Decision Support Systems for Security

Fred Cohen
Fred Cohen & Associates
04/11/2008 | Session Code: BUS-402

Want to make better security decisions?

- This session will help you do it.
  - The discussion will identify the state-of-the-art in decision support;
  - Discuss key issues in making better security decisions; and
  - Describe emerging technologies, companies and trends.

Donn Parker: (1980s)
"87.4% of all computer attacks go undetected"
DoD – Identity Assurance Executive (2007)
"Identity assurance has reduced the number of successful attacks by 47% in one year"

Outline

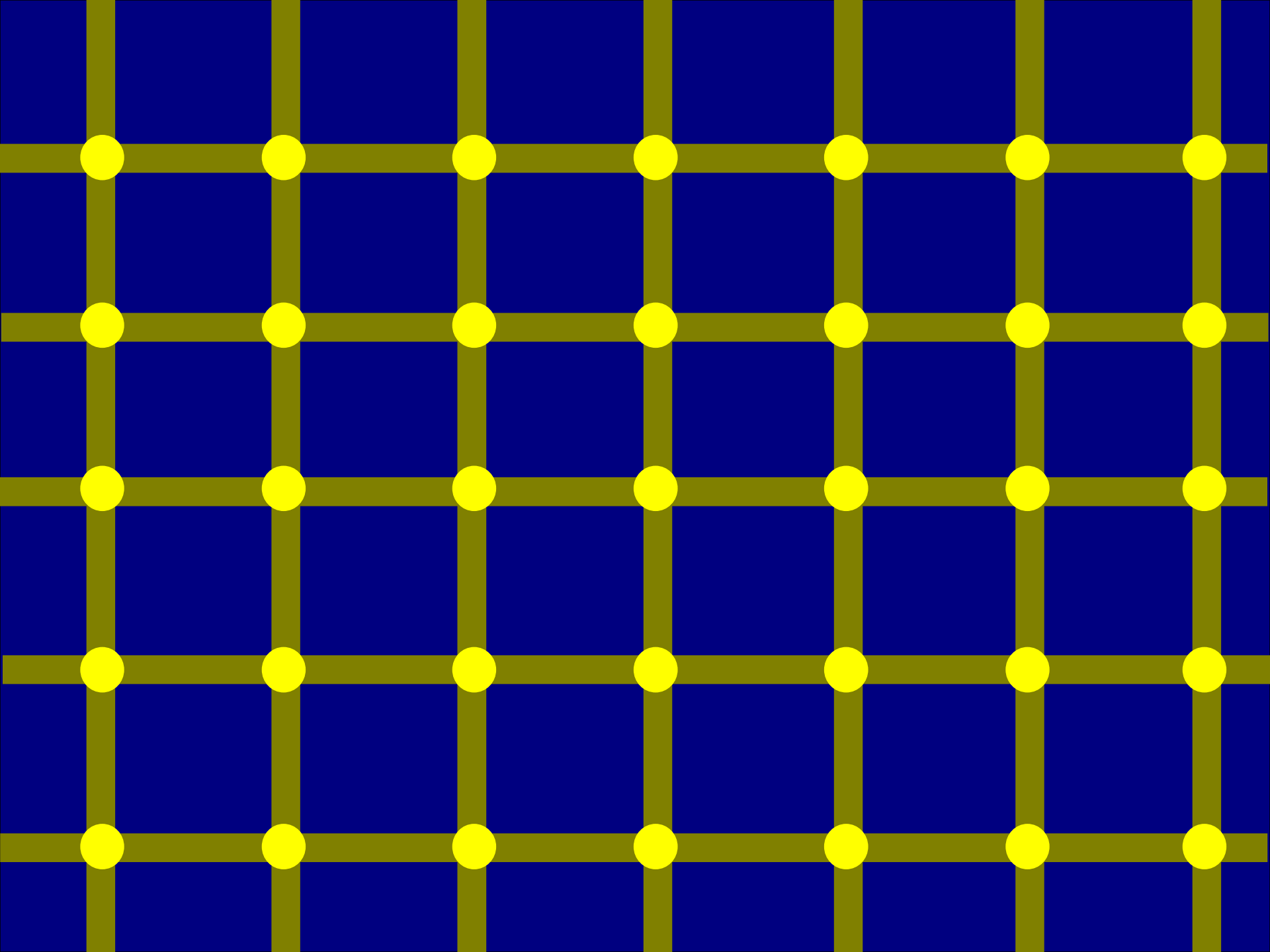
- Background
  - *How this talk came to be*
- Cognition and errors
  - *Cognitive errors and their causes and reduction*
- Decision support systems
  - *Parameters of the space*
- Applying it to computer security
  - *Tools and techniques*
- Conclusions
  - *Questions & Comments*

How did this talk come to be?

- I spent 20 years of my career on the bits
  - *1977: C-MU BSEE*
  - *1980: U of Pittsburgh MS IS*
  - *1981: USC: Fault tolerance and testing of digital systems*
  - *1983: USC: Computer viruses and defenses*
  - *1992: FCA/SAIC/DISA: Critical infrastructure protection: "Information Assurance"*
  - *1996: Sandia National Laboratories: Digital forensics, Y2K infrastructures, CyberCops, information warfare*
  - *1998: White Glove*
  - *2000: ForensiX*
- And then...

How did this talk come to be?

- **And then...**
  - ***Deception ToolKit***
  - ***Model-based situation anticipation and constraint***
  - ***The Invisible Router and Responder***
  - ***Frauds Spies and Lies – and How to Defeat Them***
  - ***World War 3 ... Information Warfare Basics***
  - ***Influence, Decider, Security Decisions***
  - ***The CISO ToolKit – Governance Guidebook, Metrics, Checklists, etc.***
- **So what happened?**
  - ***It's magic...***

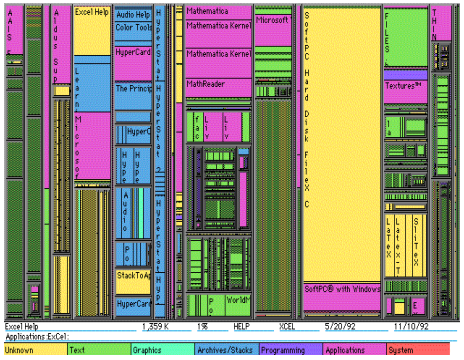


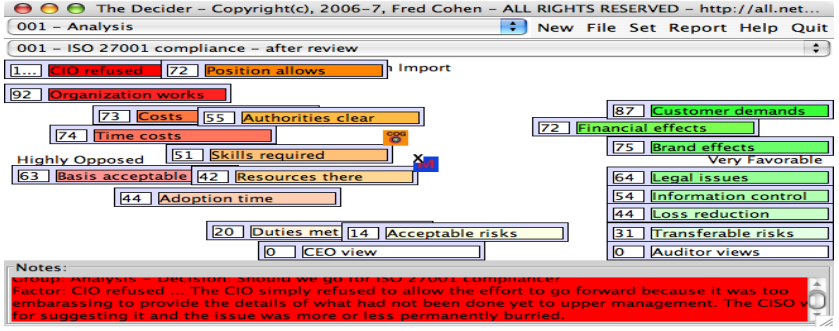
Outline

- Background
  - *How this talk came to be*
- Cognition and errors
  - *Cognitive errors and their causes and reduction*
- Decision support systems
  - *Parameters of the space*
- Applying it to computer security
  - *Tools and techniques*
- Conclusions
  - *Questions & Comments*

People make mistakes

- **We cannot and do not propose to eliminate them all**
  - » ***Example: you turn left instead of right and get hit by a car instead of meeting a new friend***
    - **Perfect prediction of the future – not quite yet**
  - » ***Example: you examined the options, selected the best one on a rational basis, and it didn't work out right***
    - **Perhaps we can help you do the analysis so as to make sure you gather and analyze as much of the best information as you can, characterize it well, and improve over time**
    - **But perfect prediction of the future... not quite yet**
  - » ***Example: You listened to the sales pitch and bought without giving it a second thought and it went bad***
    - **Here we may be able to help you...**





An example

- An experiment to demonstrate (or not) a type of cognitive error
  - *I am going to split the room in half*
  - *Then I will pose one problem for evaluation for each half of the group*
  - *Raise your hand when you agree with the answer as shown on the slide*
  - *Do not speak until the experiment is over*
- Here's a practice round...

Raise your hand when you agree

- We are rating a firewall design based on what evaluators have indicated on their forms:
  - *It costs more than we had planned on spending*
  - *It has a great management and user interfaces*
  - *It will last a long time and adapt to our needs*
  - *It performs well on current penetration tests*
  - *It has limited total bandwidth*
  - *The company has a great reputation*
  - *It will require retraining our technical staff*
- Raise your hand to rate this design (1 worst)
  - *1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 - NO TALKING PLEASE!!!*
  -

Group 1

- Everybody in group 2 – turn around
-
-
-
-
- We're waiting...

- Raise your hand when you agree
  - Performs very well on penetration tests
  - Cost is well within our budget
  - Plenty of bandwidth for expansion
  - Staff already knows how to work it
  - Poor management and user interfaces
  - Needs replaced or upgraded in 2 years
  - Manufacturer is inexperienced
- Key points: strong, fast, inexpensive, easy
- Raise your hand to rate this design (1 worst)
  - *1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 - NO TALKING PLEASE!!!*

Group 2

- Everybody in group 1 – turn around
- Everybody in group 2 – face front
-
-
-
- We're waiting...

- Raise your hand when you agree
  - Poor management and user interfaces
  - Needs replaced or upgraded in 2 years
  - Manufacturer is inexperienced
  - Cost is well within budget
  - Staff already knows how to work it
  - Performs very well on penetration tests
  - Plenty of bandwidth for expansion
- Keys: hard to manage, temporary, shaky team
- Raise your hand to rate this design (1 worst)
  - *1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 - NO TALKING PLEASE!!!*

Everybody face front

- Group 1:
-
- Group 2:
-
- Now let's look at what you evaluated

Both groups saw the same facts

- Rate this firewall:
  - *It has poor management and user interfaces*
  - *The cost is well within our budget*
  - *It will need to be replaced or upgraded in 2 years*
  - *It performs very well on current penetration tests*
  - *The company that made it is inexperienced*
  - *It has plenty of bandwidth for anticipated expansion*
  - *Our staff already knows how to work with it*
- Key points: different points noted as key

What is the difference?

- Presented in different orders
  - » *Primacy and recency effects*
- Presented with different emphasis
  - » *Sharpening and leveling effects*
- Limited time and presentation format
  - » *Hard to reformulate into different sorts and compare*
- These are cognitive errors
  - » *Specific classes of cognitive errors*
  - » *Intentionally induced by the presentation*
- These are errors we might be able to reduce!
  - » *There are many more of them...*

Timing Patience, deadline, speed, fait accompli, surprise, status quo, stretchout
Inspection Open, limited, confession, qualified, third party, no admittance
Association Alliances, associates, disassociates, United Nations, Bribery
Authority Limited, approval, escalation, missing man, arbitration
Amount Fair and reasonable, Bullwarism, nibbling, budget bogey, blackmail, escalation, intersection, non-negotiable, Chinese auction
Brotherhood Equal, bigger, smaller, long-lost, brinkmanship
Detour Decoy, denial, withdrawal, good and bad guys, false statistics and errors, scrambled eggs, low balling, scoundrel

Tactics

Cause	Emotion	Behavior	Cure
Frustration	Hostility	Aggression/apathy	Venting
Threat	Fear	Fight/flight	Safety
Conflict	Anxiety	Inefficiency	Resolution
Violation of values	Guilt	Arbitrary Rejection	Punishment
Loss	Sorrow	Crying	Grieving
Failure	Self-pity	Overindulgence	Try try again

Reciprocation
- Costs more => worth more
- People tend to reciprocate any gifts

Contrast
- Substantial differences tend to be exaggerated

Reject and retreat
- Ask for something then lower request

Authority
- Experts know more

Commitments
- Are honored

Consistency
- Highly valued

Liking
- Say yes to who you like
- Physical attraction +
- Similarity +
- Compliments +
- More contact +
- Groups together bond
- Groups competing hate
- Associate with things that enhance self-image

Commitment
- Small commitments lead to big ones
- Active commitments better than passive
- Public image leads to self-image
- Increased compliance with investment
- Consistency causes decisions

Social proof
- Interpret as others do
- Replaces hard proof in uncertainty

Scarcity
- Scarcity implies value
- Loss > Gain
- Want restricted stuff
- Have it our way
- Exclusive info more valued
- Drop from abundance => more valued

Authority
- Cultural duty to authority
- Appearance => authority

Automaticity
- Desire not to think
- Strong desire not to rethink
- Default decision process
- Because
- Enhanced by rush, stress, ..

Mechanisms

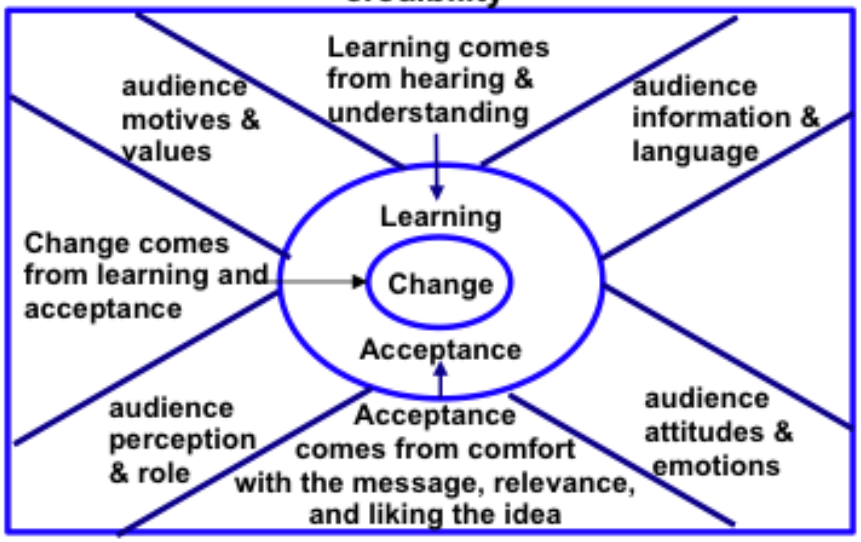
Persuasion Model

Message content & appeal

Present both sides
favored viewpoint last
start /end remembered
end remembered best
state conclusions
repetition helps
arouse need then fulfill
threats are rejected
desirable message first
ask for more, get more
stress similarities
tie hard issues to easy
don't create defensive
don't belittle other views
friendly/sympathetic
ask advice
appeal to self-worth, fairness, excellence

Introduce as an expert and you will be believed as one
Unless you're damned sure, say I reckon - Media may lend credibility

credibility



media choice

situation setting & rewards

make the audience feel worthwhile
reinforce opinions
people like balance
ambiguity upsets
tendency to resolve ambiguity quickly
social forces
account for audience facts, methods, goals, and values
power issues

Letters are good when establishing justification or to get a letter back or when interruption is dangerous
Face to face is better when presence brings regard/respect, visual indicators will help, or more or less may be desired

Influence

Ahah!!!

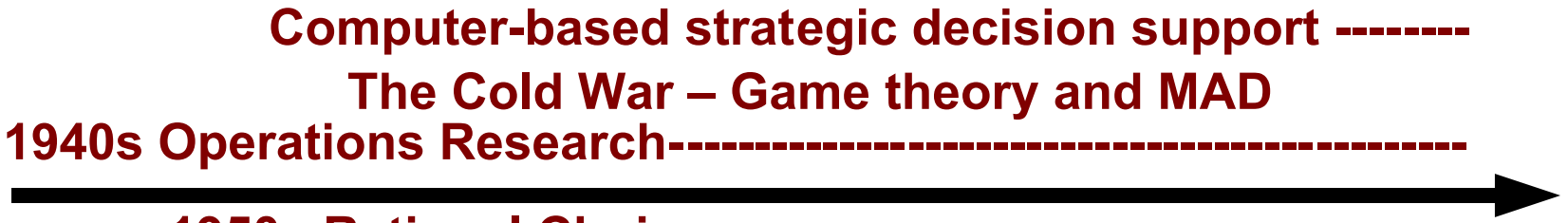
- **Making better decisions may be about:**
  - ***Making fewer errors***
- **To induce / suppress select cognitive errors**
  - ***Design mechanisms to suppress their causes***
- **Additional reading**
  - ***Cialdini: "Influence" - Gillovich: "How we Know what Isn't so"***
  - ***Karrass: "The Negotiating Game" - Handy: "Understanding Organizations"***
  - ***"An Arsenal of Deceptions for INFOSEC (OUO)", PM-1167-NSA, Oct, 1999,***
  - ***JCS Memorandum of Policy (MOP) 113 (Field Manual 90-02)***
  - ***Col. James Hughes-Wilson: "Military Intelligence Blunders"***
  - ***The Psychology of Judgment and Decision Making (Plough)***
  - ***Frauds, Spies, and Lies – and How to Defeat Them***
  - ***Don't use the Wikopedia list – it's really not right***
  - ***Do go to the Web sites of real researchers***

Outline

- Background
  - *How this talk came to be*
- Cognition and errors
  - *Cognitive errors and their causes and reduction*
- Decision support systems
  - *Parameters of the space*
- Applying it to computer security
  - *Tools and techniques*
- Conclusions
  - *Questions & Comments*

History of decision support

- **It turns out that a lot of research has been done on judgment and decision making...**
  - ***World War 2 and the beginnings of operations research led to optimization approaches***
  - ***Economics studied JDM as models of "rational choice" in the 1950s***
  - ***The Cold War led to game theory and its limitations in modeling decision processes***
  - ***Cognitive error mechanisms associated with JDM were studied in the early 1900s, but heavily in the 1980s and forward – largely related to marketing***
  - ***Computer-based decision-making started in the 1940s and flourished in the 1960s and forward***



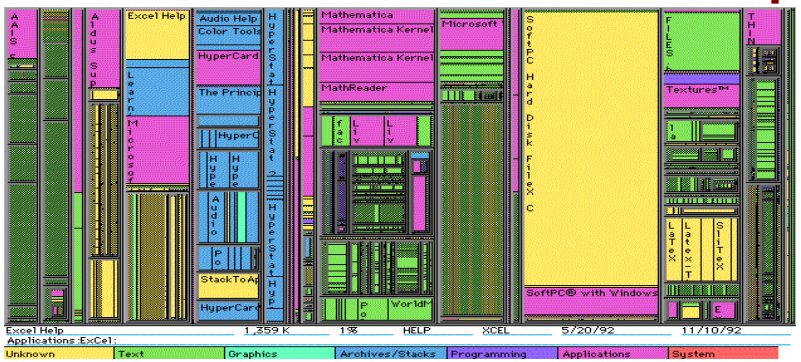
The decision support space

- Objective / Subjective
- Quantitative / Qualitative
- Normative / Ordinal / Interval / Ratio
- Hierarchical / Flat
- Simple / Complex
- Explanatory / Predictive
- Group / Individual
- Casual / Formal
- Amplitude / Architecture
- Text / Visualization
- Tactical / Strategic
- [Optimizing / Satisficing / Incremental / Cybernetic / Random] Model
- [Communications / Data / Model / Knowledge / User] Driven
- Evaluation criteria
- Interaction rates and operational tempo

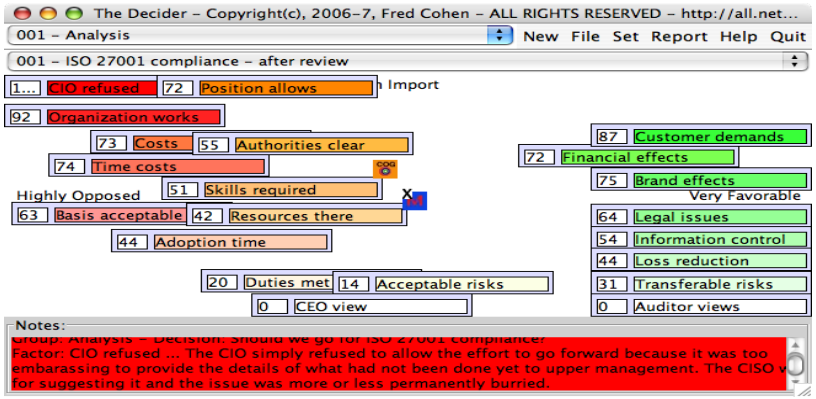
Two approaches

- **Most explored path**
  - ***Important decision must be made right or the consequences may be dire***
  - ***Spend a lot of time and effort getting it right***
    - **Objective, Quantitative, Ratio, Hierarchical, Programmed, Group, Formal, Text and number, Tactical, Optimizing, Amplitude**
  - ***Design for repetition when feasible***

A treemap



- **The path less travelled**
  - ***Common decisions***
    - **Subjective, Qualitative, Ordinal and Ratio, 1-3 levels, Exploratory, Individual or group, Casual, Visualization, Strategic, Incremental, User and model driven, Architectural, human speed**
  - ***The aggregate value of lots of better small decisions may outweigh the big decisions***



Decider decision space

Outline

- Background
  - *How this talk came to be*
- Cognition and errors
  - *Cognitive errors and their causes and reduction*
- Decision support systems
  - *Parameters of the space*
- Applying it to computer security
  - *Tools and techniques*
- Conclusions
  - *Questions & Comments*

Tools for making security decisions

- Tools cover a large part of the security space
- Real-time automated decision makers
  - *IDSs, Firewalls, operating system protections, and all sorts of other similar things*
  - *They all make real-time (machine) cognitive errors*
  - *They form much of the technical security architecture today*
  - *These are all exploitable by smart attackers*
  - *They are becoming more complex over time*
- Real-time fully automated
- Not management decision tools
- Technical decisions only
- Must be fully pre-programmed / known adaptations
- They also interact with management systems and humans and bring cognitive errors up the ladder

Packets show up → real-time decisions

Security has a lot of decisions

- **But the tools have not worked their way up to the executive decision making part of the space**
  - ***Business modeling decisions***
  - ***Oversight decisions***
  - ***Risk management decisions***
  - ***Duty to protect, what to protect, and how well***
  - ***Power and influence decisions***
  - ***And on and on...***
    - **A picture is worth ... a lot of words**

Area	Policy Standards Procedures	HR Legal	Risk	Testing & Change Control	Technical Safeguards Physical / Information	Incidents	Audit	Knowledge and Awareness	Document
Create / Specify	1	0	3	0	0	0	1	0	0
Manage	3	0	3	1	4	1	1	6	0
Process	6	0	3	4	20	8	3	8	0
Execute	5	1	3	10	125	39	5	11	0

Some security DS tools

- **Expert analysis tools - DEMO**
  - *Security Decisions – reduce errors by expertise*
- **Checklists and similar measurement tools - DEMO**
  - *Metrics – reduce errors by exhaustion*
- **Risk management tools – NO DEMO**
  - *Name your poison – lots of them at the show – limited executive utility*
- **Policy analysis and design tools – DEMO**
  - *Policy Assistant – reduce errors by consideration*
- **General decision-making tools - DEMOS**
  - *The Decider – reduce/induce cognitive biases*
  - *Influence – influence groups to achieve success*
- **To try these examples out:**
  - *http://manalytic.com*
  - *Free download of all tools shown here – for non-commercial use only*

Tools in this part of the space

- **Policy management tools**
  - *Polivec – Zequel - Policy Assistant (shown – internal tool)*
- **Risk management tools**
  - *Citicus - Milliman - Relational Security - RiskWatch - SecureInfo - SourceSentry - Telos/Xacta – Skybox (none shown)*
- **Security decisions - expert analysis tools**
  - *Burton Group's "Reference Architecture" tools*
  - *"Security Decisions" tool (shown)*
- **Metrics tools (checklists, etc.)**
  - *Metrics (shown – internal tool)*
  - *Go to the Metrics talks at RSA or elsewhere*
- **General tools**
  - *Tree maps and many other similar methodologies*
  - *FCA's "Decider" and "Influence" (shown)*

Outline

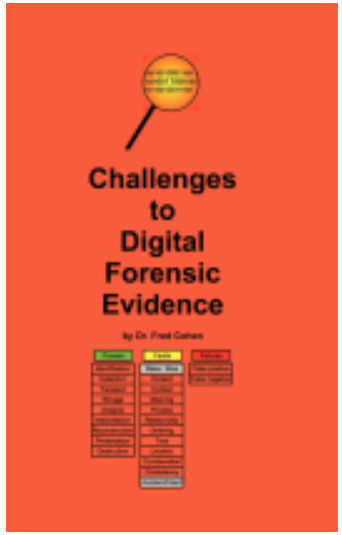
- Background
  - *How this talk came to be*
- Cognition and errors
  - *Cognitive errors and their causes and reduction*
- Decision support systems
  - *Parameters of the space*
- Applying it to computer security
  - *Tools and techniques*
- Conclusions
  - *Questions & Comments*

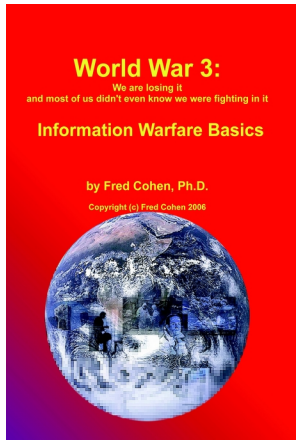
The hard sciences

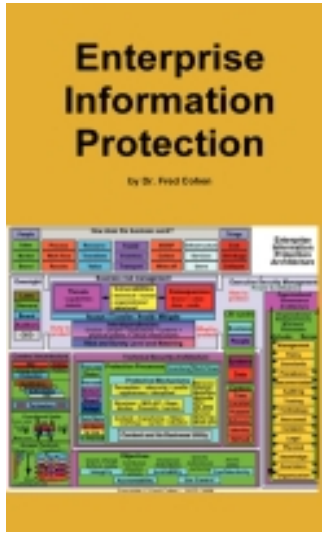
- I have a saying...
  - *The "soft" sciences are the hard sciences*
  - *The "hard" sciences are the easy sciences*
- But my experience biases me...
  - *Learning analytical techniques and applying them is easy for me – or at least I am used to it.*
  - *Understanding how people work is hard for me – and I don't seem to be able to get as used to it*
  - *Trying to find interfaces that reduce errors takes a lot of time and effort - implementing them does not*

More magic

- The WayBack Machine – the Internet Archive
  - *Many recent cases have tried to use the WayBack Machine to prove what happened in the past*
  - *But the WayBack Machine has some problems in this regard*
- A DEMONSTRATION
  - *Either I am a fantastic magician*
  - *OR the WayBack Machine provides illusions*
- To find the answer, check out..
  - *3 recent books (two were in the bookstore)*
- Here's the real deal
  - *Why do speakers show you their books?*
  - *Because the conference bookstore FORCES THEM TO*
  - *I promised to show them to you to get my books in the store*
  - *So I kept my promise – but you should complain!!!*







The science of magic...

- **Arthur C. Clarke:**
  - *"Any sufficiently advanced technology is indistinguishable from magic" - But when I explain it to you, it loses its mystery... and may even cause resentment*
  - *That's the nature of knowledge*
- **To make better security decisions, we can:**
  - *Get better facts*
    - Usually costs more, takes longer, and is far harder to do
  - *Better use the facts we get*
    - Little added cost, faster in many cases, and fairly easy to do
    - But it means getting a better handle on decision-making
    - And identifying and reducing cognitive errors
  - *Understanding cognitive errors is a two-edged sword!*

Thank You

Questions? Discussion?!

Dr.Cohen at Mac.Com
http://all.net/