Let's Play Poker: Effort and Software Security Risk Estimation in Software Engineering

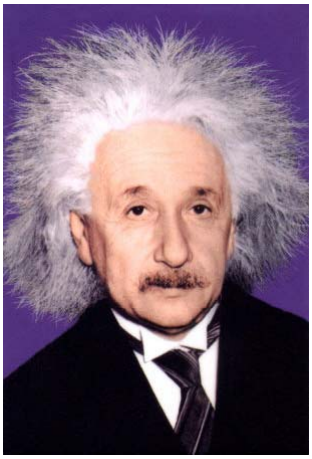
Laurie Williams
williams@csc.ncsu.edu

Picture from http://www.thevelvetstore.com

Another vote for…

"Everything should be made as simple as possible, but not simpler."

--Albert Einstein



http://images.ash.allposters.com/images/pic/CMAG/956-037~Albert-Einstein-Posters.jpg

Two Kinds of Estimation

Pictures from http://www.doolwind.com , http://news.cnet.com and http://www.itsablackthang.com/images/Art-Sports/irving-sinclair-the-poker-game.jpg

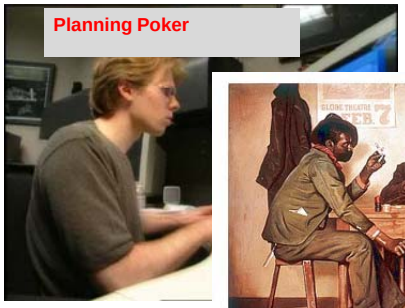
Estimation

Pictures from http://www.doolwind.com , http://news.cnet.com and http://www.itsablackthang.com/images/Art-Sports/irving-sinclair-the-poker-game.jpg

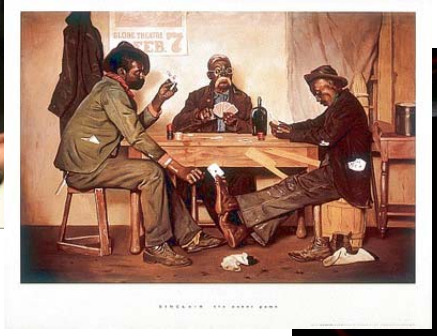
Estimation

Pictures from http://www.doolwind.com , http://news.cnet.com and http://www.itsablackthang.com/images/Art-Sports/irving-sinclair-the-poker-game.jpg

Estimation



Planning Poker

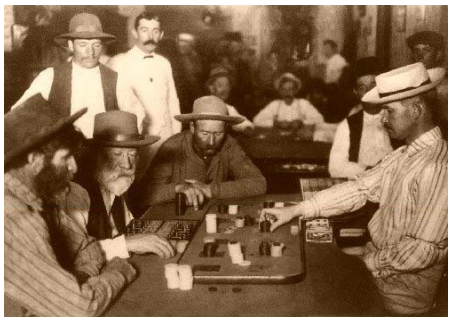


Protection Poker

Pictures from http://www.doolwind.com , http://news.cnet.com and http://www.itsablackthang.com/images/Art-Sports/irving-sinclair-the-poker-game.jpg

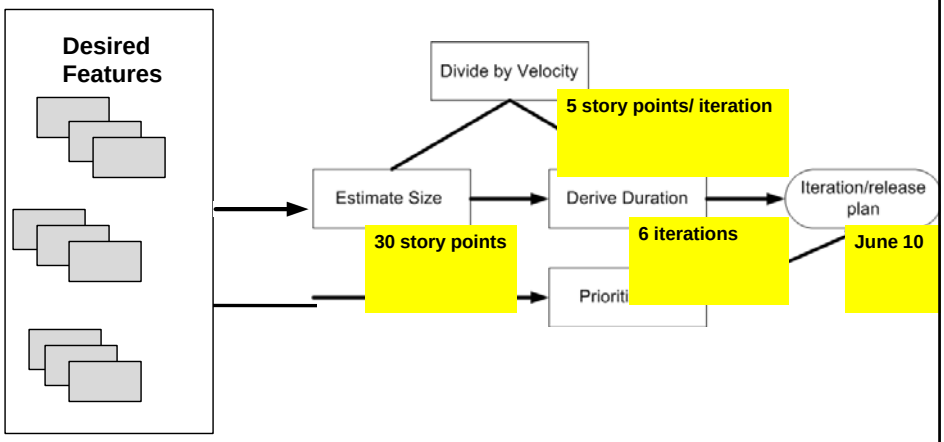
Effort Estimation: Planning Poker

How many engineers?
How long?



Pictures from http://www.doolwind.com , http://www.legendsofamerica.com/photos-oldwest/Faro2-500.jpg

Coming up with the plan



Estimating "dog points"

- **Estimate each of the dogs below in dog points, assigning each dog a minimum of 1 dog point and a maximum of 10 dog points**
- **A dog point represents the height of a dog at the shoulder**
  - **Labrador retriever**
  - **Terrier**
  - **Great Dane**
  - **Poodle**
  - **Dachshund**
  - **German shepherd**
  - **St. Bernard**
  - **Bulldog**

Estimating "dog points"

- **Estimate each of the dogs below in dog points, assigning each dog a minimum of 1 dog point and a maximum of 10 dog points**
- **A dog point represents the height of a dog at the shoulder**
  - ~~**Labrador retriever**~~
  - **Terrier**
  - ~~**Great Dane**~~
  - **Poodle**
  - **Dachshund**
  - **German shepherd**
  - **St. Bernard**
  - **Bulldog**





What if?

- Estimate each of the dogs below in dog points, assigning each dog a minimum of 1 dog point and a maximum of 100 dog points
- A dog point represents the height of a dog at the shoulder
  - Labrador retriever
  - Terrier
  - Great Dane
  - Poodle
  - Dachshund
  - German shepherd
  - St. Bernard
  - Bulldog

Harder or easier?

More or less accurate?

More or less time consuming?

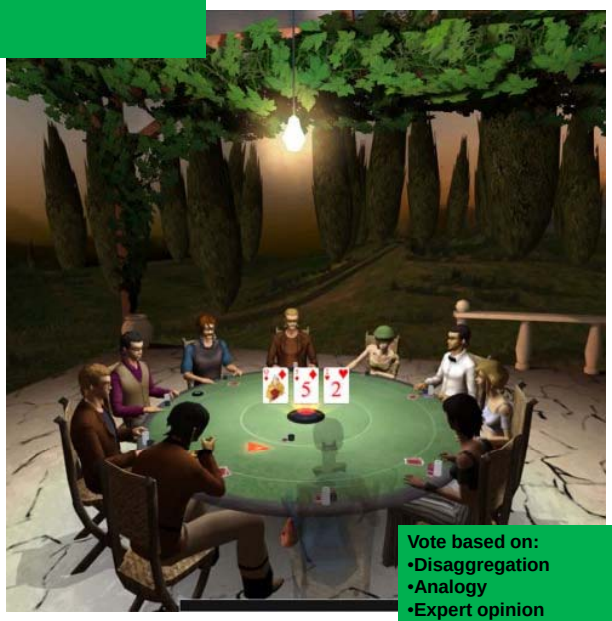
Estimating story points

- Estimate stories relative to each other
  - Twice as big
  - Half as big
  - Almost but not quite as big
  - A little bit bigger
- Only values:
  - 0, 1, 2, 3, 5, 8, 13, 20, 40, 100

Near term iteration "stories"

A few iterations away "epic"

Diversity of opinion is essential!



Vote based on:
- Disaggregation
- Analogy
- Expert opinion

(Subjective) Results of Planning Poker

- **Explicit result (<20%):**
  - Effort Estimate
- **Side effects/implicit results (80%+):**
  - Greater understanding of requirement
  - Expectation setting
  - Implementation hints
  - High level design/architecture discussion
  - Ownership of estimate

Security Risk Estimation: Protection Poker

What is the security risk?

http://news.cnet.com and
http://swamptour.net/images/ST7PokerGame1.gif

Software Security Risk Assessment via Protection Poker

		Ease	
		Difficult to Exploit	Easy to Exploit
Value	Low Impact	Lowest Priority	
	High Impact		Highest Priority

Computing Security Risk Exposure

Traditional Risk Exposure	probability of occurrence	X	impact of loss

Ease points **Value points**

Protection Poker Overview

"Diversity of ideas is healthy, and it lends a creativity and drive to the security field that we must take advantage of."
-- Gary McGraw

- **Calibrate value of "assets"**
- **Calibrate ease of attack for requirements**

- **Compute security risk (value, ease) of each requirement**
- **Security risk ranking and discussion**

Picture from: http://farm1.static.flickr.com/203/488795952_9007f93c71.jpg

Diversity of devious, attacker thinking is essential!

Collaborative threat modeling and misuse case development.

Memory Jogger

Value Points

1 . .2 . . 3. . . .5. . . . 8. . . . . .13 . . . . . .20. . . . . .40 100

Low Value

High Value

Consider the **value** of the "asset" wh
likewise.

Valuable to whom?

- The Company running the software
  - How critical is the process
  - How critical is the data in th
    - Can the data be re
    - How harmful to the
- The Attacker:
  - Who would benefit from a
  - What can be done with the
  - How much can damage can
  - What is the impact of a attacker's business (e.g. w

Ease Points

1 . .2 . . 3. . . .5. . . . 8. . . . . .13 . . . . . .20. . . . . .40 100

Hard to Attack **Easy to Attack**

Consider the following as some criteria for the candidates for hardest to attack:

- Story does not create any new pages or user input fields.
- Story reduces the current number of pages or user input fields.
- Exceptions are all handled properly to prevent information leakage.

Consider the following as some criteria for the candidates to easiest to attack:

- Story adds new pages.
- Story adds new user input fields
- Story has few (or one) role(s) with significant read, write, update authority.
- Story requires a significant change in access control (permissions).
- Story provides default usernames and passwords when the product is shipped.
- Story does not enforce strong passwords.
- Story does not have any logging or logging does not identify the specific user.

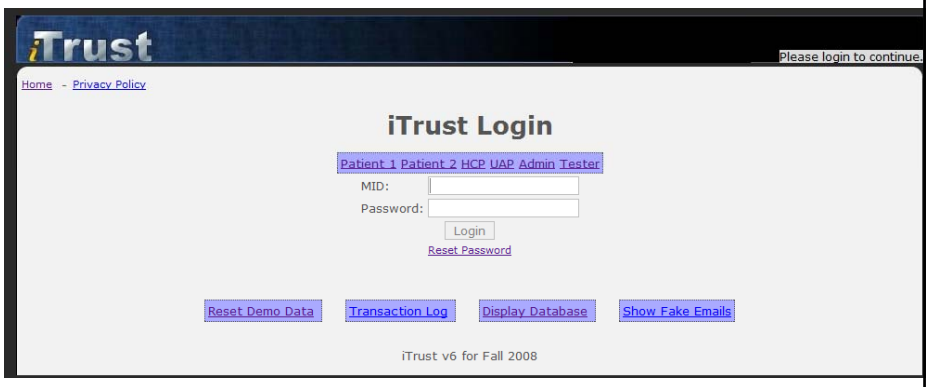
Security Risk Assessment

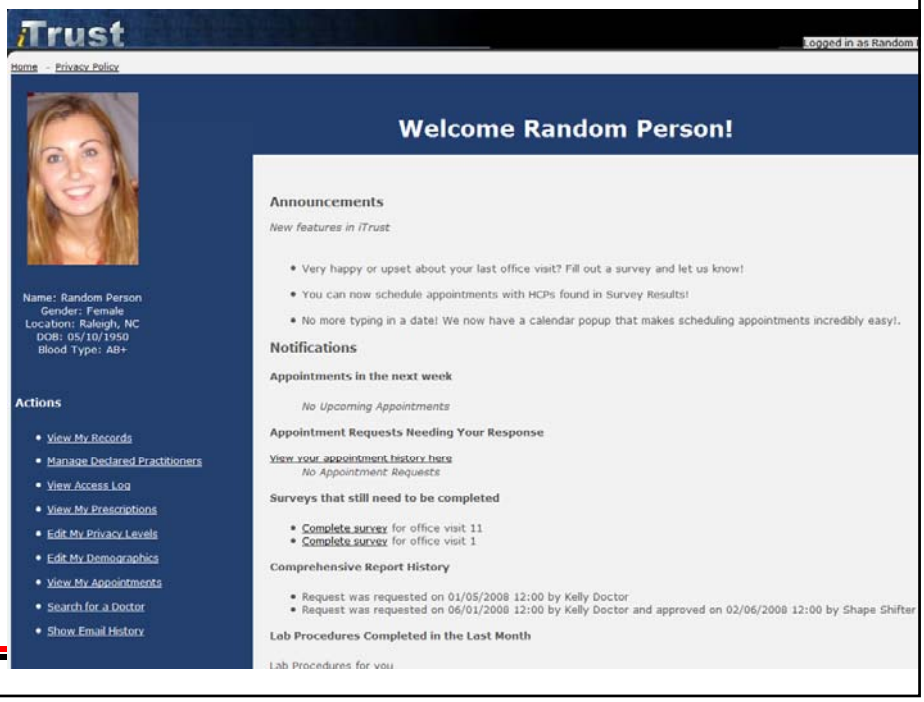
Requirement	Ease Points	Value Points	Security Risk	Ranking
Req 1	1	100	100	3
Req 2	5	1	5	6
Req 3	5	1	5	6
Req 4	20	5	100	3
Req 5	13	13	169	2
Req 6	1	40	40	5
Req 7	40	60	2400	1

Sum of asset value (e.g. one 20 and one 40)

Protection Poker High Level Overview

1. **Calibrate value of database tables**
2. **Calibrate ease of attack for requirements**
3. **Compute security risk of requirements**
4. **Security risk ranking and discussion**


iTrust
Please login to continue.
Home - Privacy Policy
iTrust Login
Patient 1 Patient 2 HCP UAP Admin Tester
MID:
Password:
Login
Reset Password
Reset Demo Data
Transaction Log
Display Database
Show Fake Emails
iTrust v6 for Fall 2008


iTrust
Logged in as Random
Home - Privacy Policy
Welcome Random Person!
Name: Random Person
Gender: Female
Location: Raleigh, NC
DOB: 05/10/1950
Blood Type: AB+
Actions
View My Records
Manage Declared Practitioners
View Access Log
View My Prescriptions
Edit My Privacy Levels
Edit My Demographics
View My Appointments
Search for a Doctor
Show Email History
Announcements
New features in iTrust
Very happy or upset about your last office visit? Fill out a survey and let us know!
You can now schedule appointments with HCPs found in Survey Results!
No more typing in a date! We now have a calendar popup that makes scheduling appointments incredibly easy!.
Notifications
Appointments in the next week
No Upcoming Appointments
Appointment Requests Needing Your Response
View your appointment history here
No Appointment Requests
Surveys that still need to be completed
Complete survey for office visit 11
Complete survey for office visit 1
Comprehensive Report History
Request was requested on 01/05/2008 12:00 by Kelly Doctor
Request was requested on 06/01/2008 12:00 by Kelly Doctor and approved on 02/06/2008 12:00 by Shape Shifter
Lab Procedures Completed in the Last Month
Lab Procedures for you

Name: Kelly Doctor
Location: CityName, NY

- Add Patient
- Edit Patient
  - Edit Representatives
  - Edit PHR
  - Edit Basic Health Information
  - Document Office Visit
  - Chronic Disease Risks
- Add UAP
- Edit UAPs
- Epidemic Detection
- Cause of Death Trends
- Office Visit Reminders

Welcome Kelly Doctor!

Announcements

New features in iTrust

- No more typing in a date! We now have a calendar popup that makes scheduling appointments incredibly easy!.

Notifications

Appointments in the next week

No UpcomingAppointments

Appointment Requests Needing Your Response

View your appointment history here

- Request from Andy Programmer reason: *none*
- Request from Andy Programmer reason: I feel sick

Comprehensive Report History

- Request was requested on 01/01/2008 12:00 by Kelly Doctor
- Request was requested on 01/02/2008 12:00 by Kelly Doctor and approved on 02/02/2008 12:00 by Shape Shifter
- Request was requested on 01/03/2008 12:00 by Kelly Doctor and rejected on 02/03/2008 12:00 by Shape Shifter
- Request was requested on 01/04/2008 12:00 by Kelly Doctor, approved on 02/04/2008 12:00 by Shape Shifter, and viewed on 03/04/2008 12:00 by Shape Shifter
- Request was requested on 01/05/2008 12:00 by Kelly Doctor
- Request was requested on 06/01/2008 12:00 by Kelly Doctor and approved on 02/06/2008 12:00 by Shape Shifter

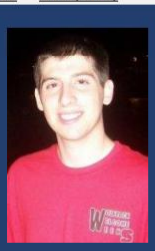
Lab Procedures Completed in the Last Month

View All Lab Procedures here

iTrust

Logged in as Shape Shi

Home - Privacy Policy



Name: Shape Shifter
Location: CityName, NY

Welcome Shape Shifter!

- Edit HCP Assignment to Hospital
- Manage Hospital Listing
- Edit CPT ProcedureCodes
- Edit ND Codes
- Edit ICD Codes
- Edit LOINC Codes
- Add HCP
- Edit Personnel
- Edit My Demographics
- Change Global Session Timeout
- View All Report Requests
- Search for a Doctor

Req 1: Emergency Responder

Currently the only roles in iTrust are licensed health care professional, unlicensed health care professional (a.k.a secretarial support), administrator and patient. The need for another role has arisen: emergency responder (ER). An emergency responder is defined as follows: police, fire, emergency medical technicians (EMTs), and other medically trained emergency responders who provide care while at, or in transport from, the site of an emergency. The only capability provided to an ER is access to an emergency report for a patient which provides basic but important information such as: allergies, blood type, recent short-term diagnoses, long term, chronic illness diagnoses, prescription history, and immunization history. The patient is sent an email to notify them of the viewing of their records by an emergency responder.

Req 2: Find qualified LHCP

A patient has just been diagnosed with a condition and wants to find the licensed health care professionals (LHCPs) in the area who have handled that condition. The patient chooses 'My Diagnoses" and is presented with a listing of all their own diagnoses, sorted by diagnosis date (more recent first). The patient can select a diagnosis and will be presented with the LHCPs in the patient's living area (based upon the first three numbers of their zip code) who have handled this diagnosis in the last three years. The list is ranked by the quantity of patients the LHCP has treated for that diagnosis (each patient is only counted once regardless of the number of office visits).

Req 3: Update diagnosis code table

The American Medical Association has decided that beginning January 1, 2010 all diagnoses must be coded with ICD-10 rather than ICD-9CM. These new codes need to be saved for eventual use by the iTrust application.

Req 4: View access log

A patient can view a listing of the names of licensed health care professionals that viewed or edited their medical records and the date the viewing/editing occurred is displayed.

Step 1: Calibrate value of database tables

- **Which iTrust database table would be least attractive to an attacker?**
- **Which iTrust database table would be most attractive to an attacker?**
- **Use your planning poker cards to assign relative point values for the "value" of each database table, giving a 1 to the least attractive.**
- **Circle the database tables in Table 1 and put the value points in the appropriate column.**
- **There are your "value" endpoints for the rest of the exercise.**
- **At this time, do not assign a value to all the other tables.**

Step 2: Calibrate ease of attack for requirements

- **Which requirement adds functionality that will make an attack easiest?**
- **Which requirement adds functionality that will make attack hardest?**
- **Use your planning poker cards to assign relative point values for the "ease" of each requirement.**
  - **Easy to attack: high number**
  - **Hard to attack: low number**
- **Record ease values in Table 3.**
- **There are your "ease" endpoints for the rest of the exercise.**
- **At this time, do not assign a value to all the other requirements.**

Step 3: Compute security risk of requirements

- **For each requirement:**
  - **Identify database tables used in that requirement and record in Table 2. For each:**
    - » **Table already have a "value"? Use it.**
    - » **Table doesn't have a "value"? "Poker" a value and put it in Tables 1 and 2**
  - **Put sum of all database values in Table 3.**
  - **"Poker" a value for ease points for each requirement and record in Table 3.**
  - **Compute security risk in Table 3 by multiplying value by ease.**

Step 4: Risk Ranking and Discussion

- **Rank your risks.**
- **Any surprises? Satisfied with values you gave?**
- **What plans would you put in place now that you are more aware of the security risk?**

Anticipated Results of Protection Poker

- **Explicit result (20%):**
  - **Relative security risk assessment**
- **Side effects/implicit results (80%):**
  - **Greater awareness understanding of security implications of requirement**
  - **Allocation of time to build security into new functionality "delivered" at end of iteration (appropriate to relative risk)**
  - **Knowledge sharing and transfer of security information**