

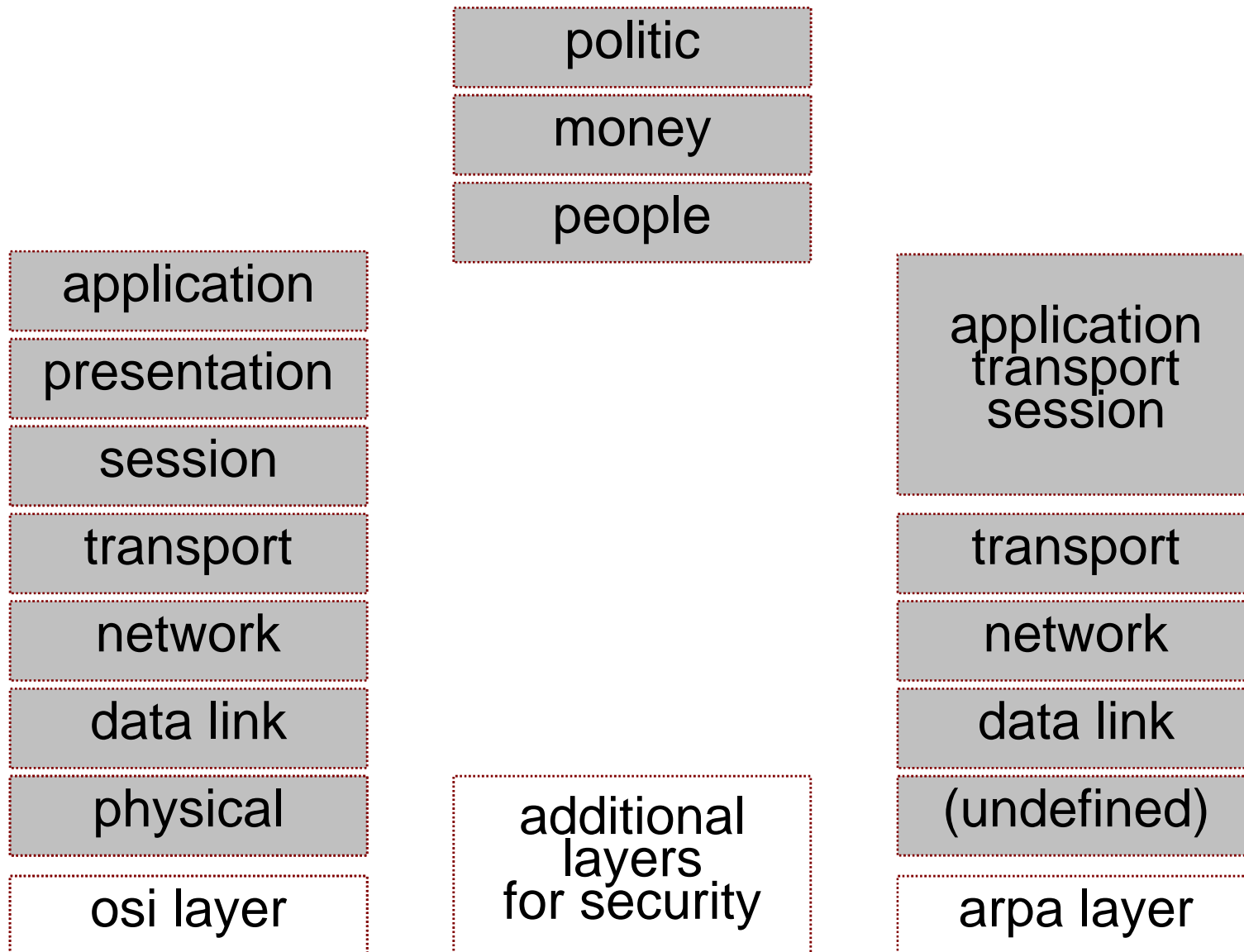
# it security illusion

## what the pros should understand

Gildas Deograt, CISSP, ISO27001 LA



# 10 “security layers”



- We've used firewall, IPS, End-Point Security, DLP, Anti Virus, SSL, IPsec, Biometric, Smart Card, RFID, .... (you can list any type of security technologies here!)
- What we believe...
  - (according to Gartner) – this vendor is the best
  - (according to ISO) – certification is the king
  - (according to our security vendor) – use our solution then you'll be secure
  - **We've followed Gartner and our vendors then we are secure :(**
- Do we know that we've hacked?

- If hacking is difficult then
  - IT security is 10 times more difficult than hacking
  - Information Security is 100 times more difficult than hacking
- **If hacking** our information or IT is **nearly impossible** then
  - **Information and IT Security is an illusion**
- Security is based on access control process :  
Identification - Authentication - Authorization - Audit
- Fool proof identification is almost impossible
  - Identification relies on authentication
  - Even DNA can be spoofed!

- “Hackers” (Attackers)
  - Amateurs hack the systems
  - **Pros hack the people**
- Information Security Professionals ???
  - **Human aspect** in security architecture design?
    - ◆ **How if the security manager is malicious?**
  - **Human aspect** in security audit, assessment and penetration test?
    - ◆ Audit the auditor checklist
    - ◆ Assess the assessment / pentest RFP
  - **Human aspect** in security budget?

# does your vendor do wrong things?



- No!
- They do their jobs
  - Make products
  - Sell them
- Do we do our jobs properly???
  - Do we really understand the technology?
  - Do we do awareness to everyone?
  - Do we information security classification?
    - ◆ Do we perform risk analysis properly?
    - ◆ Do we implement the protection regarding the classification properly?
  - (too many questions...)

physical security  
"security theater"

# fundamental security principle



- No physical security = No security
- Are we physically secure?

# where's the physical boundary?



- Building – Floor – Room
  - How do the security guards check?
  - People don't care or hesitate to challenge each other
- Wireless
  - Microwave, VSAT, Voice
  - Electronic emanation “magically” turns non-wireless devices becoming wireless device!
- Cable
  - The rack is secured?
  - How to secure the backbone cable?
- How about mobile users?

cryptography  
"it's not the silver bullet"

# let's crack the nsa's aes “message”



- Blowfish is more secure than Rijndael
- AES a.k.a Rijndael (read “Rhine dahl”)
  - Key size of 128, 192 or 256 bits
  - The 192 or 256 key lengths approved by NSA for TOP SECRET information
  - AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.
  - As of 2006, the best known attacks are on 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit keys

# let's crack the nsa's aes “message”



NIST guidelines for public key sizes for AES			
ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

# side channel attacks



- Don't attack the algorithm
- But its implementation

operating system  
"administrator is the real problem"

is it logic?



**If I walk (do non administrator's activities) on  
the highway (for speed and convenience)  
then  
I'm still safe.**

# the administrator?



- Identified
  - IT Administrators
  - Users with “Authorize” Local Administrator Privilege
- Potential (can be administrator)
  - Local privilege escalation vulnerability combine with malicious or unaware users
  - People who have physical access
    - ◆ Doesn't matter how complex the administrator's password is

**pssst...**

**local administrator = domain administrator**

- Boot sequence
  - Evil Made Attack
- Memory
  - Cold Boot Attack
- Virtual memory
- Temporary files

network security  
"is it really private network?"

If there are **100 people** (ports/devices/hosts) in  
my house (network)

then

it's still **private**.

**Busway line** (MPLS, Broadband Fiber Optic,  
VSAT) is **private** (VPN) then the **president**  
(sensitive information) **doesn't need**  
**protection** (encryption) to go to another  
house.

- Who (people and machine) are inside our network now?
- Who (people and machine) are inside the IP "VPN" network now?
- Is there any wireless connections inside the internal network?
- How are network devices managed?

- Digital Certificate
  - Users know nothing
  - What does IT or security professional know?
- Who are Certificate Authorities?
- The server private key
  - How is it transmitted from CA to user ?
  - How is it used and stored?
- 99% of SSL implementation uses no mutual authentication
  - "Security Warning!!!" do want to continue?

critical infrastructure  
"virtual attacks = real damages"

If it is designed to be completely isolated and  
need 100% integrity and availability

then

use wireless network and install the most  
common and the most vulnerable OS family in  
the controller

- How to exchange information between critical infrastructure systems and business systems?
- How to protect 1000-10,000 KM of fiber optic cable?
- How to protect thousands of computer without physical protection?
- How to protect from SCADA / network / system engineers?

what to do?

is it logic?



If **70%** of information security problems is  
due to **human problems**

**then**

spend **3%** of security budget for  
information security **education.**

- People are the key
  - Security Awareness
  - Security Training
- 
- You are alone can do nothing
  - You are alone can destroy the whole defense mechanism

