BOSTON
UNIVERSITY

Cyber Security Research Projects at BU

Presented by Azer Bestavros

Professor and former Chair of Computer Science
Director of Hariri Institute for Computing
Founding Member of RISCS

June 20, 2011

Broad Security-Related Research

- Foundations of Cryptology and Information Theory
- Quantum Computing and Complexity
- Formal Specification and Verification Methods
- Safe Programming Languages and Software Certification
- Cryptographic Security and Privacy Protocols
- Trusted Hardware Architectures
- Economics Inspired Computing and Mechanism Design
- Internet Architectures and Protocols
- Cloud Computing and Virtualization
- Internet and Web Traffic Measurement and Modeling
- Data Mining and Machine Learning
- Social Network Analysis and Mining

Example Research Projects (~$3M/yr)

- Formal Verification of Software and Networks [Kfoury & Bestavros]
- Memory-Safe Programming Languages and Software [Xi & West]
- Distributed Spatial Anomaly Detection [Crovella]
- Low-Rate Network Exploits [Bestavros & Matta]
- Attack Resistant Cryptographic Hardware [Karpovsky & Tobin]
- Data Authentication for Outsourced Databases [Kollios & Reyzin]
- Anonymous Peer-to-Peer Overlays [Bestavros & Goldberg]
- Market-Based SPAM Management [van Alstyne]
- Privacy-preserving Mining of Social Networks [Terzi]
- Towards Composable Security Analysis [Canetti]
- Secure BGP Routing [Goldberg & Reyzin]
- Clean-Slate Internet Architectures using RINA [Matta]
- Securing the Open Softphone [Crovella et al]
- Trustworthy Cloud Computing [Bestavros et al]

Formal Verification of Software and Networks [Kfoury & Bestavros]

- ***Motivation & Goals:*** Ensure overall security while meeting component security properties

- ***Approach & Results:*** Design Domain-Specific formal Languages to
  - Encapsulate safety properties
  - Support compositional/scalable verification
  - Applied to real-time & QoS properties of cyber-physical systems and flow networks

Safe Programming Languages and Software [Xi & West]

- ***Motivation & Goals:*** Enhance security by making software artifacts less vulnerable to program exploits

- ***Approach & Results:*** Develop "safe" programming languages and execution environments that are not vulnerable to attacks through software exploits
  - Provably ensure memory safety
  - Enable programmers to assert security properties
  - Enable verification of asserted security at compile time
  - Applied to development of device drivers (using ATS) as well as to virtualization environments (using sandboxing)

Distributed Spatial Anomaly Detection [Crovella]

- ***Motivation & Goals:*** Detect Internet Traffic Volume Anomalies

- ***Approach & Results:*** Leverage observations at multiple locations based on following principles:
  - Avoid global communication and centralized control
  - Augment current parametric anomaly detection methods with non-parametric methods
  - Annotate anomalies with probabilistic quantifier of its importance, (not just identify possible anomalies)
  - Used effectively for Internet – basis for “Guavus” startup

Low-Rate Exploits of Network Dynamics [Bestavros & Matta]

- ***Motivation & Goals:*** Harden systems and networks against stealthier DoS and RoQ attacks that exploit protocol dynamics

- ***Approach & Results:*** Develop signatures for low-rate attacks and study vulnerability of multiple protocols
  - Used control theory to define and evaluate exploits of network and system adaptation dynamics
  - Applied to attacks mounted against congestion control, admission control, load balancers, virtual machines, among others

Attack Resistant Cryptographic Hardware [Karpovsky & Tobin]

- ***Motivation & Goals:*** Transactions are moving into open and mobile environment, resulting in new threats and attacks

- ***Approach & Results**:* Design secure, low-cost, low-power special-purpose hardware devices based on asynchronous fine grain pipelining and robust encoding of data, resulting in
  - Unique tools for secure hardware design
  - Best performance per Watt
  - Multiple fault injection attack tolerance

Data Authentication for Outsourced Databases [Kollios & Reyzin]

- ***Motivation & Goals:*** Enable clients at the edge of an untrusted cloud to access and query the data efficiently, while getting assurance of integrity

- ***Approach & Results**:* Several new approaches are proposed, and analytically and experimentally studied
  - Solutions extend existing indexing structures (e.g., using Merkle Trees)
  - Applied to a range of DB query processing forms, including range queries
  - Shown to work very well even for very large datasets

Anonymous Peer-to-Peer Overlays [Bestavros & Goldberg]

- ***Motivation & Goals:*** P2P structured overlays could be potentially used to enhance secure communication and circumvent censorship technologies

- ***Approach & Results*:** Identified potential (Zenith) attacks against P2P overlays targeting popular content and developed appropriate, efficient defenses
  - Techniques tested on multiple DHT structured overlays
  - Novel DHT lookup protocols that are immune to Zenith attacks have been developed and tested
  - Trustworthy resource discovery in P2P overlays without reliance on a centralized trust authorities

Market-Based SPAM Management [van Alstyne]

- ***Motivation & Goals:*** Apply economic rather than technological or regulatory screening to manage SPAM

- ***Approach & Results:*** Instead of just blocking SPAM, recognize and promote valuable communication and provide feedback to spammers and users
  - Shift focus away from the information in the message to the information known to the sender
  - Use principles of information asymmetry to cause the spammer to incur higher costs than senders of legitimate information
  - Often outperforms "perfect" filter

Privacy-preserving Mining in Social Networks [Terzi]

- ***Motivation & Goals:*** Information leakage through social networks threatens privacy even in the presence of privacy controls

- ***Approach & Results:*** Develop models and analysis techniques to evaluate and counter the threats to privacy from "second hand" information leakage
  - Developed and tested techniques to recover information from randomized social network graphs
  - Developed and tested a framework for computing the privacy score of users in online social networks
  - Developed identity anonymization techniques for social nets

Composable Security Analysis [Canetti]

- ***Motivation & Goals:*** Combining individually-secure protocols may result in new vulnerabilities; need systematic approach to decide on composable securit
- ***Approach & Results:*** Study conditions and limitations of composability of cryptographic constructs. Research includes
  - Universal composability with global set-up
  - Composability of cryptographic protocols
  - Trading off soundness, simplicity and efficiency
  - Application to software obfusctation

Secure BGP Routing on the Internet [Goldberg & Reyzin]

- ***Motivation & Goals:*** Routing remains the "weakest link" on the Internet due to the lack of authentication of route advertisement in BGP

- ***Approach & Results:*** Develop new secure BGP protocols that are provably correct and study approaches to their deployment
  - Showed security vulnerabilities in many proposed S*BGP protocols and developed alternatives
  - Studied market-driven approaches to the deployment of S*BGP on the Internet

Clean-Slate Internet Architectures using RINA [Matta]

- ***Motivation & Goals:*** Security is an after tought in current Internet architecture – plugging holes is hopelessly inadequate; need clean-slate design

- ***Approach & Results:*** Adopt RPC as the main and only building block for Internet protocols and services, which can be recursively constructed
  - No standard protocols or naming convention
  - Security is tailored for each application
  - Approach demonstrated for applications in mobile and wireless settings

Securing the Softphone [Crovella ++]

- ***Motivation & Goals:*** New smart phones are increasingly open and easily susceptible to exploits due to ubiquity of "apps" and of multi-channel communication

- ***Approach & Results:*** Develop a multi-pronged approach using clean-slate designs
  - Hardens the physical layer (hardware)
  - Develop incentive-compatible protocols
  - Develop centralized and distributed defenses

Trustworthy Cloud Computing [Bestavros ++]

- ***Motivation & Goals:*** Cloud computing introduces opportunities and challenges for security – need to make security an integral part of cloud SLAs

- ***Approach & Results:*** Develop expressive SLAs and associate delivery and validation mechanisms to enhance trust in cloud interactions, including
  - Ability to check data integrity and consistency
  - Develop SLA mechanisms for fair market valuation
  - Develop protocols for safe SLA transformations for automated service colocation, negotiation, and optimization

BOSTON
UNIVERSITY

Cyber Security Research Projects at BU

Discussion