



# Layered Network Security

Achmad Mardiansyah

[achmad@glcgroup.co.id](mailto: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

## OSI model

### 7. Application layer

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

### 6. Presentation layer

MIME · XDR

### 5. Session layer

Named pipe · NetBIOS · SAP · PPTP · RTP ·  
SOCKS · SPDY · TLS/SSL

### 4. Transport layer

TCP · UDP · SCTP · DCCP · SPX

### 3. Network layer

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

### 2. Data link layer

ATM · SDLC · HDLC · CSLIP · SLIP · GFP ·  
PLIP · IEEE 802.2 · LLC · L2TP · IEEE 802.3 ·  
Frame Relay · ITU-T G.hn DLL · PPP · X.25

### 1. Physical layer

EIA/TIA-232 · EIA/TIA-449 · ITU-T V-Series ·  
I.430 · I.431 · 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 · RS-232 ·  
RS-449





# Network Protocols Map

TCP/IP MODEL

TCP/IP

UNIX/HP/Sun

Novell

Microsoft

SAN

IBM

Apple

VoIP

VPN/Security

ISO

OSI MODEL

## Application Layer

Defines interface to user processes for communication and data transfer in network  
Manages user sessions, logic links and dialogues

Masks the differences of data formats between dissimilar systems and specifies architecture-independent data transfer format  
Encodes and decodes data  
Encrypts and decrypts data  
Compresses and decompresses data

## Application Layer

Masks the differences of data formats between dissimilar systems  
Provides standardized services such as virtual terminal, file and job transfer, and operation

## Transport Layer

Manages end-to-end message delivery in network

Provides reliable and sequential packet delivery through error recovery and flow control mechanisms  
Provides connectionless oriented packet delivery

## Transport Layer

Manages end-to-end message delivery in network

Provides reliable and sequential packet delivery through error recovery and flow control mechanisms  
Provides connectionless oriented packet delivery

## Network Layer

Determines the best way to transfer data among network devices

Routes packets according to unique network addresses  
Provides flow and congestion control to prevent network resource depletion

## Network Layer

Determines the best route to transfer data among network devices

Routes packets according to unique network addresses  
Provides flow and congestion control to prevent network resource depletion

## Network Access Layer

Defines procedures for operating the communication link

Provides framing and sequencing  
Detects and corrects received frame errors

## Data Link Layer

Defines procedures for operating the communication link

Provides framing and sequencing  
Detects and corrects received frame errors

## Physical Layer

Defines physical means of sending data over network devices

Interfaces between network medium and devices  
Defines optical, electrical, and mechanical characteristics

## Physical Layer

Defines physical means of sending data over network devices

Interfaces between network medium and devices  
Defines optical, electrical, and mechanical characteristics

**ANSI**  
American National Standards Institute  
23 West 42nd Street, 4th Fl.  
New York NY 10018-5900  
Tel: 212-542-9900  
www.ansi.org

**ETSI**  
European Telecommunications Standards Institute  
650, Route des Lucioles  
06921 Sophia Antipolis Cedex, France  
Tel: 33 (0)4 92 94 42 00  
www.etsi.org

**FCC**  
Federal Communications Commission  
445 12th Street SW  
Washington DC 20554 USA  
Tel: 888-225-5322  
www.fcc.gov

**IEEE**  
Institute of Electrical and Electronics Engineers, Inc.  
445 Hoes Lane  
Piscataway, NJ 08855-1331 USA  
Tel: 732-981-0060  
www.ieee.org

**ISO**  
International Organization for Standardization  
One rue de Varembe CH-1211  
Case Postale 56  
Geneva 26, Switzerland  
Tel: 41 22 749 0111  
www.iso.ch

**ITU**  
International Telecommunications Union  
ITU - Place des Nations  
CH-1211 Geneva 20, Switzerland  
Tel: 41 22 99 51 11  
www.itu.ch

**ISOC**  
Internet Society  
www.isoc.org  
ICTFP: Internet Engineering Task Force  
www.ietf.org  
1775 Winkle Ave, Suite 102  
Reston VA 20190 USA  
Tel: 703-325-9880

**IEC**  
International Electrotechnical Commission  
3, rue de Varembe  
CH-1211 Geneva 20, Switzerland  
Tel: 41 22 919 02 11  
www.iec.ch

Network Protocols Map Copyright ©2006 Javvin Technologies, Inc.

now, lets talk about security...

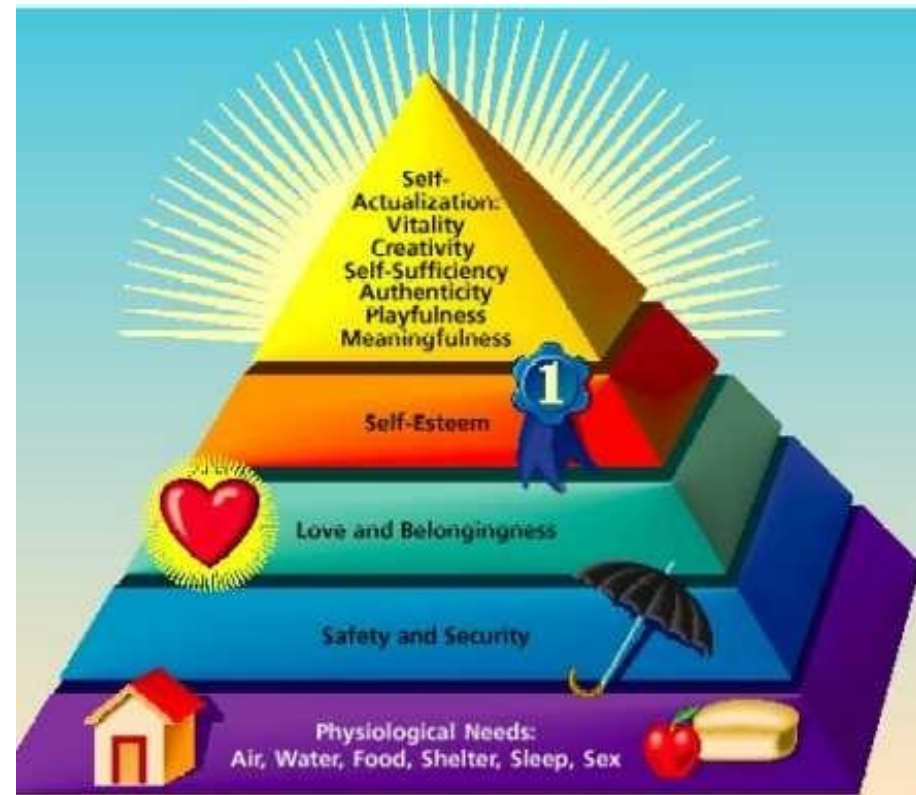


# Why Security?

## 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/INnqY9i4XHGDNS2YgJRolD08FFSTs5MlqobVojrvxgvDWDWiiRe2OvNX8d5DjSQqmcZHx1mDzli8KHzOt7kbMpwm02njyhKZ/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](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**.

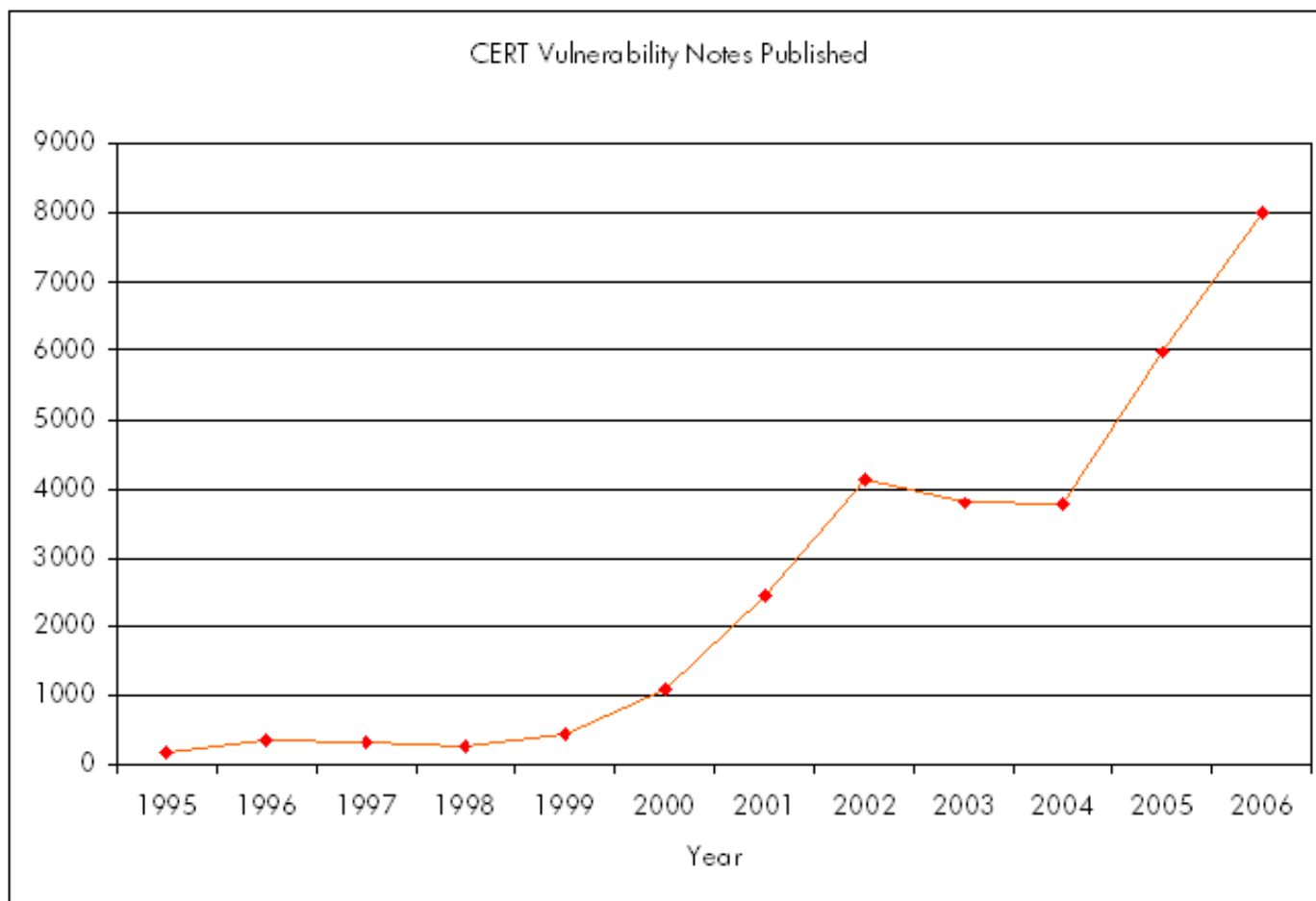


Source:

<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..



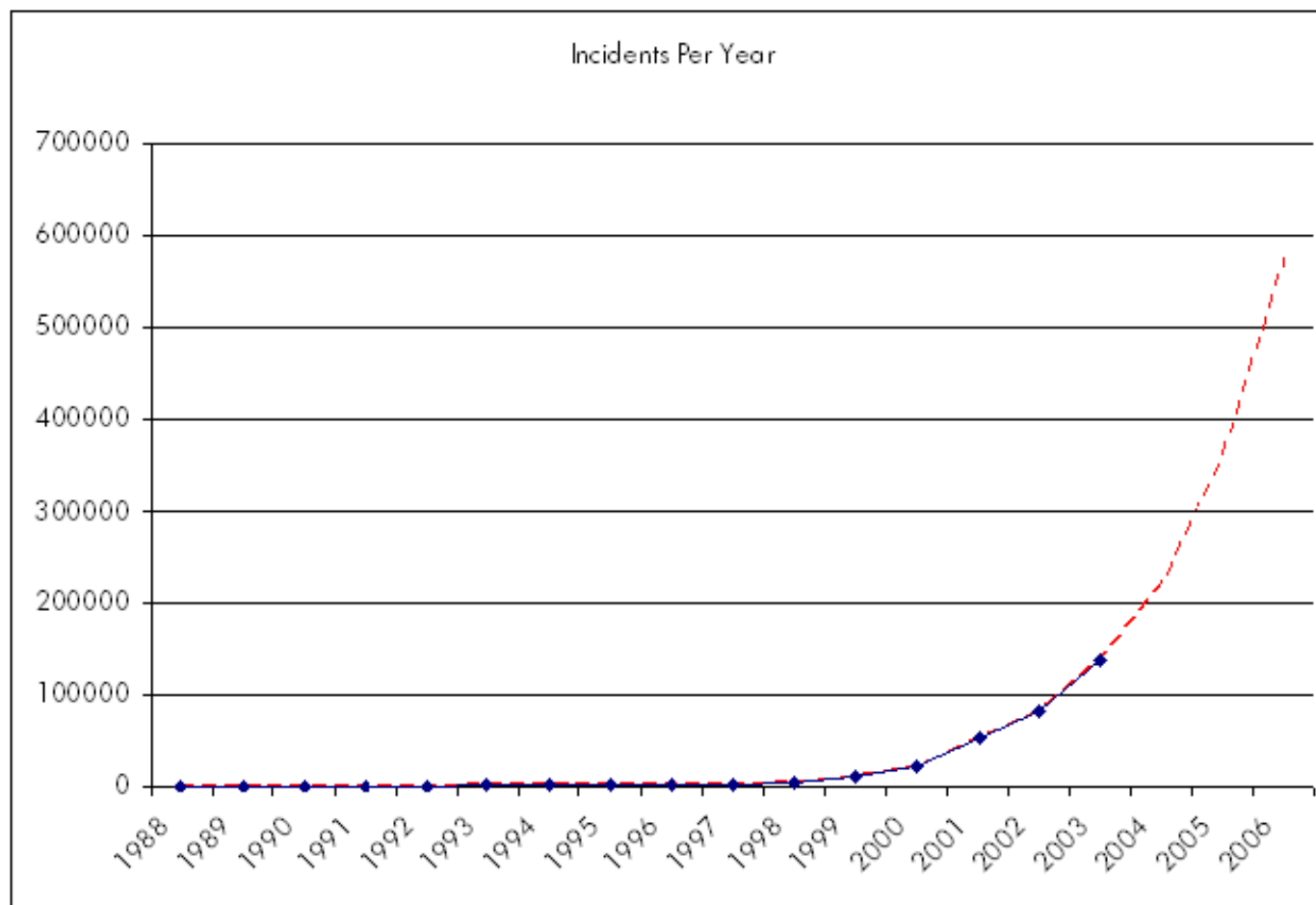
Source:

<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](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>



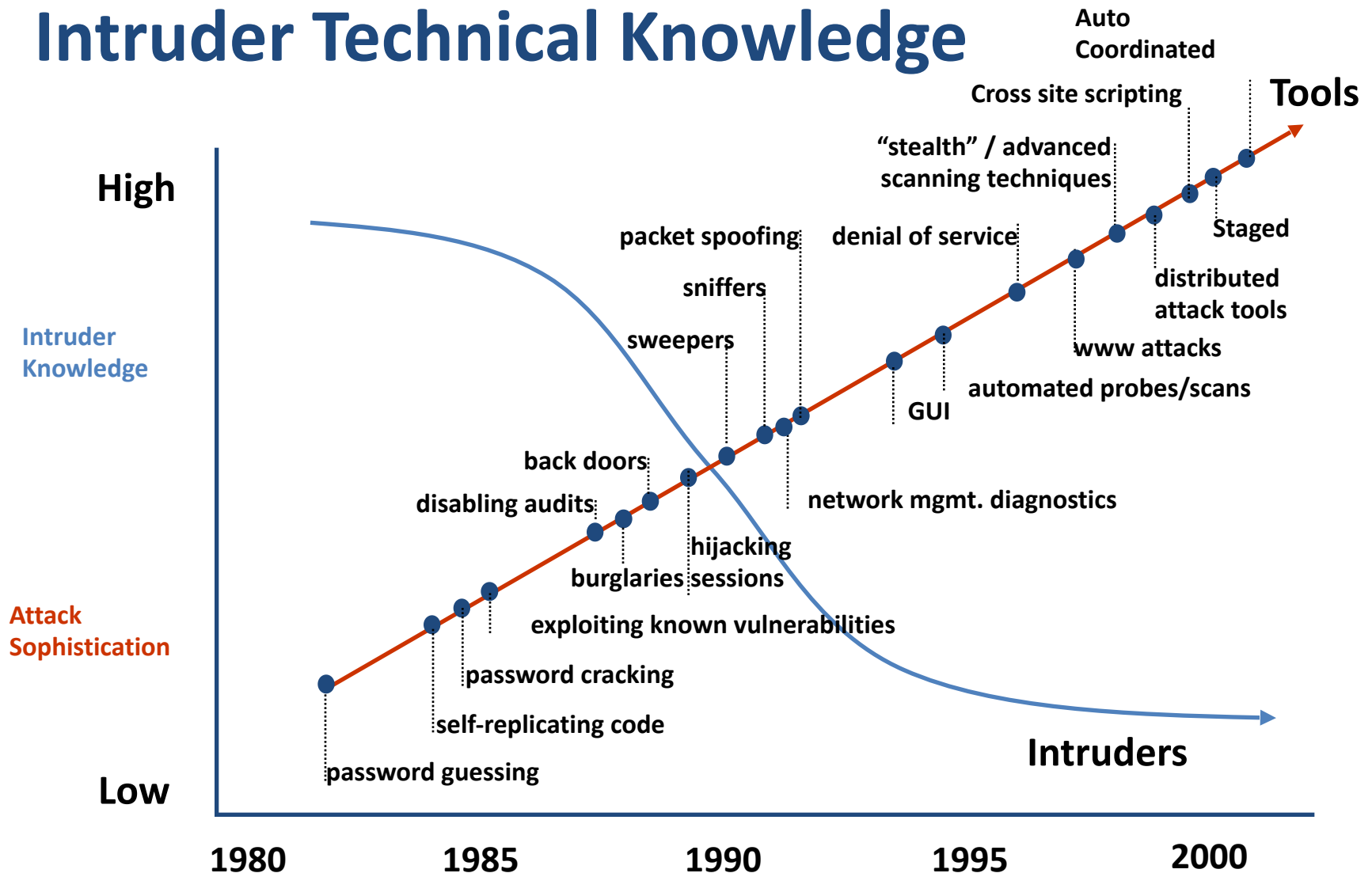
So....

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](http://www.cert.org/archive/ppt/cyberterror.ppt)

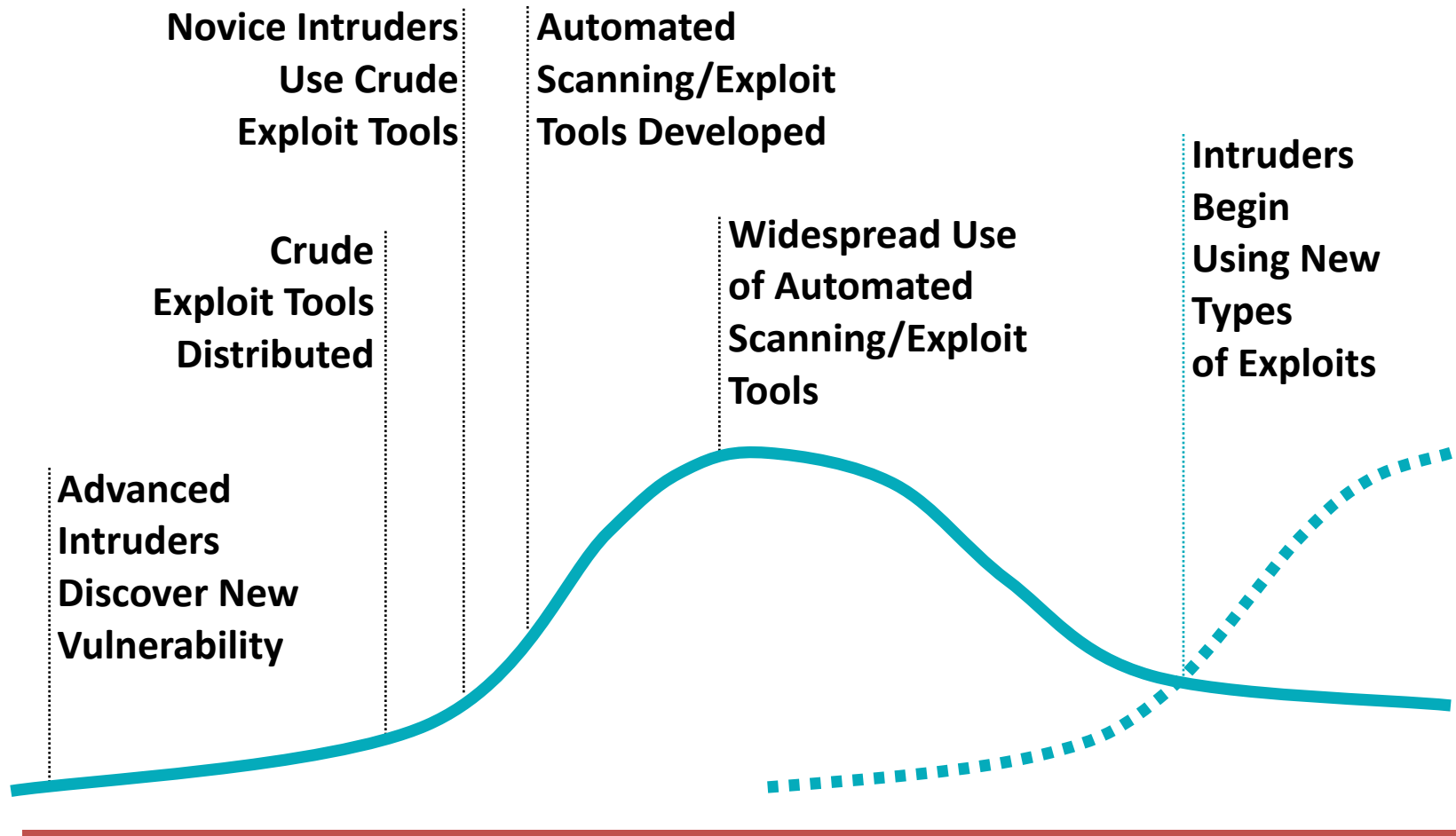


# A story..

**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



# 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](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



Alice

$X$  or  $Y$



Bob

This analogy is often used in security illustration.

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

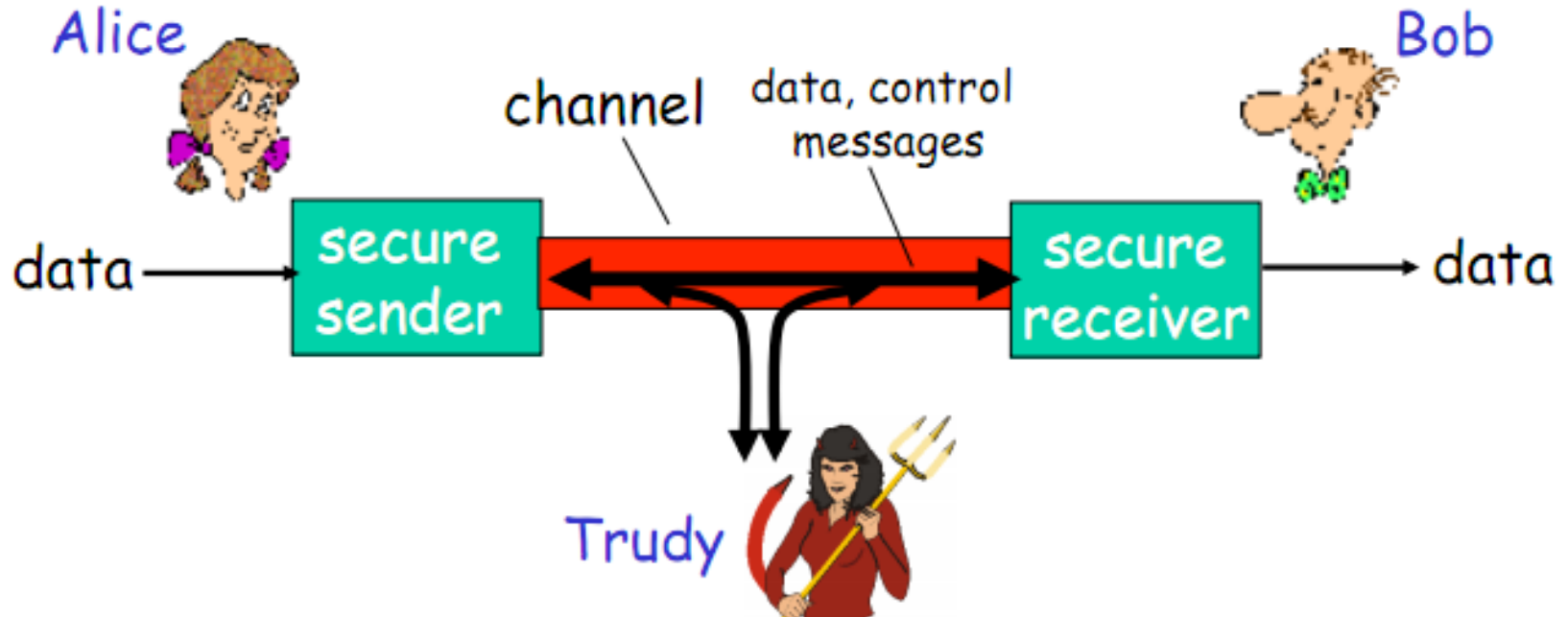
**Authentication, Access Control, Confidentiality,  
Integrity, Non-repudiation?**



Source: kurose & ross, computer networking

[www.glclearningcenter.com](http://www.glclearningcenter.com)

# What will happen?



# 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

## Top Threats

## TCP/IP Vulnerabilities

## Anti-Malware

## IDS/IPS

## AAA

## Firewall

## VPN

## Layered Defense

### Windows Systems

- Windows Services
- Internet Explorer
- Windows Libraries
- Microsoft Office and Outlook Express
- Windows Configuration Weaknesses

### Cross-Platform Applications

- Backup Software
- Anti-virus Software
- PSP-based Applications
- Database Software
- File Sharing Applications
- Music Players
- Instant Messaging Applications
- Media and PDA Software
- Other Cross-platform Applications

### Unix Systems

- UNIX Configuration Weaknesses
- Mac OS X

### Networking Products

- Cisco IOS and non-IOS Products
- Jumper, CheckPoint and Symantec Products
- Cisco Routers Configuration Weaknesses

### Widely Used Attack Tools

- AirSnort: Recorders WLAN encryption keys
- SniffIt: Automates many attacking process
- Cain & Abel: A suite of attack tools such as ARP cache poisoning, WLAN detection and sniffing
- EtherSniff: Network sniffing tool
- GoSecure: Automate queries against Google search systems to find vulnerable systems
- Metasploit: Aid in the development and use of exploits for vulnerabilities
- Netsniff-ng: Forge packets to compromise, crash, or stall systems or network equipment
- Netmap: Port scanner
- Paros proxy: Manipulate Web applications
- PyTutor: A set of tools to manage local and remote systems
- THC-Hydra: Password guessing
- Wifite: A Linux tool for WLAN discovery
- Yersinia: Manipulate Layer 2 protocols and frames

### Business Practices

- Secure information management
- Finding fraud in business transactions
- Security skill development
- Forensics and auditing tools
- Regulatory compliance tools
- Log management
- Disaster recovery plan

### Application Layer

### Data Security

- Encryption
- Access control/user authentication
- Virtual Private Networks (VPNs)
- Site validation
- Data backup

### Presentation Layer

### Application Security

- Application shield
- Access control/user authentication
- Input validation
- Patch configuration and applications
- Application security testing

### Session Layer

### Host Security

- Host IDS
- Host Firewall
- Host vulnerability assessment
- Network access control
- Anti-virus and anti-spyware
- Access control/user authentication
- Host backup

### Transport Layer

### Network Security

- Intrusion detection (prevention) system (IDS/IPS)
- Vulnerability management system
- Network access control
- Access control layer authentication
- Network penetration testing

### Network Layer

### Perimeter Security

- Firewall
- Network-based anti-virus
- VPN encryption
- Hardening network components with security features

### Data Link Layer

### Physical Security

- Establish policies for facility access
- Device security policy compliance
- Monitor and log facility access

### Physical Layer

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.isaalliance.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>

Network security dictionary and encyclopedia: [www.networkdictionary.com](http://www.networkdictionary.com) Network Security Map © Copyright © 2007 Javvin Technologies, Inc. [pradheep@javvin.com](mailto:pradheep@javvin.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)

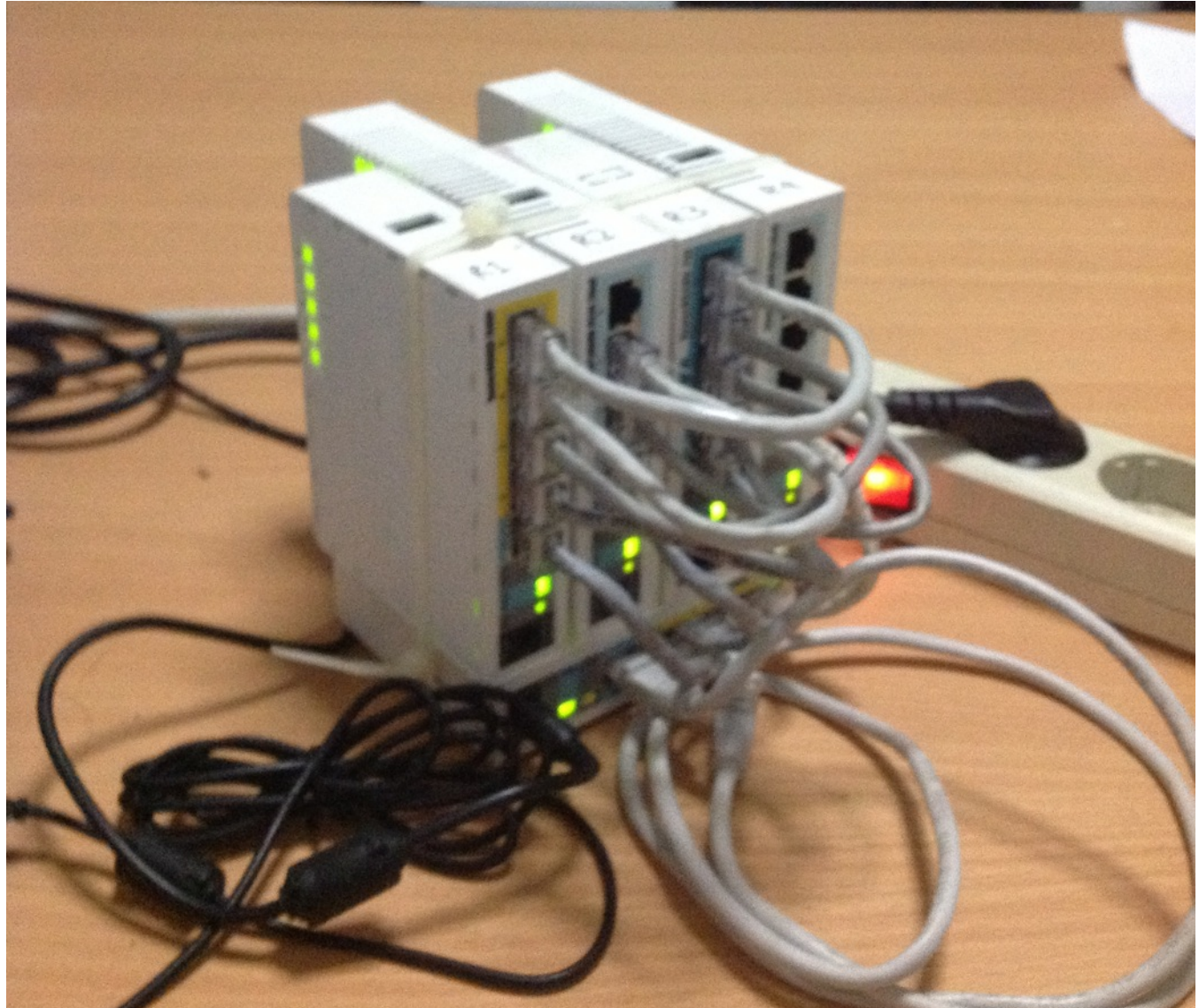
- If you are **developer**, understand deeply how the protocols/algorithms works, implement them on your code efficiently.
- If you are **security researcher**, see all above.
- If you are **script kiddies**, you can do better than that.

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





# Demo...



# Thank You

- Q & A

