Ensuring Security, Privacy, and Authenticity in a WWW Connected World

New York Dreamweaver User Group
Wednesday, February 13, 2008

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- Stored/Staged data is obsolete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

- Wired Broadband
- Wi-Fi
- Cellular

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
  - Broadband-class performance
  - Verizon (deploying EV-DO)
  - Sprint (1xEV-DV)
  - reported in USA Today, 25 March 2004, page 3B

Security, Privacy, Authenticity

- Whom do you trust?
- Whom can you trust?
- Is somebody going ’phishing’?
- Is the information sensitive?

Proving Authenticity –

- trust – identity checked by someone trusted
- on the ’net, it means X.509 Certificates
- Issued by whom?
  - recognized CA – Verisign, Thawte, GoDaddy
  - not general authority – Microsoft
  - self signed – DO NOT DO THIS

What does an X.509 Certificate Prove –

- Legitimate access to the domain name
- Business Documents Check
- Can be used to sign other X.509 Certs

What does't an X.509 Certificate Prove –

- Similar sounding/appearing names
- Legitimacy of requestor

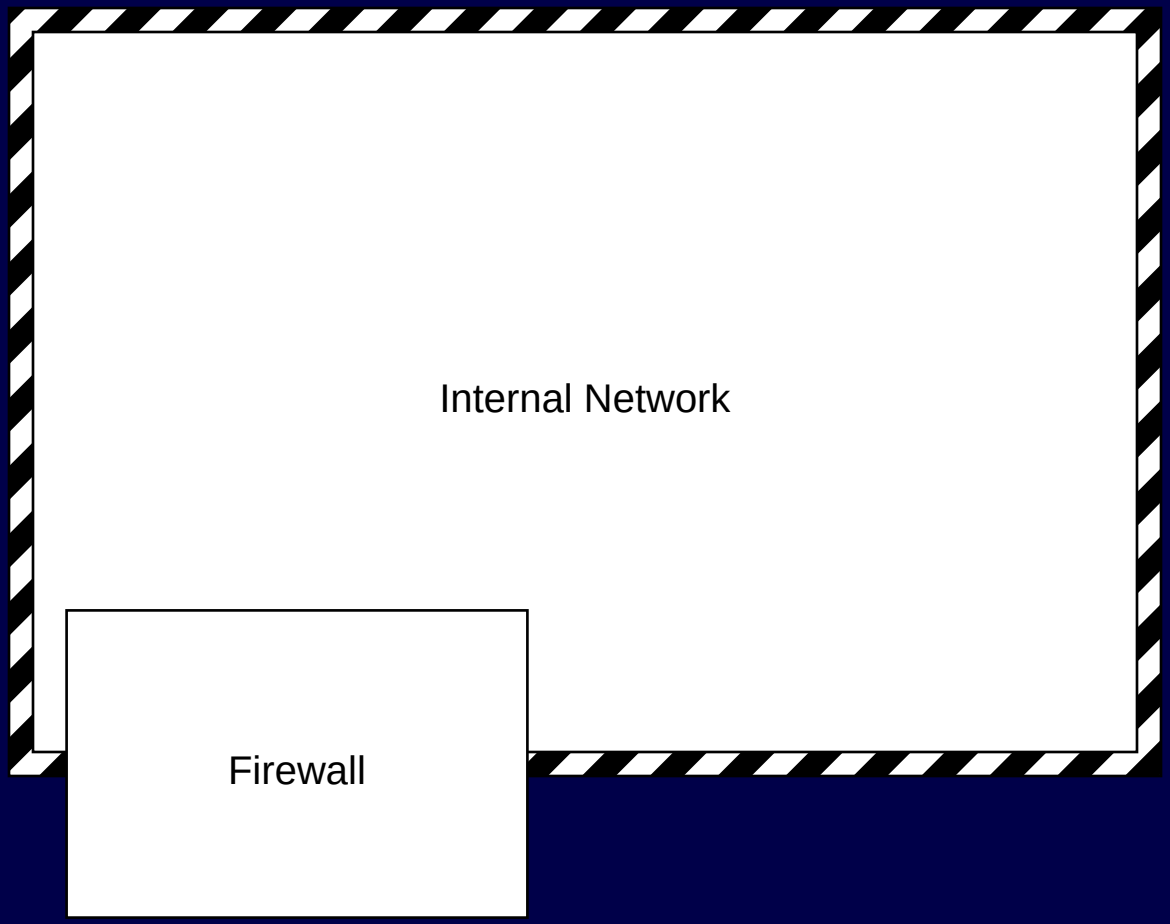
Security & Privacy –

- Eavesdropping thwarted by encryption
- SSL/TLS as an underlayer for HTTP -> HTTPS
- Authentication provided by X.509 certificates
- Known CAs
- Individual session keys

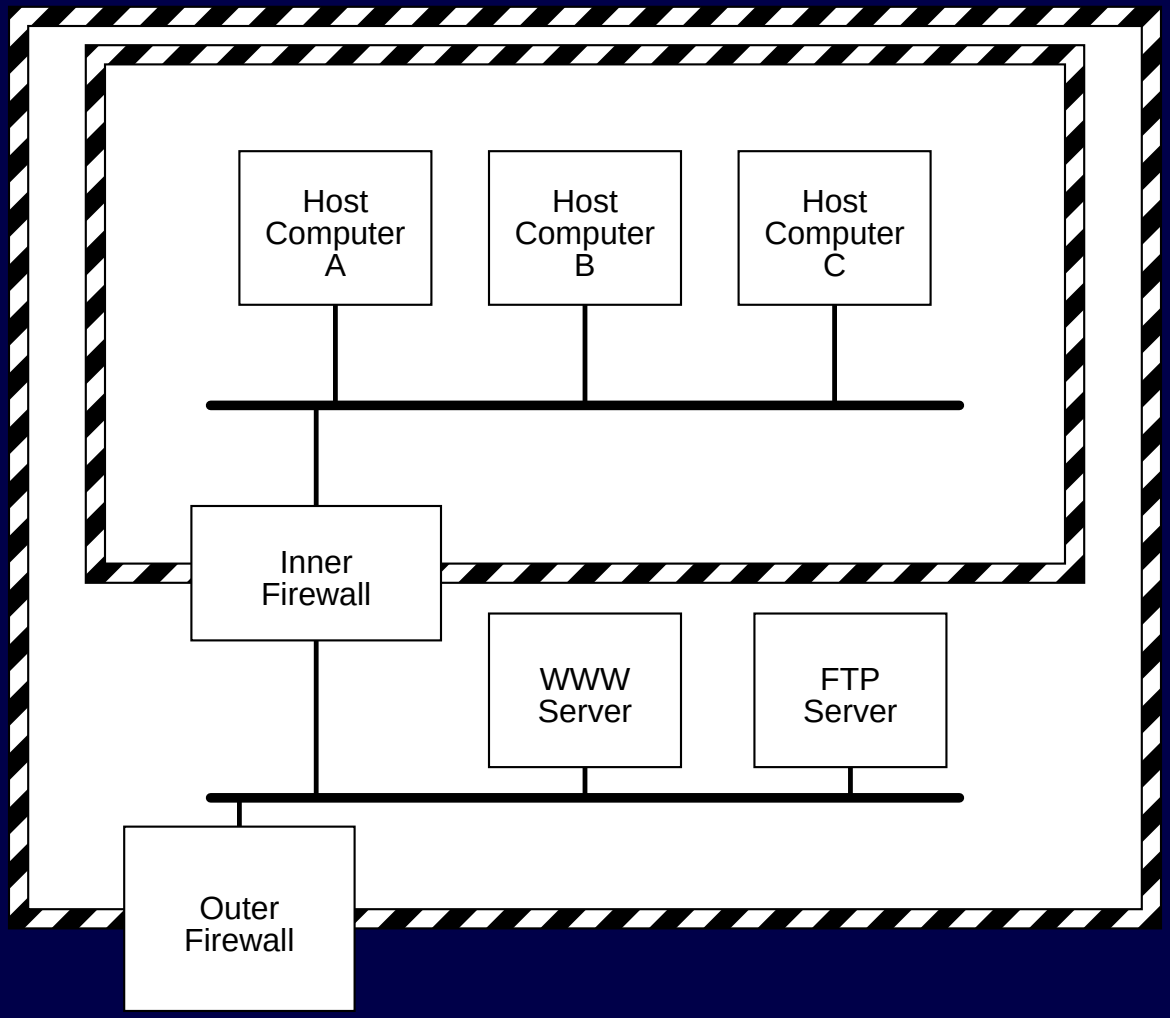
Us vs. Them –

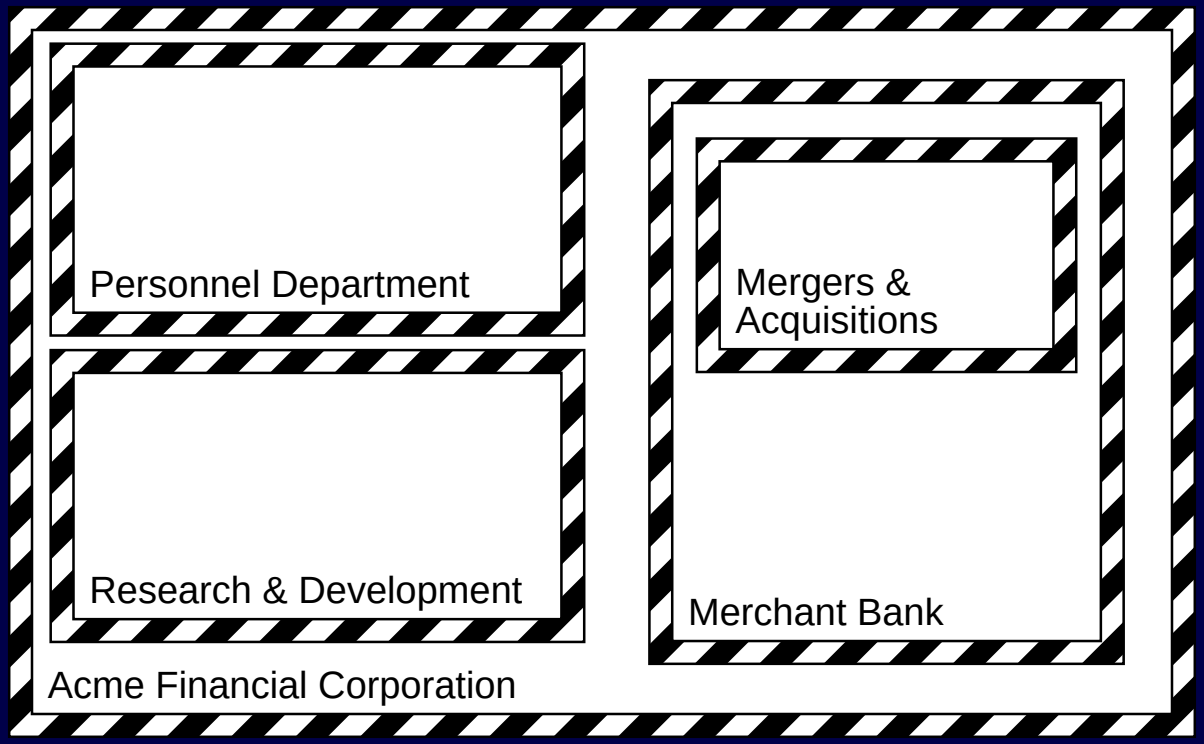
- It is not a question of inside/outside
- Who is an outsider?

Canonical Firewall Architecture

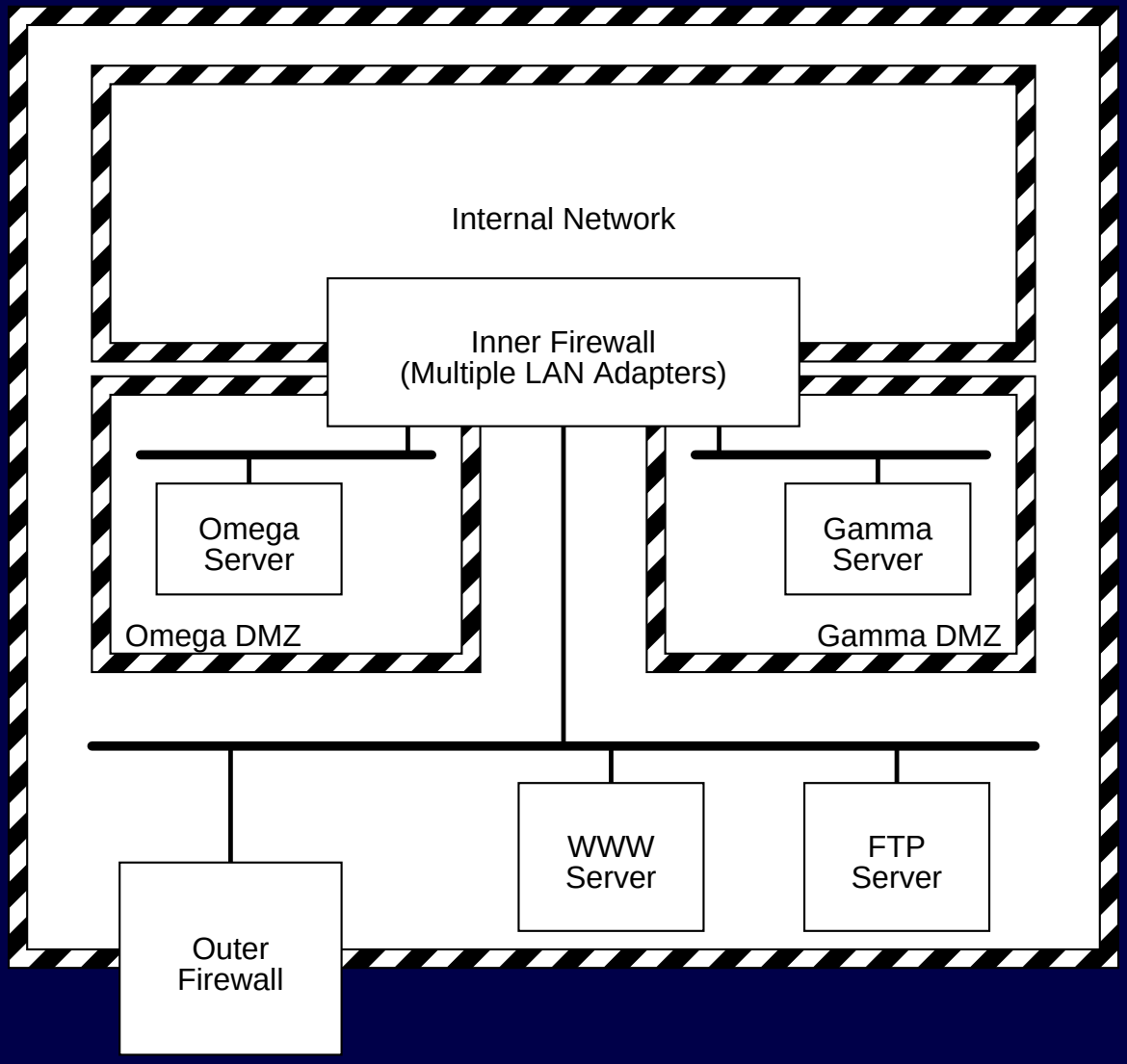


Traditional Simplistic Firewall Architecture with DMZ





Nested and Sibling Security Domains



Summary

- Security is feasible and inexpensive
- A small amount of advance planning is all that is needed
- The cost of doing privacy correctly is not high
- Certificates are easily obtained
- Litigation is expensive

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/dreamweaver/nyc/2008/websecurity.html