Internet Dial Tones & Firewalls: One Policy Does Not Fit All

IEEE Schenectady Section
Computer Society Chapter
Friday, October 15, 2004

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
http://www.rlgsc.com

Information Access Trend

- Online data is more accurate
- Stored/Staged data is obsolete
- Types of data
  - package tracking
  - technical data (private and public)
  - news and financial data
  - government filings
  - interwoven applications using XML

Internet Access has become expected

- Broadband
  - on every desktop
  - public accomodations/hotels
  - parks
  - home
  - stores
  - 24x7x365 access
  - 50% of Enterprises Wi-Fi enabled (Gartner)

Internet Access has become expected (cont'd)

- Wi-Fi (wireless)
  - coffee shops (Starbucks/T-Mobile)
  - bookstores (Borders/T-Mobile)
  - copycenters (Kinko's/T-Mobile)
  - airports
  - public spaces (NYC's Bryant Park)
  - phone booths (Verizon)
  - conferences
  - 24x7x365 access, at will, wherever one is

Internet Access has become expected (cont'd)

- Cellular Data
  - Verizon (deploying EV-DO)
    est. Summer 2004 in 75 markets
  - Sprint (1xEV-DV)
    +1–2 years
  - reported in USA Today, 25 March 2004, page 3B

However, inside enterprises –

- Outside, access is (or is becomming) ubiquitious
- Inside, access is increasing in complexity
- Past model was “gatehouse”, hard outside inside was/is fairly soft
- One size fits all, no texture or subtlety
- Levels of Trust (payroll, health, proprietary)
- Ease of breach/theft (e.g., script kiddies)
- Rogue Access Deployments

The Real Issue – TRUST

- the word TRUST means different things in different contexts
- the word TRUST means different things to different communities
- In human relationships, TRUST is often used in an absolute sense
- In legal contexts, TRUST is a far different concept
- Oddly enough, people can often agree on wording easier than the concept

Legal/Technical TRUST – What does it mean?

- Liability exposure
- Need to Know

Technical TRUST – What does it mean?

- Things may not work as planned
- When building houses, carpenters:
  - toe-nail
  - cross-brace
  - hurricane straps

All of engineering & structural design is about safety factors.

The art of ensuring safety in the face of error, uncertainty, and imperfection.

Data and Liability –

- R & D
- Deal Making
- Client Confidentiality/Privacy
- For employee's own protection

In God we trust –
All others we polygaph.

– Tom Clancy

Whom do you trust? What context?

- physician
- clergy
- attorney
- employer
- co-workers
- friends

Technical TRUST –

- If you don't breach the barrier, it isn't really there; is it?
- Insufficent walls create catastrophic failures – the "Titanic/Comet Syndrome"

Original Internet – Total TRUST

- No safeguards
- No integrity checks
- No compartmentalization
- Total Net Crash – IMP caused
- Trusting server processes (e.g., sendmail)

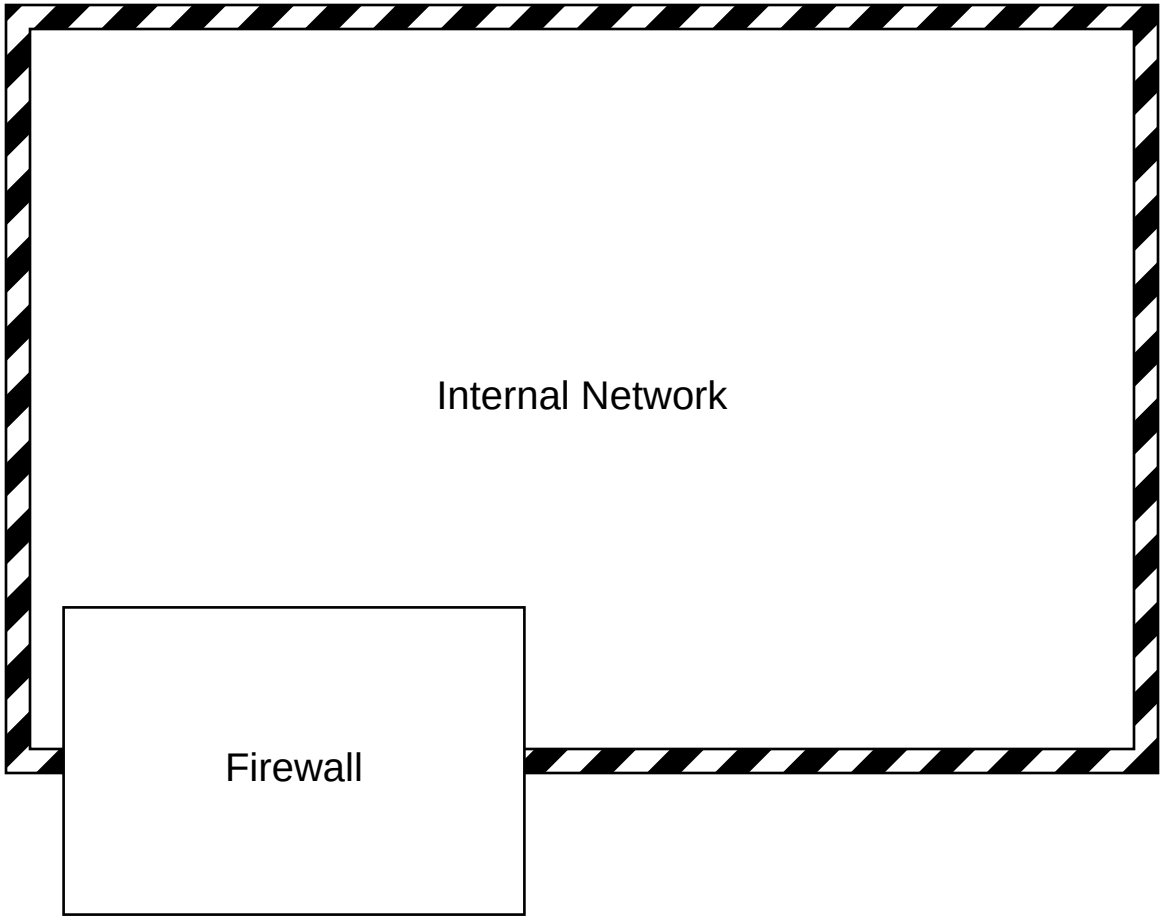
The Age of Innocence

- Machines are rare
- Inherantly restricted access
- Few players, all known to each other

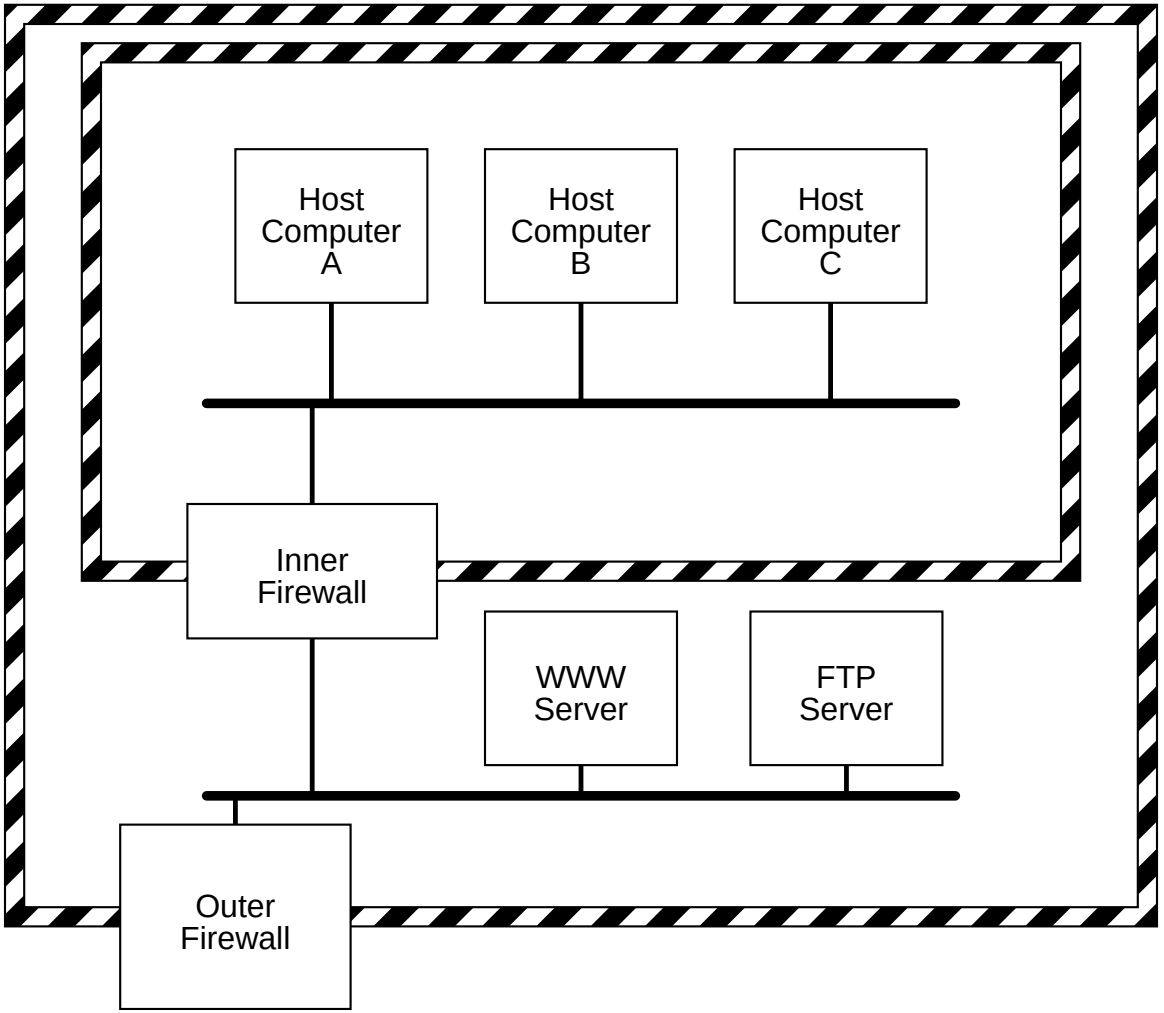
The Age of Ubiquitous Computing/Connectivity

- Huge number of machines
- Easy access to essentially unrestricted bandwith/connectivity
- Worldwide connectivity – essentially anonymous
- “On the Internet, nobody knows that you are a ‘dog’”

Traditional Simplistic Firewall Architecture



Traditional Simplistic Firewall Architecture with DMZ



Analyze the Threats

- Internal information control (“Need to Know”)
- Curiosity (e.g., celebrity tax returns)
- Insider Fraud
- “Loose lips sink ships”
- Criminal
- Visitor-borne contagion

Internal Access Obligations/Restraints

- Internal Security – Pricing, Internal data
- National/Homeland Security
- Regulatory – SEC, FDIC, FRB
- Legal – HIPAA, other protected
- Less monolithic teams

"Inside" Community is more Diverse

- Employees
- Contractors
- Vendors
- Salesman
- Customers
- Colleagues
- Regulators
- Interviewees

Technology Concerns

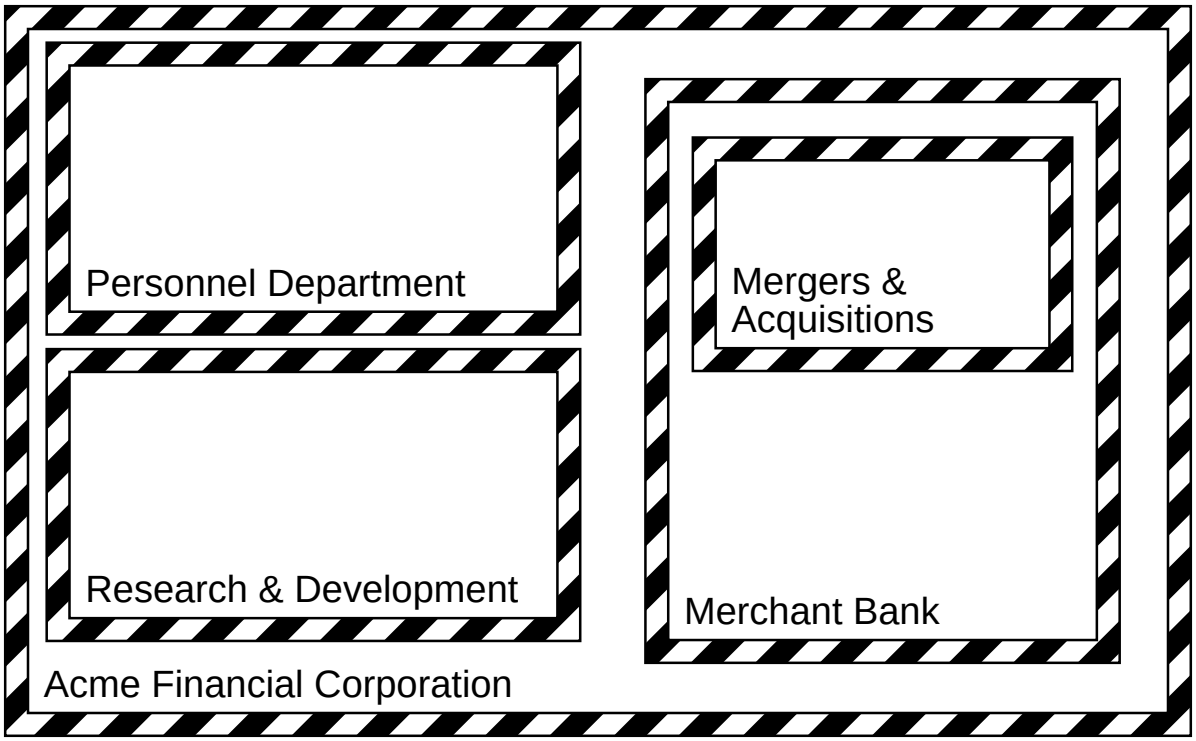
- both wired, Wi-Fi, and cellular have security concerns
- but, in a sense, the concerns/issues are the same
  - Are wall sockets really secure?
  - Passive attack – sniffing/eavesdropping
  - Trojan Horse (software/hardware)
  - The “Remote Control” syndrome

Security/Access Concerns

- authentication
- privacy/anti-eavesdropping
- bandwidth allocation
- springboard elimination

Security Domains

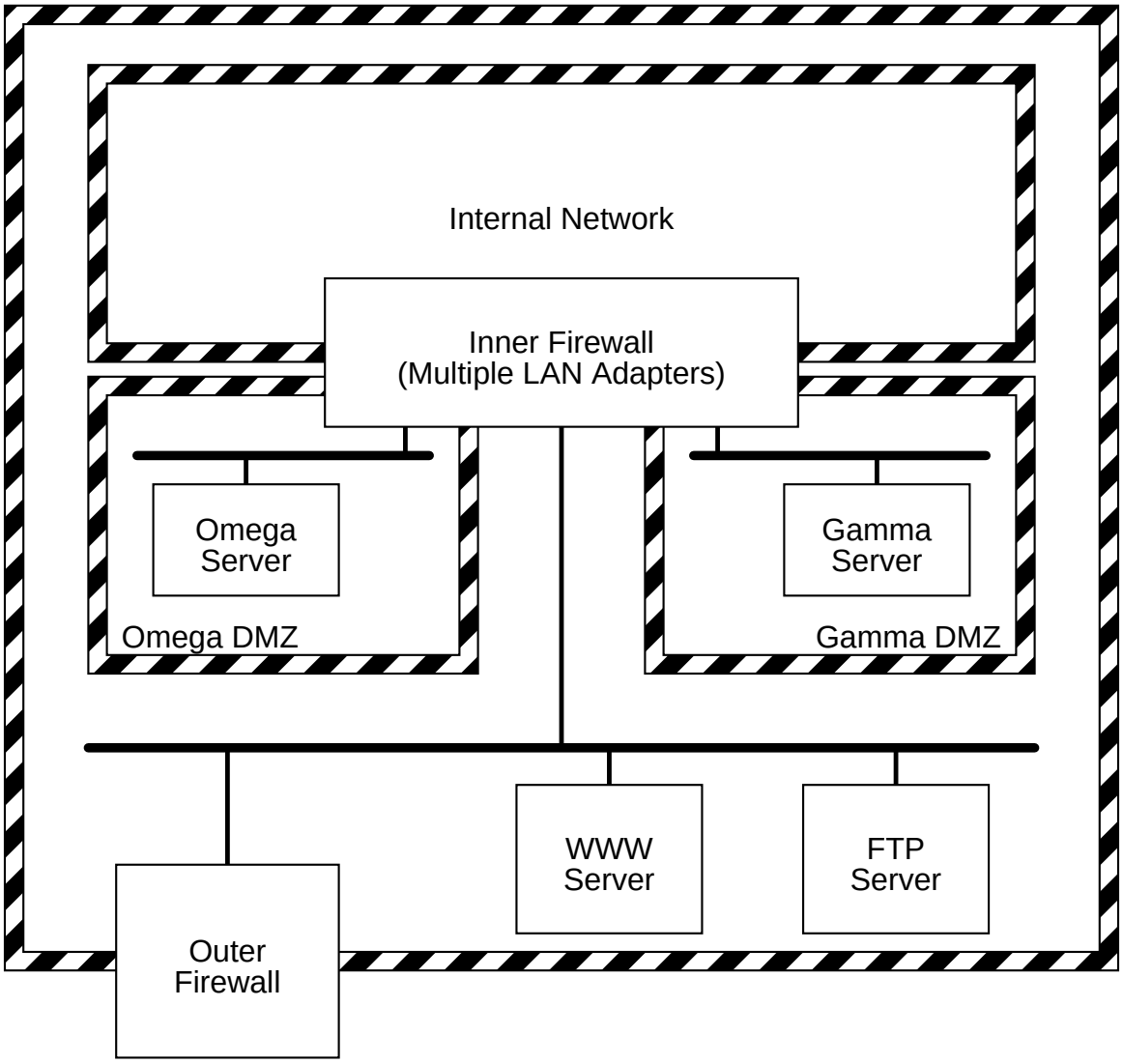
- Security by Architecture/Structure
- Limit and Control Trust and delegation
- Monolithic Domains cannot factor the problem space
- Sibling and Child Security Domains
- DMZs
- Cul-de-sacs
- pseudo-Public access to dial-tone
- HTTPS/X.509 Certificates within organization



DMZs

- not just between Internet and intranet
- each organization contains many relative outsiders
- firewalls are internal security partitions
- VPN's even within the organization
- X.509 Certificates/HTTPS for Intranets when sensitive business/personal information is present

Nested and Sibling Security Domains



Cul-de-sacs

- WAPs are only digital dial-tone
- getting out of a cul-de-sac requires VPN
- extensive use of proxy servers
- assumption of compromised network media
- where is WAP relative to gateway
- WPA (and WPA2) only address the “last meter”

Questions?

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
http://www.rlgsc.com

Session Notes & Materials:
http://www.rlgsc.com/ieee/schenectady/2004-10/index.html