

Security Re-Engineering for Fun? and Profit???

Jan Jannink 10/17/02

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

1

Re-engineering Case Study

- The Napster story in and of itself is interesting
- The original engineering work was impressive
- The beta release of the new service was remarkable
- Sadly politics, litigation, business model doomed the whole enterprise

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

2

Napster

- Wildly popular peer to peer music exchange service
- Exponential growth since first beta software release in 1999
- More than 2 million simultaneous users at peak
- Early days were fun, the sky was the limit (it seemed)

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

3

RIAA & Metallica Attack

- Legal situation leads to a crossroads in early 2001
- March 2001 injunction to remove copyrighted works (notice and takedown)
- Name based file blocking mechanism added to existing service
- Subscription service due by July 2001

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

4

Business Reality

- Revenue stream needed
- Agreements with record labels needed
- Too few developers, too little time
- Temporary bandaids needed for existing service
- Secure subscription service needed for future survival

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

5

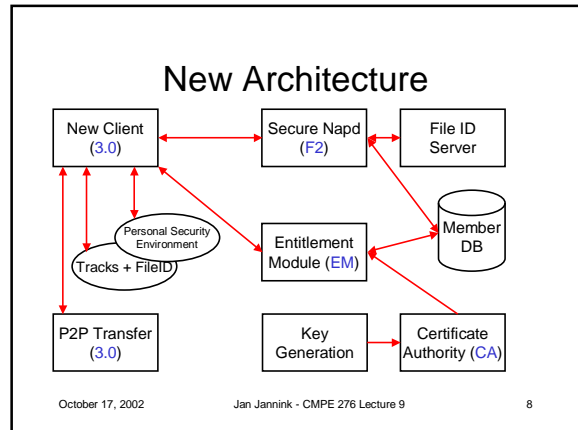
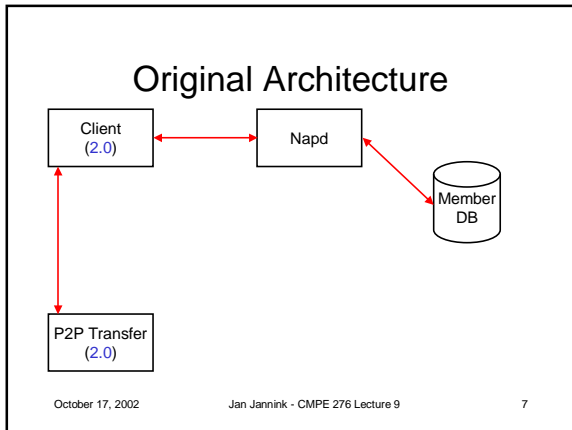
System Design

- Client supports login, IM, chat, search, & transfer functions
- Server supplies user index, song directory
- Database stores user information
- What can be done to build a business out of the system?

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

6



- ### New Bits
- User keys (public/private keypairs)
 - content is individualized
 - Certificate authority
 - user permissions are periodically renewed
 - FileID
 - audio is identified by fingerprinting
 - Entitlement module
 - download, CD burn, device export enabled
- October 17, 2002 Jan Jannink - CMPE 276 Lecture 9 9

- ### New Bits (continued)
- Secure communication
 - SSL session established with login
 - Secure file format
 - .nap based on mp3 with encryption layer
 - Secure transfer
 - files converted on the fly for new owner
 - Long term security
 - updatable anti hacking technology
- October 17, 2002 Jan Jannink - CMPE 276 Lecture 9 10

- ### Record Labels' Curveballs
- First Design
 - fixed subscription fee
 - unlimited downloads
 - May 2001 => Limited downloads
 - multiple user levels
 - unlimited playability
 - Nov. 2001 => Subscription Timeout
 - music expires with subscription
 - total number of downloads limited
- October 17, 2002 Jan Jannink - CMPE 276 Lecture 9 11

- ### Cavalry to the Rescue
- Loans from Bertelsmann
 - Subcontractors brought in:
 - billing
 - rights accounting
 - file fingerprinting
 - security (6 companies)
 - Gigabeat acquisition (15 engineers)
 - IP & rapid development experience
- October 17, 2002 Jan Jannink - CMPE 276 Lecture 9 12

S_(pending) O_(ther) P_(eoples') M_(oney)

- Critical elements to getting the job done
 - Contract quality
 - Clear deliverables, remedies for breach
 - Project management
 - Involvement in all parts of development
 - Realistic Timelines
 - Engineering input in planning
 - Employee & contractor commitment
 - Get people to believe and buy in to plans

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

13

IT Infrastructure

- Linux servers, red hat 6.2, tthtpd
- Solaris security servers
- Cisco switches, net app storage
- Oracle 8 (solaris, linux)
- Client development (windows, mac, linux)
- Release software: cvs, perforce

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

14

Project Timeframe

- Architecture defined: End January 2001
- Coding begun: March
- Integration meeting: Mid April
- Drop dead date: Begin July
- Service shutdown: July
- Demo-able code drop: August
- First public beta: End December 2001

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

15

DRM Team's Deliverables

- Architecture & Documentation
- Subscriber Keypair Generation
- SSL & Certificate Authority
- Client Anti-Hacking & Obfuscation
- File Format & Transfer Support
- Database Redesign
- Entitlement Module
- Integration

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

16

Nuts and Bolts

- Performance considerations
 - pre-generating RSA keys
 - asynchronous database interface
 - limit interserver communications
- Don't reinvent the wheel
 - SSL
 - standard public key infrastructure (CA)
 - PGP style mp3 encryption

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

17

Functionality Encapsulation

- Database API implemented with stored procedures
 - DB performance tuning won't break system
 - design DB access to minimize real-time reliance on persistent data
 - use DB strengths: transactions/persistence
- Swappable security modules
 - cat and mouse game with hackers
 - future developments difficult to predict

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

18

When Modularity isn't Good

- Clean coding style can be a drawback
 - if a category of code users is malicious
- Need a tight knit team of twisted minds to develop the security code
 - benefits: reverse engineering is tough
 - drawbacks: maintenance is tough (costly)
- Design build system for anti-hacking
 - every compile produces different code

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

19

Engineering Practices

- Well defined work products
 - flesh out the specs as much as possible
 - API's between teams are critical
- Integration team well versed in specs
 - need constant interaction for spec updates
 - updates are a de facto part of the process
- Design for the long term
 - latent design flaws are very painful to fix

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

20

Key Elements for Success

- Top quality release engineer
 - package components for deployment
 - document correct system upgrade
- Engineering exec who understands people
 - focus team on common goals
- Quick feedback to resolve glitches
 - person with system-wide understanding

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

21

Conclusion

- Real world software engineering projects are as much about people as they are about code
- Successful engineering does not make a successful company, but even then it still can be personally rewarding
- Paradoxically, both attention to details and global vision are critical

October 17, 2002

Jan Jannink - CMPE 276 Lecture 9

22