Causes of (in)security in decisions

- Cognitive limitations
- Rewards and outcomes
- It's all about risk
- Garbage in, garbage out

- What to do?
It’s all in your head

Let’s look at the individuals first

Houston, we have a problem

- Users do not think they are at risk
- Users aren’t stupid, they are unmotivated
- Safety is an abstract concept
- Feedback and learning from security-related decisions is weak

R. West “The Psychology of Security”, 2008 (CACM)
Houston, we have a problem

- Making trade-offs between risk, losses, gains and costs
- Users are more likely to gamble on a loss than accept a guaranteed loss
- Losses are perceived disproportionately to gains
- Security is a secondary task

R. West “The Psychology of Security”, 2008 (CACM)

Users do not think they are at risk

- People tend to believe that they are less vulnerable than others. This includes a wide range of scenarios from consumer products to health to computer security
- Thus, why patch/firewall/antivirus…? Nothing bad can happen
Users aren’t stupid, they are unmotivated

- Cognitive miser = limited capacity for information processing
- Thus, multitask and rely on heuristics...
  - … which bring good outcomes MOST of the time
- What do you do when a warning pop-up shows on the screen?

Safety is an abstract concept

- Concrete outcomes dominate abstract
  - Yet, “secure” choice frequently has no visible outcome or visible threat
  - Thus, click that link!
- Also, fall back on the heuristics
Feedback and learning

- Typical learning: do something right, get a reward. Do something wrong, get a penalty
- Security: do something right, and nothing bad happens
- Security: do something wrong, and the negative impact is not immediate or direct

- Thus, learning of consequences is difficult

Gain\loss tradeoffs

- Scenario 1: guaranteed GAIN of $5 versus a coin toss with the outcomes $0, $10
Gain\loss tradeoffs

- Scenario 2: guaranteed LOSS of $5 versus a coin toss with the outcomes $0, -$10

---

Gain\loss tradeoffs

R. West "The Psychology of Security", 2008 (CACM)
Other factors of gains\losses

- Scale – people do not conceptualize very large or very small magnitudes well
- Probability – generally hard to estimate, but the magnitude is also a problem (particularly small one)

Look out!

- Average number of deaths in a year caused by…

---

---
Look out!

- Average number of deaths in a year caused by...

< Image of a shark >

Look out!

- Average number of deaths in a year caused by...

< Image of a snake >
Look out!

- Average number of deaths in a year caused by…

5.5

Look out!

- Average number of deaths in a year caused by…
Look out!

- Average number of deaths in a year caused by…

53

Look out!

- Average number of deaths in a year caused by…
Look out!

- Average number of deaths in a year caused by...

130

Data from http://historylist.wordpress.com/2008/05/29/human-deaths-in-the-us-caused-by-animals/

Yet, who are we afraid of?
Security is a secondary task

- When under time pressure, people tend to focus more on the losses affecting their immediate task

- Thus, take shortcuts, ignore policies, etc.

Losses perceived disproportionally

- When users perceive a gain and a loss to have the same value, loss is actually more motivating

- Thus, even if the cost of security effort is “small”, it may seem worse for the users
Conditional probability

Got brakes?

- Munich Taxi study (early 1980s)
- Used ABS brakes on 50% of cabs
- Accelerometers installed unknown to drivers

- Results:
  - No significant difference in accident rates
  - Cabs with ABS were driven more aggressively (acceleration, harsh stops)
  - http://www.drivers.com/article/411
A driving lesson

- British study: accidents by type of training
  A. Driving school only
  B. With friends or relatives only
  C. Combined training

- Atlanta, DeKalb County, Georgia - similar variation by the number of training hours (Safe Performance Curriculum, basic training, no formal training)

A driving lesson

- British study: results (km driven per accident)
  A. 19,392
  B. 22,801
  C. 14,536

- Atlanta, DeKalb County, Georgia
  - No significant difference in crashes for minimal training or no formal training
  - MORE accidents for SPC

http://psyc.queensu.ca/target/chapter/06.html
Risk Homeostasis Theory

- In all activities, people balance subjective estimates of risk with the benefits they are hoping to receive.

- There may be such thing as “too little risk”
  - i.e., “optimal” risk level is not equal to zero.

---

Controls?

Fundamentally, only THREE countermeasures are available to protect critical information infrastructures.
Solutions

- Technical
  - Doesn’t look like it’s working – from ABS to antivirus
- Policies/processes (enforcement)
  - Sometimes it’s working, if the rewards are positive
  - Beware of reactance; reciprocity
- People-oriented (education)
  - Sometimes it’s working, if it focuses on positive reinforcement and simple messages
  - Beware of building overconfidence

Miles Edmundson, RSA talk http://www.youtube.com/watch?v=InVAtzklpFc

Strength in numbers

Corporate decision making
Ways of dealing with risk

- Accept
  - “Do nothing” – does not mean being oblivious to risk!
- Transfer
  - Legal agreement, insurance, pooling arrangements
- Mitigate
  - Implement countermeasures yourself
Qualitative versus Quantitative Risk Assessment

- It is impossible to conduct risk management that is purely quantitative.
- Usually risk management includes both qualitative and quantitative elements, requiring both analysis and judgment or experience.
- It is possible to accomplish purely qualitative risk management.

Qualitative risk assessment

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Med. risk</td>
<td>High risk</td>
</tr>
<tr>
<td>Low risk</td>
<td>Med. risk</td>
</tr>
<tr>
<td>Low risk</td>
<td>Low risk</td>
</tr>
</tbody>
</table>

Likelihood

Impact
Quantitative risk assessment

- ALE = ARO x SLE
  - SLE = AV x EF

  - ALE = Annualized loss expectancy
  - ARO = Annual rate of occurrence
  - SLE = Single loss expectancy
  - AV = Asset value
  - EF = Exposure factor

Is there something wrong with this approach?

Economics, rationality and risk

- What is “economic rationality”?

- What is “rational” attitude towards risk?

- Alternative theories of risk
  - Value at risk
  - Ruin theory
  - Info-gap decision theory
Meanwhile, on the dark side...

Black market at work

Zeus

- Accounted for about 50% of all financial information stolen in 2009-2010
- Basic configuration tool sold for $700, versions with updates(!) and support(!!!!) sold for up to $15,000
- Highly customizable
- 55% of infected machines had up-to-date antivirus (effective detection rate of 23% - Trusteer 2009)
Zeus is dead? All hail SpyEye!

- Competition between trojans
- Zeus writer announced “retirement” in Oct. 2010
- Word was that SpyEye writers bought out Zeus
- Zeus source code leaked to public in May’11

- In March 2011, there were 230 verified SpyEye C&C servers, 25 with files online
- Average detection rate by antivirus is 29.72% (malwarehelp.org)
Evolution of Zeus and SpyEye

- Variants for Android, Blackberry platforms
- Capable of bypassing two-factor authentication (e.g., via intercept of text messages)
- Intercepting bank web pages and presenting fake account balances in the browser

Designing effective controls

Workflows and Social Networks
Overview

- Personal data can be stolen by employees
- Knowledge of partial information can lead to derivation of further information
- Sometimes knowing a specific value is dangerous
- Workflow manipulation
- All of this is made easier with electronic records and the Internet

Examples from Reality

- CNN, 2008: passport files of former president Clinton, and then candidates Obama and McCain accessed without authorization by State Department contractors
- Coombes, 2008: IRS employee sentenced for snooping into tax data for almost 200 people (including celebrities)
- Mohajer, 2008: former UCLA employee sold medical data of celebrities to tabloids
- Since 2003: records of 1000 patients involving 165 hospitals inappropriately accessed
- Lemos, 2009: hackers used location where Sarah Palin and husband met to access her Yahoo e-mail account via the “secret question”
US Government Response

- Federal Information Security Management Act (FISMA) for federal agencies
- Gramm-Leach-Bliley Act (GLBA) for financial services
- Health Insurance Portability and Accountability Act (HIPAA) for healthcare sector
- Agencies that handle individual’s personal information bear the burden of safeguarding information
- Compliance is non-trivial and a creative process

Operational Model of Security

- Protection = Prevention + Detection + Response

- Three classes of controls:
  - Preventive – stop bad things from happening
  - Detective – identify security breaches
  - Corrective – stop the breach, restore to a secure state
Traditional Approach

- Access controls based on roles of agents in the system
- Identifies access privileges to information
- Does not capture the dynamic nature of the workflow

Our Approach

- A well-designed business workflow able to provide processing capacity and information protection at the same time
- Optimizing employee assignment given the security constraints
- Capture potential conflicts
- Trade-off efficiency with conflicts
- May be hard or soft constraints
Modeling Concepts

- **Tasks**
  - Elemental tasks are conflict-free
- **Skill qualifications**
  - Some tasks require specialized employees
- **Authority levels**
  - Some tasks cannot be performed by employees with a lower level of authorization
- **Conflicts**
  - Between specific values, attribute groups, and/or history
- **Dynamic elements**
  - Loops, forks
- **Efficiency**
  - Employees utilization, order waiting time

Online Pharmacy
Tasks and Access

- P: pharmacist, T: technical staff, N: non-technical staff, A: accountant

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Information Access</th>
<th>Skill Qualification</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Order Entry</td>
<td>Order and patient demographic data</td>
<td>P, N, T, A</td>
</tr>
<tr>
<td>T2</td>
<td>Credit and Compliance Check</td>
<td>Client credit information, payment history</td>
<td>P, T</td>
</tr>
<tr>
<td>T3</td>
<td>Fulfill Order</td>
<td>Medication information</td>
<td>P, T</td>
</tr>
<tr>
<td>T4</td>
<td>Pharmacist’s Assessment</td>
<td>Medication history</td>
<td>P</td>
</tr>
<tr>
<td>T5</td>
<td>Shipping and Handling</td>
<td>Address Information</td>
<td>P, N, T, A</td>
</tr>
<tr>
<td>T6</td>
<td>Billing</td>
<td>Insurance and payment information</td>
<td>P, N, T, A</td>
</tr>
<tr>
<td>T7</td>
<td>Update Ledgers</td>
<td>Accounting Information</td>
<td>A</td>
</tr>
</tbody>
</table>

Security Conflicts

- Fraud concerns:
  - T2 and T6 -> access to name, address, credit status + billing records (fake invoices)
  - T3 and T6 -> asset misappropriation covered by billing

- Privacy concerns:
  - T3 and T5 -> access to customer address and name + medication (compromise of patient’s medical status)
  - T2 and T5 -> gender + address (some females are sensitive to disclosing this type of information)
Employee Parameters

<table>
<thead>
<tr>
<th>Employees</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
<th>T4</th>
<th>T5</th>
<th>T6</th>
<th>T7</th>
<th>Skill</th>
<th>Cost/Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infin</td>
<td>9</td>
<td>10.5</td>
<td>11</td>
<td>5</td>
<td>11</td>
<td>11</td>
<td>0</td>
<td>P</td>
<td>40</td>
</tr>
<tr>
<td>Mary</td>
<td>9</td>
<td>10.5</td>
<td>10.5</td>
<td>6</td>
<td>11</td>
<td>10</td>
<td>0</td>
<td>P</td>
<td>40</td>
</tr>
<tr>
<td>Charles</td>
<td>13.5</td>
<td>13</td>
<td>12.5</td>
<td>0</td>
<td>13</td>
<td>11</td>
<td>0</td>
<td>T</td>
<td>20</td>
</tr>
<tr>
<td>Infrn</td>
<td>14</td>
<td>14</td>
<td>16</td>
<td>11</td>
<td>14</td>
<td>12.5</td>
<td>10</td>
<td>I</td>
<td>20</td>
</tr>
<tr>
<td>David</td>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>16</td>
<td>12</td>
<td>0</td>
<td>N</td>
<td>15</td>
</tr>
<tr>
<td>Robert</td>
<td>13.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>13.5</td>
<td>0</td>
<td>N</td>
<td>15</td>
</tr>
<tr>
<td>Emily</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>11.5</td>
<td>11.5</td>
<td>10</td>
<td>A</td>
<td>20</td>
</tr>
</tbody>
</table>

Optimal Assignments

<table>
<thead>
<tr>
<th>Without Security</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
<th>T4</th>
<th>T5</th>
<th>T6</th>
<th>T7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Josh</td>
<td>Mary</td>
<td>Josh</td>
<td>Mary</td>
<td>Mary</td>
<td>Robert</td>
<td>Robert</td>
<td>Emily</td>
</tr>
<tr>
<td>David</td>
<td>Charles</td>
<td>Mary</td>
<td>Mary</td>
<td>David</td>
<td>Robert</td>
<td>Robert</td>
<td>Emily</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Measure</th>
<th>Without</th>
<th>With</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Waiting Time/Order (h)</td>
<td>3.2</td>
<td>2.2</td>
</tr>
<tr>
<td>Waiting Cost/Day</td>
<td>38.7</td>
<td>26.3</td>
</tr>
<tr>
<td>Personnel Cost/Day</td>
<td>95</td>
<td>110</td>
</tr>
<tr>
<td>Total Cost per Hour</td>
<td>133.7</td>
<td>136.3</td>
</tr>
</tbody>
</table>
Optimization Model

- $M$: Number of available employees
- $N$: Number of tasks
- $x_{ij}$: Binary decision variable (1 if we assign employee $i$ to task $j$; 0 otherwise)
- $y_i$: Binary decision variable (1 if employee $i$ is assigned at least one task; 0 otherwise)
- $A_k$: Conflict set
- $s_i$: Whether or not employee $i$ is capable of doing task $j$ (skills)
- $t_k$: Whether or not employee $i$ is authorized to do tasks in conflict set $k$
- $U_i(X)$: Utilization of employee $i$
- $W(X)$: Average waiting time of an order going through the workflow

Objective Function

- $C_W$: Cost of waiting per time unit
- $a_E$: Total external arrival rate
- $c_i$: Cost of employee $i$

$$f(X,Y) = C_W a_E W(X) + \sum_{i=1}^{M} c_i y_i$$
Optimization Problem

\[
\min f(X,Y) \quad \text{Total cost per time unit}
\]

\[
\text{s.t.} \quad \sum_{j=1}^{n} x_{ij} = 1, \forall j
\]

\[
y_{i} \leq \sum_{j=1}^{n} x_{ij} \leq N_{i}, \forall i
\]

Each task assigned to exactly one employee

Employees with assigned tasks

\[
X \leq S
\]

Skill constraint

\[
U_{i}(X) < 1, \forall i
\]

Workload per employee do not exceed employee capacity

\[
\sum_{j \in A} x_{ij}(1-t_{ij}) \leq |A|-1, \forall i, k
\]

Unauthorized employees not assigned all tasks in a conflict set

\[
x_{ij}, y_{i} \in \{0,1\}, \forall i, j
\]

General Results: Naturally Secured Workflows

- Assigning all the tasks in a conflict set to the same employee makes infeasible the employee’s workload
- In the case of a single-entry point there is a computable threshold value

\[
a \geq \max_{j} \frac{1}{\sum_{j=1}^{p} \theta_{j} \mu_{j}}
\]

\[
\theta = (I - P)^{-T} c_{i}
\]

- For our online pharmacy this is about 7.49 orders/hour
General Results: Minimum Disruption

- Two scenarios after adding a new conflict set:
  - Add a new employee and assign a subset of the conflicting tasks
  - Keep same personnel and re-distribute tasks
  - Scenario 1 is better when it is possible to balance the loads between the new employee and the employee with the conflict

General Results: Efficiency

- After adding a new conflict set and a new employee, the optimal waiting cost will be lower as long as the new employee is assigned at least one task and does not replace any other employee
Assignment Strategies Comparison

Employee Load Comparison
Reassigning Versus Adding Employees

New employee is better

Reassignment is better

Conclusions
- New model and methodology to secure workflows
- High traffic is good for security
- Common sense (minimum disruption) strategies do not perform as well as optimizing
- Model not hard to implement in practice:
  - Parameters can be measured (arrival and service rates)
  - Conflict sets are not hard to create
  - Employee skills and authorization levels are given
Thank you!