Trends in Internet Security

Steven M. Bellovin
smb@research.att.com
AT&T Labs -- Research

Current Trends

- “Sniffers”, enhanced sniffers.
- Active attacks.
- World-Wide Web.
- Hacking for profit.
- Denial of service attacks.
- Encryption standards.
- Strong authentication.
- Firewalls losing potency.

Sniffers

- Password collection has been going on sinc at least late 1993.
- Other uses are possible:
  - NFS file handle collection
  - Credit card numbers
  - DNS spoofing

Active Attacks

- IP spoofing.
- Session hijacking possible with canned programs.
  - Requires eavesdropping ability.
  - Canned programs seem to be avaible.
- Cryptographic stunts.
  - None yet, but...

More Active Attacks

- DNS cache contamination
  - Exploit script widely available
  - Was done for commercial purposes; fight well-publicized
- False route advertisements
  - Given a recent well-publicized accidental incident, a deliberate version seems likely.

IP Spoofing

- Attack described in a 1985 paper by Morris.
- First known use against Tsutomu Shimomura --bu it's hard to detect.
- Attacks are escalating; the problem did *not* vanish with Mitnick's arrest.
- At least two different implementations in use.
- Cryptographic authentication is a strong defense, is rarely used.
- A simpler defense has been developed, but it is no yet widely deployed.

Implications of Active Attacks

- Remote login is no longer secure, even whe protected by hand-held authenticators.
- Login through a firewall is not safe, either.
- Other protocols are subject to similar attack

World-Wide Web

- By far the fastest-growing service on the Internet.
- Traffic grows by 20% per *month*.
- Potentially a serious security threat to both clients and servers.

Web Problem Areas

- Complex administration: easy to get wrong
  - It took one site I know of three tries to get even simple access controls correct.
- Complex structure
  - the servers try to validate source addresses; che passwords; parse file names; implement acce restrictions; switch uids (which means they must run as root); etc.
  - Scripts...

WWW Scripts

- Scripts are, in essence, programs that provide network services. Are they secure?
- Most such scripts are written by ordinary users…
- The languages used to write these scripts are ofte inappropriate. Perl5, for example, has security problems.
- The existence of these scripts implies the need fo these interpreters (and for programs they invoke especially for shell scripts) to be accessible to th Web servers.

The Web and Credit Cards

- Sniffing is easy
  - Web queries are short and very easy to monitor
  - The number is probably in one packet.
  - Credit card numbers are self-checking.
- Even if the number is protected in transit, it sitting on a Web server, in a file accessible to a Web script...

Client Problems

- The server is telling the client what to do.
- Bogus URLs can exploit buggy code.
- Plug-ins, active content, etc.

Active Content

- Outsiders supplying code to be executed on user's machine.
- Can this code be trusted?
- Can it be contained?
- How can we give active content enough power to be useful, while still keeping it safe?
  - Can users administer fine-grained controls?

Java

- Nominally runs in a “sandbox”
- Relies on very complex model to ensure security.
  - But at least Sun did try to address the problem.
- Many bugs have been found.
- Code signatures being added.

ActiveX

- No execution-time protection.
- Sole security is digital signature.
  - Is the provider really trustworthy?
  - Was the provider hacked?
  - Has the user correctly validated the certificate chain (I.e., `MICROSOFT.COM` vs. `MICR0S0FT.COM`, or `NASA.GOV` vs. `NASA.COM`)?

Javascript

- Javascript can do almost anything the end-user can do -- the human is out of the loop
- No simple protection model.
- Both design and implementation bugs have occurred, by both Netscape and Microsoft

Hacking for Profit

- A vendor reports prices changed on a Web page.
- One ISP was hacked by a competitor
- At least two customers on pay-per-packet n were targets of packet storms.

Denial of Service Attacks

- Attacks don't break in, but they deny you access to your own resources.
- Several recent incidents reported; more are likely.
- Defending against such attacks is *very* hard If it's cheaper for the attacker to send a message than for you to process it, you lo

Encryption

- Starting to be deployed.
- Standards still in a state of flux, though tha
  improving rapidly.
- Has been held up by patent issues and expo
  restrictions.
- *Not* a panacea; an encrypted channel to a
  buggy program will still let hackers in.

Firewalls

- A barrier between “us” and “them”.
  - “They” may be another part of the same compa
- Limit communication to the outside world.
- Firewalls work because only a few machin running a few services are exposed to attack.

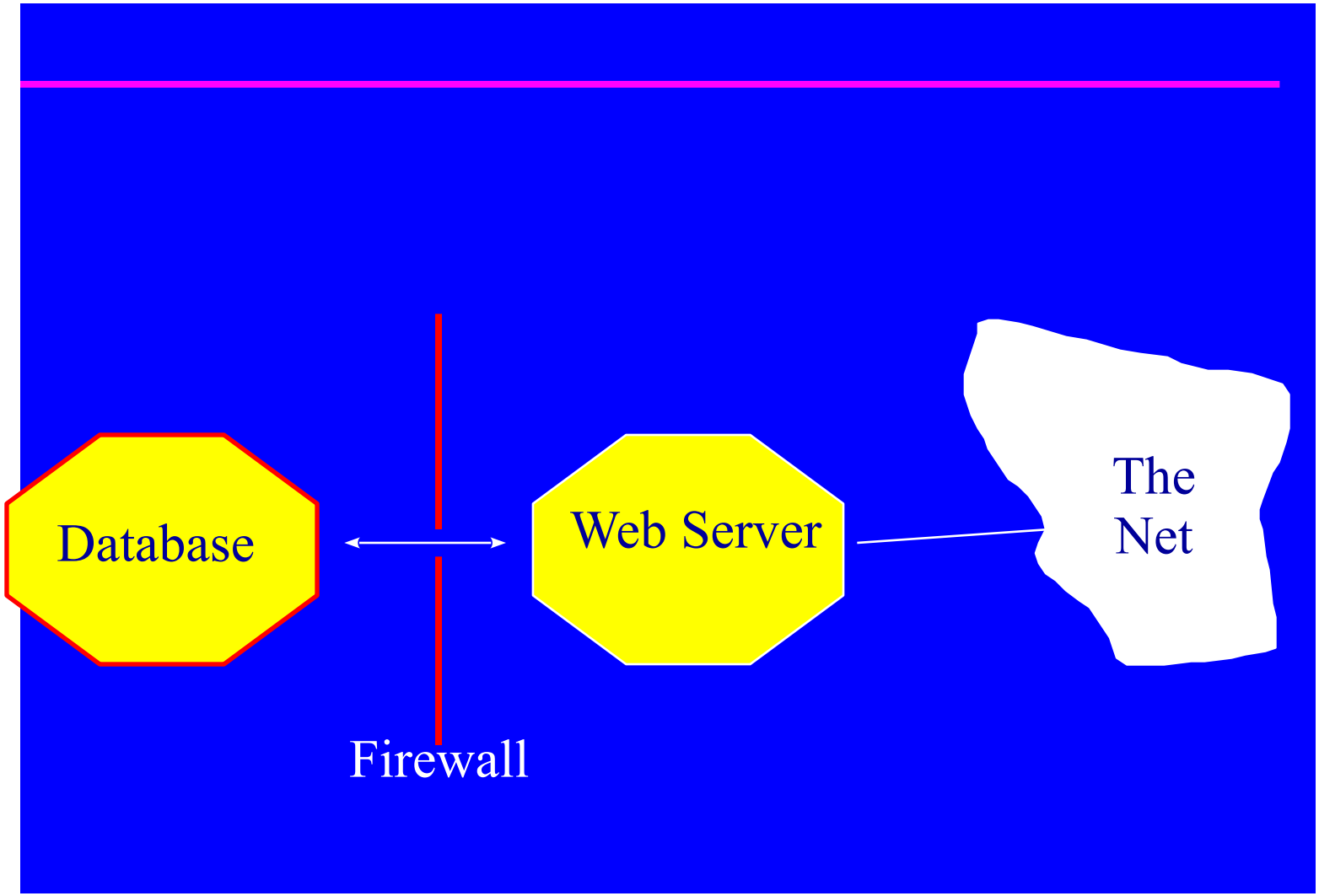
How to Use Firewalls

- Large corporate-scale firewalls are dinosau
- They are best used as one element of a tota security structure.
  - Shield legacy systems and system components that cannot economically protect themselves.
- Placement is critical.

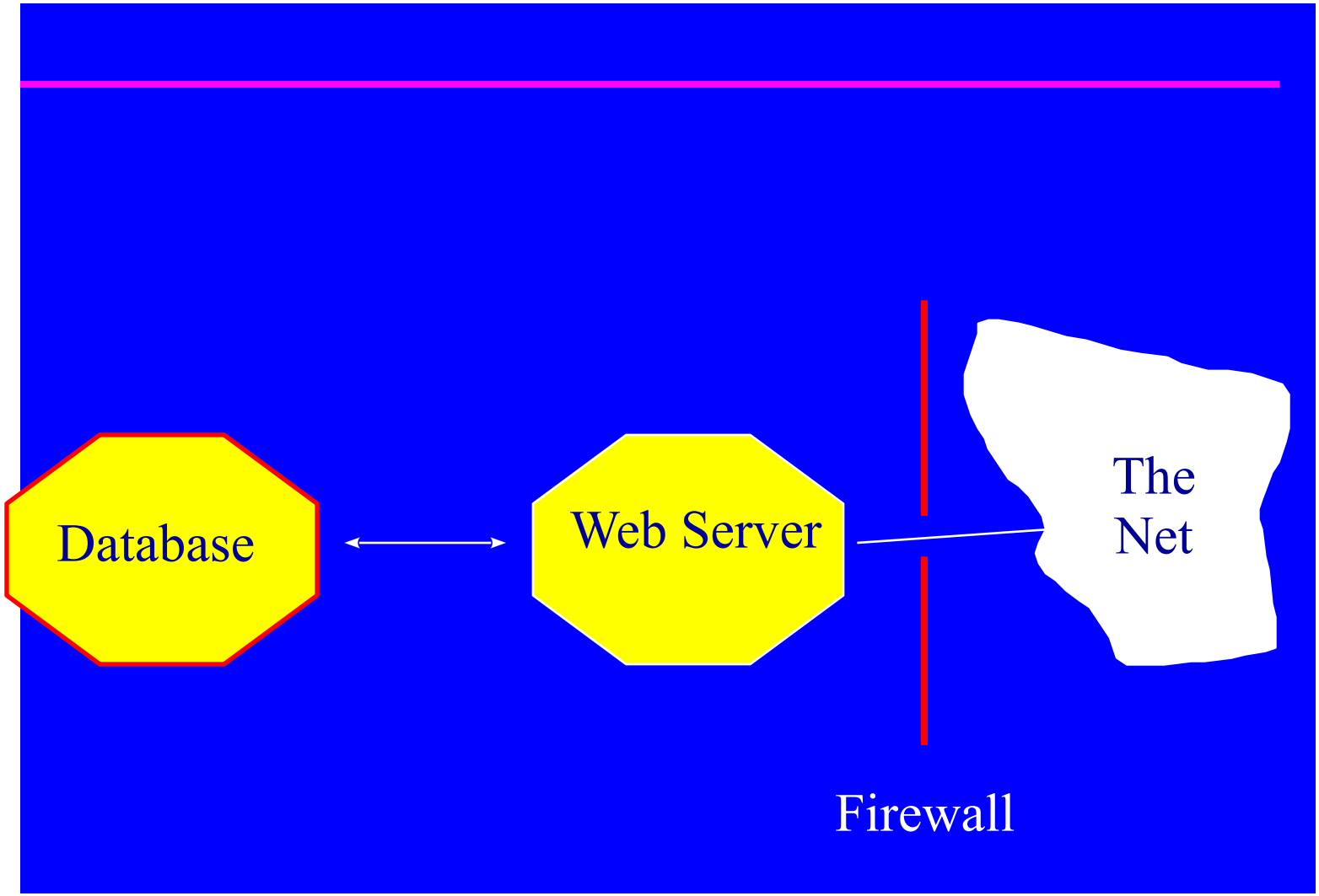
Why Are Firewalls Dying?

- There is too much connectivity that bypass the firewall.
- Too many protocols are being allowed through the firewall.
- There is too much “transitive trust” -- trust machines that have their own connections untrustworthy parties.

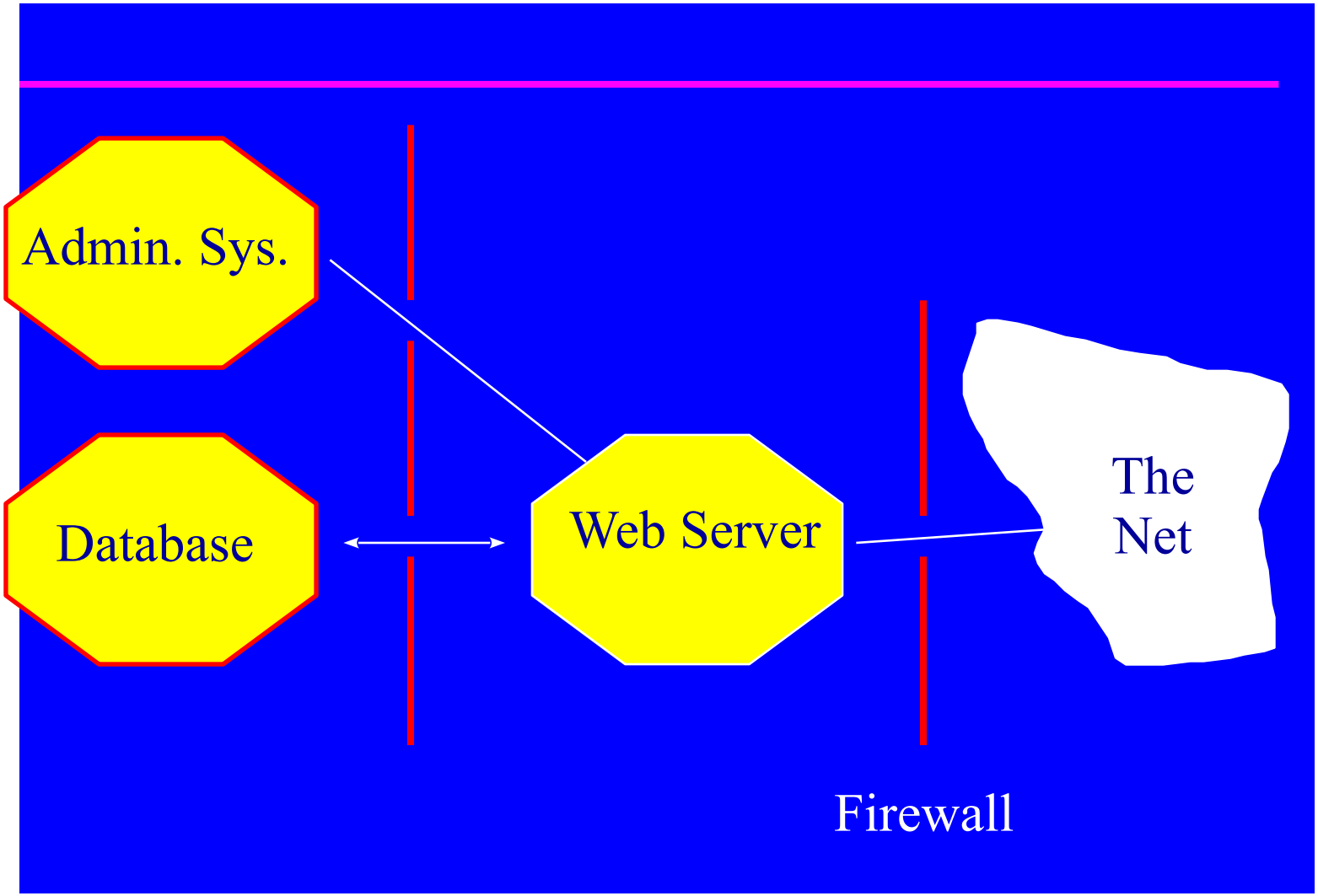
Firewalls and Databases



The Wrong Choice



Other Channels



Limitations of Firewalls

- Cannot protect against inside attacks.
- Increased interconnectivity makes attacks from inside -- though not necessarily by *insiders* -- more likely.
- Cannot block attacks at higher level of the protocol stack.

Hacker Trends

- Increased sophistication of attacks.
- Copious “cookbooks” and packaged kits.
- Great emphasis on operational security.
- Most “hackers” aren’t worthy of the name.
  - A few are *very* good.
- The hackers share tools and knowledge mo than the good guys do.

Should Businesses Disconnect?

- There are risks in doing anything. Even doing nothing carries risks.
- There are no guarantees of absolute safety.
- The trick is to *manage* the risk.

Where to From Here?

- We *must* deploy strong cryptography, as so
  as possible.
- We need more secure hosts.
- Smaller, “point” firewalls will continue to b
  useful.