WWW Problems

Steven M. Bellovin

smb@research.att.com

908-582-5886

AT&T Labs Research

Murray Hill, NJ 07974

Web Security — What Does it Mean?

- Client security.
- Transmission security.
- Server security.
- Server host security.

Client Security

- Can the client be subverted by the server?
- What about Java, Javascript, ActiveX, plug-ins, helper applications?
- Are browsers overly complex?
- What about pre-existing problems via a different vector, i.e., password-sniffing viruses?

  In other words, can a malicious client lie to the server?

Transmission Security

- Currently, we have SSL and equivalents. Are they good enough?
- Is the protocol correct?
- Many people use 40-bit encryption? Is that good enough, even for casual use? (By one estimate, the capital cost of a brute-force cracking engine is $400.)
- How good is the certificate chain? How well do users check?
- What about `microsoft.com` versus `MICROSOFT.COM`? Should it be `nasa.gov` or `nasa.com`?

Server Security

- Is the HTTP server secure?
- Are all the access control mechanisms set up properly? (It took one site that I know of three tries to get even simple access controls right.)
- Are all the complex CGI scripts correct?
- In a pay-for-play world, is one user attacking the others?
- Are “servlets” used? Are they secure? (Hint: they're written in Java. . .)

Server Host Security

- Can someone hack into the server by other means?
- What about the databases stored on the server host? (Customer profiles, credit card numbers, information for sale?)
- Many real applications rely on a large variety of back-end systems. Can an attacker penetrate those instead?

Conclusions

- There is no single “Web security” problem.
- Rather, there are (at least) four different problems.
- The problems don't overlap much, which means we need many different solutions.
- Some of the solutions are contradictory — we may not be able to use strong cryptography if we can't trust the end-points.