

CS290i - Lecture 11

Security papers

Scalable Internet Services and Systems, Winter 2002

Thorsten von Eicken
Department of Computer Science
University of California at Santa Barbara

Implementing HTTPS

■ Securing the private key

- Problem: server needs private key, where is it stored?
- Solutions: file, typed-in, encrypted file

■ SSL accelerator devices

- Accelerator cards / network cards
- External accelerator devices

2

Personalization on Yahoo

■ Examples

- Yahoo toolbar
- Inside Yahoo search results

■ Privacy issues

- Protecting user info is important
- Need to have internal privacy champions

■ Predictability

- Allows experimentation
- Sometimes one wants the same info everyone else is getting

■ Usage patterns

- Most users never customize
- Gotta make the default good
- Many people do not understand
- Power users will do crazy things
- Learning from users is essential

3

DoS attacks

■ Inferring Internet Denial-of-Service Activity

- D. Moore, G. Voelker, S. Savage, CAIDA, UCSD
- 2001 *USENIX Security Symposium*, Washington D.C., August 2001
- Trick: use backscatter analysis

4