

Cyber Conflict

Dorothy E. Denning

Department of Defense Analysis

Naval Postgraduate School

dedennin@nps.edu

<http://faculty.nps.edu/dedennin/>

Topics in Cyber Conflict

- **Hacktivism**
 - Cyber attacks by non-state actors for political and social reasons
 - Includes patriotic hacking, social hacking, and electronic jihad
- **Cyberterrorism**
 - Cyber attacks for political and social reasons that cause severe harm and generate fear
- **Cyber warfare (cyberwar)**
 - Cyber attacks by nation-state against nation-states
- **User authentication**
 - One form of cyber defense

Hacktivism - Findings

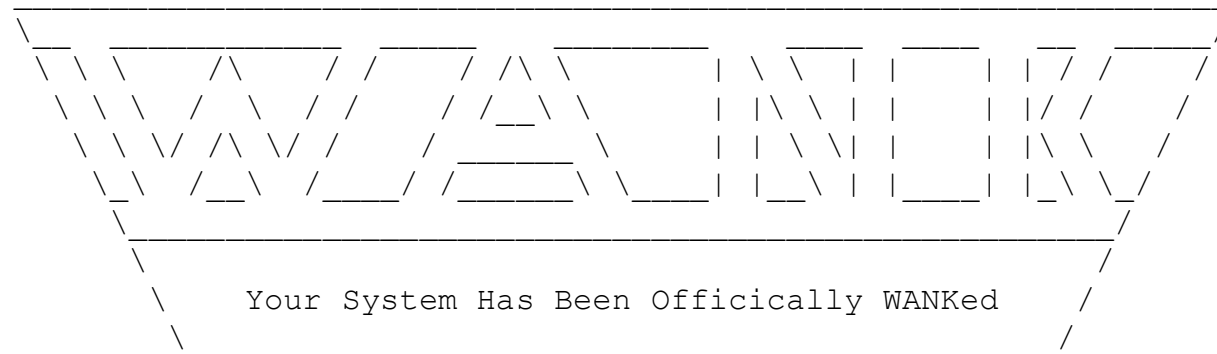
- Began over 20 years ago
- Tied to conflicts and issues beyond cyberspace
 - Kosovo, Kashmir, Mideast, GWOT, Chechnya, Estonia, Georgia, spy plane
- Supported by websites and forums
 - Offer hacking tools, instructions, targets, attack coordination
- Disruptive but not destructive
 - Web defacements, DoS/DDoS, email floods



<http://hacktivism.tao.ca>

NASA WANK Worm

W O R M S A G A I N S T N U C L E A R K I L L E R S



You talk of times of peace for all, and then prepare for war.

October 1989, just before launch of shuttle carrying Galileo probe.

Booster system was fueled with radioactive plutonium.

Spread on NASA's SPAN network

Took weeks to eradicate and cost NASA \$500,000.



United States

Department of Energy

Science, Security and Energy: Powering the 21st Century

May 1999

AT A GLANCE

NEWS & INFO

PEOPLE & PAGES

SCIENCE
EDUCATION

CONTENT MAP

SEARCH

HEADLINES

TECHNOLOGICAL ADVANCES

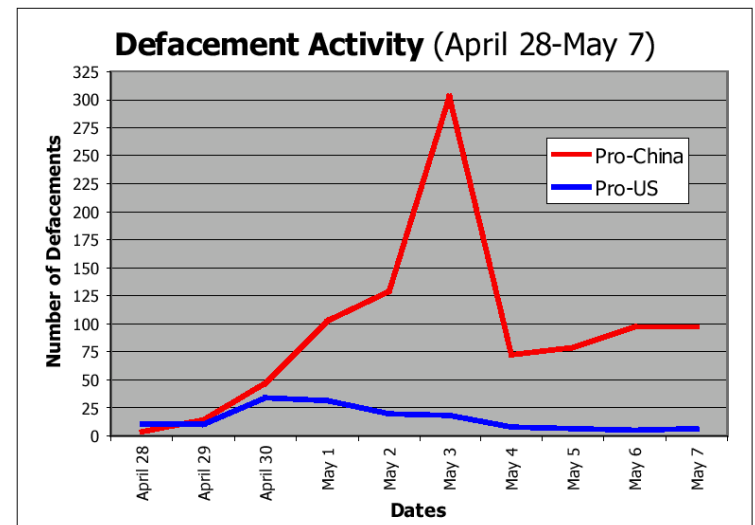
PROTEST U.S.A.'S NAZI
ACTION!

PROTEST NATO'S BRUTAL
ACTION!



Spy Plane Incident (April 1, 2001)

- Organized, sustained cyber attacks, mainly 4/28/01-5/8/01
 - Over 1,400 defacements from 140 separate hacker handles
- Pro-Chinese hackers
 - Honker Union of China, China Eagle group, Green Army Corps
 - Internet postings and IRC to plan, coordinate assault
 - Defacements, e-mail floods, DDoS attacks against White House, CIA
- Pro-US hackers
 - Pr0phet, Hackweiser, World of Hell



GForce Pakistan Strikes back!

GWOT Hacktivism - Oct 17, 2001 defacement of National Oceanic & Atmospheric Administration
Announced Al Qaeda Alliance Online
Gforce Pakistan, Pakistan Hackerz Club, Anti-India Crew

WAR AGAINST ISLAM?

Though GForce Pakistan, condemns the attacks on US, We also stand by Al-Qaeda. Usama Bin Laden is a holy fighter, and whatever he says makes sense. While Sharon murders innocent mulims in palestine, Bush has dinner with him. Now what's that suppose to mean? and is that not terrorism?

Tears come out of my eyes when I see the innocent infant baby with no face... why? because some Israeli decided to shoot a 2 month old infant

Mirror saved on 10/02/2005

Defacer: IHS IRAN HACKERS SABOTAGE

Domain: http://wiki.novell.com

IP address: 130.57.4.37

System: Linux

Web server: Apache

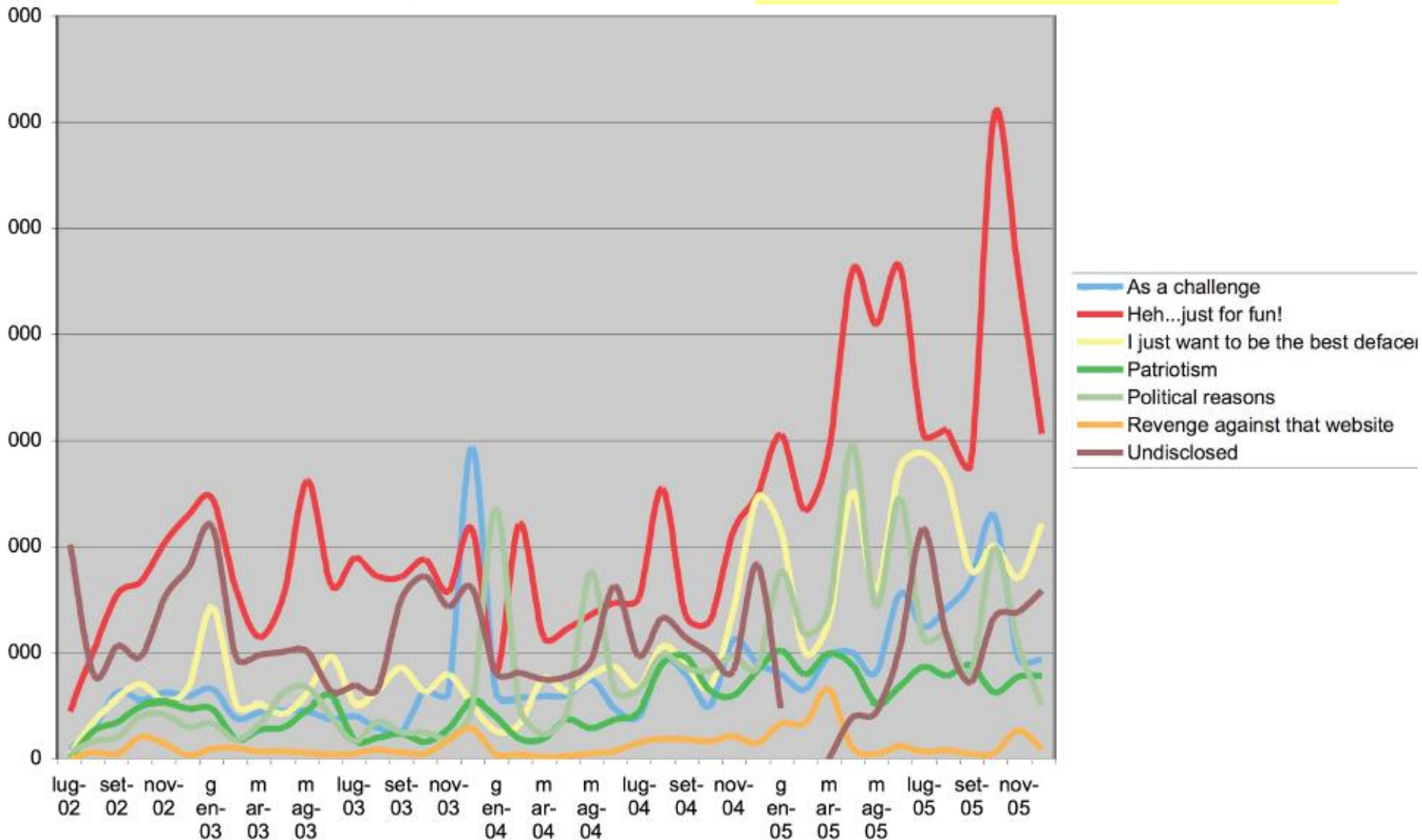
Attacker stats



IHS IRAN HACKERS SABOTAGE WAS HERE

Atomic energy is our right

even with threatening us NO one can rule us not to use atomic power , it is our right and we (all
iranian people) are united in this matter
we are being industrialized and being industrialized means need for more energy and this energy
should come from somewhere
we want from iran government than quit NPT as soon as possible and close the UK embassy in
iran where all of these problems come from



Electronic Jihad

M. As-Salim, *39 Ways to Serve and Participate in Jihad*, 2003

Principle 34 (Electronic Jihad) on media operations and cyber attacks

Hacking "... is truly deserving of the term 'electronic Jihad' since the term carries the meaning of force; to strike and to attack. So whoever is given knowledge in this field, then he should not be stingy with it in regards to using it to serve the Jihad. He should concentrate his efforts on destroying any American websites, as well as any sites that are anti-Jihad and Mujahidin, Jewish websites, modernist and secular websites."

Anwar al Awlaki, *44 Ways of Supporting Jihad*, 2009 (in English)

Principle 29 (WWW Jihad) covers media operations but *not* cyber attacks

Danish Cartoon Attacks



Response to publication of cartoons satirizing Prophet Mohammad in Danish paper *Jyllands-Posten*

Web defacements [Zone-h.org]

- 2,817 Danish websites [1/21/06 - 2/22/06]
- Roberto Preatoni, Zone-h, said that it was about 10-20 times more than normal and “the biggest, most intense assault” he’d seen

Denial of Service (DoS) attacks

- *Jyllands-Posten* website primary target
- 3asfh.com released video purportedly documenting their attack
 - Video and still shots at <http://haganah.org.il/harchives/005456.html>
- Republishers also hit, including Michelle Malkin’s blog

Coordinated through al-Ghorabaa website

Electronic Jihad DoS Tool

- Version 2.0 features
 - Gets targets from al-jinan site
 - Handles different Internet speeds
 - Proxies override website blocking
 - Awards to attackers

- Targets websites critical of Islam
2nd campaign 2007

love4all.us

islameyat.com

aldalil-walborhan.com

rapsaweyat.com

investigateislam.com

meca-me.org

ladeeni.net

meca-love4all.com



Version 1.5

Talk Big – But

- **Massive DoS attack to disable 13 root name servers**
 - Posting on jihadi forum discusses possibility, but got no response
 - Claims it “would help destroy all of the west” and cause fall of global economy
 - Source – Terrorism Research Center, Jun 26, 2006
- **Disabling all electronic networks around the world**
 - To include military nets that control radars, missiles, and communications
 - Claims that disabling for a day will bring about total collapse of the West and breakdown of world economy and stock markets
 - Source – Alshech, Cyberspace as a Combat Zone, *MEMRI*, Feb 27, 2007
- **Suggestions for electronic war**
 - Disable and paralyze battlefield C2 networks, GPS, GPRS, GSM
 - Disrupt enemy banks, oil control grids, navigation techniques
 - Target enemy’s data flowcharts to paralyze life in country – but “do not ask me what flow charts are”
 - Disable American missile attack or redirect missiles to launch site

UK Trio



- Convicted of using Internet to incite terror murder
 - Waseem Mughal
 - Younes Tsouli (Irhabi007/Terrorist007)
 - Tariq al-Daour
- Used stolen credit card info obtained via phishing and Trojan horses
 - Charged over \$3.5 million against cards at online stores
 - Laundered money through gambling sites
 - Accounts set up with stolen credit card numbers
 - Winnings withdrawn and transferred to own accounts
- Set up jihadi Web forums and sites
 - At least 72 cards used to register over 180 web sites at 95 hosting firms
 - Used FTP site of Arkansas Highway and Transportation Dept., GWU
 - Posted 20p “Seminar on Hacking Websites”
- David McGuire, *Washington Post*, 7/13/04; Brian Krebs, *Terrorism’s Hook Into Your Inbox*, *Washington Post*, 7/5/07

Hacktivism - Questions

- How will hacktivism evolve?
 - Will some hacktivists become cyber terrorists?
- Should states be responsible for their hackers?
 - Can states control their hackers?
 - Are patriotic hackers encouraged or supported by their states?
- How should states respond to hacktivism?
 - Defense only? Prosecution? Attack back?

Cyberterrorism - Findings

- It hasn't happened
- Hacktivists/jihadists not currently interested or capable
- Jihadists sometimes talk big
 - But lack capability to deliver
- But ... critical infrastructures are vulnerable and have suffered damaging attacks



Cyber Attacks on Critical Infrastructures

- Hackers caused 28 power outages in Wisconsin affecting 30,000 customers [1999]
 - Joseph Konopka & members of “Realm of Chaos”; damages of \$800,000 in NE Wisconsin [‘Dr. Chaos’ Goes to Prison for Hacking, *CNN*, 12/1/05]
- Former insider attacked Australian sewage system [1999]
 - Caused raw sewage overflows (\$13K damages; \$100K monitor)
- 24-year-old man caused \$11.4 million run on Columbia’s Davivienda Bank [1999]
 - Sent e-mails to private individuals and employees urging withdrawal of funds in light of pending government intervention
- 14-year-old built infrared device to control Polish tram system [2008]
 - Derailed 4 trams and caused emergency stops and injuries

CI Vulnerabilities Revealed

- Worms (Code Red, Slammer, etc.) have disrupted numerous systems
 - Banking & ATMs, 911 systems, airline booking, train signaling, nuclear power plant monitoring
- Botnet hit computers at Northwest Hospital & Medical Center, 2005
 - Operating room doors didn't open, computers in intensive care shut down, and doctors' pagers failed
- Spies penetrated US power grid and left malware behind, 2009
 - From China, Russia, elsewhere [Siobhan Gorman, Electricity Grid in US Penetrated by Spies, *WSJ*, 4/8/09]
- Staged cyber attack shows vulnerability in power grid, 2007



Attack conducted at Idaho National Labs

<http://www.cnn.com/2007/US/09/26/power.at.risk/index.html>

<http://www.youtube.com/watch?v=fJyWngDco3g>

Cyberterrorism - Questions

- Will some hacktivists become cyberterrorists?
- Will some terrorists become cyberterrorists?
 - Will they develop the capability or outsource it?
- How can we assess the threat?
 - What are the indicators of a forthcoming capability or attack?
- Do we need special defenses?

Cyber Warfare – Findings

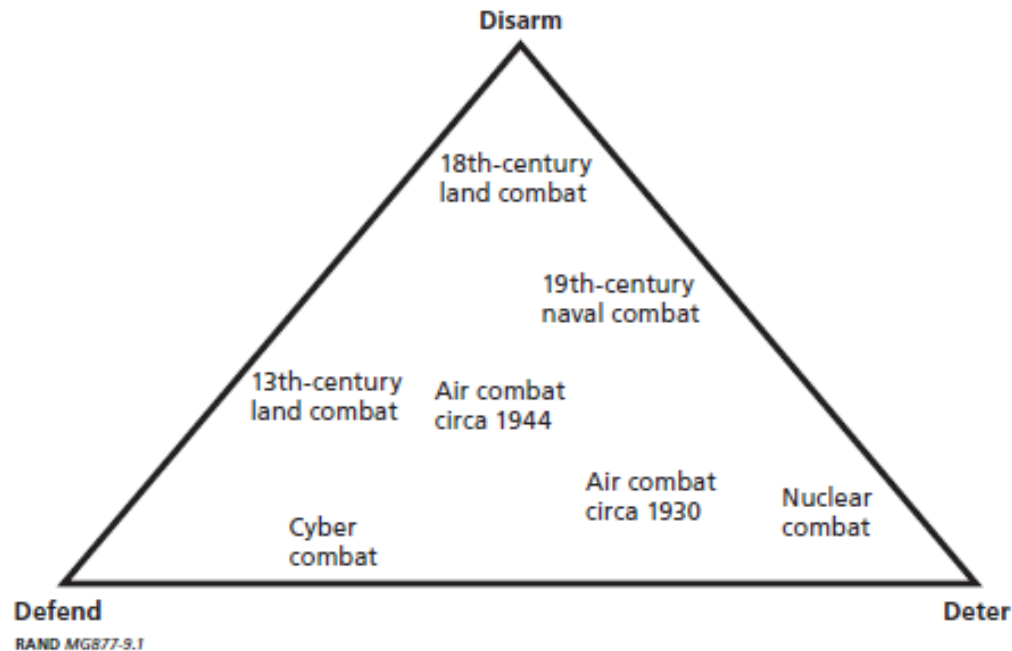
- Over 100 nations are developing capability
 - Fewer with advanced capabilities
- Attacks positively attributed to states have been narrowly focused to achieve specific results
 - Israel conducted cyber attack against Syrian air defenses to assist air strike against Syrian target in Sept. 2007
- Attribution has been a major challenge
 - Attacks by patriotic hackers are frequently attributed to states, but without presenting compelling evidence
- There are no explicit norms for cyber warfare
 - Applying norms of armed conflict is doable, but hard
- Numerous unresolved policy issues

Cyber Warfare – Questions

- **Role of cyberspace in warfare**
 - What will be or should be its role? What are its limits?
 - What attacks and targets are lawful and ethical?
 - Are treaties needed to declare norms and constrain attacks?
- **Effects of cyber attacks**
 - How do you determine or anticipate effects, including collateral damage?
 - When will it constitute an act of war?
- **Attribution and response**
 - How can you know who attacked you?
 - How should you respond to an attack? Go public? Attack back?
 - How can you anticipate how others will respond to your attacks?
- **Cyber deterrence**
 - Is it workable or even relevant?
 - Should deterrence policy be explicit?

Deter-Disarm-Defend

Figure 9.1
Where Various Forms of Combat May Fit in the Deter-Disarm-Defend Triangle



Martin Libicki, *Cyberdeterrence and Cyberwar*, RAND, 2009.

Cyber Defense: User Authentication – Findings

- **Methods for user authentication**
 - Cyberspace: secrets (passwords/PINs, backup questions)
 - Physical world: biometrics, things, social
- **Password rules don't scale for users**
 - So users don't follow the rules
- **Password rules don't address all major threats**
 - Phishing
 - Malware (Trojans, keyloggers, etc)
 - Circumvention
- **Active research area**

Biometrics

A TRUE STORY
CHANGELING IN SELECT THEATERS OCTOBER 24TH
EVERYWHERE OCTOBER 31ST

{ PREVIOUS } { CLOSE } { NEXT }



<http://www.changelingmovie.net/>

Biometrics & Digital Signatures

- Both can be used for authentication
- Both use publicly available information to authenticate
- Both assume that only the correct person can produce the authenticator
 - Digital Signatures use secrets (private keys)
 - Assumption fails if private key is stolen, cracked, or shared
 - Security requires protecting secrets and changing compromised secrets
 - Biometrics use biology (personal characteristics)
 - Assumption fails if person can be mimicked
 - Security requires discrimination and liveness

Social Authentication – Vouching

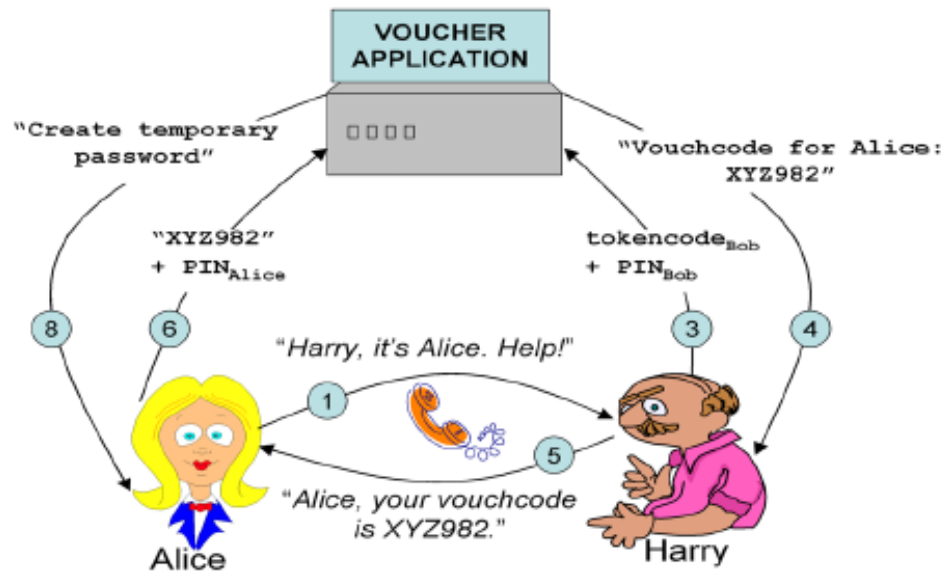


Figure 1: A schematic of the basic vouching process: Harry the helper aids Alice to obtain a temporary password. Step numbers correspond to those in text description (and some are omitted).

J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, M. Yung,
Fourth-Factor Authentication: Someone You Know, *CCS'06*.

Social Authentication

Possible Scenario for Social Network Site

System: **Enter your username: Alice**

System invites 3 people in Alice's network to authenticate her
2 people respond

Bob: **Who is your youngest niece? Nancy**

Bob accepts response

Carol: **When did you visit me in New York? October 2005**

Carol accepts response

System allows login

Authentication with Secrets About Your Network

Possible Scenario for Social Network Site

System: **Enter your username: Alice**

System: **Name someone in your network: Bob**

System: **Who is his youngest daughter? Nancy**

System: **Name someone else in your network: Carol**

System: **Where does Carol live? New York**

System allows login

Cyber Defense:

User Authentication – Questions

- Could we move away from secrets to biometrics?
- Can we make better use of things as authenticators?
- Can social networks play an effective role in authentication (and other areas of security)?
- Which authentication methods scale best for users (if every site used this ...)?

Recent Articles on Cyber Conflict

- Denning, D. E., “Cyber Conflict as an Emergent Social Phenomenon,” *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (T. Holt and B. Schell eds.), IGI Global, to appear.
- Denning, D. E., “Barriers to Entry: Are They Lower for Cyber Warfare?” *IO Journal*, April 2009.
- Denning, D. E., “Terror's Web: How the Internet is Transforming Terrorism,” to appear in *Handbook on Internet Crime* (Y. Jewkes and M. Yar, eds.), Willan Publishing, 2009.
- Denning, D. E., “Assessing the CNO Threat of Foreign Countries,” in *Information Strategy and Warfare* (J. Arquilla and D. Borer eds.), Routledge, 2007.
- Denning, D. E., “The Ethics of Cyber Conflict,” in *Information and Computer Ethics* (K. E. Himma and H. T. Tavani eds.), Wiley, 2007.
- Denning, D. E., “A View of Cyberterrorism Five Years Later,” *Readings in Internet Security: Hacking, Counterhacking, and Society* (K. Himma ed.), Jones and Bartlett Publishers, Boston, 2006.

pdf's at <http://faculty.nps.edu/dedennin/> .