A Survey Of Web Security

Aviel D. Rubin
Daniel E. Geer Jr.

- "...with an internationally connected user network and rapidly expand Web functionality, reliability and security are critical."

Outline

- Server and host environments security
- Mobile code security
- Data transport security
- Anonymity and privacy

Server security

- Configuration basics
- Setting up roots
  - Server root & Document root
  - Which user should the web server run as
- Server-side include

Server security (continued)

- Authentication
  - Basic authentication
  - Digest authentication
- Scripting
  - Non-script-aliased CGI & Script-aliased CGI
  - Scrub user input carefully

Securing the host

- Audit the host system regularly
- Notice host security bulletins and recent intrusions reported

Securing data transport

- Secure Socket Layer
  - A application-layer security protocol
    - Initial handshake (PKI)
    - Opaque data mode (Symmetric Key)
    - Closing handshake
  - A generic security protocol
  - A problem of SSL

Q: Why not use public-key to encrypt data but symmtric key?

Mobile code security

- Sandbox limits the executable's privileges
- Code signing checks whether the executable is trustworthy
- Firewall limits the programs a client can run based on the executable's properties

Anonymity and privacy

- Mixes are suited to anonymous e-mail
- Proxy rewrites client requests
- Crowds provide some formal guarantees of anonymity

Conclusion

- "...use of web for business will inevitably result in a more serious approach to security."
- Public-key infrastructure tends to be skeleton of Web security