

Security challenges for the future*

Brian King
Purdue School of Engineering and Tech., IUPUI
briking@iupui.edu

*Supported by the Lily Endowment and IU Pervasive Technology Labs

Security Challenges for the future

The Institute for Information Infrastructure Protection (I3P)* focusing on cybersecurity and information infrastructure research and development has identified key research areas they are:

- Enterprise Security Management
- Trust Among Distributed Autonomous Parties
- Discovery and Analysis of Security Properties and Vulnerabilities
- Secure System and Network Response And Recovery
- Traceback, Identification, and Forensics
- Wireless Security
- Metrics and Models
- Law, Policy, and Economic Issues

**http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf*

Enterprise Security Management

- Pieces of the information infrastructure are operated by single entities yet they are interconnected
- Research needs to continue to study ways to integrate several security mechanisms into a consistent capability for managing both access of resources and the use of enterprises

Trust Among Distributed Autonomous Parties

- Individuals, organizations, and entities need to be able to establish a “relationship over this interconnected world (*cyberspace*)”
- We need to be able to do this without having a resource like a “*trusted central authority*”
- Research needs to continue to focus on methods to provide seamless ways for parties to establish “relationships” over this interconnected world

Discovery and Analysis of Security Properties and Vulnerabilities

- Information infrastructures are LARGE and COMPLEX, pieces of the infrastructures are located in:
 - Hardware Software Firmware Multimedia
- Research needs to continue to focus on understanding the different designs of these information structures—look for design flaws, incompleteness, anything that may lead to understanding their potential security vulnerabilities

Secure System and Network Response and Recovery

- Information infrastructures are complex and large — *response from* and the *ability to recover from attacks* are affected by the size and complexity
- Further research needs to continue on improving their survivability skills and developing proactive intrusion detection

Traceback, Identification, and Forensics

- After an attack has been initiated on a system—the organization needs to make an appropriate response and address this attack—including determining *who, what, where* and *when*
- Research needs to identify improved methods that allow these organizations to trace such attacks

Wireless Security

- Wireless networks have become essential in our ability to deliver services and resources.
- Unfortunately the devices that are interconnected in this wireless world are DIVERSE, such devices include laptops, PDAs, cellular handsets, sensors,
- It is difficult to initiate an *all-in-one solution* to the security concerns that can fit the potential security vulnerabilities when working within the wireless world on “lightweight devices”

Metrics and Models

- We rely on our information infrastructures. To gauge that these infrastructures are adequately protected and secured we need to develop acceptable levels of risk.
 - what are they?
 - don't risks differ for some?
- The basis of these risk levels need to be grounded on well analyzed models and metrics for security and so further research needs to be developed to provide such models

Law, Policy, and Economic Issues

- Decisions affecting the security of information infrastructures are often made in a mind-set in which one either misunderstands or lacks enough complete information concerning the different issues of economics, laws, regulations and government policies
- Research needs to be done to magnify the importance of the cybersecurity problem and the complex relationship of the issues and organizations that affect the protection of the information infrastructure

Some security challenges we are focusing on at IUPUI

- Enabling secure applications
 - Electronic voting & electronic laws—verifiable democracy
- Lightweight security/cryptography
 - Public-key cryptography
 - Key management
- Security applications/securing the delivery of information
 - Secure transmission of images
 - Secure M-commerce

Lightweight security/cryptography

- Network technology advancements like **I-light** have provided greater network connectivity and bandwidth.
- The greater connectivity together + advancements in hardware technology



compute when needed
with whatever computing devices that are available
—no matter how limited

Lightweight security/cryptography

- Today more and more “lightweight devices” devices are required to participate in the computing mainstream
 - Problems arise
 - Resource starved devices
 - Small bandwidth, limited processing, limited storage
 - Devices that were not originally developed for the internet
- Traffic (data) that may not previously have traveled through these communication systems will now frequent them. New vulnerabilities will be introduced.

Lightweight security/cryptography

- Public-key cryptography is needed for exchanging keys, authentication, confidentiality algorithms,
- Characteristics of public-key cryptosystems
 - Larger keys e.g for RSA we should be using 1024 bits
 - Significant more processing
- We look for efficient public-key cryptosystems—as computing becomes more pervasive, more devices are required to support public-key cryptography

Elliptic Curve cryptography (ECC)

- ECC is a **much more** mathematically complex public-key cryptosystem than the integer based (like RSA)
- Why study/why use?
 - Better utilization of resources
 - Key size
 - Bandwidth
 - Processing speed
 - Digital signature generation is faster than RSA
 - Key exchange faster than Diffie-Hellman

Public-key cryptography

key comparison symmetric vs. asymmetric cryptosystems

symmetric key size	ECC over Z_p size of p	ECC over $GF(2^n)$ size of n	RSA modulus size
80	192	163	1024
112	224	233	2048
128	256	283	3072

comparison between RSA and Elliptic Curve Cryptography for comparable security levels

	1024-bit RSA	163 bit ECC
certificate size	over 256 bytes	over 62 bytes
key and signature		
key generation (ms)	285, 630	397
signature generation (ms)	20,208	528
signature verification (ms)	900	1,142

Elliptic Curve cryptography—some recent results from our lab

- New *Galois Field arithmetic* algorithms and a new elliptic curve scalar addition technique using point halving—integral towards achieving the least amount of processing required when using ECC over *Galois Fields*
- New point compression algorithm which is optimal for certain elliptic curves—an integral algorithm to achieve the minimal amount of bandwidth required when using ECC

Security applications/securing the delivery of images

- The research is a collaboration with Paul Salama (IUPUI)
- Typically in an application which requires both compression and encryption, compression will be applied first and then we encrypt the result—in terms of processing we need to visit each member of the bitstream twice
- Our goal was to develop an **efficient secure image encryption** system that will allow one to secure content at a level for which the content demands – dynamically set the security level

Security applications/securing the delivery of images

Input stream to SE BOX



What is Selective Encryption and why it works?



Image 1



Combining



Composite Image



Image 2



What are the benefits of Selective Encryption?

- The result is that we have
 - less bandwidth usage (since we are compressing)
 - Less processing (rather than processing the bitstream twice we are processing bitstream approximately once)
- The result is an efficient method which both encrypts and compresses
- We can increase security if we wish by increasing the amount of data that is encrypted

Conclusion

- Information infrastructures are key resources and need to be protected. Security today plays an important role in providing access to these infrastructures to those that are permitted access, as well as securing the services and enterprises that they support.
- As technology improves, smaller lightweight devices will play an increasingly more important role in the computing mainstream and security will become even more critical.

Lightweight security/cryptography

- Two keys: private key $K_{priv, A}$ and public key $K_{pub, A}$
- Publicizing the $K_{pub, A}$ does not reveal any information concerning $K_{priv, A}$

Lightweight security/cryptography

Two most common applications of public-key cryptography

– ***Key exchange***

- Two or more parties use public key to exchange key to be used use to achieve private communications

– ***Digital signatures***

- user **A** would like to authenticate message **M** this is done by digitally signing **M** with their private key $K_{priv, A}$
- Anyone can verify the signature using the public-key $K_{pub, A}$

Security applications/securing the delivery of information

- Today we rely more and more on having information on-demand
- In the future “lightweight” personal devices would be required to provide the delivery of visual data (images, video, images with text)
- Need to develop methods to secure images that provide good performance in a limited resource environment, without compromising bandwidth

Security applications/securing the delivery of images

- Current state-of-the-art video compression techniques - either *scalable* or *non-scalable*. *Rate-scalable* video compression - permits the decoding of a single compressed video stream at multiple rates, with increasing quality as more data is decoded
- Data elements that affect the perceived quality of the decompressed video the most are placed at the beginning of the data stream. Data elements can be encoded in such a way that the coding of a current data element is dependent on the encoding of prior elements
- By *Selectively encrypting* only those sections of the stream on which the entire stream depends we reduce the amount of processing that needs to be performed on encryption

What is Selective Encryption and why it works?

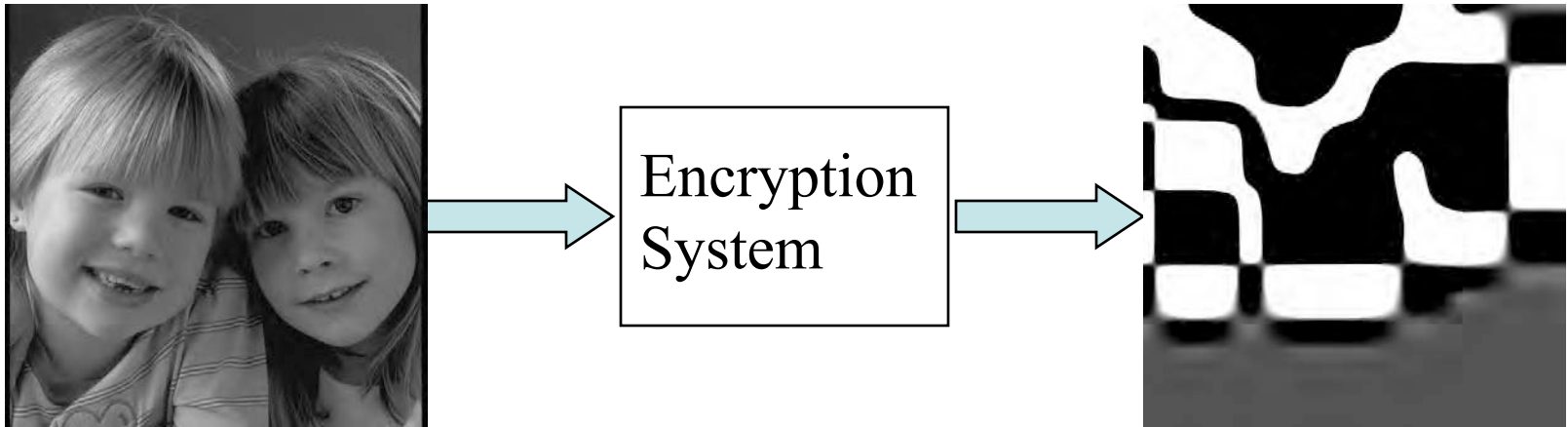
Input stream to SE BOX



When the leading N bits are encrypted

The remaining bits sent in the clear provide no relevant information about original image

What is Selective Encryption and why it works?



Original Image

Unauthorized
Decryption