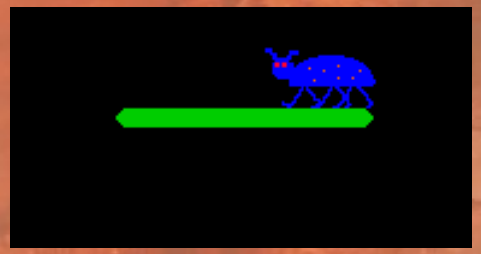
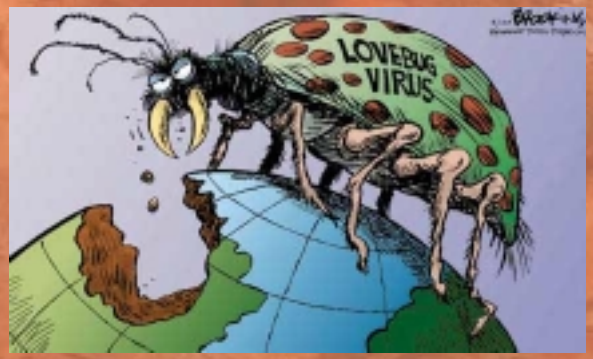

Security
and
Privacy

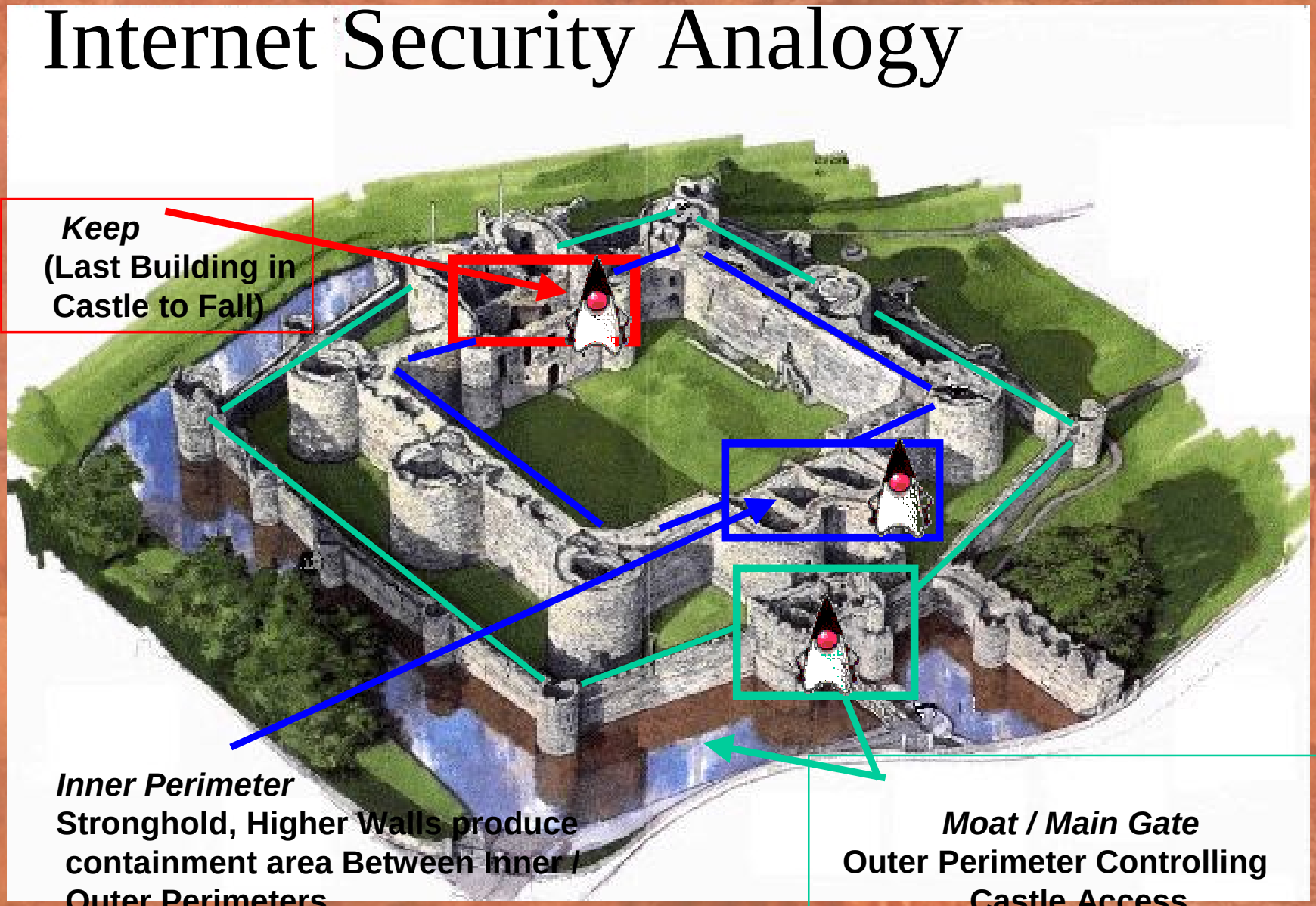
The Internet has met its Serious Enemies

They are called Security, Privacy, Viruses, Hackers and Governments!





Internet Security Analogy

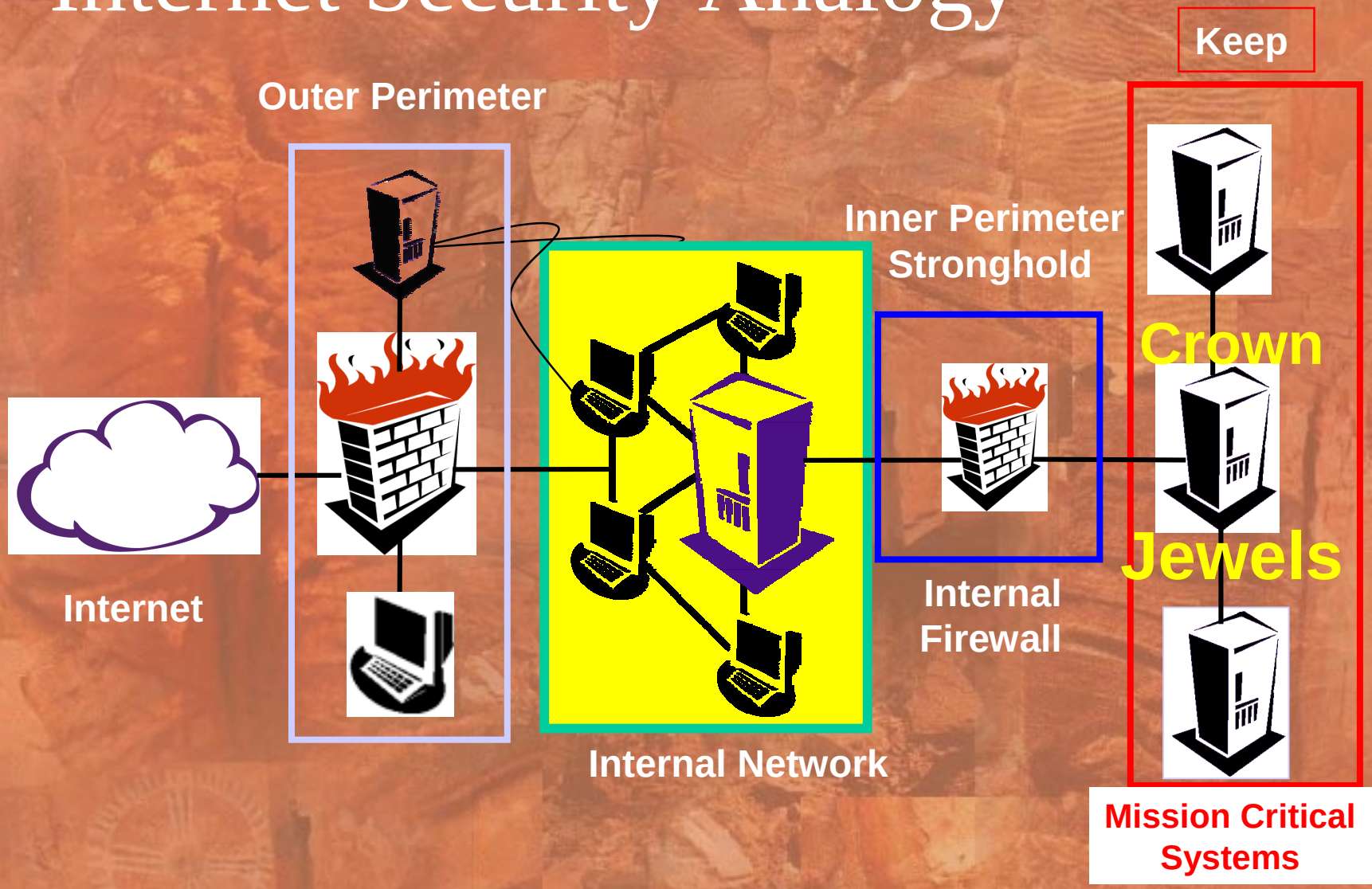


Keep
(Last Building in Castle to Fall)

Inner Perimeter
Stronghold, Higher Walls produce containment area Between Inner / Outer Perimeters

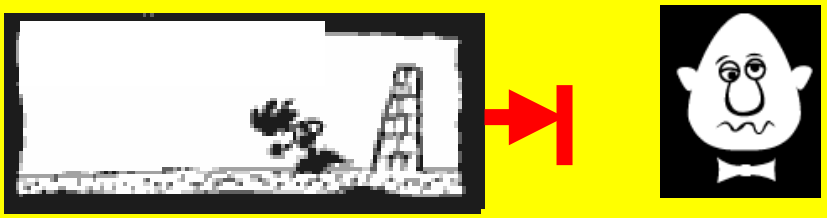
Moat / Main Gate
Outer Perimeter Controlling Castle Access

Internet Security Analogy



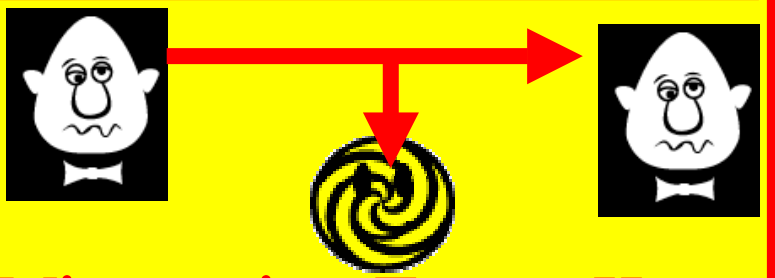
Internet Attacks

Disruption of Service



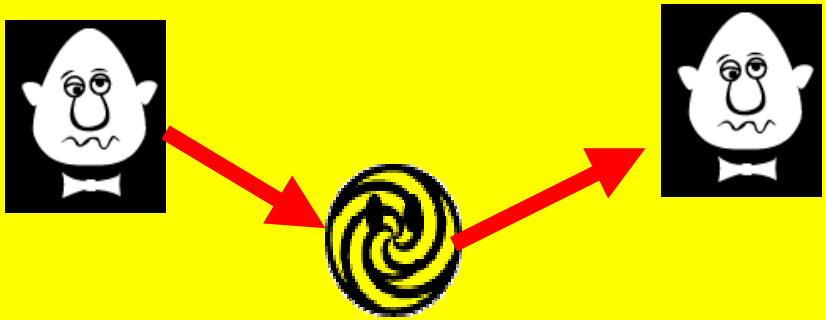
Brute Force, Hidden,...

Eavesdropping (secrecy)



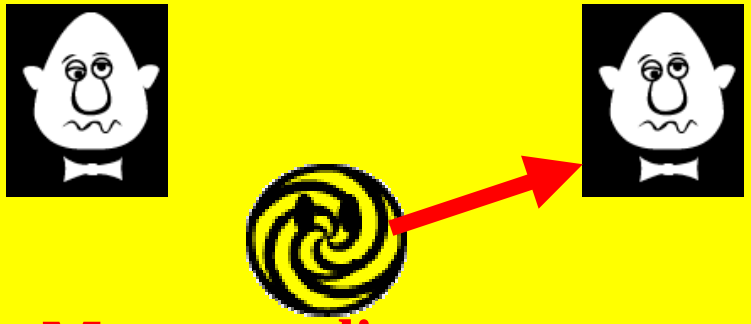
Wiretapping, Troyan Horse

Modification (Integrity)



Man-in-the M., Viruses, ...

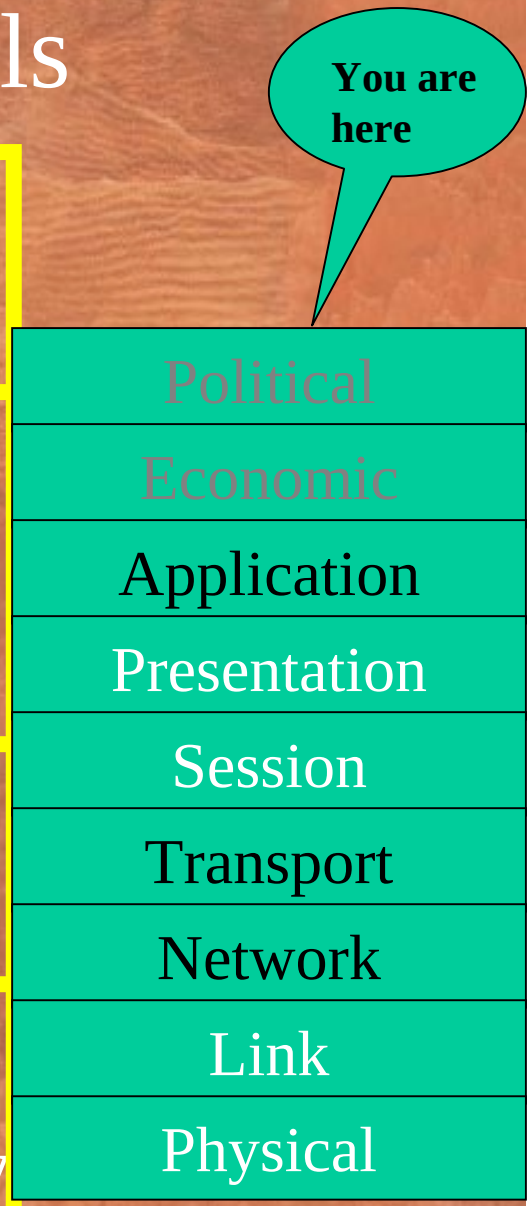
Fabrication (Authentication)



Masquerading, ...

Some Internet Security Protocols

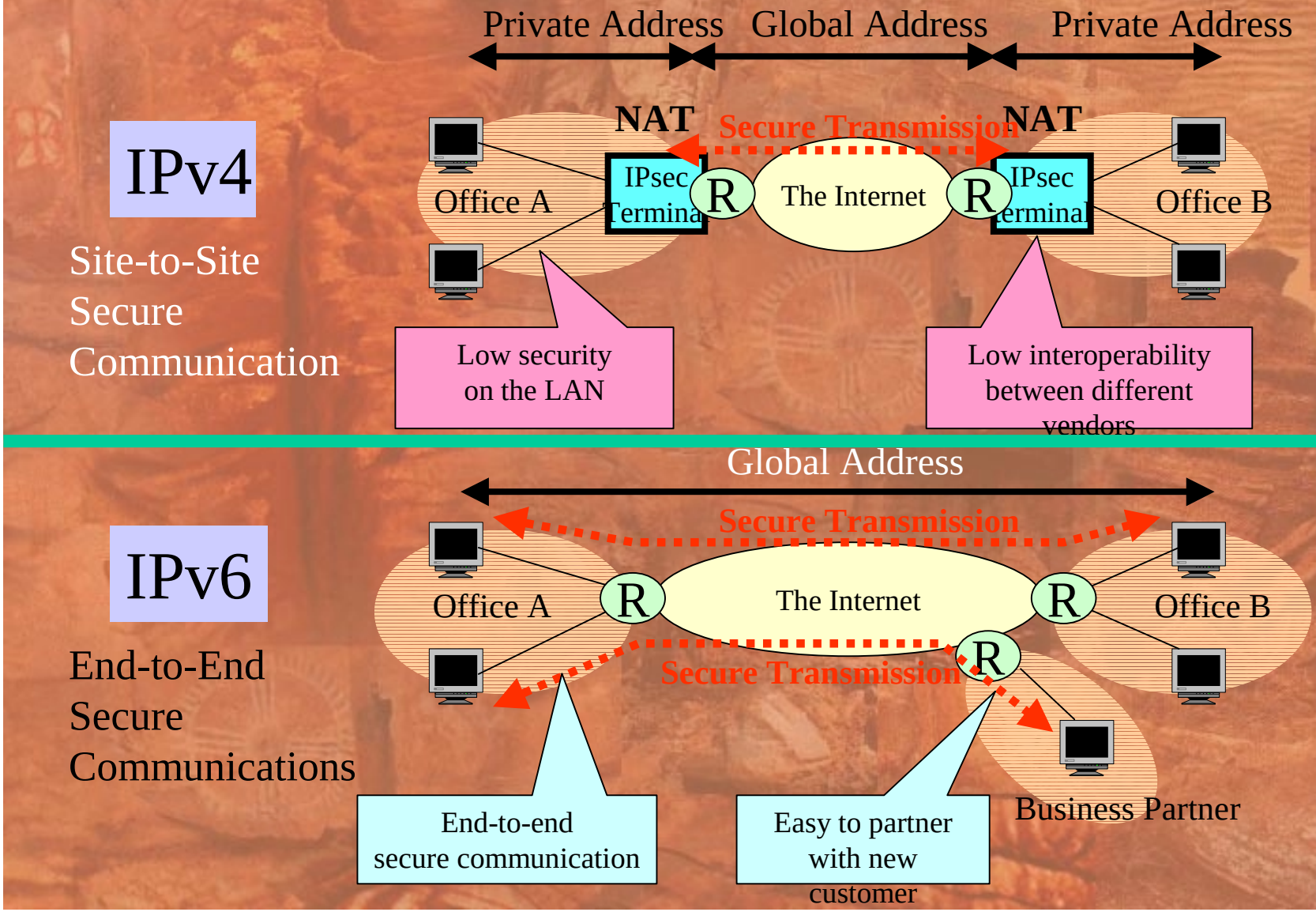
Application	**- e-mail** **+ PGP, S/MIME**
Transport	**- Primarily Web** **+ SSL/TLS** **+ Secure Shell (SSH)**
Network	**- IP Security** **+ IPsec**
Infrastructure	**+ DNSSec** **+ SNMPv3 security**



Internet Security and Privacy with IPv6 -Analogy

End-to-End Secure Communication

Easy to setup IP-VPN between end-to-end terminals with IPv6



Internet Security
(Security-101)

- **Policy Definition**
  - **Determining what is and is not acceptable**
- **Architecture to Implement Policy**
  - **Determine how to meet policy requirements**
- **Security Implementation**
  - **Identify specific security tools to meet the architecture and policy requirements**
- **Operational Security Procedures**
  - **Ensure that software & people do the right** things

Internet Security Protocols

- **Application Layer Security**
  - **Should Be Independent of Network Layer but 'Details Can Bite'**
- **Transport Layer Security**
  - **Should Be Independent of Network Layer but Some Implementations May Not Be**
- **Network Layer Security**
  - **IP Security (IPSec) - IPv4 & IPv6**
- **Infrastructure protection**
  - **Name System (DNS) crucial for IPv6**

Internet Security and IPv6

- **DNS Essential for IPv6 Operation**
  - **IPv6 Addresses Not ‘Human Rememberable’**
  - **No IPv6 Address Can Be Considered ‘Static’**
  - **Name System Must be as Dynamic as Addresses**
- **DNS Crucial for Transition**
  - **A Dual IP (v4 & v6) Node Will Have Different Address for IPv4 and IPv6**
  - **DNS Provides Info Needed to Determine Required Addresses**

IPsec

- **Protects all upper-layer protocols.**
- **Requires no modifications to applications.**
  - **But smart applications can take advantage of it.**
- **Useful for host-to-host, host to gateway, and gateway-to-gateway.**
  - **Latter two used to build VPNs.**

Doesn’t IPsec work with IPv4?

- Yes, but…

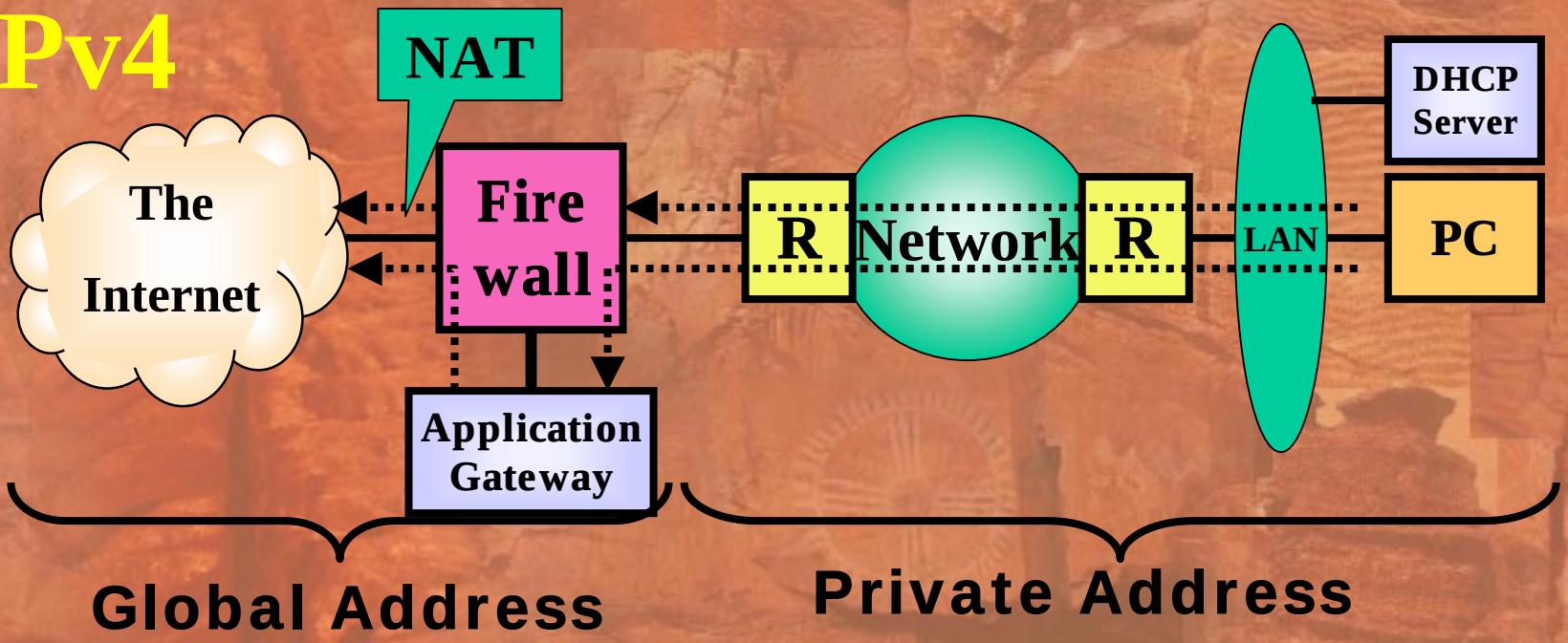
- It isn’t standard with v4.
- Few implementations support host-to-host mode.
  - Even fewer applications can take advantage of it.

No NATs

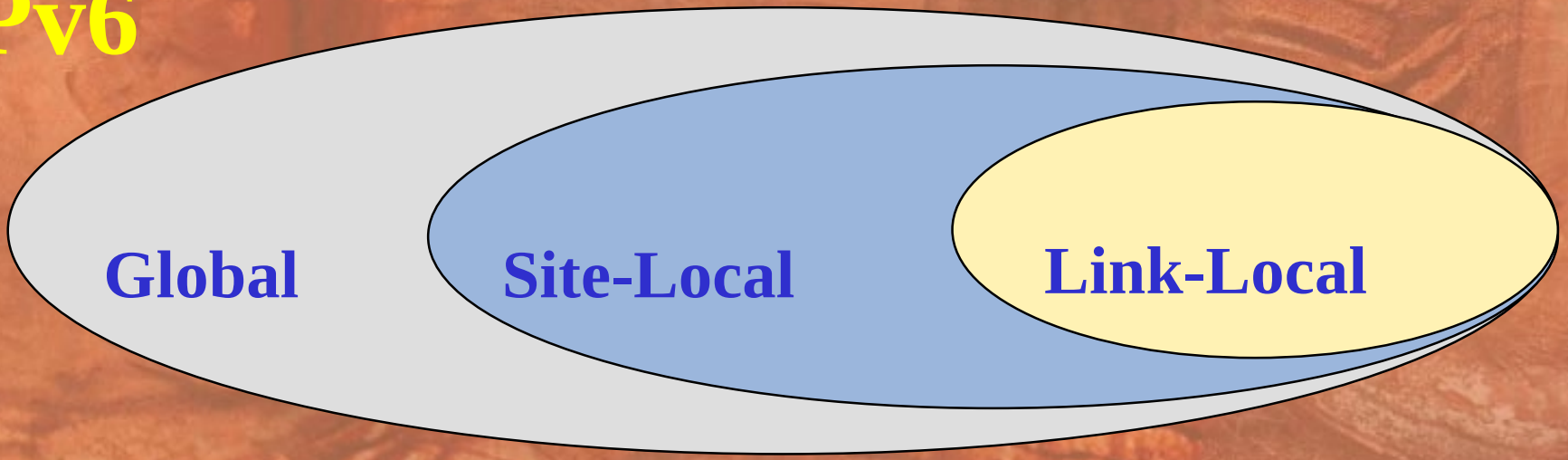
- NATs break IPsec, especially in host-to-host mode.
- With no NATs needed, fewer obstacles to use of IPsec.
- Note carefully: NATs provide no more security than an application-level firewall.

PRIVACY: Addressing Model

IPv4



Pv6



Privacy: What‘s the Issue?

The headline:

- **IPv6 addresses contain a permanent "serial number"**
- **Can be used to track individual's network access**

The full story:

- **Like IPv4 today, IPv6 has multiple ways of assigning addresses (static assignment, DHCP, etc.)**
- **IPv6 also defines a new way of assigning addresses called stateless address autoconfiguration**
- **(Original) stateless autoconfiguration raises privacy issues in *some* environments, but IETF has a solution environment**

Stateless Address Autoconfiguration

- Machines need an address to use network.
- New machines should not require configuration before first use.
- DHCP not an option in all environments (e.g., home, strangers on a train, etc.)
- How it works:
  - Routers advertise a network prefix
  - Advertised prefix + MAC address form an IPv6 address
  - Use of MAC address ensures that IPv6 address is unique

The Concern

- Applies *only* to addresses formed via traditional stateless Address autoconfiguration
- IPv6 address contains embedded MAC address
- When device moves (e.g., home, car, office) IPv6 address may change, but MAC portion stays the same
- Granularity of tracking possible when compared to IPv4

Privacy Extensions For Stateless Address Autoconfiguration

Need for two kinds of addresses:

- **Public (permanent) address that allows device to be called (e.g., telephone)**
- **Temporary address that device *initiates* communication from (e.g., web browser) Single device uses both simultaneously**

Temporary address:

- **Used for short period of time (hours, days)**
- **Generate new temporary address daily**
- **Changing addresses over time makes correlation of activities infeasible**

Open Internet Security Issues

- Due to these ad-hoc security solutions, too many non-interop encryption /authentication systems and products.
- PKI Infrastructure inexistent. Not too many PKI-ready products. 3 competing PKI Forums.
- Mobility security (binding updates). Fixed in version 17.
- Vendors prefer to sell their own embedded security modules and methods.

Conclusions

- IPv6 mandates and enables an important improvement in security.
- Much of the improvement comes from standard, usable, IPsec.
- The very large address space may provide for other, innovative security mechanisms.

The Business Activity	Level 0 PRE-INTERNET	Level 1 BASIC PROSPECTING	Level 2 BUSINESS INTEGRATION	Level 3 BUSINESS TRANSFORMATION
New Abilities and Benefits	1995 – Increasing desktop functionality – Increasing levels of enterprise networking – Databases – Client-server systems – Static data – Boundaries clearly defined	1994-99 – Static web presence – Distinct from general enterprise applications and systems – Increasing levels of information available – Intranet – E-mail – Marketing, PR	1998-2002 – Simple transactions – Low-level data sharing between enterprises – Intranet/extranet integration issues – Extranet	2000 - – All or part of supply chain online – High transaction values – High-level data sharing – More advanced apps – CRM, extranet, secure messaging, payment processing, etc. – Major intranet/extranet integration issues
Who Benefits	– HQ employees	– General public – HQ and remote employees	– HQ, remote employees – Business partners	– Business partners, suppliers, buyers, etc.
Security Needs	– Native security & access control mechanisms in the resource layer (OS, applications, file systems) – Authentication Mechanism using Passwords	– New perimeter layer (Firewall, Anti-virus, Intrusion detection) – Native resource layer security – Authentication Mechanism using Passwords	– Perimeter layer (Firewall, Anti-virus, Intrusion detection, VPN) – Native resource layer security – New control layer (access control) – Authentication mechanisms (Passwords, Tokens, Certs - mainly SSL)	– Perimeter layer (Firewall, Anti-virus, Intrusion detection, VPN) – Native resource layer security – Control layer (Digital Identity & Entitlements Management) – Authentication Mechanisms (Passwords, Tokens, Certs, Biometrics)