Center for Security Technologies

Joseph A. O’Sullivan, PhD

Electrical and Systems Engineering

Associate Director, Center for Security Technologies

Chair, Faculty Senate

Director, Electronic Systems & Signals Research Laboratory
Introduction to the Center for Security Technologies

- Washington University Center for Security Technologies
- Example Projects
- Advisory Board
- Conclusions
Center for Security Technologies

Ronald Indeck    Joseph O’Sullivan    Robert Pless
Director           Associate Director   Assistant Director
Washington University and the Center for Security Technologies

Securing our World through Technology

- Washington University
  - *USNWR*: ranked 9th nationally, top 10 in endowment
  - 8 Schools: Medicine, Social Work ranked in the top 3

- CST
  - interdisciplinary academic research center (5 schools)
  - built on existing strengths in security research
CST Mission

To advance research in basic science, mathematics, and engineering in those areas which can most directly improve security including:

• physical aspects of security (intrusion detection, border security, biological and chemical substance identification)

• information aspects of security (networking, searching of massive databases, and information theory)

• law, economics, public policy

and to transfer these technologies into practice
CST Scope

• First interdisciplinary security research center
  – 50 faculty from five schools
  – More than cybersecurity
  – More than counterterrorism
    • A variety of ‘attacks’ including natural disasters
  – Integrate research
    • Through projects and testbeds
    • Across disciplines, schools
    • Sensors → Processing → Systems Integration → Technology Transfer

• Synergy between technology and policy
  – Privacy/public policy as ‘design criteria’
Center for Security Technologies

Broader Vision

• Planned and Unplanned Events
  – Event detection: technology
  – Event classification: science
  – Coordinated response: science, technology, and policy

• The Role of Academics
  – Science and technology research and development
  – Role of policy, economics, law
CST Research and Applications

• Sensors through signal processing to implementations
• Security of food, water, access, network, borders
• Information awareness
• Synergy between technology and policy
• Systems integration leading to technology transfer
CST Goals

- Establish critical mass in security technologies
- Address fundamental scientific and engineering issues
- Integrate economic and privacy issues
- Manage many complementary projects
- Realize widespread applications
- Transition University technology into practical use
- Guide standards and impact policy
- Build synergy between WUSTL, region, and nation
Knowledge Dissemination

- Peer-reviewed publications
- Conference presentations, publications
- Industry and government meetings
  - Individual
  - Group or small conference
- Patents and licensing
- Contracts to work with industry
- Formation of new companies
Example Project: Magneprint

• Scientific measurements in late 1980’s
  – Repeatability of magnetic noise
  – Papers published
  – Range of applications identified; patents

• Use in magnetic recording
  – Novel recording technologies to exploit microstructure; papers and patents
  – Eventually reached no commercialization

• Use in combating credit card fraud
  – Patents
  – Partner with Magtek
  – Chips and systems developed at Washington University
  – Successful field trials in Malaysia; potential world-wide
  – Extensions: identification cards, container security
A bit about Bytes

• 1’s and 0’s: a trim alphabet
• bits and Bytes: usually 8 bits/Byte
• kilo, Mega, Giga, Tera, Peta, Exa: $10^3$
  – kilobyte: printed page of text
  – Megabyte: novel
  – Gigabyte: movie
  – Terabyte: US library of Congress
  – Petabyte: all US academic research libraries
  – Exabyte: every word produced by humans
Massive Data

- Storage industry will ship 6,000,000,000,000,000,000,000 Bytes this year;
  - Cost decreasing ~3%/week;
- MasterCard recently installed 200 TBytes of disk;
- Humanoids have produced 12 Exabytes over the past ~30,000 years
  - Next 12 Exabytes in just over a year!
Application: Intelligence Data

• Lots of data
  – US intelligence collects data equaling the printed collection of the US Library of Congress every day!

• Changing constantly

• Many perturbations
  – Osama, Osamma, Ossamma, . . .

• Query and field types aren’t known \textit{a priori}
Application: Image Databases

Challenging database

- Massive data sets
- Unstructured
- Don’t know what we need to look for in each picture
Project Status

- DSSI Formed in 2003
- Housed in Center for Emerging Technologies
- http://www.datasearchsystems.com/
CST External Advisory Board

Mr. Earle Harbison (retired President and COO, Monsanto), Chair
Dr. Massoud Amin (Director of Infrastructure Security, EPRI)
Dr. Allen Atkins (Vice President, Boeing)
Dr. Tony Cantu (Chief Scientist, US Secret Service)
Mr. Scott Charney (CSO, Microsoft)
Prof. Jerry Cox (Senior Professor, Washington University)
Col. Tim Daniel (Director, Missouri Office of Homeland Security)
Mr. Will Eatherton (Chief Architect, Cisco)
Mr. Richard Fleming (CEO, RCGA)
Mr. Jerry McElhatton (President GTO, MasterCard International)
Dr. Sharon Nunes (Vice President, IBM)
Mr. Joe Leonelli (Vice President, Veridian Systems)
Gen. Tony Robertson (retired AF)
Dr. Don Ross (Chairman, Ross and Baruzzini: Cernium)
Dr. Robert Thibadeau (CSO, Seagate Technologies)
Hon. William Webster (retired Director, CIA and FBI)
Prof. Murray Wedeinbaum (Washington University)
U.S. officials say Osama bin Laden is posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites.

(AP News)
Steganography in Text

We start with plaintext:

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.
and apply a word shifting algorithm:

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.
Steganography in Text

... and uncover:

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.

... explore the world wide web ...
Steganography in Pictures

Renoir
Covert Data

Long-range Aviation Airfield
‘Composite’ Image
Undetectable (unless aware)
Digital Fingerprinting and Traitor Tracing

• Digital fingerprinting
  – Authenticate
  – Who bought/sold/...
  – Printers/copiers

• Mark copies to find out where the data are being compromised
Bootleg copies of Oscar-nominated movies showing up on Internet

AP Jan. 14, 2004


– “The Los Angeles Times reported that security features on the tape [Cold Mountain] indicated that it belonged to Ivan Kruglak, an academy member and president of a wireless data communications company.” AP Jan. 15, 2004

– Fingerprinting based on Philips Research Lab Technology
Oscar Bootlegs 2004

- Fri Jan 16, 2:12 AM ET By Gregg Kilday and Paul Bond (Hollywood Reporter)
- FBI confirmed involvement
- "Illegal copies ... have been traced ... to character actor Carmine Caridi, a member of the Academy of Motion Picture Arts and Sciences"
- "It was a pretty professional job... all visible markings were removed."
- "This year the screeners carried invisible markings for the first time; the studios were able to identify the Academy member for whom they had been intended."
Consider . . .

This process can perfectly hide data so that no one, not even the ‘good guys’, can find it.

What about teens and music ‘sharing’?
The Balancing Act Between Privacy and Security

- Information Searches: Security and Privacy
- Information Hiding: Steganography and Copyright Protection
- Cameras and Sensing
Policy Analysis

Understanding the Liberty/Security Space
- Tradeoffs between liberty and security?
- Plot the space
Policy Analysis

Where is a given policy with respect to a theoretically optimal frontier?
Policy Analysis

• Implications for new technologies?
  - Some offer more “L” or more “S”
  - What if we offer BOTH?
  - Use this as a design criterion!
  - CST Examples

The CST is doing for security what imaging has done for medicine
Information

- Generation and storage
- Transmission
- Securing of information
  - ... security ↔ privacy
Satellite Data

- Low orbit fly-over every 90 minutes
- Look for *differences* in images
  - Large objects
  - Troops
  - Changes to landscape
- Flag, transmit these differences immediately
- National Reconnaissance Office
- City assessors . . .
How do we find what we’re looking for most effectively?!
Task: Search all Books in the Library for a Particular Word

Process:
• Transfer books to home
• Read each one
• Keep those interested
• Go get more books . . .
To find what we’re looking for most effectively . . .

. . . push the request to the data!
Dramatic Performance Gains – 200x (per device)

- Security & intelligence
- Medical & genomics
- Internet & search engines
- Unstructured data: Text, images & signals
- Personal & server computers
Example: The Case of Maury Travis

Suspect in over 20 murders
Sent map to Post-Dispatch
Contacted Expedia (M’Soft)
ID’ed IP address
Contacted MCI-Worldcom
Tailed him . . . Apprehended!

Per Sgt. Muffler
Questions:

• Who has access to these data?
  – Who grants access?
  – Can we search blindly *then* obtain court order?

• Consider medical records:
  – Can be an incredible medical research tool
  – Can be ‘useful’ for insurance actuaries
Data Transmission

• 120 TBytes/sec internet peak rate
• 120 PBytes/month Internet
• 100 PBytes/month telephone
What’s the problem?

– Computer virus infections are spreading
  • New virus spreads though email and web

– Copyrights on digital content are violated
  • Rampant sharing of music and videos

– Confidential data are leaking through company networks
  • Trade secrets stolen

– Internet infrastructure is at risk
What needs to be done?

Distinguish between legitimate and illegitimate content
- Stop the illegitimate traffic
- Forward legitimate traffic
- Don’t slow down the network
A Potential Solution:
The Network Watchman

- Electronic postmen
  - direct packets to destination via headers
- Secure network
  - watch headers
  - view payload
  - copy/redirect/stop packets
- Identifies & acts on content in Internet packets without delay
What Can We Do Now?

- Routinely update system software, especially security patches
- Enable your firewall, especially wireless
Concerns

• Who is allowed to read your email or monitor your buying habits?
  – Law enforcement officers? Marketers?
  – Compare to paper mail or telephone; store card purchasing data

• Who controls and supervises this access?
  – Legislature? Public interest groups?
Smart Borders – Smart Cameras
Surveillance in a Dynamic Environment

Conventional motion detection ineffective
Background Model Training

Learning the environment
Anomalous Motion Detection

After 15 seconds of training
X-ray Scanning and Security Imaging

Conventional Transmission
Scanning at Borders/Airports

Low Energy Backscattered

Behavior Analysis
Network of Video Cameras

- Missouri Rapid Screen
- License plate ID system
  - consider sniper case
Thoughts

• Do you want to be in these pictures?
  – It might demonstrate your innocence
  – Ubiquitous covert cameras in watches, cell phones

• Consider the AVID chip
  – Think about cell phone ‘tracking’!
Safe at Home

• Technology expected to (and will!) respond with improved solutions to new threats
  – applies to both planned and natural attacks
• Coordinate with law, privacy, economics, and public policy
  – expect that reason will be applied
THANKS!
... many other doors at WUSTL!