Securing the Open Softphone

Kickoff Colloquium
September 1, 2010

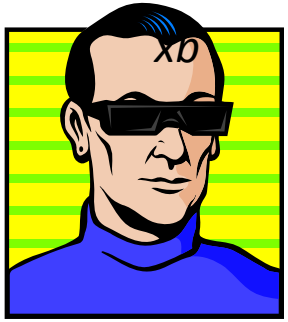
Brain Teaser 1

Brain Teaser 2

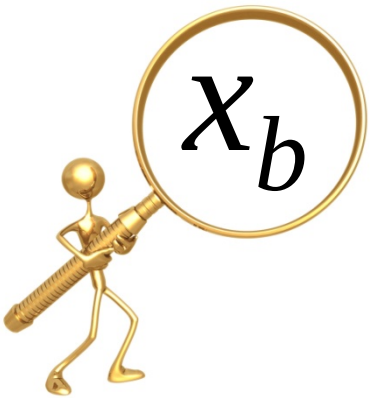
1. Alice chooses two reals by an unknown process

$x_0 < x_1$

2. Bob chooses a uniformly random bit b



3. You get only x_b



Your goal: guess b with probability better than 50%

What's the Problem?

- Wallpaper apps on Android Market are found to be gathering phone numbers, subscriber ID, etc, and transmitting to an unknown server registered in China
- Thieves steal your car and GPS and use it to find your home, stealing your other car
- Hackers plant malware in Windows Mobile games that make expensive calls to Somalia

FLEXISPY

Protect Your Children | Catch Cheating Spouses

FlexiSPY Direct OFFLINE

Home | Features | Phones | Demo | Support | Community | Reseller | Affiliates | About Us | Cart

Is Someone Keeping Secrets from You?
Reveal All with the Worlds Most Powerful Spyphone

- Download FlexiSPY spyphone software directly onto a mobile phone and receive copies of SMS, Call Logs, Emails, Locations and listen to conversations within minutes of purchase.
- Catch cheating wives or cheating husbands, stop employee espionage, protect children, make automatic backups, bug meetings rooms etc.
- Learn all about FlexiSPY. Still have questions, try Live Chat who are waiting to help

FLEXISPY - PRO - X

PRO-X | FULL DETAILS | Supported Phones

TOP OF THE RANGE SPYPHONE

- Listen to actual phone calls
- Use as a secret mobile gps tracker
- Includes all PRO features
- Change phones as often as you like
- Symbian, Windows Mobile & BlackBerry

ORDER NOW: **$349.0** (per year)

LEARN ABOUT SPYPHONE FEATURES HERE — Buy Now

NEW FLEXISPY iPhone

iPhone | FULL DETAILS

Worlds Most powerful iPhone spy phone

- Secretly read SMS, Email, Call Logs
- Track location on map
- Make secret spy calls
- BASIC version from $ 39.99

ORDER NOW: **$349.0** (per year)

Buy Now

FLEXISPY - PRO

PRO | FULL DETAILS | Supported Phones

MID RANGE SPYPHONE

- Spyphone to bug a room or person
- Read their SMS, EMAIL and Call Logs
- BUY NOW for Instant Download
- Change phones as often as you like
- Symbian, Windows and Blackberry

ORDER NOW: **$249.0** (per year)

ALL YOUR QUESTIONS ANSWERED HERE — Buy Now

NEW FLEXIRECORD

RECORD | FULL DETAILS

RECORD SPYCALLS ON A PC

- Automatically records SPY calls to PC
- Ideal companion to any PRO or PROX
- Control multiple target directly from PC

ORDER NOW: **$249.0** (one time)

Buy Now

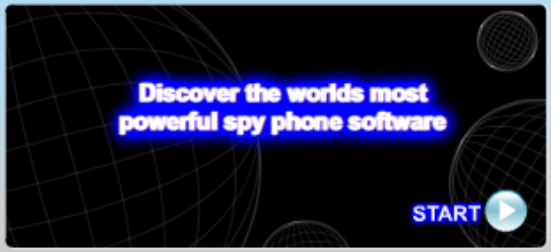
FlexiSPY Android Community Edition

FREE Android Spy Phone software lets you secretly read Call Records, SMS Messages and GPS locations

ready to get started?
FREE DOWNLOAD

Visit the new Flexispy Forum

TWITTER
DO YOU FOLLOW ME?



HOW CAN FLEXISPY HELP YOU

- UNCOVER Employee espionage
- CATCH cheating husbands and cheating wives
- TRACK THEIR location using GPS
- PROTECT your children from SMS abuse.
- ARCHIVE all your own SMS for the future.
- SAVE your call history.
- BUG Meeting rooms and CHECK babysitters
- Ten Day MONEY BACK GUARANTEE

Winners Choose FlexiSPY

Softphone

- Mini laptop/netbook
- +….
- Powerful sensors

Location (GPS)

Motion (Accelerometer)

Camera

Microphone

Compass

How bad could it get?

- Bring down 911 systems?
- Blind air traffic control?
- Facilitate espionage?

Friend or Foe?

What's the good news?

- We have an opportunity for clean-slate development of softphone security
- Softphone platforms are nascent and relatively fluid architecturally
- New modalities to leverage in support of security
  - Physical proximity
  - Mobility
  - Rich sensor data stream

Overview

User Security and Privacy

System Security

Attacks on the Hardware

Protecting User Privacy

Authentication

Attack Detection

Incentives

User Security and Privacy

- **Attacks on the Hardware**
  - *Securing the Hardware*
    - Avoid creating side channels, design of hardware with built-in attack detection – M. Karpovsky
  - *Hardware Hardened Modules*
    - Preventing side channel leakage – L. Reyzin
  - *Managing Leakage*
    - Exposure-resistant cryptography – L. Reyzin
- **Protecting User Privacy**
    - Secure, distributed sensing – N. Triandopoulos

User Security and Privacy

- **Leveraging Sensing to Authenticate**
  - *Sensor-Based*
    - Sensor-generated secrets – L. Reyzin
  - *Proximity-Based*
    - Sensor-based proximity verification – L. Reyzin, D. Starobinski, and A. Trachtenberg

System Security

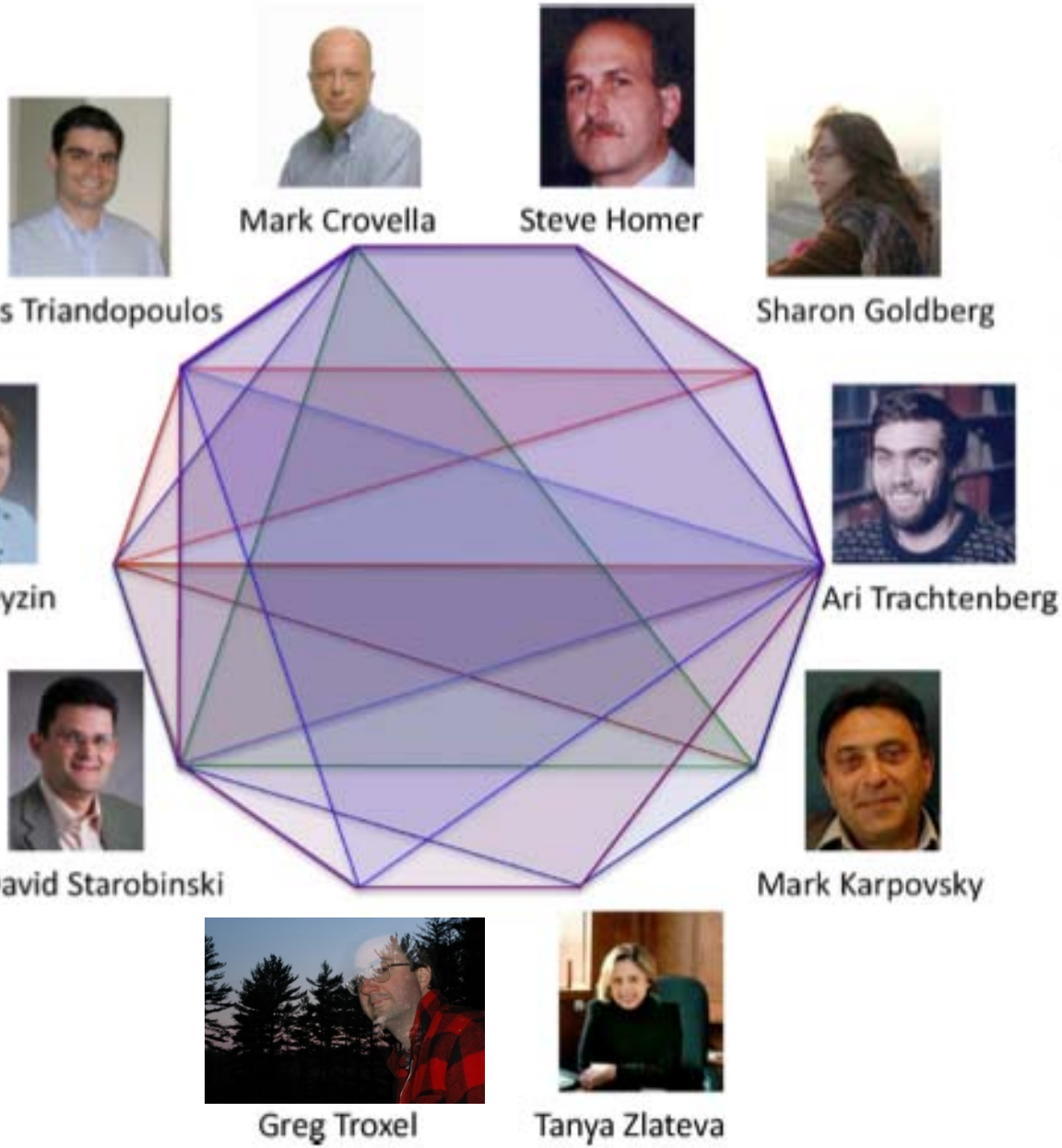
- **Attack Detection**
  - *Physical Layer, esp SDR*
    - Analyzing SDR threats – M. Crovella, D. Starobinski, G. Troxel
  - *Statistical Attack Detection*
    - Crowd-sourced attack detection – M. Crovella
- **Advanced Authentication**
  - *Code authentication*
    - Resilient over-the-air programming – A. Trachtenberg and D. Starobinski
  - *Data authentication*
    - Distributed data authentication – N. Triandopoulos

System Security

- **Economics**
  - *Economics and security impact of spectrum management*
    - D. Starobinski
  - *Incentive-compatible traffic control*
    - Protocol design – S. Goldberg
  - *Economic approach to unwanted traffic*
    - Attention bonds for spam suppression – S. Homer

A Unique Team

- All *nine* of the principal investigators are faculty members at Boston University
  - Very rare to have such a broad and deep collection of expertise under one roof
- Cross-cutting collaboration between
  - Computer Science,
  - Electrical and Computer Engineering, and
  - Metropolitan College Computer Science



Proposal Areas

§2.1.1 Hardware attacks
§2.1.2 User privacy
§2.1.3 Leveraging sensing

§2.2.1 Detecting attacks
§2.2.2 Preventing attacks
§2.2.3 Aligning incentives

§3.1 Curriculum development
§3.2 External collaboration

Collaborators

- **Raytheon BBN Technologies**
  - Experts in software defined radio
- **University of Warwick**
  - Digital forensics, malware propagation, formal modeling

- **Deutsche Telekom**
  - Major handset vendor (T-Mobile) and network service provider
  - Extensive security experience

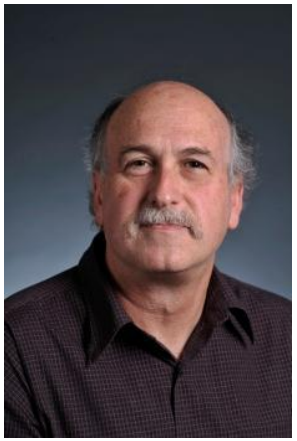
Mark Crovella

Professor
Computer Science Department
College of Arts and Sciences
http://www.cs.bu.edu/fac/crovella

Research Interest

- Performance evaluation
- Parallel and networked computer systems
- Internet measurement and modeling
- Self-similarity and heavy-tailed distributions in network traffic

Steven Homer



Professor
Computer Science Department
College of Arts and Sciences
http://www.cs.bu.edu/fac/homer

Research Interest

- Theoretical computer science
- Complexity theory
- Quantum computing
- Learning theory
- Parallel and probabilistic algorithms

Sharon Goldberg

Assistant Professor
Computer Science Department
College of Arts and Sciences
http://www.cs.bu.edu/fac/goldbe

Research Interest

- Network Security

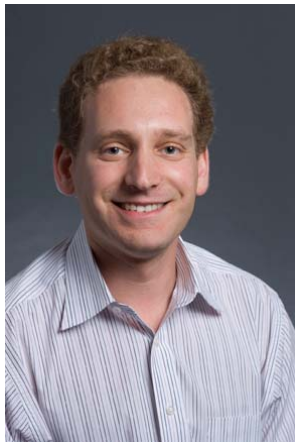
Mark Karpovsky

Professor
Electrical and Computer Engineering
College of Engineering
http://mark.bu.edu

Research Interest

- Design of secure cryptographic devices and smart cards
- Routing in interconnection networks design and protection of cryptographic devices
- Fault-tolerant computing
- Error correcting codes
- Testing and diagnosis of computer hardware

Leonid Reyzin



Associate Professor
Computer Science Department
College of Arts and Sciences
http://www.cs.bu.edu/fac/reyzin

Research Interest

- Cryptography

David Starobinski

Associate Professor
Electrical and Computer Engineering
College of Engineering
http://people.bu.edu/staro

Research Interest

- Wireless networking and security
- Network economics
- Stochastic Processes
- Algorithms

Ari Trachtenberg

Associate Professor
Electrical and Computer Engineering
College of Engineering
http://people.bu.edu/trachten

Research Interest

- Error correcting codes
- Security and algorithms
- Data synchronization
- Location detection
- Sensors, PDAs, smartphones

Nikos Triandopoulos

Research Assistant Professor
RISCS Center and Computer Science
http://www.cs.bu.edu/~nikos

Research Interest

- Information Security & Privacy
- Network Security
- Distributed System Security
- Secure Protocol Design

Tanya Zlateva

Associate Professor
Computer Science Department
Metropolitan College
http://people.bu.edu/zlateva

Research Interest

- Computational Modeling of Visual Perception, Recognition, Three Dimensional
- Representations of Object Shape, Parallel and Distributed Processing

Integrated Security

- **Economics**
  - Metadata (MC)
  - Cost for inconvenience (DS)
- **Hardware**
  - High costs for security (MK)
  - Can sensor mitigate costs? (AT)
- **Network and System Level**
  - Crowdsourcing anomaly detection (MC)
  - Smartphone as a sensor network (DS)
  - Software-defined radios (GT)

The Promise of Ubiquitous Communication and Computation

- **Unrestrained collaboration in groups large and small**
- **Examples:**
  - Crime-reporting with protection from corruptible authorities (when police are potentially corrupt)
  - Political organizing without (state-owned?) media filters
  - Real-time traffic monitoring
  - Disaster relief
- **Problems:**
  - How do you get valid information
  - In a way that preserves individual privacy
  - In a way that gives people a reason to participate
  - (no privacy $\Rightarrow$ no participation)
  - (no validity $\Rightarrow$ data pollution $\Rightarrow$ no participation)

Privacy - more than confidentiality

- **a general concern, decomposable into**
  - confidentiality of contents of communication (TLS)
  - freedom from traffic analysis (Tor for IP, ?)
  - freedom from query analysis (private information retrieval)
  - confidentiality of location (?)
  - ? (?)

- **softphone-related particular challenges**
  - location, location, location!
  - always-with-human and multifaceted (entertaintment/payment/work/play/love): surveillance like never before

Information Reliability & Integrity

Also a general concern with various aspects:

- **Validity of reports or shared informa**tion
  - reputation-based, ground-truth checkable,...
- **User authentication**
  - using password, sensors, proximity, anonymous credentials,...
- **Reliable distributed data management**
  - p2p-based, best-effort vs. 100% accuracy,...
- **Dynamic group formation**
  - based on user registration/revocation, access controlled,...

- **Non-solution for <u>any</u> of the above:**
  - Register every cell phone to a name, punish for bad communication

What's different (given all this prior work)

- **Promises** (not available on PCs):
  - *High mobility*
  - *Opportunistic networking*
  - *Rich sensing*
  - *Always-on*
  - *Peer-to-peer* (wifi/bluetooth) and infrastructure mode

- **Challenges** (not the same as PCs):
  - *Computing constraints* (e.g., for evaluation of sensory data or running heavy protocols): memory, speed, power
  - *Fixed protocols* at the phone network layer that are both privacy unfriendly and insecure
  - *Central control* (large companies/government regulation) that may be unaligned with user incentives