“And the walls came tumbling down”
EBU Networks 2006

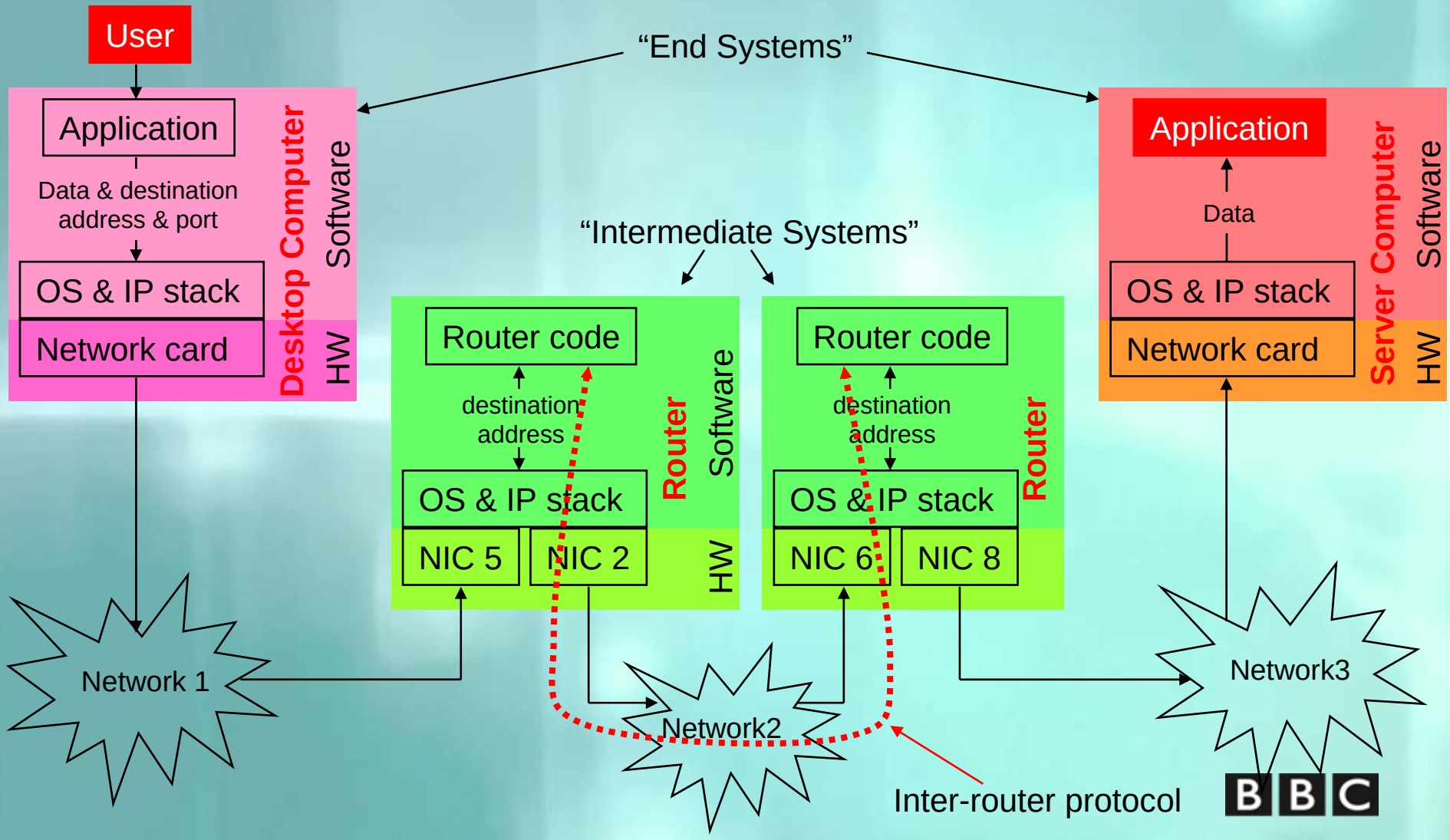
Andy Leigh
Head of Information Security Strategy
BBC

BBC

What I’m going to say

- A quick tutorial on Routing
- A quick history of attacks and firewalls
- The walled citadel
- Disruptive change
- Where we are headed
- The impact of the collapsing perimeter
- The Jericho Forum Commandments
- Conclusions

A tutorial on routing



Early Internet to modern times

- Then:
  - Pre-Internet modem access to mainframe (no PCs!)
  - Early “Internet nodes” were mini-computers, not routers
  - No concept of ISPs. Telecom involvement limited
  - Manual configuration & joining
- Now:
  - Dedicated routers
  - Tiered levels of infrastructure (including Telecoms)
  - Many single-ended “domestic” users via ISPs
  - Corporate entities aggregated behind “gateways”
- Early “Inter-nauts” would be unfamiliar with “now”

Why firewall

- Attacks:
  - Morris worm (1988)
  - Evening with Berford (1992)
  - etc.
- Poor “LAN”-centric protocols:
  - File-server systems used “chatty” protocols
  - Operating Systems assume they are on a disconnected LAN
- Systems too trusting of network users
- Systems badly written with back-doors and flaws
- Lack of public addresses (NAT)
- Single point to monitor/patch (reducing operational costs)

Firewall types

7. Application	FTP, HTTP	Server	ACL	Application proxy
6. Presentation				
5. Session				
4. Transport	TCP, UDP			
3. Network	IP	Router	ACL	Packet Filter / Stateful Packet Filter
2. Data Link	Ethernet	Switch	ACL	
1. Physical				

The walled citadel model

- Early/middle 90's most companies use firewalls
- Everyone inside was trusted
- Everyone outside was not trusted
- BUT, only limited network-based business transactions:
  - Email,
  - FTP
  - Web (later)
- Contrast this with inter-broadcaster networks and the early Internet

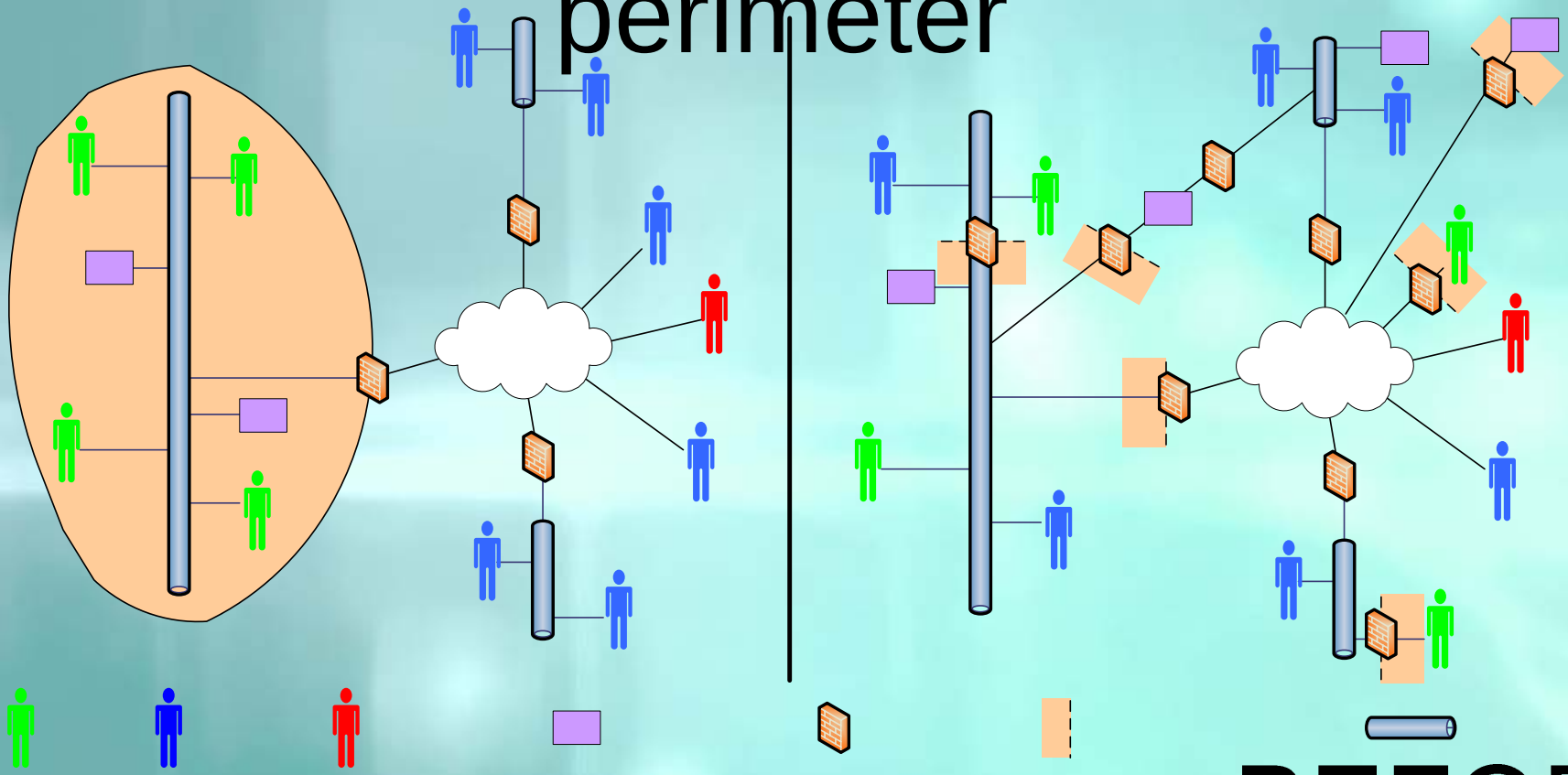
Disruptions to the walled citadel

- Many staff can work from home (DSL-fuelled)
- “Road warriors” working in hotels and cafes
- “Shrink-wrapped” systems that:
  - a) dial the supplier if there’s a fault
  - b) require the supplier to login to fix
- Many attacks engage the user’s curiosity and so circumvent the firewalls

Disruptions to the walled citadel 2

- Outsourcing:
  - Services, equipment and people that used to be inside “trusted” are now outside - “untrusted?”
  - Might be from a country with different laws
- SOA and Internet-based applications
  - Service Oriented Architecture – utility computing
  - Business-to-business using XML and web-services
- Direct bi-directional customer relations

Direction: the changing perimeter



BEFORE

- For business-to-business operations need non-technical standards and methodologies
- What are the implications to the way we define procure and build information solutions?

BBC

The Jericho Forum & The Open Group

- Jericho Forum in a nutshell: “Your security perimeters are disappearing: what are you going to do about it?”
- The Jericho Forum mission is to act as a catalyst to accelerate the achievement of the Vision, by:
  - Defining the problem space
  - Communicating the collective Vision
  - Challenging constraints caused by current vendor IT security models and thus creating an environment for innovation
  - Demonstrating the market and thus influencing future products and standards
- The Open Group:
  - works towards enabling access to integrated information within and between enterprises based on open standards and global interoperability.
- http://www.opengroup.org/jericho

BBC

Jericho Forum's 11 commandments

- Fundamentals (3)
- Surviving in a hostile world (2)
- The need for trust (2)
- Identity, management and federation (1)
- Access to data (3)

Fundamentals

1. The scope and level of protection must be specific and appropriate to the asset at risk.

- Business demands that security enables business agility and is cost effective.
- Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves.
- In general, it's easier to protect an asset the closer protection is provided.

Fundamentals

2. Security mechanisms must be pervasive, simple, scalable and easy to manage.

- Unnecessary complexity is a threat to good security.
- Coherent security principles are required which span all tiers of the architecture.
- Security mechanisms must scale:
  - from small objects to large objects.
- To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms.

Fundamentals

3. Assume context at your peril.

- Security solutions designed for one environment may not be transferable to work in another:
  - thus it is important to understand the limitations of any security solution.
- Problems, limitations and issues can come from a variety of sources, including:
  - Geographic
  - Legal
  - Technical
  - Acceptability of risk, etc.

Surviving in a hostile world

4. Devices and applications must communicate using open, secure protocols.

- Security through obscurity is a flawed assumption
  - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use.
- The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added on.
- Encrypted encapsulation should only be used when appropriate and does not solve everything.

Surviving in a hostile world

5. All devices must be capable of maintaining their security policy on an untrusted network.

- A “security policy” defines the rules with regard to the protection of the asset.
- Rules must be complete with respect to an arbitrary context.
- Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input.

The need for trust

6. All people, processes, technology must have declared and transparent levels of trust for any transaction to take place.

- There must be clarity of expectation with all parties understanding the levels of trust.
- Trust models must encompass people/organisations and devices/infrastructure.
- Trust level may vary by location, transaction type, user role and transactional risk.

The need for trust

7. Mutual trust assurance levels must be determinable.

- Devices and users must be capable of appropriate levels of (mutual) authentication for accessing systems and data.
- Authentication and authorisation frameworks must support the trust model.

Identity management & federation

8. Authentication, authorisation and accountability must interoperate/exchange outside of your locus/area of control.

- People/systems must be able to manage permissions of resources they don't control.
- There must be capability of trusting an organisation, which can authenticate individuals or groups, thus eliminating the need to create separate identities.
- In principle, only one instance of person/system/identity may exist, but privacy necessitates the support for multiple instances, or once instance with multiple facets.
- Systems must be able to pass on security credentials/assertions.
- Multiple loci (areas) of control must be supported.

Access to data

9. Access to data should be controlled by security attributes of the data itself.

- Attributes can be held within the data (DRM/Metadata) or could be a separate system.
- Access/security could be implemented by encryption.
- Some data may have “public, non-confidential” attributes.
- Access and access rights have a temporal component.

Access to data

10. Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges

- Permissions, keys, privileges etc. must ultimately fall under independent control
  - or there will always be a weakest link at the top of the chain of trust.
- Administrator access must also be subject to these controls.

Access to data

11. By default, data must be appropriately secured both in storage and in transit.

- Removing the default must be a conscious act.
- High security should not be enforced for everything:
  - "appropriate" implies varying levels with potentially some data not secured at all.

What do we end up with

- Clearly our hard shell dissolves a bit
- Devices, OSs, databases and applications are better written and can self-protect
- Critical assets are strongly patrolled
- Better business-to-business interoperability
- Improved business dynamism and flexibility
- BUT less technology dynamism and flexibility of choice

Questions to the audience

- Are you outsourcing and partnering?
- Could all of your systems survive directly on the Internet?
- Are you planning federated identity solutions
- Are you already planning for deperimeterisation?
- Is deperimeterisation being forced on you by your business or by others?

BBC

Conclusions

- It used to be good practice to have a walled-citadel with a strong shell and soft centre
- BUT we and our competitors are more dynamic now
- Outsourcing means “they” are inside
- Mobile workers mean “we” are outside
- Many attacks can traverse our strong walls
- Have to strengthen the middle first, then weaken the edges
- Jericho Forum have proposed 11 commandments to assist us to find a path towards a softer shell, stronger centre
- The walls will come tumbling down – will it be us or someone else that pushes them?

Thanks for listening

Any questions?