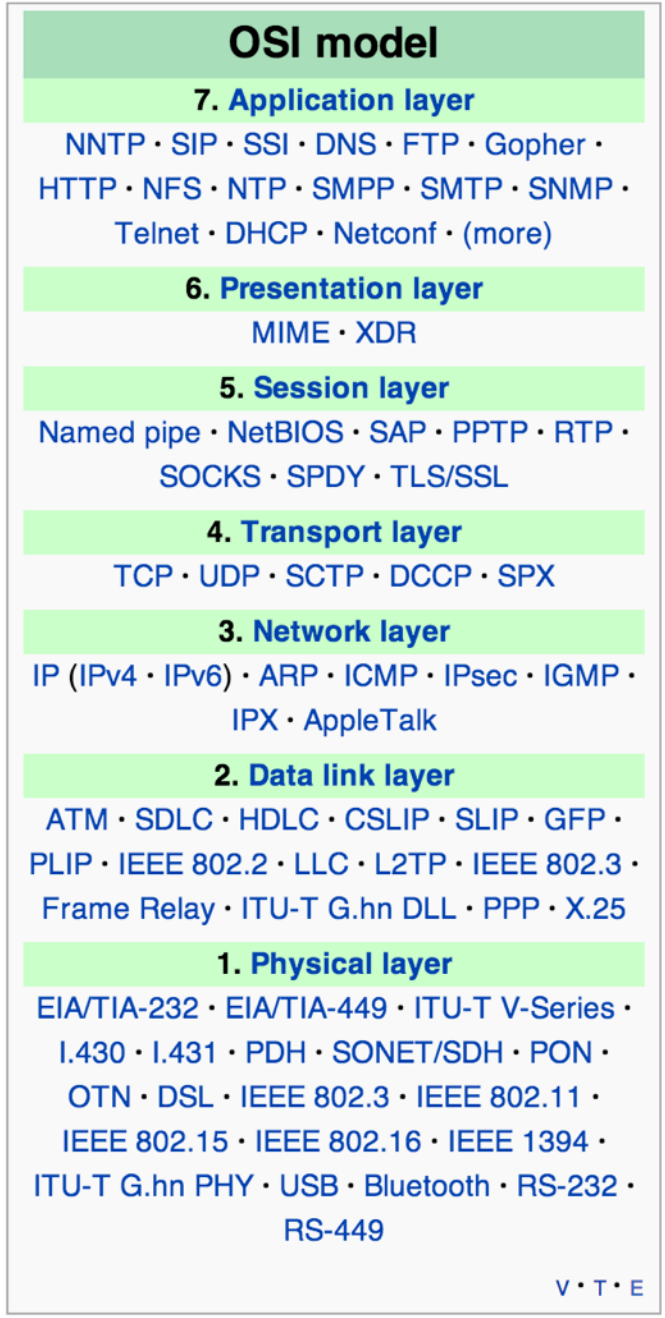
About GLC

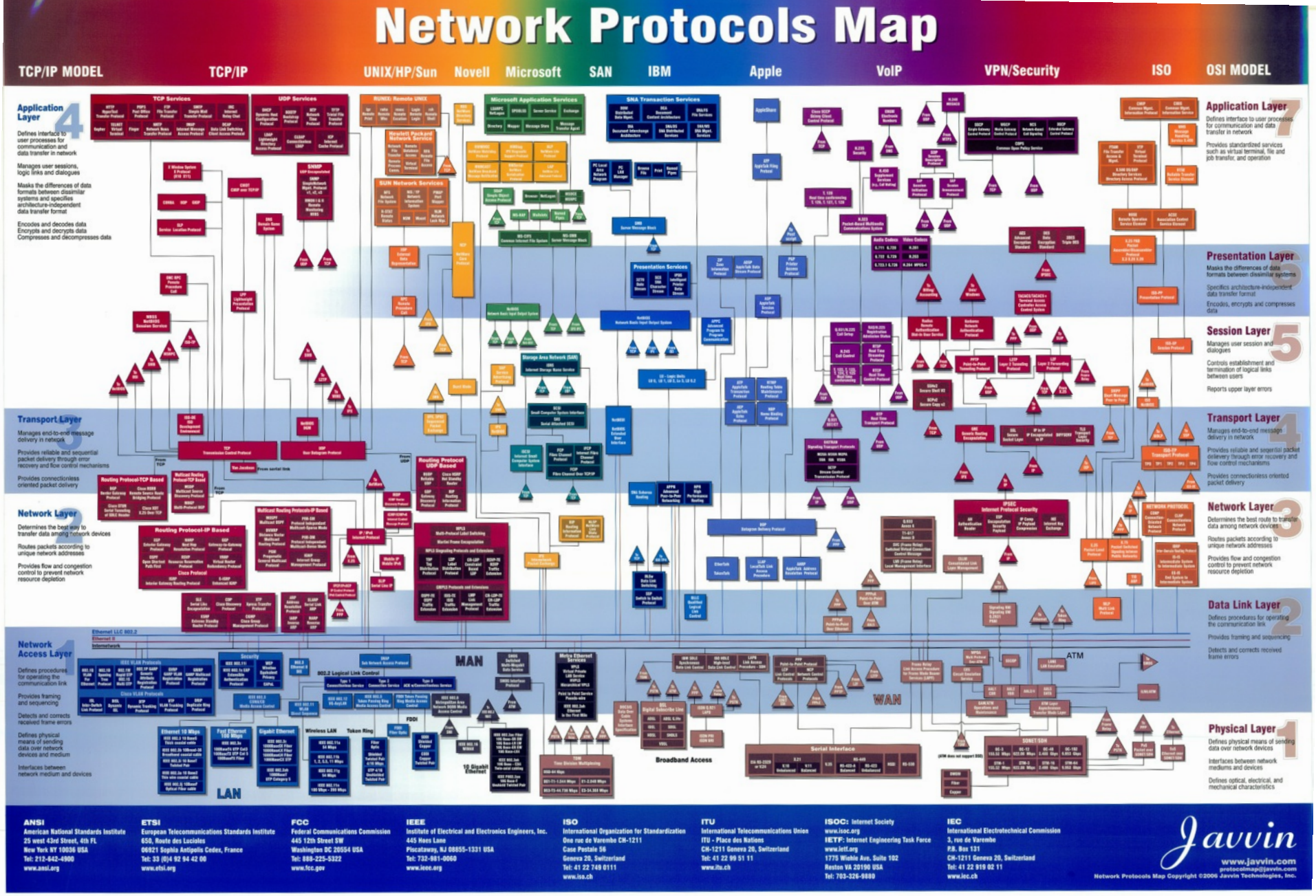
- GLC: Garda Lintas Cakrawala
- Mikrotik Certified Training Partner
- Based In Bandung and Jakarta
- Provides Mikrotik training & IT Consulting

Layered network (why?)

- Modular Engineering (localise problem)
- Accelerate Innovation
- Standardise interface (interoperability)
- Simplify Teaching and learning

All rules will be written in protocol & there an encapsulation process




Network Protocols Map
TCP/IP MODEL
TCP/IP
UNIX/HP/Sun
Novell
Microsoft
SAN
IBM
Apple
VoIP
VPN/Security
ISO
OSI MODEL
Application Layer 4
Transport Layer
Network Layer
Network Access Layer
Application Layer 7
Presentation Layer 6
Session Layer 5
Transport Layer 4
Network Layer 3
Data Link Layer 2
Physical Layer 1
LAN
MAN
WAN
ATM
Broadband Access
ANSI
ETSI
FCC
IEEE
ISO
ITU
ISOC: Internet Society
IETF: Internet Engineering Task Force
IEC
Javvin
www.javvin.com
Network Protocols Map Copyright ©2006 Javvin Technologies, Inc.

now, lets talk about security…

Why Security?

Hierarchy of human needs (maslow)

- Physical
- **Safety**
- Love and Belonginess
- Self esteem
- Actualization

If you need security,

It means you are a human

Source: http://api.ning.com/files/INnqY9i4XHGdNS2YgJRoID08FFSTs5MIqobVojrvxgvDVDWiiRe2OvNX8d5DjSQqmcZHx1mDzIi8KHzOt7kbMpwm02njyhKZ/MASLOW.jpg

Some kinds of security and evolution..

- Information Security
  - Physical & administrative means. Eg. Filing cabinet
- Computer Security
  - Local computer
- **Network/Internet Security**
  - Protection of transmitted data
  - Our focus

Source:
http://www.dailynews.lk/2009/07/27/z_page-06-Defining-cyber-..jpg

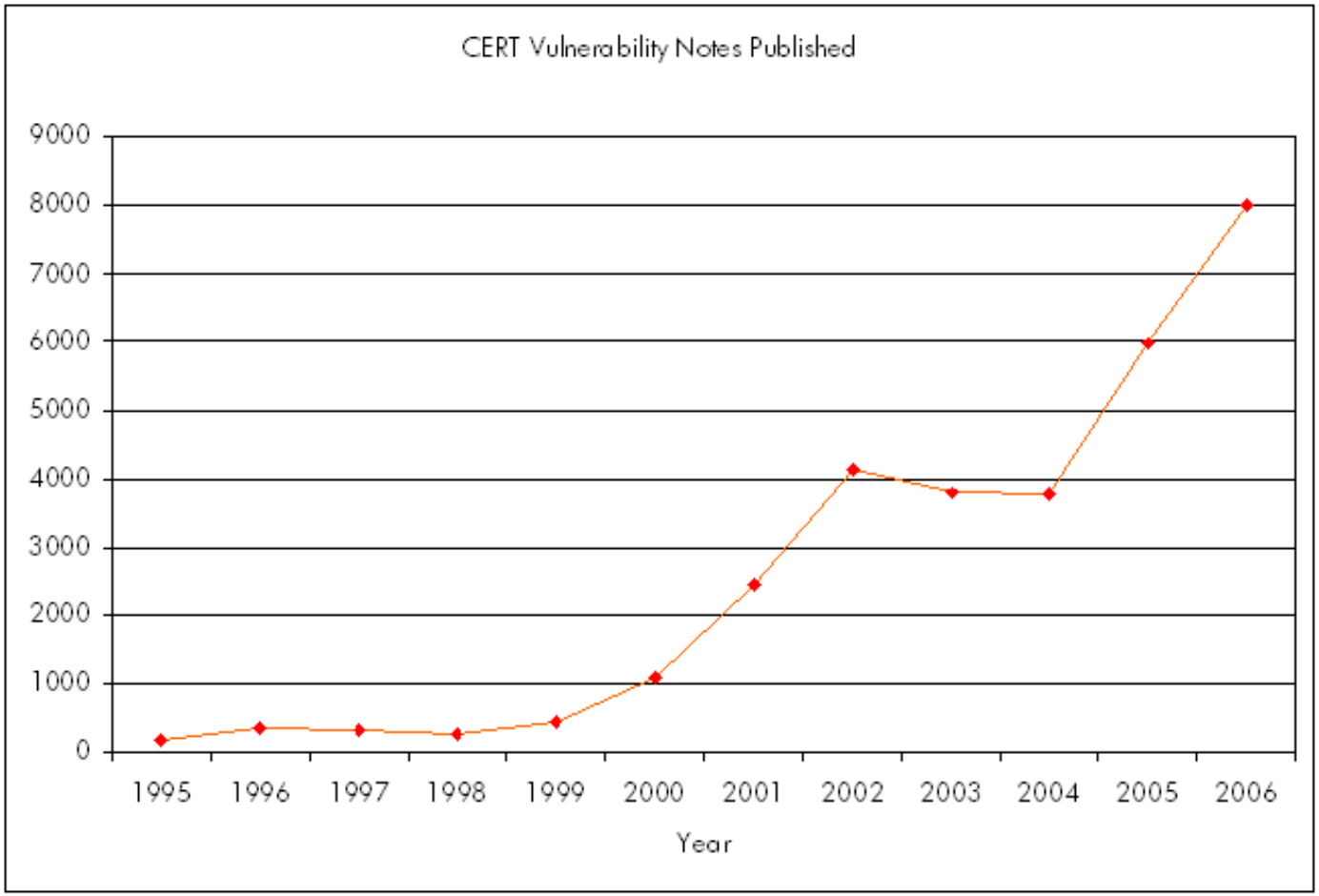
Vulnerability & incident

A vulnerability means: a **weakness** of a system.

If this is exploited, the results is **incidents**.

Source:
http://www.dl4all.com/software/17107-web-vulnerability-scanner-v5.1.70829.html

Vulnerability is growing…



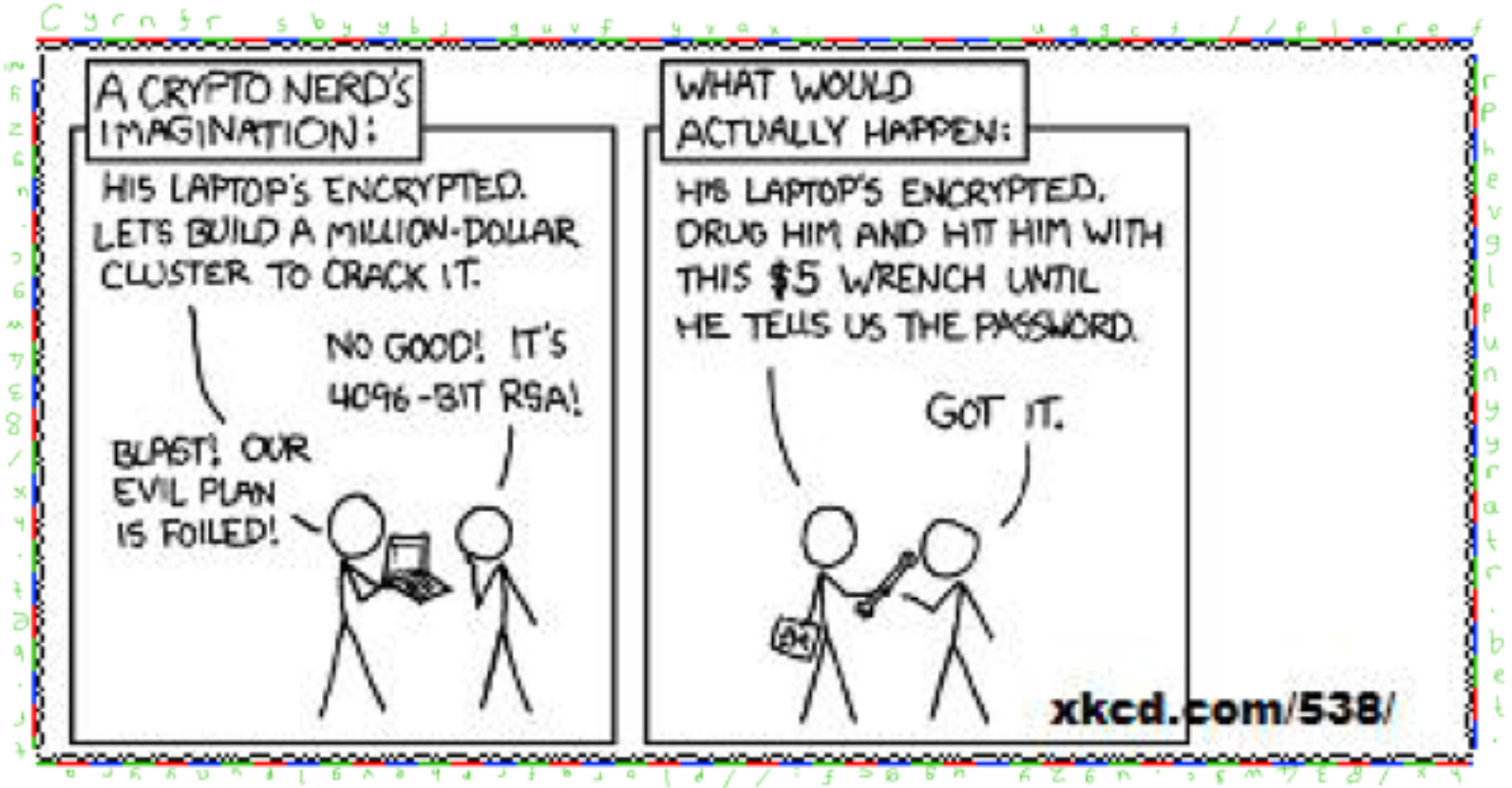
Source:
http://docs.hp.com/en/5991-7435/img/VulNotesPub.png

Some sources of vulnerability

- Flaws in software / protocol **design**
  - Eg. NFS, TFTP
- Weaknesses in **how protocols implemented**
  - Eg. Email system (open relay, no sender auth)
- Weaknesses in **how software implemented**
  - Eg. Microsoft file-sharing (IPC)
- Weaknesses in **system**
  - Eg. password cracking, privilege escalation
- Weaknesses in **network** configuration
  - Eg. Anonymous FTP

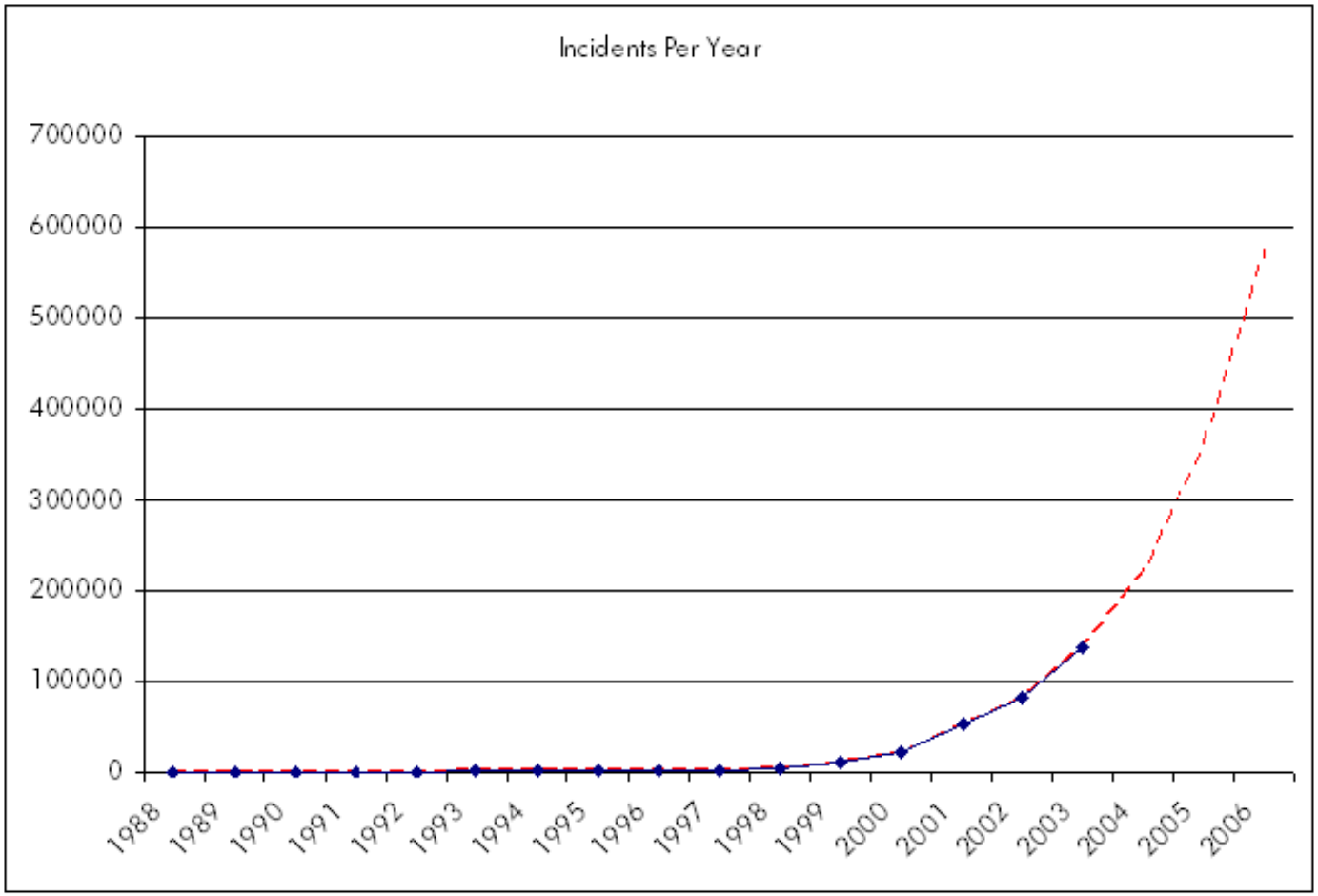
Source:
http://www.bhconsulting.ie/weaklink.jpg

Vulnerability isn't always techie..



Source:
http://www.jibble.org/cyber-security-challenge-uk-winner/xkcd-decoded.png

Incidents & internet growth

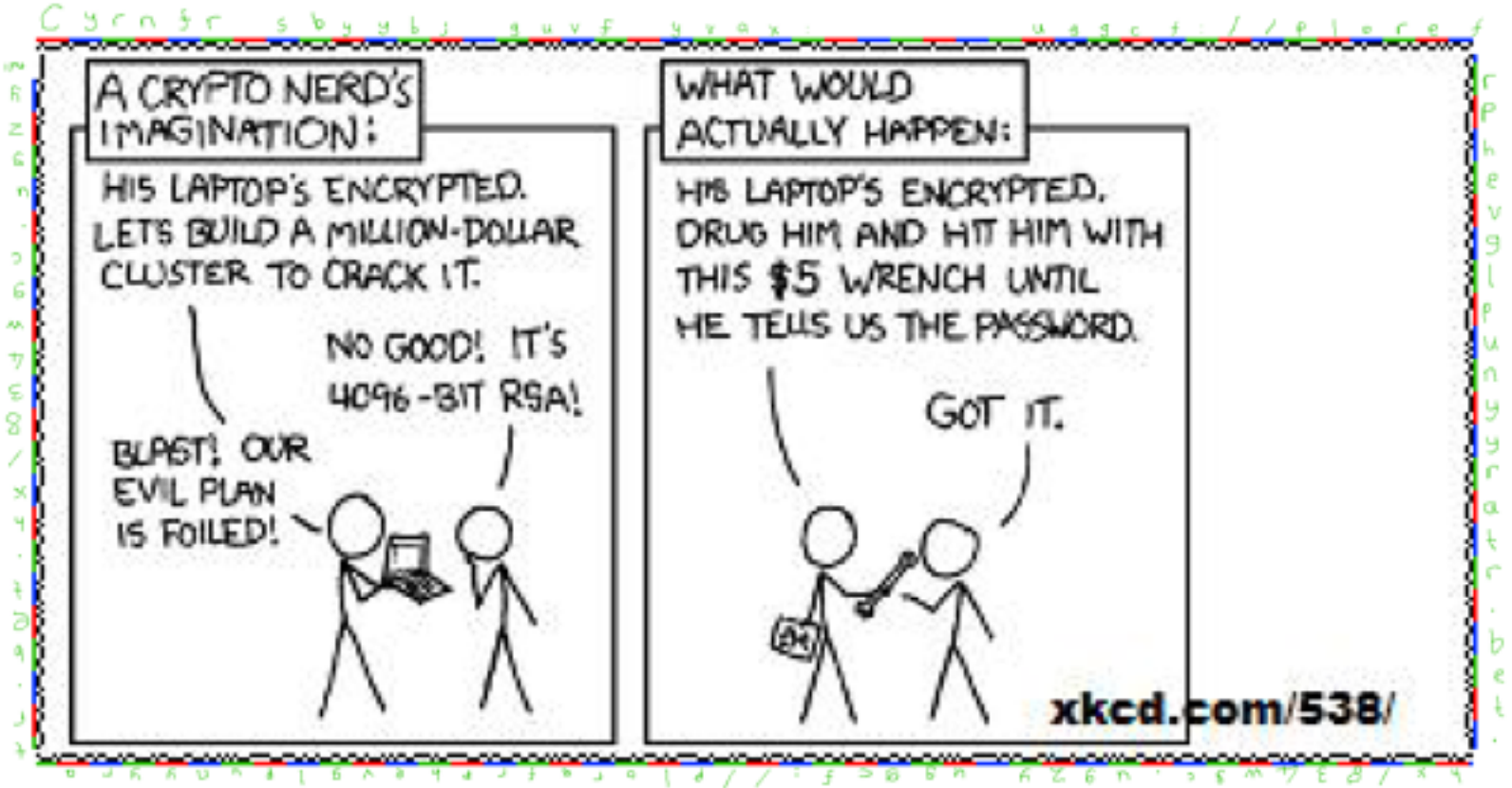


Some sources of incidents

- **Probe**, unusual attempts to gain information
- **Scan**, large number of probes
- **Account compromise**, unauthorized use of an account
- **Sniffer**, similar to above
- **Root compromise**, captures information
- **Denial of Service (DOS)**, makes services not available
- **Exploitation of trust**, make trust of foreign system
- **Malicious code**, cause undesired result. Eg. Virus, deface, injection
- **Infrastructure attack**, attack to network/telco infrastructure
- **Etc…**

Source:
http://www.cert.org/encyc_article/tocencyc.html

Incidents aren't always techie..



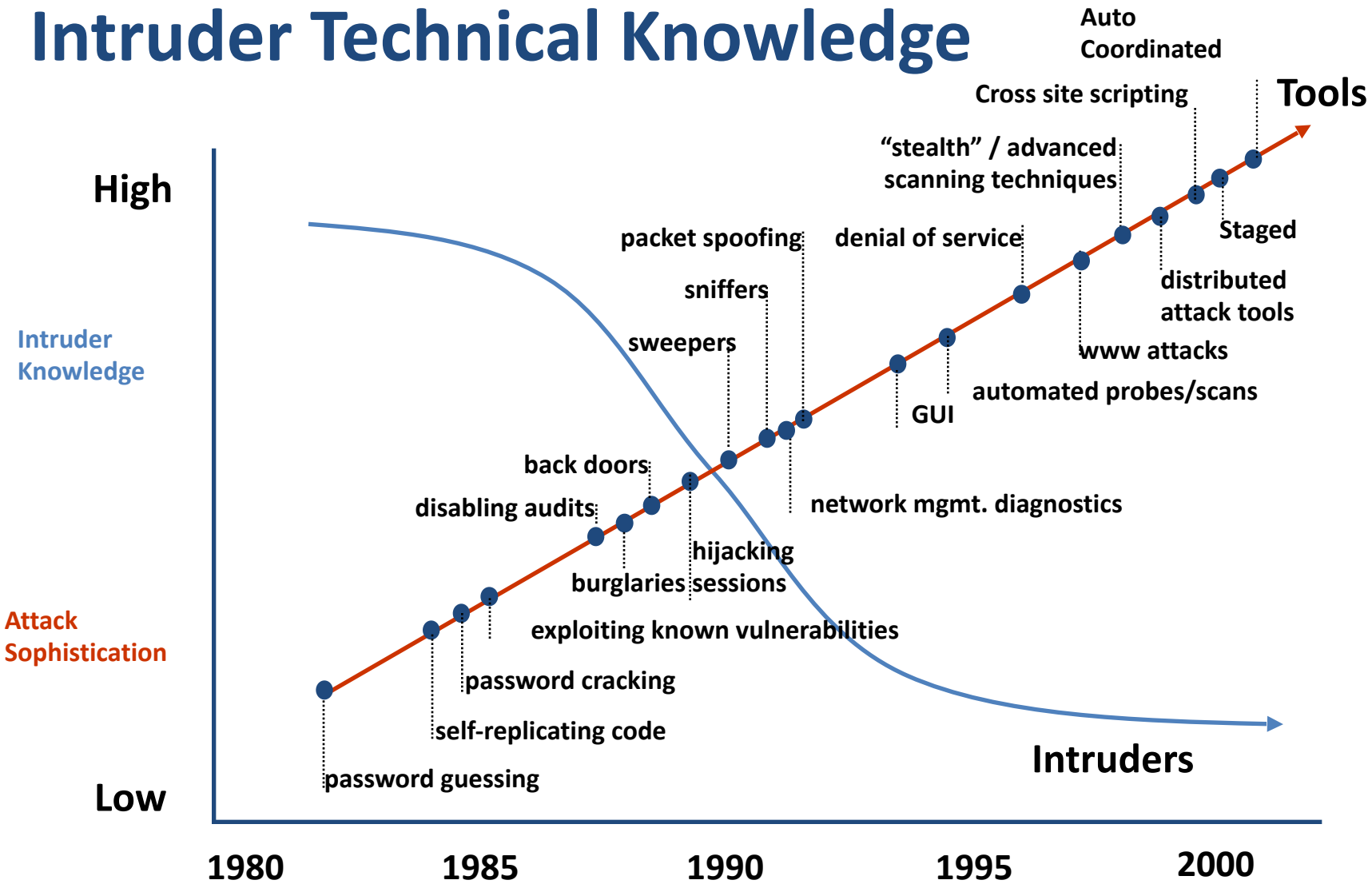
Source:
http://www.jibble.org/cyber-security-challenge-uk-winner/xkcd-decoded.png

So….

With the increasing trend, does this means more attacker becomes more smart…?

NOT REALLY…

Attack Sophistication vs. Intruder Technical Knowledge

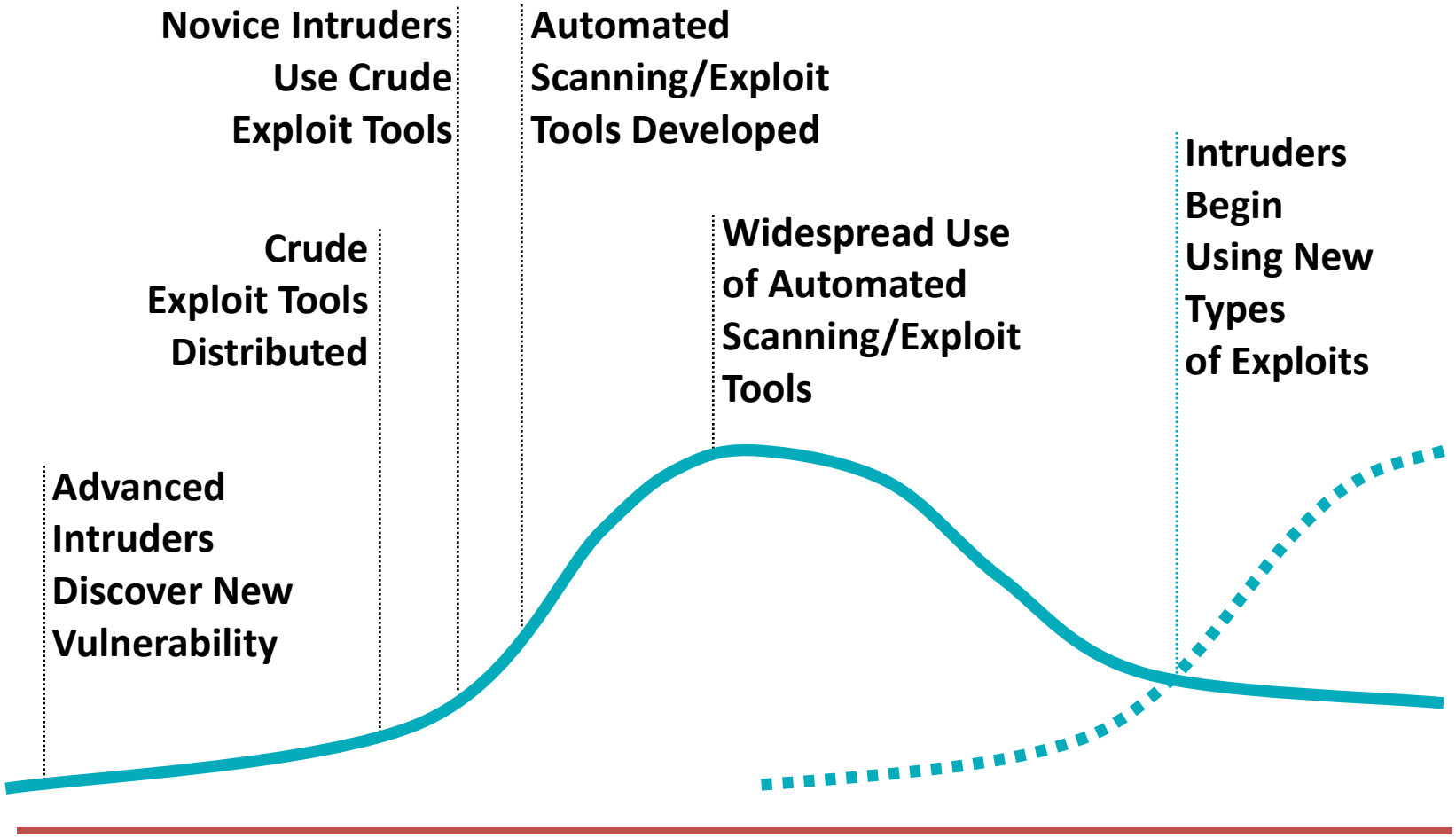


Source:
www.cert.org/archive/ppt/cyberterror.ppt

A story..

Relate story of intruder who used tool to get into UNIX box and gain administrator privileges, then couldn't use it because intruder did not know UNIX commands

Vulnerability Exploit Cycle



Source:
www.cert.org/archive/ppt/cyberterror.ppt

Several terms..

- Threat & attack (RFC2828)
  - Threat: potential violation of security
  - Attack: an assault to a system, can be passive/ active
- Security services: services to provides security
- Security mechanism: a mechanism to detect, prevent , or recover from security attack

So, what is network security?

- Well, you already know about the security things…
- Could you please define it?
- What? Many definitions?

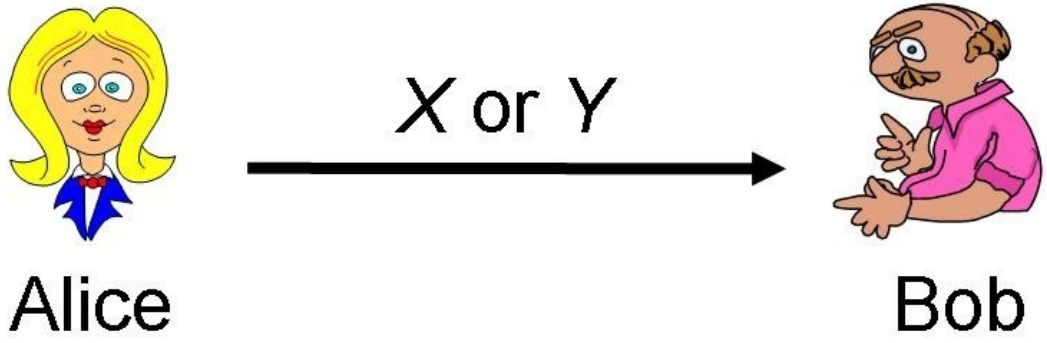
- Aahh, clearly we need a **standard** to define security services

Source: http://www.isicpro.com/site/images/stories/network_security.jpg

Security services, ITU-T X.800

- **Authentication**, the communicating entity is the one that it claims to be
- **Access Control**, prevention from unauthorized resources
- **Confidentiality**, protection from unauthorized disclosure
- **Integrity**, authenticity of the data (no modification)
- **Non-repudiation**, protection against the denial of involved communicating entity

Alice, Bob & security services



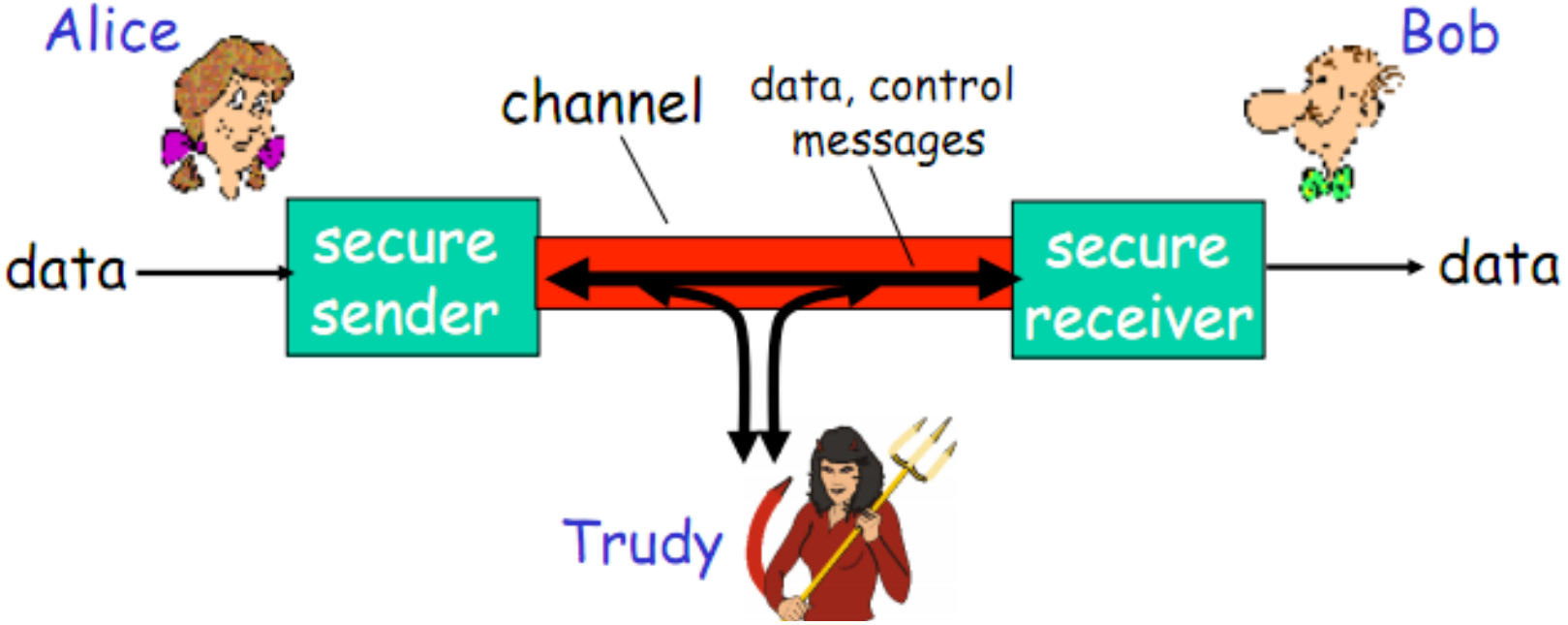
This analogy is often used in security illustration.

Alice & **Bob** could be: real persons, server/client, e-banking, email, browser, DNS, routers, etc.

Authentication, Access Control, Confidentiality, Integrity, Non-repudiation?

Source: kurose & ross, computer networking

What will happen?



Source: kurose and ross, computer networking

Security mechanism…

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Source: william stalling, network security essentials

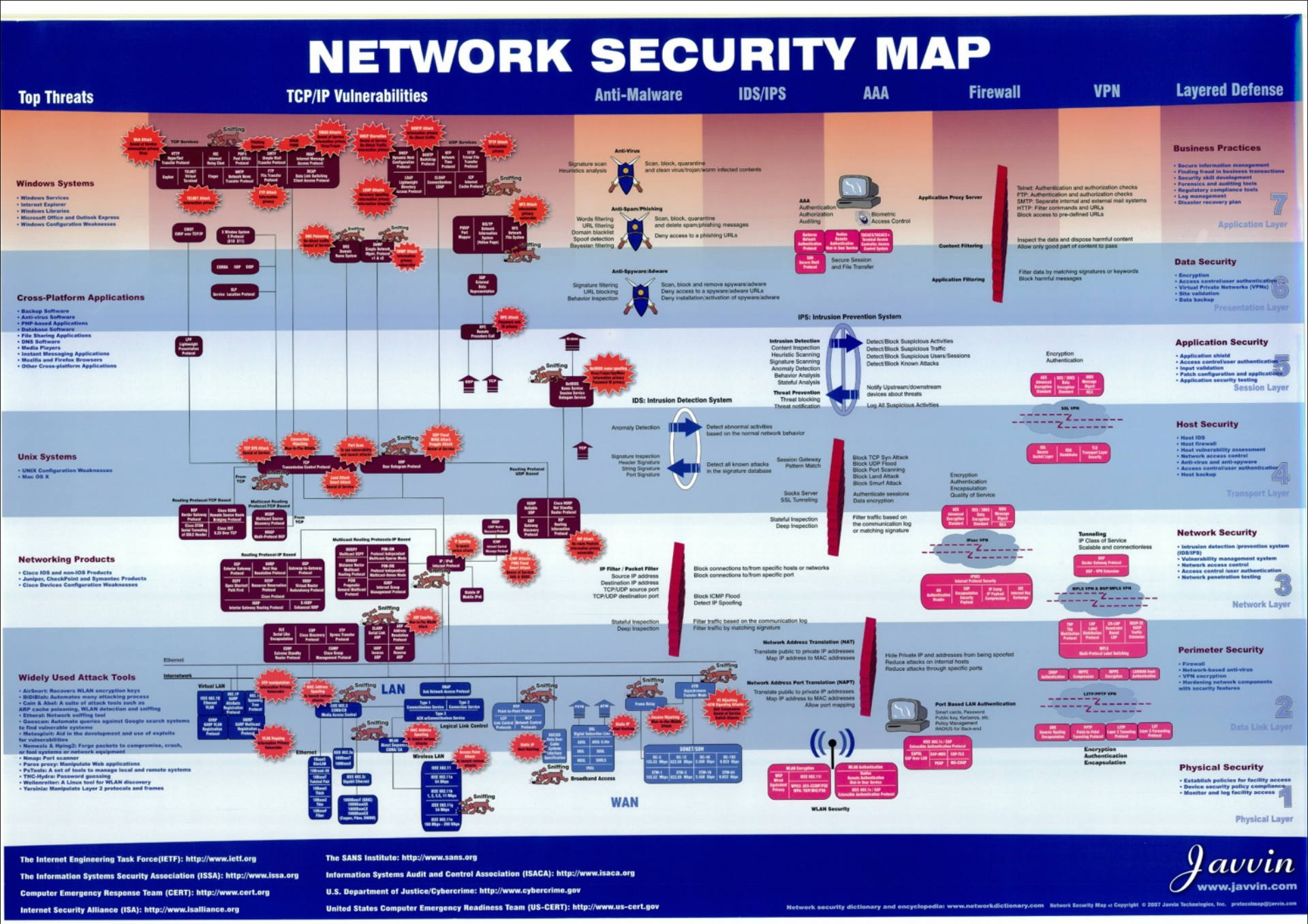
Some implementations…

- Security policy, supported by law
- Security practices, use a good password, update system, secure programming, etc
- Security technology: cryptography(RSA, CBC, etc), hash (SHA, MD5), one-time password, firewalls

Now lets talk about layered network security

- By the use of layered network protocols, security can also be implemented in layered model naturally.
- therefore, if one layer is compromised, we still have another layer as defense -> layered defense :-)
- Unfortunately, some security technologies break the modularity/independence of layered technology development. in other words: the apps need to be modified in other to be secure. eg: http -> https, ftp -> ftps

NETWORK SECURITY MAP



The Internet Engineering Task Force(IETF): http://www.ietf.org
The Information Systems Security Association (ISSA): http://www.issa.org
Computer Emergency Response Team (CERT): http://www.cert.org
Internet Security Alliance (ISA): http://www.isalliance.org
The SANS Institute: http://www.sans.org
Information Systems Audit and Control Association (ISACA): http://www.isaca.org
U.S. Department of Justice/Cybercrime: http://www.cybercrime.gov
United States Computer Emergency Readiness Team (US-CERT): http://www.us-cert.gov

Javvin
www.javvin.com

Network security dictionary and encyclopedia: www.networkdictionary.com

So, what should I learn? (1)

Depends on what **skills** you desire:

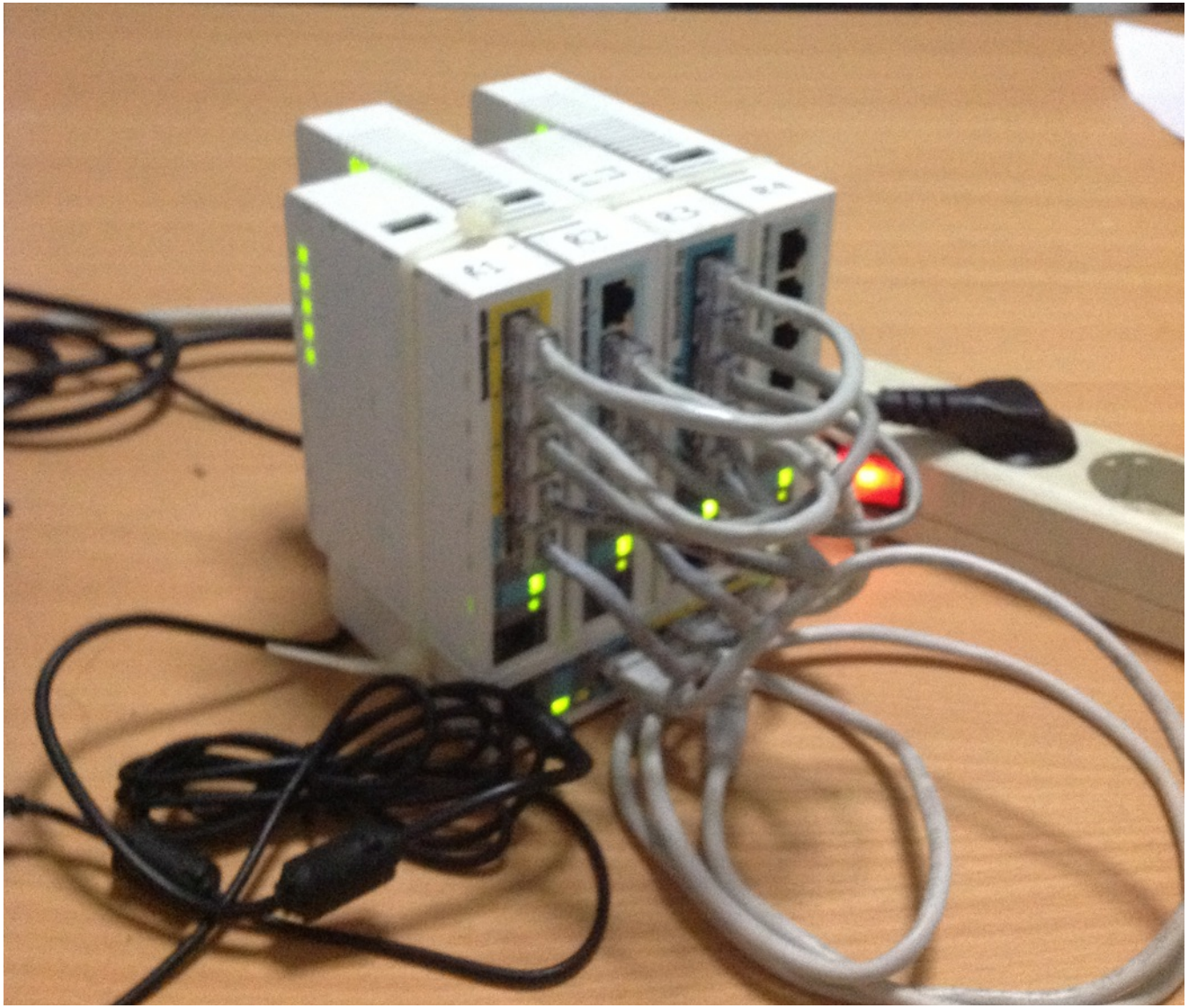
- If you just want to be a **ordinary user**, just get knowledge how to use apps securely.
- If you are **net/sys admin**, be expert on the administration things (system/network). Understand how the security/protocols works, and get knowledge how to implement them in your system.

what should I learn? (2)

- If you are **developer**, understand deeply how the protocols/algorithms works, implement them on your code efficiently.
- If you are **security researcher**, see all above.
- If you are **script kiddies**, you can do better than that.

Please note: security mechanisms requires **lots of math & programming**, if you hate them, security is not your career.

Demo…



Thank You

- Q & A