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

Nov. 07, 2014
Department Research Areas

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

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

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

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

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

- **Power & Energy**
  - T. Dhakal
  - A. Rostogi
  - E. Wu
  - Z. Zhang
  - N. Zhou
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
Real or Fake?

- floor
- trees
- metro
- station

- scaling peaks
- JPEG compression peaks
Real or Fake?
Real or Fake?
Research Interests

- overall interest: reliable and efficient assessment of media authenticity based on a minimal set of working assumptions
Research Interests

- overall interest: reliable and efficient **assessment of media authenticity** based on a minimal set of working assumptions
- understand acquisition/recording processes and resulting artifacts

![Comic strip image](http://xkcd.com/1014)
Research Interests

- overall interest: reliable and efficient **assessment of media authenticity** based on a minimal set of working assumptions
  - understand acquisition/recording processes and resulting artifacts
  - model and detect manipulation artifacts

http://xkcd.com/648
Research Interests

- overall interest: reliable and efficient **assessment of media authenticity** based on a minimal set of working assumptions

  ▶ understand acquisition/recording processes and resulting artifacts
  ▶ model and detect manipulation artifacts
  ▶ inspect and analyze core file structures of different media formats
Research Interests

- overall interest: reliable and efficient **assessment of media authenticity** based on a minimal set of working assumptions
- understand acquisition/recording processes and resulting artifacts
- model and detect manipulation artifacts
- inspect and analyze core file structures of different media formats
- anticipate counterfeiters who attempt to impede ("attack") forensics

2008 Iranian missile test; manipulation, original, "attack"
Research Interests

- overall interest: reliable and efficient assessment of media authenticity based on a minimal set of working assumptions
- understand acquisition/recording processes and resulting artifacts
- model and detect manipulation artifacts
- inspect and analyze core file structures of different media formats
- anticipate counterfeiters who attempt to impede (“attack”) forensics

- the broader picture: explore and leverage relations to fields like security, privacy, computer vision, “big data”, computer forensics, ...
- end-user authentication
- forensics-enhanced smartphone apps
- media anonymization
Recent Student Project

- electrical network frequency of a power grid varies systematically over time
- many mains-powered audio recordings contain a weak ENF signal

- How about recordings made with battery-powered devices?
Forensic Authentication of Digital Media
Prof. Matthias Kirchner

http://ws.binghamton.edu/kirchner

PhD position available!
Digital forensics

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. Software → FBI (used in court and intelligence gathering)

- **Data provenance**
  - Image / video / scan origin (hardware specific)
  - Integrity verification (digital forgery detection)
- **Use fingerprint as a template for processing history recovery**
  - rotation, cropping, scaling, lens distortion correction, digital zoom, …
- **Pixels defects reveal approximately when a picture was taken**
- **Featured in movie “Beyond the Reasonable Doubt” by P. Hyams (Michael Douglas)**
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, privacy and intellectual property protection, but can be misused for criminal activities
• 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
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.
- Demo
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.
Problem: Malicious hardware can be hidden inside of a circuit via selective optimization, allowing production of covert Trojans that are highly resistant to detection.

Objective: Research methods for the detection of malicious optimizations, and thus covert Trojans.

Approach: Mathematically model the methods applied by a well-intentioned optimization algorithm. Develop criteria by which malicious optimizations can be identified.

Outcome: Mathematically-proven methodology for the reliable, automated identification of covert hardware in an optimized circuit.
Generalized Detection Methodology

By enforcing two mathematical principles, we can detect all invalid optimizations- and thus detect Covert Trojan circuits.
Limits of Detection: Implantation of Covert Hardware

Amount of Valid Implementations

Amount of Valid Optimizations

Number of Inputs

Number of Implementations

10^11

10^12

10^13

10^14

10^15

10^16

10^17

10^18

10^19

10^20

10^21

10^22

10^23

10^24

10^25

10^26

10^27

10^28

10^29

10^30

10^31

10^32

10^33

10^34

10^35

10^36

10^37

10^38

10^39

10^40

10^41

10^42

10^43

10^44

10^45

10^46

10^47

10^48

10^49

10^50

10^51

10^52

10^53

10^54

10^55

0

2

4

6

8

10
Yu Chen: Trust, Security and Privacy in Ubiquitous Sustainable & Survivable Computing ($US^2C$) Technology

- **Research Interests**
  - **Network Security**
    - Securing the network using Reconfigurable Hardware Devices
    - Countermeasures against Distributed Denial of Services (DDoS) attacks
  - **Security-oriented Information Fusion using Cloud Computing**
    - Big Data analysis for fast anomaly detection in Telemedicine Cloud and Smart Grid
    - Fault Tolerant and Data Recovery in Cloud Storage
    - Cloud Security Auditing based on Behavioral Modeling
      (collaborating with Prof. Victor Skormin)
  - **Hardware Security in Dark Silicon** (joint work with Prof. Aaron Carpenter)
    - Physical Uncloneable Functions
    - Moving Target Defenses
  - **Adaptive Self-Powered Cyber Infrastructure based on Energy Harvesting**
    - Energy Aware Algorithm for Self-Powered Wireless Sensor Networks in Sustainable Smart Infrastructure
Current Projects

Intelligence Measure of Cognitive Radio Networks (supported by NSF EARS Program)
- Using Cattell-Horn-Carroll human intelligence model to measure the intelligence as a CRN IQ (intelligence quotient) based on psychometrics
- Quantitatively study the Cognitive Capabilities and Intelligence of CRNs
- IQ-based Denial-of-Service (DoS) Attack Immunity

A Secure, Real-Time Resource Provisioning Cloud Architecture for Elastic Information Fusion (supported by Intelligent Fusion Technologies, Inc.)
- Real-time exploitation and information fusion of WAMI (Wide-Area Motion Imagery), FMV (Full Motion Video) are essential for mission critical emergency applications.
- An elastic information fusion cloud is proposed on the container-based virtualization technology.
- Dynamic data driving resource provisioning with near native performance and execution flexibility to compensate for uneven job parallelism.