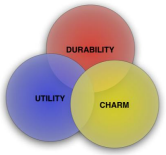
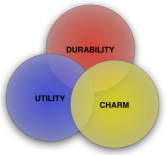


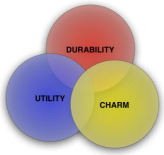
Class 5 EMTM 604

Gregg Vesonder
University of Pennsylvania
Penn Engineering - Computer & Information Science



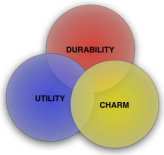
Roadmap

- Schedule
- Logbook
- Privacy Technologies
- Current readings: Schneier, chapters 9 & 15
- Other readings - automotive
- Readings next Oram & Viega, chapters 9 & 12



Security

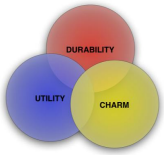
- Nearly two-thirds of U.S. companies said they have been victims of cybersecurity incidents or data breach. The number of cyber incidents reported by federal agencies over a five-year period spiked, increasing from 5,503 cyber incidents in 2006 to 41,776 in 2010, the report said. Trends point to "cyber criminals' continued focus on stealing customer records, including personally identifiable information, payment card data, email addresses, and other customer data."
- Gerry Smith – Huffington Post



Privacy

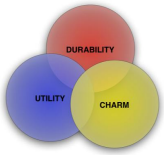
- He advised logging off sites like Google and Facebook as soon as practicably possible and not using the same provider for multiple functions if you can help it. "If you search on Google, maybe you don't want to use Gmail for your e-mail," he said.
- If you do not want the content of your e-mail messages examined or analyzed at all, you may want to consider lesser-known free services like HushMail, RiseUp and Zoho, which promote no-snooping policies. Or register your own domain with an associated e-mail address through services like Hover or BlueHost, which cost $55 to $85 a year. You get not only the company's assurance of privacy but also an address unlike anyone else's, like me@myowndomain.com.
- Or you can forgo trusting others with your e-mail correspondence altogether and set up your own mail server. It is an option that is not just for the paranoid, according to Sam Harrelson, a middle-school teacher and self-described technology aficionado in Ashville, N.C., who switched to using his own mail server this year using a $49.99 OS X Server and $30 SpamSieve software to eliminate junk mail.

http://www.post-gazette.com/stories/business/technology/how-to-muddy-your-tracks-on-the-internet-634276/



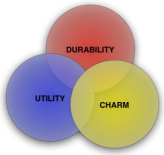
Sentiment Analysis

- IBM has unveiled a new security tool designed to help bosses seem out "disgruntled" employees who may leak company secrets or act disloyally.
- The tool uses Big Data to scan emails, financial transactions, Web visits, and even social media activity to help companies root our disloyal employees who may pose a threat to the company. The tool can even spot an employee who "expresses something upbeat to a manager and portrays things differently to a peer, parsing language patterns to determine if the sentiment is positive, negative or neutral." In other words, if you tell your supervisor "That's a great idea!" then post on Facebook that your idiot manger's idea is ridiculous, Big Data knows. This feature is known as "sentiment analysis."
- http://www.inquisitr.com/502491/new-computer-security-tool-alerts-employers-to-complainers/#a94ctUILxW7bhwhx.99



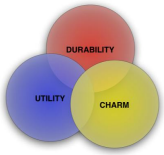
Privacy-China

- According to The Times, the cyberassaults took place over four months, beginning during an investigation by the newspaper into the wealth reportedly accumulated by relatives of the Chinese premier, Wen Jiabao
- Chinese authorities responded to the Times' reports on Wen's family members by blocking access to The Times' website in mainland China.
- The first thing you do is make sure that everything you have is encrypted both in storage or transmission”
- http://www.cnn.com/2013/02/01/tech/china-nyt-wakeup/
- And then there is the Wall Street Journal



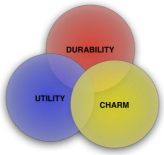
Security China

- The U.S. military's so-called Cyber Command will grow five-fold over the next few years, from 900 employees presently to nearly 5,000 civilian and military personnel – CBS News



Information Entropy

- Information contained in a message
- A fair coin has entropy 1, unfair coin, uncertainty is lower - a flip provides less information since we know something before the flip!
- RELATIONSHIP TO PASSWORDS??
  - An 8 character password selected by user has 18 bits entropy, randomly selected has ~52.7 bits (Jackson http://www.gcn.com)
  - Password strength measures
- Useful for many other things - compression, communications, …



TOR!

- TOR = The Onion Router
- IRC, browsing, …
- The TOR process
  - Unencrypted connection to TOR directory server and gets list of TOR nodes
  - TOR client establishes encrypted connection to random TOR node (entry node)
  - Entry node establishes connection with random second TOR nde
  - Second node establishes connection to a random third node, the exit node
  - Exit node connects to your party
  - Entry node changed every 10 minutes
  - Added security if you are also a TOR node - is it you or is it TOR?