Research in Information Assurance & Cyber Security
Dept. of Electrical & Computer Engineering

Thomas J. Watson School of Engineering and Applied Science
Binghamton University, State University of New York
Binghamton, NY 13902

December 2015
Department Research Areas

**Controls & Laser Comm**
- V. Nikulin
- V. Skormin
- E. Wu

**Info Security**
- Y. Chen
- S. Craver
- J. Fridrich
- V. Skormin
- L. Guo
- M. Kirchner
- D. Summerville

**DSP & Comm**
- M. Fowler
- E. Li
- S. Zahorian

**Computer Design**
- Y. Chen
- Z. Jin
- D. Summerville

**Micro- & Opto-Electronics**
- S. Choi
- D. Klotzkin
- A. Rastogi

**Power & Energy**
- T. Dhakal
- A. Rostogi
- E. Wu
- Z. Zhang
- N. Zhou
Yu Chen: Intelligence Measure of Cognitive Radio Networks

(In Collaboration with Prof. Edward Li)

- **Goal:** to construct a CRN intelligence model from the Cattell-Horn-Carroll human intelligence model
- **Cognitive Radio Networks (CRNs)**
  - In order to resolve the impending spectrum shortage problem
  - Achieve extremely high spectrum efficiency and guarantee the peaceful coexistence with legacy systems
- **Cognitive capabilities and intelligence are vital**
  - They are necessary for optimizing spectrum efficiency and guaranteeing safe coexistence in the presence of the spectrum uncertainty
  - Their quantitative study is still largely an open area
- **Task:** Collective IQ-based Denial-of-Service (DoS) attack immunity
  - Prompt anomaly detection using sequential (quickest) change-point detector
  - Adaptive spectrum assignment decision making engine
Yu Chen: Mission-Critical Urban Surveillance in Fog

- **Smart City: an Attractive Proposition**
  - The Internet makes the city connected
  - The Internet of Things (IoT) makes the city sentient
  - Situational awareness (SAW) makes the city smart
    - Efficient information abstraction
    - Instant decision making

- **Fog Computing vs. Cloud Computing**
  - Mission critical applications are latency sensitive
    - Cloud is far away, but Fog is on the ground

- **Main Challenges**
  - Addressing the gap between the large amount of dynamic data and limited computing resource available at the network edge
  - Enabling a homogeneous paradigm through “softwareisation” of hardware built at the edge of the networks
  - Supporting instant decision making by elastically orchestrating the tradeoffs between resource utility efficiency and Quality-of-Service requirements
An insider modifies a biometric database so that an attacker can impersonate a target user.

In the simplest case, we can overwrite user’s data with attacker’s data, but this simple attack has side-effects:

- Target is no longer recognized by system.
- Attacker is conspicuously misclassified.
- Attach extra mode to user B in database
- Mode matches to user A only when signal is conspicuously modified (sidestep)
- Attacker can now trigger misclassification only when desired.
Sidestepping Attacks on Biometric Databases

Scott Craver, Alireza Farrokh baroughi, Kenneth Weimer · EECE department, Binghamton University

Code from OpenCV to “train” a face recognizer with local binary pattern histograms

```cpp
void LBPH::train(InputArrayOfArrays _in_src, InputArray _in_labels, bool preserveData) {
    // ...
    for(size_t sampleIdx = 0; sampleIdx < src.size(); sampleIdx++) {
        // calculate lbp image
        Mat lbp_image = elbp(src[sampleIdx], _radius, _neighbors);
        // get spatial histogram from this lbp image
        Mat p = spatial_histogram(
            lbp_image, /* lbp_image */
            static_cast<int>(std::pow(2.0, static_cast<double>(_neighbors)) ),
            _grid_x, /* grid size x */
            _grid_y, /* grid size y */
            true);
        // add to templates
        _histograms.push_back(p);
    }
}
```

They just dump all the histograms into a user’s database entry
Sensor fingerprint

- Origin: formed by small differences among pixels (size, silicon homogeneity, circuitry)
- Unique: specific camera or sensor
- Universal: CCD, CMOS, Foveon, scanners, …
- Robust: Survives processing (natural “digital watermark”)
- Technology transfer: BU algorithms → PAR, Inc. SW → FBI (used in court and intelligence gathering)
Steganography
- Seeing is not believing. The image on the right contains a 230kB PDF document encoded by slightly changing the pixel colors.
- Hiding information can be used for security and privacy and intellectual property protection.
- We study the fundamentals – how much information can be safely hidden (uncompressed and JPEG formats).

Steganalysis
- Discovering the presence of secretly-hidden data, reading the message.
- Synthesis of signal processing and artificial intelligence (machine learning).
- Developing reliable steganalysis methods is important for homeland security, law enforcement, and forensic analysts.
- Main challenge: porting the techniques from lab to real world.
Dr. Linke Guo’s Research

- Security and Privacy in Social Networks
  - Secure Content Sharing and Trust-based Friend Recommendation in Mobile/Online Social Networks
  - Privacy-preserving Location-based Services
Dr. Linke Guo’s Research

- Security and Privacy in Healthcare
  - Privacy-preserving Computation Outsourcing and Verification in Cloud-based Healthcare Monitoring
  - Attribute-based Privacy-preserving Authentication in eHealth/mHealth System

Mobile Health Monitoring System
Is this image real or fake?

Photo: Bernd Busche

floor
trees
metro
station

scaling peaks
JPEG compression peaks
Digital Media Forensics (Prof. Kirchner)

- Assess the *integrity* and *authenticity* of digital media based on a small set of working assumptions

- Rapidly growing research field at the intersection of *signal processing*, *machine learning* and *information security*

**Research Activities:**

- Understand media forensics in a broad context; explore and leverage relations to fields like security, privacy, computer vision, computer forensics, …

<table>
<thead>
<tr>
<th>End-user authentication</th>
<th>Forensics-enhanced smartphone apps</th>
<th>Media Anonymization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor end-user authentication schemes based on smartphones’ inherent physical properties</td>
<td>Enrich or generate media data such that it provides forensically relevant data for later analysis</td>
<td>Anonymization of media shared online in times of “big data” (journalism, whistleblowing, …)</td>
</tr>
</tbody>
</table>
FA-9550-12-1-0077, $2.2M
SEMANTIC APPROACH TO BEHAVIOR-BASED IDS AND ITS APPLICATIONS

PI: Victor Skormin, Research Scientist: Andrey Dolgikh

Monitoring

Aggregation

Graph Compression/Functionality Mining

Functionality Analysis

Cyber Physical System

System Events

Event Graphs

Functionalities

Completed Research

Target Acquisition

Detection of malicious Insider

Detection/mitigation of anomalous hardware operation

Navigation

SCADA Security Attack mitigation

PLC attack

Machinery

Computers

Operators

vskormin@binghamton.edu
Security Approach for Industrial Control Systems

PI: Victor Skormin, Research Scientist: Andrey Dolgikh

Networked computers implementing a fixed set of legitimate programs

System call data

Functionality extraction

Frequency, executions/minute

Customized normalcy profile

Extracted functionalities

Abnormal profile indicative of attack

Extracted functionalities

Figure 4. Industrial Control Security Testbed Diagram
Unfunded research: optimization of a hybridization scheme with a fuel cell

Parameter identification of the model

Fuel Cell
Fuel Cell Model
Genetic Optimization
Optimal Design of the FC

Optimization of the Hybridization Scheme

Simulation model of the hybridization scheme
Load
Electric Drive
Fuel Cell
Super capacitors
Controls
Sensors
Hydrogen supply
Commutation circuits
Power Management Rule
System efficiency criteria
Power management threshold values

Fuel Cell characteristic

Physical Characteristics
Covert Hardware Trojans Implantation, Detection and Prevention -- Douglas Summerville

dsummer@binghamton.edu

Objective: Ensure trusted ASIC/FPGA supply chain free of covert Trojans

Goals:
- Trusted supply chain for FPGA or ASIC designs
- Allow use of COTS tools and IP
- Trust-preserving design techniques.

Accomplishments:
- Automatic implantation of low-impact covert HTHs
- Tool-independent generalized detection methodology without reference design
Ultra-Lightweight Anomaly Prevention for IoT Devices
--Douglas Summerville

dsummer@binghamton.edu

Objective: Strong intrusion prevention for insecure embedded IoT devices

Goals:
• Very small hardware footprint
• High-resolution attack detection
• Automatic deployment

Accomplishments:
• Lightweight anomaly detection with throughputs of 170k packets per second
• Low-area hardware and software implementation
• Integration with Xtables