NSF/CISE CNS

NSF Security Program Overview

March 26, 2009

CNS Trustworthy Computing PM: Karl Levitt

OCI PM: Kevin Thompson

IIS PMs: Amy Baylor, Sylvia Spengler

CCF PMs: Rich Beigel, Lenore Zuck

ONR PM but previously on detail to NSF: Ralph Wachter

DDs: Ty Znati, Haym Hirsh, Sampath Kannan

CISE AD: Jeannette Wing

Our Take-away Message -- The Threat

Our country faces serious cyber threats upon our national infrastructures

- A massive cyber attack upon our Nation's critical infrastructures which is credible and that would have staggering adverse consequences
- Technology convergence, innovation and even rapid obsolescence open cyber vulnerabilities faster than old vulnerabilities can be closed
- Globalization of information technology despite its benefits also has adversely affected our technical leadership and competitiveness

NSF and the Trustworthy ComputingProgram have an obligation

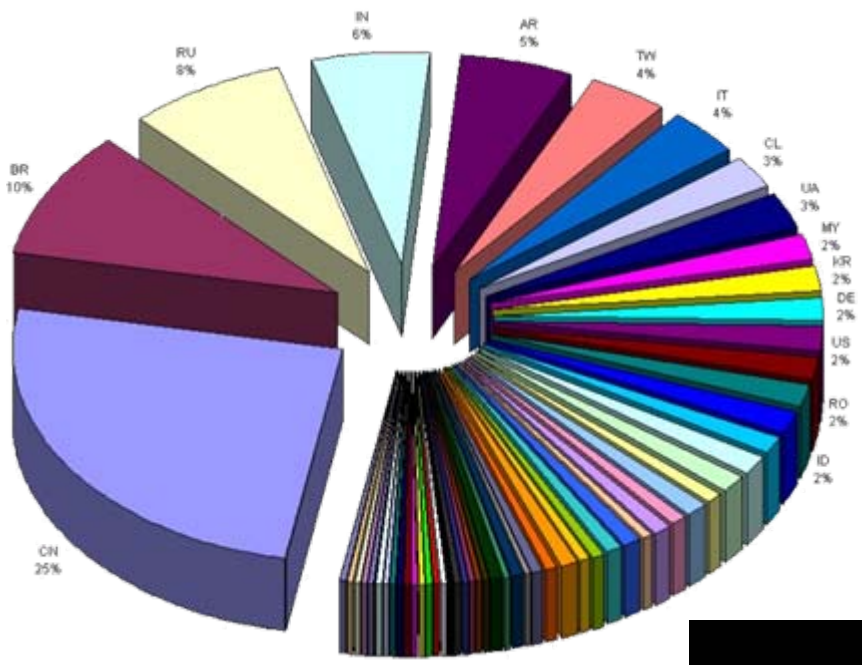
- Exercise leadership in science and technology to build trust in cyberspace
  - Ensure scientific and technical excellence
  - Balance portfolio of theoretical and experimental research
- Meet and exceed the expectations of the legislation enacting CyberTrust
- Create a technological future for cyber space that benefits and advances society for generations to come

Without trust in cyber space
our critical infrastructures and privacy are at significant risk

More Security Research is Needed

- On-line crime is reputed to cost $200B/year
- There is the real specter of cyber terrorism on our nation
  - Estonia and Taiwan cases are but forewarnings
- Ubiquitous/Pervasive computing *despite its many advantages* poses a threat to citizens' privacy
- The future of electronic voting and, even, Internet voting poses threats to our nation's democratic institutions
- Cyber attacks a on our nation's critical infrastructures are increasing and having cascading effects
- Botnets are the *attack du jour*, but other kinds of crippling attacks are predicted

Cornflicker Botnet

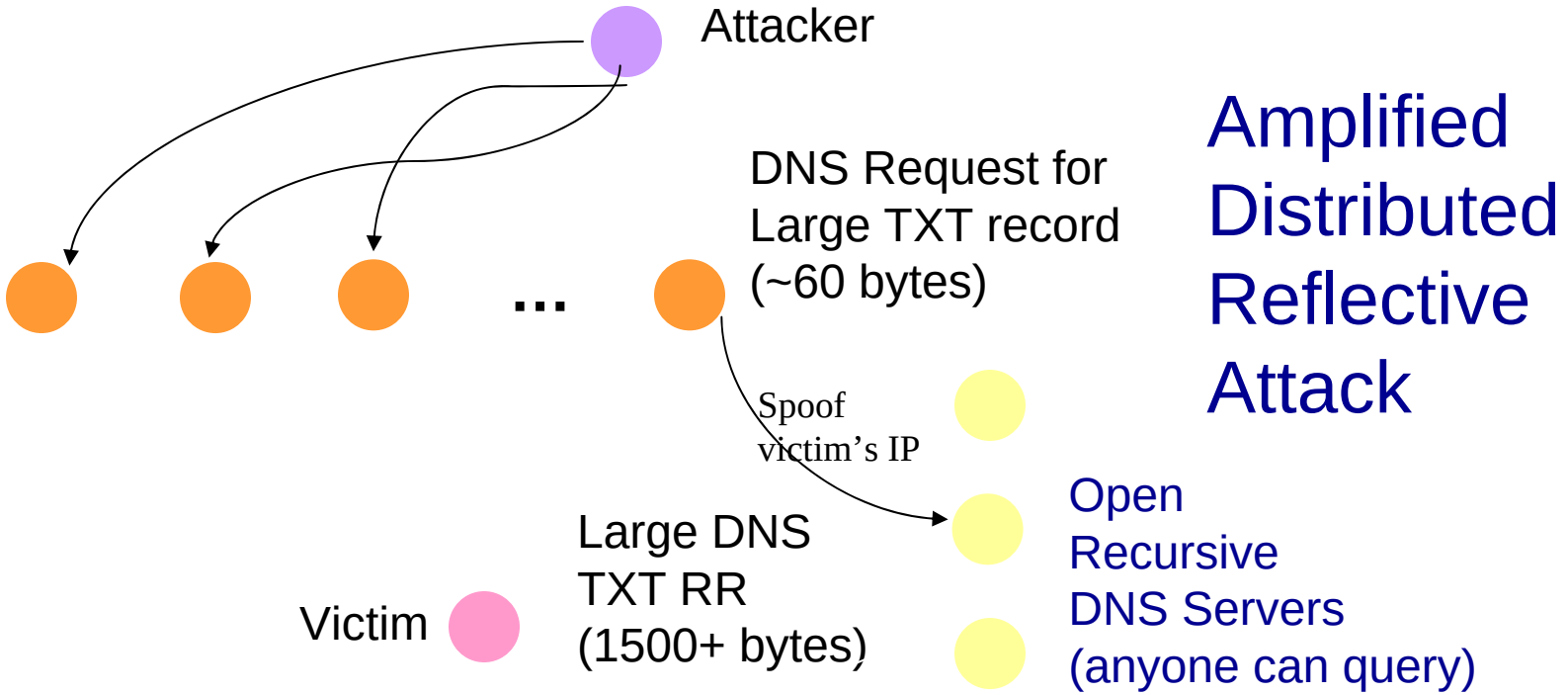


Cumulative Infections
31 January 2009, SRI International

- Over 10,000,000 IPs affected worldwide
- Command and control mechanism identified and shut down by the *Conficker Cabal*
- New versions of malware released on the Internet, SRI NSF project identified new versions and new threats

Attack Example

Botnets increasingly used for amplified distributed reflective attacks



Outline

- CyberTrust and evolution to Trustworthy Computing
- CT Centers, Large ITRs, and STC
- Other awards
- Testbeds
- NSF's role in CNCI
- International Activities
- Towards a *Science of Security*
- Security education
- Future directions

A Short History of the NSF's Security Program

FY01: Research Program "Trusted Computing" initiated ($4-6M/yr)

FY02: Boehlert/Hall Bill, Committee on Science, for NSF and NIST

- THE Cyber Security Research and Development Act (H.R. 3394)
- Bill called for authorization of nearly $600M for NSF in 5 CT focus areas

FY03: Increasing focus in specific research programs

- Trusted Computing
- Security-related network research (NeTS)
- Data and Application Security
- Embedded and Hybrid Control Systems Security

FY04: Integrated CISE-wide program – "Cyber Trust"

- Entire suite of cyber security activities managed under one integrated, cross-cutting program to foster multidisciplinary collaboration - computer scientists, engineers, mathematicians, and social science researchers
- Two Center-scale activities awarded: CCIED, STIM (now SAFE)

FY05-08: Continuing "Cyber Trust" program

- Two Center-scale awards: TCIP, ACCURATE
- 15 Team/Large awards, 60 individual/small group awards -- per year
- $35M for FY05, $24M for FY06, $34M for FY07, $33M for FY08

NSF Strategic Mission in Trustworthy Computing

Support leading-edge fundamental research on computer-based systems and networks that

- ✓ Function as intended, especially in the face of cyber events
- ✓ Process, store and communicate sensitive information according to specified policies
- ✓ Address the concerns of individuals and society about privacy
- ✓ Educate the next workforce and inform the public

Systems of national significance, e.g., in critical infrastructures, finance, elections, healthcare, national defense, national-scale databases, air traffic control, and **systems important to individuals**, e.g., automobiles, office systems, homes

Collaborative activities addressing the full scope of dependable systems (reliability, safety, security, etc.) and other research areas (e.g., confidentiality and usability of research data)

The Many Topics of Security funded by Cyber Trust (over 400 ongoing projects, 387 PIs and Co-PIs)

Cryptography: provable security, key management, lightweight cryptographic systems, conditional and revocable anonymity, improved hash functions

Formal methods: access control rule analysis, analysis of policy, verification of composable systems, lightweight analysis, on-line program disassembly

Formal models: access control, artificial diversity and obfuscation, deception

Defense against large scale attacks: worms, distributed denial of service, phishing, spam, adware, spyware, stepping stone and botnets

Applications: critical infrastructures, health records, voice over IP, geospatial databases, sensor networks, digital media, e-voting, federated systems

Privacy: models, privacy-preserving data-mining, location privacy, RFID networks

Hardware enhancements for security: virtualization, encryption of data in memory, high performance IDS, TPM

Network defense: trace-back, forensics, intrusion detection and response, honeynets

Wireless & Sensor networks: security, privacy, pervasive computing

New challenges: spam in VoIP, "Google-like" everywhere, virtualization, quantum computing, service oriented architecture

Metrics: Comparing systems wrt security, risk-based measurement

Testbeds and Testing Methodology: DETER. WAIL, Orbit and GENI, scalable experiments, anonymized background data

Research spans the space: foundations, hardware, operating systems, networks, applications, usability

Cyber Trust Basic Activities

Cyber Trust program awards ($24M in FY06, $34M in FY07, $35M in FY08)

- Single investigator, Teams, Large, Exploratory Research
- Centers, but not since 2005

Related awards in NSF and CISE wide programs (GENI, NeTS, NeTSE, CSR, CRI, MRI, IIS, CCF, Cyber Physical Systems)

Related (still active) ITR awards

Related CAREER awards (up to 15 per year)

Related Science and Technology Center award: TRUST

Related IUCRC awards (ENG)

Scholarship for Service (EHR)

Advanced Technological Education (EHR)

Collaboration at NSF (IIS, CCF, and OCI)

NSF Security Funding in FY08:

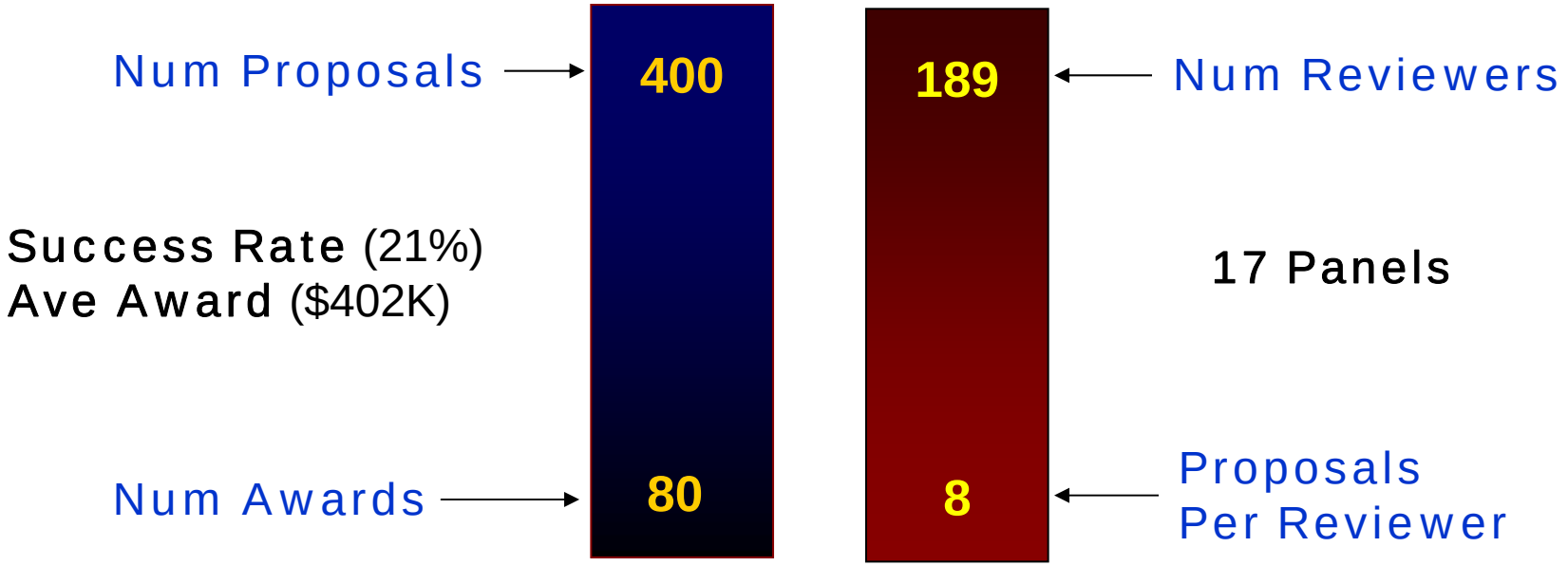
- ***CISE: $93.5M***
- ***NSF total: $96.7M***

In FY2009 Cyber Trust transitioned into Trustworthy Computing (TC)

Deeper and broader than CT

Five areas; proposals that cut across *privacy* and *usability* *particularly welcome:*

- Foundations: new models that are analyzable, cryptography, composability (even though security is not a composable property), new ways to analyze systems
- Privacy: threats, metrics, security, regulation, database inferencing, tradeoff with other requirements
- Usability: for lay users and security administrators
- Security Architecture: Beyond point solutions, putting techniques together (like intrusion tolerance), towards a future Internet (including secure hosts and applications)
- Evaluation: especially experimental, testbed design and deployment



	Small	Team & Large	Explor. Res.	Total
Proposals	282	86	31	**399**
Awards	56	18	8	**82**
Funds Committed For New Awards	$14M	$17M	$2M	**$33M**

FY08-funded CAREERs (add 15 awards $6.0 M)

NSF Inter-Agency Activities including Planning and Coordination

Joint research funding and activities

- DARPA co-funding: FY04 Cyber Trust awards
  - Secure Core: processor, OS kernel, security services (Princeton, USC-ISI, NPS)
  - Formal verification using ACL2 (U. Texas Austin)
  - Detect security-related software errors (UC Berkeley, UMD, Stanford)
- DHS and DoE co-funding: FY05 Cyber Trust center-scale award on Trustworthy Cyber Infrastructure for the Power Grid (TCIP)
- DHS co-funding: ITR on biometrics (UWV, Clarkson), DETER testbed
- DNI, DoD: National Cyber Defense Initiative (NCDI)
- ARO: Co-organized workshop on security/privacy for sensor networks & embedded systems
- DoD Panel on Network Security Issues: NSF GENI Overview
- NIH: Planning joint solicitation on confidentiality & usability of research data
- SBE, Microsoft, IBM: Workshop on privacy and data confidentiality
- Treasury: Discussions on secure and resilient recovery mitigation of systems against insider attacks and possible co-sponsorship
- Japan and European Commision: Workshops leading to focused collaborations; EU focused on experimental evaluation, collaborative defenses and privacy; supplemental travel grants for Japanese researchers and NSF researchers for collaborative research by respective S&T agencies

NSF has a leadership role that fosters inter-agency collaboration

- INFOSEC Research Council (IRC)
- National Coordination Office (NCO) Cyber Security and Information Assurance (CSIA)

TRUST Science and Technology Center
(UCB, Stanford, Cornell, Vanderbilt, SJS, Mills, Smith)

Three *Grand Challenge* Pillars of TRUST

Objective

- Increase relevance and maximize impact of TRUST research
- Build on the successes of the past years and further align and focus our research, education, and knowledge transfer efforts
- Create a **Science of Security**

Rationale

- Center research activities organized around three target application areas
- Areas selected to emphasizes fundamentally different trustworthiness problems
- TRUST is well positioned to contribute fundamental advances to address trustworthiness challenges in each area
  - Trusted operating systems
  - Reliable computing
  - Languages and tool support for writing secure code
  - Cryptographic protocols
- TRUST actively engaged with stakeholders from each area

Financial Infrastructures

- Web browser and server security
- Botnet and malware defenses
- Data breach notification laws
- Secure software and systems infrastructure

Health Infrastructures

- Privacy Modeling and Analysis
- Health Information Systems and Patient Portal Architectures
- Patient Monitoring Sensors

Physical Infrastructures

- Embedded systems for SCADA and control systems
- Sensor networks for Demand Response systems
- Information privacy and security

Contextual Integrity, Law & Cyberspace

TRUST: Team for Research in Ubiquitous Secure Technology

Create new technologies and perhaps even new social institutions to build inherently secure computer software and networks

- FY05 5-year, $20M award (renewable to 10 years) to UC Berkeley (prime)
- Carnegie Mellon University, Mills College, San Jose State University, Smith College, Stanford University and Vanderbilt University
- Industrial and other partners are Bellsouth, Cisco Systems, ESCHER (a research consortium that includes Boeing, General Motors and Raytheon), Hewlett-Packard, IBM, Intel, Microsoft, Oak Ridge National Laboratory, Qualcomm, Sun Microsystems and Symantec

Science & Technology

Personal data

The logic of privacy

Jan 4th 2007

From *The Economist* print edition

A new way to think about computing and personal information

PEOPLE do not have secret trolleys at the supermarket, so how can it be a violation of their privacy if a grocer sells their purchasing habits to a marketing firm? If they walk around in public view, what harm can cameras recording their movements cause? A company is paying them to do a job, so why should it not read their e-mails when they are at work?

How, what and why, indeed. Yet, in all these situations, most people feel a sense unease. The technology for gathering, storing, manipulating and sharing inform has become part of the scenery, but there is little guidance on how to resolv conflicts created by all the personal data now washing around.

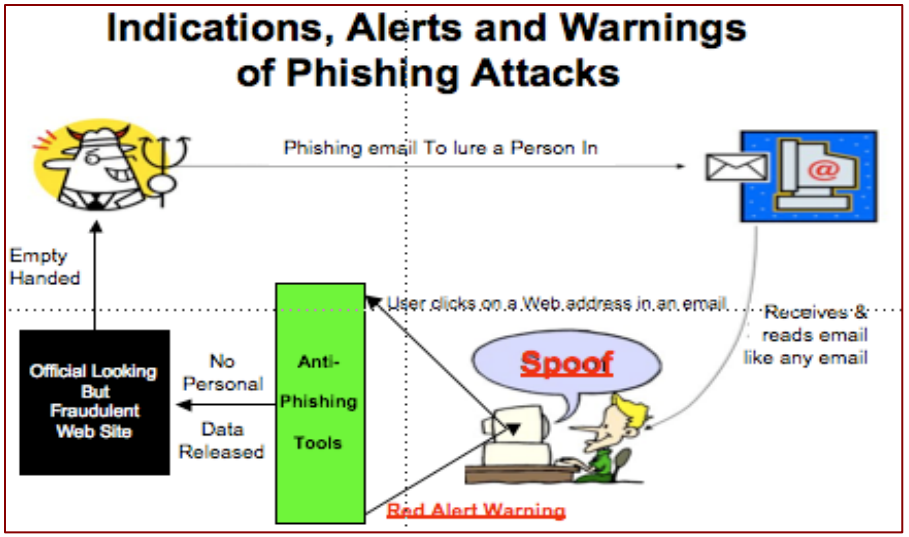
A group of computer scientists at Stanford University, led by John Mitchell, has started to address the problem in a novel way. Instead of relying on rigid (and easily programmable) codes of what is and is not acceptable, Dr Mitchell and his colleagues Adam Barth and Anupam Datta have turned to a philosophical theory called contextual integrity. This theory acknowledges that people do not require complete privacy. They will happily share information with others as long as certain social norms are met. Only when these norms are contravened—for

Usable Security against Phishing

ITR: Sensitive Information in a Wired World

The project on Privacy, Obligations, and Rights in Technologies of Information Assessment, known as the PORTIA project, concerns protection of the rights of data owners, users, and subjects, and their data in the online world that is increasingly beset with fraud and theft.

- FY03 5-year, $6M award
- Stanford, Stevens, Yale, U. New Mexico, NYU



A phishing attack steals user passwords by sending fake emails that direct users to a spoofed bank web page. The PORTIA tools warn the user and ensure that users only send a useless version of their password.

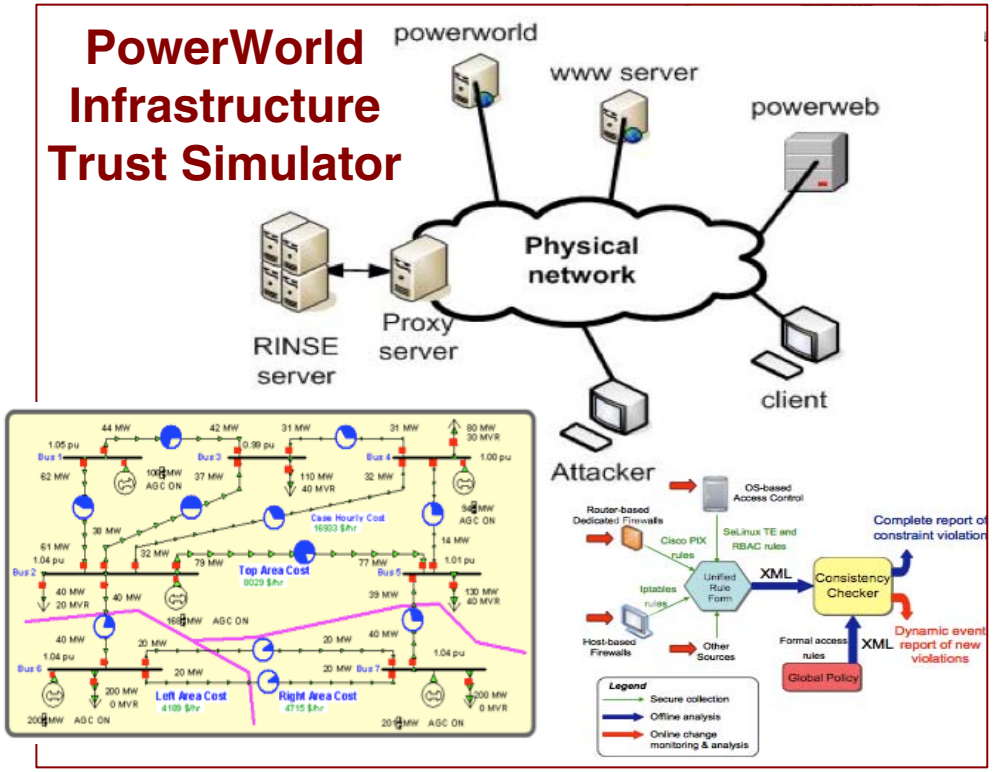
PowerGrid Infrastructure Control to achieve Security

TCIP: Trustworthy Cyber Infrastructure for Power

Address technical challenges motivated by power grid problems in by developing Secure and Reliable Ubiquitous exposed infrastructure, Real-time data monitoring and control, wide area information coordination and information sharing

- FY05 5-year, $7.5M award
- Co-funded with DHS, DoE
- University of Illinois · Dartmouth College · Cornell University · Washington State
- EPRI, Sandia, Siemans, CISCO, PNNL, Cyber Defense Agency…

PowerWorld Infrastructure Trust Simulator



- Multiparty interactions
  - Partial & changing trust requirements
  - Regulatory limits on information sharing
- Large-scale, rapid propagation of effects
- Need for adaptive operation

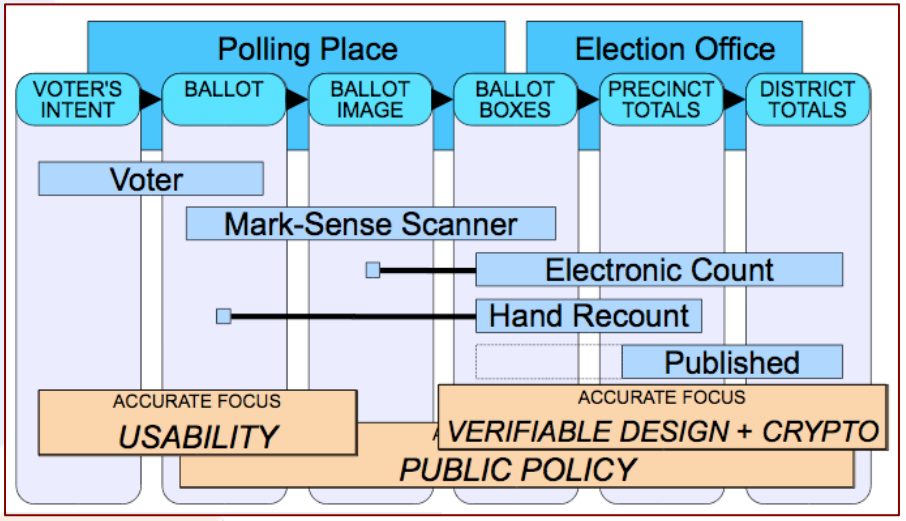
Towards Trustworthy *e*Voting

ACCURATE: A Center for Correct, Usable, Reliable, Auditable, & Transparent Elections

Improving the reliability and trustworthiness of voting technology through new architectures, tamper-resistant hardware, crypto-graphic protocols

- FY05 5-year, $7.5M award to Johns Hopkins University (*prime*)
- Rice University; Stanford University; the University of California, Berkeley; the University of Iowa and SRI International

Chain of Evidence for Mark Sense Reader



- ✓ **Research at intersection of technology, social, legal, and political**
- ✓ **Congressional testimony**
- ✓ **eVoting systems deployed are**
  - Highly vulnerable to fraud
  - Vulnerable to wholesale tampering
  - Without voter verification
  - Without proper audit capability

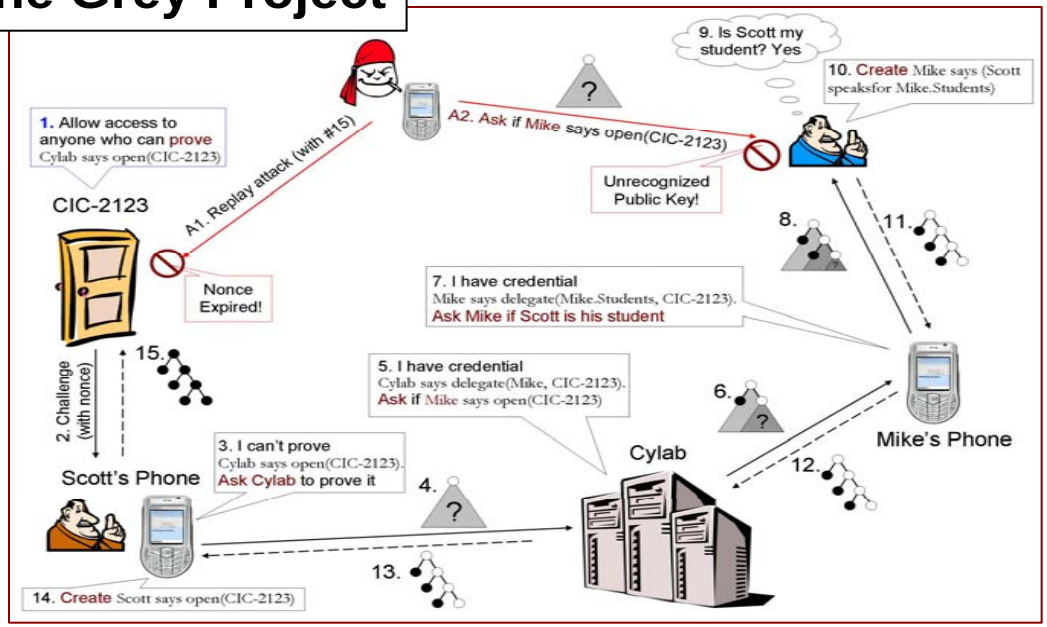
Mark Sense Reader

SAFE – Usable Security (CMU)

Computer defenses can be dramatically improved, in both efficacy and usability, by modeling experience and context in a way that allows the models to become an integral element for defending the system

- FY05 5-year, $7.5M award
- Carnegie Mellon University

The Grey Project



- Distributed System Security via Logical Frameworks and Policy Enforcement
  - Formal techniques for proving authorization
  - Delegation of Authority & Access control
- Secure access-control device via software extensions to off-the-shelf "smart phones"

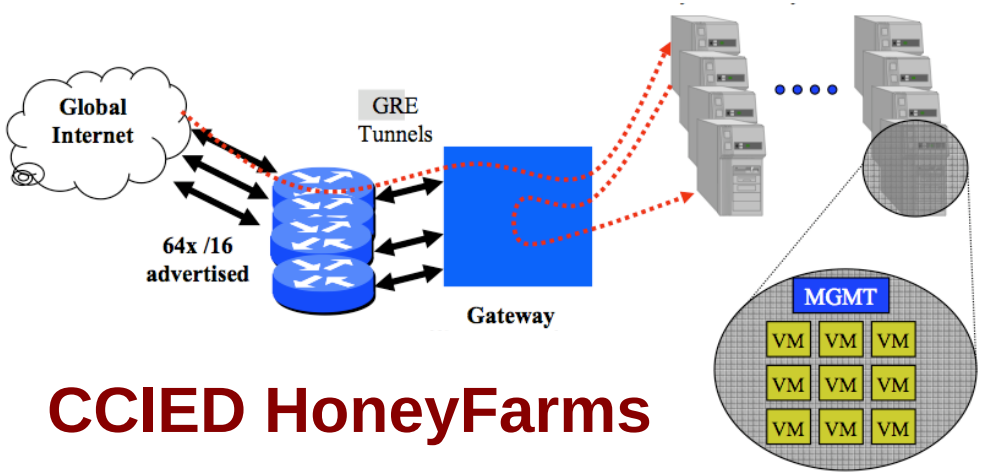
CCIED: Automated Worm Defense

Collaborative Center for Internet Epidemiology and Defenses

analyzing the behavior and limitations of Internet pathogens (e.g., worms, viruses), reverse-engineering of worms, developing early-warning and forensic capabilities, and defending against new outbreaks in real-time

– FY04 5-year, $7.5 award

– UC San Diego and UC Berkeley, International Computer Science Institute



CCIED HoneyFarms

- **Emulate significant fraction of Internet hosts** (>1M)
- **Multiplex large address space on smaller num of servers**
  - Temporal & spatial multiplexing
  - Physical HoneyFarm Servers
- **Potemkin: large number Virtual Machines (VM) per host**
  - Delta Virtualization: copy-on-write VM image
  - Flash Cloning: on-demand VM (<1ms)

FENCE: Security Services for Health Care Applications (*Purdue University*)

Objectives:

To develop security services for healthcare applications and data that:

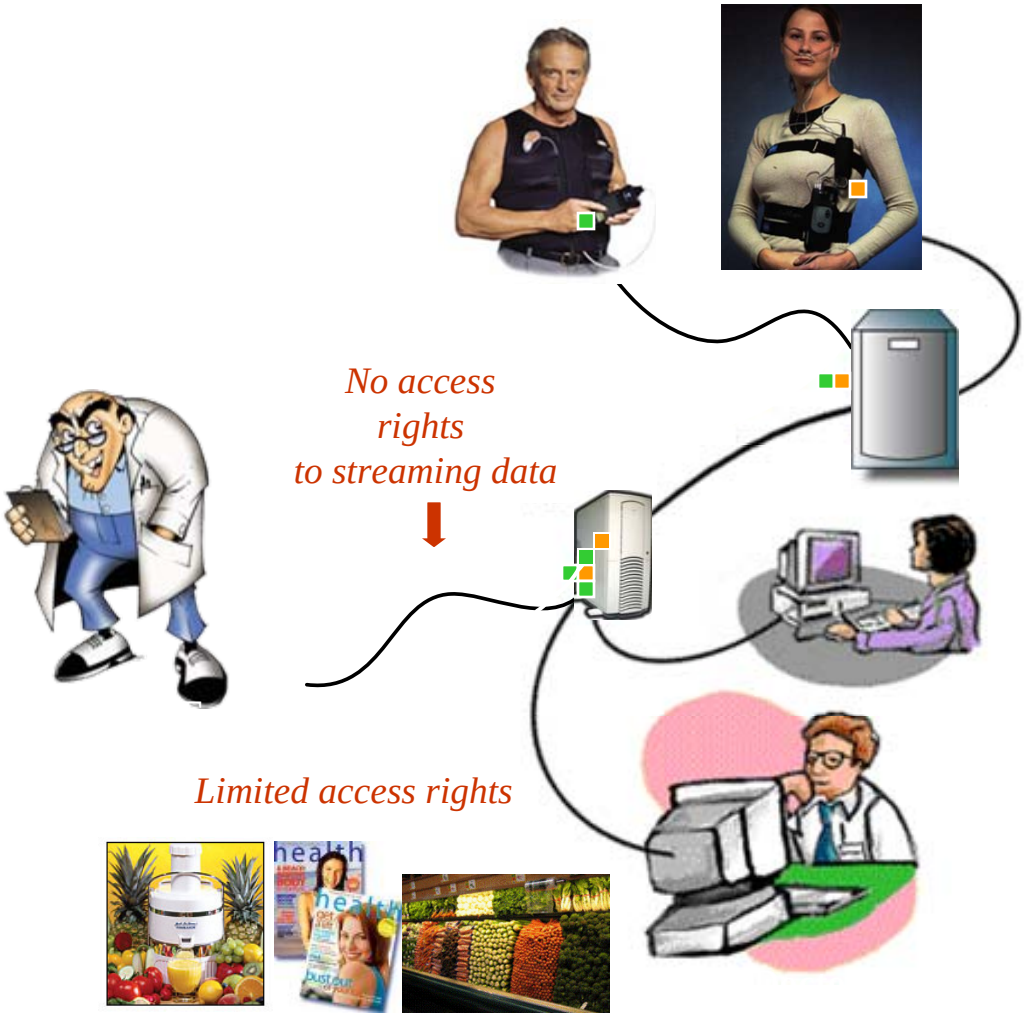
•support functions for digital identity management, authentication, access control;
•are based on policy languages;
•are based on service-oriented architectures and web services.

Plans:

• Make available to the open source community:
  •PRBAC
  •Postgres DBMS extended with the anomaly detection and response systems
•Extend VeryIDX with biometric data
•Develop flexible authentication policies taking into account events and contexts
• Develop secure systems for the personal management of HC data

•Continuous Access Control Enforcement in Dynamic HC Data Stream Environments (**FENCE**):
  Policies are specified by the data provider (the patient) and embedded in the data streams through security punctuations
•Privacy-aware role based access control (PRBAC):
  It extends RBAC with elements (purposes, obligations, conditions) for data privacy enforcement based on HIPAA
•Anomaly detection and response for databases:
  It extends Hippocratic Databases with protection from insider threats. It monitors user activities, detects anomalies, and automatically reacts according to anomaly response policies
•Multi-domain digital identity management in HC environments (VeryIDX)
  It supports a privacy-preserving approach to identity verification in the context of e-prescriptions

Patient Monitoring – Policies in FENCE



Health Improvement Services

Social Network Vulnerabilities (Gtech)

Vulnerabilities analogous to traditional media

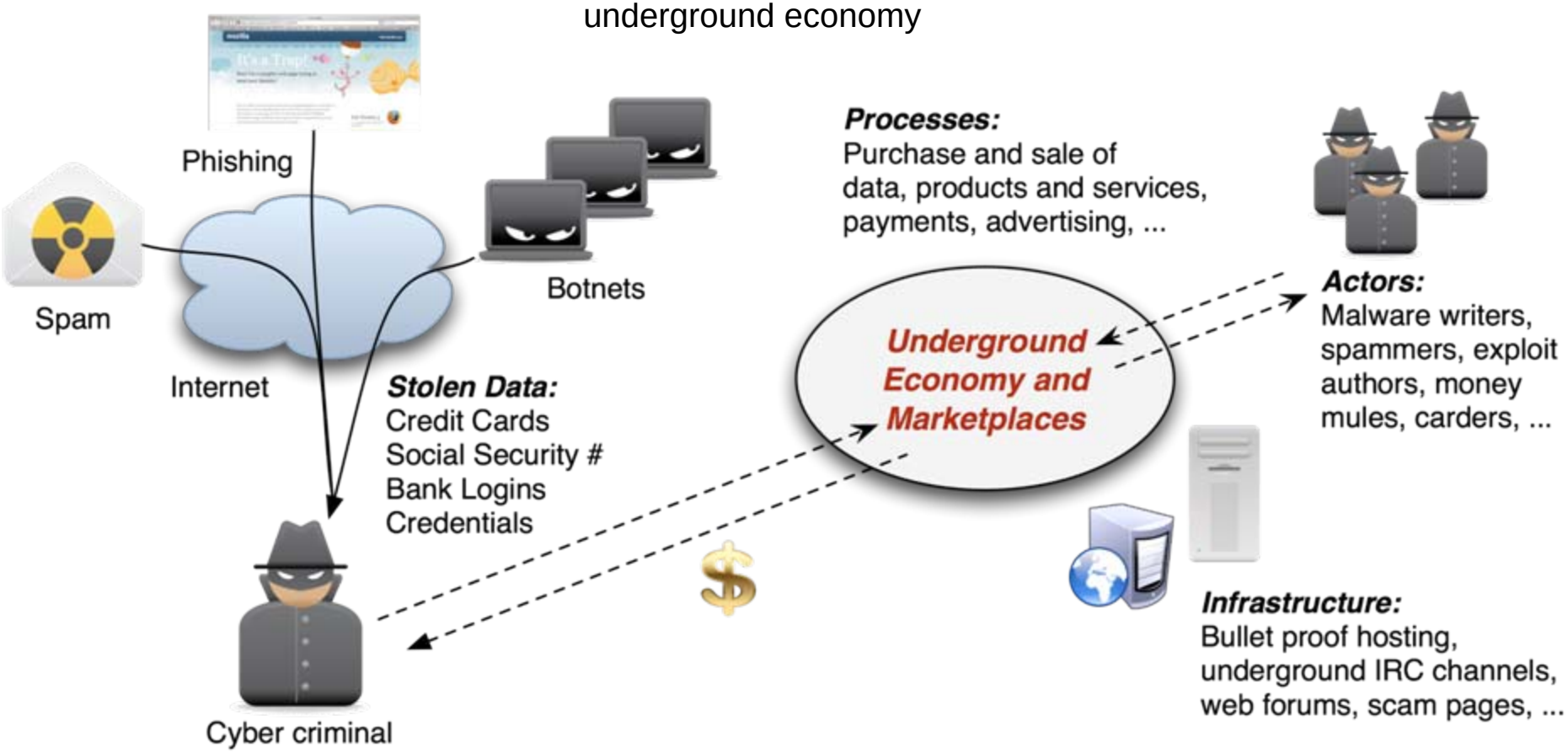
- Social-network enhanced phishing
- Message spam
- Malware propagation

Impersonation risk

- Some obvious
- Some not-so-obvious

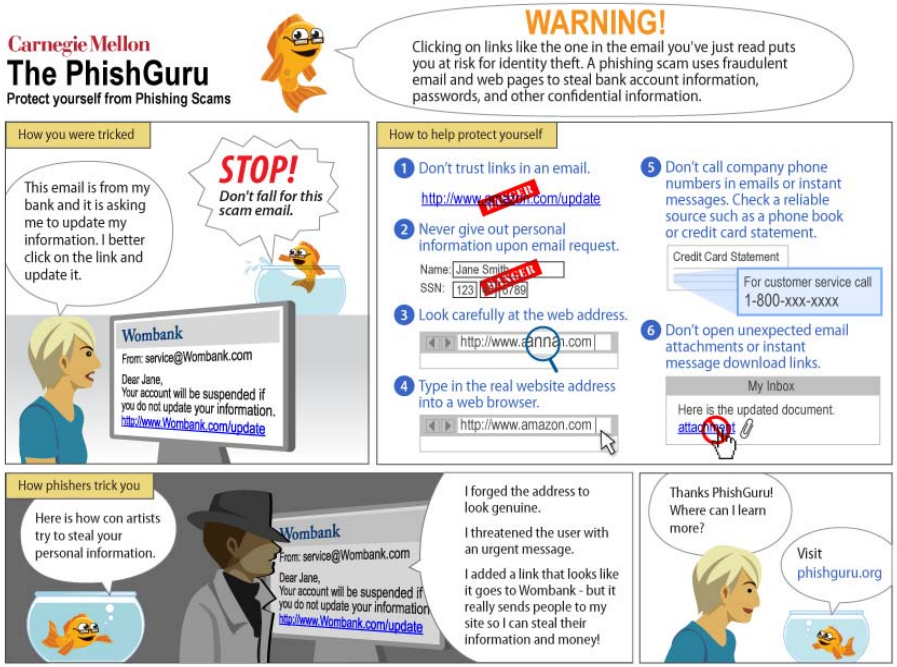
Understanding the Underground Economy (UCSB)

analyze underground economy (actors, processes, infrastructure)
build upon this understanding to disrupt underground economy



PhishGuru: Embedded training (CMU)

- Users don’t seek out or read security training
- Send emails that looks like phish, if recipient falls for it, intervene with training
- Studies show people learn and remember embedded training
- Same training sent directly isn’t effective
- Interventions designed using learning science principles
- Takes advantage of “teachable moments”



http://phishguru.org/

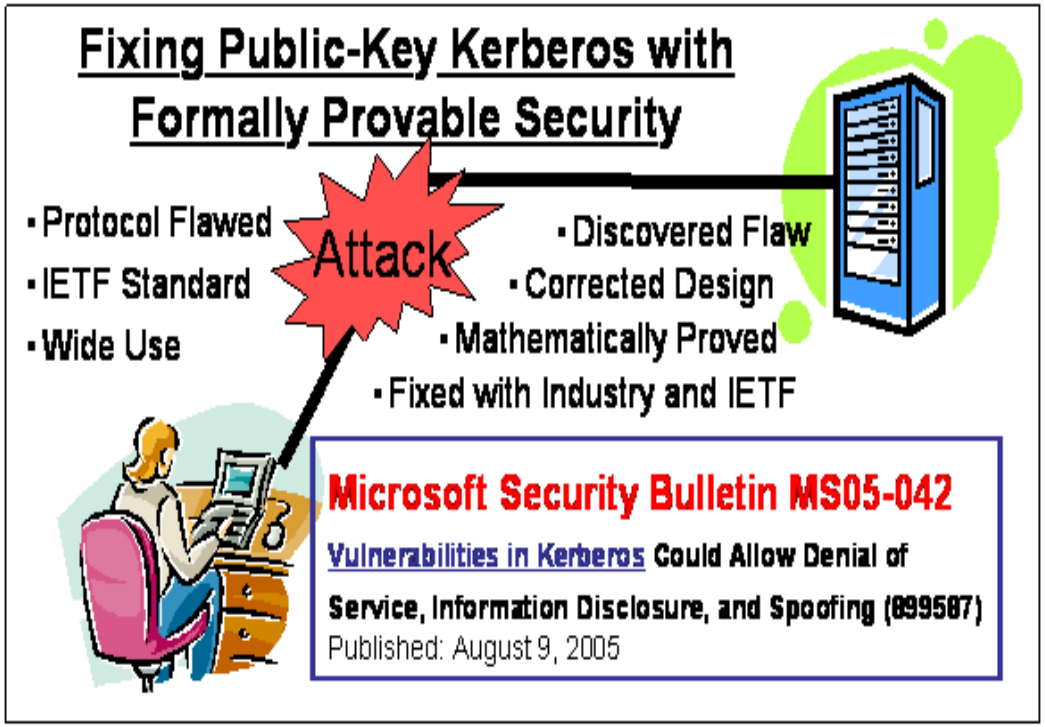
P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. Cranor and J. Hong. **Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer.** *Proceedings of the 2nd Annual eCrime Researchers Summit,* October 4-5, 2007, Pittsburgh, PA, p. 70-81.

Decade-old Kerberos Fault Found using Formal Methods

Collaborative research: High-Fidelity Methods for Security Protocols

Logical methods based on symbolic execution of protocols and computational methods involving probability and polynomial-time are integrated in design and security analysis of crypto-protocols, the most fundamental and challenging security research

- FY04 4-year, $2M award
- Stanford, U.Pennsylvania, U.Texas, UCSD
- Co-sponsor ONR



The flaw was discovered in the specification of the public-key extension to the Kerberos protocol. The flaw was implemented faithfully in the authentication software by major software developers. The defect placed millions of computers worldwide at risk. The methodology developed in this analysis of Kerberos is applicable to a wide range of security protocols.

Security Testbeds

- **DETER:** USC/ISI, UCB
  - Development mostly funded by NSF with co-funding from DHS
  - Currently, operation and maintenance mostly funded by DHS
- **GENI:** BBN plus others
- **WAIL:** Wisconsin, BU
- **Orbit:** Rutgers

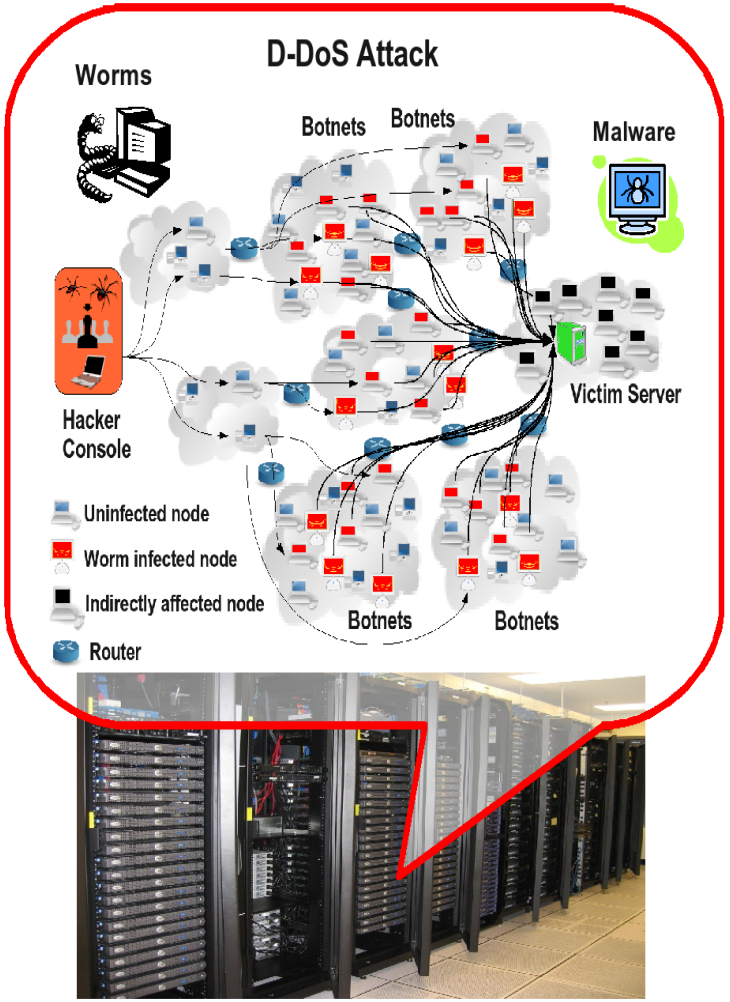
DETER Cyber Security Testbed (USC, UCB)

Unique national-scale resource, providing a rich and flexible experimental environment for cyber-security research.

Enables testing of cyber defenses against threats such as worms, viruses, denial of service, and routing attacks.

Performing research in testbed architectures for federation, experiment construction and risky experiment management

Use DETER to create a science of security experimentation



GENI supports Fundamental Challenges
Network Science & Engineering (NetSE)

Understand the complexity of large-scale networks

- Understand emergent behaviors, local-global interactions, system failures and/or degradations
- Develop models that accurately predict and control network behaviors

Network science and engineering researchers

Develop new architectures, exploiting new substrates

- Develop architectures for self-evolving, robust, manageable future networks
- Develop design principles for seamless mobility support
- Leverage optical and wireless substrates for reliability and performance
- Understand the fundamental potential and limitations of technology

Distributed systems and substrate researchers

Enable new applications and new economies, while ensuring security and privacy

- Design secure, survivable, persistent systems, especially when under attack
- Understand technical, economic and legal design trade-offs, enable privacy protection
- Explore AI-inspired and game-theoretic paradigms for resource and performance optimization

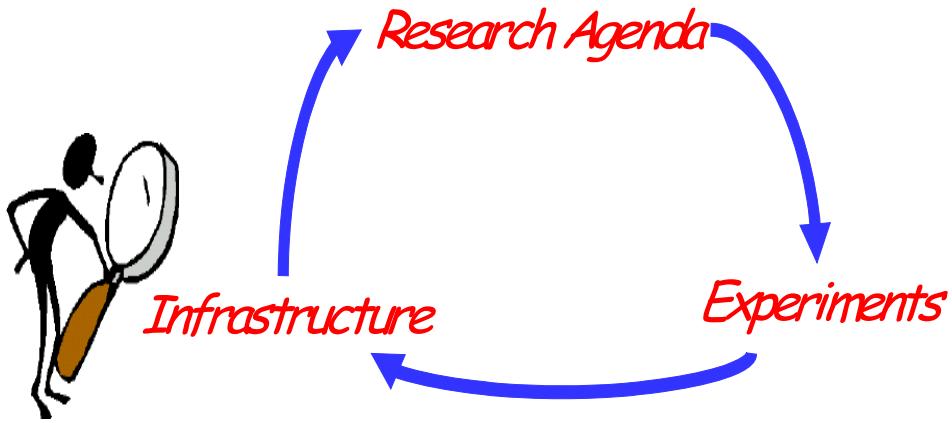
Research Agenda to Experiments to Infrastructure

Research agenda

- Identifies fundamental questions
- Drives a set of experiments to validate theories and models

Experiments & requirements

- Drives what infrastructure and facilities are needed



Infrastructure could range from

- Existing Internet, existing testbeds, federation of testbeds, something brand new (from small to large), federation of all of the above, to federation with international efforts
- No pre-ordained outcome

Existing Input

Clark et al. planning document for Global Environment for Network Innovations

Shenker et al. "I Dream of GENI" document

Kearns and Forrest ISAT study

Feigenbaum, Mitzenmacher, and others on Theory of Networked Computation

Hendler and others in Web Science

Ruzena Bajcsy, Fran Berman, and others on CS-plus-Social Sciences

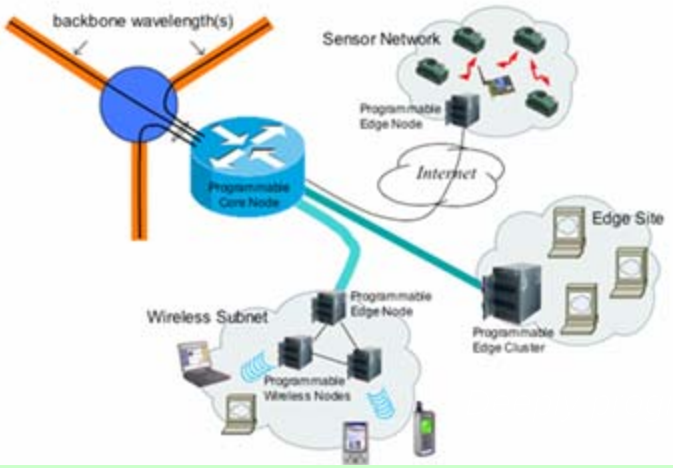
NSF/OECD Workshop "Social and Economic Factors Shaping the Future of the Internet"

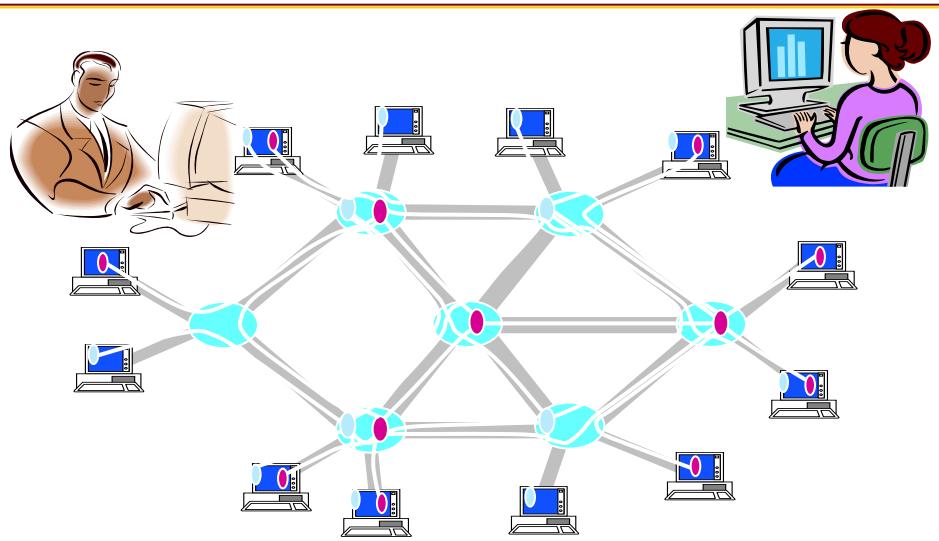
NSF "networking" programs

- FIND, SING, NGNI

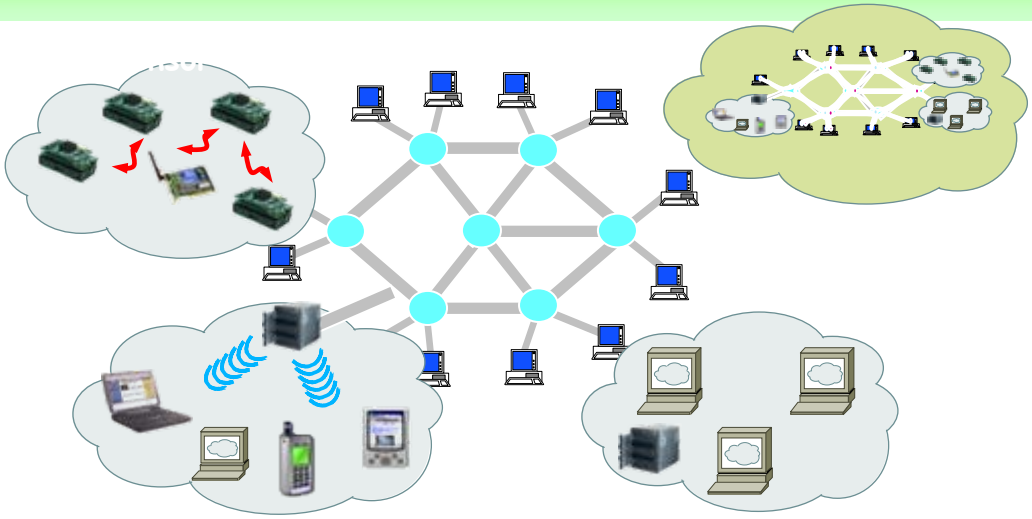
The GENI Vision

A national-scale suite of infrastructure for long-running, realistic experiments in Network Science and Engineering





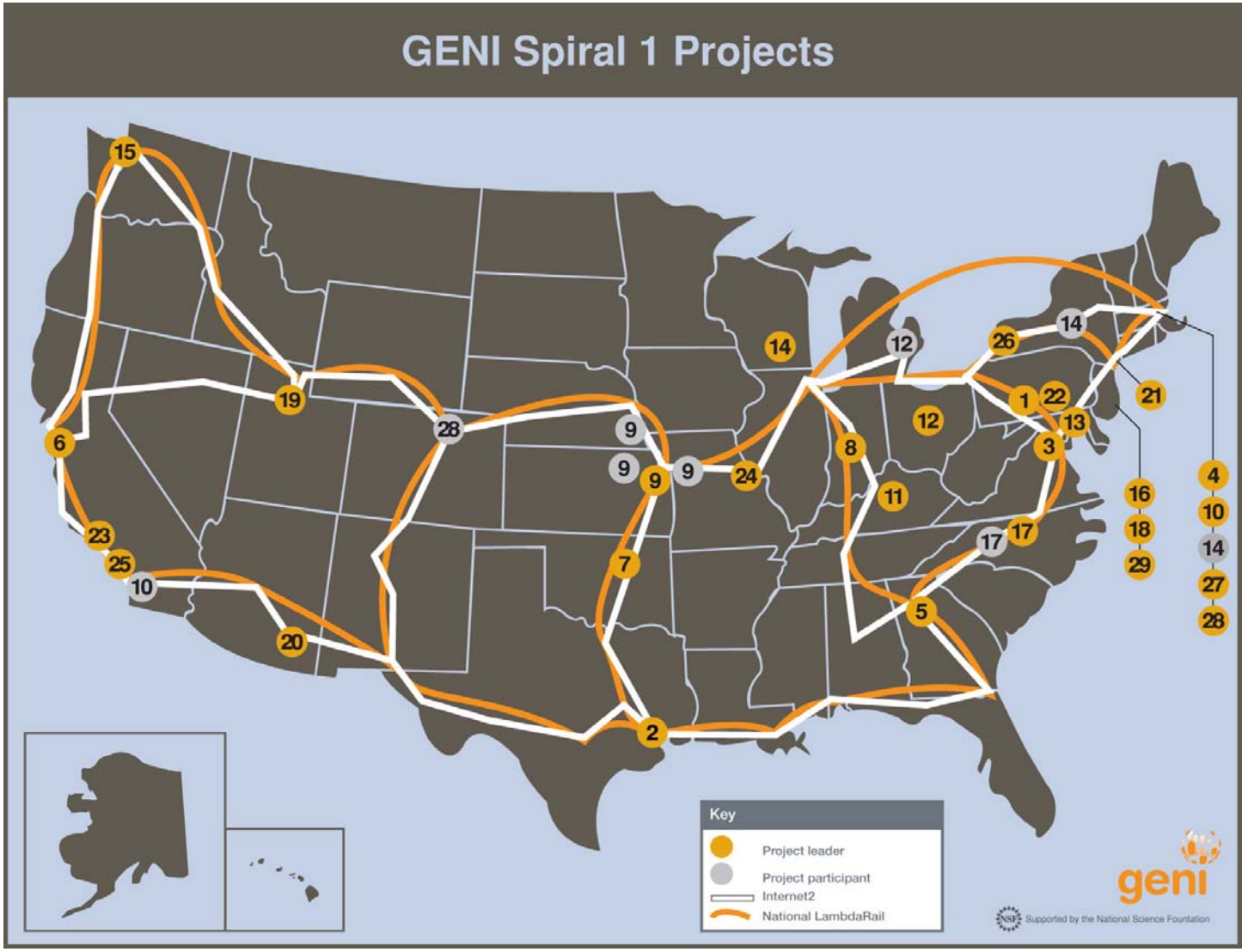
Programmable & federated, with end-to-end virtualized "slices"



Current status - GENI Spiral 1

Rapid prototyping, integration, and early experiments

More security projects are being solicited



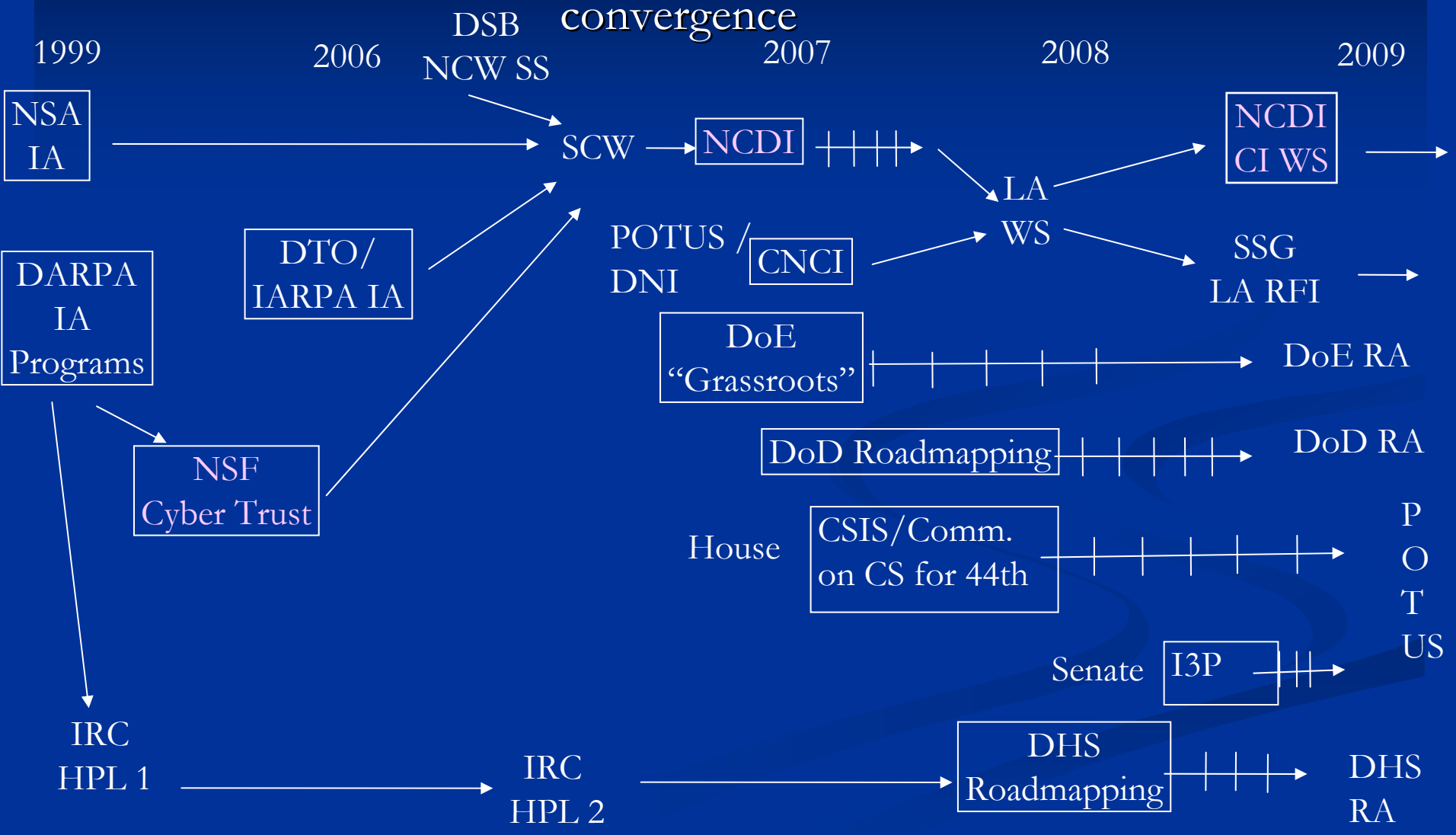
NSF Inter-Agency Activities including Planning and Coordination (cont.)

CNCI activities

- With IARPA/DHS/ONR formed NCDI (National Cyber Defense Initiative)
- “Grass-Roots” research-directed effort that morphed into “Leap-Ahead”
- Organized workshops
  - Mostly on planning
  - But, also at the intersection of security, policy and economics
  - Industry-Academia workshop with industry in November 2008
- March 2009: organized a teleconference between Melissa Hathaway and 30 NSF PIs to provide input for the “60 day plan”.
- Also, participating in CNCI’s education effort with the goal of more security experts at many different levels

Weaving a National Initiative?

- Striving for convergence



NSF Security Education Activities

- CPATH: **Funds use of security testbeds in education (USC-ISI)**
- Scholarship for Service
- Participate in CNCI Education Activities
- K-12 Security Education

Carnegie Cadets:
The MySecureCyberspace Game

An interactive game designed for 4th and 5th graders that teaches Internet safety and computer security in a safe, fun setting

Children take on the role of cadets of the Carnegie Cyber Academy

Through a series of "missions," children learn the skills they need to protect themselves online

- Filter out all the spam emails from the good emails of Cyberspace
- Keep the chatroom safe from weirdo strangers asking for personal information
- Help identify Web site dangers by collecting sample specimens

Reinforces principles of safe, responsible, and appropriate online behavior

Players learn the real-world consequences of cyber crimes

www.carnegiecyberacademy.com

Is There a Science of Security?

Are there *impossibility* results?

Are there powerful *models* (like Shannon's binary symmetric channel) so that realistic security and privacy properties can be computed? Possibilies include:

- Control Theory for security
- Kirchoff-like laws to capture normal behavior for routers

Is there a theory that enables:

- Secure systems to be *composed* from insecure components, or even
- Secure systems to be composed from secure components

***Metrics:* Is there a theory such that systems can be ordered (or even partially ordered) with respect to their security or privacy?**

Can entire systems (hosts, networks) and their "defenses" be *formally verified* with respect to realistic security objectives and threats?

Are there security-related hypotheses that can be validated *experimentally*?

What kind of an instrument (*testbed*) is needed to validate such hypotheses?

NSF/IARPA/NSA organized a workshop on SOS, Nov. 2008

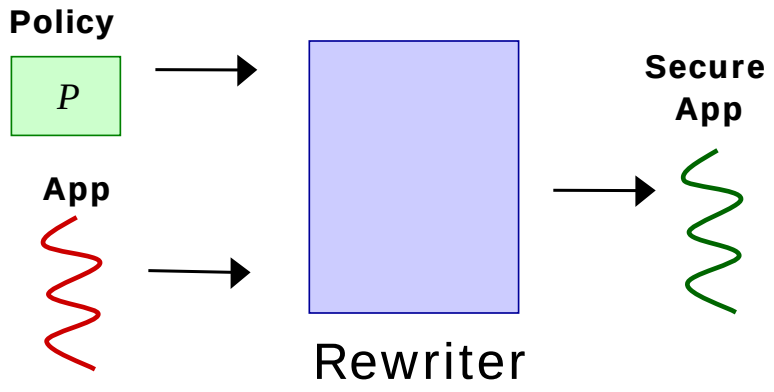
Enforcement by Program Rewriting: Are two security applications the same?

Fundamental issues:

- Does the application behave the same?
- Can the application subvert enforcement code?

Pragmatic issues:

- What policies can be enforced?
- What is the overhead of enforcement?



Opportunities/Needs for International Cooperation

Much attack activity is indiscriminant ⇒ significant utility in sharing information via distributed sensors

- With caveat that even so, perspectives are *not* homogeneous

⇒ Non-local defenses require international coordination

- Whether proactive (e.g., anti-spoofing) or reactive

⇒ Incident response & forensics require international coordination

Some facets of organized cybercrime appear to have national components (e.g., Russian mafia)

NSF (with DHS) is collaborating with the EC (and other bodies on the design of a Future Internet

NSF offers supplements to U.S. PIs

Envisioning a Rich Inter-site Analysis for Cooperative Attack Mitigation

Sites deploy *activity repositories* using common data format

Site A can send request for analysis against activity seen by Site B

- E.g. “have you seen the following access sequence?”
- Done by sending an *analysis program*
- Note: due to co-aligned threat models, it’s often in B’s interest to investigate

B runs query against their repository …

- … can also install same query against future activity

B decides what (sanitized) results to return to A

- If request was unreasonable, B can **smack** requestor

Opportunities and Future Directions for NSF Security Research

Future Directions: Increasing emphasis

- Understand the key assumptions that will drive security research
- Anticipating and understanding future cyber threats arising from advances in
  - Pervasive computing (*esp* privacy, provenance, attestation)
  - Service oriented architectures (*esp* composable provable trusts, policies)
  - Cross-enterprise (and cross-coalition) sharing and interoperation
- Research into the foundations of trust
  - The limits of what can and cannot be known about trust
  - Is there a Science of Security
  - Covert channels and information hiding affecting security and trust
- Special economic and societal impact
  - Anonymity, anti-spam, anti-spyware, competitiveness, critical infrastructures
- Towards an overarching security architecture that integrates the many but specific solutions NSF PIs have developed

Test beds and Methodology for Experimentation and Evaluation

- Continued joint development of research testbeds including DETER, ORBIT, …
- Repository of anonymized sharable test data based on actual events/behaviors
- Open source software and wide-distribution of benchmark results

The Meaning of Security Defense has Changed

1st Generation
(Prevent Intrusions)
'80s

Trusted computing base, access control, crypto

Intrusions will Occur

Firewalls, VPNs, PKI, Intrusion Detection Systems

2nd Generation
(Detect Intrusions, Limit Damage)
'90s

Some Attacks will Succeed

Intrusion tolerance, graceful degradation, hardened cores, real-time situation awareness and response…

3rd Generation
(Operate Through Attacks)
'00s

"Intel" Will Direct Defenses

4th Generation in '10s
(E.g.,prediction of vulnerabilities, cross-enterprise negotiation before attacks, real-time reverse engineering of attacks and malware, planning methods to deal with expected attacks, automatic patch synthesis and distribution)

SUMMARY

Strong multi-disciplinary basic research program addressing fundamental issues of security and privacy of societal and economic importance

Fiscal health is excellent but variability in future funding for FY08 and beyond will affect planning

Excellent opportunities for co-sponsorship with other S&T agencies including international agencies

Major role in strategic planning for a National Cyber Defense Initiative (NCDI) with senior directors at DOD/NSA/DNI

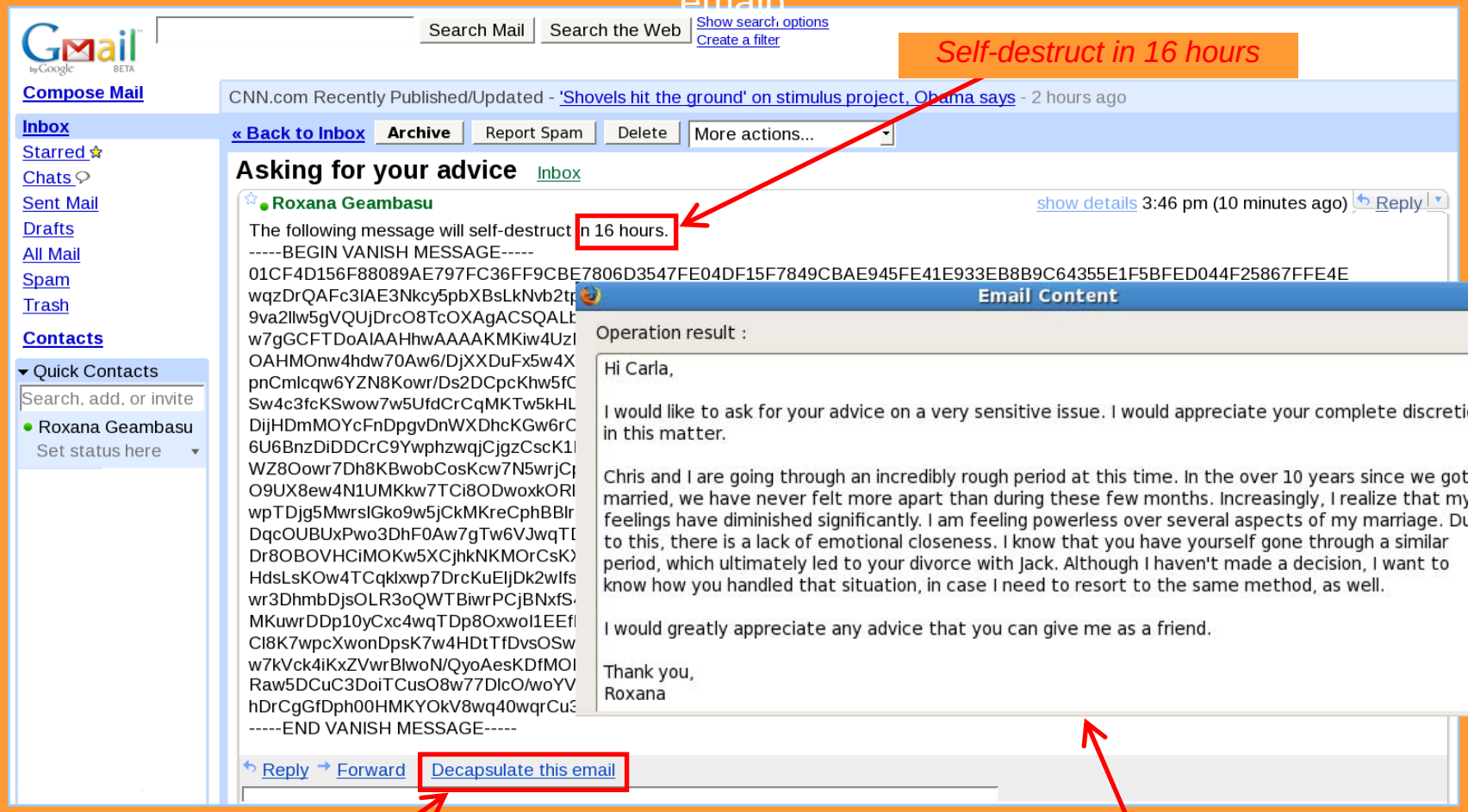
Meeting the challenges for improving quality of life and society in cyber space

Appendix:
More Examples

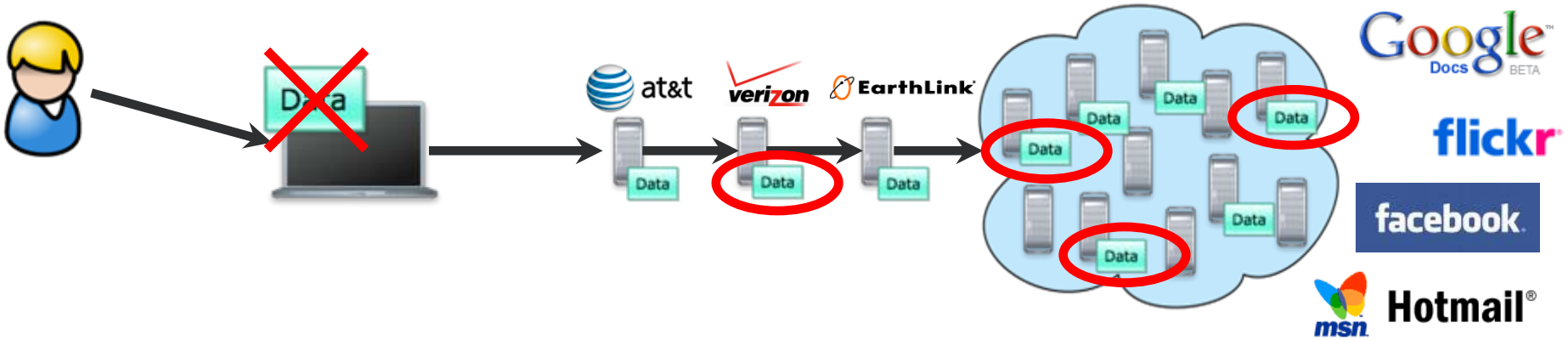
Disappearing Data: Overcoming New Risks to Privacy

Screenshot of GMail prototype plugin

(Email stored by GMail, but will self-destruct and become permanently unreadable after 16 hours, regardless of where GMail stores or archives the email)



Disappearing Data: Overcoming New Risks to Privacy



New risks to privacy

Encryption alone does *not* solve the problem

protect privacy of archived data

Disappearing Data: Overcoming New Risks to Privacy

Online Spam and Deception

Project: *Adaptive Attacks & Defenses in Denial of Information*

- Georgia Tech, Univ. Georgia, and collaborators

Objectives: Find *structural patterns* in spam content, metadata, construction, and delivery mechanisms to identify spam reliably despite adaptive attacks (e.g., randomization of content)

Results: Reliable defenses based on structural patterns that are successful against adaptive attacks in various media

- Text: Reliable spam identification despite camouflage
- Image: Distinguishing (text-rich) image spam
- Web: Predicting spam before loading page (HTTP headers)
- Social network: Identifying deceptive profiles and behaviors

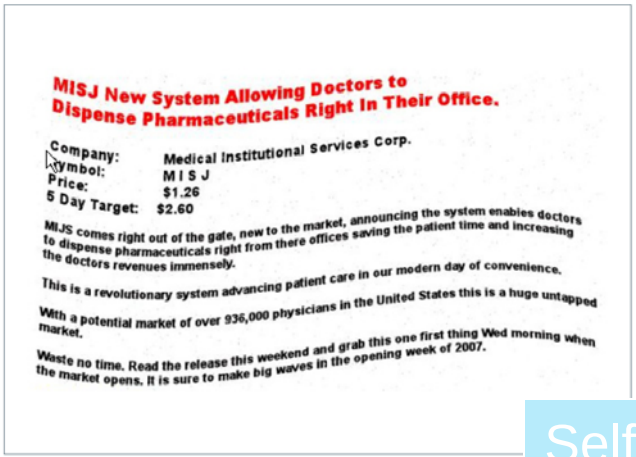
Plans to strengthen defenses against spam

- Public data set collection for evolutionary studies of attack techniques and evaluation of defenses
- Spam in social media (e.g., vandalism in blogs and Wikipedia) and other media (e.g., VoIP, Instant Messaging)

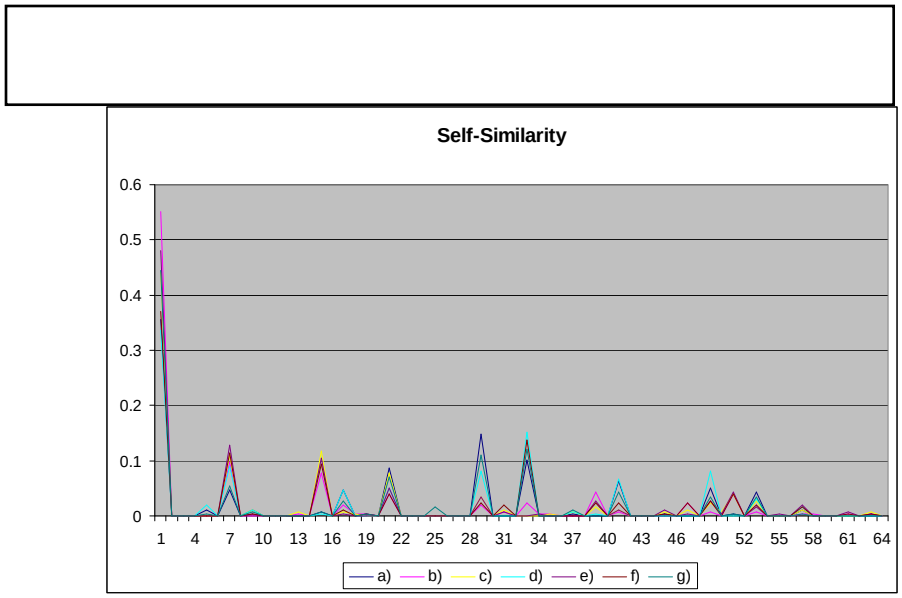
Structural Patterns in Image Spam

Image spam needs conspicuous text for "selling the product"

- image equivalent of "shouting" (few, strong colors), self-similarity due to text



Self-Similar



Identity Management is Central to Security

The current situation with source addresses

- They are often used to identify end users
- But, they can be forged
- And, it is impossible to extract information from the network to permit traceback

Some thoughts on how a future Internet could improve the situation

- Network could require a binding between a packet's source address and the identity of the sender
- But, this permits the network to violate end-users' privacy
- There is a middle-of-the road possibility: The linking of a user to a source address is held by a trusted third party that can (partially) revoke anonymity

In any event, new protocols and network services are needed

Towards an Accountable Internet Protocol (AIP)

- Georgia Tech, Berkeley, MIT
- Key idea: New addressing scheme for networks and hosts
- Addresses are self-certifying
- Simple protocols that use properties of addressing scheme as foundation
  - Anti-spoofing, secure routing, DDoS shut-off, etc.

AIP Addressing

Autonomous domains, each with unique ID

An AD…

Would fail together
Single administrative domain

Key Idea:

AD and EID are *self-certifying flat names*

- AD = hash(public_key_of_AD)

a glo

- Self-certification binds name to named entity

Botnets Are a Long-Term Problem

Individual Machines Used to Be Targets ---

Now They Are Resources

Bot (Zombie)

- Software Controlling a Computer Without Owner Consent
- Professionally Written; Self-propagating; 7% of Internet

Bot Armies (Botnets)

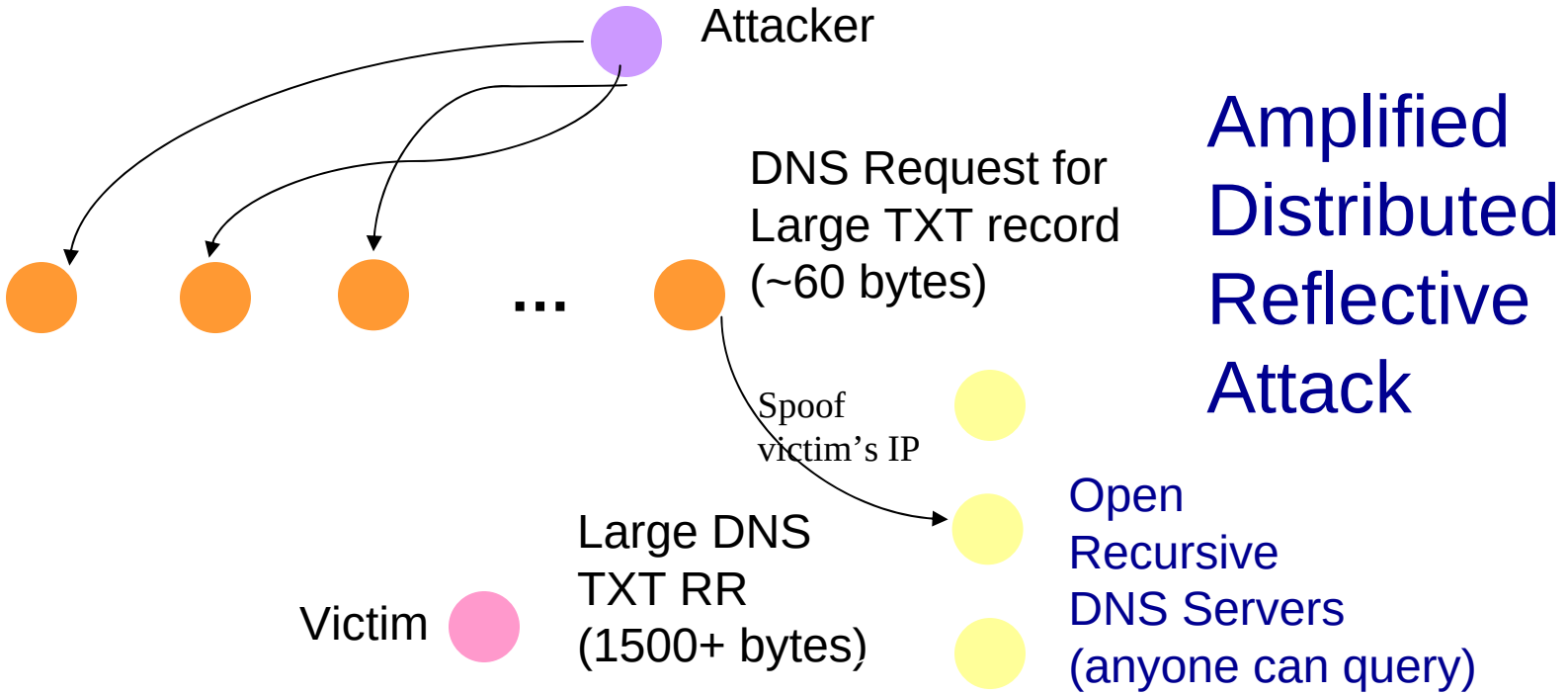
- Networks of Bots Controlled by Criminals
- Key Platform for Fraud and other For-Profit Exploits

Botnet Epidemic

More Than 90% of All Spam
All Denial of Service (DDOS) Attacks
Clickfraud
Phishing & Pharming Attacks
Key Logging & Data/Identity Theft
Key/Password Cracking
Anonymized Terrorist & Criminal Communication

Attack Example

Botnets increasingly used for amplified distributed reflective attacks



Thinking About the Botnet Problem

Botnets will continue to be an issue

- Any vulnerable host can become a bot
- There will always be vulnerable hosts

The source of a Botnet will be difficult to determine

Without accountability it is impossible to identify the commander of a Botnet

So, it is essential to stop or delay the growth or damage associated wth Botnets; *only the network can do this*

- An ISP or an enterprise router can detect Bot-like traffic
- And, perhaps block or delay such traffic

But, there are consequences to blocking

- Blocking consumes precious human and device resources
- False positives will lead to many calls to a help desk

Denial of Service Attacks

DDoS attacks are a consequence of Botnets

Mitigation of DDoS attacks: Host (especially service solution)

- Distribute services over many machines; packets will be routinely routed to closest machine which might not be DoSed (yet)

Mitigation of DDoS attacks: Network solution

- *Pushback* to block or delay traffic from Bots, but there are consequences due to false positives
- *Diffusion* in routing: choose a route that avoids DDoSed hosts and machines instead of the optimal route

Envisioning a Rich Inter-site Analysis for Cooperative Attack Mitigation

Sites deploy *activity repositories* using common data format

Site A can send request for analysis against activity seen by Site B

- E.g. “have you seen the following access sequence?”
- Done by sending an *analysis program*
- Note: due to co-aligned threat models, it’s often in B’s interest to investigate

B runs query against their repository …

- … can also install same query against future activity

B decides what (sanitized) results to return to A

- If request was unreasonable, B can **smack** requestor

Envisioning a Rich Inter-site Analysis for Cooperative Attack Mitigation

Sites deploy *activity repositories* using common data format

Site A can send request for analysis against activity seen by Site B

- E.g. “have you seen the following access sequence?”
- Done by sending an *analysis program*
- Note: due to co-aligned threat models, it’s often in B’s interest to investigate

B runs query against their repository …

- … can also install same query against future activity

B decides what (sanitized) results to return to A

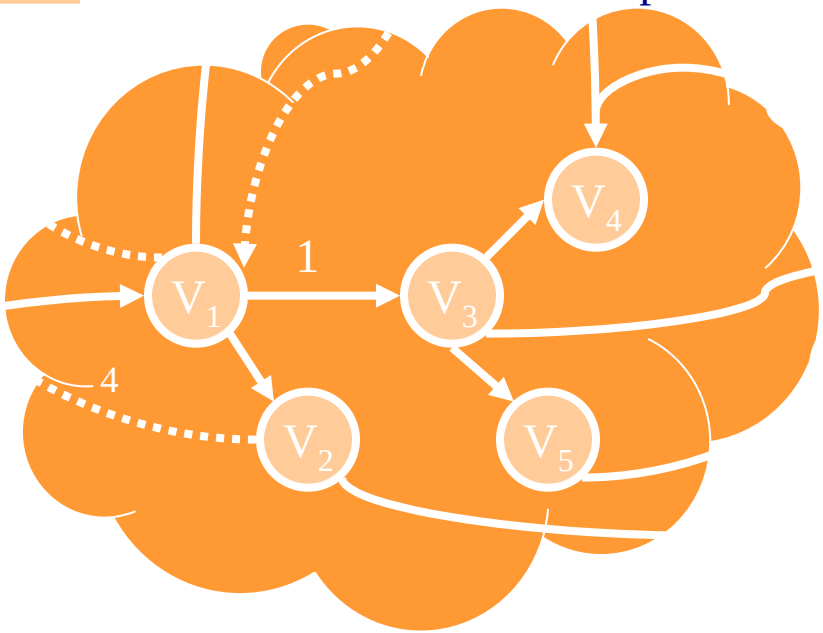
- If request was unreasonable, B can **smack** requestor

Example: KarstNet at Georgia Tech
A Botnet detection/elimination architecture

Dynamic DNS

www.hackers.com
10.0.0.1
(Command&Control box)

3': Anomaly detection and DNStop alert (10.0.0.1 is Botnet domain);
DynDNS updates `CName` to point to sinkhole



1: propagate;
"www.hackers.com"
coded in malware

Malware Author

www.hackers.com