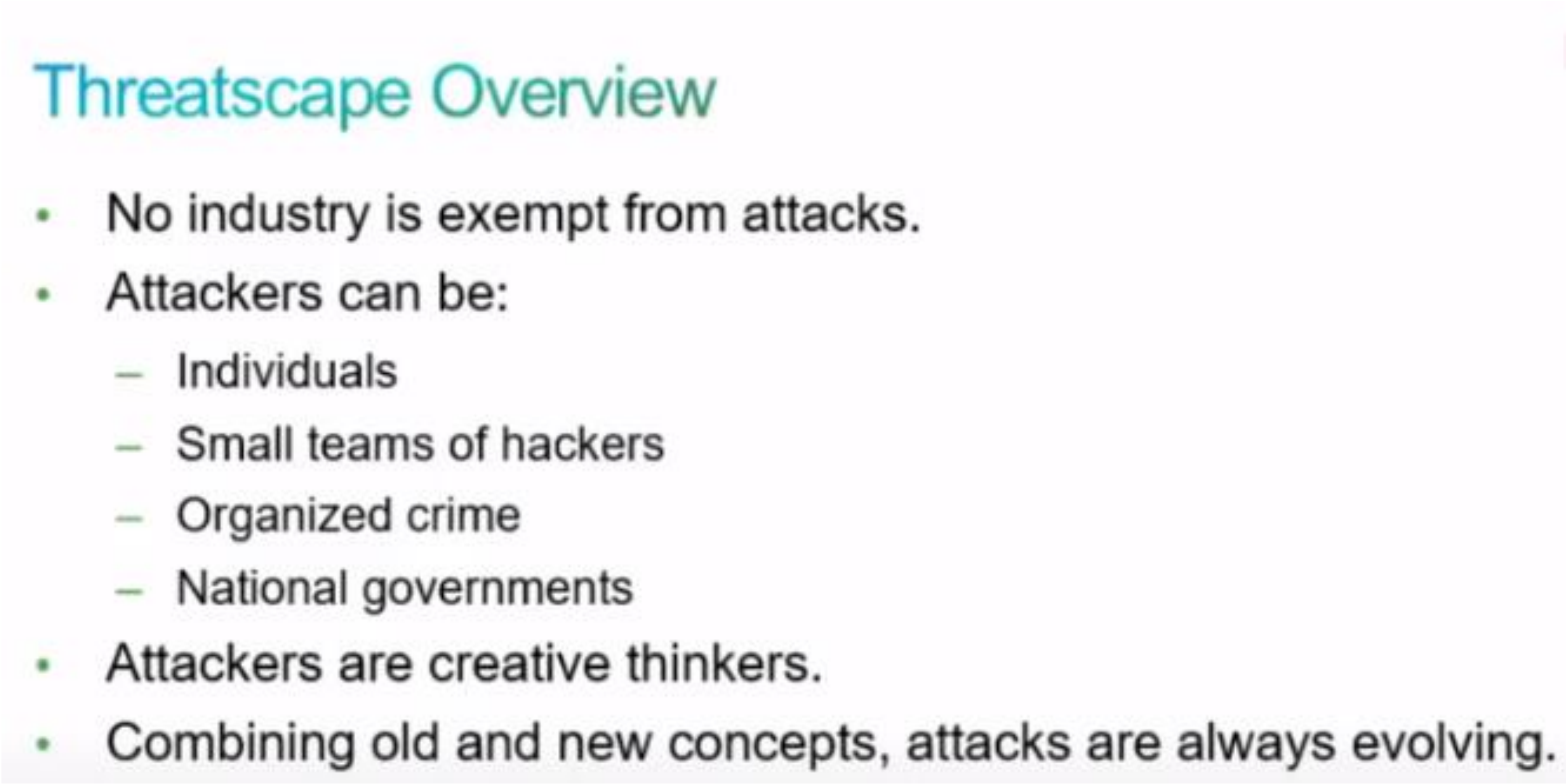
NETWORK SECURITY

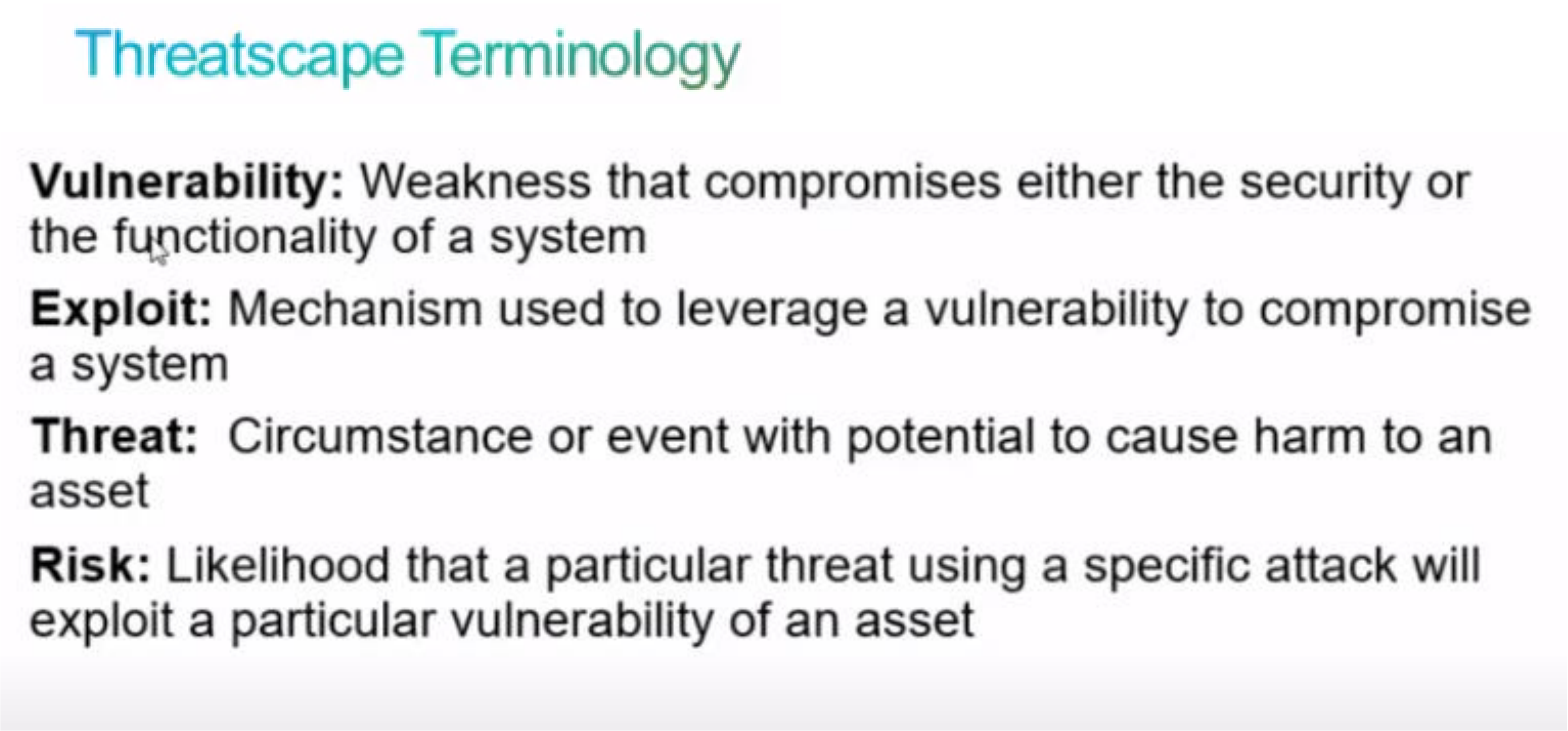
THREAT SCAPE

SECURITY CONCEPTS



Threatscape Overview

- No industry is exempt from attacks.
- Attackers can be:
  - Individuals
  - Small teams of hackers
  - Organized crime
  - National governments
- Attackers are creative thinkers.
- Combining old and new concepts, attacks are always evolving.



Threatscape Terminology

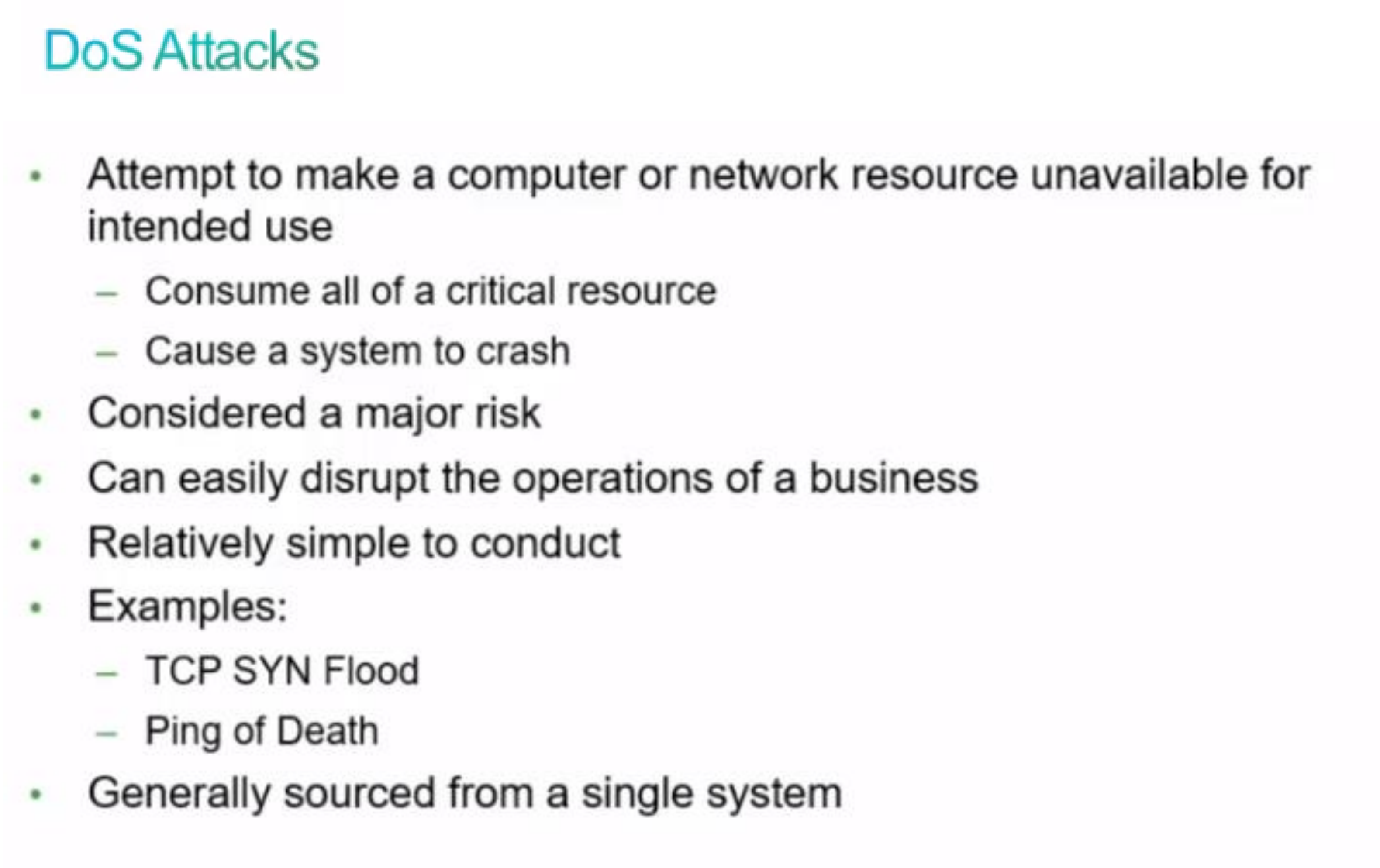
Vulnerability: Weakness that compromises either the security or the functionality of a system

Exploit: Mechanism used to leverage a vulnerability to compromise a system

Threat: Circumstance or event with potential to cause harm to an asset

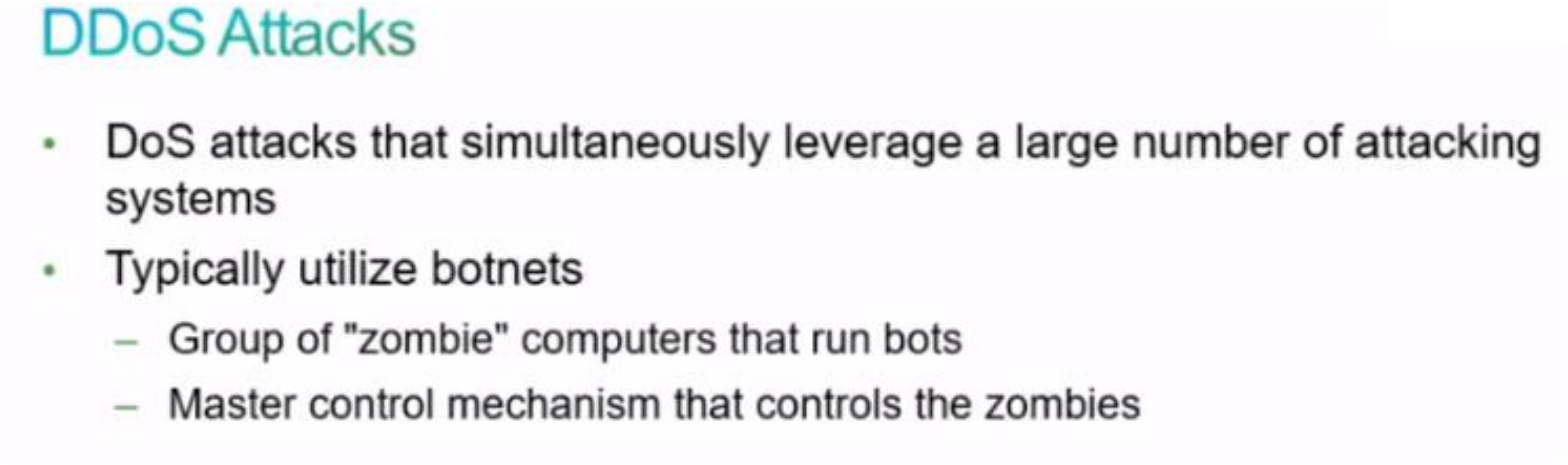
Risk: Likelihood that a particular threat using a specific attack will exploit a particular vulnerability of an asset

TYPES OF ATTACKS



DoS Attacks

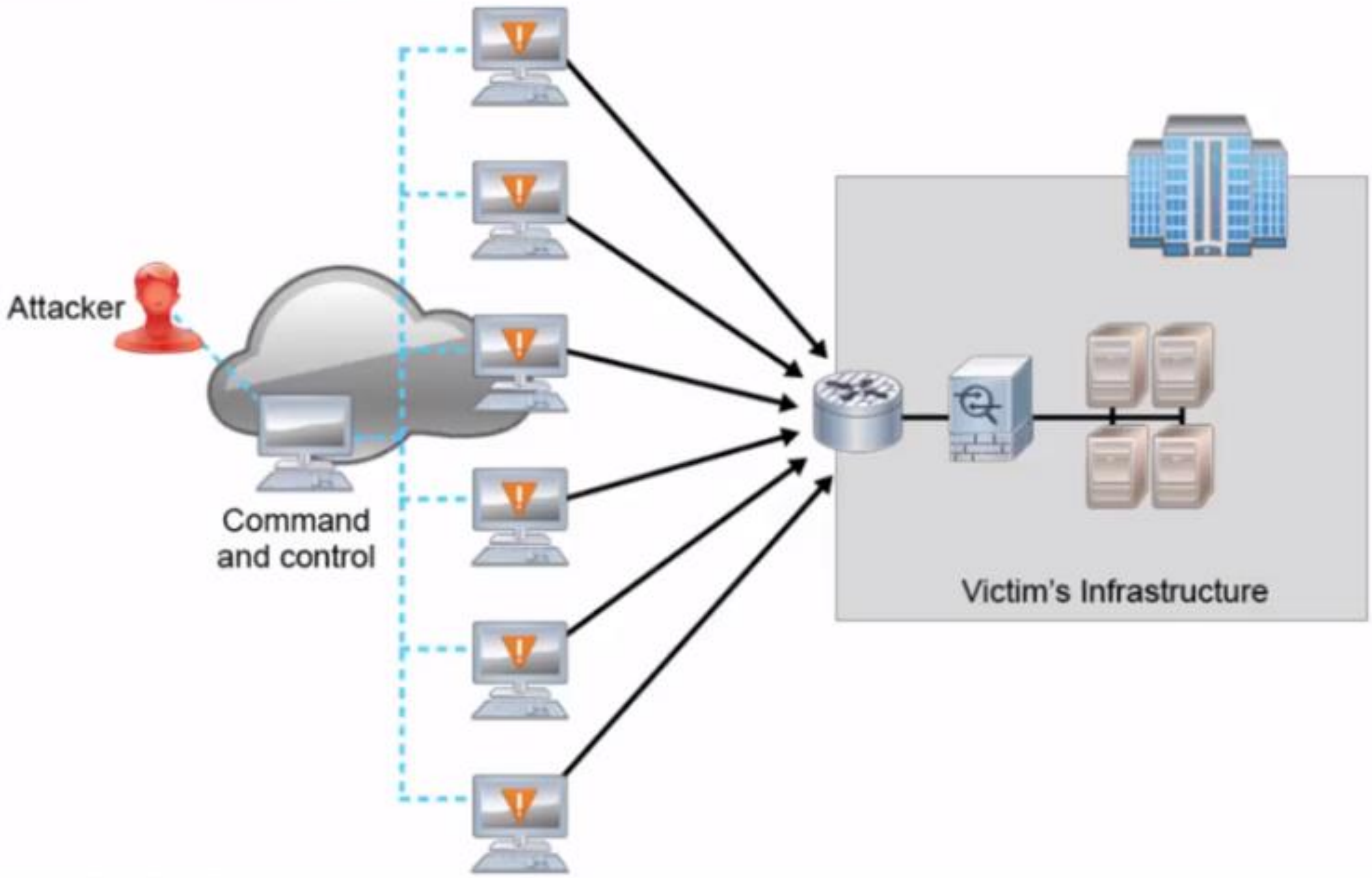
- Attempt to make a computer or network resource unavailable for intended use
  - Consume all of a critical resource
  - Cause a system to crash
- Considered a major risk
- Can easily disrupt the operations of a business
- Relatively simple to conduct
- Examples:
  - TCP SYN Flood
  - Ping of Death
- Generally sourced from a single system

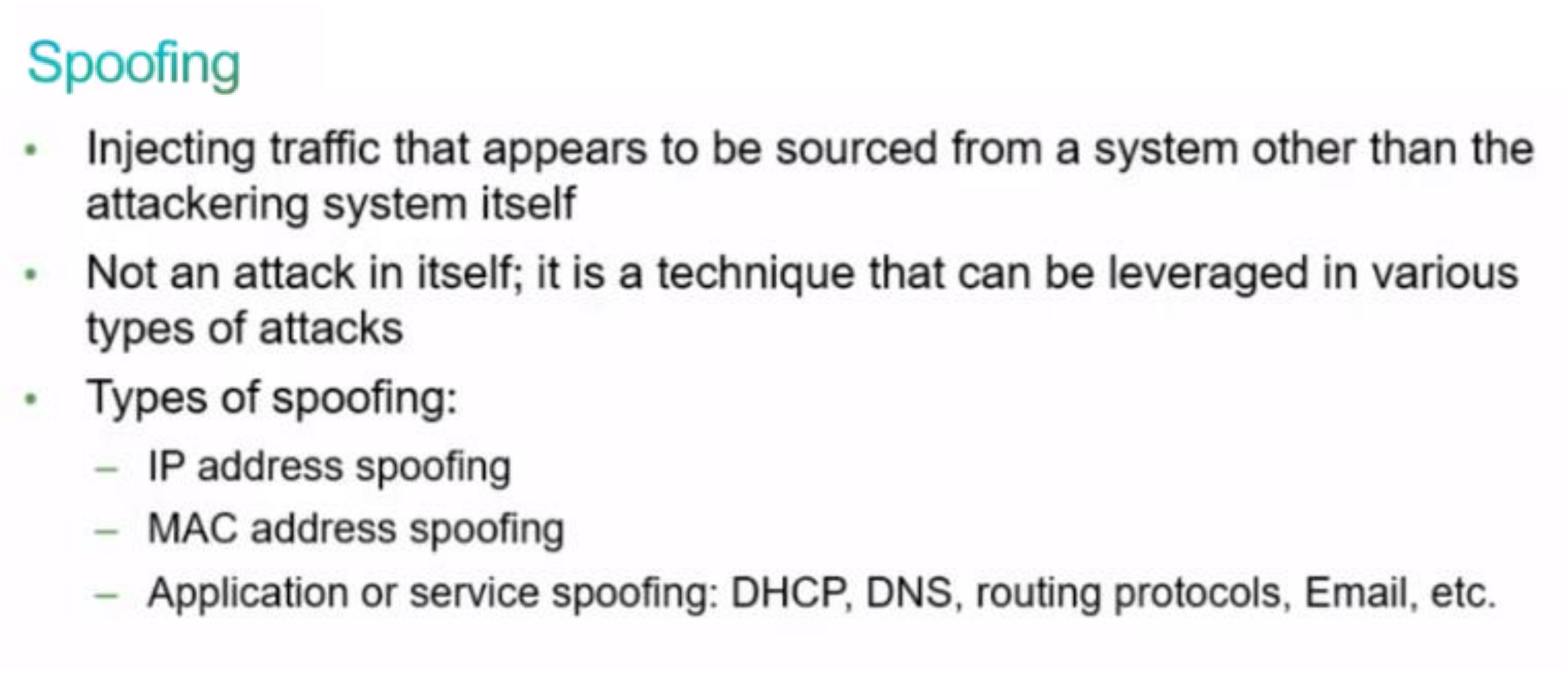


DDoS Attacks

- DoS attacks that simultaneously leverage a large number of attacking systems
- Typically utilize botnets
  - Group of "zombie" computers that run bots
  - Master control mechanism that controls the zombies

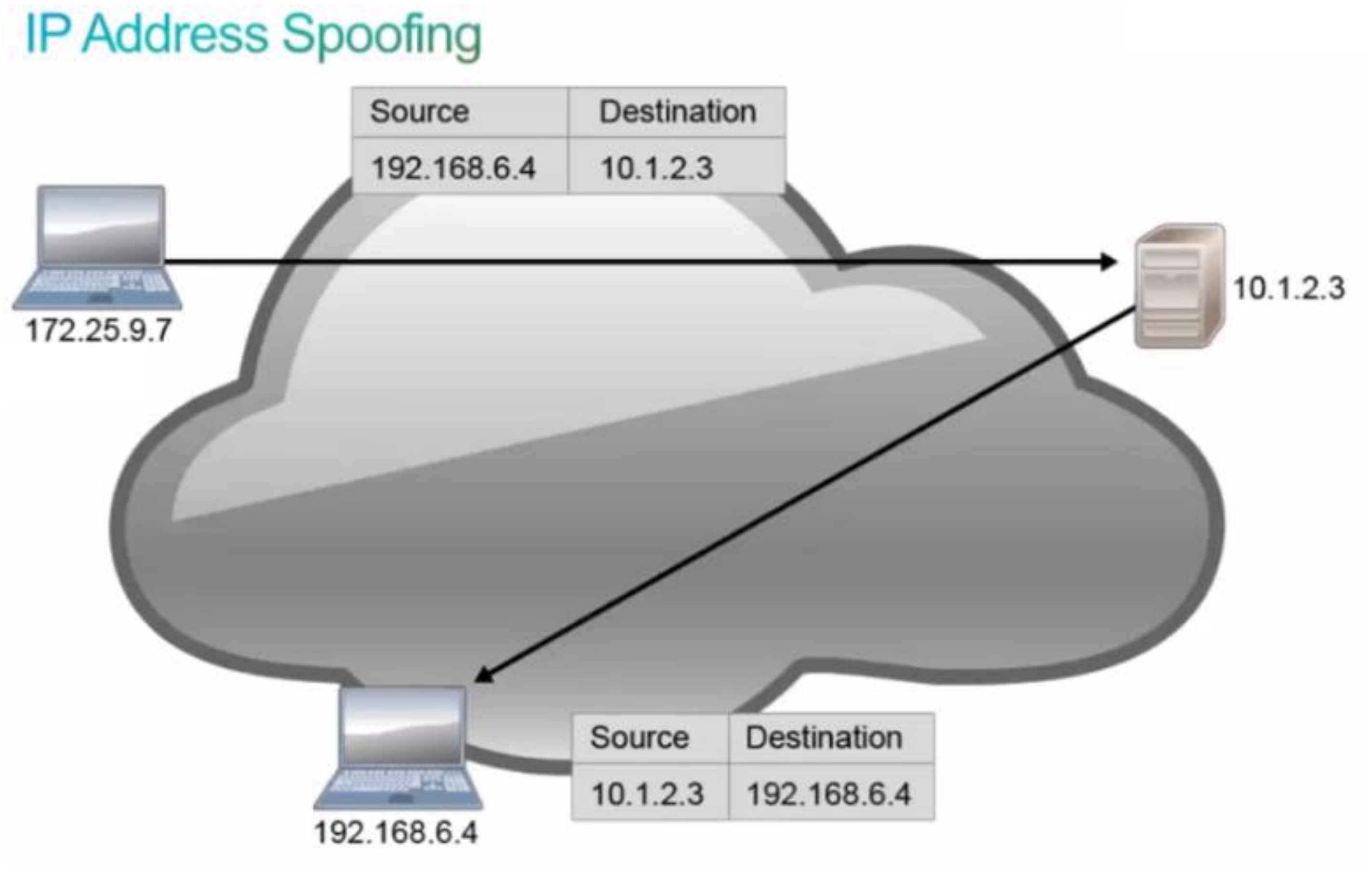
Botnet DDoS Attacks





Spoofing

- Injecting traffic that appears to be sourced from a system other than the attackering system itself
- Not an attack in itself; it is a technique that can be leveraged in various types of attacks
- Types of spoofing:
  - IP address spoofing
  - MAC address spoofing
  - Application or service spoofing: DHCP, DNS, routing protocols, Email, etc.



IP Address Spoofing

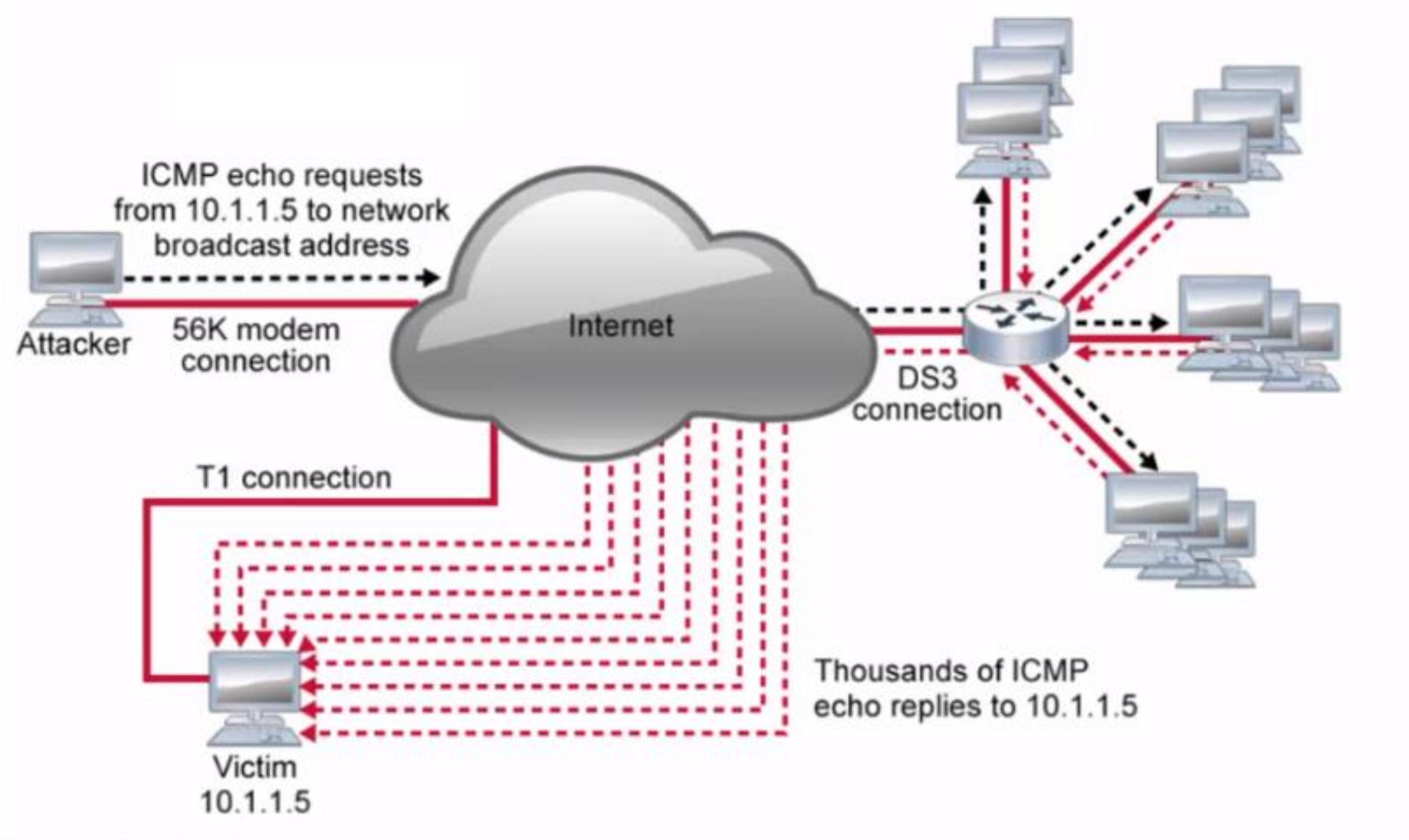
Source	Destination
192.168.6.4	10.1.2.3

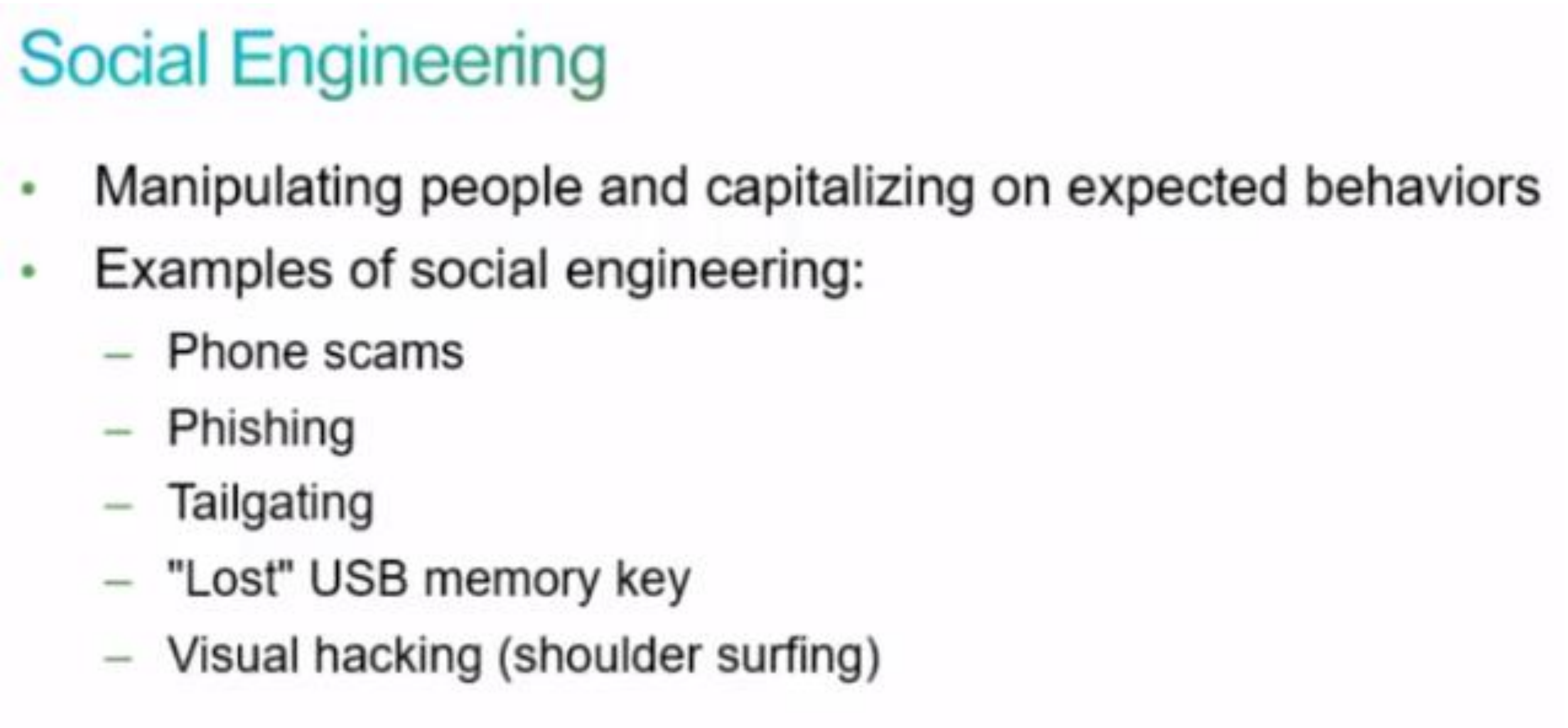
Source	Destination
10.1.2.3	192.168.6.4

Reflection and Amplification Attacks

- In a reflection attack, the attacker sends request packets with spoofed IP addresses to get other hosts to flood a victim.
- A reflection attack can also be an amplification attack if the request packets solicit a larger response.
- In an amplification attack, the attacker sends small forged request packets to elicit a large reply.
- Reflection and amplification attacks are hard to trace because the actual source of the attack is hidden.

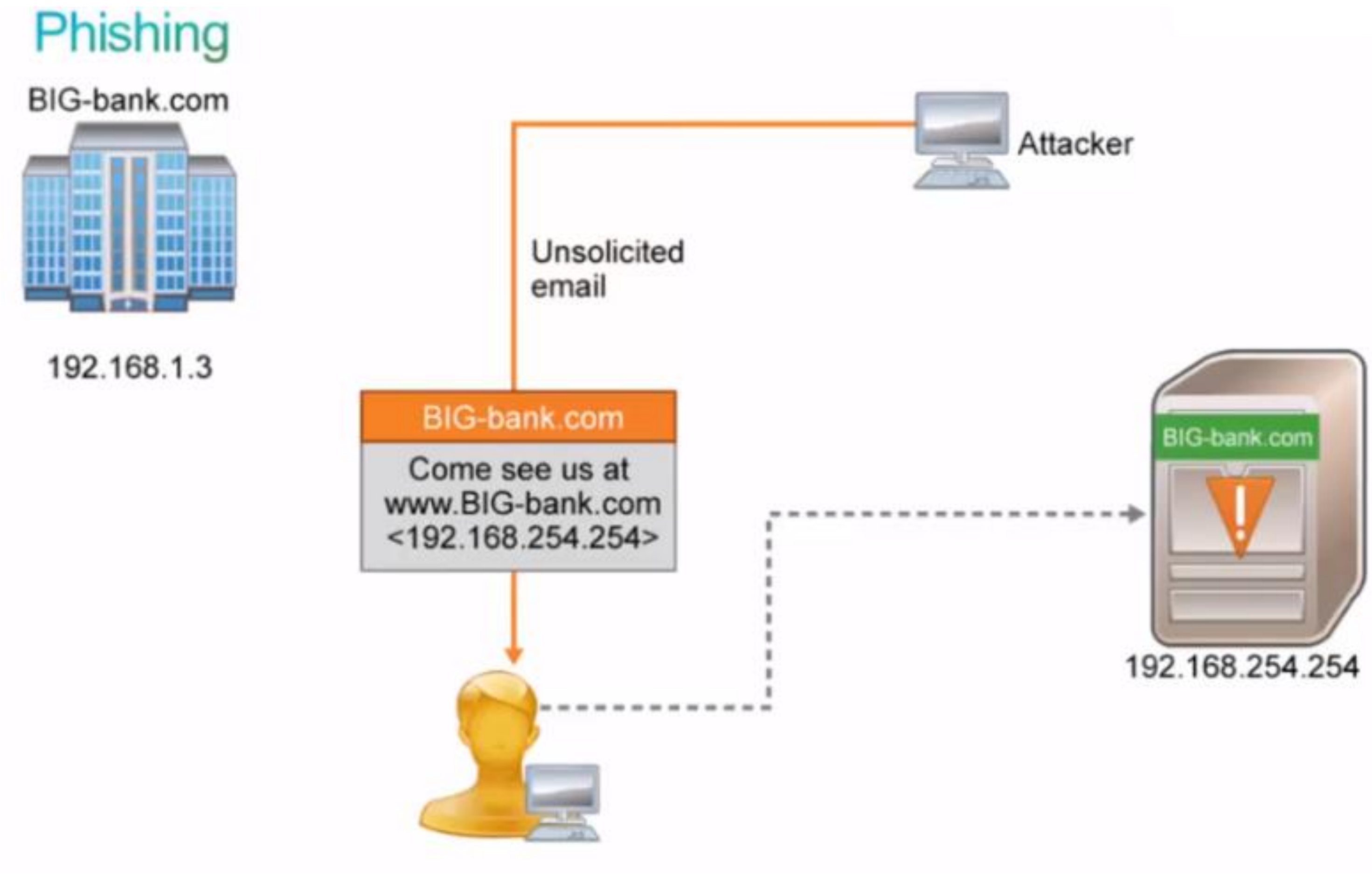
Smurf Attack


ICMP echo requests from 10.1.1.5 to network broadcast address
Attacker
56K modem connection
Internet
DS3 connection
T1 connection
Victim 10.1.1.5
Thousands of ICMP echo replies to 10.1.1.5



Social Engineering

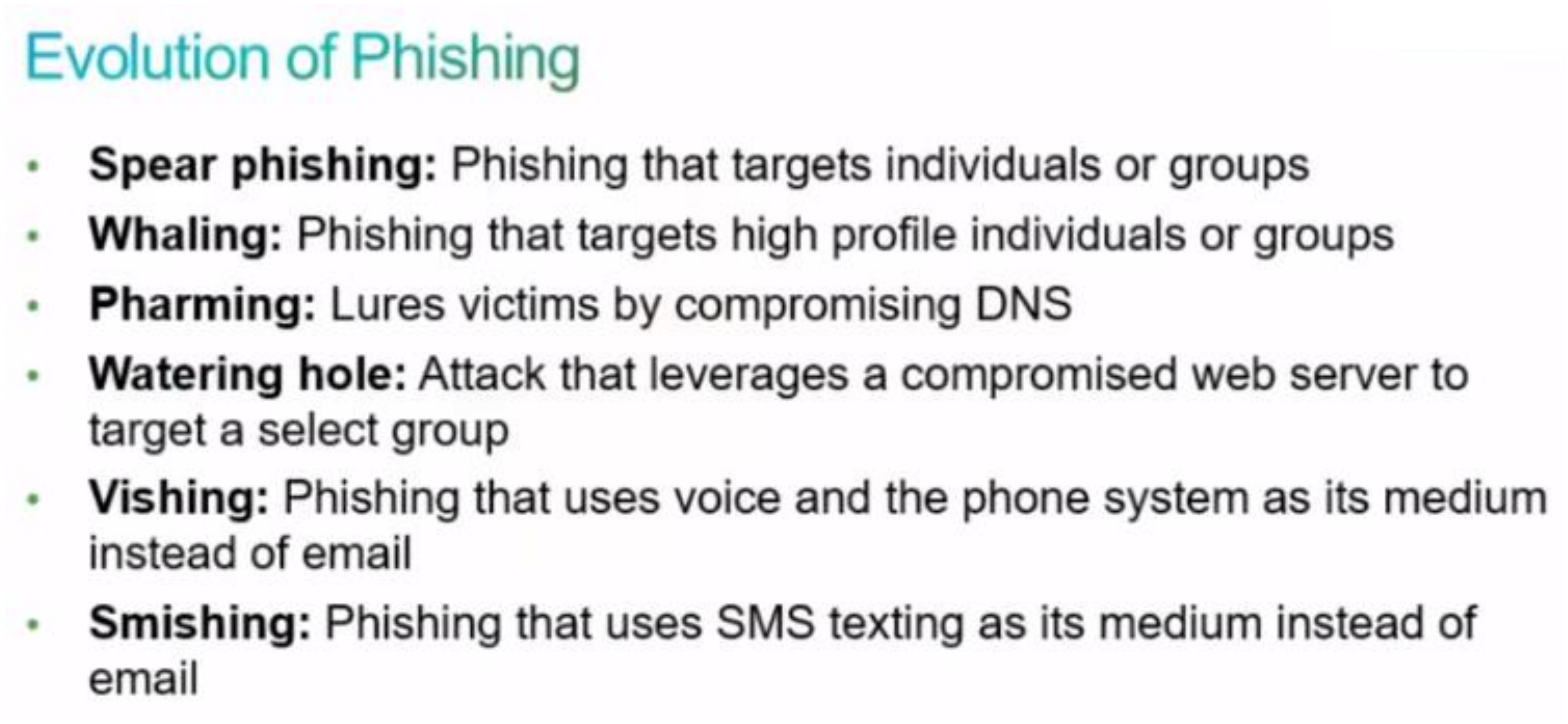
- Manipulating people and capitalizing on expected behaviors
- Examples of social engineering:
  - Phone scams
  - Phishing
  - Tailgating
  - "Lost" USB memory key
  - Visual hacking (shoulder surfing)



Phishing

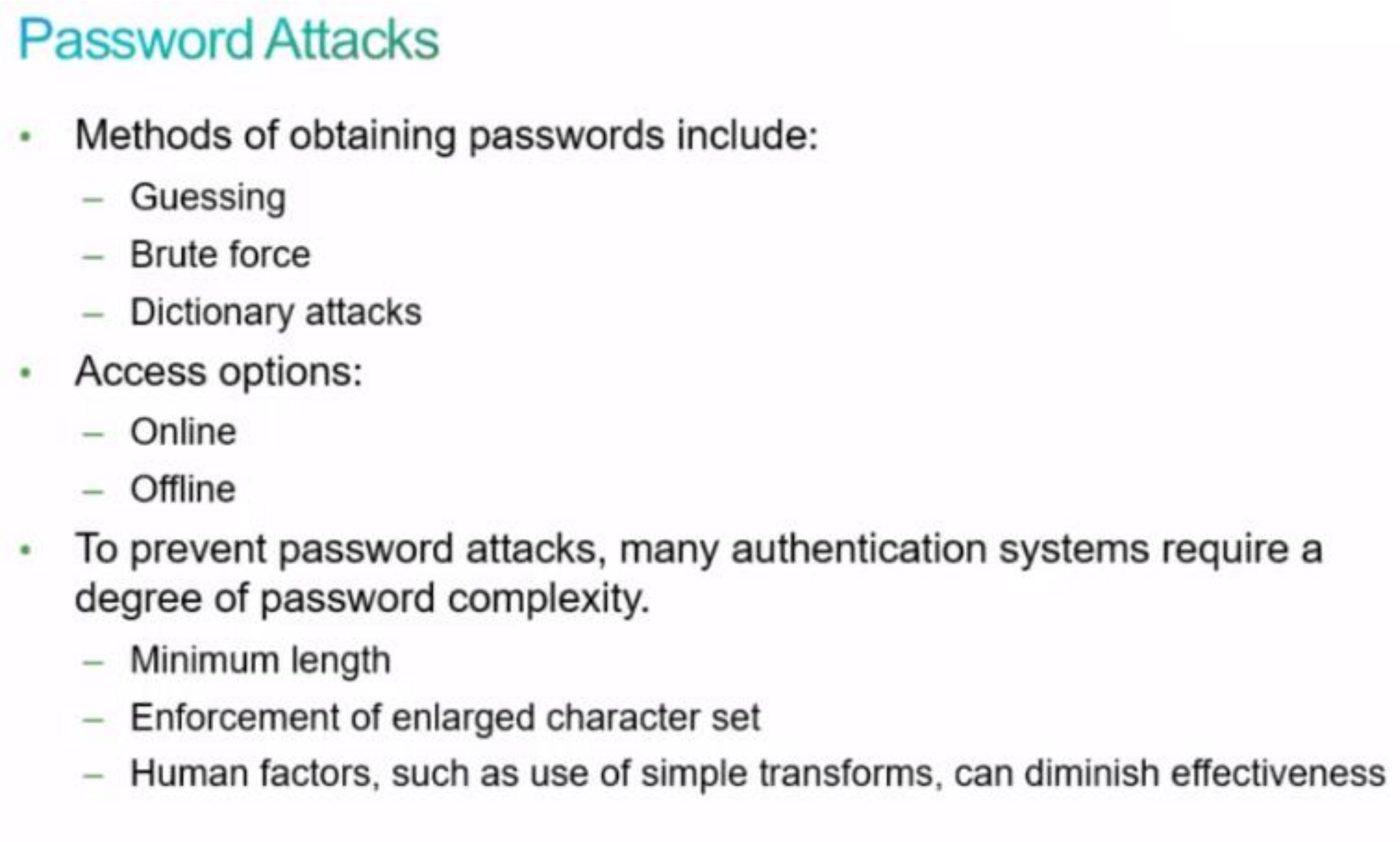
BIG-bank.com

Come see us at www.BIG-bank.com <192.168.254.254>



Evolution of Phishing

- **Spear phishing:** Phishing that targets individuals or groups
- **Whaling:** Phishing that targets high profile individuals or groups
- **Pharming:** Lures victims by compromising DNS
- **Watering hole:** Attack that leverages a compromised web server to target a select group
- **Vishing:** Phishing that uses voice and the phone system as its medium instead of email
- **Smishing:** Phishing that uses SMS texting as its medium instead of email

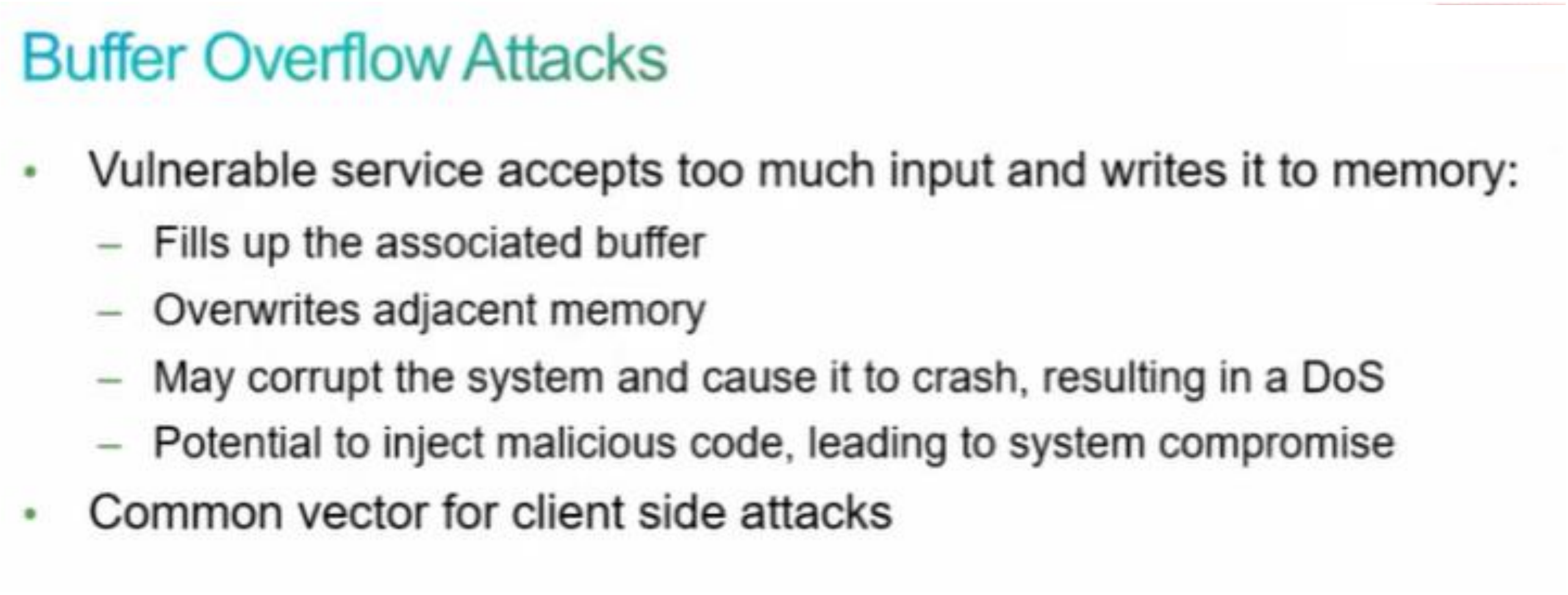


Password Attacks

- Methods of obtaining passwords include:
  - Guessing
  - Brute force
  - Dictionary attacks
- Access options:
  - Online
  - Offline
- To prevent password attacks, many authentication systems require a degree of password complexity.
  - Minimum length
  - Enforcement of enlarged character set
  - Human factors, such as use of simple transforms, can diminish effectiveness

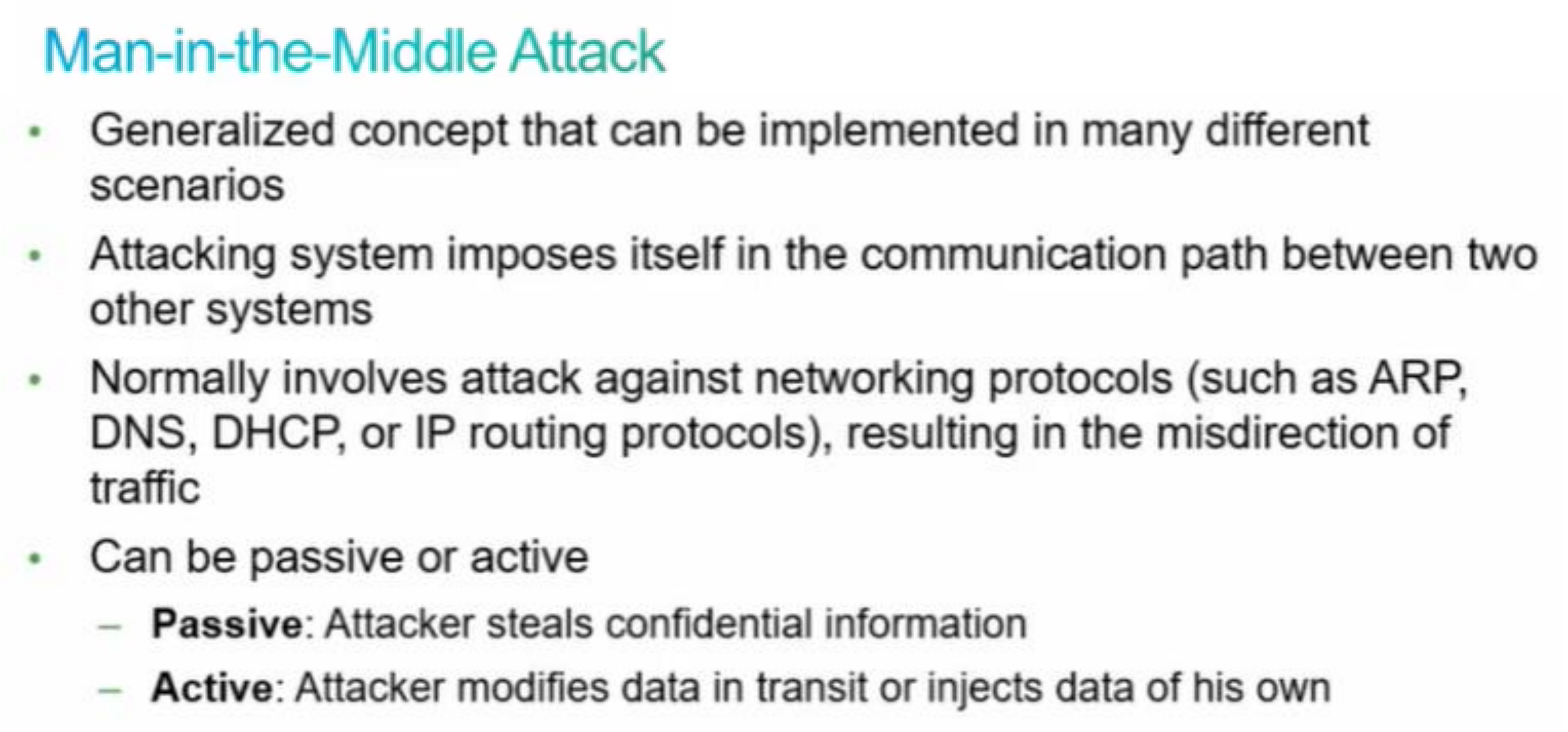
Reconnaissance Attacks

- A reconnaissance attack is an attempt to learn more about the intended victim before attempting a more intrusive attack.
- Options include:
  - Use standard networking tools such as dig, nslookup, and whois to obtain information such who owns a particular domain and what addresses have been assigned to that domain
  - Perform ping sweeps of the addresses obtained to determine which ones are live hosts.
  - Run port scans on the live hosts to determine what services are running on the hosts.
  - Use the information obtained to determine the easiest way to exploit a vulnerability.
- Vulnerability scanners can be used to locate vulnerabilities in your own network and patch them before they can be exploited.



Buffer Overflow Attacks

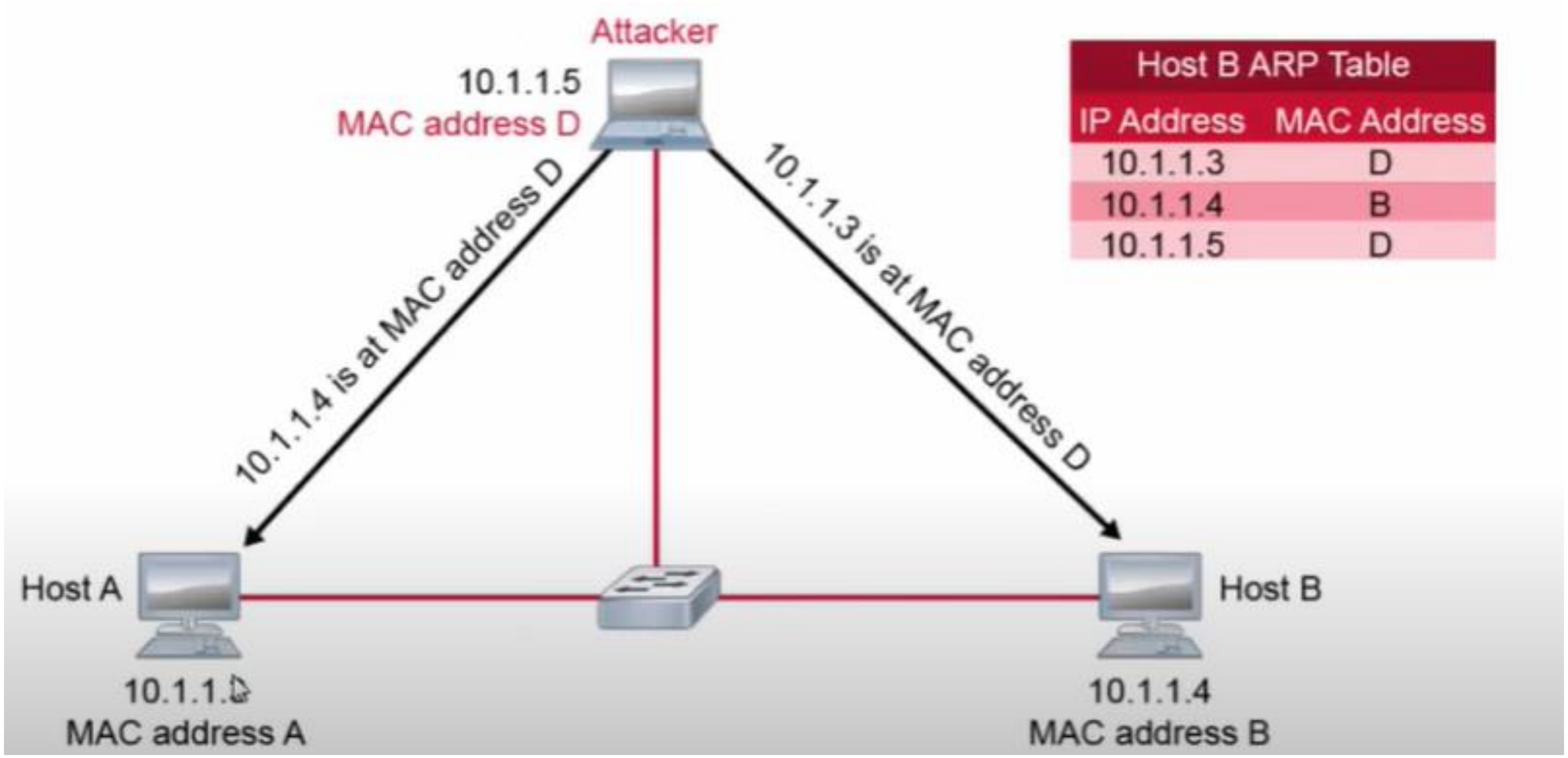
- Vulnerable service accepts too much input and writes it to memory:
  - Fills up the associated buffer
  - Overwrites adjacent memory
  - May corrupt the system and cause it to crash, resulting in a DoS
  - Potential to inject malicious code, leading to system compromise
- Common vector for client side attacks



Man-in-the-Middle Attack

- Generalized concept that can be implemented in many different scenarios
- Attacking system imposes itself in the communication path between two other systems
- Normally involves attack against networking protocols (such as ARP, DNS, DHCP, or IP routing protocols), resulting in the misdirection of traffic
- Can be passive or active
  - **Passive**: Attacker steals confidential information
  - **Active**: Attacker modifies data in transit or injects data of his own

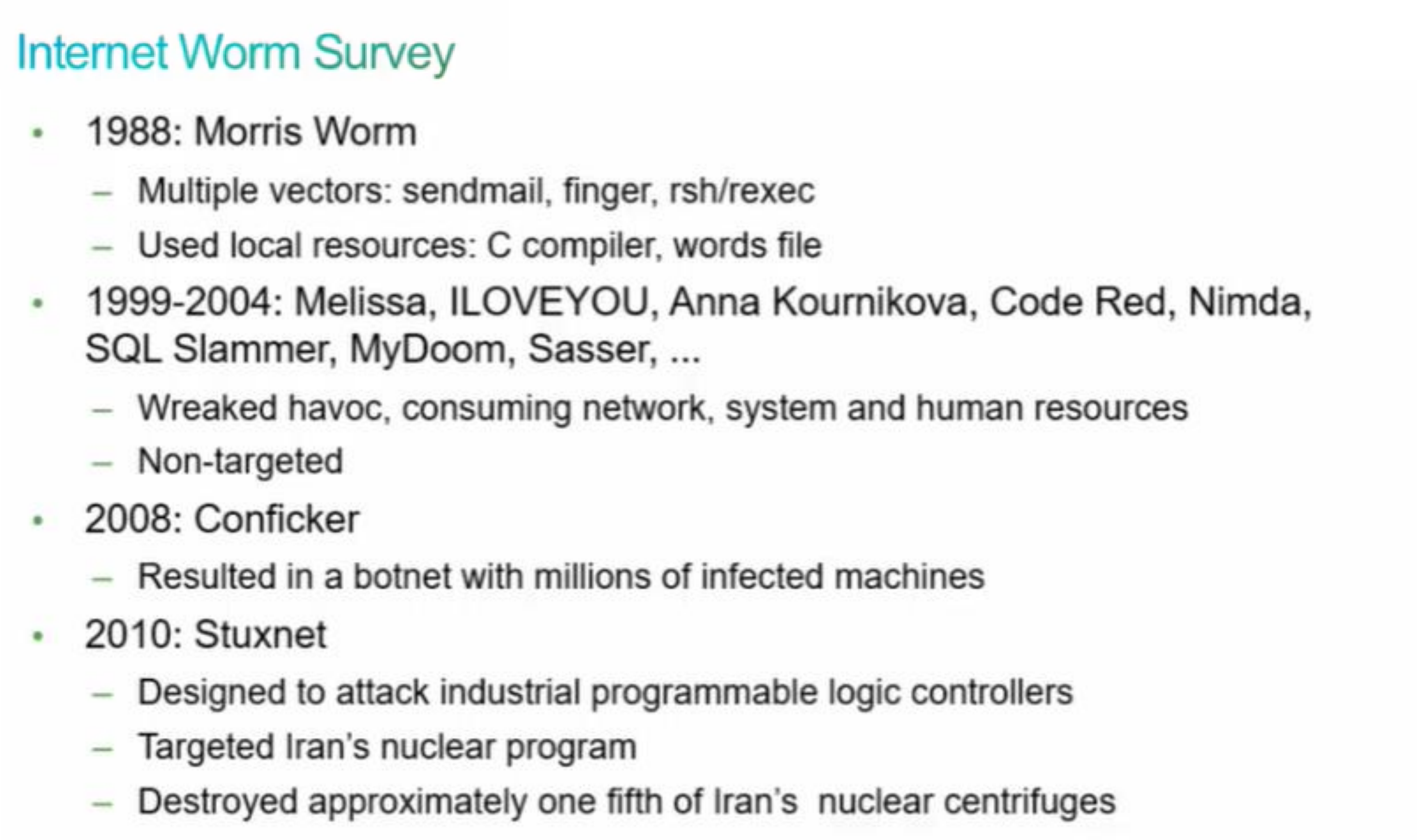
Man-in-the-Middle Attack Example



Host B ARP Table	
IP Address	MAC Address
10.1.1.3	D
10.1.1.4	B
10.1.1.5	D

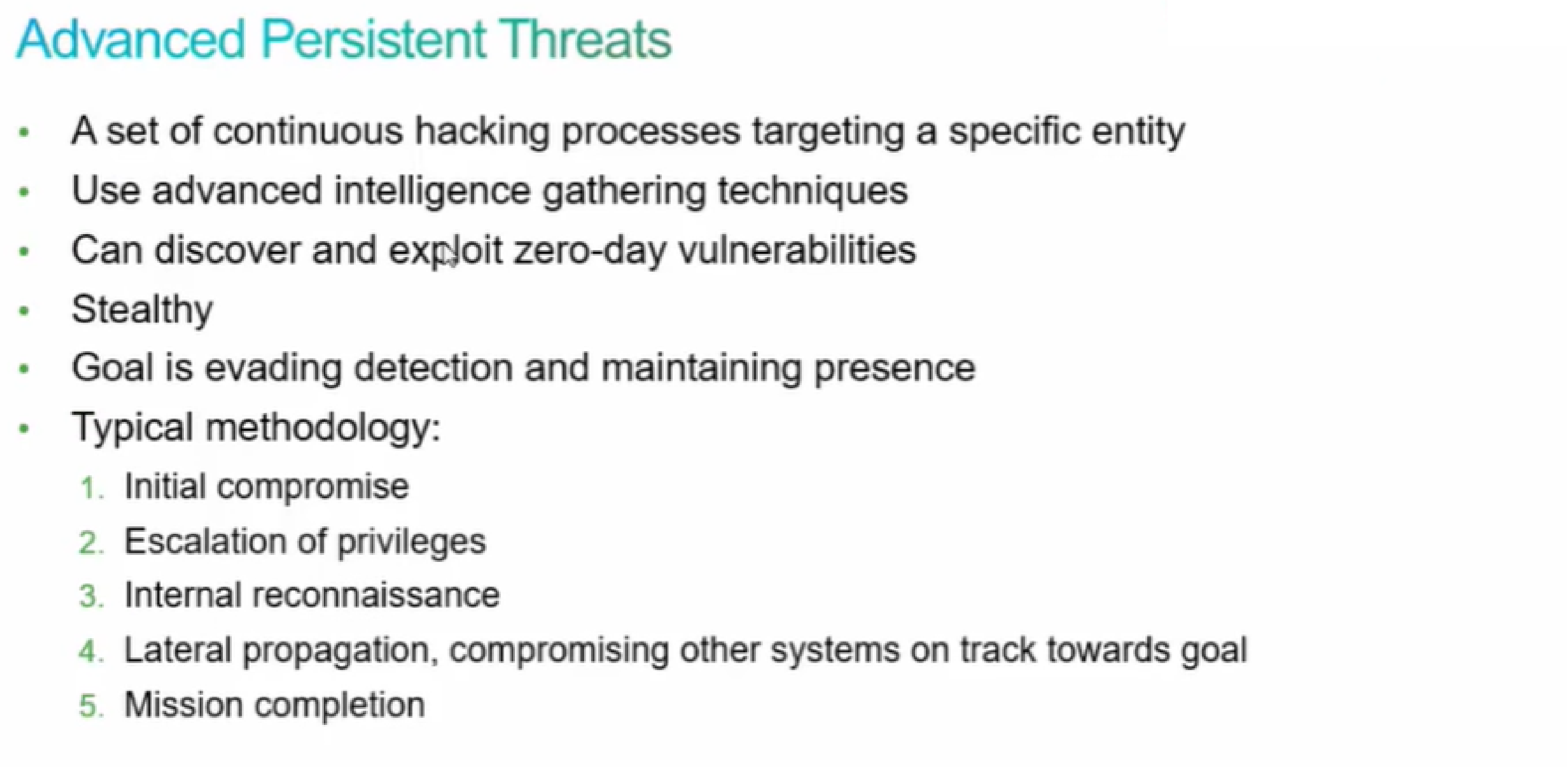
Types of Malicious Software

- Worms
- Viruses
- Trojan horses



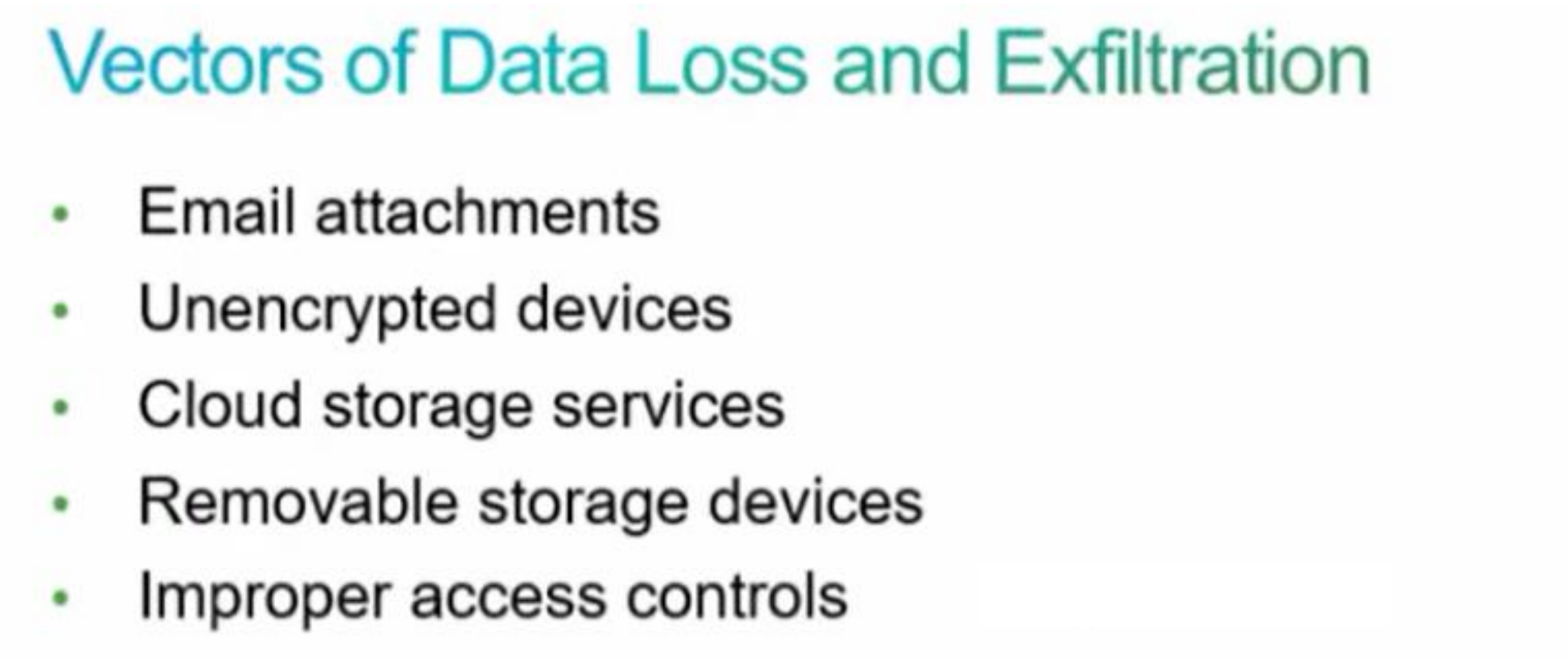
Internet Worm Survey

- 1988: Morris Worm
  - Multiple vectors: sendmail, finger, rsh/rexec
  - Used local resources: C compiler, words file
- 1999-2004: Melissa, ILOVEYOU, Anna Kournikova, Code Red, Nimda, SQL Slammer, MyDoom, Sasser, ...
  - Wreaked havoc, consuming network, system and human resources
  - Non-targeted
- 2008: Conficker
  - Resulted in a botnet with millions of infected machines
- 2010: Stuxnet
  - Designed to attack industrial programmable logic controllers
  - Targeted Iran's nuclear program
  - Destroyed approximately one fifth of Iran's nuclear centrifuges



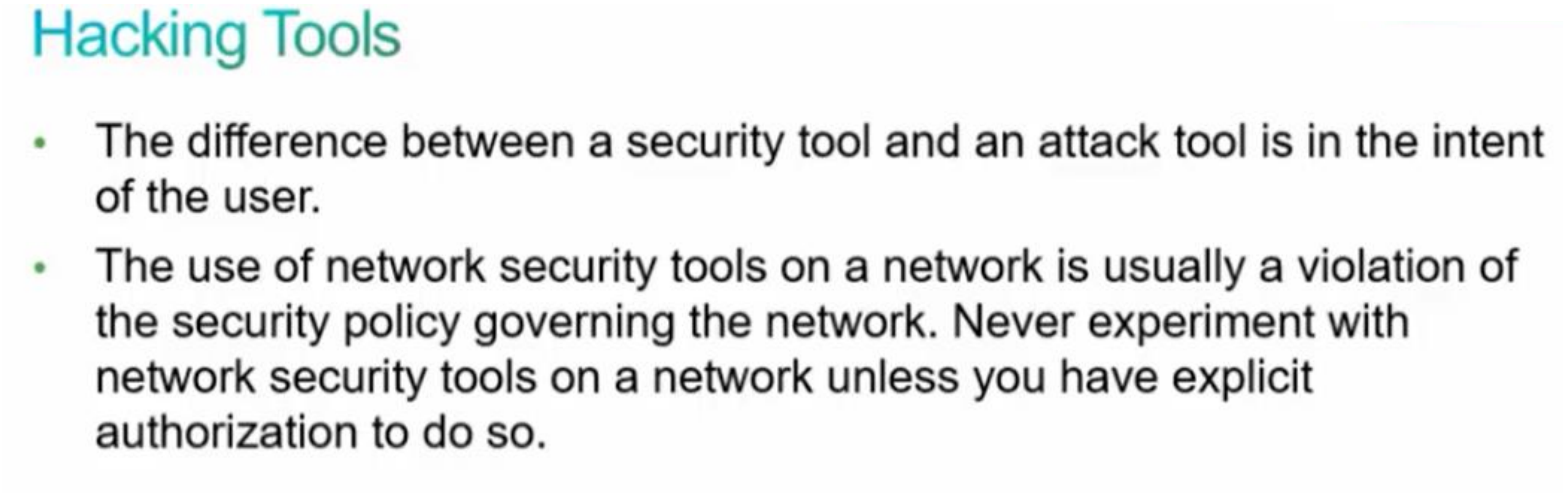
Advanced Persistent Threats

- A set of continuous hacking processes targeting a specific entity
- Use advanced intelligence gathering techniques
- Can discover and exploit zero-day vulnerabilities
- Stealthy
- Goal is evading detection and maintaining presence
- Typical methodology:
  1. Initial compromise
  2. Escalation of privileges
  3. Internal reconnaissance
  4. Lateral propagation, compromising other systems on track towards goal
  5. Mission completion



Vectors of Data Loss and Exfiltration

- Email attachments
- Unencrypted devices
- Cloud storage services
- Removable storage devices
- Improper access controls

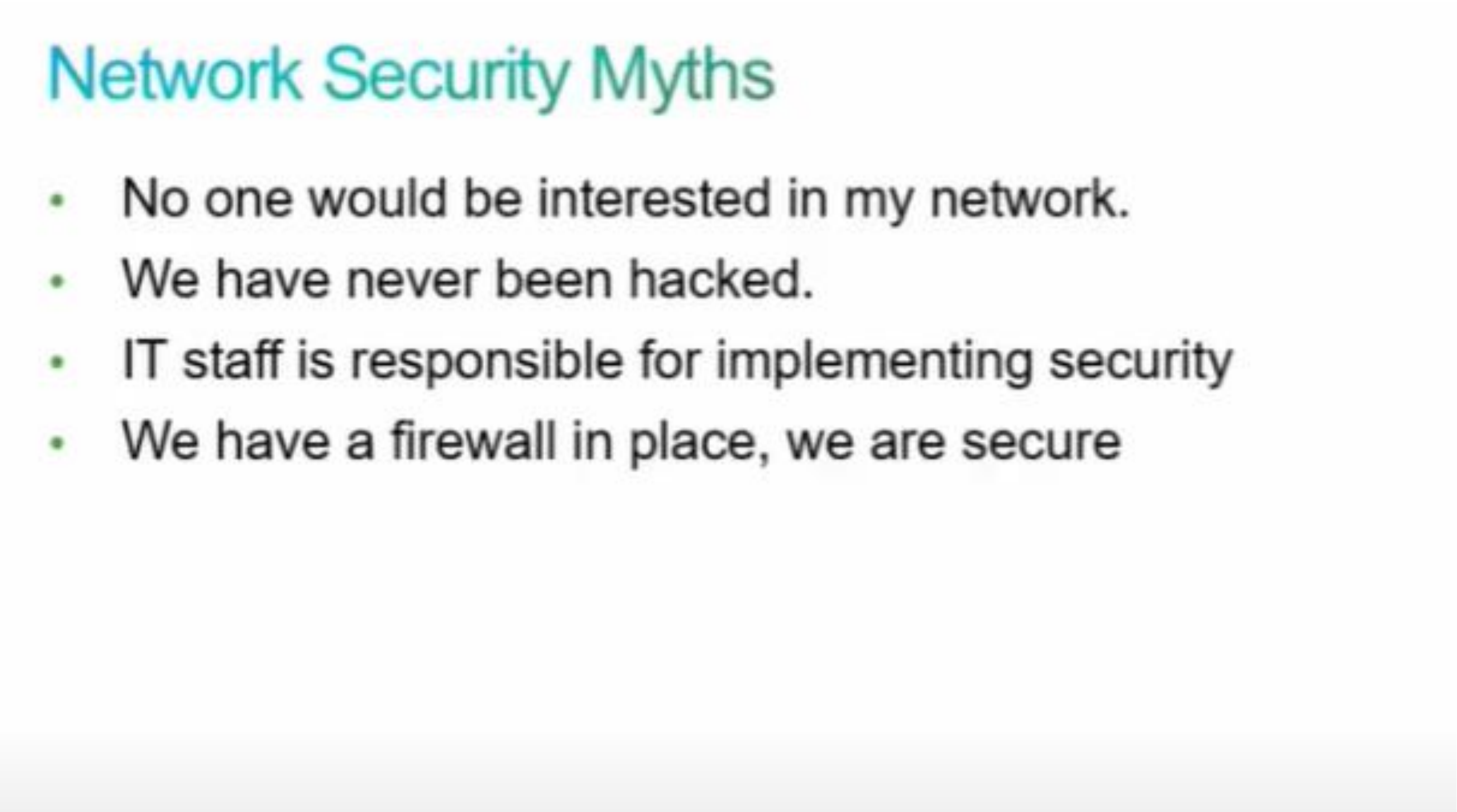


Hacking Tools

- The difference between a security tool and an attack tool is in the intent of the user.
- The use of network security tools on a network is usually a violation of the security policy governing the network. Never experiment with network security tools on a network unless you have explicit authorization to do so.

Hacking Tools (Cont.)

- sectools.org
  - Surveys the network security community and catalogs most popular security tools
  - Descriptions, reviews, links to publisher web sites
  - Password auditors, sniffers, vulnerability scanners, packet crafters, penetration test tools
- Kali Linux
  - Packages over 300 tools in a live Linux distribution
  - Well supported through more than a decade of evolution
  - Continues to be updated to remain current and relevant
- Metasploit
  - Offers hundreds of exploit modules to pair with dozens of payloads
  - Lowers the threshold of experience required to perform sophisticated attacks

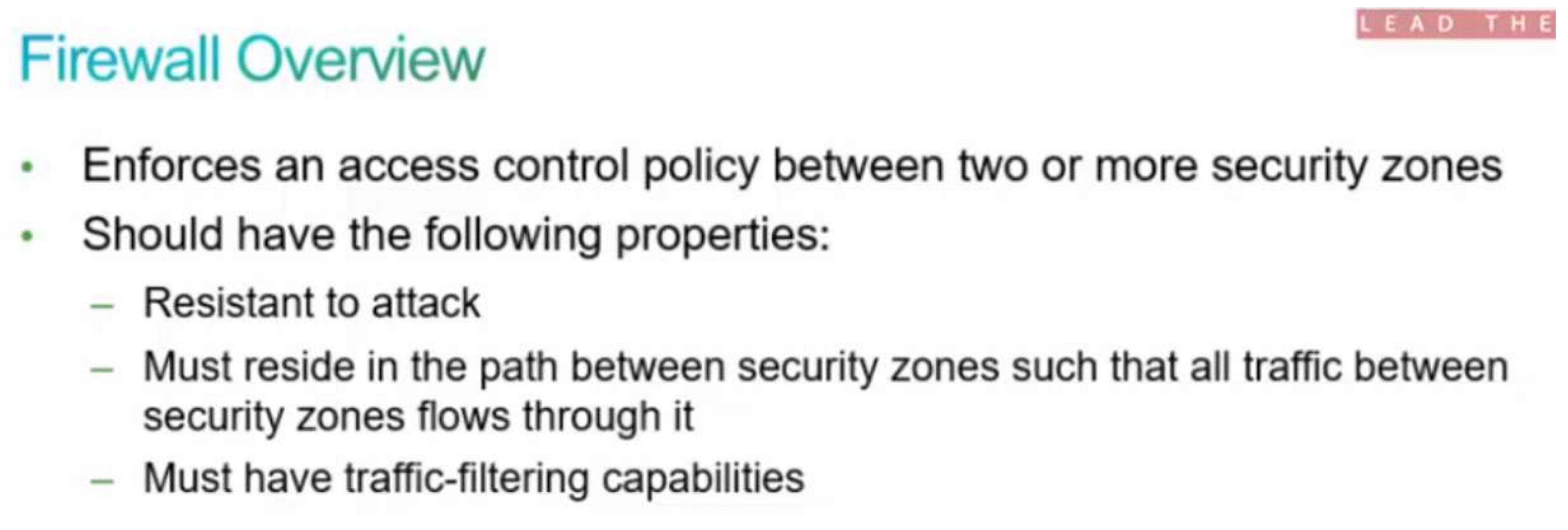


Network Security Myths

- No one would be interested in my network.
- We have never been hacked.
- IT staff is responsible for implementing security
- We have a firewall in place, we are secure

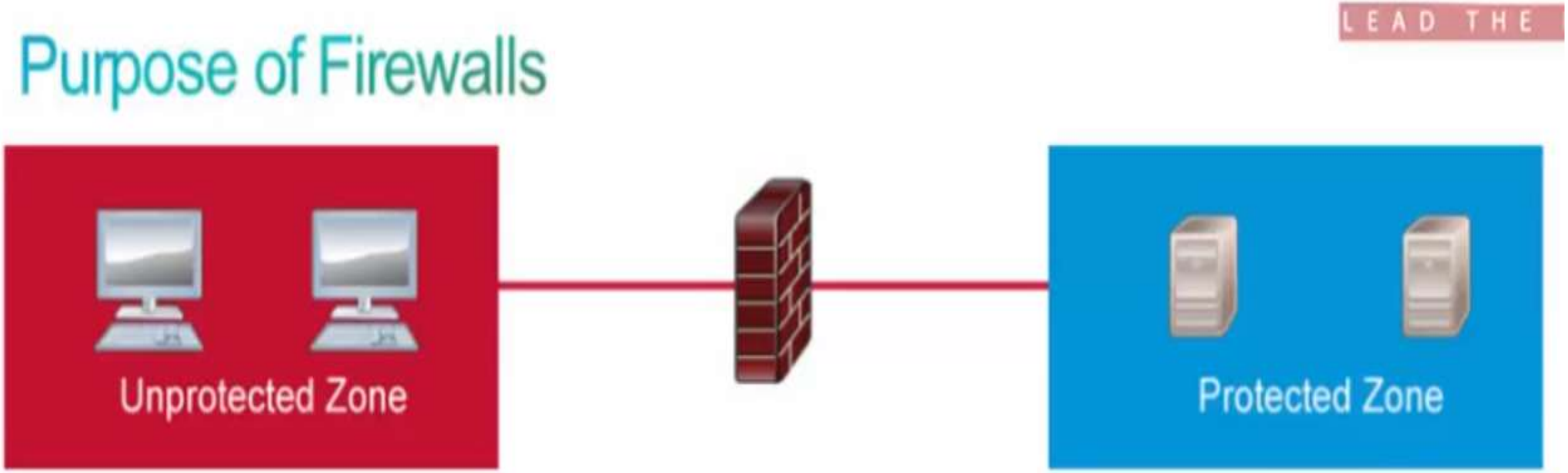
Threat defensive technology

SECURITY CONCEPTS



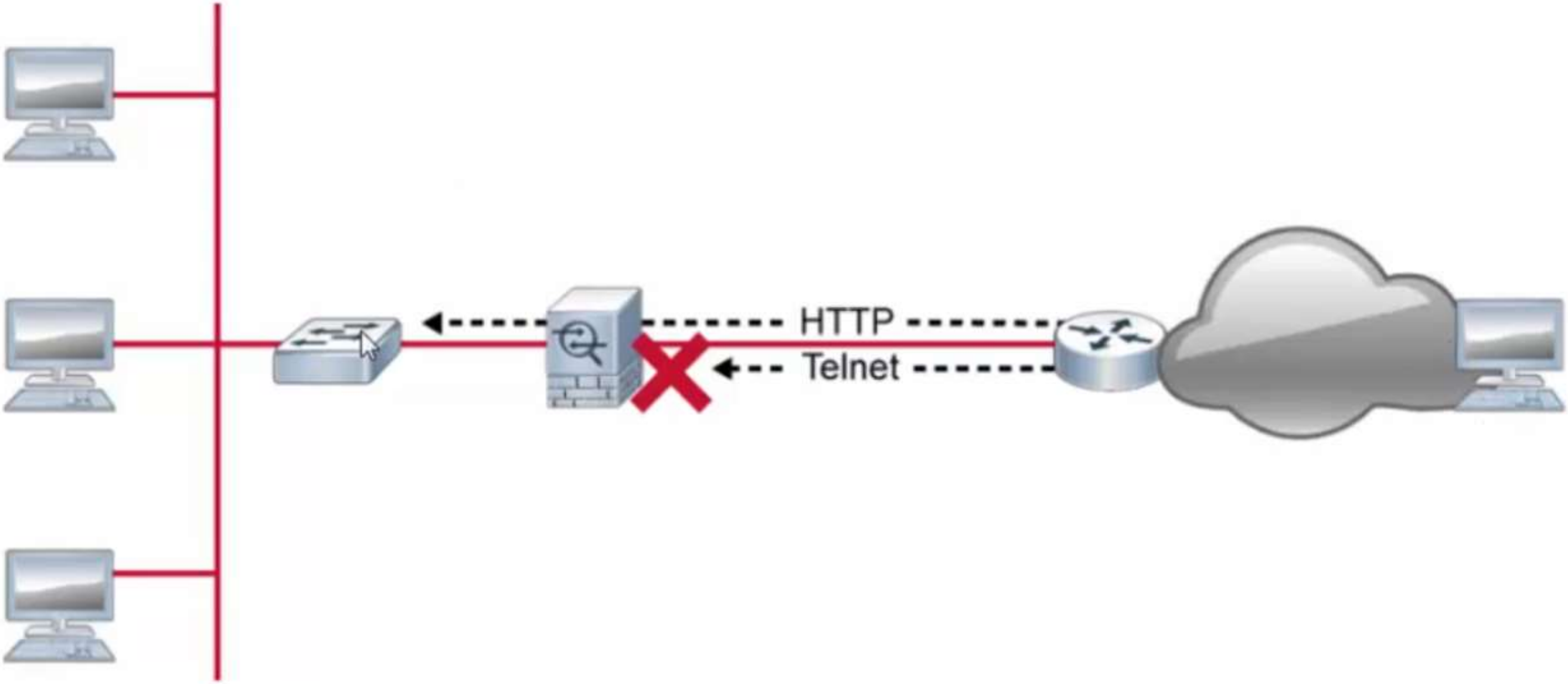
Firewall Overview

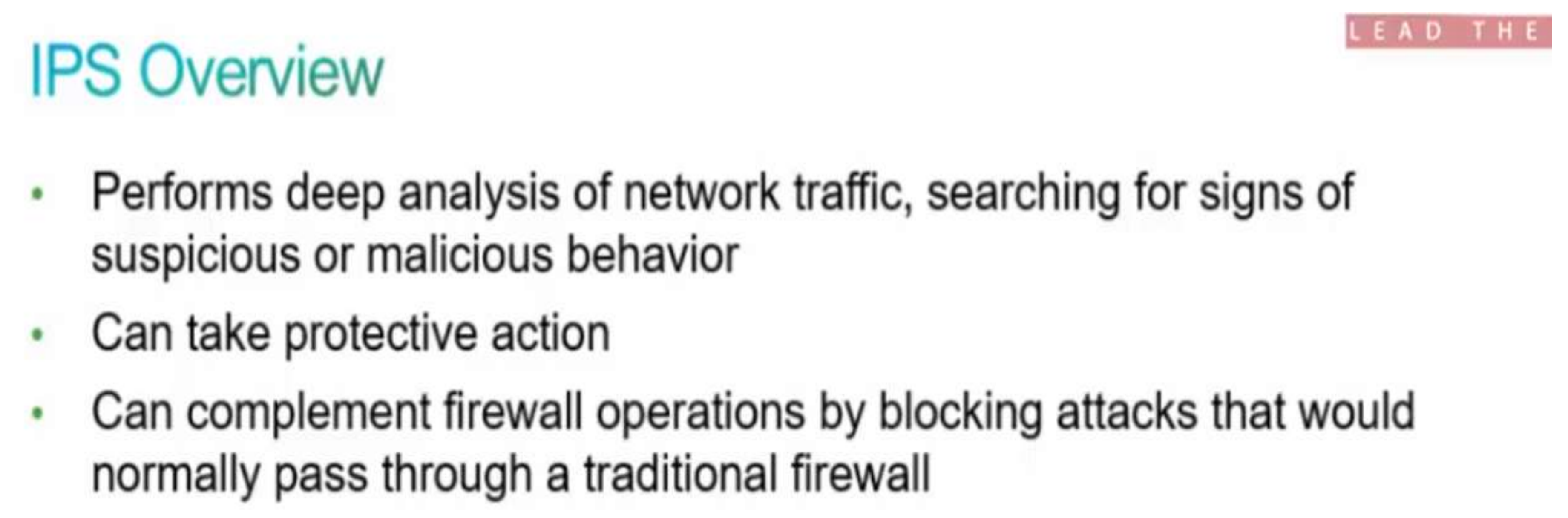
- Enforces an access control policy between two or more security zones
- Should have the following properties:
  - Resistant to attack
  - Must reside in the path between security zones such that all traffic between security zones flows through it
  - Must have traffic-filtering capabilities



Purpose of Firewalls

Firewall Functionality

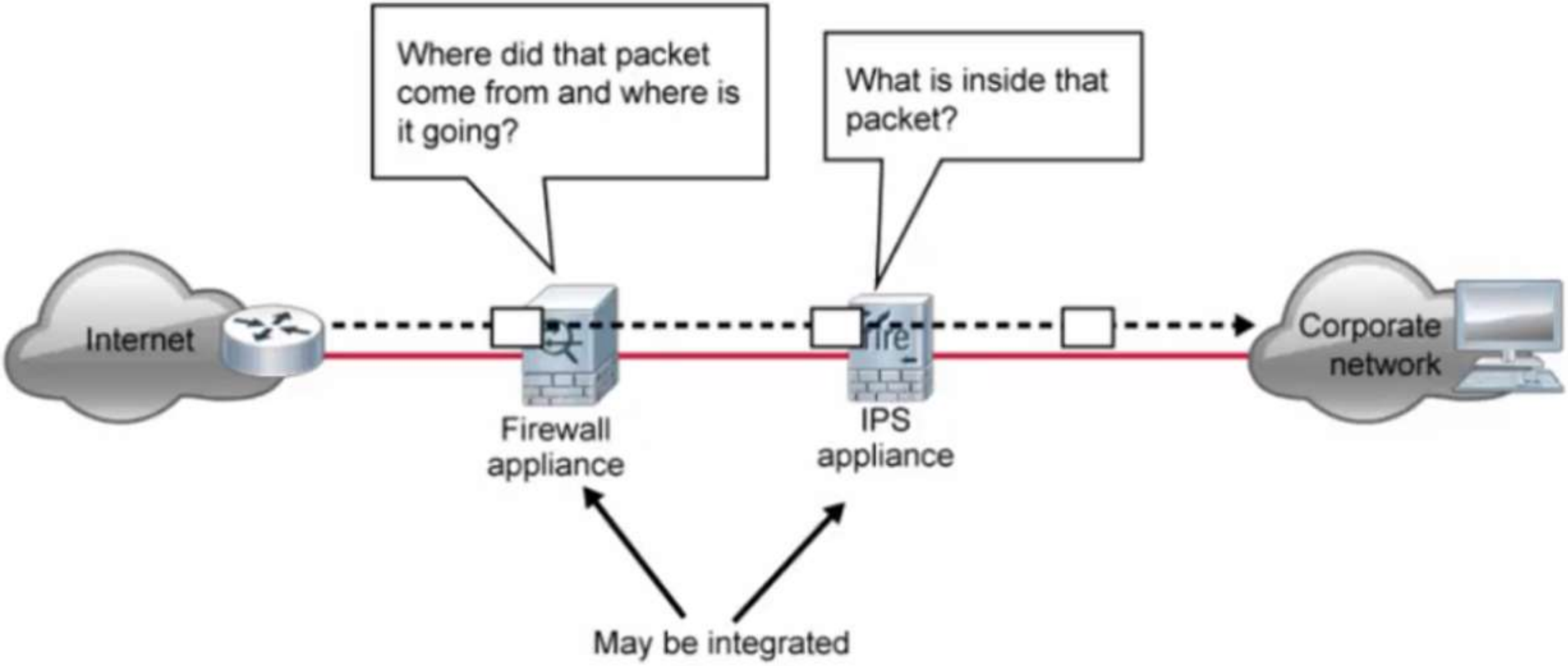




IPS Overview

- Performs deep analysis of network traffic, searching for signs of suspicious or malicious behavior
- Can take protective action
- Can complement firewall operations by blocking attacks that would normally pass through a traditional firewall

IPS Functionality



Where did that packet come from and where is it going?

What is inside that packet?

Internet

Firewall appliance

IPS appliance

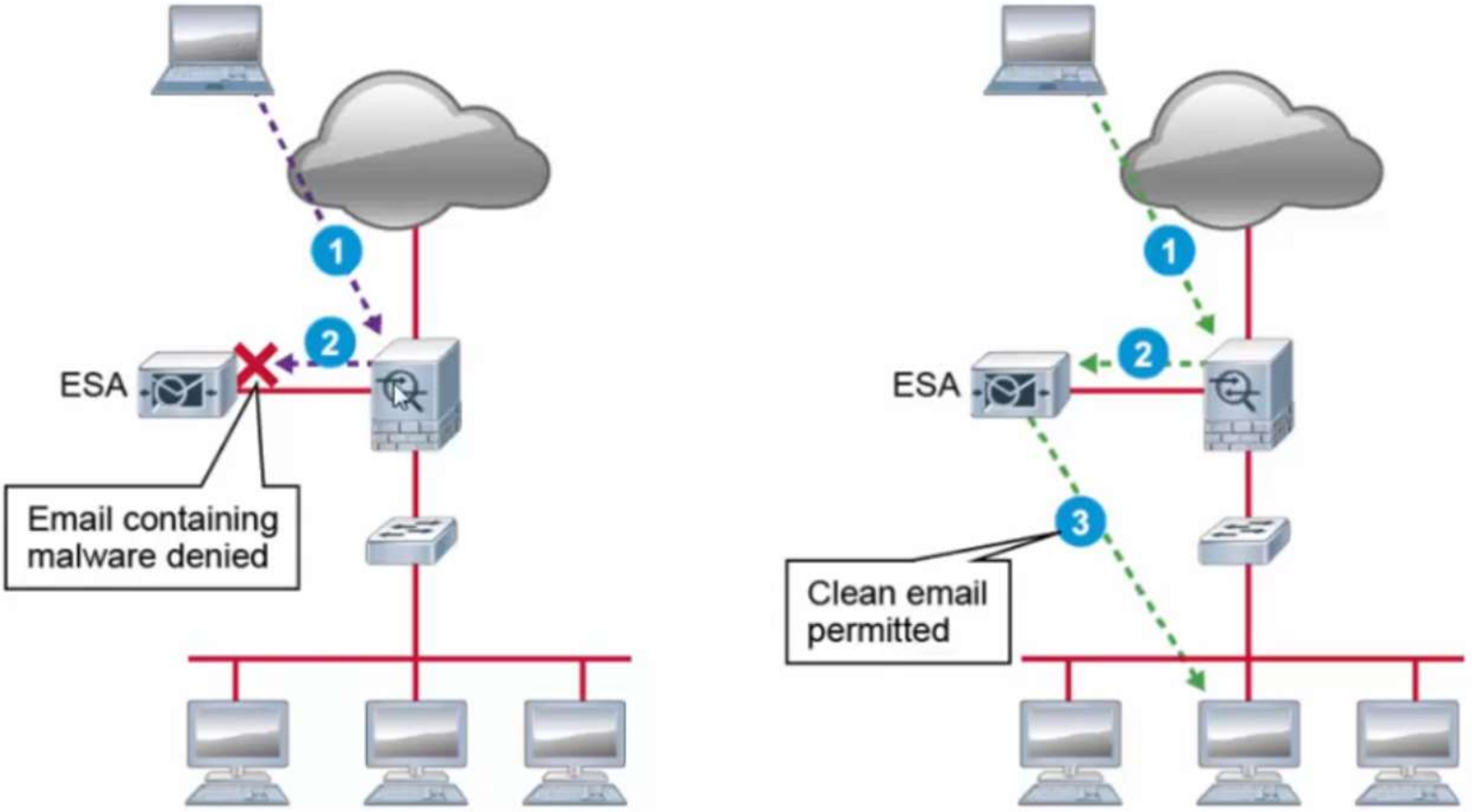
Corporate network

May be integrated

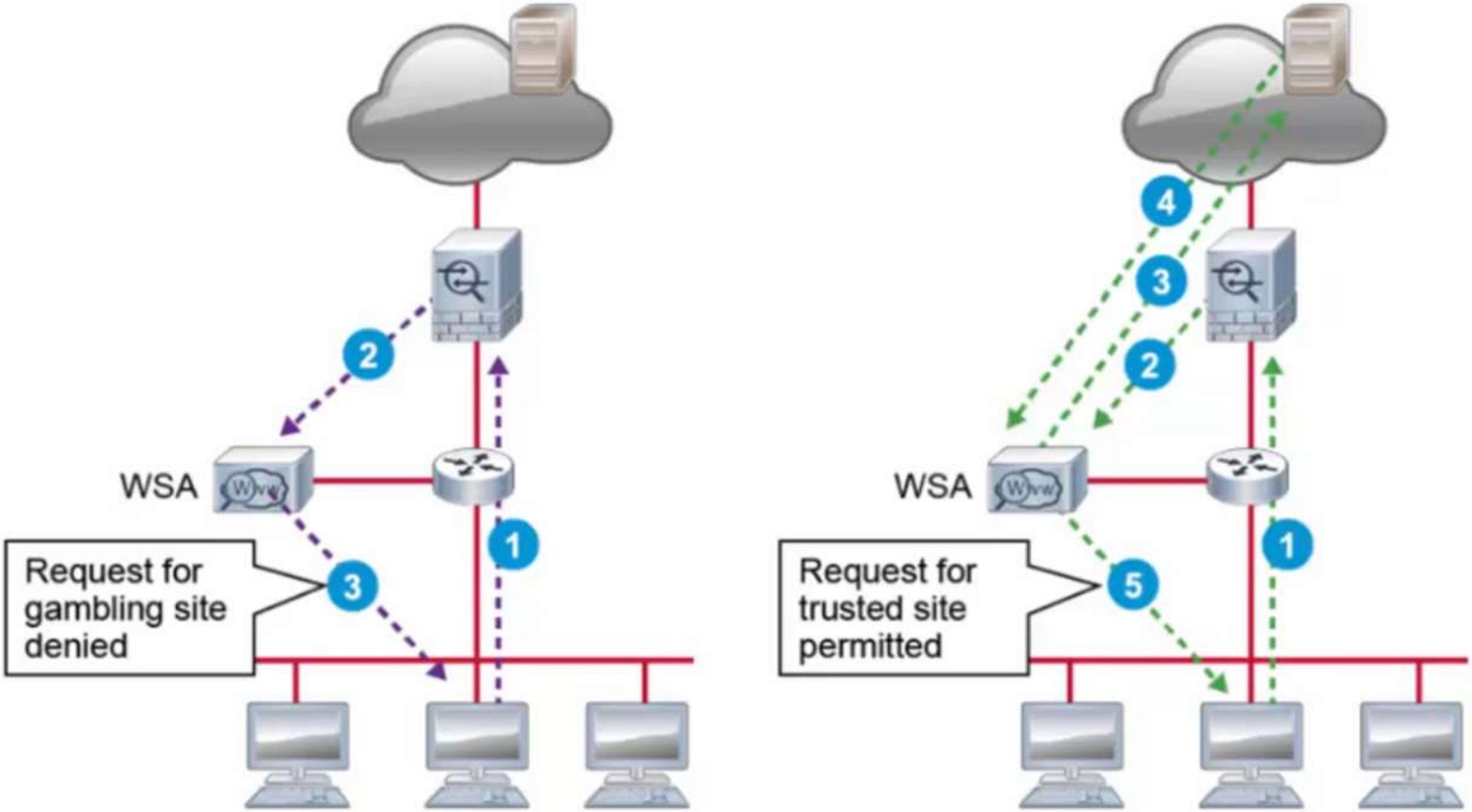
Content Security Overview

- Content security systems provide fine-grained control and security on particular network applications.
- Examples of Cisco content security products include:
  - **Cisco ESA:** A type of firewall and threat monitoring appliance for SMTP traffic
  - **Cisco WSA:** Provides secure web access, content security, and threat mitigation for web services

Cisco ESA

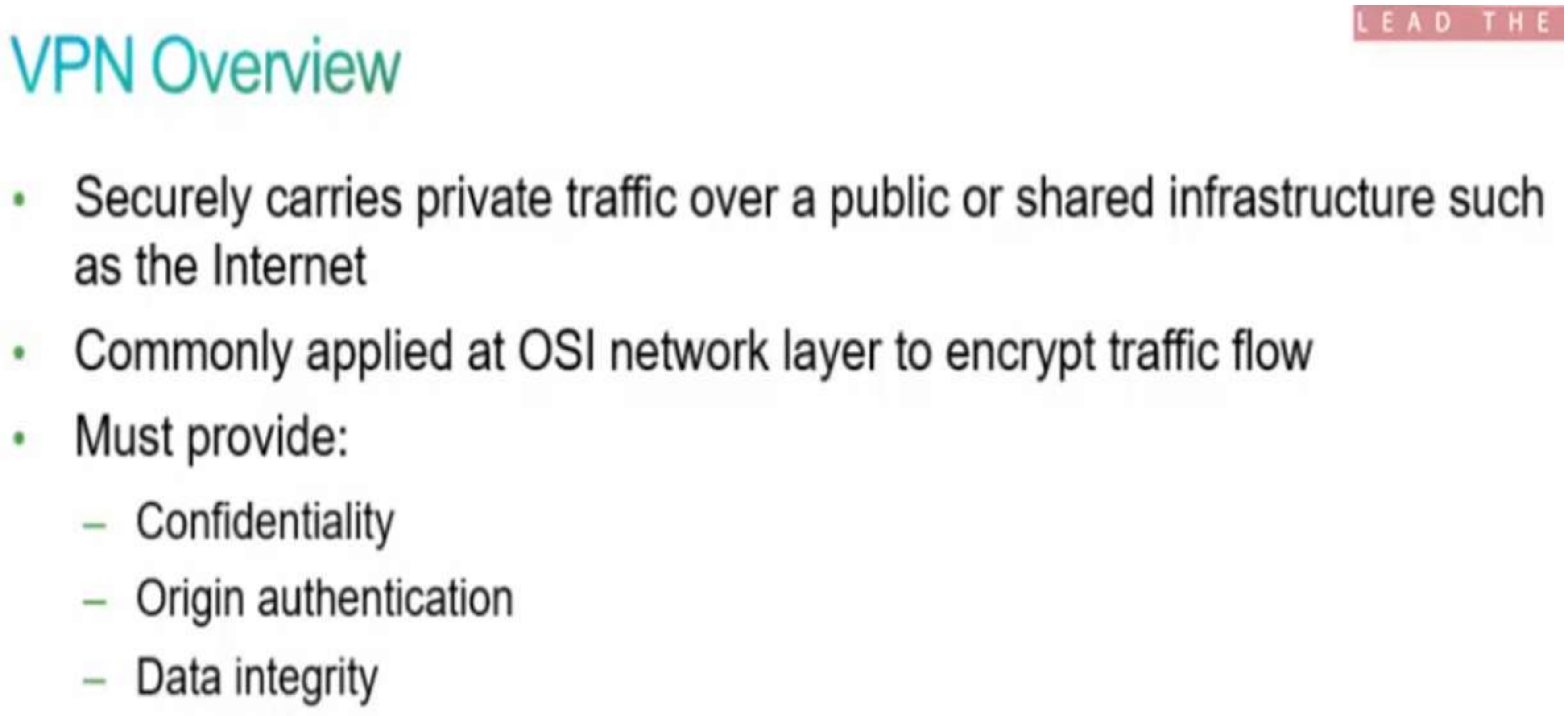

1
2
ESA
Email containing malware denied
1
2
ESA
3
Clean email permitted

Cisco WSA



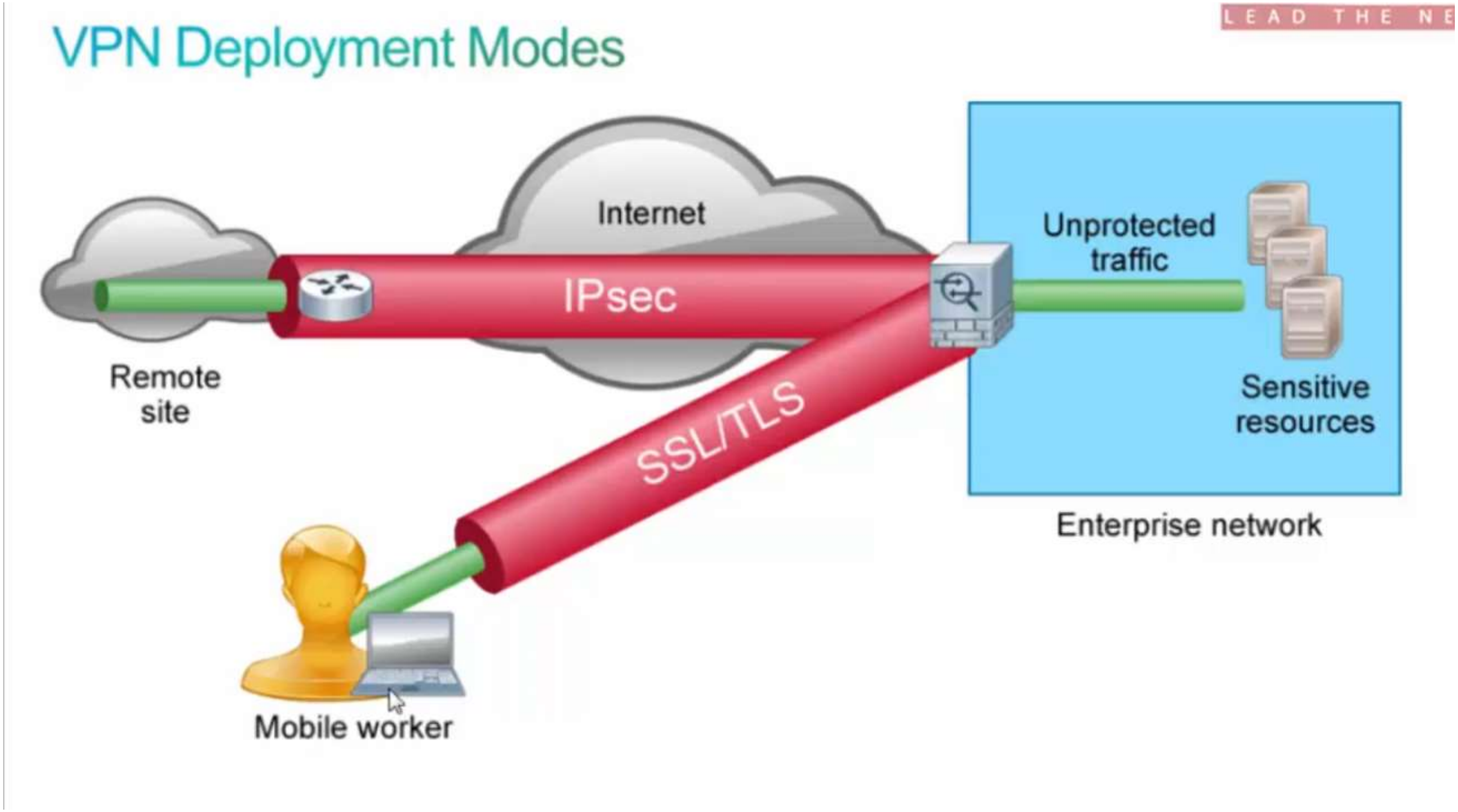
Request for gambling site denied

Request for trusted site permitted



VPN Overview

- Securely carries private traffic over a public or shared infrastructure such as the Internet
- Commonly applied at OSI network layer to encrypt traffic flow
- Must provide:
  - Confidentiality
  - Origin authentication
  - Data integrity

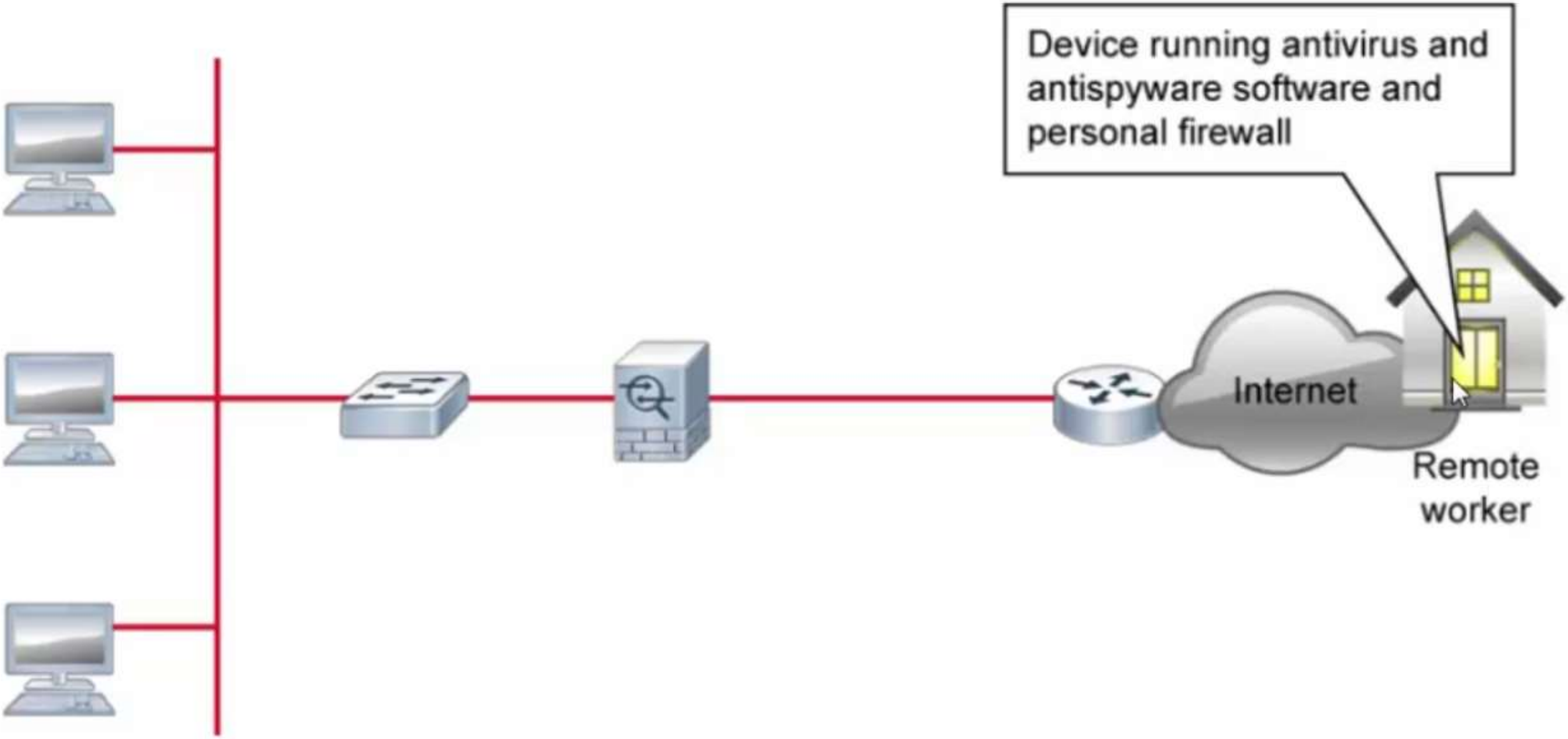


VPN Deployment Modes

Endpoint Security Overview

- Protects an endpoint device such as a user laptop
- Verifies the user, device, and device state
- Traditional endpoint security:
  - Personal firewalls
  - Antivirus software
  - Antispyware software
- Enhances network security (A secured endpoint cannot be a network attack vector.)

Traditional Endpoint Protection



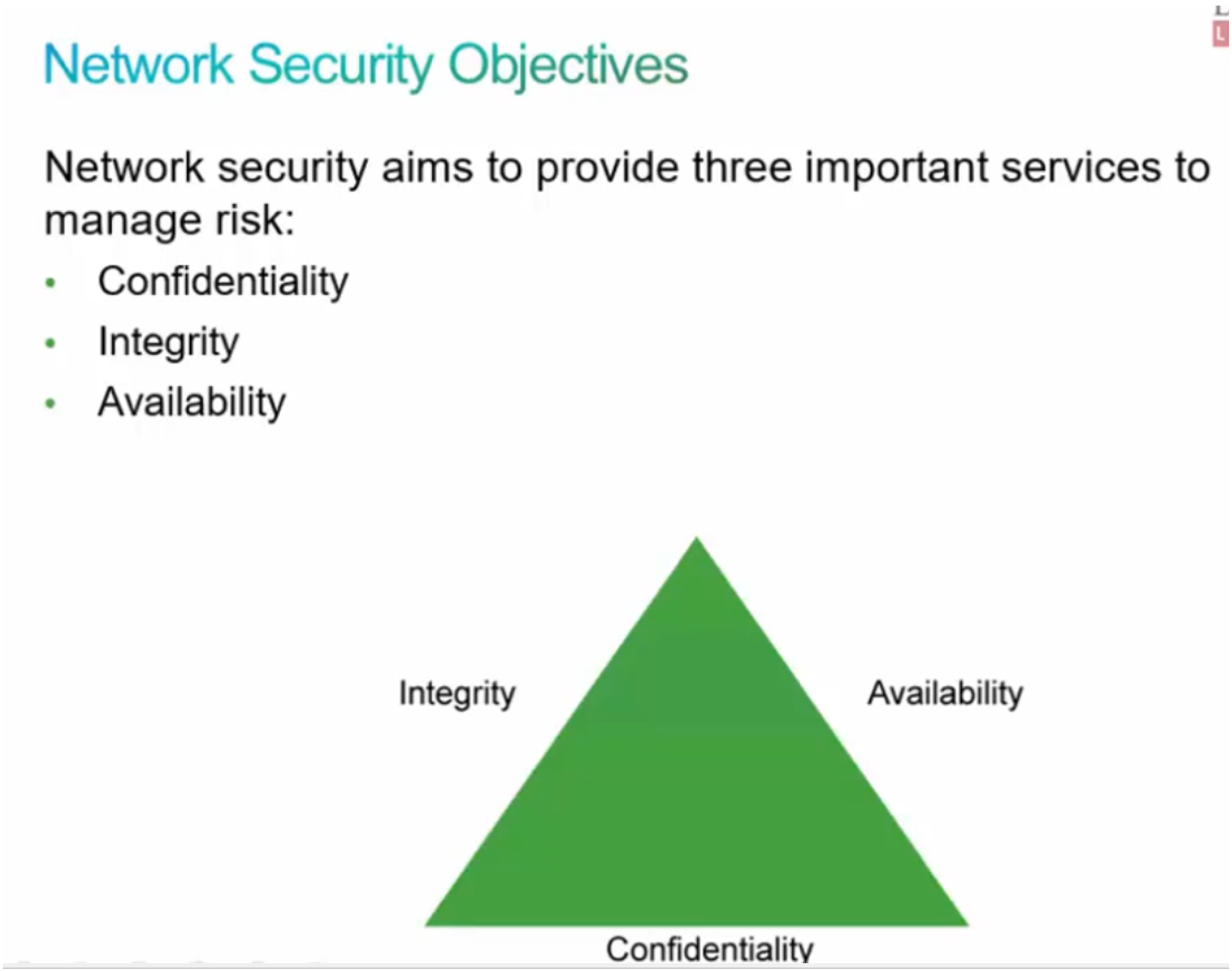
Device running antivirus and antispyware software and personal firewall

Logging

- Along with monitoring, is a critical aspect of network security
- Needed for troubleshooting and policy-compliance auditing
- Enables you to recognize the start of an attack or an attack in progress
- Supported by all Cisco security devices
- Can send logs to:
  - Console
  - Monitor
  - Memory buffer
  - Syslog server
  - SNMP trap
  - Flash memory
- Can use SIEM technology to facilitate collecting, correlating, and acting on logged information

Security policy and basic security architecture

SECURITY CONCEPTS



Network Security Objectives

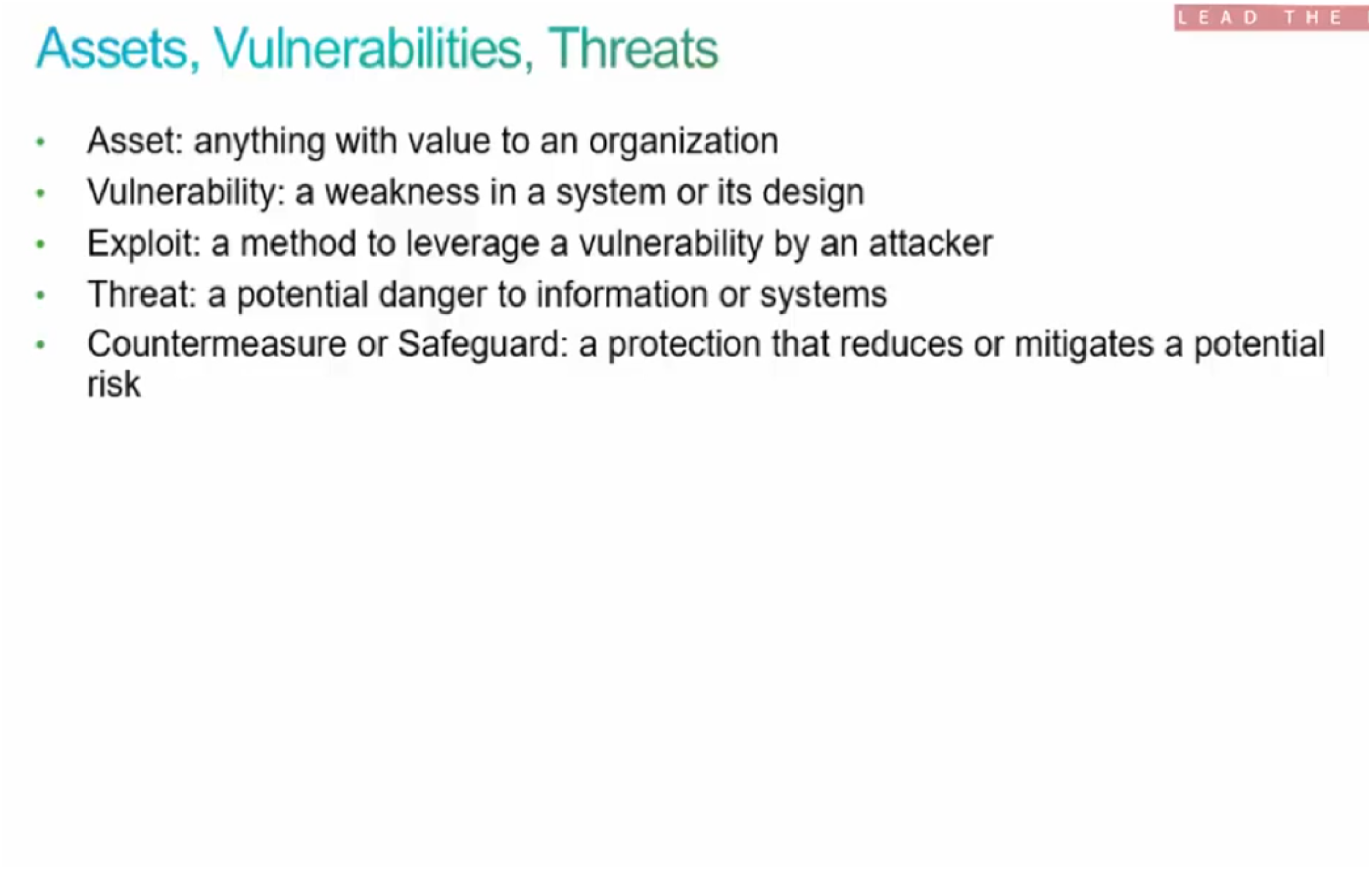
Network security aims to provide three important services to manage risk:

- Confidentiality
- Integrity
- Availability

Integrity

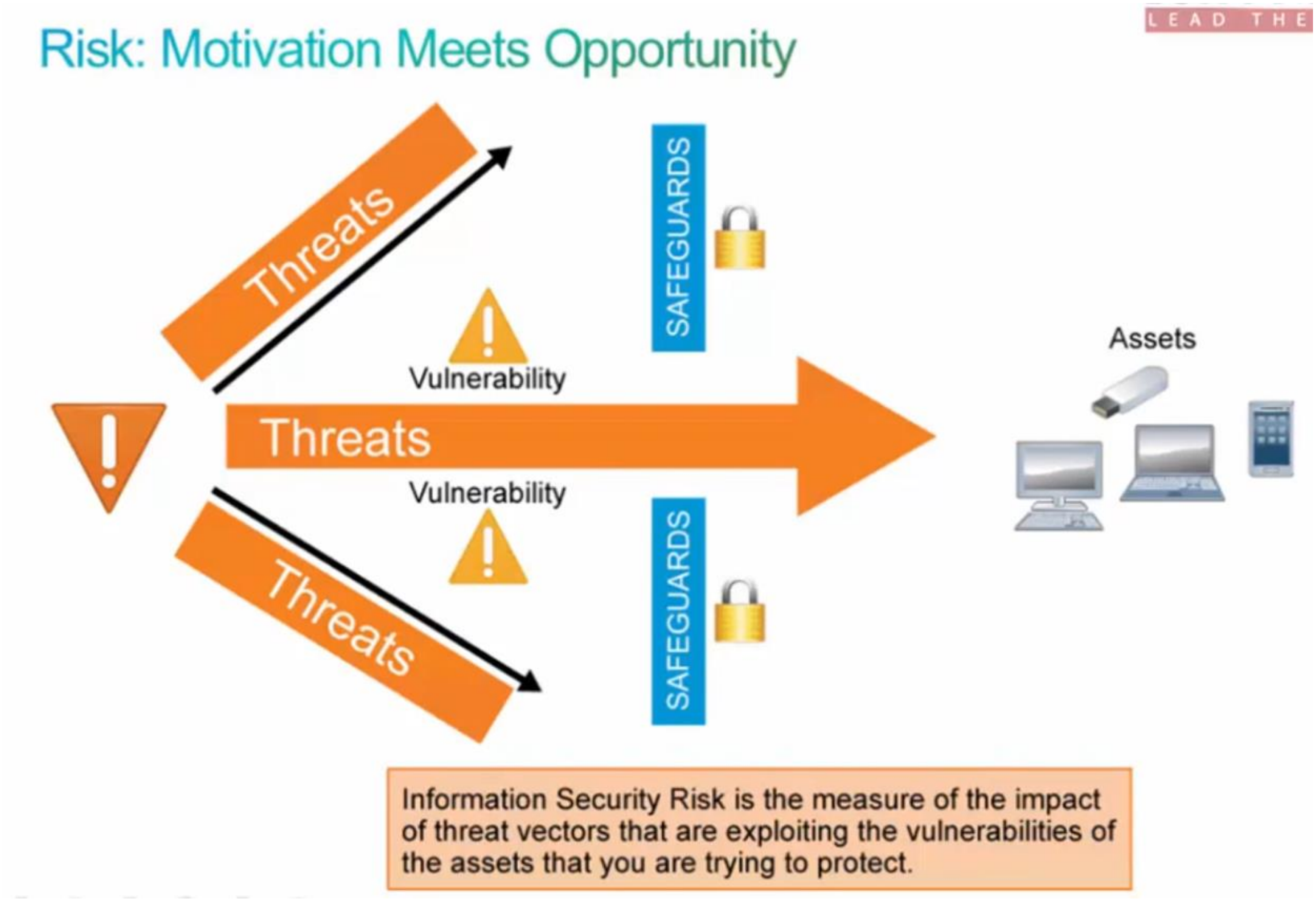
Availability

Confidentiality



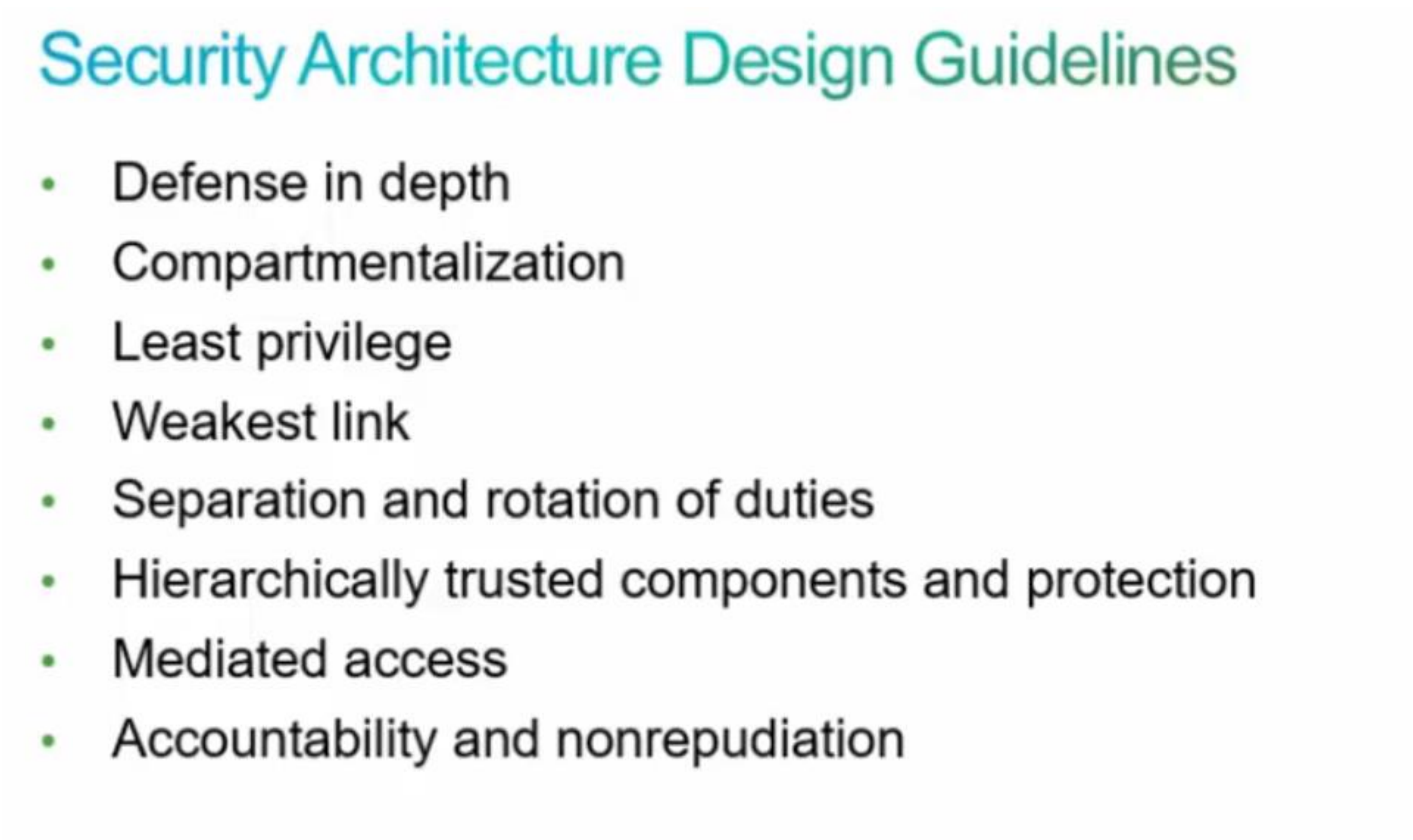
Assets, Vulnerabilities, Threats

- Asset: anything with value to an organization
- Vulnerability: a weakness in a system or its design
- Exploit: a method to leverage a vulnerability by an attacker
- Threat: a potential danger to information or systems
- Countermeasure or Safeguard: a protection that reduces or mitigates a potential risk



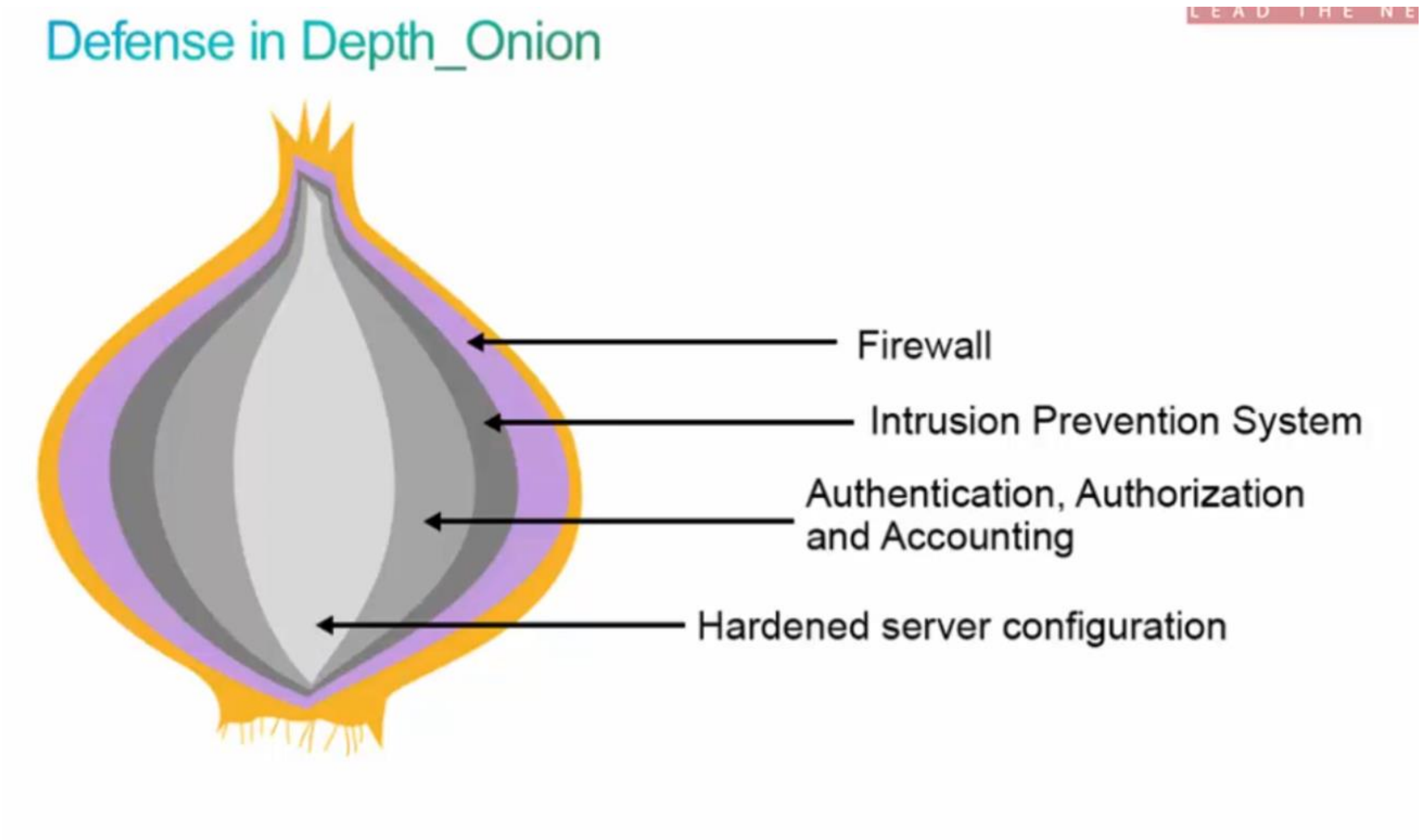
Risk: Motivation Meets Opportunity

Information Security Risk is the measure of the impact of threat vectors that are exploiting the vulnerabilities of the assets that you are trying to protect.



Security Architecture Design Guidelines

- Defense in depth
- Compartmentalization
- Least privilege
- Weakest link
- Separation and rotation of duties
- Hierarchically trusted components and protection
- Mediated access
- Accountability and nonrepudiation



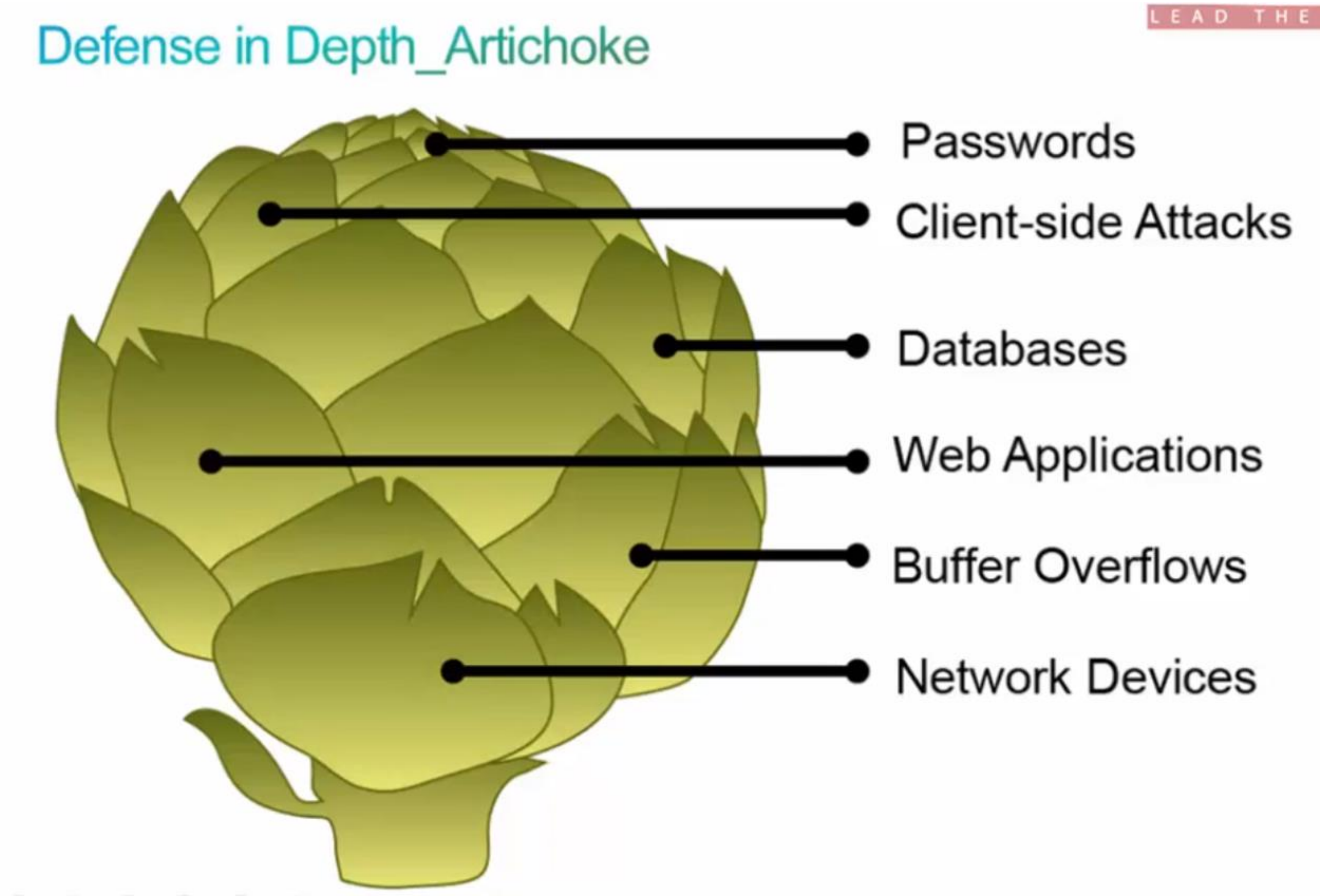
Defense in Depth_Onion

Firewall

Intrusion Prevention System

Authentication, Authorization and Accounting

Hardened server configuration



Defense in Depth_Artichoke

Passwords

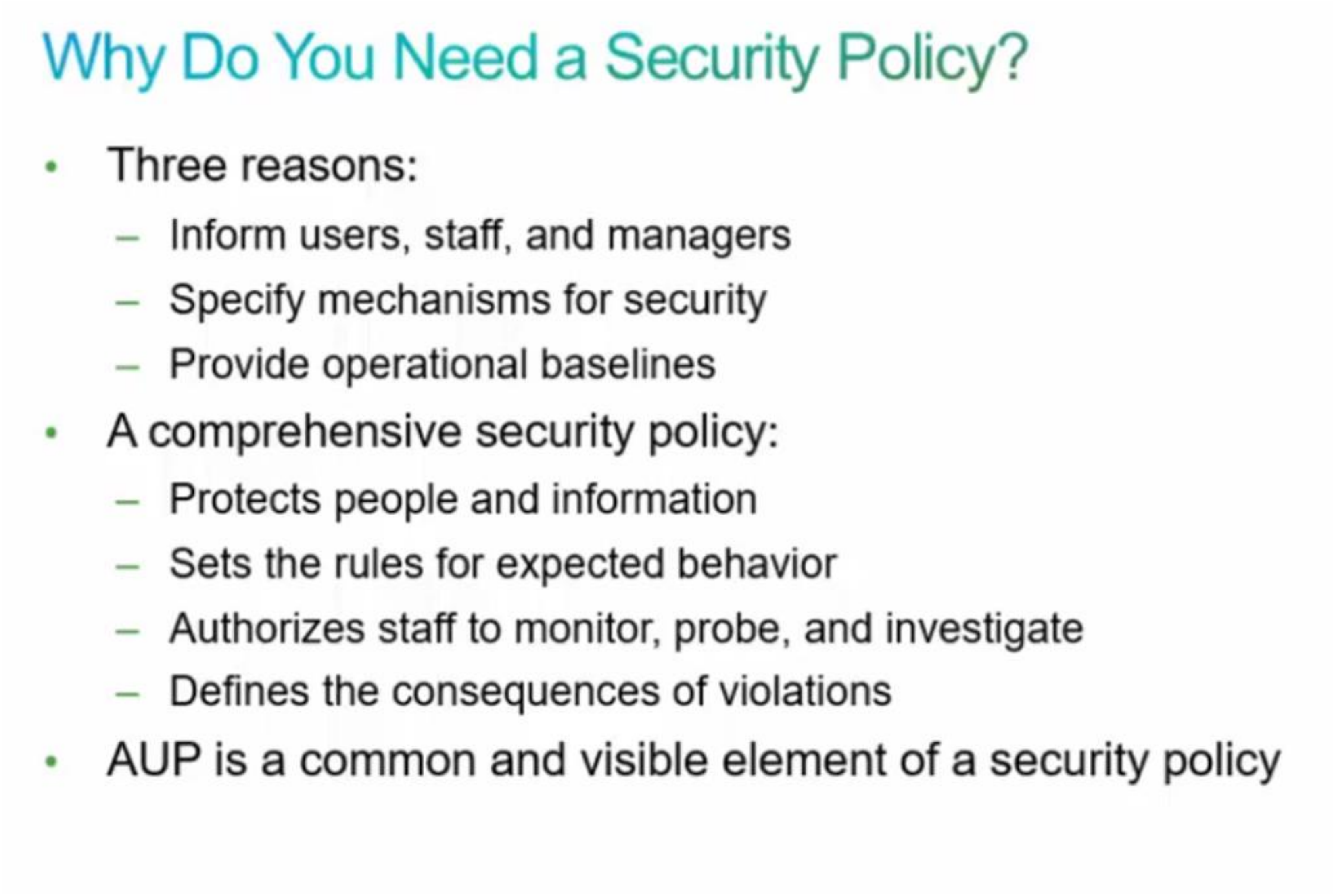
Client-side Attacks

Databases

Web Applications

Buffer Overflows

Network Devices

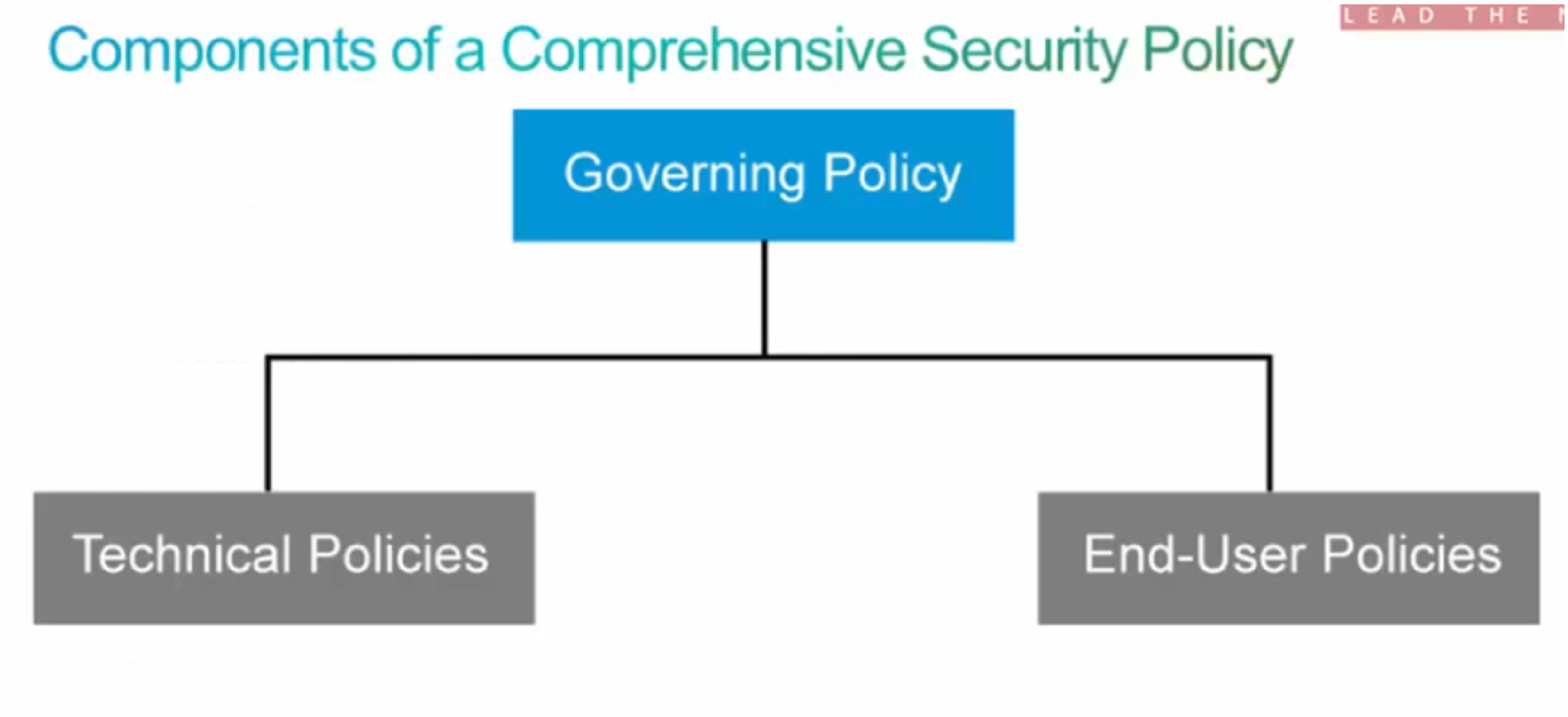


Why Do You Need a Security Policy?

- Three reasons:
  - Inform users, staff, and managers
  - Specify mechanisms for security
  - Provide operational baselines
- A comprehensive security policy:
  - Protects people and information
  - Sets the rules for expected behavior
  - Authorizes staff to monitor, probe, and investigate
  - Defines the consequences of violations
- AUP is a common and visible element of a security policy

Who Uses the Security Policy?

- Internal audiences
  - Managers and executives
  - Departments and business units
  - Technical staff
  - End users
- External audiences
  - Partners
  - Customers
  - Suppliers
  - Consultants and contractors



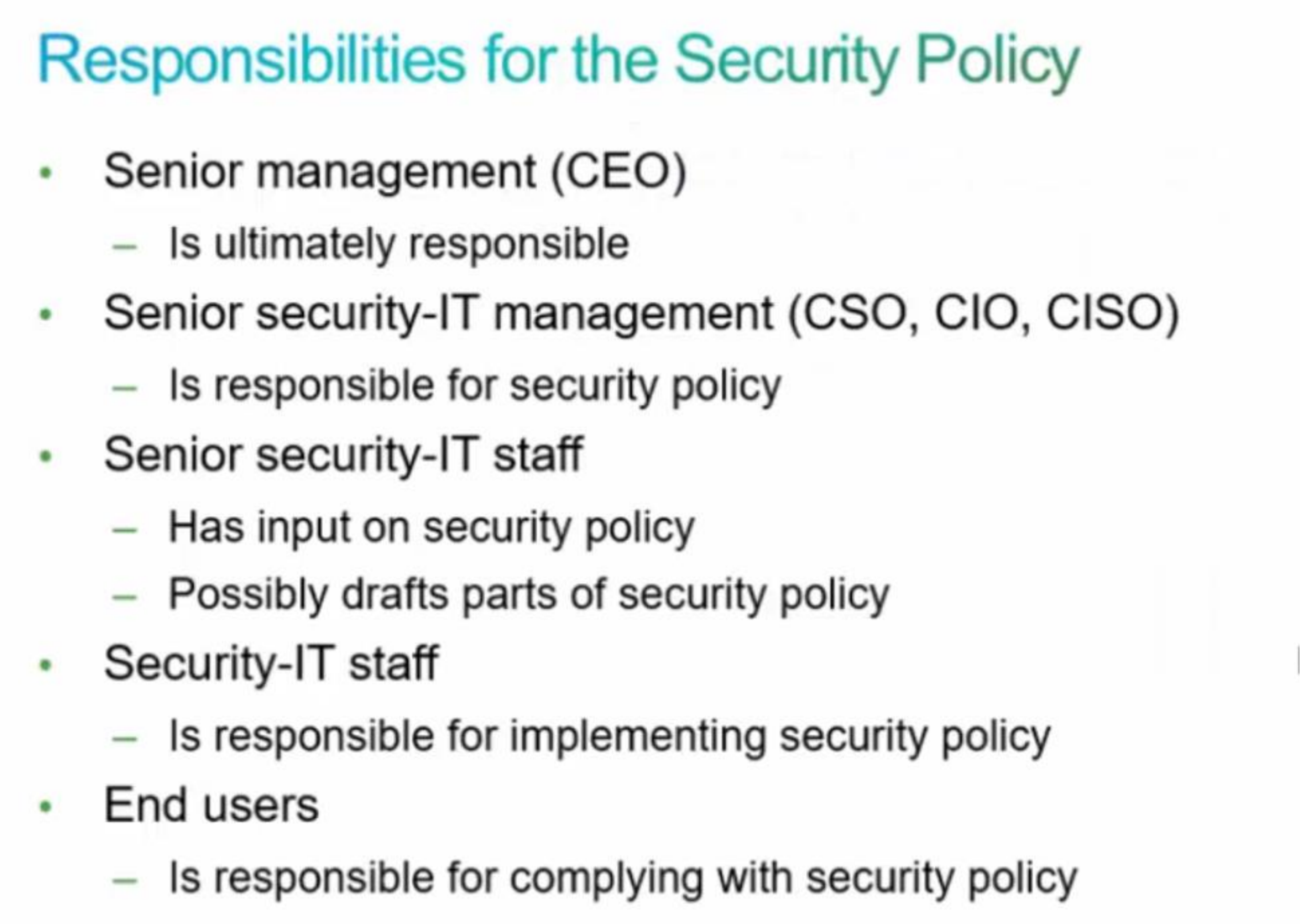
LEAD THE

Components of a Comprehensive Security Policy

Governing Policy

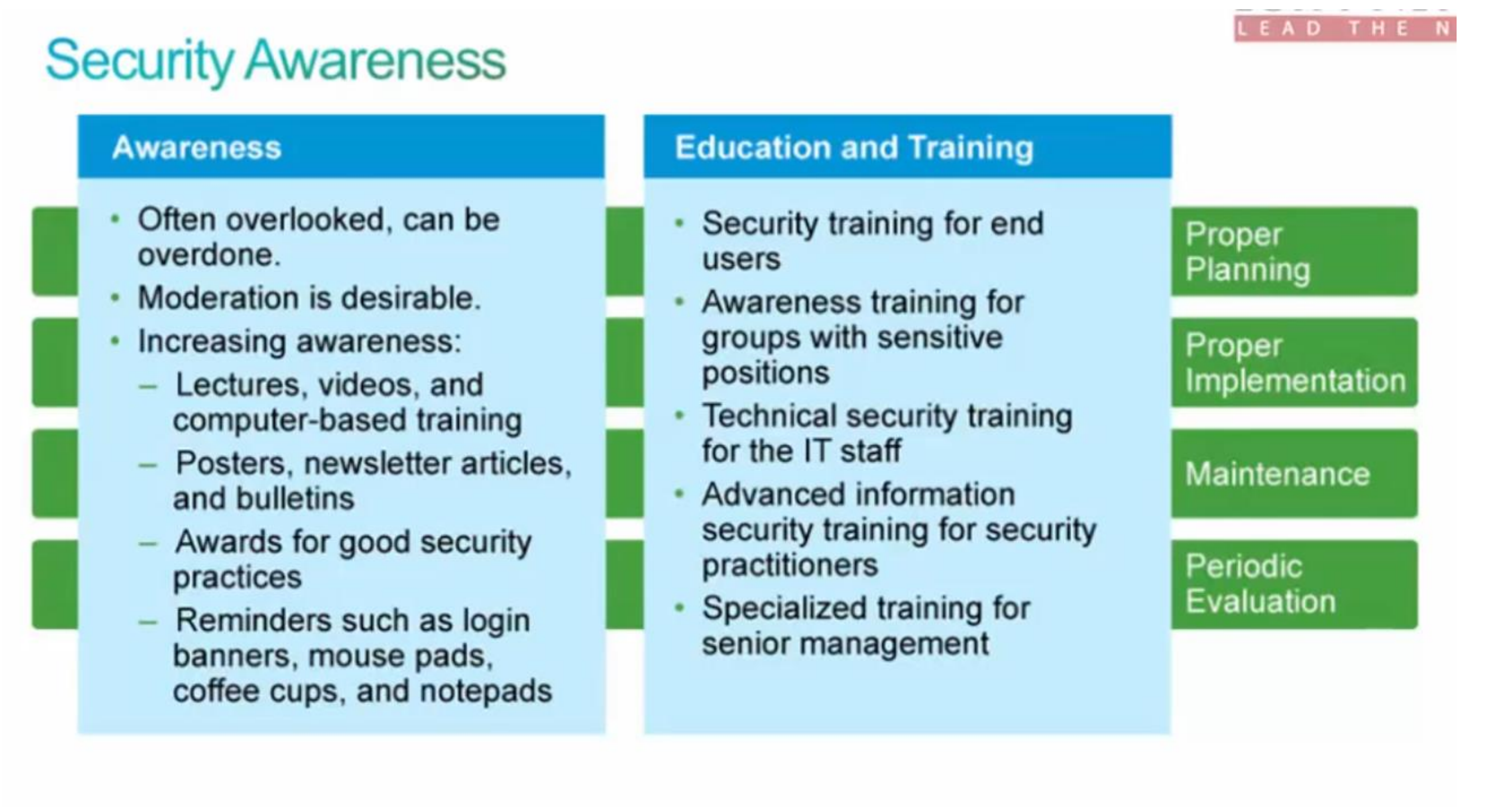
Technical Policies

End-User Policies



Responsibilities for the Security Policy

- Senior management (CEO)
  - Is ultimately responsible
- Senior security-IT management (CSO, CIO, CISO)
  - Is responsible for security policy
- Senior security-IT staff
  - Has input on security policy
  - Possibly drafts parts of security policy
- Security-IT staff
  - Is responsible for implementing security policy
- End users
  - Is responsible for complying with security policy



Security Awareness

Awareness

- Often overlooked, can be overdone.
- Moderation is desirable.
- Increasing awareness:
  - Lectures, videos, and computer-based training
  - Posters, newsletter articles, and bulletins
  - Awards for good security practices
  - Reminders such as login banners, mouse pads, coffee cups, and notepads

Education and Training

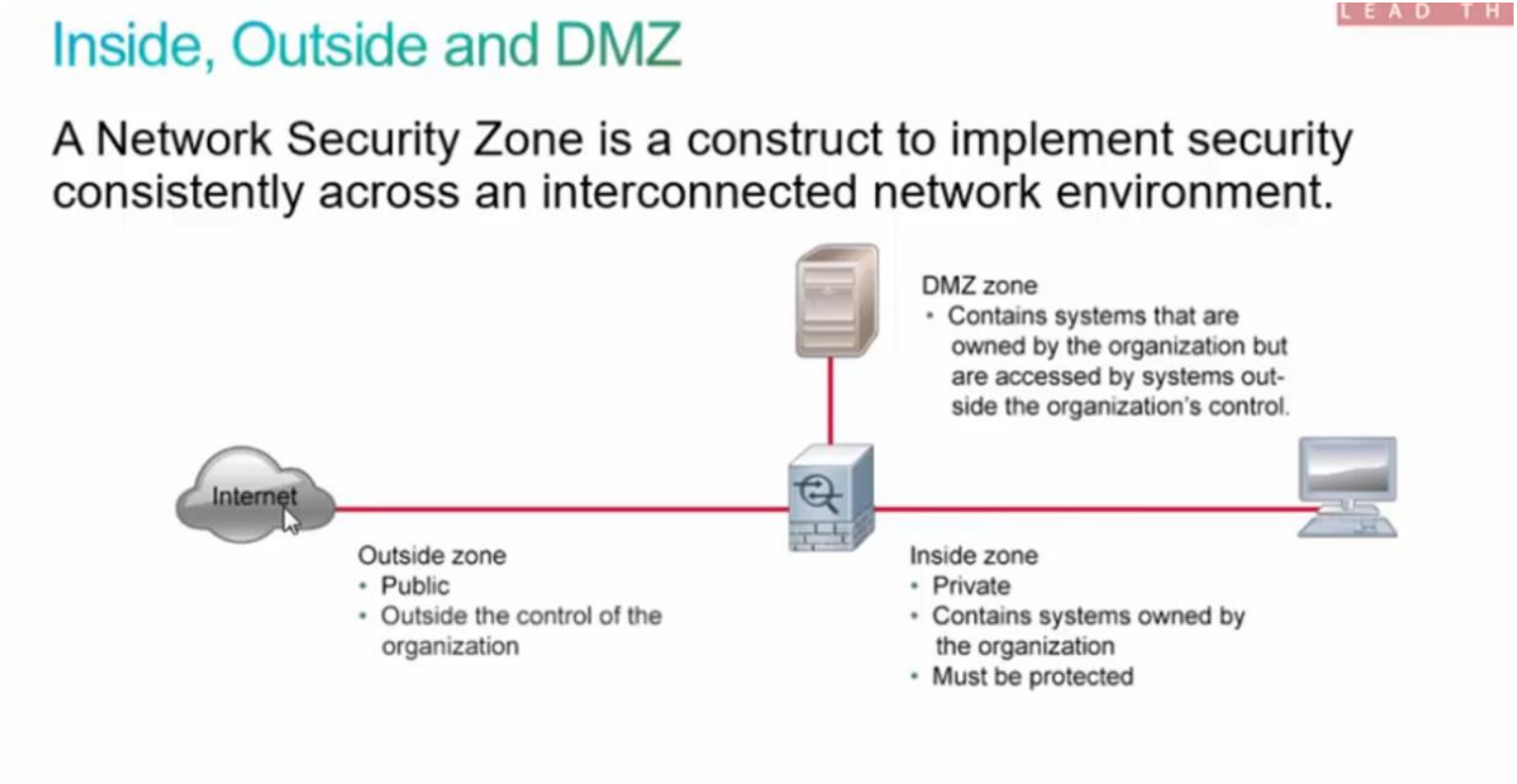
- Security training for end users
- Awareness training for groups with sensitive positions
- Technical security training for the IT staff
- Advanced information security training for security practitioners
- Specialized training for senior management

Proper Planning

Proper Implementation

Maintenance

Periodic Evaluation



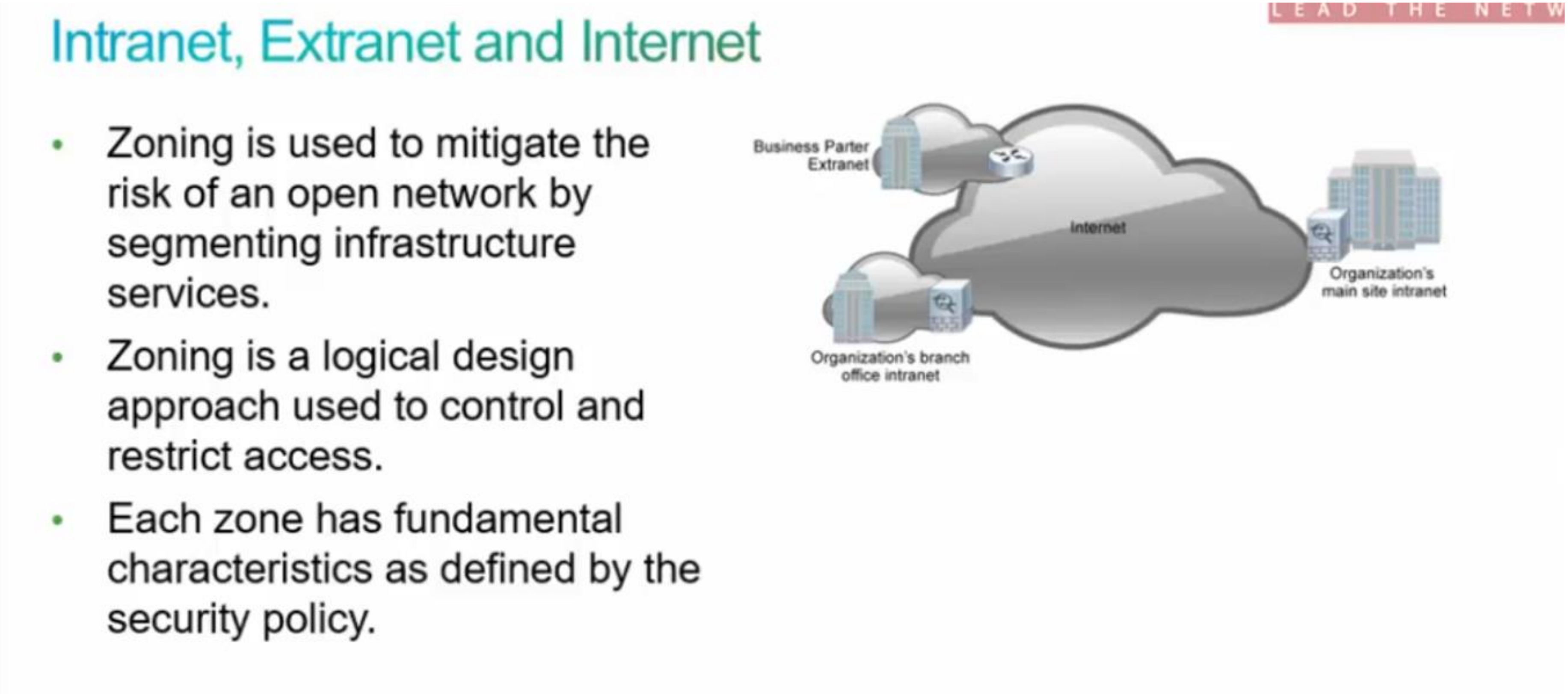
Inside, Outside and DMZ

A Network Security Zone is a construct to implement security consistently across an interconnected network environment.

DMZ zone
- Contains systems that are owned by the organization but are accessed by systems outside the organization's control.

Outside zone
- Public
- Outside the control of the organization

Inside zone
- Private
- Contains systems owned by the organization
- Must be protected

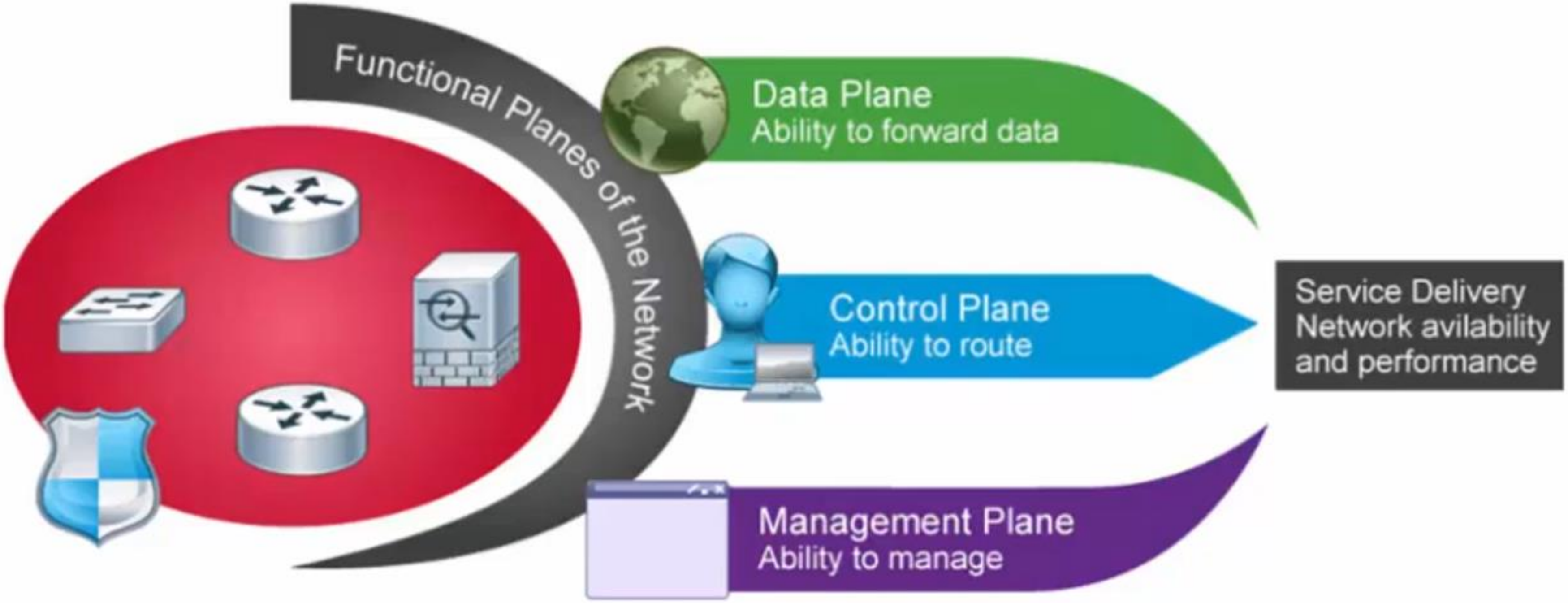


Intranet, Extranet and Internet

- Zoning is used to mitigate the risk of an open network by segmenting infrastructure services.
- Zoning is a logical design approach used to control and restrict access.
- Each zone has fundamental characteristics as defined by the security policy.

Business Parter Extranet
Internet
Organization's main site intranet
Organization's branch office intranet

The Functional Planes of the Network



Functional Planes of the Network

Data Plane
Ability to forward data

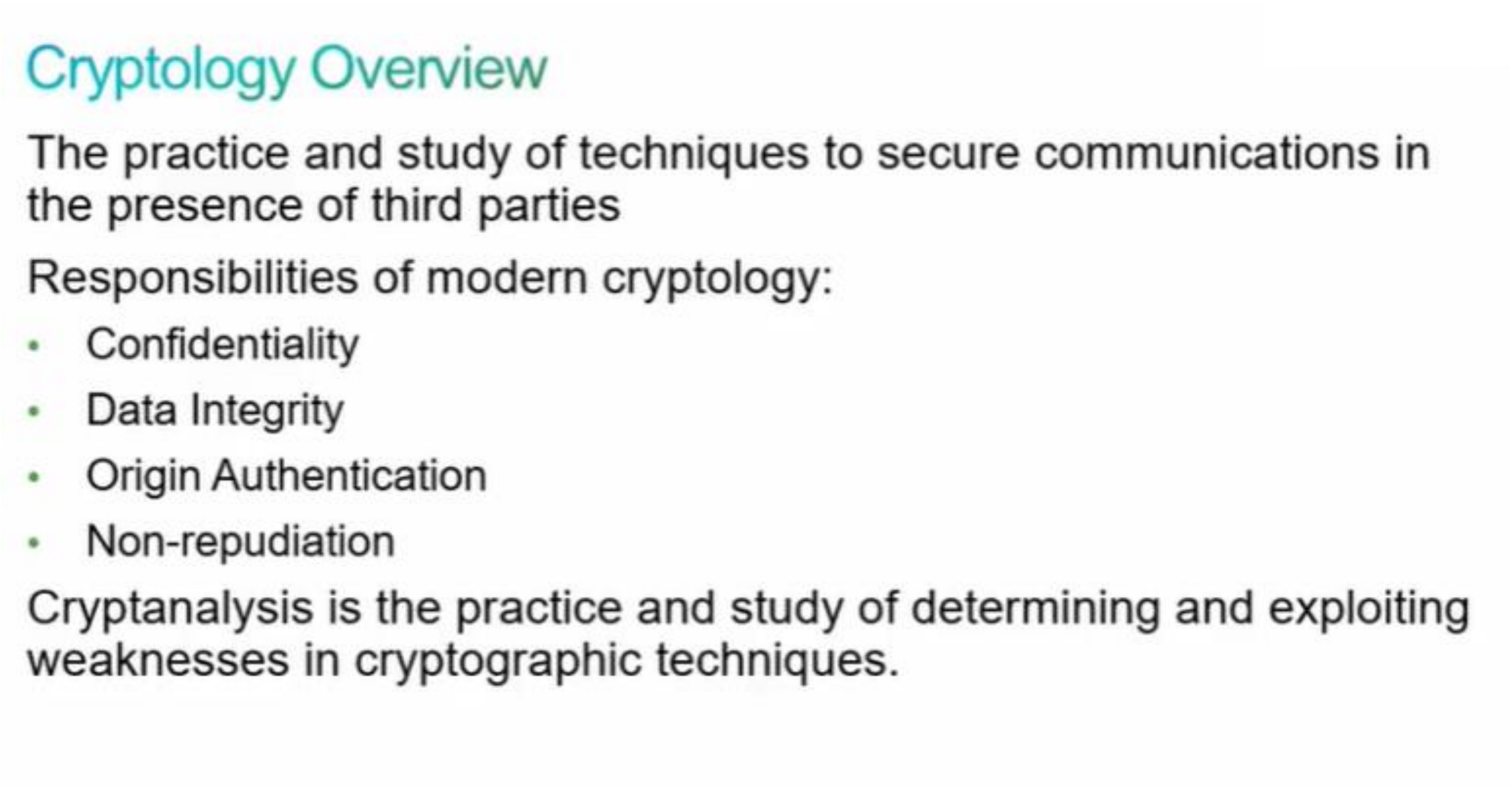
Control Plane
Ability to route

Management Plane
Ability to manage

Service Delivery
Network avilability
and performance

CRYPTOGRAPHIC TECHNOLOGIES

SECURITY CONCEPTS



Cryptology Overview

The practice and study of techniques to secure communications in the presence of third parties

Responsibilities of modern cryptology:

- Confidentiality
- Data Integrity
- Origin Authentication
- Non-repudiation

Cryptanalysis is the practice and study of determining and exploiting weaknesses in cryptographic techniques.

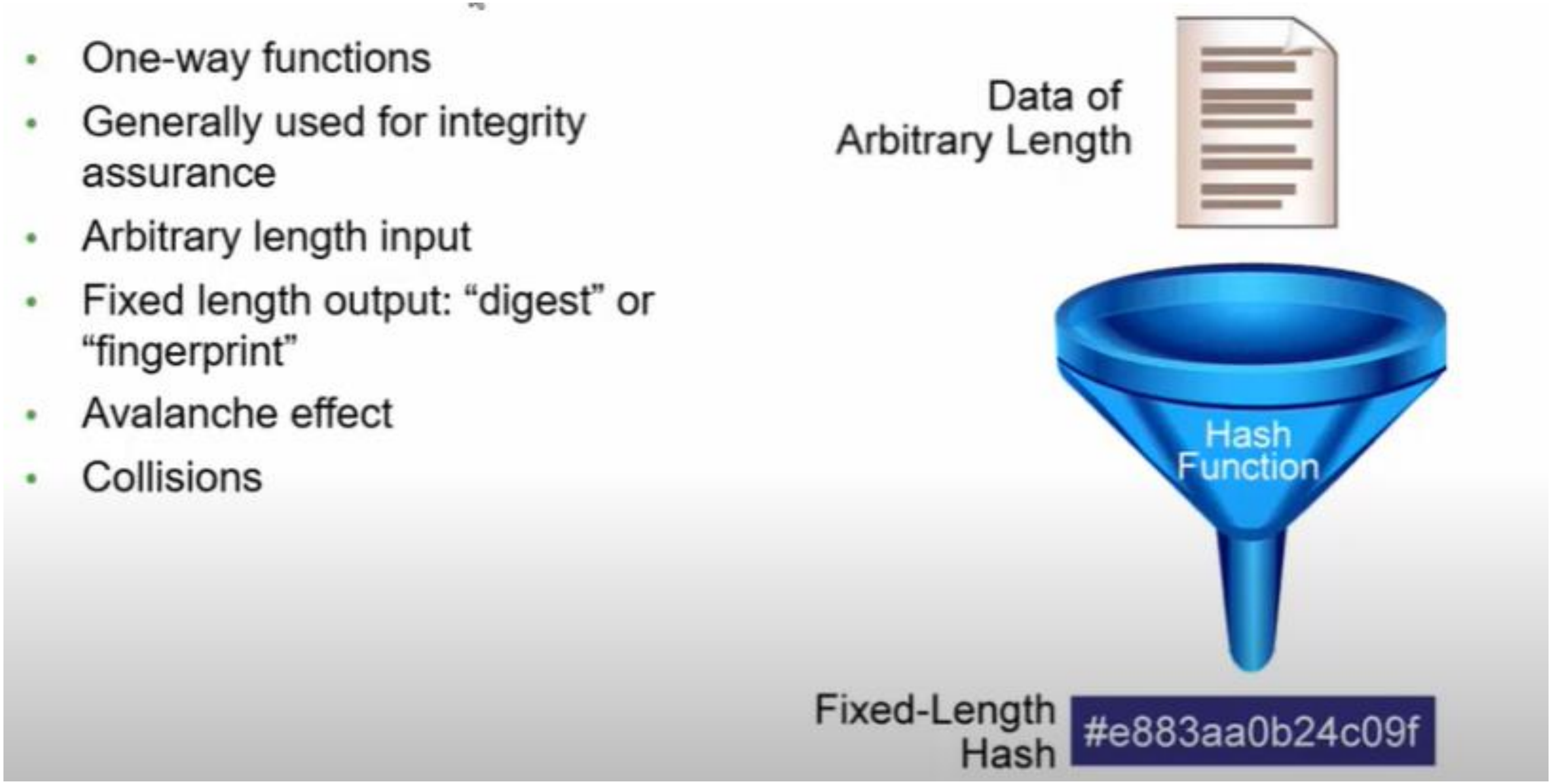
Cryptography History

- The history of cryptography can be traced back over 5000 years.
- Cryptography was first widely used in diplomatic and military circles.
- Julius Caesar used a substitution cipher to secure his military communications.
- Thomas Jefferson invented a simple 26-disk encryption system.
- Arthur Scherbius invented a machine in 1918 that was the precursor to the encryption machines used in World War II. He called it Enigma and sold it to Germany.

Jefferson Encryption Invention

Enigma

OVERVIEW OF CRYPTOGRAPHIC HASHES



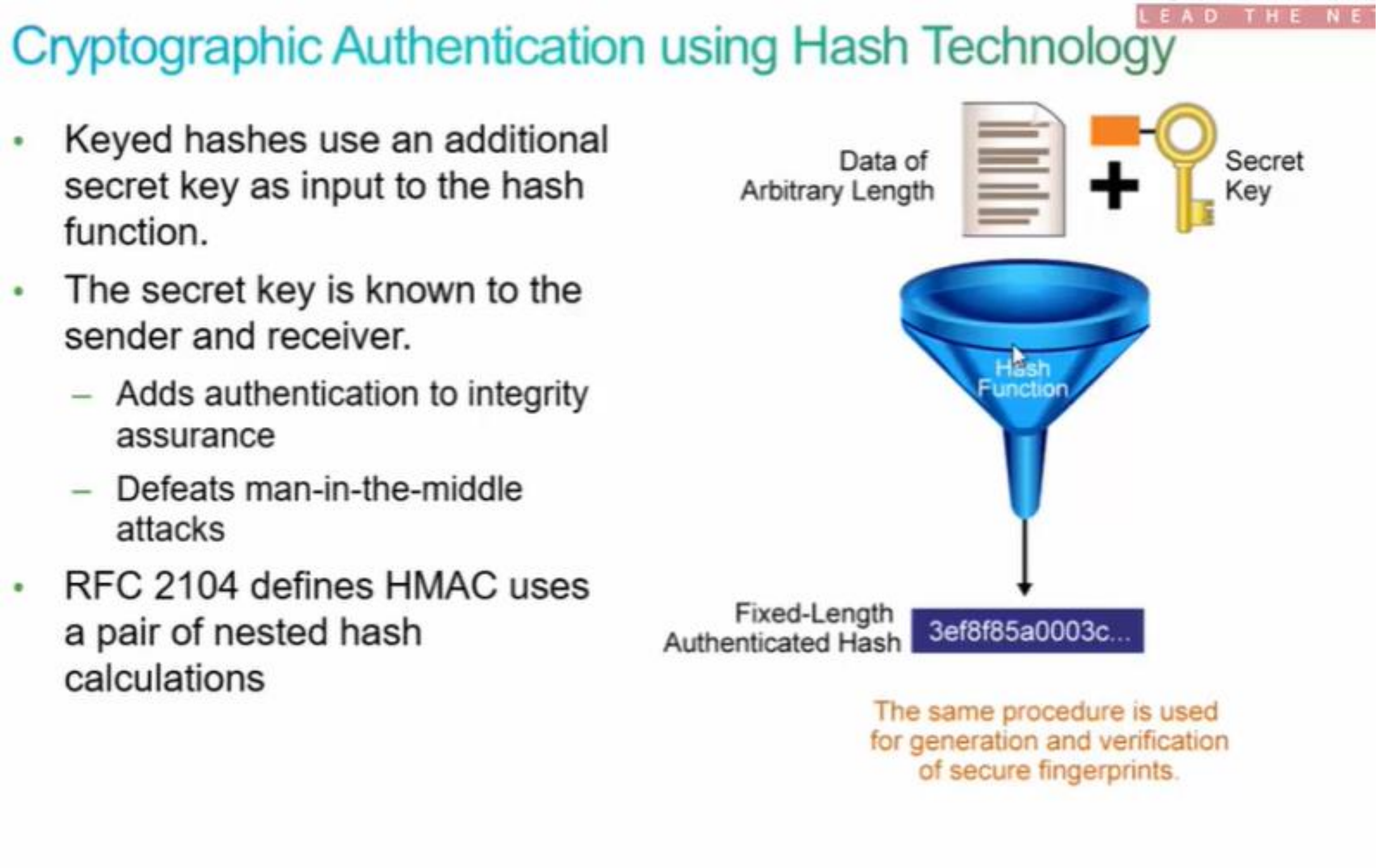
- One-way functions
- Generally used for integrity assurance
- Arbitrary length input
- Fixed length output: “digest” or “fingerprint”
- Avalanche effect
- Collisions

Data of
Arbitrary Length

Hash
Function

Fixed-Length
Hash

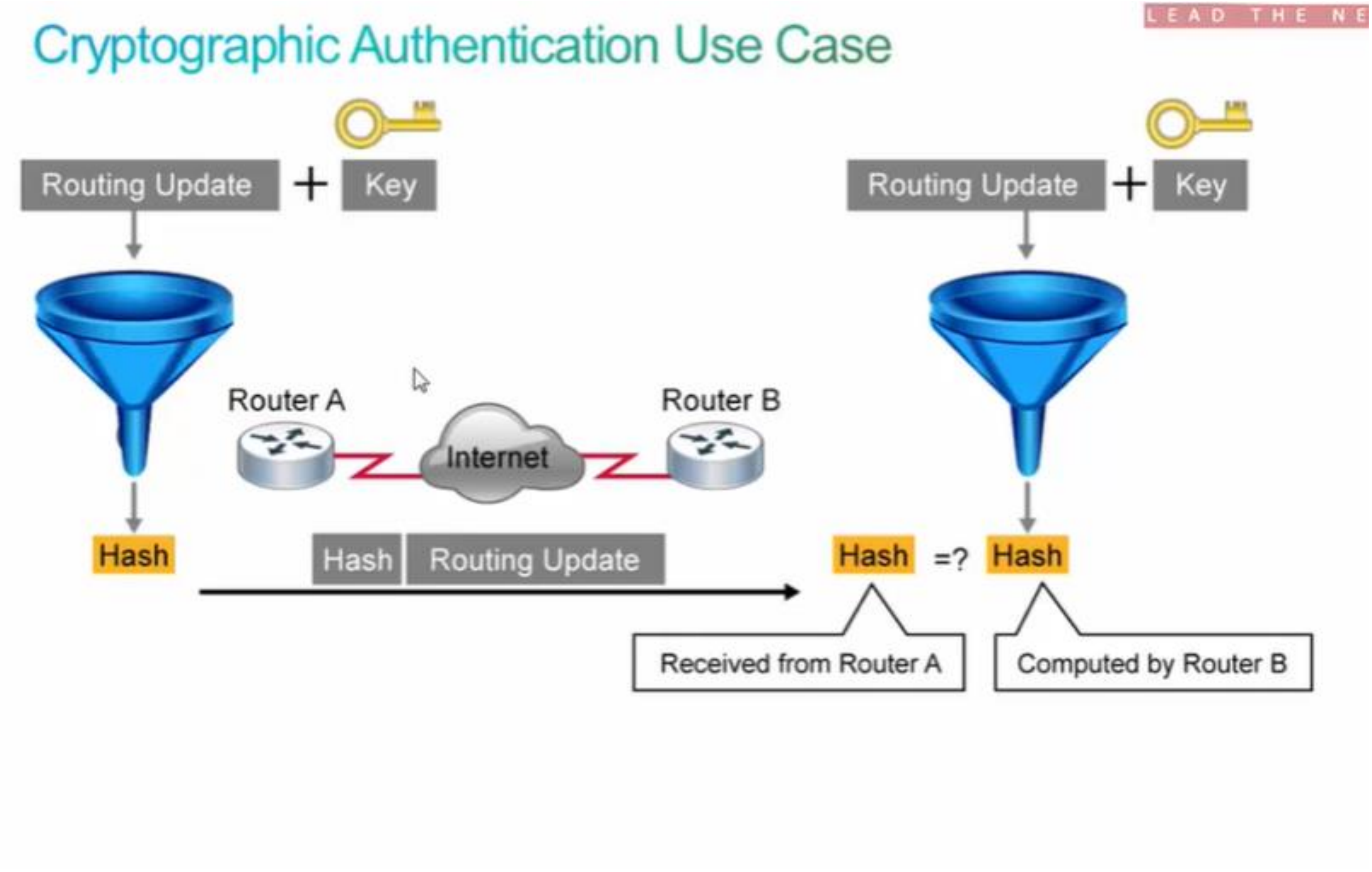
#e883aa0b24c09f



Cryptographic Authentication using Hash Technology

- Keyed hashes use an additional secret key as input to the hash function.
- The secret key is known to the sender and receiver.
  - Adds authentication to integrity assurance
  - Defeats man-in-the-middle attacks
- RFC 2104 defines HMAC uses a pair of nested hash calculations

The same procedure is used for generation and verification of secure fingerprints.



Cryptographic Authentication Use Case

Routing Update + Key

Router A

Internet

Router B

Routing Update + Key

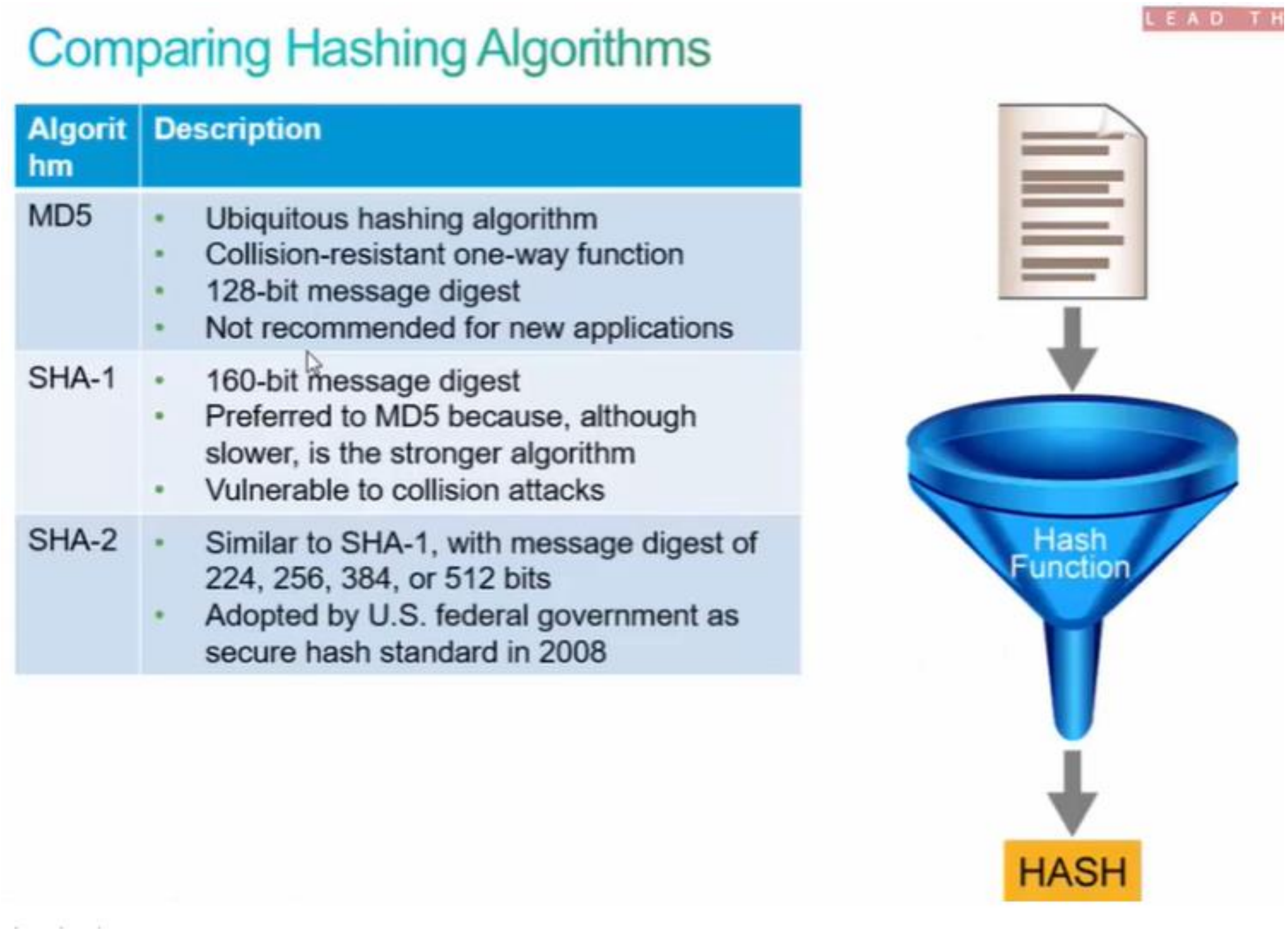
Hash

Hash | Routing Update

Hash =? Hash

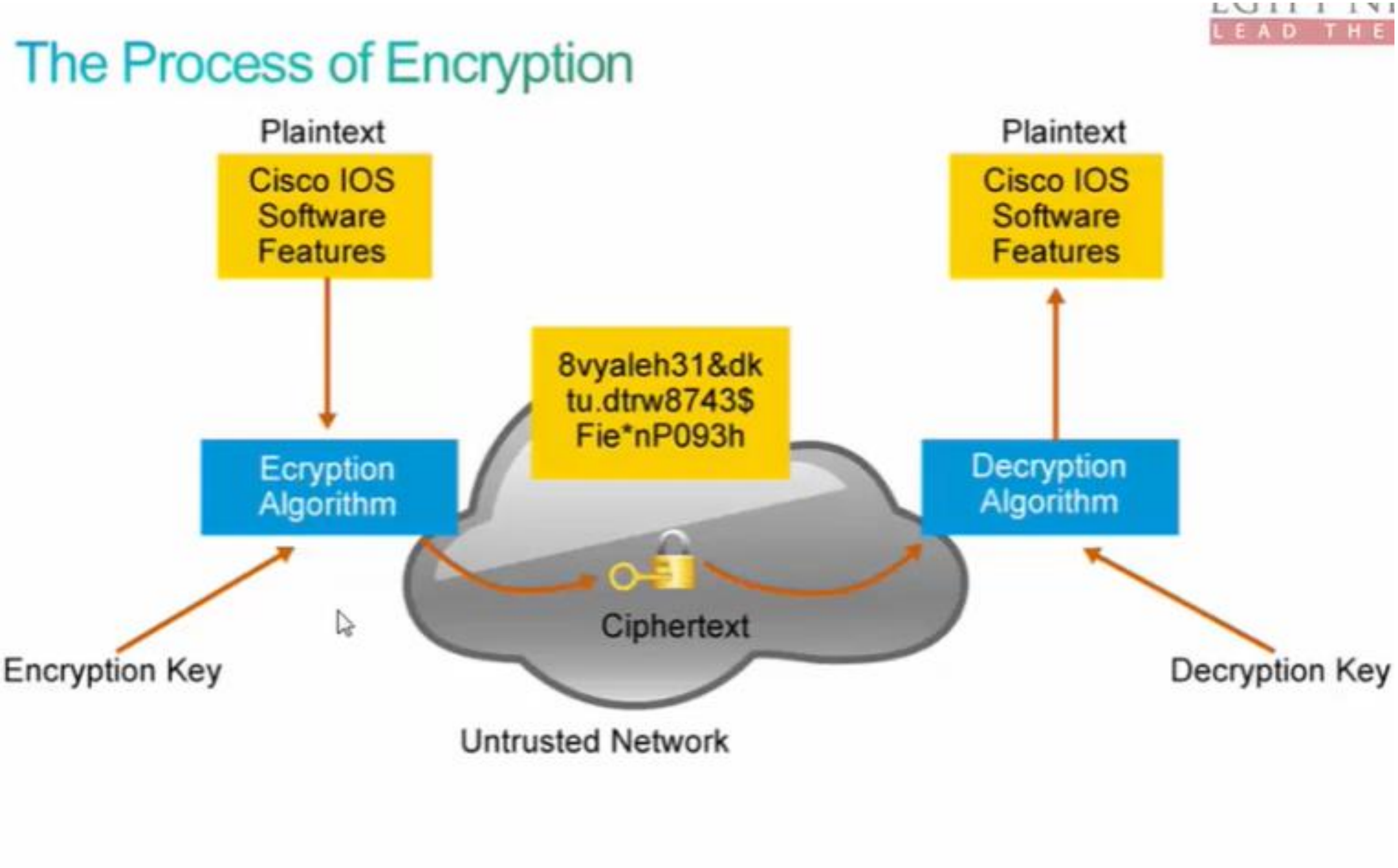
Received from Router A

Computed by Router B



Comparing Hashing Algorithms

Algorit hm	Description
MD5	- Ubiquitous hashing algorithm - Collision-resistant one-way function - 128-bit message digest - Not recommended for new applications
SHA-1	- 160-bit message digest - Preferred to MD5 because, although slower, is the stronger algorithm - Vulnerable to collision attacks
SHA-2	- Similar to SHA-1, with message digest of 224, 256, 384, or 512 bits - Adopted by U.S. federal government as secure hash standard in 2008



The Process of Encryption

Plaintext

Cisco IOS Software Features

Ecryption Algorithm

Encryption Key

8vyaleh31&dk tu.dtrw8743$ Fie*nP093h

Ciphertext

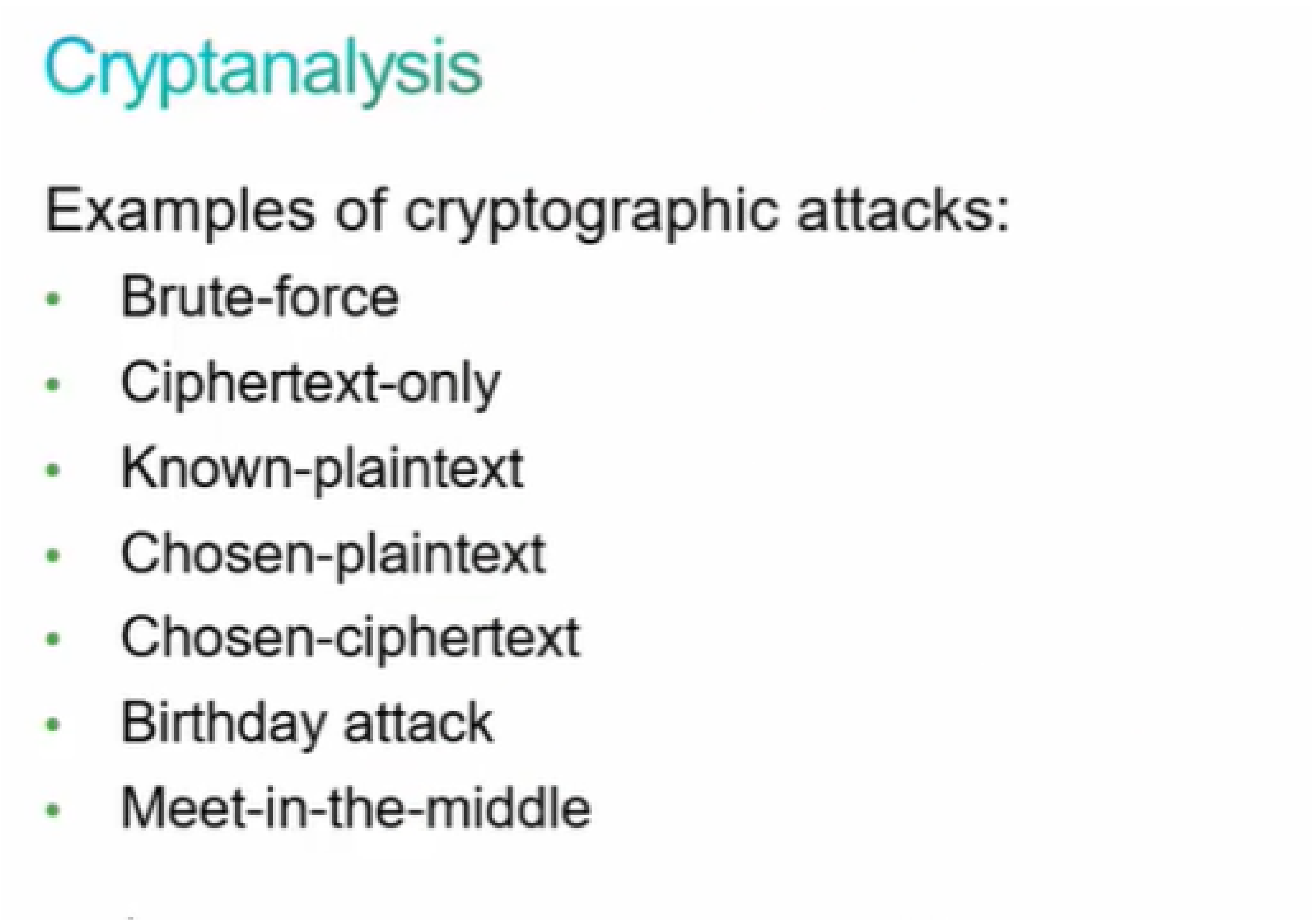
Untrusted Network

Decryption Algorithm

Decryption Key

Plaintext

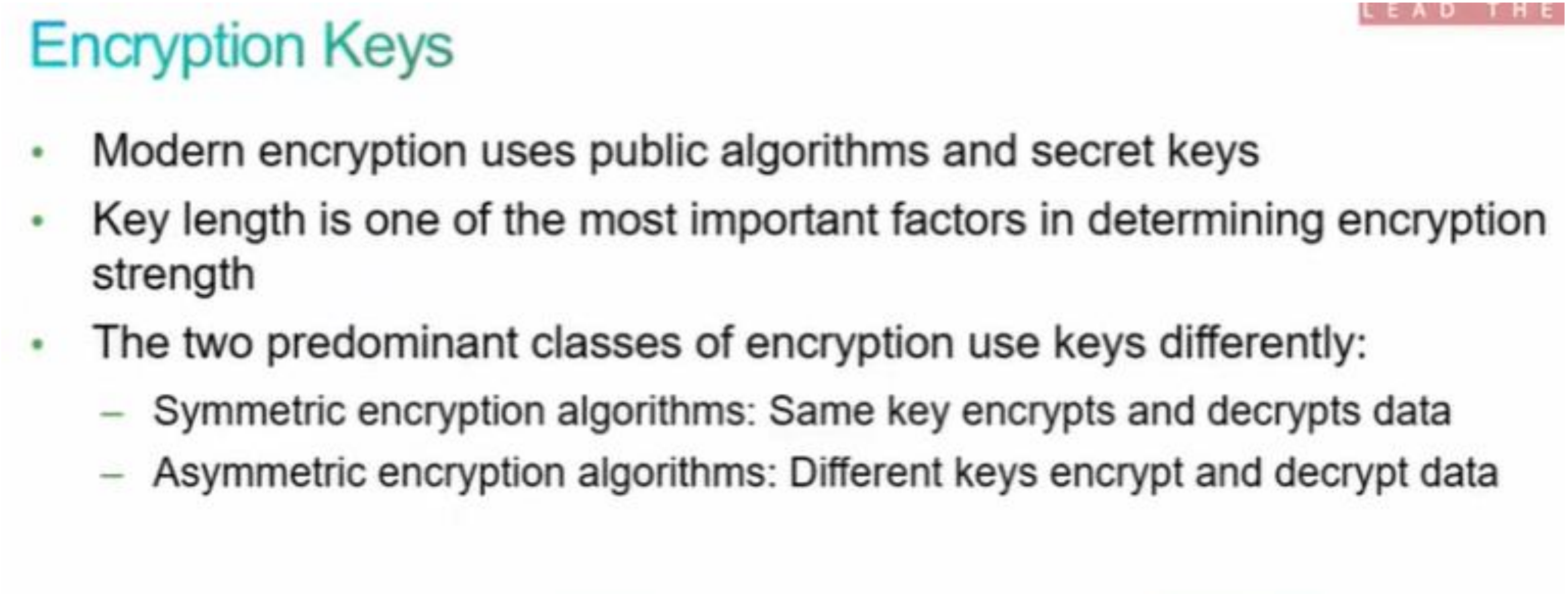
Cisco IOS Software Features



Cryptanalysis

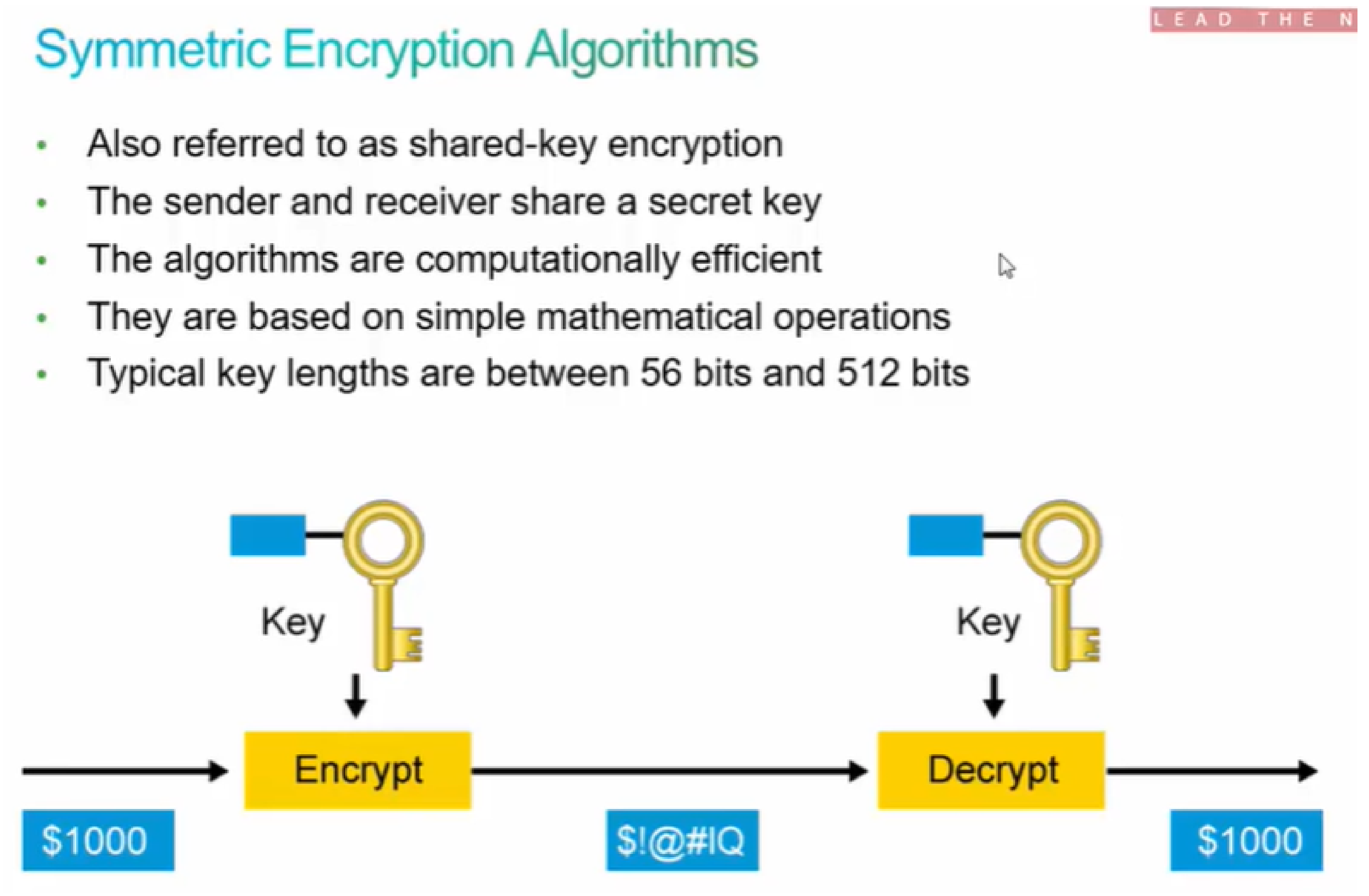
Examples of cryptographic attacks:

- Brute-force
- Ciphertext-only
- Known-plaintext
- Chosen-plaintext
- Chosen-ciphertext
- Birthday attack
- Meet-in-the-middle



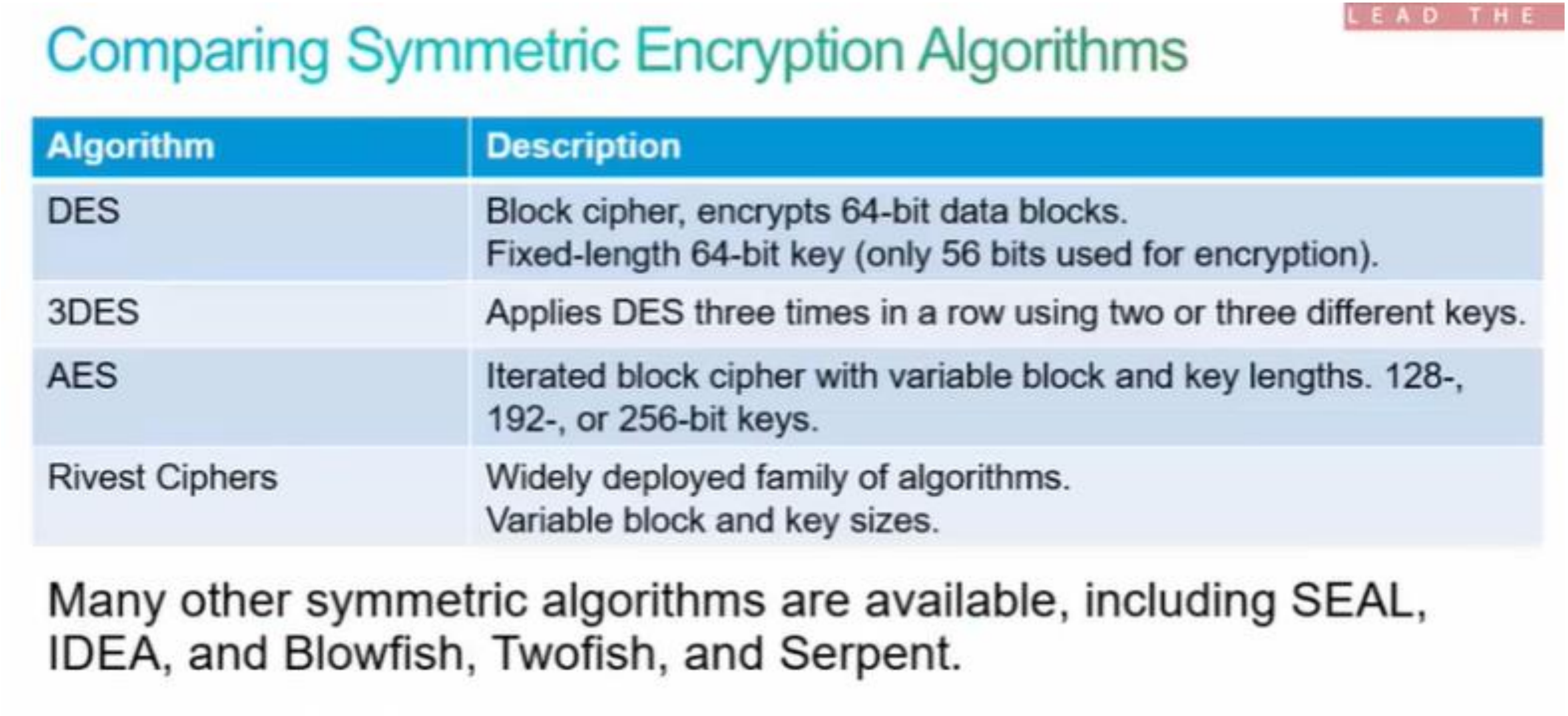
Encryption Keys

- Modern encryption uses public algorithms and secret keys
- Key length is one of the most important factors in determining encryption strength
- The two predominant classes of encryption use keys differently:
  - Symmetric encryption algorithms: Same key encrypts and decrypts data
  - Asymmetric encryption algorithms: Different keys encrypt and decrypt data



Symmetric Encryption Algorithms

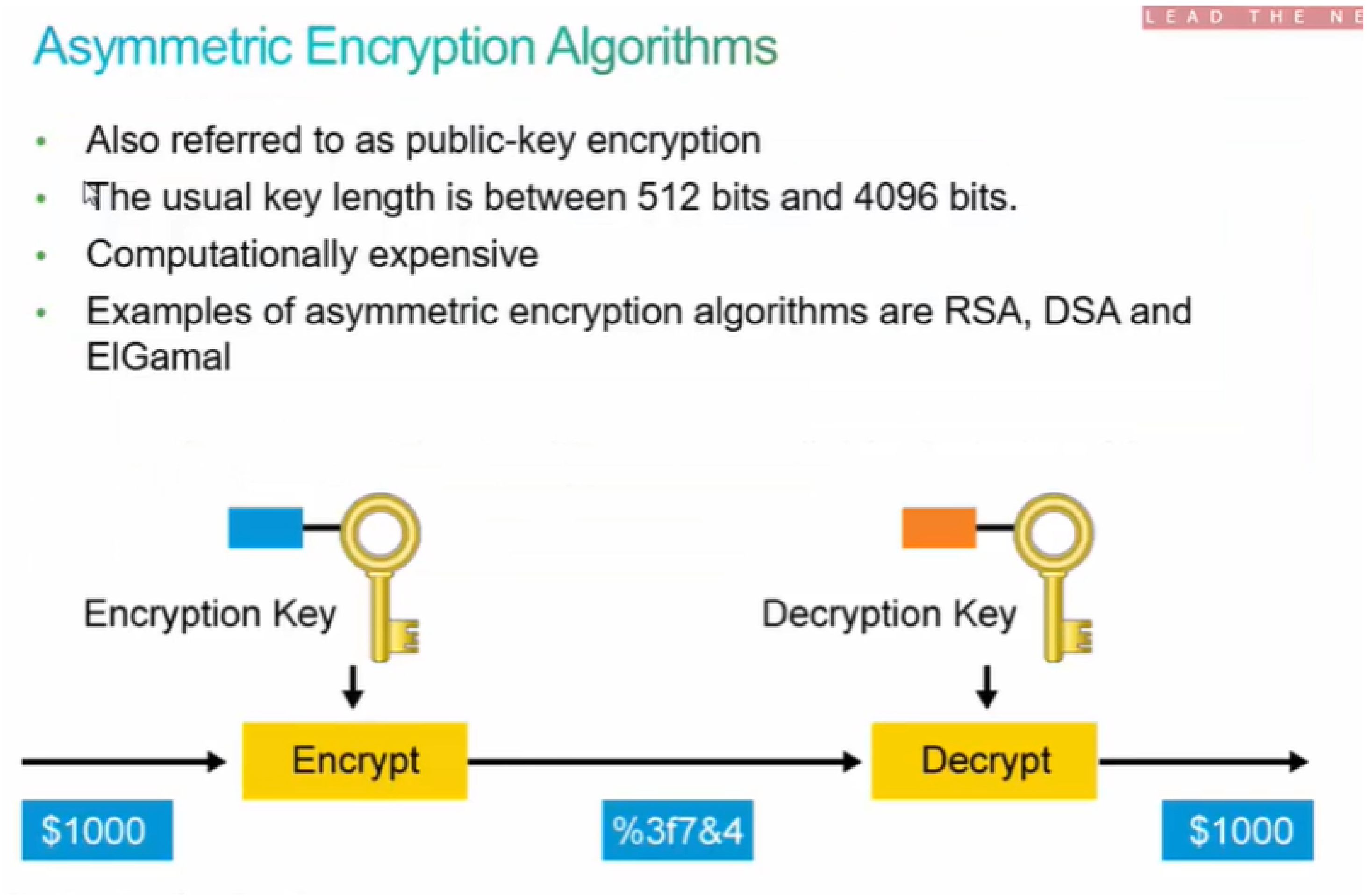
- Also referred to as shared-key encryption
- The sender and receiver share a secret key
- The algorithms are computationally efficient
- They are based on simple mathematical operations
- Typical key lengths are between 56 bits and 512 bits



Comparing Symmetric Encryption Algorithms

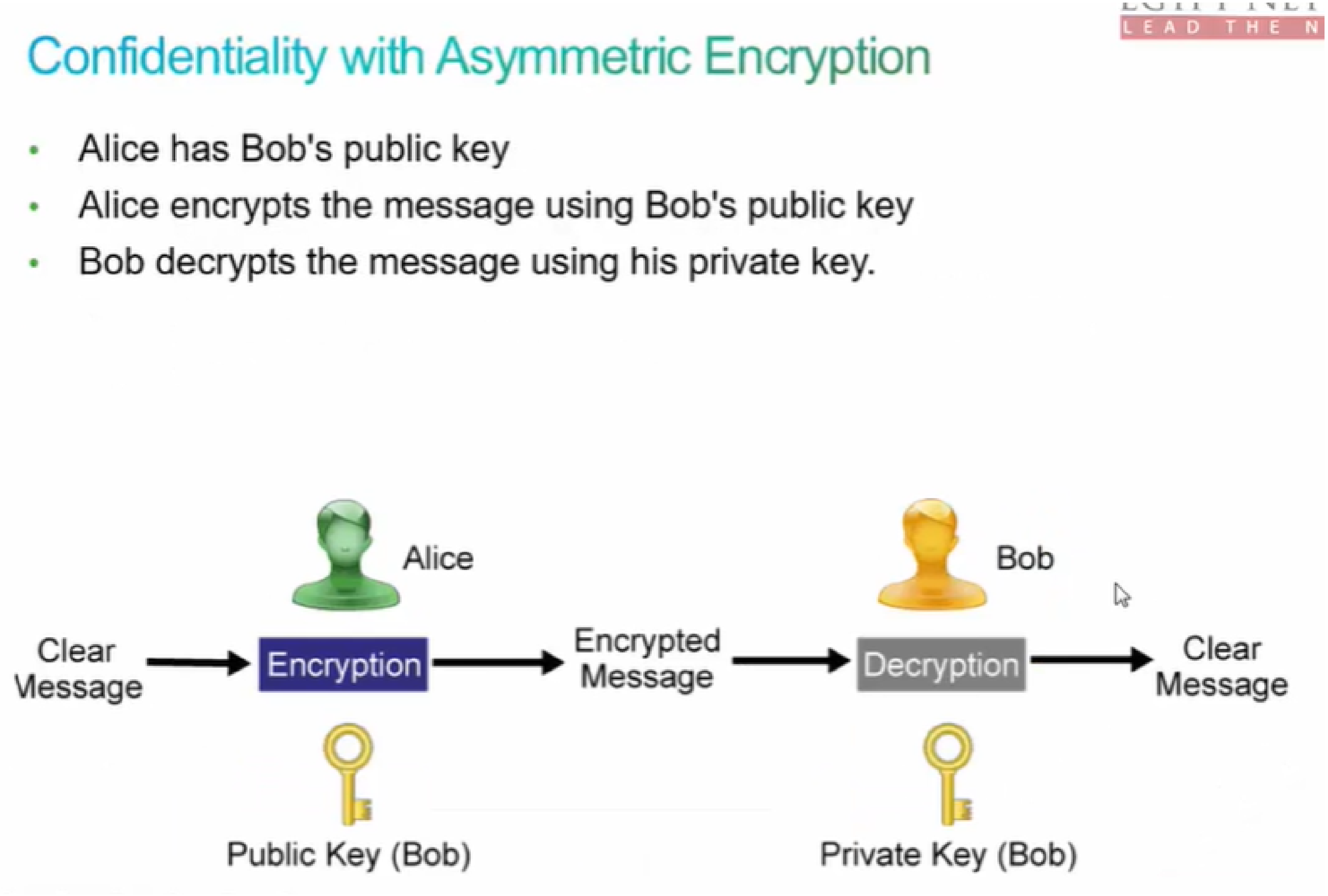
Algorithm	Description
DES	Block cipher, encrypts 64-bit data blocks. Fixed-length 64-bit key (only 56 bits used for encryption).
3DES	Applies DES three times in a row using two or three different keys.
AES	Iterated block cipher with variable block and key lengths. 128-, 192-, or 256-bit keys.
Rivest Ciphers	Widely deployed family of algorithms. Variable block and key sizes.

Many other symmetric algorithms are available, including SEAL, IDEA, and Blowfish, Twofish, and Serpent.



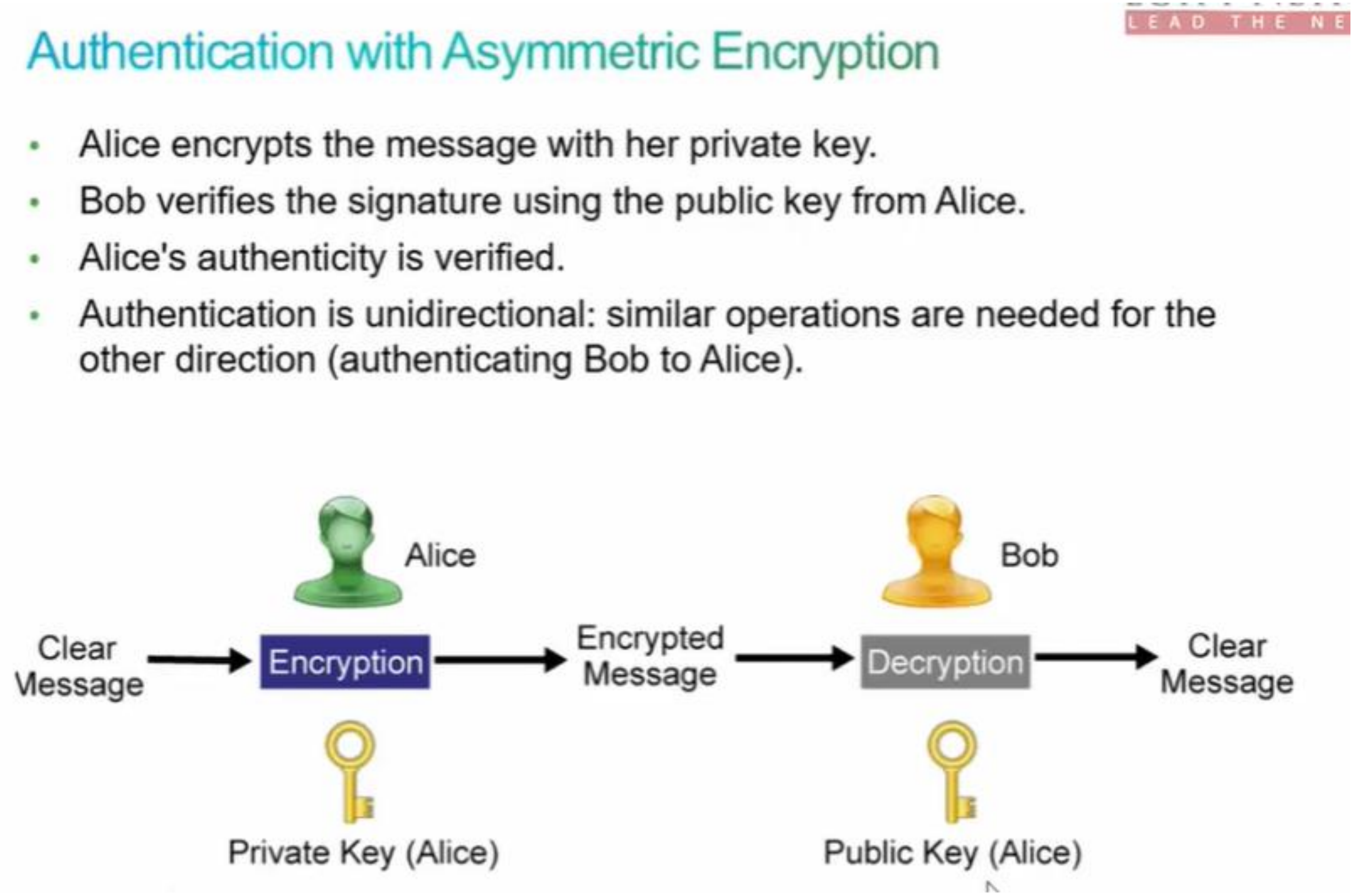
Asymmetric Encryption Algorithms

- Also referred to as public-key encryption
- The usual key length is between 512 bits and 4096 bits.
- Computationally expensive
- Examples of asymmetric encryption algorithms are RSA, DSA and ElGamal



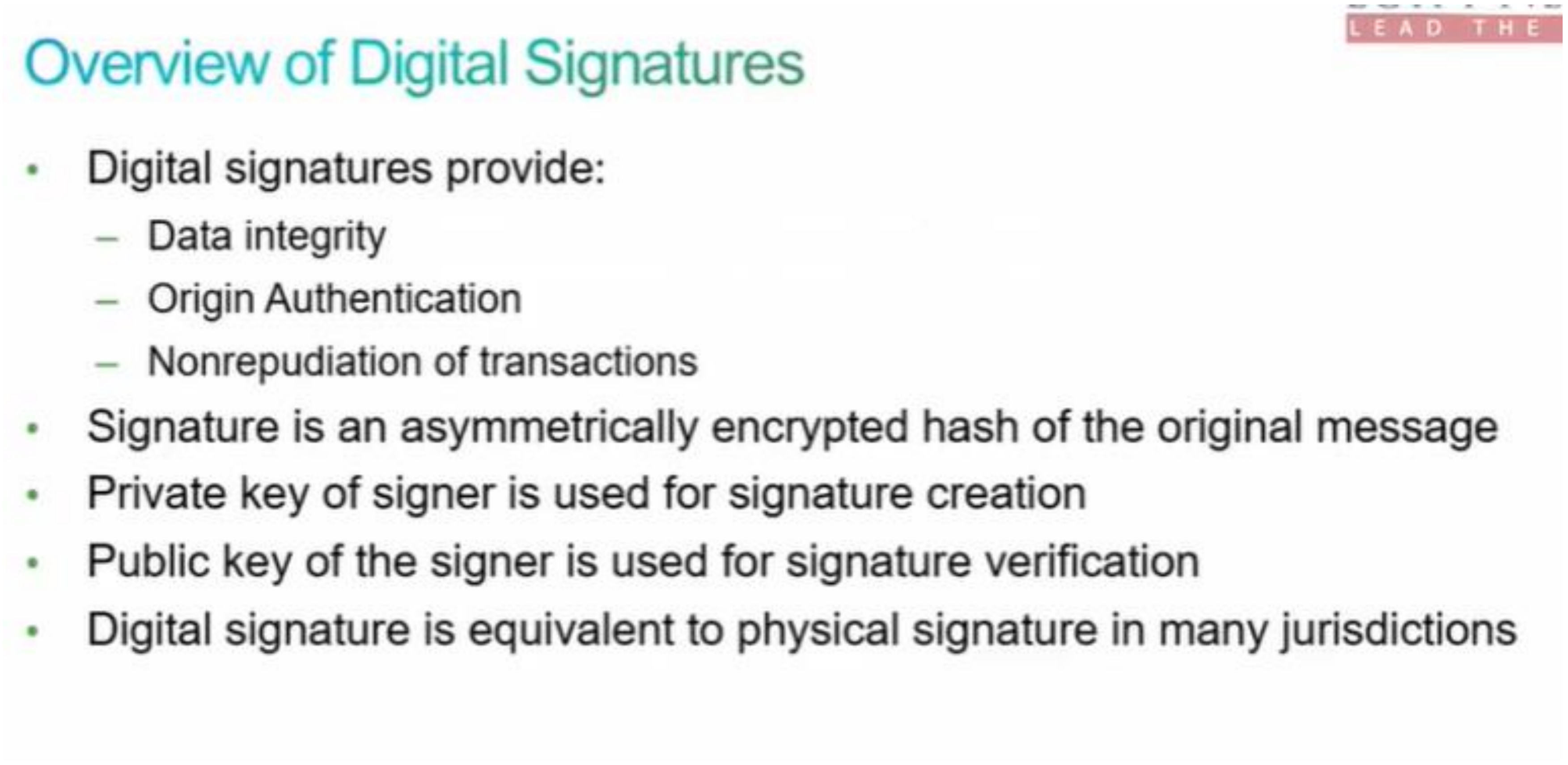
Confidentiality with Asymmetric Encryption

- Alice has Bob's public key
- Alice encrypts the message using Bob's public key
- Bob decrypts the message using his private key.



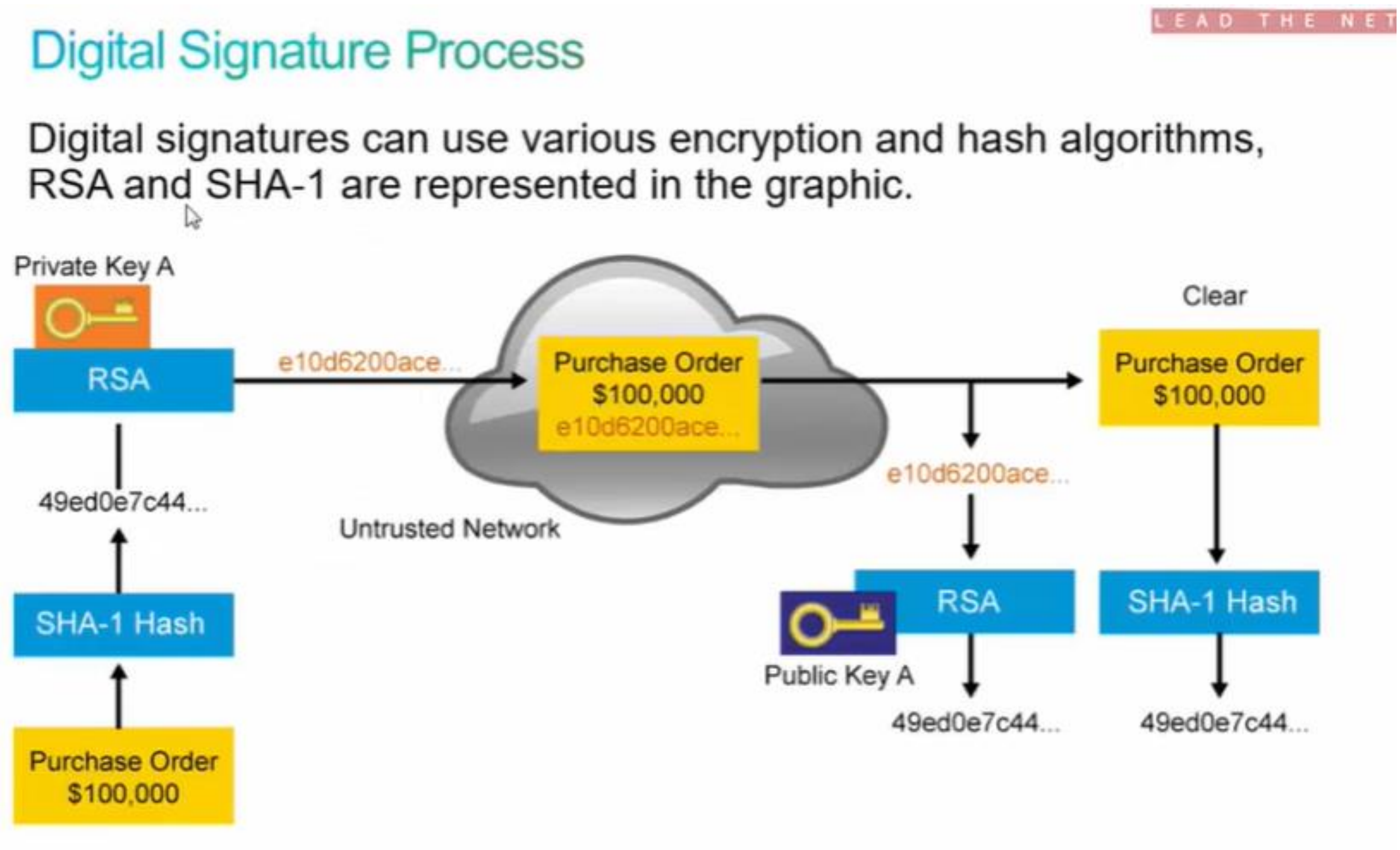
Authentication with Asymmetric Encryption

- Alice encrypts the message with her private key.
- Bob verifies the signature using the public key from Alice.
- Alice's authenticity is verified.
- Authentication is unidirectional: similar operations are needed for the other direction (authenticating Bob to Alice).



Overview of Digital Signatures

- Digital signatures provide:
  - Data integrity
  - Origin Authentication
  - Nonrepudiation of transactions
- Signature is an asymmetrically encrypted hash of the original message
- Private key of signer is used for signature creation
- Public key of the signer is used for signature verification
- Digital signature is equivalent to physical signature in many jurisdictions



Digital Signature Process

Digital signatures can use various encryption and hash algorithms, RSA and SHA-1 are represented in the graphic.

Private Key A

RSA

e10d6200ace...

49ed0e7c44...

SHA-1 Hash

Purchase Order
$100,000

Purchase Order
$100,000
e10d6200ace...

Untrusted Network

Clear

Purchase Order
$100,000

e10d6200ace...

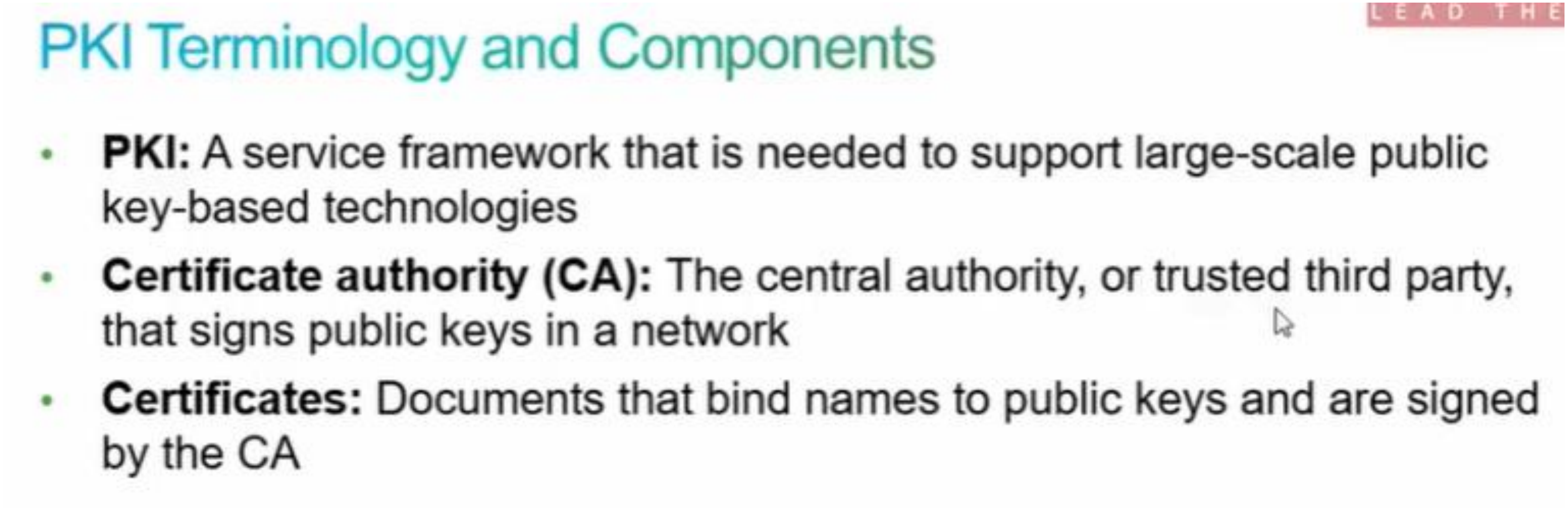
RSA

Public Key A

49ed0e7c44...

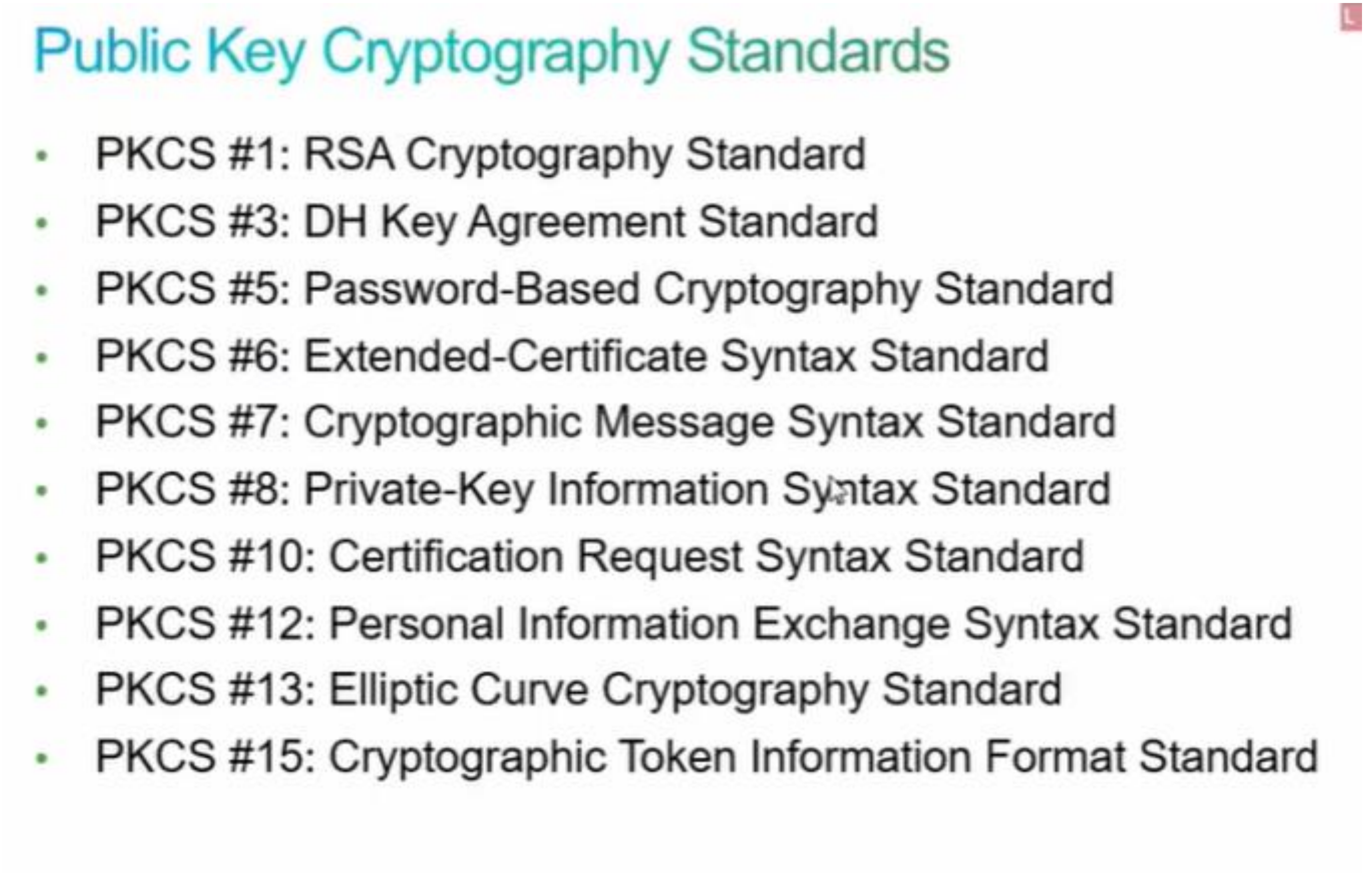
SHA-1 Hash

49ed0e7c44...



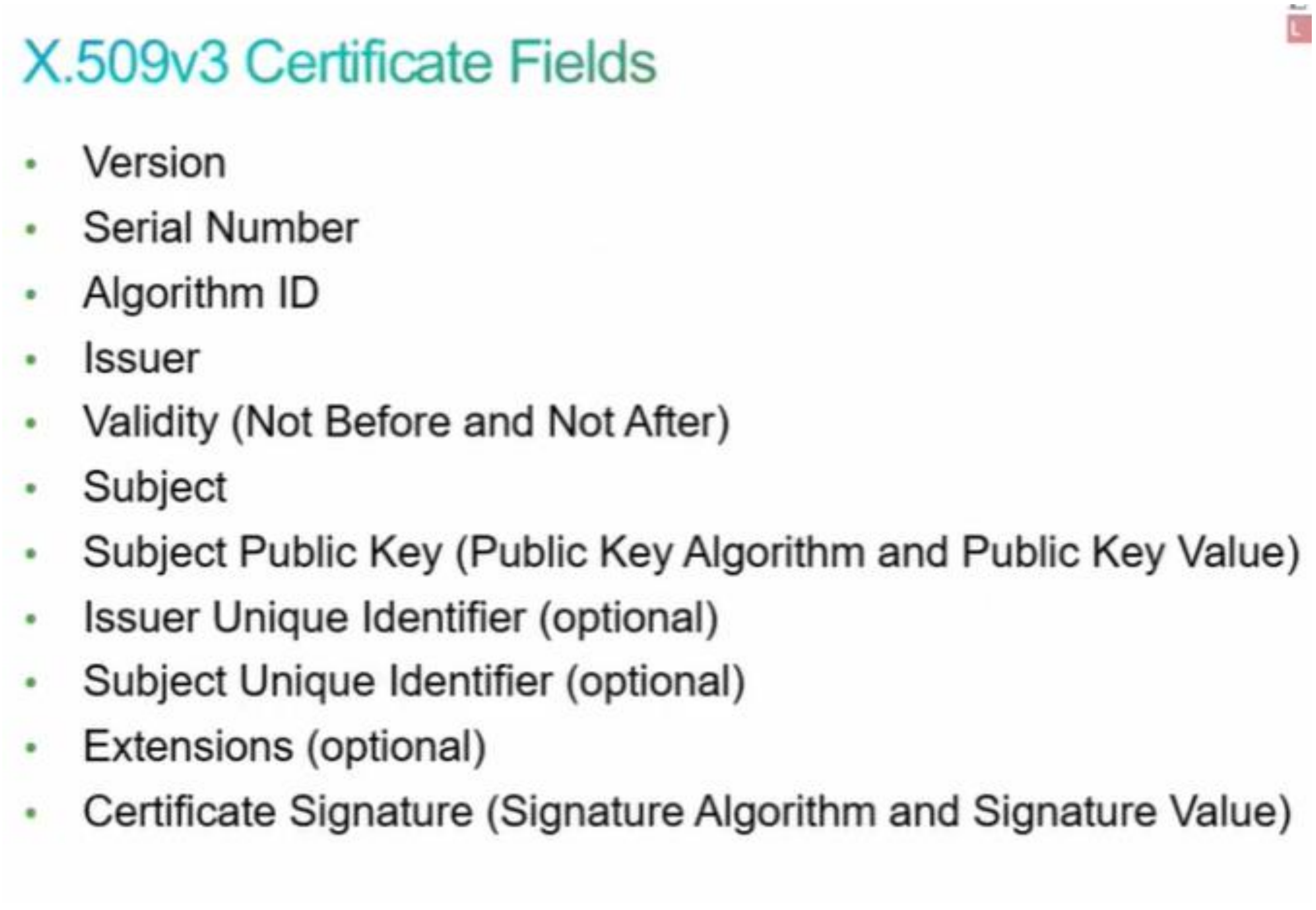
PKI Terminology and Components

- **PKI:** A service framework that is needed to support large-scale public key-based technologies
- **Certificate authority (CA):** The central authority, or trusted third party, that signs public keys in a network
- **Certificates:** Documents that bind names to public keys and are signed by the CA



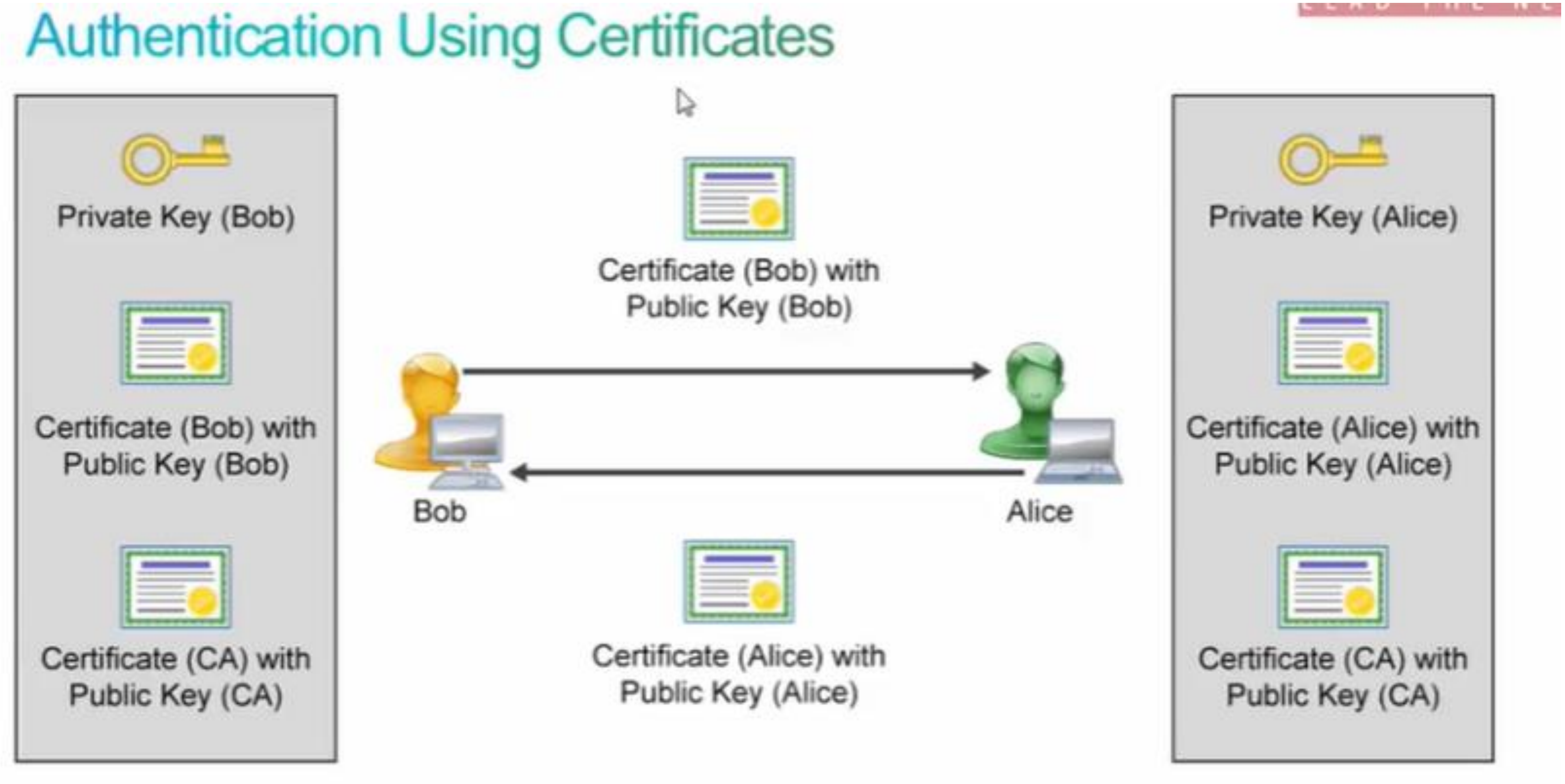
Public Key Cryptography Standards

- PKCS #1: RSA Cryptography Standard
- PKCS #3: DH Key Agreement Standard
- PKCS #5: Password-Based Cryptography Standard
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #10: Certification Request Syntax Standard
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #15: Cryptographic Token Information Format Standard



X.509v3 Certificate Fields

- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity (Not Before and Not After)
- Subject
- Subject Public Key (Public Key Algorithm and Public Key Value)
- Issuer Unique Identifier (optional)
- Subject Unique Identifier (optional)
- Extensions (optional)
- Certificate Signature (Signature Algorithm and Signature Value)



Authentication Using Certificates

Private Key (Bob)

Certificate (Bob) with Public Key (Bob)

Certificate (CA) with Public Key (CA)

Certificate (Bob) with Public Key (Bob)

Bob

Alice

Certificate (Alice) with Public Key (Alice)

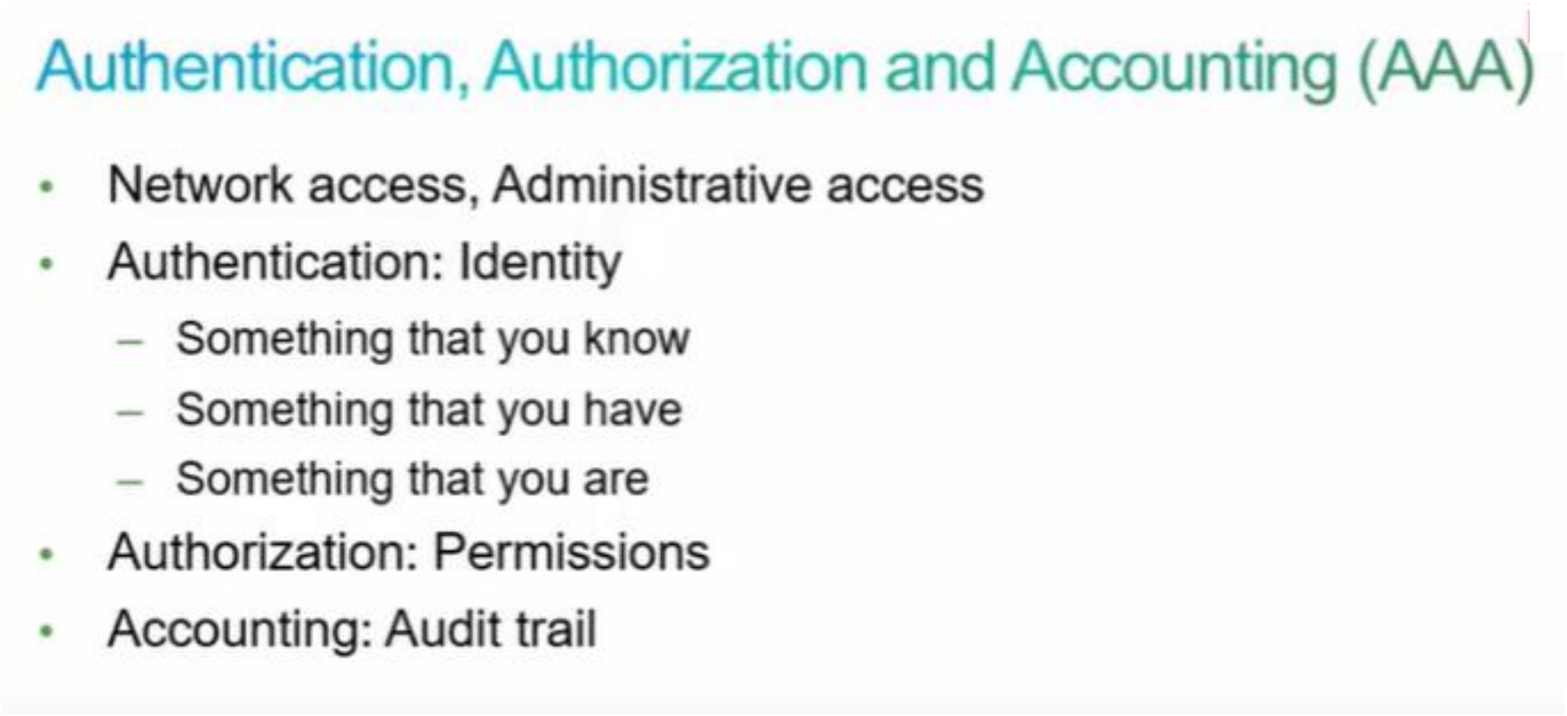
Private Key (Alice)

Certificate (Alice) with Public Key (Alice)

Certificate (CA) with Public Key (CA)

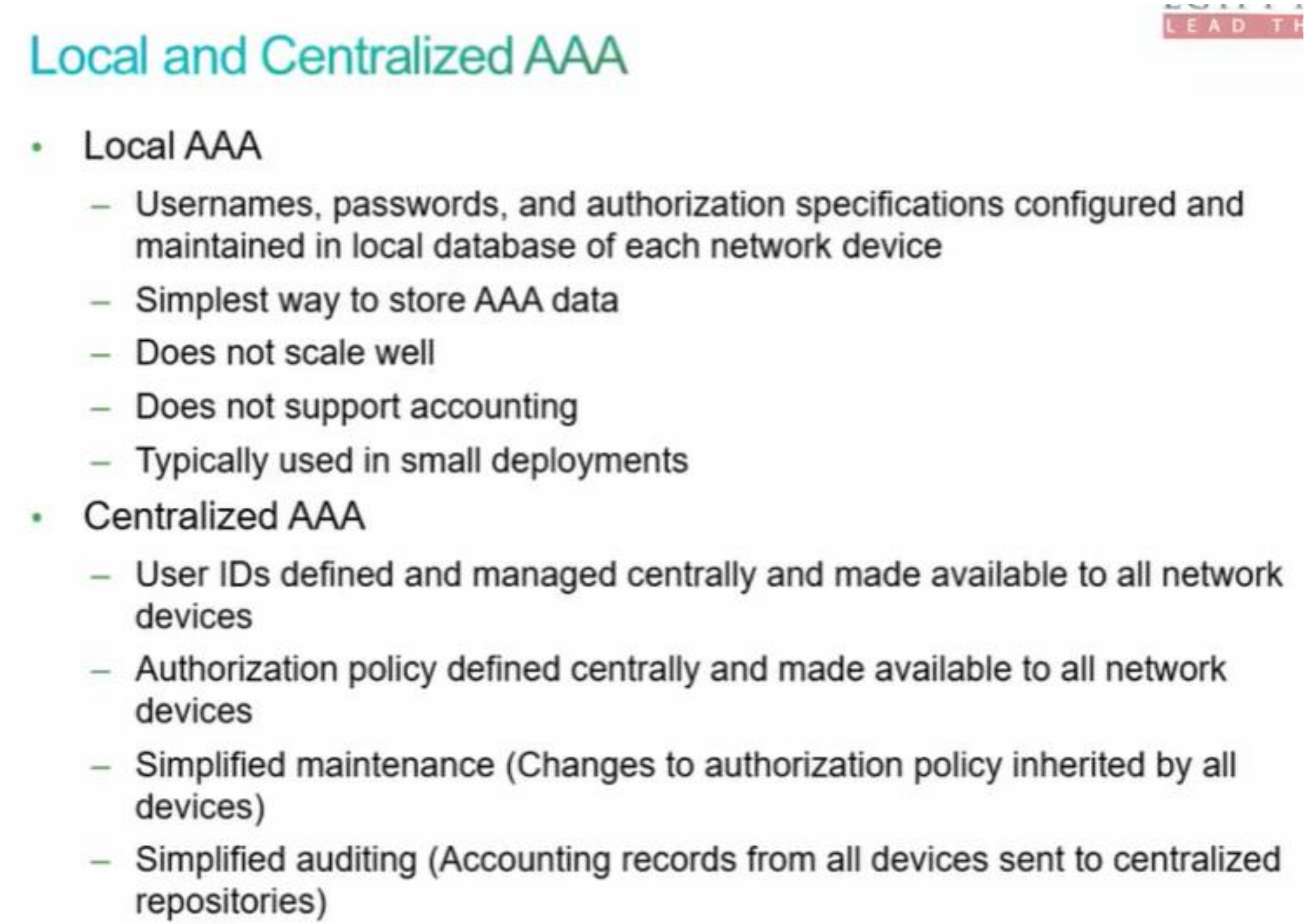
AAA

SECURE NETWORK DEVICES



Authentication, Authorization and Accounting (AAA)

- Network access, Administrative access
- Authentication: Identity
  - Something that you know
  - Something that you have
  - Something that you are
- Authorization: Permissions
- Accounting: Audit trail

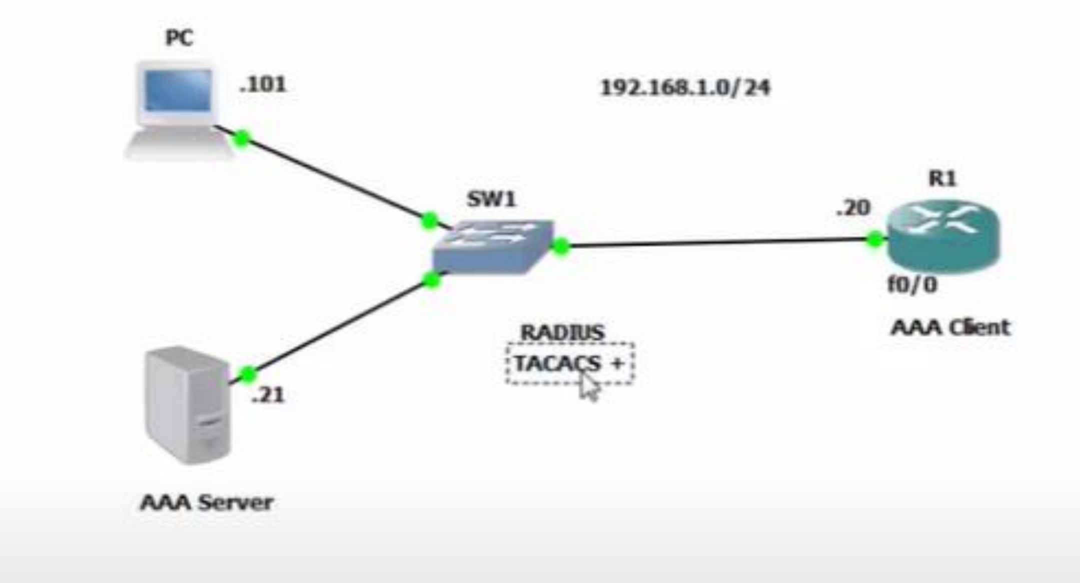


Local and Centralized AAA

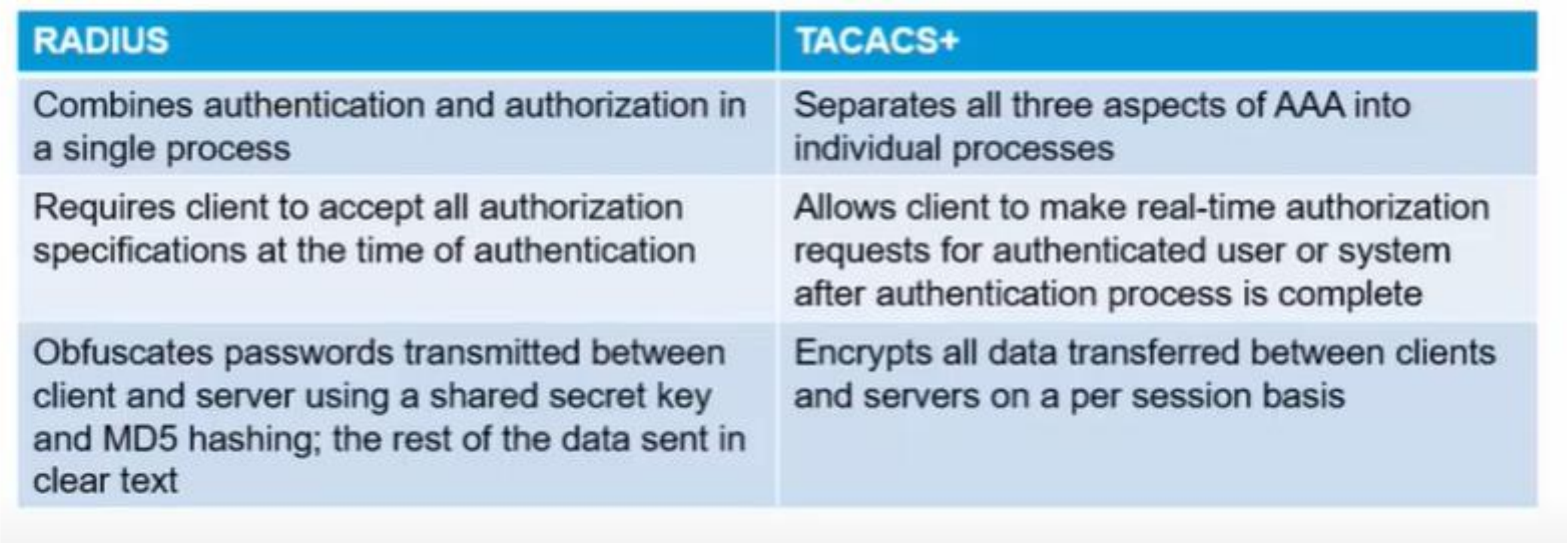
- Local AAA
  - Usernames, passwords, and authorization specifications configured and maintained in local database of each network device
  - Simplest way to store AAA data
  - Does not scale well
  - Does not support accounting
  - Typically used in small deployments
- Centralized AAA
  - User IDs defined and managed centrally and made available to all network devices
  - Authorization policy defined centrally and made available to all network devices
  - Simplified maintenance (Changes to authorization policy inherited by all devices)
  - Simplified auditing (Accounting records from all devices sent to centralized repositories)

AAA Protocols

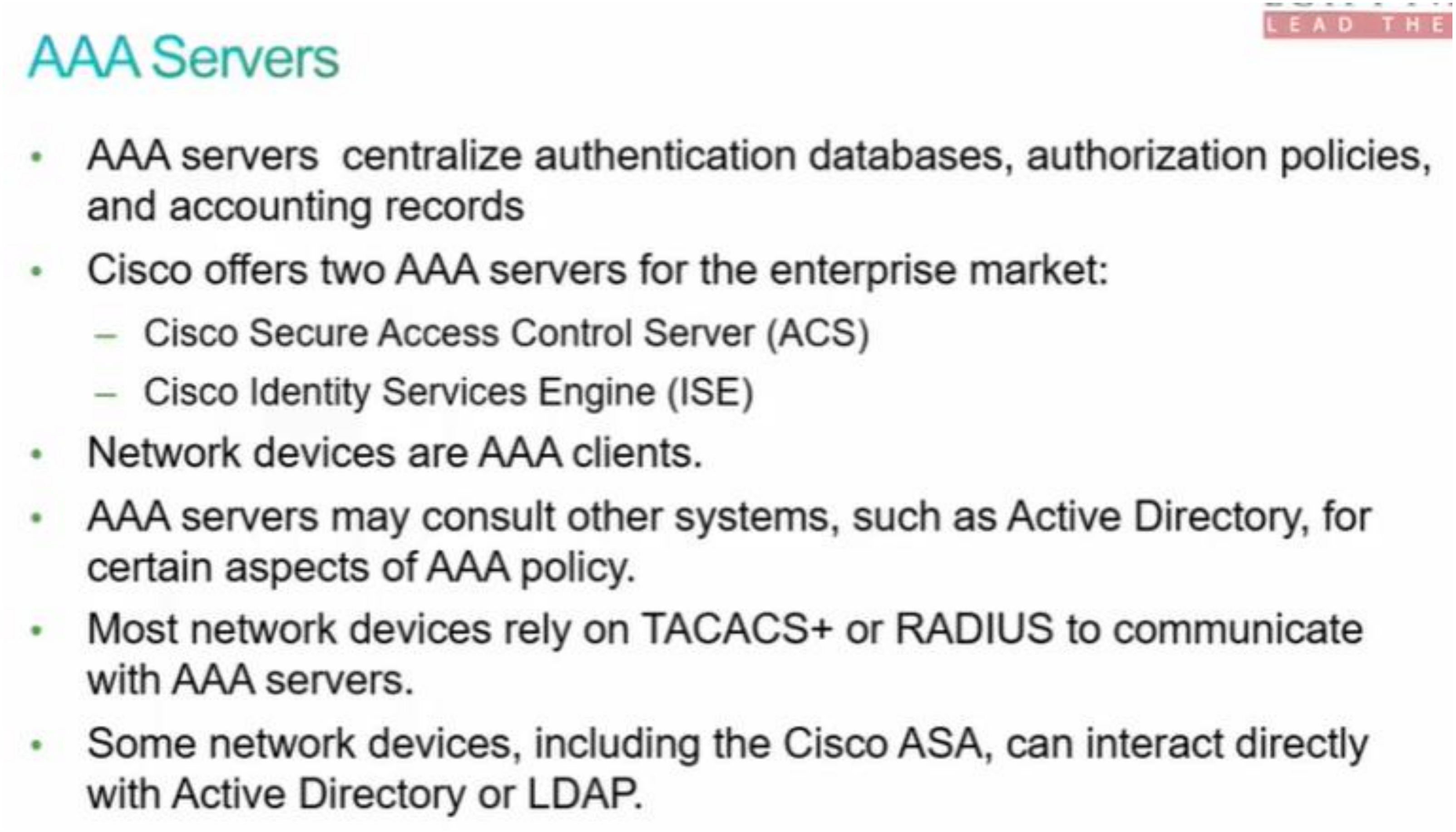
- AAA clients (network devices) communicate with AAA servers
- Two widely-used AAA protocols:
  - RADIUS
    - Server listens on UDP port 1645 (legacy) or 1812 for authentication and authorization
    - Server listens on UDP port 1646 (legacy) or 1813 for accounting
  - TACACS+
    - Servers listen on TCP port 49 for authentication, authorization, and accounting



Functional Differences Between RADIUS and TACACS

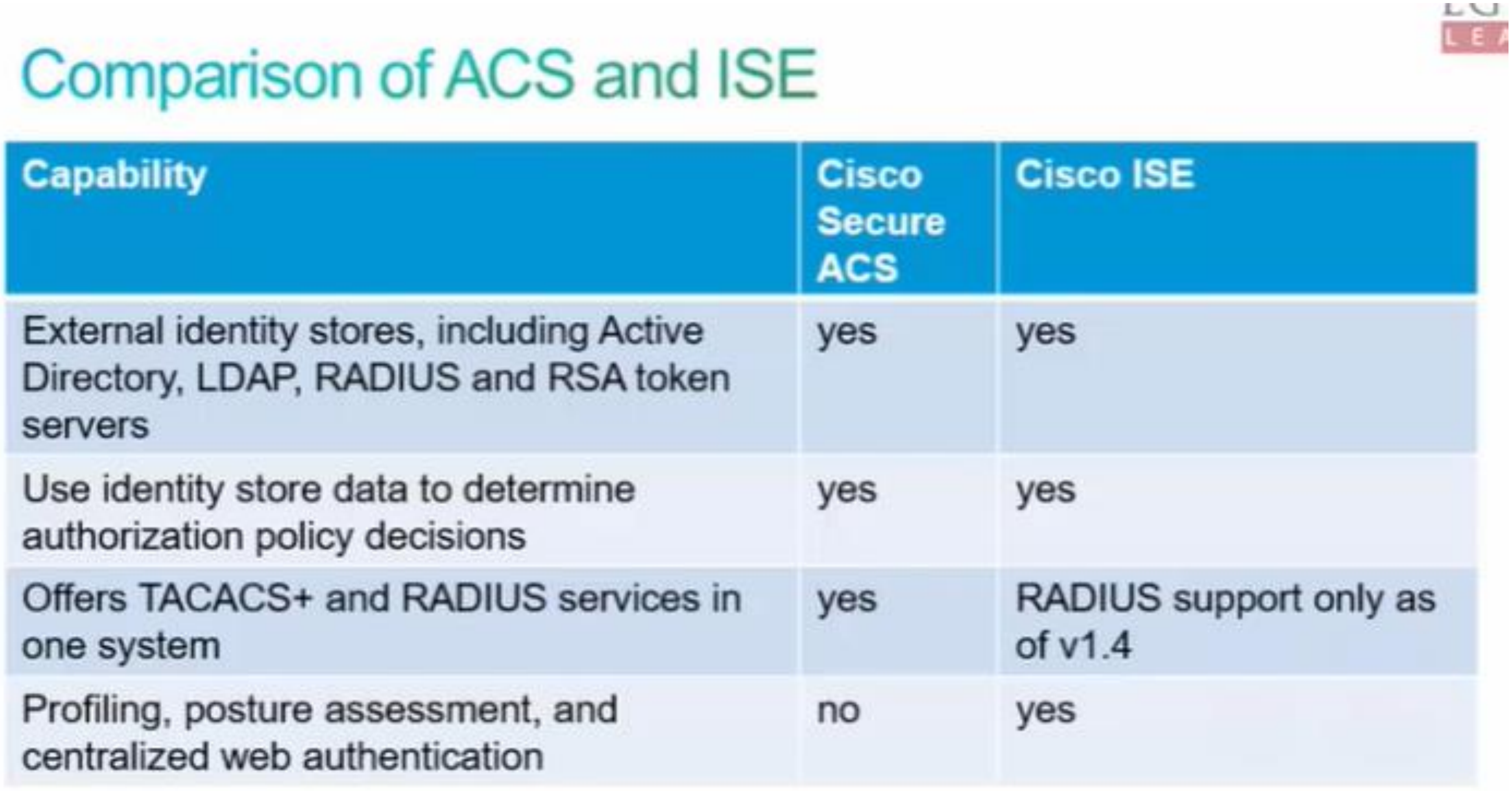


RADIUS	TACACS+
Combines authentication and authorization in a single process	Separates all three aspects of AAA into individual processes
Requires client to accept all authorization specifications at the time of authentication	Allows client to make real-time authorization requests for authenticated user or system after authentication process is complete
Obfuscates passwords transmitted between client and server using a shared secret key and MD5 hashing; the rest of the data sent in clear text	Encrypts all data transferred between clients and servers on a per session basis



AAA Servers

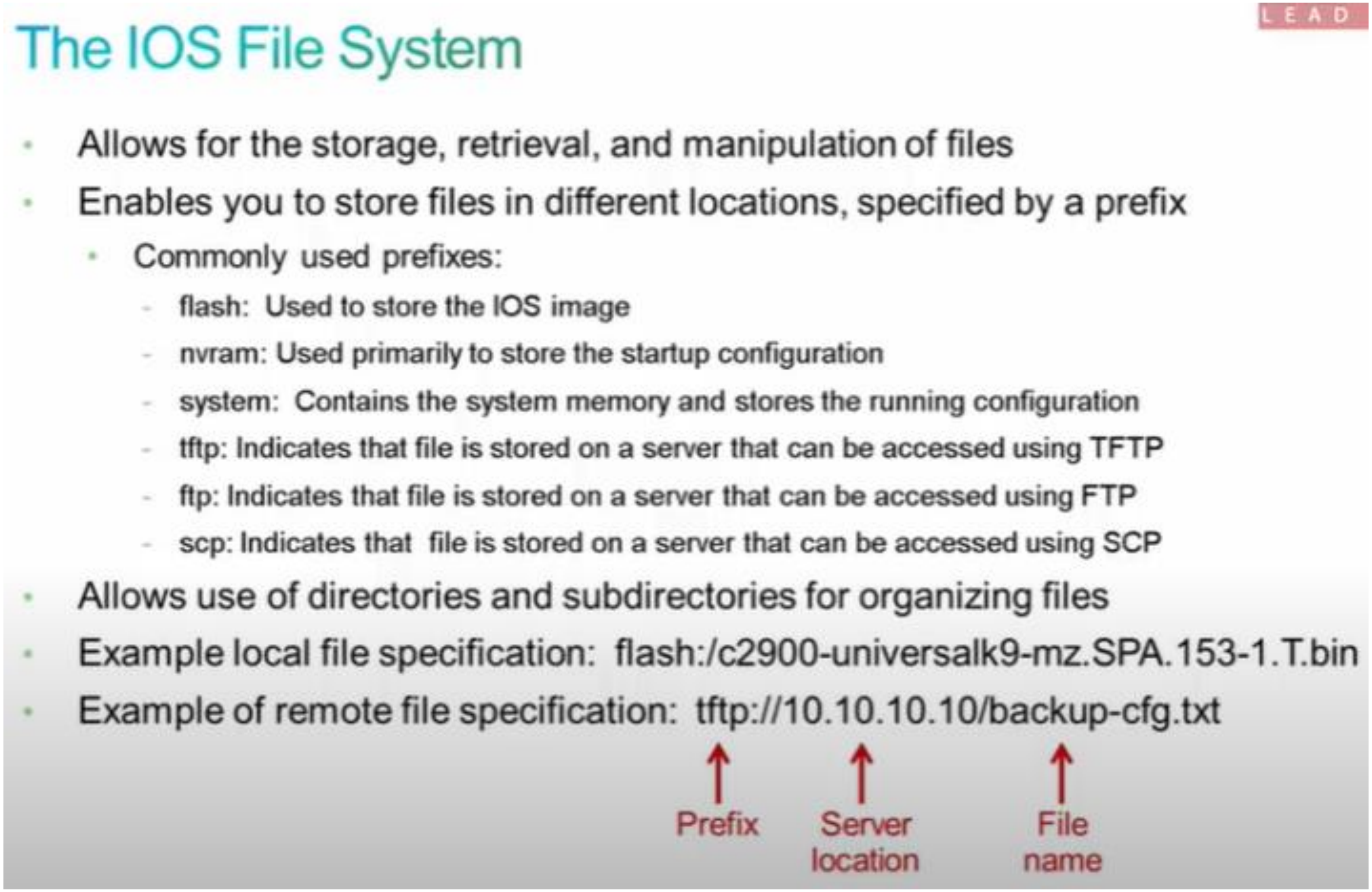
- AAA servers centralize authentication databases, authorization policies, and accounting records
- Cisco offers two AAA servers for the enterprise market:
  - Cisco Secure Access Control Server (ACS)
  - Cisco Identity Services Engine (ISE)
- Network devices are AAA clients.
- AAA servers may consult other systems, such as Active Directory, for certain aspects of AAA policy.
- Most network devices rely on TACACS+ or RADIUS to communicate with AAA servers.
- Some network devices, including the Cisco ASA, can interact directly with Active Directory or LDAP.



Comparison of ACS and ISE

Capability	Cisco Secure ACS	Cisco ISE
External identity stores, including Active Directory, LDAP, RADIUS and RSA token servers	yes	yes
Use identity store data to determine authorization policy decisions	yes	yes
Offers TACACS+ and RADIUS services in one system	yes	RADIUS support only as of v1.4
Profiling, posture assessment, and centralized web authentication	no	yes

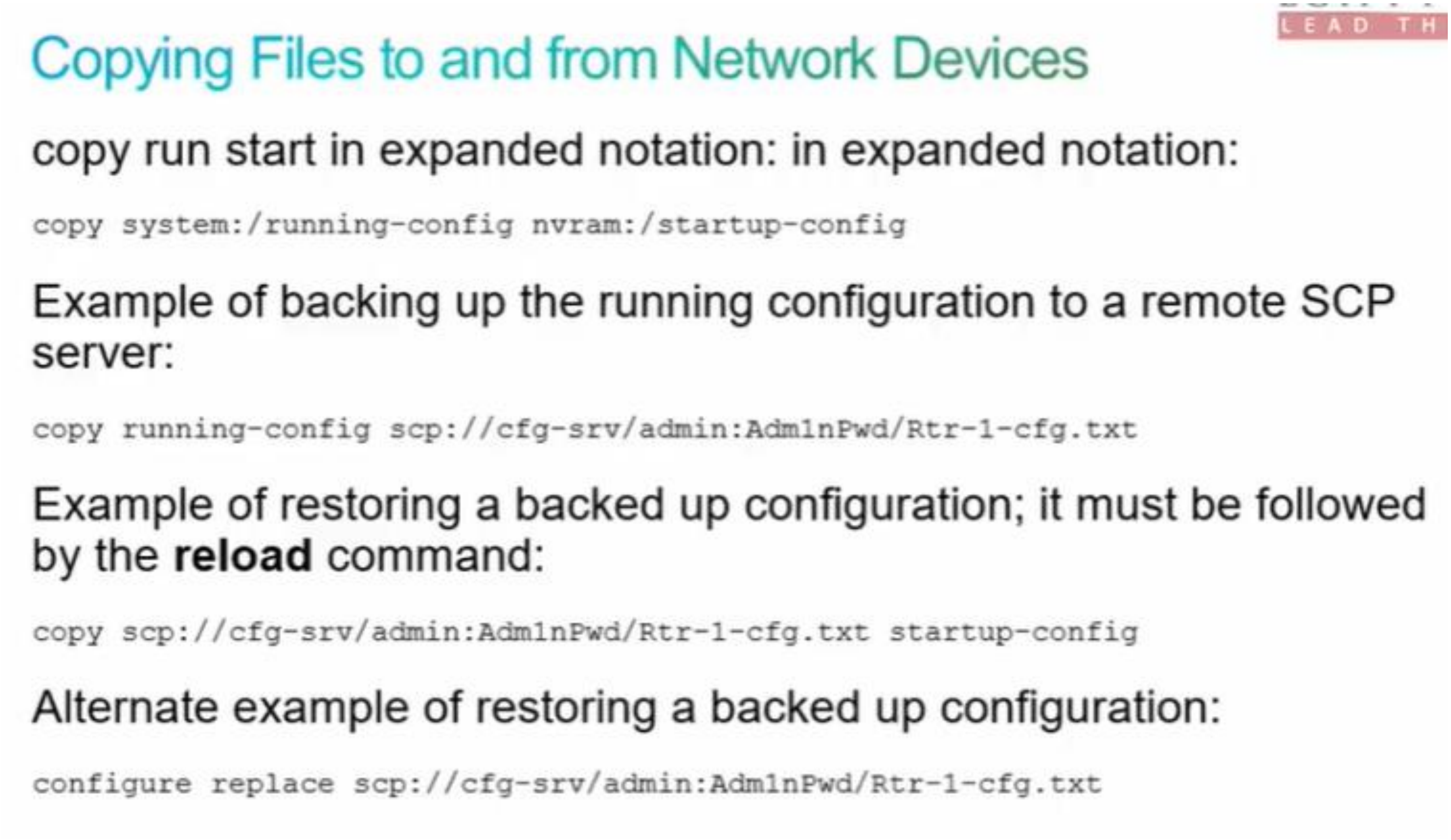
Management Protocols and Systems



The IOS File System

- Allows for the storage, retrieval, and manipulation of files
- Enables you to store files in different locations, specified by a prefix
  - Commonly used prefixes:
    - flash: Used to store the IOS image
    - nvram: Used primarily to store the startup configuration
    - system: Contains the system memory and stores the running configuration
    - tftp: Indicates that file is stored on a server that can be accessed using TFTP
    - ftp: Indicates that file is stored on a server that can be accessed using FTP
    - scp: Indicates that file is stored on a server that can be accessed using SCP
- Allows use of directories and subdirectories for organizing files
- Example local file specification: flash:/c2900-universalk9-mz.SPA.153-1.T.bin
- Example of remote file specification: tftp://10.10.10.10/backup-cfg.txt

↑ Prefix ↑ Server location ↑ File name



Copying Files to and from Network Devices

copy run start in expanded notation: in expanded notation:

```
copy system:/running-config nvram:/startup-config
```

Example of backing up the running configuration to a remote SCP server:

```
copy running-config scp://cfg-srv/admin:Adm1nPwd/Rtr-1-cfg.txt
```

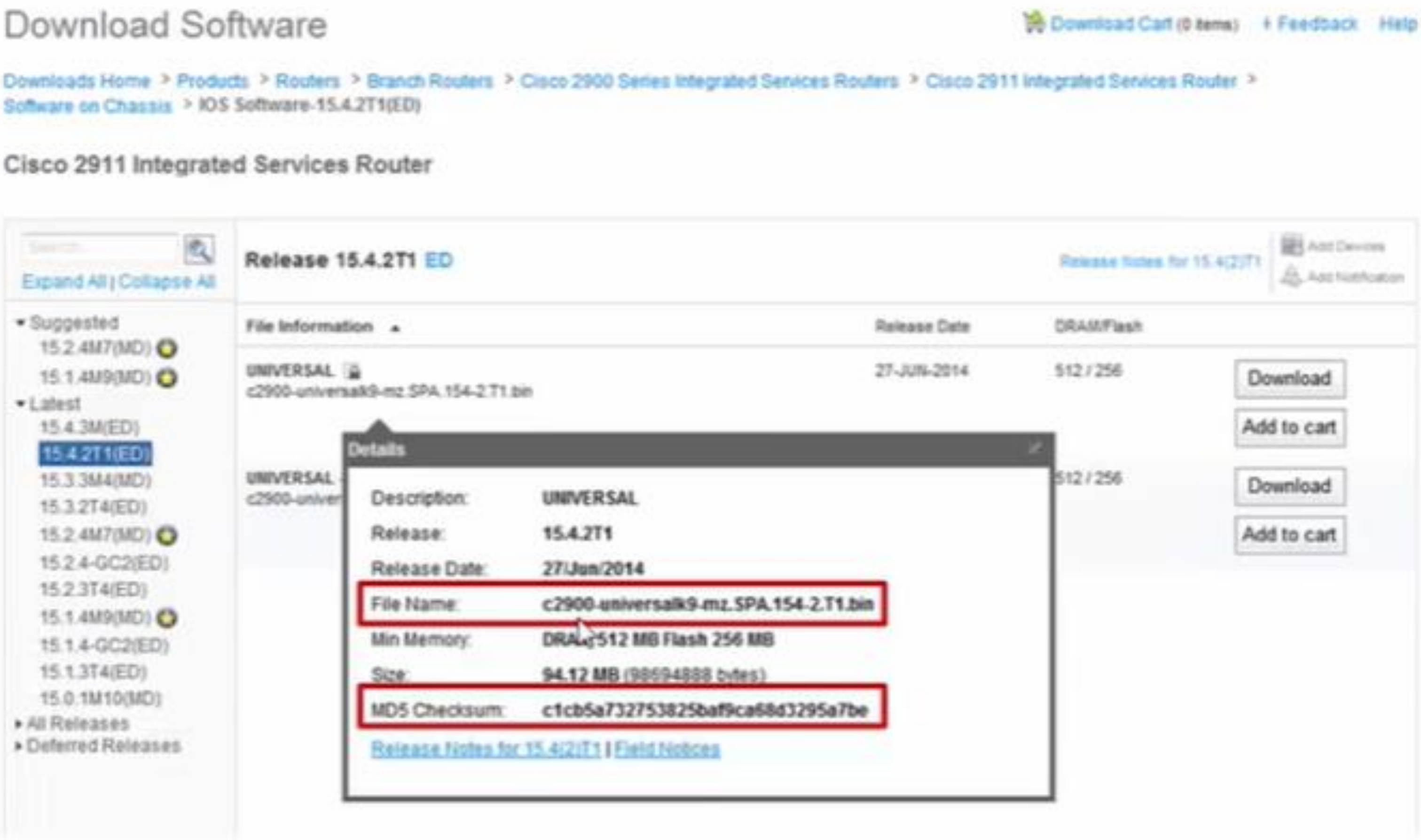
Example of restoring a backed up configuration; it must be followed by the **reload** command:

```
copy scp://cfg-srv/admin:Adm1nPwd/Rtr-1-cfg.txt startup-config
```

Alternate example of restoring a backed up configuration:

```
configure replace scp://cfg-srv/admin:Adm1nPwd/Rtr-1-cfg.txt
```

Validating IOS Images using MD5



Download Software

Downloads Home > Products > Routers > Branch Routers > Cisco 2900 Series Integrated Services Routers > Cisco 2911 Integrated Services Router > Software on Chassis > IOS Software-15.4.2T1(ED)

Cisco 2911 Integrated Services Router

Release 15.4.2T1 ED

File Information	Release Date	DRAM/Flash
UNIVERSAL c2900-universalk9-mz.SPA.154-2.T1.bin	27-JUN-2014	512 / 256
UNIVERSAL c2900-univer		512 / 256

Description: UNIVERSAL

Release: 15.4.2T1

Release Date: 27/Jun/2014

File Name: c2900-universalk9-mz.SPA.154-2.T1.bin

Min Memory: DRAM 512 MB Flash 256 MB

Size: 94.12 MB (98694888 bytes)

MD5 Checksum: c1cb5a732753825baf9ca68d3295a7be

Release Notes for 15.4(2)T1 | Field Notices

```
Rtr-1#verify /md5 flash:/c2900-universalk9-mz.SPA.154-2.T1.bin
.........<…Output Omitted…>............................ c1cb5a732753825baf9ca68d3295a7be
```

Digitally Signed Images

- Available for ISR series routers and other network devices
- Three character string within the filename:
  - c2900-universalk9-mz.SPA.153-1.T.bin
- Verify running image: **show software authenticity running**
- Verify image in file system:

```
Rtr-1#software authenticity file flash:/c2900-universalk9-mz.SPA.153-1.T.bin
File Name                        : flash:/c2900-universalk9-mz.SPA.153-1.T.bin
Image type                       : Production
    Signer Information
        Common Name              : CiscoSystems
        Organization Unit        : C2900
        Organization Name        : CiscoSystems
    Certificate Serial Number    : 50B3F3FE
    Hash Algorithm               : SHA512
    Signature Algorithm          : 2048-bit RSA
    Key Version                  : A
```