Five research projects that didn't get funded
... that I think should have

Fred Cohen
Fred Cohen & Associates

NebraskaCERT 2005

Drop a card for a chance for 6-weeks of free security mentoring

Outline

Five research projects that didn't get funded

and should have...

Project 1...

Project 2...

Project 3...

Project 4...

Project 5...

...

Questions / Comments?

Drop a card for a chance at 6-weeks of free security mentoring

Some Background

1960-70s: I worked on a variety of computer security related things before college and eventually started to focus on it

1975: Digital Analog times permutation lock

1976: Secure protocols for DISN, Autovon, ...

1983: First computer virus experiment

Starting then I didn't get funded in computer security...

NSF reply to research proposal in 1987: Not an interesting subject

1993: Critical infrastructure protection paper and book

NSF reply to research proposal in 1995: Not an interesting subject

2000: Research in cyber terrorism

NSF reply to research proposal in 2001: Not an interesting subject

And the beat goes on... (not just the NSF by the way)

Outline

Five research projects that didn't get funded

and should have...

Project 1: Deception for protection

Project 2...

Project 3...

Project 4...

Project 5...

...

Questions / Comments?

Deception research

1990s: Proposed deception toolkit

- Rejected by management
- So over my Thanksgiving vacation, I wrote DTK
- Freely available to anyone who wants to download it
- Simulates ports on computers to defeat scanners
- Allows simulation of several (scores of) IP addresses per computer
- Doesn't interfere with other operations significantly
- Dramatically increases attacker work load
- Legal, ethical, moral, etc.
- Easy to implement and use
- Thousands of folks got it and loved it
- So I figured...

Deception research

Proposal to DoD group

Build network-level deceptions that are effective at defending operational DoD networks

Done and done

- Now operating in parts of the tactical Internet
- Time to expand the effort for even more effective deceptions

Project completion – no more funding

- Drat – it was just getting interesting
- Following are some of our results that we could not move on

What we know we can do

Leading attackers through attack graphs

Disrupting attack group processes

Reducing desire to attack

Falsify “fist” (or hand)

Reduce confidence in attack

Increase time to attack systems

Decrease likelihood of success (time)

Create realistic deceptions that fool people

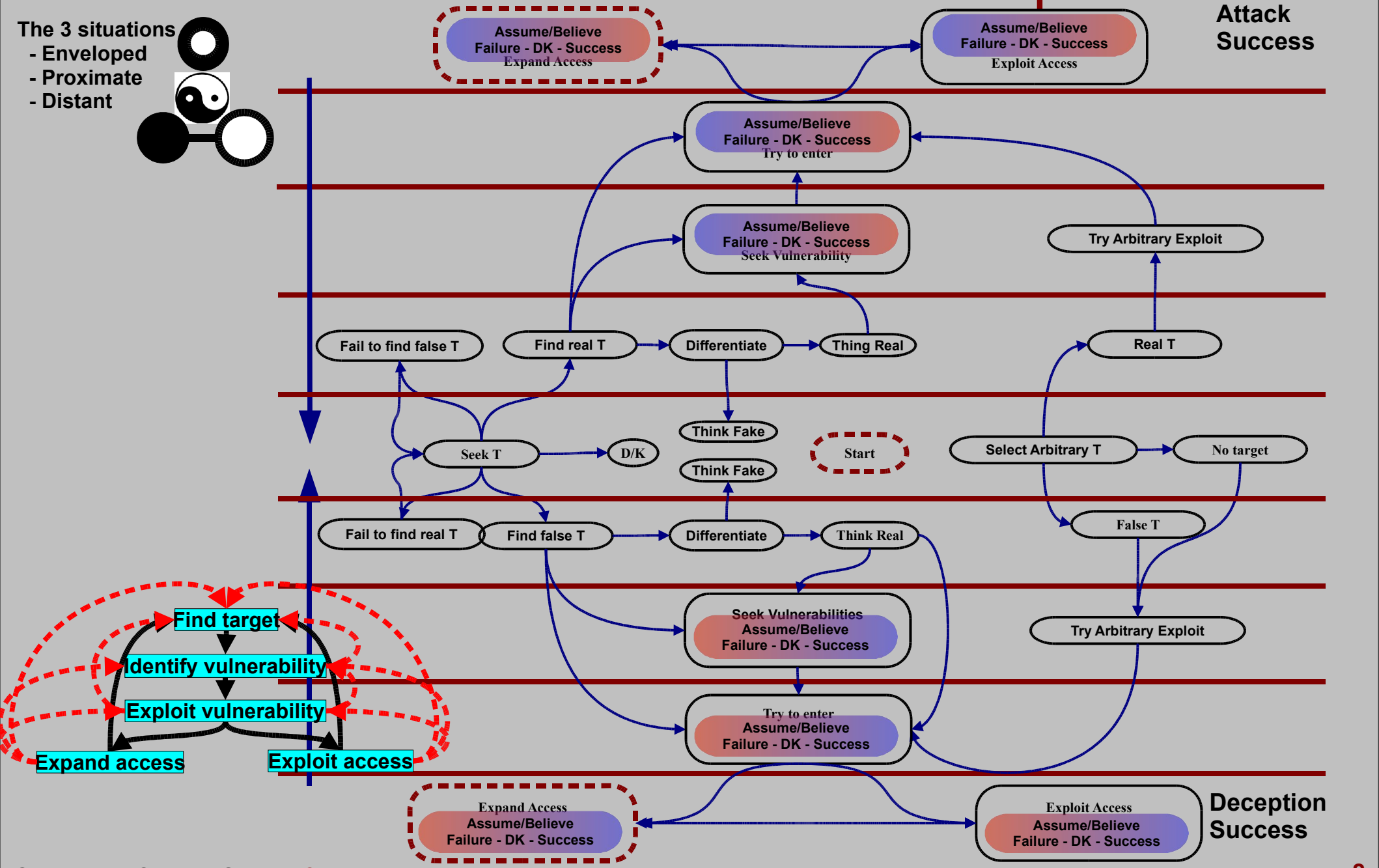
Create deceptions that fool software analysis

Induce type-1, type-2, or type-3 errors at will

Disrupt common attack tools from functioning

Cause attackers to move away from the target

The generic attack graph under deception



What we want to be able to do

Automatically generate deception plans that will work

Put metrics on success of techniques in situations

Expand out models to larger-scale information war

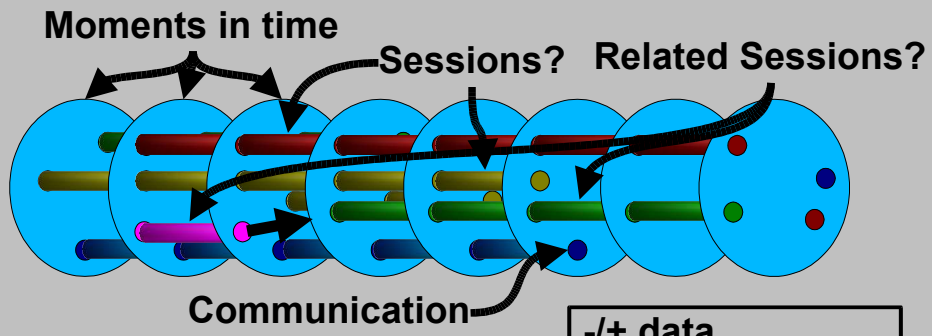
Improve our internal deceptions against insiders

Continue experiments and R&D of working tools

Apply “Responder” for military applications

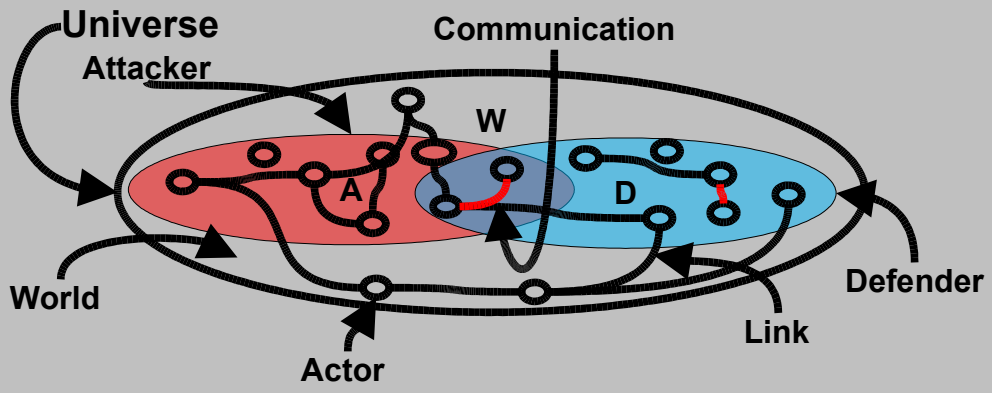
Do ongoing work in the field

Ongoing deception of “hand”



PASSIVE

- -/+ data
- -/+ session
- -/+ association
- -/+ consistency
- -/+ inconsistency
- -/+ understand



Outline

Five research projects that didn't get funded

and should have...

Project 1: Deception for protection

Project 2: Level 3 attribution

Project 3...

Project 4...

Project 5...

...

Questions / Comments?

Level 3 attribution

Congressional testimony in 2000: we need attribution

Attribution issues:

- Level 1: Which IP address/port did the attack come from
  - Often easily done if attack is detected – but of little help
- Level 2: What IP address/port directed the activity
  - Often very hard to solve when using multiple indirect elements
- Level 3: What human/system directed the activity
  - May often be easier to solve because of “hand”
  - Ties into deception of hand research
  - Often multiple IP sources for same hand
  - Hand often tracked over lifetimes
- Level 4: What organization directed the activity
  - Calls for classic intelligence problem
  - Not really solvable by computers under any current notions

Level 3 attribution project

We got funded by DoD via another company

The other company bid us but didn't use us

- and failed in the research which is now shut down

Meanwhile we have a testbed and capabilities

- but no funding to do the work
- so we do it as part of our investigative practice
- and await funding for the good stuff

What can we do?

- Record and simulate “hand” (part of deception work)
- Differentiate some number of hands
- Associated specific characteristics with history
  - Education, type of keyboard, type of computer and operating system, native language and how long since the change, etc.

Level 3 attribution

What do we want to do?

- Generate and build a collection of known parties
- Track them throughout their lifetimes
- Determine how they are evolving
- Be able to correlate who across multiple incidents
- Use distributed sensors to track them down in time
- Figure out how to use characteristics in PsyOps
- Understand how to forge hand
- Provide the means to create arbitrary hands
- Create custom hands for operators to enhance deceptions

Outline

Five research projects that didn't get funded

and should have...

Project 1: Deception for protection

Project 2: Level 3 attribution

Project 3: Components and composites

Project 4...

Project 5...

...

Questions / Comments?

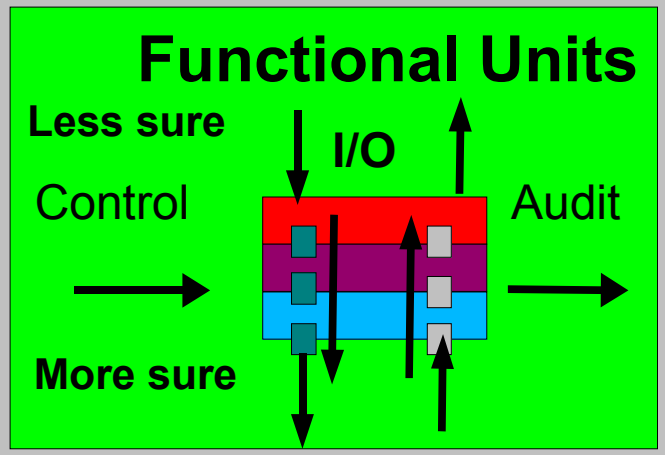
Components and composites

- Build far more secure systems at lower cost
  - By building components with known characteristics
  - Combining the components into composites
  - Being able to calculate composite characteristics
  - Being able to design composites with characteristics
  - Ultimately a design process for secure systems
- Others have theoretical models and summaries
- What have we done so far?
  - Secure server projects
    - Secure DNS (SDNS)
    - Secure Web Server (thttpd)
    - Secure Gopher server
  - Secure composite bootable CD (White Glove)

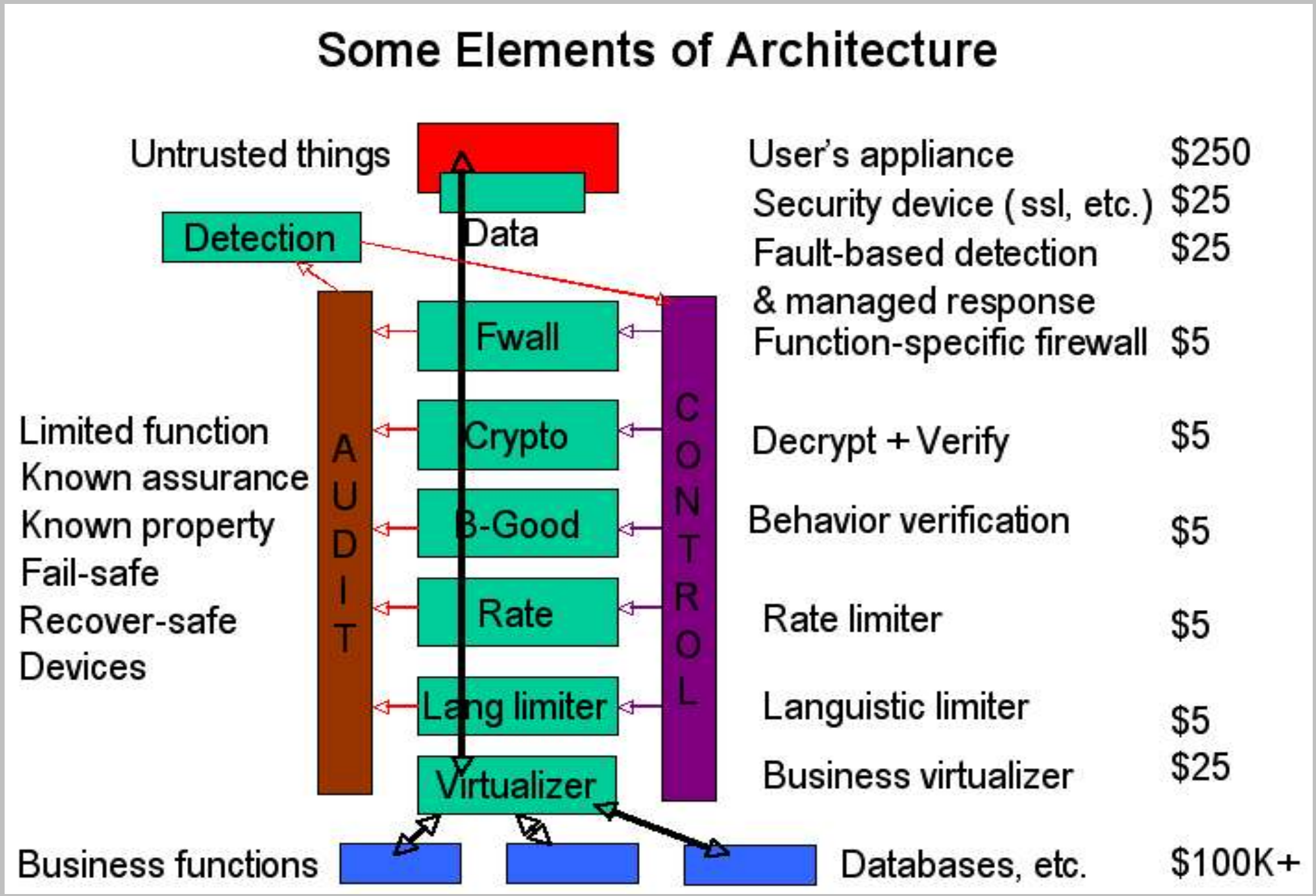
Components and composites

A decomposition approach

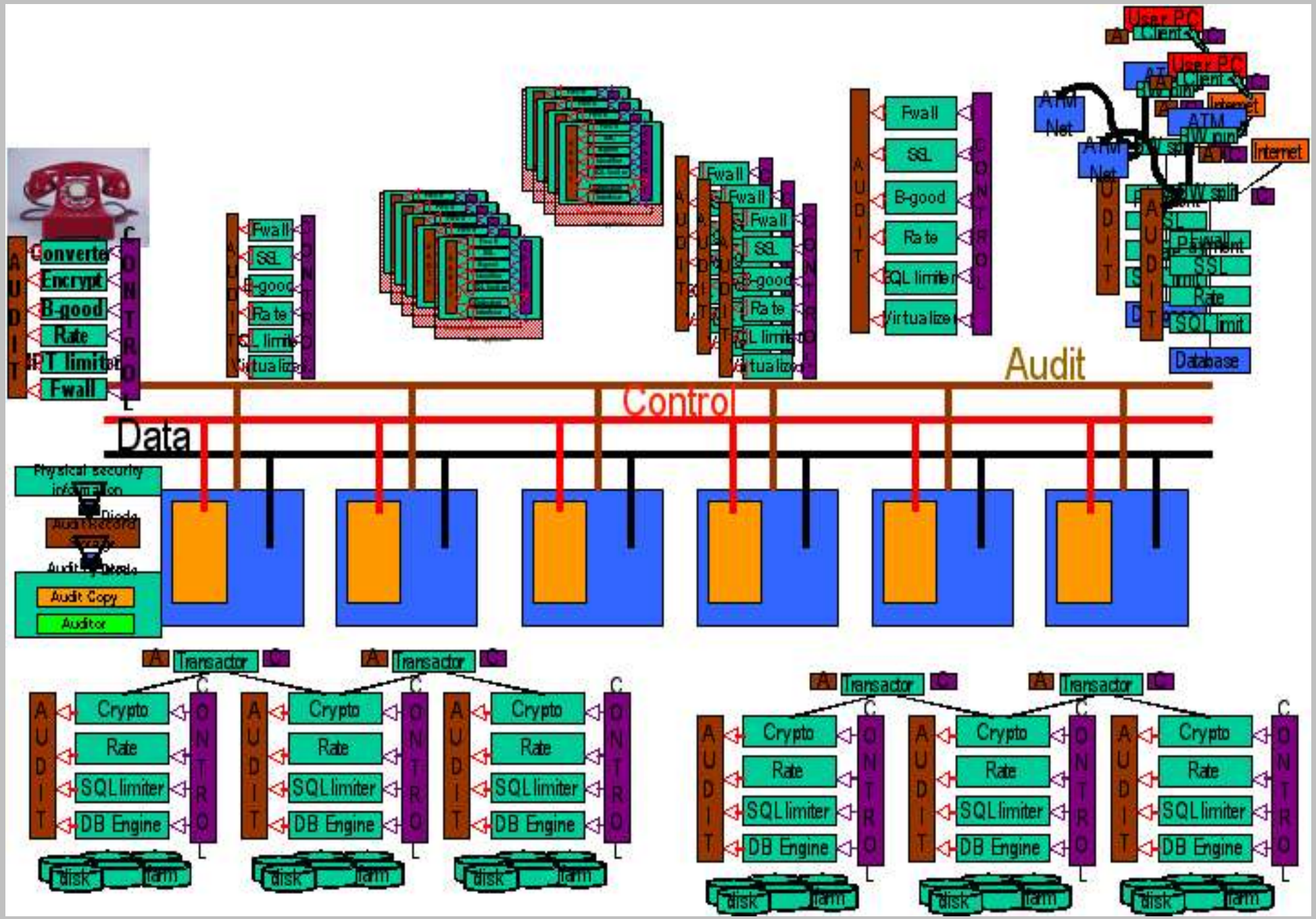
- Team decomposed modern security architecture to create a proposed secure architecture for 8-10 years out
- Functional units as layered systems
- Separate control from data from audit
- Layers implement different defenses
- Example layers:
  - Classic IP firewall
  - Decryption and authentication
  - Syntax check
  - State machine check
  - Size check
  - Rate check
  - Function
  - Business virtualizer



Sample composite (2007)



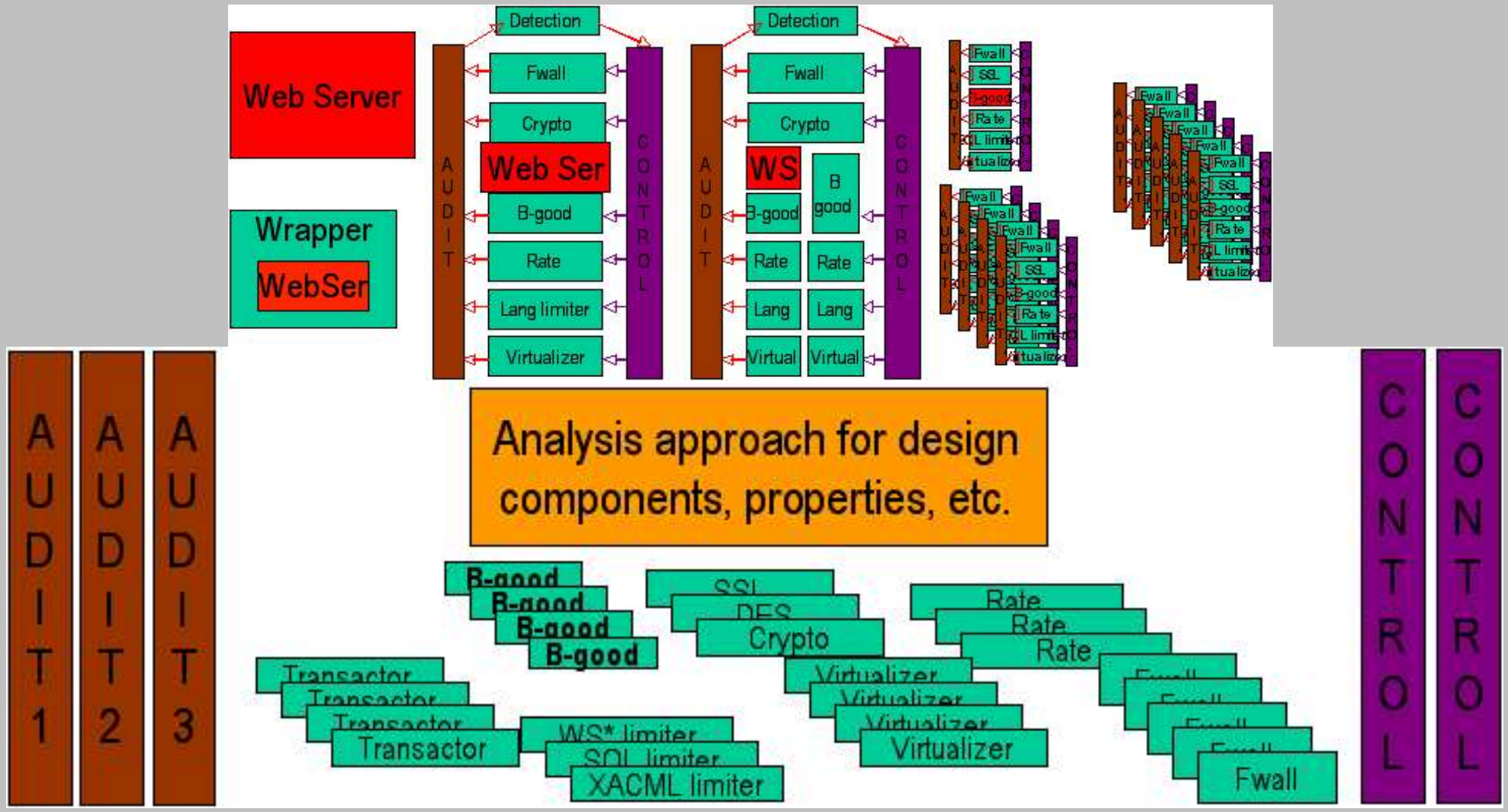
Enterprise-scale composite



Components and composites

Not just a bunch of parts - a methodology for

building, assembling, testing, tracking, replicating, changing, and measuring properties of parts and composites



Outline

Five research projects that didn't get funded

and should have...

Project 1: Deception for protection

Project 2: Level 3 attribution

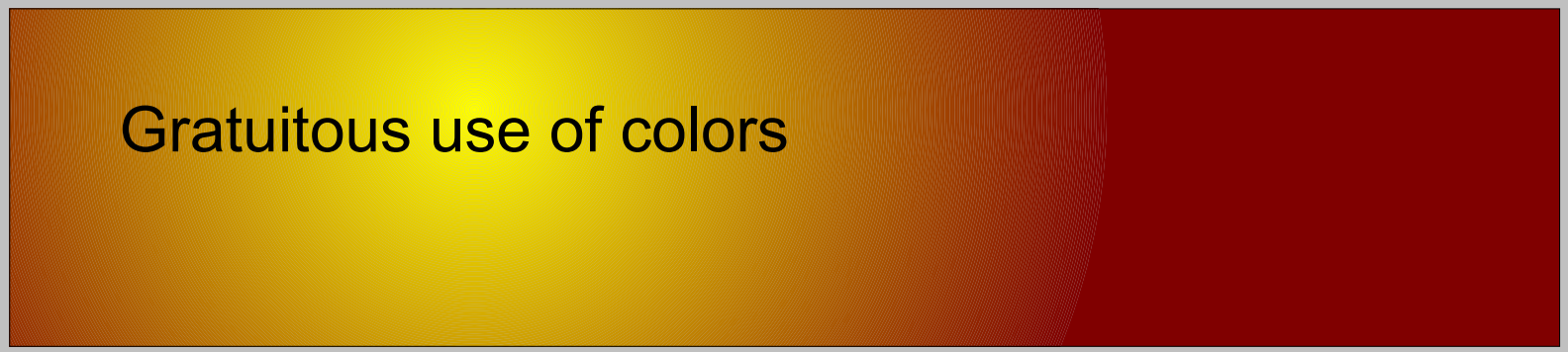
Project 3: Components and composites

Project 4: Multidisciplinary security simulations and research

Project 5...

...

Questions / Comments?



Multidisciplinary center

Since security is so complex and multidisciplinary

Create a center to try to work across the space

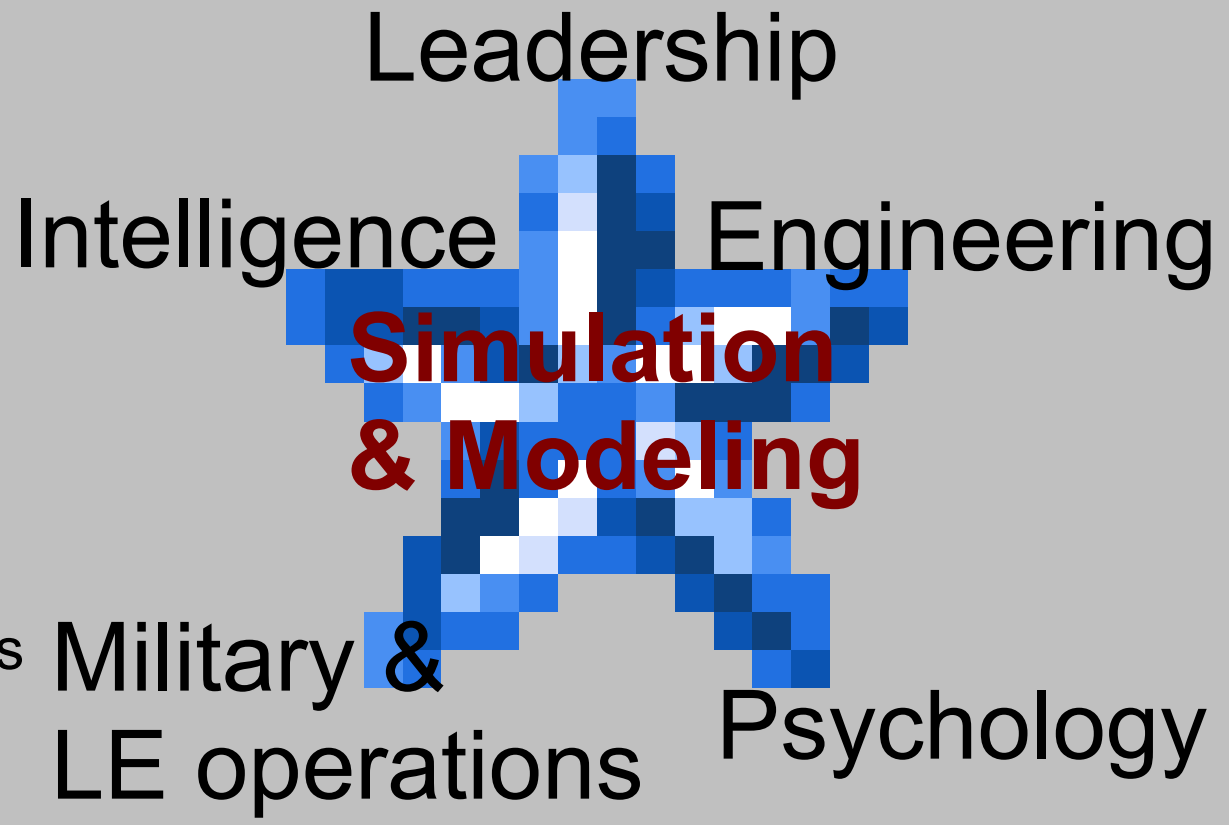
Found the center on the concept of strategic and tactical simulations of conflicts and learn as you teach

Critical Infrastructures

Power and energy
Water and waste
Communications
Government services
Finance
First responders

Learning and doing

Normal educational program
With simulated complex incidents
Incidents exercise learning
We learn from the incidents



Multidisciplinary Center

- Not just a notion – a facility
  - Different schools within an educational institution participate
  - Each has a wing of the building for their area of expertise
  - The building itself has all the the critical infrastructures
  - The building control systems are designed to model the controls of national critical infrastructures
- In incidents
  - The facility turns into the simulator
  - The people go into their operational roles
- Between incidents
  - The people adapt the facility to better survive
  - The people learn how to cope and what to do
- Education, research, and simulation fused together

Outline

Five research projects that didn't get funded

and should have...

Project 1: Deception for protection

Project 2: Level 3 attribution

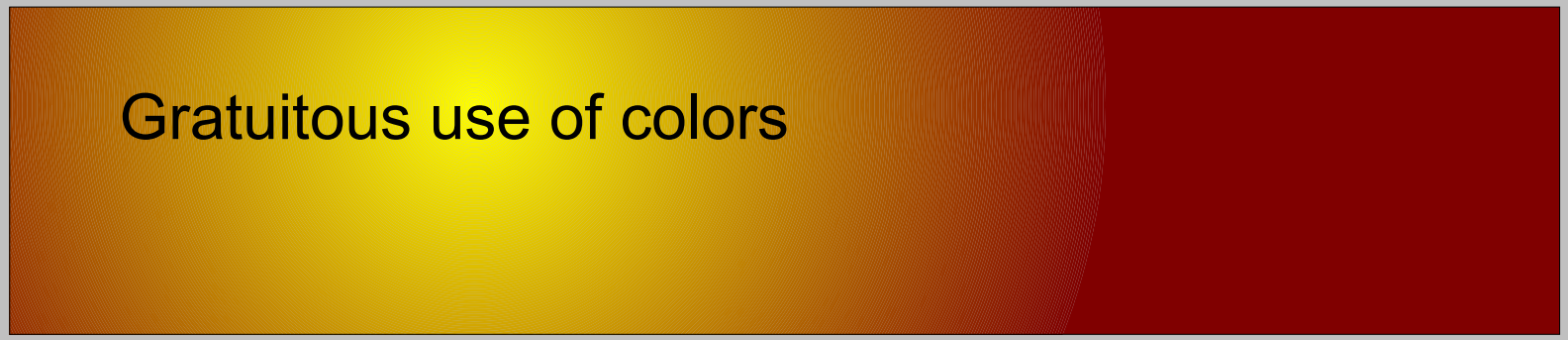
Project 3: Components and composites

Project 4: Multidisciplinary security simulations and research

Project 5: Automated intelligence aides

...

Questions / Comments?



Automated intelligence aides

I have done a lot of work collecting and fusing information together for research and reports

- Any serious research effort starts with all source intelligence
- We go out and collect lots of material on a subject
- We fuse it together into a cohesive picture of the situation
- We consider alternatives and do experiments
- We learn from the results

I apply it in lots of areas – for example:

- Research and development efforts (1970s-now)
- Investigations and forensic investigations (1980s-now)
- Critical infrastructure protection (1992-now)
- Deception and perception management (1997-now)
- Research into cyber-terrorism studies (1998-now)

Automated intelligence aides

Somewhere around 2000...

- The Internet started to become really useful for this stuff
  - But the tools were crappy
- Search engines starting in the late 1990s helped a lot
  - But you had to read all the results first
- Citations and drill-down were always an issue
  - Web-based linkage between summaries and details helped a lot
- How would automation help us?

So we started an automated intelligence gathering and analysis project

- It had some special features that we thought were highly desirable at the time

Automated intelligence aides

Special features desired and attained (1990):

- Covert operations (privacy of gatherers?) to reduce
  - Counterintelligence effectiveness
  - Attacks against the intelligence effort and participants
  - Knowledge of the subjects that they were being gathered about
- Ability to analyze for steganography and other issues
  - Global search and detection of common steganographic content
  - Association of “hand” and sourcing to find common sources
- Desire to seek better information over time by learning
- Get partial results fast and better results eventually
- Collect and store original data and provide sorted summaries to analyst for review and drill-down
- Ability to take results directly from output and put into reports with drill-down included

Automated intelligence aides

The Florsheim Project

- Named after the famous shoemaker because it started with an “F” and because finding shoes was the example used

How we did it

- The collection systems used low-level deceptions to conceal themselves within existing Web search engines and any other Internet-based system
- The information passed inbound through a digital diode to assure that no leakage from the analysis occurs
- Steganographic analysis was done by a 100 CPU parallel processor with custom algorithms written by the team
- We exploited existing search engines for initial identification of candidate information

Automated intelligence aides

How we did it (continued)

- Parallel pull of relevant information from all engines
- Eliminate duplicate URLs
- Automatically “read” content to rank by structure
- For returned pages collect related URLs and links
- For higher ranked pages do analysis of related links sooner
  - Note this convoluted pull it all and analyze later strategy eliminates covert channels associated with feedback and reduces impacts of human responses to pulls
- Provide sorted extraction of relevant content on a Web page with drill-down to original content stored in parallel processor (100 processors @ 100Gig each = 10 Tbytes)
- It gets “smarter” for a while because better information tends to be near the top
- But after a few hours it runs out of useful information…

Outline

Five research projects that didn't get funded

and should have...

Project 1: Deception for protection

Project 2: Level 3 attribution

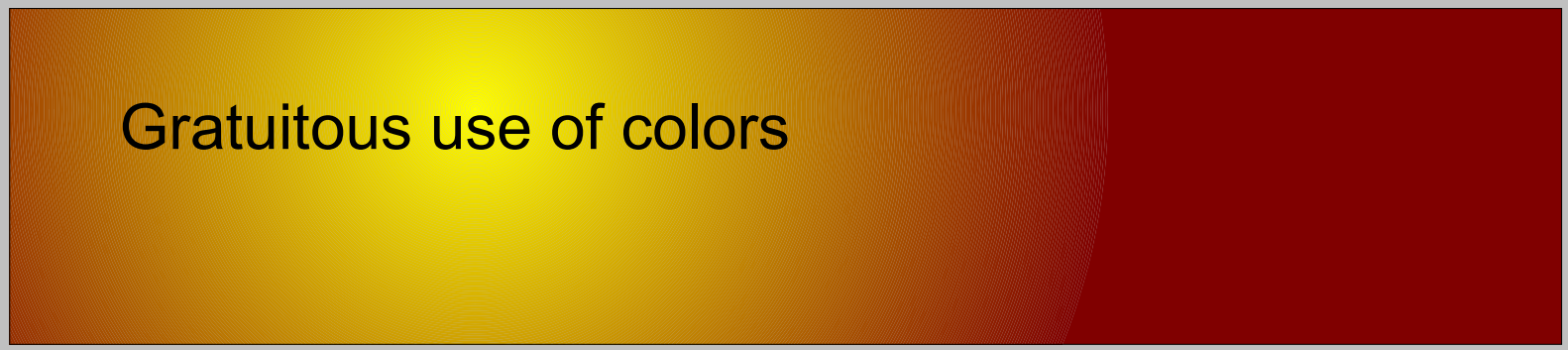
Project 3: Components and composites

Project 4: Multidisciplinary security simulations and research

Project 5: Automated intelligence aides

Where are they now?

Questions / Comments?



Where are they now

Deception work:

- No money for real experiments since 2000
- Enhanced tools for network-level deceptions (Responder)
- No progress on host-level insider defenses
- Real utility in penetration testing and investigations
- I teach a graduate course in deception, propaganda, perc...
- Wait till you see some of our information operations...

Level 3 attribution:

- Money largely dried up before it started
- Some tools for analysis
- Some infrastructure for collection
- An ability to restart
- Some use in investigations and forensics cases

Where are they now

Components and composites:

- The last of the “other researcher” funding ended in 2004
- DARPA funded work cut because not immediately applicable to the war effort
- Our components operate today and have for a while
- Composites are now getting too old to use and we can't keep them up to date (not that they need to change much)

Multidisciplinary research center:

- Congressional line item in 2004 – cut in committee
- Proposed to DARPA – not directly applicable to war effort
- We keep trying to convince folks to do it but...
- PKI is as close as anyone has come so far
- And it is a long way away – but still obtainable

Where are they now

Automated intelligence aides:

- Steganographic work had to be cut (DMCA made it illegal)
- Later a university was funded to work on related things but used none of the pre-existing results and failed
- Cover collection still works (for me) but rarely used except in select law enforcement investigations
- Analysis engine is pretty old but part of some White Glove distributions and almost usable

And me?

- Teaching at the University of New Haven
- Principal analyst at Burton Group
- CEO - Fred Cohen & Associates
- Principal Scientist at SecurityPosture here in Omaha
- Looking for the next good idea that won't get funded

Outline

Five research projects that didn't get funded

and should have...

Project 1: Deception for protection

Project 2: Level 3 attribution

Project 3: Components and composites

Project 4: Multidisciplinary security simulations and research

Project 5: Automated intelligence aides

Where are they now?

Questions / Comments?

Drop a card for a chance at 6-weeks of free security mentoring